JEAN-PIERRE SERRE
THOMAS HAGEDORN (réd.)

Topics in Galois cohomology

Cours de Jean-Pierre Serre, tome 11 (1990)
<http://www.numdam.org/item?id=CJPS_1990__11_>

Topics in Galois Cohomology

J-P. Serre, Harvard, Fall 1990

notes by Thomas Hagedorn

Contents

.../

...1

Lecture 1

What is Galois cohomology? What is it good for?

Let K/k be a Galois extension of fields, $[K:k] < \infty$. Let $A(K)$ be a group attached to K (e.g. K^*, $GL_n(K)$) with a $G = Gal(K/k)$ action.

To define $H^i(Gal(K/k), A(K))$ for all i, one must assume that $A(K)$ is abelian. Otherwise, H^i can only be defined for $i = 0, 1$.

$$H^0(Gal(K/k), A(K)) \stackrel{def}{=} A(K)^{Gal(K/k)} \quad \left(\stackrel{usually}{=} A(k)\right)$$

To define H^1, let G be a finite group acting on a group A on the left: $s(a) = {}^s a = s \cdot a$. A 1 cocycle a is a map $G \to A$, $s \mapsto a(s)$ such that $a_{st} = a_s \, {}^s a_t$. Two cocycles a, a' are said to be cohomologous if there exists $b \in A$ such that

$$a'(s) = b^{-1} \, a(s) \, {}^s b. \qquad (1)$$

If a, b are given and a' is defined as in (1), it is a cocycle since

$$\begin{aligned} a'(st) &= b^{-1} \, a(st) \, {}^{st} b = b^{-1} \, a(s) \, {}^s a(t) \, {}^{st} b \\ &= (b^{-1} a(s) \, {}^s b)({}^s(b^{-1} a(t) \, {}^t b)) \\ &= a'(s) \, {}^s a'(t) \end{aligned}$$

$H^1(G, A)$ is the quotient of the 1-cocycles by this equivalence. It is not a group but a set with a basepoint (denoted by 0 or 1).

What is it good for?

By an "object" X, we will mean ① a tensor, ② a quadratic form, ③ an algebra, ④ an algebraic group, as well as some other things. One looks at X over k and considers "K/k forms of X." They are objects X'/k which are isomorphic to X after a base extension from k to K. Galois cohomology classifies K/k forms.

General principle:

$$\boxed{K/k \text{ forms of } X \quad \overset{1\text{-}1 \text{ correspondence}}{\longleftrightarrow} \quad H^1(Gal(K/k), A(K))}$$

where $A(K) = Aut_K(X)$ (e.g. in ①, V vector space, t tensor, $Aut((V,t))$ is the subgp of V fixing t.

in ②, $A(K)$ is the orthogonal group fixing a form
③, " is the automorphisms of an algebra)

Let X, X' be objects, $\varphi: X_K \longrightarrow X'_K$ an isomorphism over K.
If φ is invariant under G, then φ is an isomorphism over k.
For $s \in G$, ${}^s\varphi: X_K \longrightarrow X'_K$ is an isomorphism. Define a 1 cocycle a by

$$\boxed{{}^s\varphi = \varphi \circ a(s)}, \quad a(s) \in \mathrm{Aut}(X_K)$$

$${}^{st}\varphi = {}^s({}^t\varphi) = {}^s(\varphi \circ a(t)) = \varphi \circ a(s) \circ {}^s a(t)$$

$$\| \qquad \Rightarrow \quad a(st) = a(s) \cdot {}^s a(t) \text{ and } a \text{ is a 1-cocycle}$$
$$\varphi \circ a(st)$$

The class of a doesn't depend on the choice of φ ($\varphi \longmapsto \varphi \circ b$, b automorphism), and one must check that this gives the one to one correspondence stated above.

By introducing principal bundles, H^1 can be interpreted as a classifying space.
Let P be the functor $\mathrm{Isom}(X, X')$ for X, X' K/k forms.
$P(K) = \mathrm{Isom}_K(X, X')$ has two different structures.

1. Right action by $A(K)$ makes it a principal homogeneous space
2. Left action by $\mathrm{Gal}(K/k)$

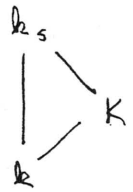
We have $\boxed{X' = P \times^A X}$, $\varphi \in P, x \in X$, $\varphi a \cdot x = \varphi \cdot ax$ for $a \in A$,

Notation: ${}_pX$

a fibre-space with fibre X and H^1 can be viewed as a classifying space

---

Let K/k be a finite extension. Let k_s be the separable closure of k.



$$\underline{\text{def}}: \quad H^1(k, A) = \varprojlim_{\substack{K/k \\ \text{Galois}}} H^1(\mathrm{Gal}(K/k), A(K))$$

Trivial case: $A = \{1\}$, X has "no automorphisms" $\Rightarrow$ every K/k form of $X \cong X$

Quadratic Forms: (Assume char $k \neq 2$) Let $n \geq 1$ be fixed. Two nondegenerate forms of dimension n become isomorphic after extracting at most n square roots. Hence all nondegenerate quad. forms are k_s/k forms.

"Theorem": Isomorphism Classes over k of Nondegenerate quadratic forms over k of dimension n $\xleftrightarrow{\text{Correspond in a 1-1 way}}$ $H^1(k, O(q))$

Similarly,

Isom. classes/k of nondegenerate symplectic forms of dim. $2n$ $\xleftrightarrow{\text{1-1 correspondence}}$ $H^1(k, Sp_{2n})$

Since it is well-known that there is only 1 nondegenerate symplectic form over any k of dimension $2n$ we have shown $H^1(k, Sp_{2n}) = 1$

One can show $\boxed{H^1(k, GL(n)) = 1 \quad , \quad H^1(k, SL(n)) = 1}$

Objects with the same automorphism groups have the same K/k-forms.

Example: 1st object: G_2
2nd object: a Cayley algebra C

$Aut(G_2) = G_2 = Aut(C) \Rightarrow$ G_2 forms correspond to C-forms.

Example: Let X be a smooth projective curve /k of genus 0. After base extension, $X \cong \mathbb{P}^1$. But in general X is not isomorphic to $\mathbb{P}^1$ over the ground field. Let $k = \mathbb{R}$, $k_s = \mathbb{C}$. The curve $x^2 + y^2 + z^2 = 0$ is a curve of degree 0 and is a $\mathbb{C}/\mathbb{R}$ form of $\mathbb{P}^1$.
Now $Aut(\mathbb{P}_1)$ consists of linear transformations $z \longmapsto \frac{az+b}{cz+d}$ and is equal to $PGL_2(k)$. Hence $Aut\, \mathbb{P}_1 = PGL_2$ as a functor.

k-forms of $\mathbb{P}^1$ = curves of genus 0/k $\xleftrightarrow{\text{1-1 correspondence}}$ $H^1(k, PGL_2)$

Now central simple algebras / k of rank 4 (e.g. M_2 2×2 matrices) have PGL_2 as their automorphism group. Every central simple algebra $\cong M_2$ after suitable base extension. Hence, they are classified by $H^1(k, PGL_2)$ and.

Curves of genus 0 / k $\longleftrightarrow$ (1-1 correspondence) classes of quaternion algebras / k.

We give this correspondence explicitly. Let $1, i, j, k$ generate our quaternion algebra with $i^2 = \alpha$, $j^2 = \beta$, $ij = k$, $k^2 = -\alpha\beta$ over k (char $k \neq 2$). Let $q = xi + yj + zk$. $Nq = q\bar{q} = -q^2 = -\alpha x^2 - \beta y^2 + \alpha\beta z^2$. This gives a conic $\alpha x^2 + \beta y^2 - \alpha\beta z^2 = 0$. To show this correspondence is bijective, one has to show that a curve of genus 0 is given by a conic in the plane. The canonical class "K" exists / k and has degree $2g - 2 = -2$. Applying Riemann-Koch to $-K$, one finds a map $X \longrightarrow \mathbb{P}_2$. The image is a conic and every conic can be written in the form above.

It is harder to give the direct correspondence in the other direction.

Severi-Brauer varieties and the Brauer group

The Severi-Brauer variety of dimension n is a k_s/k form of $\mathbb{P}_n$. They are described by elements of $H^1(k, PGL_{n+1})$. By the same argument as before $H^1(k, PGL_d)$ = isomorphism classes of simple central algebras over k of dimension d^2. As a set, $H^1(k, PGL_d) \subset Br(k)$. where the embedding is induced from the maps $H^1(k, PGL_d) \longrightarrow H^1(K, PGL_{dd'})$

$$\alpha \longmapsto \begin{pmatrix} \alpha & & 0 \\ & \alpha & \\ & & \ddots \\ 0 & & \alpha \end{pmatrix}$$

Another Description of $Br(k)$.

Let $G = Gal(K/k)$. $H^2(G, K^*)$ classifies extensions of G by the group K^* (for a given action of G on K^*). Let $\varphi \in H^2(G, K^*)$, and let G act on K^* by $gkg^{-1} = {}^g k$.

Let $1 \longrightarrow K^* \longrightarrow E \longrightarrow G \longrightarrow 1$ be the extension corresponding to φ.

E is generated by K^*, G and multiplication is defined by

$$g \cdot g' = \varphi(g, g') \cdot gg'.$$

Each class mod K^* can be completed by a "0". The direct sum of these is an algebra $\tilde{E}$.
One can show that $\tilde{E}$ is a central simple algebra / k and defines an element of $Br(k)$, which is the opposite of $\delta\varphi$, where

$$\delta : H^1(PGL_n) \longrightarrow H^2(G_m).$$

Outline of the course: This will not be a systematic treatment of Galois cohomology (see Lecture Notes #5 or Shatz's book). We will study.

1) The Trace form on K/k (Bayer-Lenstra, American Journal of Mathematics, 1990 or 1989)
2) Galois Cohomology of $k(T)$, applications to the construction of Galois groups.

Problem: Given $ax^2+by^2+cz^2=0$, $a,b,c \in \mathbb{Z}$, $\text{MAX}(|a|,|b|,|c|)<$
For some a,b,c, this has no rational points, but for some it does. How many have rational points
Total number of points is $\approx X^3$.

$$\frac{X^3}{\log X} \quad \text{the number with rational points} \quad \ll \frac{X^3}{(\log X)^{3/2}}$$

3) Chernousov, $H^1(k, E_8)=0$ if k is a totally imaginary number field
E_8 the exceptional group of 248 elements.
let G be a simple, simply connected Lie group. It was known that $H^1(k_v, G)=0$ and conjectured that $H^1(k, G)=0$.
The only case left to prove of the conjecture:
k totally imaginary, G simple, simply connected
$\Rightarrow H^1(k, G)=0$

was for $G=E_8$.
Using this, Kottwitz could show that $\tau(G)=1$, where $\tau(G)$ is the Tamagawa number.

not done in the course ←

Lecture 2

Kummer theory

Let K be a field, n an integer prime to the characteristic of K. The nth roots of unity, written μ_n, lie in K_s and the long exact sequence: $1 \to \mu_n \to K_s^* \xrightarrow{(n\text{th power})} K_s^* \to 1$ gives

$$1 \to (\mu_n)_K \to K^* \xrightarrow{n} K^* \to H^1(K, \mu_n) \to 1$$

$$0 \to H^2(K, \mu_n) \to H^2(K, K_s^*) \xrightarrow{n} H^2(K, \mathbb{G}_m)$$

$$\| \\ H^2(K, \mathbb{G}_m)$$

Hence

$$\boxed{\begin{aligned} H^1(K, \mu_n) &\cong K^*/(K^*)^n \\ H^2(K, \mu_n) &\cong Br_n(K) \end{aligned}}$$

($=$ Kernel of multiplication by n map in $Br(K)$)

Suppose there is a map $A \otimes B \to C$. There is a cup product (anti-commutative).

$$H^p(A) \times H^q(B) \to H^{p+q}(C).$$ One defines $\varphi \cdot \psi$ as the cocycle

$$(s_1, \cdots, s_{p+q}) \longmapsto \varphi(s_1, \cdots, s_p)^{s_1 \cdots s_p} \psi(s_{p+1}, \cdots, s_{p+q})$$

for $\varphi \in H^p(A)$, $\psi \in H^q(B)$ cocycles.

This cup product can be used to get explicit elements in $Br_n(K)$.

$$\begin{array}{ccccc} H^1(K, \mathbb{Z}/n\mathbb{Z}) & \times & H^1(K, \mu_n) & \to & H^2(K, \mu_n) = Br_n(K) \\ \cup & & \cup & & \\ \varphi & & \psi & \longmapsto & \varphi \cdot \psi \in Br_n(K) \end{array}$$

Assume that $\varphi \in H^1(K, \mathbb{Z}/n\mathbb{Z}) = H^1(\mathrm{Gal}(K^s/K), \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z})$

cyclic $\qquad$ $\|$ G_K

φ corresponds to L/K a field extension of degree n. Let σ be the generator of $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$

Let $\psi = [b]$, for $b \in k^*$. We must now construct the cross product algebra $A = (L/k, b)$.

Let A be the algebra over k with center k, of dimension n^2, generated by (L, y), where

$$y^n = b$$
$$y l y^{-1} = \sigma(l), \quad l \in L$$

Hence, $A = \bigoplus_{i=0}^{n-1} L \cdot y^i$

One can prove that A is a simple algebra and defines an element of $Br(k)$.

Theorem: $[A] = \varphi \cdot \psi$

Modulo the sign, this is easy to prove. The hard part is to check the sign (see Corps Locaux, chapter XIII).

One has a standard isomorphism $H^2(\mathbb{Z}/n\mathbb{Z}, L^*) \xleftarrow{\theta} k^*/Nk^*$.
$H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ classifies extensions of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$. Let $u \in H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$ correspond to the extension

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0.$$

Given $b \in k^* = H^0(\mathbb{Z}/n\mathbb{Z}, L^*)$, $\theta(b) = u \cdot b \in H^2(\mathbb{Z}/n\mathbb{Z}, L^*)$

Hence $\theta b \in H^2(\mathbb{Z}/n\mathbb{Z}, L^*) \subset H^2(G_k, k_s^*) = Br(k)$. Let $\theta b = [A]$.

Recall that φ is homomorphism from G_k to $\mathbb{Z}/n\mathbb{Z}$, $\delta\varphi \in H^2(G_k, \mathbb{Z})$. If $b \in H^0(G_k, G_m)$, $\delta\varphi \cdot b \in H^2(G_k, G_m)$. One has

$$[A] = \delta\varphi \cdot b$$

Since $\delta\varphi$ and b have even degree, b and $\delta\varphi$ commute; hence $[A] = b \cdot \delta\varphi$.

More generally, consider $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$

$$0 \to A_n \to A \xrightarrow{n} A \to 0$$

for an n-divisible G_k-module A. If $\varphi \in H^1(\mathbb{Z}/n\mathbb{Z})$, $b \in H^0(A)$, then $\delta\varphi \in H^2(\mathbb{Z})$, $\delta b \in H^1(A_n)$. Since $\mathbb{Z}/n\mathbb{Z} \times A_n \to A$,

one has $\chi \cdot \delta b \in H^2(A)$.

Lemma: In $H^2(A)$, $\boxed{\delta\chi \cdot b = \chi \cdot \delta b = -\delta b \cdot \chi}$

Proof: Let $s,t \in G_K$. Let $\bar{\chi}(s) \in \mathbb{Z}$ be a lifting of $\chi(s) \in \mathbb{Z}/n\mathbb{Z}$.

Then
$$(\delta\chi)(s,t) = \frac{\bar{\chi}(s) + \bar{\chi}(t) - \bar{\chi}(st)}{n}$$

Write $b = nc$, $c \in A$.

$$(s,t) \longmapsto (b \cdot \delta\chi)(s,t) = c \cdot (\bar{\chi}(s) + \bar{\chi}(t) - \bar{\chi}(st))$$

On the other hand, $(\delta b)(s) = s(c) - c$. $\delta b \cdot \chi$ is represented by
$(s,t) \longmapsto (s(c) - c) \cdot \bar{\chi}(t) = s(c) \cdot \bar{\chi}(t) - c \cdot \bar{\chi}(t)$

Now $\delta b \cdot \chi + \delta\chi \cdot b = c \cdot \bar{\chi}(s) + s(c)\bar{\chi}(t) - c\,\bar{\chi}(st)$
$= \delta f(s,t)$

for $f(s) = c\bar{\chi}(s)$

Hence the cohomology classes are the same and $\delta f \cdot b = \chi \cdot \delta b$

Now let $n = 2$: Denote $H^i(G_K, \mathbb{Z}/2\mathbb{Z}) = H^i(G_K)$

$$\begin{cases} H^1(G_K) = K^*/(K^*)^2 \\ H^2(G_K) = Br_2(K) \end{cases}$$

Given the obvious cup-product $H^p(G_K) \times H^q(G_K) \longrightarrow H^{p+q}(G_K)$,
one considers $(a)(b) \in Br_2(K)$ for $a, b \in K^*$.
$(a)(b)$ is the class of the Brauer group of the quaternion algebra $(a,b)_K$
generated by $1, i, j, k$, $i^2 = a$, $j^2 = b$, $ij = -ji$, $k^2 = -ab$.

Theorem: (Merkurjev) $H^2(G_K)$ is generated by the cup products $(a)(b)$ for $a, b \in K^*$.

Quadratic Forms: Let $f = \sum_{i=1}^{n} \alpha_i x_i^2$, $\alpha_i \in k^*$. One defines invariants in $H^i(G_k)$. One has $(\alpha_i) \in H^1(G_k)$, $1 + (\alpha_i) \in \oplus H^i(G_k)$.

Define $w(f) = \prod (1 + (\alpha_i)) = 1 + w_1(f) + w_2(f) + \dots$

$$w_1(f) = (\alpha_1) + \dots + (\alpha_n) = (\alpha_1 \cdots \alpha_n) = (d(f))$$
$$w_2(f) = \sum_{i<j} (\alpha_i)(\alpha_j) \in Br_2(k)$$

Theorem: If f_1, f_2 are equivalent quadratic forms, then $w(f_1) = w(f_2)$. Hence the $w_i(f)$ are invariants of f.

Pf: The theorem only needs to be proved for forms of dimension $1, 2$ since by a lemma of Witt, if $\underbrace{\alpha_1 x_1^2 + \dots + \alpha_n x_n^2}_{q} \simeq \underbrace{\beta_1 x_1^2 + \dots + \beta_n x_n^2}_{q'}$, there exists a sequence $q_i = \sum_{k=1}^{n} \alpha_{ik} x_k^2$ with $q_0 = q$, $q_m = q'$, $q_i \simeq q_{i+1}$ and the coefficients of q_{i+1} differ from those of q_i in at most two places.

Let $f = \alpha x^2 + \beta y^2$. Let $C(f)$ be the Clifford algebra $\overset{(\alpha,\beta)}{\wedge}$ generated by e_1, e_2, with $e_1^2 = \alpha$, $e_2^2 = \beta$, $e_1 e_2 + e_2 e_1 = 0$. Now $w_2(f) = (\alpha)(\beta) = (\alpha, \beta)$ and two Clifford algebras are isomorphic if the forms are; hence, w_2 is an invariant. w_1 is obviously an invariant.

Exercise: Show that a form over $\mathbb{R}$ is determined by its Stiefel-Whitney invariants. ($w_i \in H^i(G_{\mathbb{R}}) \simeq \mathbb{Z}/2\mathbb{Z}$)

Theorem: (Witt) A quadratic form in $n \leq 3$ variables is determined by w_1, w_2 up to equivalence.

Remark: The theorem is false for $n \geq 4$ for suitable K.

Proof of the theorem: Let $f = \alpha x^2 + \beta y^2 + \gamma z^2$. Now $d(f) = d = \alpha\beta\gamma$ is known (modulo squares). The form $F = df$ has $d(F) = 1$.

$$\begin{aligned} w_2(F) &= (d\alpha)(d\beta) + (d\alpha)(d\gamma) + (d\beta)(d\gamma) \\ &= w_2(f) + (d, d) \\ &= w_2(f) + w_1(f)\, w_1(f) \end{aligned}$$

Hence, we only need to show that $F = \alpha x^2 + \beta y^2 + \gamma z^2$ with $\alpha\beta\gamma$ a square is determined by the class of (α, β).

Let D = the quaternion algebra $(-\alpha, -\beta)$.
Then $N(xi + yj + zk) = \alpha x^2 + \beta y^2 + \alpha\beta z^2 \simeq F$.

$$w_2(F) = (\alpha)(\beta) + (\alpha)(\gamma) + (\beta)(\gamma) = (\alpha)(\beta) + (\alpha)(\alpha\beta) + (\beta)(\alpha\beta)$$

$$\begin{aligned} &= (\alpha)(\beta) + (\alpha)(\alpha) + (\beta)(\beta) \\ &= (\alpha)(\beta) + (-1)(\alpha) + (-1)(\beta) \\ &= (-\alpha)(-\beta) + (-1)(-1) \end{aligned}$$

Hence $w_2(F)$ determines $[D]$, which determines F up to equivalence.

Third Lecture

Recall that k is a field of characteristic $\neq 2$, K_s is the separable closure and $G_k = Gal(K_s/k)$. We have defined $H^i(G_k, \mathbb{Z}/2\mathbb{Z})$ which we also denote as

$$H^i(G_k) = H^i(k, \mathbb{Z}/2\mathbb{Z}) = H^i(k).$$

We saw that $H^1(k)$, $H^2(k)$ have simple interpretations:

(1) $H^1(k) = k^*/(k^*)^2$

$H^2(k) = Br_2(k)$

Moreover, we have a cup-product in cohomology and can use classes in $H^1(k)$ to get classes in $H^2(k)$. For $a \in k^*$, let (a) represent the class in $H^1(k)$ under the identification (1). Since $H^1(k)$ is abelian, we write it additively, so we have

$$(ab) = (a) + (b) \quad \text{for } a, b \in k^*$$

Last time, we showed that $(a)(b) \in H^2(k) = Br_2(k)$ corresponds to the quaternion algebra (a, b).

If $q = \sum_{i=1}^{n} \alpha_i x_i^2$, $\alpha_i \in k^*$ is a nondegenerate quadratic form of rank n, we defined the Stiefel Whitney classes $w_i(q) \in H^i(k)$ by

$$w(q) = \sum_{i=0}^{\infty} w_i = \prod_{i=1}^{n} (1 + (\alpha_i)) \in \bigoplus H^i(k).$$

In particular, we have $w_1(q) = \sum_i (\alpha_i) = (\prod_i \alpha_i) = (\text{discriminant}(q))$

We have $w_2(q) = \sum_{i<j} (a_i)(a_j)$. $w_2(q)$ is the Hasse-Witt invariant attached to q. w_1 and w_2 are the two main invariants for quadratic forms.

Now I would like to tie up some loose ends from the last lecture and present this theory of quadratic forms from the non-abelian cohomology point of view. First, I told you what (a,b) is but not when it is 0. We have

$(a,b)=0 \iff$ the conic $x^2 - ay^2 - bz^2 = 0$ has a rational point.

$\iff a$ is a norm in $K(\sqrt{b})/K$

$\iff b$ is a norm in $K(\sqrt{a})/K$.

(This is slightly ambiguous ~~[illegible]~~ : $K(\sqrt{a})$ may be interpreted, if a is a square, either as K itself, or as the quadratic algebra $K[X]/(X^2-a)$. With both interpretations, the statements are correct.)

Now we have the properties (which follow from the above).

1) $(a,-a) = 0$ 2) $(a, 1-a) = 0$.

Mestre's favorite identity is $\boxed{(a,b) = (a+b, -ab)}$ (due to Witt)

NON-ABELIAN COHOMOLOGY POINT OF VIEW

Let q be a given n-dimensional non-degenerate quadratic form. It defines the orthogonal group $O(q)$. We can twist q by an element $\alpha \in H^1(K, O(q))$ to get a quadratic form q_α.

By varying α, we get all quadratic forms over k that are isomorphic to q over k_s. We should be able to get ω_1, ω_2 by a non-abelian method.

Case $n=1$: let $q = ax^2$; $a \in k^*$. Then $O(q) = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$.

Let $\alpha \in H^1(k) = H^1(k, O(q))$, $\alpha = (b)$, $b \in k^*$
$\cong k^*/(k^*)^2$

Now $q_\alpha = a\alpha x^2$ (and one checks that) $\boxed{\text{disc}(q_\alpha) = \text{disc}(q)\cdot b}$.

Now take n arbitrary | $\alpha \in H^1(O(q))$, q given.

We have the short exact sequence

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

So if $\alpha \in H^1(O(q))$; $\delta_1(\alpha) \in H^1(k)$. We have the formula.

$$\boxed{\omega_1(q_\alpha) = \omega_1(q) + \delta_1(\alpha)}$$

We could see this by just doing the computation but we can instead appeal to a general principle. We define $\omega_1(q)$ to be $\omega_1(\Lambda^n q_{\alpha n})$, where $\Lambda^n q$ is a quadratic form in 1 variable.

[Here q determines an isomorphism $V \xrightarrow{\sim} V^*$, so let $\Lambda^n q$ be the form corresponding to the isomorphism $\Lambda^n V \xrightarrow{\sim} (\Lambda^n V)^* = \Lambda^n V^*$.]

Once you convince yourself that $\Lambda^n q_\alpha = (\Lambda^n q)_\alpha$ then

$$\omega_1(q_\alpha) = \omega_1((\Lambda^n q_\alpha)) = \omega_1((\Lambda^n q)_\alpha) = \omega_1((\Lambda^n q)_{\delta_1(\alpha)}) = \omega_1(q) + \delta_1(\alpha)$$

(The same method would apply to any functor F (instead of Λ^n), with reasonable properties: $(FX)_\alpha = F(X_\alpha)$.)

The formulas are harder for $n>1$.

Exercise: $\omega_3 = \omega_1 \cdot \omega_2$

The formula of Wu says: $Sq^1 w_2 = \omega_1 \cdot \omega_2 + \omega_3$.

One defines Sq^1 as the coboundary map $H^i \to H^{i+1}$ in the long exact sequence resulting from $0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$.

If $i=1$, $\boxed{Sq^1(x) = x^2}$. We can see this by considering a universal element $P_\infty(\mathbb{R})$. $H(P_\infty(\mathbb{R})) = H(C_2) = \mathbb{F}_2[x]$ so either $x \to x^2$ or $x \to 0$. Since not every cohomology class lifts to one over $\mathbb{Z}/4\mathbb{Z}$, $x \not\to 0$ and $x \to x^2$. Also, if $x \to 0$ then it would be true for every space which we know is false. Thus, $x \to x^2$ for every space.

We want to show $Sq^1(a)(b) = 0$. [Hence, by Mercurier's result mentioned last time, $Sq^1 = 0$ on $H^2(K)$ and $\omega_3 = \omega_1 \cdot \omega_2$].

Sq^1 is a derivation so

$$\begin{aligned} Sq^1(a)(b) &= (a)\,Sq^1(b) + (b)\,Sq^1(a) \\ &= (a)(b)(b) + (b)(a)(a) \\ &= (-1)(a)(b) + (-1)(a)(b) = 0 \end{aligned}$$

Now back to w_2:

What is $w_2(q_\alpha)$ in terms of $\omega_1(q), w_2(q)$ and $\delta_1(\alpha), \delta_2(\alpha)$?

One case is simple, the case when I'm not changing the discriminant.

Since $SO(q) \to O(q) \to \pm 1$ splits,

$$H^1(K, SO(q)) \to H^1(K, O(q)) \xrightarrow{\text{onto}} H^1(K).$$

1st case: $\alpha \in H^1(K, SO(q))$. The special orthogonal group has a nontrivial covering (for $n \geq 2$) of degree 2, $\widetilde{SO}(q) = Spin(q)$.

For $n \geq 3$, this is a universal covering.

The central extension $\pm 1 \to \widetilde{SO}(q) \to SO(q) \to 1$ gives

$\Delta : H^1(K, SO(q)) \to H^2(\pm 1) \simeq H^2(K)$. Call the composition δ_2.

Thm: $w_2(q_\alpha) = w_2(q) + \delta_2(\alpha)$

In general, $O(q)$ is not connected and it does not make sense to speak of its "universal covering". I shall define an algebraic group $\widetilde{O}(q)$ such that

$$\begin{array}{ccccccc} 1 & \to & \pm 1 & \to & \widetilde{O}(q) & \to & O(q) \to 1 \\ & & \| & & \cup & & \cup \\ 1 & \to & \pm 1 & \to & \widetilde{SO}(q) & \to & SO(q) \to 1 \end{array}$$

and I will get $\delta_2 : H^1(K, O(q)) \to H^2(K)$.

Thm: $w_2(q_\alpha) = w_2(q) + w_1(q)\,\delta_1(\alpha) + \delta_2(\alpha)$

Combining theorems,

Thm: $1 + w_1(q_\alpha) + w_2(q_\alpha) = (1 + w_1(q) + w_2(q))\,(1 + \delta_1(q) + \delta_2(\alpha))$ modulo terms of degree ≥ 3.

Now in the exact sequence of algebraic groups / K, $1 \to \pm 1 \to \tilde{G} \to G \to 1$, the map is usually not onto on rational points. Instead, we have

$$1 \to \pm 1 \to \tilde{G}(k) \to G(k) \xrightarrow{\delta} H^1(k, \pm 1) \to \dots$$

In the special case when $G = SO(q)$, δ is the spinor norm.

Spinors: Let V be a n-dimensional vector space with a nondegenerate quadratic form q. We still assume char $k \neq 2$.

Let $C = C(V, q)$ be the Clifford algebra. It has dimension 2^n and is generated by $V \hookrightarrow C$.

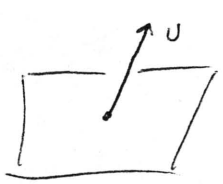
Let $B(x,y) = q(x+y) - q(x) - q(y)$ be the symmetric, bilinear form attached to q. $B(x,x) = q(x)$.

We want $x \in V \Rightarrow$ $x \cdot x = q(x)$ in C
$x \cdot y + y \cdot x = B(x,y)$

Let $e_1, \dots, e_n$ basis of V and $B(e_i, e_j) = 0$ for $i \neq j$
$q(e_i) = \alpha_i$.
Then C is generated by $e_1, \dots, e_n$ with relations $e_i^2 = \alpha_i$
$e_i e_j + e_j e_i = 0$ if
Its basis $e_{i_1} \cdots e_{i_k}$ for $i_1 < \dots < i_k$.

We introduce spinors to understand the symmetries of hyperplanes.

Remark: Let $v \in V$ such that $q(v) = 1$. Let H_v = the hyperplane orthogonal to v. Let s_v be the symmetry with respect to H_v. (It sends $v \to -v$ and fixes H_v). For $x \in V$, consider $x \longmapsto vxv$.



If $x = v$, $vxv = v^3 = v$

If $x \in H_v$, $vxv = -vvx = -x$

So map $x \longmapsto -vxv$ realizes the symmetry s_v.

Every element of the orthogonal group is a product of symmetries

so we can do this for any element. More precisely, we define $\widetilde{SO}$.

For $x \in \mathbb{C}$, we say $x \in C_+ \iff$ x is a linear combination of products of an even number of elements of V.

We define C_- to be the odd part and

$$C = C_+ \oplus C_-.$$

We need an involution on C: $x \longrightarrow x'$ characterized by $x' = x$ if $x \in V$, $(xy)' = y'x'$

Define $\boxed{\widetilde{SO}(q) = \text{group of elements } x \in C_+ \text{ such that } xx' = 1, \quad xVx^{-1} = V}$

This defines an algebraic group. $\widetilde{SO}(q)$. $x \in \widetilde{SO}(q)$, $\rho_x(v) = xvx^{-1}$

$x \longmapsto \rho_x \in SO(q)$.

Symmetries are generated by elements of norm 1 after base extension!

So write $s_{v_1}, \dots, s_{v_{2n}}$ for $v_1, \dots, v_{2n} \in Spin$.

We ~~define~~ : $\widetilde{O}(q) = \widetilde{SO}(q) \cup \widetilde{O}(q)_-$, where $\widetilde{O}(q)_-$ is the set $\{ x \in C_- \text{ such that } xx' = 1, \ xVx^{-1} = V \}$.

$\widetilde{O}(q)_-$ could be empty over the ground field but not after base extension.

We have

$$\begin{array}{ccc} \widetilde{O}(q) & \longrightarrow & O(q) \\ \cup & & \cup \\ \widetilde{SO}(q) & \longrightarrow & SO(q) \end{array}$$

by $x \longmapsto \rho_x(v) = xvx^{-1}$ for $x \in \widetilde{SO}(q)$,

$x \longmapsto -\rho_x(v)$ for $x \in \widetilde{O}(q)_-$

(note the minus sign!)

Let's see what this gives us: when $n = 1$:

$\widetilde{SO} = \{\pm 1\}$, $SO = 1$, $O(1) = 1$ and we have

$$1 \to \pm 1 \to \widetilde{O} \to \underset{\{\pm 1\}}{O} \to 1$$

Thus $\widetilde{O}$ is of type $(2,2)$; $\widetilde{O}(k_s) = C_2 \times C_2$ ("groupe du matelas")

It is a (2,2) group with action of $Gal(k_s/k)$ defined by a homomorphism, namely the one attached to a, $q = ax^2$.

If $a=1$, the action is trivial and we can lift it in a rational way to the Clifford group. When a is not a square, we must go to the quadratic extension, get a lifting and see what changes it. So $\tilde{\mathcal{O}}$ is not so trivial.

Now if $\alpha \in H^1(\mathcal{O})$; we want to show $\omega_2(q_\alpha) = \omega_2(q) + \omega_1(q)\delta_1(\alpha) + \delta_2(\alpha)$

To show this when $n=1$, we have to show $\delta_2(\alpha) \overset{?}{=} \omega_1(q)\delta_1(\alpha)$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ $\|$ $\qquad$ $\|$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ (a) $\qquad$ (α)

We recall the definition of δ_2: Take a cohomology class in $\mathcal{O}$. From LN5, let $1 \to A \to B \to C \to 1$ with a G-action and let $A \subset B$ be contained in the center of B. Then we can define $\Delta: H^1(G,C) \to H^2(G,A)$

Given $s \longmapsto c_s$, $c_{st} = c_s {}^s c_t$,

lift c_s to b_s, and define $a_s = b_s {}^s b_t \, b_{st}^{-1}$

Lecture Four

n=1 →

Recall: Let $q = ax^2$. $\tilde{O}(q)$ is an algebraic group of dimension one. Over the separable closure of K, it is a group X of type $(2,2)$ with the natural exact sequence $0 \to \mathbb{Z}/2\mathbb{Z} \to X \to \mathbb{Z}/2\mathbb{Z} \to 0$. G_K acts on X by the obvious automorphism $(a): G_K \to \mathbb{Z}/2\mathbb{Z}$ attached to the discriminant of $q = ax^2$. One views (a) as an element in $H^1(K)$ and is given by matrices of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. For $\alpha \in H^1(O(q))$, we need to compute $\Delta\alpha \in H^2(K)$.

Let A, C be abelian groups, $B = A \times C$. Let G act trivially on A, C and the G-action on B be given by $\chi: G \to \mathrm{Hom}(C, A)$. Let Δ be the usual map arising from $1 \to A \to B \to C \to 1$.

Theorem: Let $\alpha \in H^1(G_K, C)$. Then: $\Delta\alpha = \chi \cdot \alpha$

Proof: α is represented by a 1 cocycle $s \longmapsto c_s \in C$. Let b_s be the natural lifting of c_s to B. (e.g. $b_s = (0, c_s) \in A \times C$). $\Delta\alpha$ is represented by the cocycle $(s,t) \longmapsto b_s \, {}^s(b_t) \, b_{st}^{-1}$.

$$b_s \, {}^s b_t \, b_{st}^{-1} = {}^s b_t \, b_t^{-1} \underbrace{b_s \, b_t \, b_{st}^{-1}}_{1} = {}^s b_t \, b_t^{-1}$$

Written additively, $\Delta\alpha = {}^s b_t - b_t$.

On the other hand, $(\chi \cdot \alpha)(s,t) = \chi(s)(\alpha(t)) = \chi(s)(c_t)$. For $b = (0,c) \in A \times C$, ${}^s(0,c) = (0,c) + (\chi(s)c, 0)$ and hence $\chi(s) \cdot \alpha(t) = {}^s b_t - b_t$.

Exercise 1 ~~Lemma~~: Let $0 \to A \to B \xrightarrow{\pi} C \to 0$ be an exact sequence of G-modules. Let δ be the map $H^q(G,C) \to H^{q+1}(G,A)$, let χ be a 1 cocycle $G \to \mathrm{Hom}(C,A)$. Define a new action of G on B by

$$\boxed{{}^s\chi(x) = s(x) + \chi_s(s\,\pi(x))}$$

The 1-cocycle gives a new map $\delta_\chi: H^q(G,C) \to H^{q+1}(G,A)$ such that

$$\boxed{\delta_\chi(\alpha) = \delta(\alpha) + \chi \cdot \alpha} \quad \text{for} \quad \alpha \in H^q(G,C)$$

Exercise 2. Let $1 \to \mu_2 \to \mu_4 \to \mu_2 \to 1$ be the exact sequence of G_K-modules, ass. to μ_4 and $\delta: H^1(K) \to H^2(K)$.

1. Show that $\delta = 0$
2. Change the action of G_K by using the character (-1). The new sequence becomes $0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ and $\delta\chi = Sq^1$. In this way, one recovers the known formula:

$$(x)(x) = Sq^1(x) = (-1)(x) \quad \text{for } x \in H^1(K).$$

Recall the formula we are trying to prove:

$$\boxed{w_2(q_\alpha) = w_2(q) + w_1(q)\,\delta_1(\alpha) + \delta_2(\alpha)} \tag{1}$$

One reduces to the one-dimensional case by using the decomposition of α as a direct sum.

Let q^1, q^2 be non-degenerate quadratic forms of dimension n^1, n^2 respectively such that $q = q^1 \oplus q^2$, $n = n^1 + n^2$.

$\boxed{O(q^1) \times O(q^2) \hookrightarrow O(q)}$ so for $\alpha^i \in H^1(K, O(q^i))$ $(i=1,2)$ we can view $\alpha^1 \oplus \alpha^2 \in H^1(K, O(q))$

It is trivial that $\delta_1(\alpha^1 \oplus \alpha^2) = \delta_1(\alpha^1) + \delta_1(\alpha^2)$

Lemma: $\boxed{\delta_2(\alpha^1 \oplus \alpha^2) = \delta_2(\alpha^1) + \delta_1(\alpha^1)\,\delta_1(\alpha^2) + \delta_2(\alpha^2)}$

Proof: $\widetilde{O}(q^i) \hookrightarrow \widetilde{O}(q)$ $(i=1,2)$. In $O(q)$, $O(q^1)$ commutes with $O(q^2)$, but they don't in $\widetilde{O}(q)$. Elements of $\widetilde{O}(q^1)$ and $\widetilde{O}(q^2)$ commute except if they are both odd, in which case they anticommute. To see this, one reduces to the case of symmetries (a symmetry corresponds to a vector and $x^2 = 1$, $xy = -yx$).

Let α^i be a 1-cocycle $s \mapsto a^i_s \in O(q^i)$ $(i=1,2)$. $\alpha^1 \oplus \alpha^2$ is the cocycle represented by $s \mapsto a^1_s a^2_s$ with the product computed in $O(q)$. Let $s \mapsto b^i_s$ be a lifting of a^i_s in $\widetilde{O}(q^i)$ $(i=1,$ $\Delta(\alpha^1 \oplus \alpha^2)$ is represented by $(s,t) \mapsto b^1_s\, b^2_s\, {}^s(b^1_t)\, {}^s(b^2_t)\, (b^2_{st})^{-1}\, (b^1_{st})$

(*)

One introduces the signature attached to $a_i' \in O(q^i)$
One writes $a_s' \longmapsto (-1)^{\mathrm{sgn}(a_s')}$ and

$$* = (-1)^{\mathrm{sgn}(b_t')\mathrm{sgn}(b_s^2)} b_s'^{\,s(b_t')}\left[b_s^{2\,s(b_t^2)}(b_{st}^2)^{-1}\right](b_{st}'')^{-1}$$

$\left[b_s^{2\,s(b_t^2)}(b_{st}^2)^{-1}\right]$ is the coboundary of α^2 and is in the center.
Hence

$* = U\cdot V\cdot W$

$U = (-1)^{\mathrm{sgn}(b_t')\mathrm{sgn}(b_s^2)}$ corresponds to $\delta_1(\alpha')\delta_1(\alpha^2)$

$V = b_s'^{\,s(b_t')}(b_{st}')^{-1}$ " " $\delta_2(\alpha')$

$W = b_s^{2\,s(b_t^2)}(b_{st}^2)^{-1}$ " " $\delta_2(\alpha^2)$

Remark: If $n \geq 2$, any $\alpha \in H^1(O(q))$ is decomposable, i.e. $\alpha = (\alpha'; \alpha^2)$ for a non-trivial decomposition of q as $q' \oplus q^2$.
Much more is true if $q = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2$, V a vector space with basis $e_1, \ldots, e_n$, $e_i \cdot e_j = 0$ if $i \neq j$.
Let T_2 = the maximal torus in $O(q)$ = $(2, 2, \ldots, 2)$ (n times) modulo $\begin{pmatrix} \pm 1 & & 0 \\ & \ddots & \\ 0 & & \pm 1 \end{pmatrix}$.

Then

$$\underbrace{k^*/(k^*)^2 \times \cdots \times k^*/(k^*)^2}_{n \text{ times}} = H^1(k, T_2) \twoheadrightarrow H^1(k, O(q))$$

The map is not injective but is surjective which shows that every class is decomposable.

To prove our formula (1), one uses induction on n. For $n \geq 2$, one assumes $\alpha = \alpha_1 \oplus \alpha_2$.

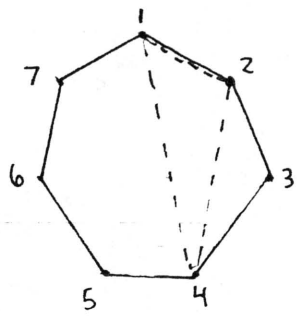
$$q = q^1_{\alpha_1} \oplus q^2_{\alpha_2}.$$

$$w_2(q_\alpha) = w_2(q^1_{\alpha_1} \oplus q^2_{\alpha_2}) = w_2(q^1_{\alpha_1}) + w_1(q_{\alpha_1}')\, w_1(q^2_{\alpha_2}) + w_2(q^2_{\alpha_2})$$

$$= \left(w_2(q') + w_1(q')\delta_1(\alpha_1) + \delta_2(\alpha_1)\right) + \left(w_1(q') + \delta_1(\alpha_1)\right)\left(w_1(q^2_{\alpha_2}) + \delta_1(\alpha_2)\right) + \left(w_2(q^2) + w_1(q^2)\delta_1(\alpha_2) + \delta_2(\alpha_2)\right)$$

$$= w_2(q) + w_1(q)\delta_1(\alpha) + \delta_2(\alpha)$$

G_2 – entertainment



One can define a Cayley algebra using the heptagon and triangle shown.

Let $e_0, e_1, \dots, e_7$ be the basis of the algebra and define $e_i^2 = -1$.

Using the triangle on the left one defines

$$e_1 \cdot e_2 = e_4 = -e_2 \cdot e_1$$
$$e_2 \cdot e_4 = e_1 = -e_4 \cdot e_2$$
$$e_4 \cdot e_1 = e_2 = -e_1 \cdot e_4$$

Rotating the triangle around the heptagon, one has

$$e_2 \cdot e_3 = e_5, \quad e_3 \cdot e_5 = e_2, \quad e_5 \cdot e_2 = e_3, \text{ etc.}$$

Since any 2 points can be connected by the triangle, the entire multiplication table is defined.

For $q = \Sigma x_i e_i$, $\bar{q} = x_0 e_0 - (x_1 e_1 + \dots + x_7 e_7)$.

Over the reals, this construction gives the compact form of G_2.

The Twisted Cayley Algebra: Let $\alpha, \beta, \gamma \in K^*$ and

$$\boxed{\begin{aligned} e_1^2 &= \alpha \\ e_2^2 &= \beta \\ e_3^2 &= \gamma. \end{aligned}}$$

One defines multiplication by

$$\boxed{\begin{aligned} e_1 e_2 &= e_4 \\ e_2 e_3 &= e_5 \\ e_3 e_4 &= e_6 \\ e_4 e_5 &= \beta e_7 \\ e_5 e_6 &= \beta\gamma e_1 \\ e_6 e_7 &= \alpha\gamma e_2 \\ e_7 e_1 &= \alpha e_3 \end{aligned}}$$

and finds that

$$e_4^2 = -\alpha\beta$$
$$e_5^2 = -\beta\gamma$$
$$e_6^2 = \alpha\beta\gamma$$
$$e_7^2 = -\alpha\gamma$$

For $q = \Sigma x_i e_i$, let $\bar{q} = x_0 e_0 - (x_1 e_1 + \dots + x_7 e_7)$.

Then the norm form $q\bar{q} = x_0^2 - \alpha x_1^2 - \beta x_2^2 - \gamma x_3^2 + \alpha\beta x_4^2 + \beta\gamma x_5^2 - \alpha\beta\gamma x_6^2 + \alpha\gamma x_7^2$

Define $\langle \alpha \rangle = \alpha X^2$

$\langle \alpha \rangle \oplus \langle \beta \rangle = \alpha x^2 + \beta y^2$.

In this notation,

$$\boxed{q\bar{q} = (\langle 1 \rangle \oplus \langle -\alpha \rangle) \otimes (\langle 1 \rangle \oplus \langle -\beta \rangle) \otimes (\langle 1 \rangle \oplus \langle -\gamma \rangle)}$$

is a 3-Pfister form.

More generally, $(\langle 1 \rangle \oplus \langle a_1 \rangle) \otimes \dots \otimes (\langle 1 \rangle \oplus \langle a_m \rangle)$ is a m-Pfister form

The values are multiplicative and Pfister forms can be used to show that the product of two sums of sixteen squares is a sum of sixteen squares

Two forms are equivalent $\Leftrightarrow$ the norm forms are the same.

One has,

$$H^1(K, G_2) = \text{classes of the octonians} = \text{classes of 3-Pfister form}$$

Hence the classes of 3-Pfister forms can be computed via cohomology. Attach to a 3-Pfister form the element $e = (\alpha)(\beta)(\gamma) \in H^3(K)$.

Theorem: (Arason) w depends only on the class of the quadratic form and two forms are equivalent if their w's are equal.

One sees $H^1(K, G_2) \hookrightarrow H^3(K, \mathbb{Z}/2\mathbb{Z})$

Let q be a 3-Pfister form, $w(q) \in H^3(K)$., $w_1 = w_2 = w_3 = 0$ for q.
One has $w_4(q) = (-1)^4 + (-1)\, e$

Example

$K_0 = \mathbb{C}$, $K_1 = \mathbb{C}((\alpha))$, α an indeterminate.

$\overline{K}_1 = \bigcup_{n \geq 1} \mathbb{C}((\alpha^{1/n}))$, $\quad G_{K_1} = \varprojlim \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}$

$K_2 = K_1((\beta))$ $\qquad G_{K_2} = G_{K_1} \times \hat{\mathbb{Z}} \cong \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$

$K = K_3 = K_2((\gamma))$ $\qquad G_K = \hat{\mathbb{Z}} \times \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$

Take the obvious 3 Pfister form on K.

Now $H^*(G_{K_1}, \mathbb{Z}/2\mathbb{Z})$ is an exterior algebra on $(\alpha), (\beta), (\gamma) \in H^1$.
In particular $e = (\alpha)(\beta)(\gamma)$ is a non-zero element in H^3

The Pfister form is not trivial, but $H^4 = 0$, $w_4 = 0 = w_1 = w_2 = w_3$
(its e-invariant is not 0)

Lecture 5

The orthogonal group in characteristic two

The orthogonal group behaves ~~strangely~~ differently depending on the parity of n.

$n=1$: $O(1) = \mu_2$.

For n odd, $O(n)$ is not smooth but can be written as $\mu_2 \times SO(n)$, for $SO(n) = \ker\{\det: O(n) \to \mu_2\}$

Galois cohomology is best adapted to separable extensions. Here, one needs to use flat cohomology:

$$H^1_{flat}(K, \mu_2) = K^*/(K^*)^2$$

If n is even, $O(n)$ is smooth. One has $1 \to SO(n) \to O(n) \to \mathbb{Z}/2\mathbb{Z} \to 1$, and the map replacing the determinant map is the Dickson invariant.

For n even, $H^1(O(n)) \xrightarrow[\text{invariant}]{\text{Arf}} H^1(\mathbb{Z}/2\mathbb{Z}) = K/\wp K$,

where $\wp x = x^2 + x$

Now assume (again) that characteristic $K \neq 2$.

Witt Simplification Theorem: If q^1, q^2 are stably equivalent quadratic forms (of the same rank) they are equivalent.

def: Two forms q^1, q^2 are stably equivalent if there exists a form q^3 such that $q^1 \oplus q^3 \cong q^2 \oplus q^3$

We view $O(q^1) \to O(q^1 \oplus q^3)$. Let $\alpha \in H^1(K, O(q^1)) \to H^1(K, O(q^1 \oplus q^3))$ and $\alpha \longmapsto 0$ (or 1).

Hence, Witt's theorem is equivalent to showing $\ker: H^1(O(q^1)) \to H^1(O(q^1 \oplus q^3))$ is trivial.

Let $A = O(q^1)(K_s)$, G acts on A, B, $A \subset B$.
$B = O(q^1 \oplus q^3)(K_s)$
$G = Gal(K_s/K) = G_K$

Let $A^G = H^0(G, A)$. We have:

$$A^G \to B^G \to (B/A)^G \xrightarrow{\delta} H^1(G, A) \to H^1(G, B)$$

(B/A: homogeneous space)

(See Lecture Notes 5 page I-64

The δ map can be defined in the following way: Take $x \in (B/A)^G$, let $\pi: B \to B/A$. Then $\pi^{-1}(x)$ is a homogeneous space. Choose $b \in \pi^{-1}(x)$ and define a_s by ${}^s b = b \cdot a_s$. (torseur with A-action)

The sequence is exact in that $\operatorname{Ker}\{H^1(G,A) \to H^1(G,B)\}$ can be identified with the orbits of B^G acting on $(B/A)^G$

In particular, the kernel is trivial $\iff$ B^G acts transitively on $(B/A)^G$.

To prove Witt's theorem, one can assume q^3 is one dimensional. (Then by induction, one proves it in general.) Let $q^3 = at^2$ and $q(x,t) = q'(x) \oplus at^2$

B/A equals the "sphere" consisting of vectors $y=(x,t)$ with $q(y) = a$.

One needs to look at invariant (rational points):

(*) Witt's Simplification Theorem is true $\iff$ $O(q)$ acts transitively on the vectors of fixed length over K.

Normally, one proves ($\Leftarrow$) to prove Witt's theorem. Galois cohomology shows that the converse holds.

Take y_1, y_2 with $q(y_1) = q(y_2) \neq 0$.

1) Assume $y_1 + y_2$ is not isotropic. Then there exists a reflection σ such that $\sigma(z) = z$ if $z \perp (y_1+y_2)$
$\sigma(y_1+y_2) = -(y_1+y_2)$.

Since $(y_1-y_2) \perp (y_1+y_2)$, $\sigma(y_1-y_2) = y_1-y_2$
and $\sigma(y_1) = -y_2$
$\sigma(y_2) = -y_1$

2) Assume y_1+y_2 is isotropic. If $q(y_1-y_2) = 0$, then
$q(y_1) + q(y_2) + (y_1, y_2) = 0$
$q(y_1) + q(y_2) - (y_1, y_2) = 0 \quad \Rightarrow \quad 2q(y_1) + 2q(y_2) = 4a = 0$
But $a \neq 0$ so $y_1 - y_2$ is not isotropic. Hence y_1 can be transformed in $-y_2$, and hence in y_2.

Springer's Theorem: Let L/k be a finite extension of odd degree, char $k \neq 2$.

Thm 1: If a quadratic form over k represents 0 over L, it does over k as well.

Thm 2: If two forms over k become equivalent over L, they are equivalent over k. In other words, $H^1(k, O(q)) \longrightarrow H^1(L, O(q))$ is injective.

Here if k_s, L_s are the separable closures of k and L, a map $k \longrightarrow L$ extends to a map $k_s \to L_s$ which induces $H^1(k, O(q)) \longrightarrow H^1(L, O(q))$.

In general, one may ask for which A (linear algebraic group), $[L:k]$ odd $\Rightarrow$ $H^1(k, A) \longrightarrow H^1(L, A)$ is injective. Bayer-Lenstra have shown this is true for unitary groups. It also holds for $A = G_2$. (Question: which primes play the same role for E_8 and 2 for G_2?)

Proof of theorem 1: Let $q = a_1 x_1^2 + \ldots + a_n x_n^2$ a form not representing 0 on k. We will use induction on $m = \dim(L/k)$. One can assume that $L = k[x]/(p(x))$ for $p(x)$ an irreducible polynomial of degree m.

There exist polynomials $x_i(X)$ of degree $\leq m-1$, not all zero, rel. prime, such that $\sum a_i x_i(X)^2 \equiv 0 \mod p(X)$. Hence $\sum a_i x_i(X)^2 = p(X)h(X)$ for $h(X)$ a polynomial of degree $\leq m-2$. Let d be the maximal degree of the $x_i(X)$ and write $x_i(X) = \lambda_i X^d +$ lower degree terms. Now $\sum a_i x_i(X)^2 = \left(\sum a_i \lambda_i^2\right) X^{2d} +$ lower terms. $\sum a_i \lambda_i^2 \neq 0$ since q doesn't represent zero over k and so $\sum a_i x_i(X)^2$ has degree $2d$. $h(X)$ must have degree $2d-m$ (odd) and let $p_1(X)$ be an irreducible factor of $h(X)$ of odd degree m_1. Since $\sum a_i x_i(X)^2 \equiv 0 \pmod{p_1(X)}$, we have a nontrivial zero of q in $K[x]/(p_1(x))$, an extension of odd degree $\leq m-2$. By induction, q represents zero over k.

Theorem 1 $\Rightarrow$ Theorem 2: $q = q^{\text{anisotropic}} \oplus (\text{sum of hyperbolic planes})$.

$\Rightarrow q|_L = q^{\text{anisotropic}}|_L \oplus (\text{sum of hyperbolic planes})$

Now suppose one has $q|_L \sim q'|_L$. By the lemma, $q \oplus (-q')|_L$ is hyperbolic.

Lemma: $q \sim q' \iff (q \oplus (-q'))$ is the sum of hyperbolic planes.

By thm 1, $q \oplus (-q')|_L$ the sum of hyperbolic planes.

$\Rightarrow q \oplus (-q')$ is the sum of hyperbolic planes in $K \Rightarrow q \sim q'$

Scharlau's Proof of Theorem 2

Let L/K be a finite extension, $s: L \to K$ a non-zero K linear map. Let $q = \sum_{i=1}^{n} \alpha_i x_i^2$ be a quadratic form over L. One defines $s(q)$, a quadratic form over K of dimension $n[L:K]$, by the rule

$$x \longmapsto s(q(x)) \in K$$

Then $s(q) = \sum_{i=1}^{n} \varphi_i$, where φ_i is a quadratic form of dimension $m = [L:K]$,

with $\varphi_i(\ell) = s(\alpha_i \ell^2)$ for $\ell \in L$.

Quadratic forms $/K$ $\underset{s \text{ map}}{\overset{\text{obvious map}}{\rightleftarrows}}$ Quadratic forms $/L$

Now assume $[L:K] = m$ is odd, $m = 1+2h$, $L = K(z)$ for some $z \in L$.
$1, z, \dots, z^{m-1}$ is a basis for L over K. Define $s: L \to K$ by $s(1) = 1$, $s(z^i) = 0$ for $1 \le i \le m-1$.
If $q = ax^2$, $a \in L$, $s(q)$ is a quadratic form in m variables.

Lemma: $a \in k^* \Rightarrow s(q) =$ q $\oplus$ (the sum of h hyperbolic planes)

Proof: For $a \in k^*$, $s(q)$ is 0 on the vector space generated by $z, \dots, z^h$.
$\Rightarrow s(q) = ax^2 \oplus$ the sum of h hyperbolic planes.

Remark: If q has dimension n, then $s(q|_L) = q \oplus (nh$ hyperbolic planes) and is a K-form

Now if $q_L \sim q'_L$ for q, q' K-forms, then $s(q_L) \sim s(q'_L)$
and $q \oplus$ hyperbolic planes $\sim q' \oplus$ hyperbolic planes.
Hence $q \sim q'$

One can prove similar results for the tensor product of forms. One has $O(q) \hookrightarrow O(q \otimes q')$ and:

Theorem: If q_1, q_2, q' are forms, $\dim q'$ is odd, then one has an injection: $H^1(O(q_1)) \hookrightarrow H^1(O(q_1 \otimes q'))$. In other words,

$$q_1 \otimes q' \sim q_2 \otimes q' \Rightarrow q_1 \sim q_2$$

The trace form of a central simple algebra

Let K (a field) $\subset S$ be central simple algebras of degree n^2 over K. Consider the reduced trace $\mathrm{Trd}: S \longrightarrow K$.

Let $q_S(x) = \mathrm{Trd}(x^2)$; one has $\mathrm{Trd}(xy) = \mathrm{Trd}(yx)$.

What are the w_1, w_2 of q_S? Looking at M_n (the standard case) ($n \times n$ matrices), one gets

$$q^{st}(x) = q_{M_n}(x) = \mathrm{Tr}_{M_n}(x^2) = \sum_{i=1}^{n} x_{ii}^2 + 2 \sum_{i<j} x_{ij} x_{ji}$$

In that case q^{st} is sum of n times the unit form x^2, and $\frac{n(n-1)}{2}$ times the hyperbolic form $x_1 x_2$ of degree 2.

Theorem: (a) If n is odd, $q_S \cong q^{st}$

(b) If n is even, $w_1(q_S) = w_1^{st}$

$$w_2(q_S) = w_2^{st} + \frac{n}{2}[S],$$

where $[S] \in Br_n(K)$

Lecture Six

October 4^{th}

Let S be a central simple algebra of dimension n^2 over K.
Let $q_S(x,y) = \mathrm{Trd}(xy)$ (reduced trace) for $x,y \in S$, and $q_S(x) \overset{def}{=} q_S(x,x)$
q_S is a quadratic form in n^2 variables.

For $S = M_n(K)$, $q^{st} = q_{M_n(K)} = \sum x_{ii}^2 + 2\sum_{i<j} x_{ij}x_{ji}$

$= \langle 1,\dots,1\rangle + \langle 1,-1,1,-1,\dots,1,-1\rangle$

$n' \overset{def}{=} \frac{n(n-1)}{2}$. n-copies of the unit form; $\frac{n(n-1)}{2}$ copies of the hyperbolic plane

$w_1(q^{st}) = n'(-1)$
$w_2(q^{st}) = m(-1)(-1)$ for some m.

Theorem: a) If n is odd, $q_S \simeq q^{st}$ ($\Rightarrow$ w_1, w_2 are the same)
b) If n is even, $w_1(q_S) = w_1(q^{st})$
$w_2(q_S) = \frac{n}{2}[S] + w_2(q^{st})$

Proof: (a) Let $S \simeq M_m(D)$ for D a division algebra over K.
There exists an extension L of K of odd degree such that
$S \otimes_K L = S_L \cong M_n(L)$
From the definition of reduced trace, $q_{S_L} \simeq q_{M_n(L)}$. By Springer's theorem, $q_S \simeq q_{M_n(K)} = q^{st}$

(b) View S as a twist of $M_n(K)$ by a cohomology class $\alpha \in H^1(K, \mathrm{Aut}\, M_n)$, $\mathrm{Aut}\, M_n = PGL_n$

q_S is a form in n^2 variables; viewed as twisted by an element of $O(n^2)$
PGL_n acts on M_n but preserves the trace form, giving a map $\varphi : PGL_n \to O(q^{st})$. Let φ be the map induced on H^1 as well.

$$H^1(K, PGL_n) \xrightarrow{\varphi} H^1(K, O(q^{st}))$$
$$\alpha \longmapsto \varphi\alpha$$

Claim: $q_S = q^{st}$ twisted by $\varphi\alpha$

Actually, $\varphi_\alpha \in H^1(k, SO(q^{st}))$ and the twisting doesn't change the discriminant. Hence $w_1(q_S) = w_1(q^{st})$

We have $w_2(q_S) = w_2(q^{st}) + \delta_2(\varphi_\alpha)$. δ_2 is the map $H^1(SO) \to H^2(\mathbb{Z}/2\mathbb{Z})$ arising from $1 \to \mathbb{Z}/2\mathbb{Z} \to \widetilde{SO} \to SO \to 1$.

Consider the diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_n & \longrightarrow & SL_n & \longrightarrow & PGL_n & \longrightarrow & 1 \\ & & \vdots \psi & & \vdots \tilde{\varphi} & & \downarrow \varphi & & \\ 1 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \widetilde{SO}_{n^2} & \longrightarrow & SO_{n^2} & \longrightarrow & 1 \end{array}$$

Since SL_n is simply connected, the map φ lifts to a map $\tilde{\varphi}: SL_n \to \widetilde{SO}_{n^2}$. By the exactness of the rows, one can define a map: $\mu_n \to \mathbb{Z}/2\mathbb{Z}$ lifting $\tilde{\varphi}$.

Claim: ψ is onto. ($\Leftrightarrow \psi: \mu_n \to \mu_2$ has form $x \mapsto x^{n/2}$)

Assume the claim is true. We have $\delta_2(\varphi_\alpha) = \psi(\Delta\alpha)$ and
$[S] = \Delta\alpha \in H^2(K, \mu_n) = Br_n(K)$.
Then $\psi([S]) = \frac{n}{2}[S]$ and the formula in b) is proven.

Now assume the claim is false and ψ is trivial. The diagram states then that for every $\varphi: PGL_n \to SO_{n^2}$, there exists a lifting $\tilde{\varphi}: PGL_n \to \widetilde{SO}_{n^2}$ making (*) commutative. We will show that this is not the case.

(*)
$$\begin{array}{ccc} & & \widetilde{SO}_{n^2} \\ & \overset{\tilde{\varphi}}{\nearrow} & \downarrow \\ PGL_n & \xrightarrow{\varphi} & SO_{n^2} \subset GL_{n^2} \end{array}$$

The standard maximal torus T of GL_n is. $\begin{pmatrix} \lambda_1 & & 0 \\ & \lambda_2 & \\ 0 & & \lambda_n \end{pmatrix}$
A linear representation of T is given by

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \longmapsto \lambda_1^{m_1} \cdots \lambda_n^{m_n} \quad \text{for } m_1, \ldots, m_n \in \mathbb{Z}.$$

Let e_i be the character $\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \longmapsto \lambda_i$

The e_i give a $\mathbb{Z}$-basis of the character group of T.

Let PT be the maximal torus of PGL_n. The characters of PT are $\sum m_i e_i$, $m_i \in \mathbb{Z}$ with $\sum m_i = 0$

The n^2 characters giving the action of PT on M_n are the $e_i - e_j$, $i \neq j$

Suppose $\tilde{e}$ exists. It is well known that $\widetilde{SO}_{n^2}$ has a spin representation. One knows the characters of that representation in terms of SO. Let $n^2 = 2m$ and consider SO_{2m} (type D_m) The weights of the obvious representation of degree $2m$ of $SO(2m)$ are $\varepsilon_1, \cdots, \varepsilon_m, -\varepsilon_1, \cdots, -\varepsilon_m$

The weights of the spin representation are

$$\frac{\pm\varepsilon_1 \pm \varepsilon_2 \cdots \pm \varepsilon_m}{2}.$$

The spin representation is not defined on SO but on a two-sheeted cover. In particular, one of the spin characters is

$$\frac{1}{2}\left(\sum_{i<j}(e_i - e_j)\right) = \frac{1}{2}\left((n-1)e_1 + (n-3)e_2 + \cdots + (n-1)e_n\right)$$

Since $n-1$ is odd, the coefficients are not in $\mathbb{Z}$. Hence the spin representation doesn't lift.

Example: Let q_0 be attached to the octonions obtained by a twist by $\alpha \in H^1(K, G_2)$. We have $\rho: G_2 \to O(8)$. G_2 is connected so $G_2 \to SO(8)$ and $w_1(q_0) = 0$

G_2 is simply connected so

$$\begin{array}{ccc} & \text{lifts} \nearrow & \widetilde{SO}(8) \\ & & \downarrow \\ G_2 & \longrightarrow & SO(8) \end{array}$$

and $w_2(q_0) = 0$

Questions

1. Witt ring. Let F be a field, char $F \neq 2$.

$$W(F) = \left(\text{Grothendieck group of quadratic forms}\right) \Big/ \left(\begin{array}{l}\text{subgroup generated}\\ \text{by hyperbolic}\\ \text{forms}\end{array}\right)$$

The degree map is defined on the Grothendieck group. Let I be generated by forms of even degree. One obtains the exact sequence

$$0 \to I \to W(F) \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

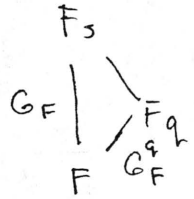
Let $I^n/I^{n+1} = gr^n(W)$.

$I/I^2 = gr^1 \xrightarrow{\sim} H^1(F) = F^*/(F^*)^2$ (easy to see).

$I^2/I^3 = gr^2 \xrightarrow{\sim} H^2(F)$ by Mercurjev's theorem.

It is conjectured that this holds in general.

2. Quadratic Cohomology:



Let F_q be the smallest field containing F where every element is a square. Then G_F^q is the largest profinite 2-quotient group of G_F.

Let $H^i_q(F) = H^i(G_F^q, \mathbb{Z}/2\mathbb{Z})$

There are natural maps $H^i_q(F) \to H^i(F)$.

Conjecture: $H^i_q(F) \simeq H^i(F)$.

More generally, $K^M F \overset{\text{def}}{=} \oplus K^M_i F$ is the ring generated by "symbols" $(\alpha)^M \in K^M_1 F$ for $\alpha \in F$. They satisfy:

$$(\alpha\beta)^M = (\alpha)^M + (\beta)^M \quad \text{for all } \alpha, \beta \neq 0$$
$$(\alpha)^M(1-\alpha)^M = 0 \quad \text{for all } \alpha \neq 0, 1$$

Let $k_i^M F \overset{\text{def}}{=} K_i^M F / 2K_i^M F$. One has the diagram,

$$\begin{array}{ccc} I^i/I^{i+1} & \longleftarrow & k_i^M \\ & & \downarrow \\ H^i & \longleftarrow & H_q^i \end{array}$$

It is conjectured that these maps are bijective. It has been proved for $i=3$

3. Pfister Forms: An i-Pfister form is a tensor product

$$\langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \otimes \cdots \otimes \langle 1, a_i\rangle \text{ of degree } 2^i$$
$$\overset{\text{def}}{=} \langle\langle a_1, \cdots, a_i\rangle\rangle$$

Let $\langle\langle a_1, \cdots, a_i\rangle\rangle \longmapsto e(q) \in H^i(F)$ with
$e(q) = (-a_1)\cdots(-a_i)$

Theorem: (Arason) $e(q)$ is well-defined on Pfister forms

Suppose $D = (a,b)$, $a,b \in F^*$. What is $F^*/\mathrm{Nrd}(D^*)$

Let $c \in F^* \longmapsto (a)(b)(c) = [D]\cdot c \in H^3(F)$ be a map.

Claim: $c \in \mathrm{Nrd}(D^*) \Rightarrow (a)(b)(c) = 0$.

Proof: Let $d \in D^*$ with $\mathrm{Nrd}(d) = c$. If $d \in F^*$, then $c = d^2$ and $(c) = 0$. If $d \notin F^*$, $F(d)$ is a quadratic field, equal to $F(\sqrt{e})$ for some $e \in F^*$, and c is a norm from $F(\sqrt{e})$ to F. Because $F(\sqrt{e})$ splits D, one can write $[D] = (e)(f)$ for $f \in F^*$. Then $(a)(b) = (e)(f)$
Now $(c)(e) = 0$ and $(a)(b)(c) = 0$.

Theorem $c \longmapsto (a)(b)(c)$ gives an embedding of $F^*/\mathrm{Nrd}\, D^*$ into $H^3(F)$

4. Trace form for separable extensions of fields (char $\neq 2$)

"Etale" algebras over K.

1. One possible definition is a product of finite separable extensions of K
2. Another definition is a scheme S of finite type over K of dimension 0
3. Another is an algebra which is a K_s/K form of $\underbrace{K \times \cdots \times K}_{n \text{ times}}$.

Let L/K be any extension. $A_L = L \otimes_K A$ is etale if A is etale.

By 3, an etale algebra is a 1-cohomology class of G_K in $\mathrm{Aut}_{\text{algebras}}(K^n)$ $\quad\|\quad S_n$

If A is an etale algebra of dimension n, K_s/K chosen, let $\Omega_A = \mathrm{Hom}_{alg}(A, K_s)$.

Ω_A has n elements. G_K acts naturally on Ω_A by composition. Given $\varphi \in \Omega_A$, ${}^{\sigma}\varphi = \sigma \circ \varphi \in \Omega_A$.

By the same principles as in Galois theory,

étale algebra $\longleftrightarrow$ finite sets with G_K-action

$A \longmapsto \Omega_A$.

In practice, one can often write $A \cong K[x]/(f(x))$ (f separable polynomial)

Then $\Omega_A \cong$ roots of f

Lecture 7

October 9

Let A be an étale algebra of dimension n over K (char $K \neq 2$). A is a K-form of $K \times \dots \times K = K^n$, twisted by an element $\alpha: G_K \to S_n$ of H^1. α is not canonical, but is defined up to conjugation.

Define $q_A(x) = \mathrm{Tr}_{A/K}(x^2)$ To compute w_1, w_2, we need to study S_n.

Let $H^i(S_n) = H^i(S_n, \mathbb{Z}/2\mathbb{Z})$

$$H^1(S_n) = \begin{cases} 0 & \text{if } n=1 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } n \geq 2 \end{cases}$$

Pf: For $n \geq 2$, we have the signature $\mathrm{sgn}: S_n \to \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$.

$$\dim H^2(S_n) = \begin{cases} 0 & \text{if } n=1 \\ 1 & \text{if } n=2,3 \quad \text{generated by } \varepsilon_n^2 \\ 2 & \text{if } n \geq 4. \quad \text{generated by } \varepsilon_n^2, s_n \end{cases}$$

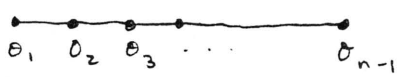
This result is due to Schur.

For $\varepsilon: G \to \mathbb{Z}/2\mathbb{Z}$, $\varepsilon^2 = Sq^1\varepsilon = 0 \iff \varepsilon$ can be lifted to $\mathbb{Z}/4\mathbb{Z}$

Consider a central extension of S_n: $1 \to C_2 \to G \to S_n \to 1$.

View S_n as a Coxeter group with generators $\sigma_i = (i, i+1)$ (transposition of ith and jth letter) with $\sigma_i^2 = 1$.

The diagram is:



where neighbors σ_i, σ_{i+1} satisfy $(\sigma_i \sigma_{i+1})^3 = 1$

and $\sigma_i \sigma_j = \sigma_j \sigma_i$ if $|j-i| \geq 2$

Schur showed that $H^2(S_n)$ ~~has at most 2 generators~~ has dimension 2 ($n \geq 4$).

Suppose one works over $\mathbb{R}$, with S_n regarded as exchanging basis vectors.

One has

$$\begin{array}{ccccccccc} 1 & \to & \pm 1 & \to & \widetilde{O}_n(\mathbb{R}) & \to & O_n(\mathbb{R}) & \to & 1 \\ & & & & \cup & & \cup & & \\ 1 & \to & \pm 1 & \to & \widetilde{S}_n & \to & S_n & \to & 1 \end{array}$$

$\widetilde{S}_n$ is a central extension of S_n by ± 1. Let $s_n \in H^2(S_n)$ be the associated class.

Properties of $\widetilde{S}_n$:

① If $\sigma \in S_n$ is a transposition, its inverse images in $\widetilde{S}_n$ are of order 2. (A transposition corresponds to a symmetry)

② If σ, τ are "disjoint" transpositions $(ij)(kl)$, then for $\tilde{\sigma}, \tilde{\tau} \in \widetilde{S}_n$, one has $\tilde{\sigma}\tilde{\tau} = -\tilde{\tau}\tilde{\sigma}$

For $n \geq 4$, Schur showed that such an extension exists with the spin representation.

If BG is a classifying space, $H^*(BG) = H^*_{\text{alg}}(G)$ for group cohomology.

$$H^*(S_n) = H^*(BS_n) \longleftarrow H^*(BO_n) \cong \mathbb{F}_2[w_1, \cdots, w_n]$$

↑ Stiefel-Whitney classes

One has $w_1, w_2, \cdots \in H^*(S_n)$ (images of the universal w_n's), $w_1 = \varepsilon_n$, $w_2 = s_n$

A_n: $H^1(A_n) = 0$, $H^2(A_n) = \begin{cases} 0 & n \leq 3 \\ \mathbb{Z}/2\mathbb{Z} & n \geq 4 \end{cases}$ with generator $a_n = \text{Res}(s_n)$

We have

$$\begin{array}{ccc} \widetilde{A}_n & \subset & \widetilde{S}_n \\ \downarrow & & \downarrow \\ A_n & \subset & S_n \end{array}$$

$\sigma \quad \tau$
$\| \quad \|$
For $n \geq 4$, $(12)(34)$ has order 2 in A_n but order 4 in $\widetilde{A}_n$. Computing in S_n, $(\tilde{\sigma}\tilde{\tau})^2 = \tilde{\sigma}\tilde{\tau}\tilde{\sigma}\tilde{\tau} = -\tilde{\sigma}^2\tilde{\tau}^2 = -1$. and $H^2(A_n)$ has a nontrivial element.

For $n=4$, $n=5$, the 2-Sylow group in A_n has type $(2,2)$ and the inverse image in $\widetilde{S}_n$ is the quaternion group with 8 elements.

$p \neq 2$ Let p be a prime, $p \neq 2$. $H^2(S_n, \mathbb{Z}/p\mathbb{Z}) = 0$

$$H^2(A_n, \mathbb{Z}/p\mathbb{Z}) = \begin{cases} 0 & \text{if } p \neq 3 \\ \mathbb{Z}/3\mathbb{Z} & \text{if } p = 3,\ n = 3,4,6,7 \\ 0 & \text{if } p = 3,\ n \neq 3,4,6,7 \end{cases}$$

For $n=3,4$, we have the non-trivial extensions:

$$1 \longrightarrow C_3 \longrightarrow C_9 \longrightarrow C_3 \longrightarrow 1 \longleftarrow H^2(A_3)$$
$$1 \longrightarrow (2,2) \longrightarrow A_4 \longrightarrow C_3 \longrightarrow 1$$

and it isn't surprising that H^2 is non-trivial. It is surprising that for $n=6,7$ there are non-trivial extensions.

Digression on the cohomology mod p of a finite group

Let G be a finite group and let S be a p-Sylow subgroup of G.
$H^i(G) \hookrightarrow H^i(S)$ and the image consists of stable elements.

Let P be a p-subgroup of G and let $\varphi: P \to S$ be given by inner conjugation ℓ_g for some element of G

See Cartan-Eilenberg

def: $\alpha \in H^i(S)$ is stable if $\varphi^*(\alpha) \in H^i(P)$ is independent of the choice of $\varphi: P \to G$

For $P = S$, stability means that α is invariant by the action of $N_G S$.

Example: A_6. Let $S \cong C_3 \times C_3$ be generated by $(123), (456)$.

$$H^2(S, \mathbb{Z}/2\mathbb{Z}) \quad ; \quad H^2(S) \cong (\text{dual of } S) \oplus \Lambda^2(\text{dual of } S)$$

has a canonical (up to sign) non-zero element α

α is invariant by the normalizer of S in A_6 (but not in S_6)

Let $P = C_3 \hookrightarrow S$. ; α vanishes on P; this proves stability for α.

$$\begin{array}{ccccccccc} 1 & \to & 3 & \to & 3A_6 & \to & A_6 & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & 3 & \to & 3 \cdot S_6 & \to & S_6 & \to & 1 \end{array}$$

non-central extension of S_6 by C_3

$$\begin{array}{ccc} 3A_6 & \subset & SL_3(\mathbb{C}) \\ \downarrow & & \downarrow \text{ kernel } \mu_3 \\ A_6 & \hookrightarrow & PGL_3(\mathbb{C}) \end{array}$$

$3A_6$ is the Valentiner group

Invariants of the trace form q_A

Let $\dim A = n$. $\varphi : G_k \longrightarrow S_n$ corresponding to A.

$$\varepsilon_n \longmapsto \varphi^* \varepsilon_n \in H^1(G_k) = H^1(k) \qquad w_1(q_A) \in H^1(k)$$
$$s_n \longmapsto \varphi^* s_n \in H^2(G_k) = H^2(k). \qquad w_2(q_A) \in H^2(k).$$

Let d = discriminant of A (defined up to squares); if e_i is a basis of A,
$d = \det(\mathrm{Tr}(e_i e_j)) = \mathrm{disc}(q_A)$

Theorem: (1) $\varphi^*(\varepsilon_n) = (d) = w_1(q_A)$
(2) $\varphi^* s_n + (2)(d) = w_2(q_A)$.

Proof: Let $n=1$: $A = K$, $q_A(x) = x^2$ and the theorem is clear.

Let $n=2$: $A = k(\sqrt{a})$, $a \in K^*$, $(d) = (a)$

$$(x + y\sqrt{a})^2 = x^2 + ay^2 + 2xy\sqrt{a} \Rightarrow \mathrm{Tr}\left((x+y\sqrt{a})^2\right) = 2x^2 + 2ay^2$$

$$w_2(q_a) = (2, 2a) = (2,2) + (2,d) = (2,d)$$

Another Digression:

Let q_A be a form in n variables, rank $n = 2^{m_1} + \dots + 2^{m_h}$, $0 \le m_1 < m_2 < \dots < m_h$
where h = the number of 1's in the dyadic expression of n.

Prop: $q_A = \varphi \oplus \psi$, where rank $\varphi = h$, rank $\psi = n - h$ and
$\varphi = \langle 1, \dots, 1 \rangle$ if $\sum m_i \equiv 0 \pmod 2$
$\varphi = \langle 2, 1, \dots, 1 \rangle$ if $\sum m_i \equiv 1 \pmod 2$.

(For $n=2$, $h=1$, $m_1 = 1$, $\sum m_i$ odd $\Rightarrow \varphi \cong 2x^2$)

Corollary to Springer's theorem: Let L/k be an extension of odd degree, let q, φ be quadratic forms over k. Assume there exists ψ such that

$$q|_L \cong \varphi|_L \oplus \psi .$$

Then such a ψ exists over k.

Proof: Consider the form $f = q \oplus (-\varphi)$. If $q = \varphi \oplus \psi$, then $f = \underbrace{(\varphi \oplus -\varphi)}_{\text{hyperbolic of rank } 2m} \oplus \psi$. Conversely if $f = h_{2m} \oplus \psi$, then $q \cong \varphi \oplus$

$= h_{2m}$

Now over L, $f = h_{2m} \oplus (*) \Rightarrow$ Witt index of f over L is $\geq m$
Hence by Springer, the Witt index of f over k is $\geq m$

Now A is associated to $\varphi : G_k \to S_n$. Let $G \subset S_n$ be the image. Let S be the 2-Sylow subgroup in G. Let $H = \{ s \in G_k \mid \varphi(s) \in S \}$. H is the Galois group G_L for $[L:K] = [G_k : S] =$ an odd number. By the corollary, we can reduce the proof of the proposition to the case $k = L$. The image of φ is a 2-group. The orbits of $S = \varphi(G_L)$ are of order powers of 2.

Lemma: There is a partition of $[1, n]$ into h sets Ω_i of order 2^{m_i}, stable under G_L.

Take a 2-power-partition with minimal number of terms, $A = A_1 \times \dots \times A_h$, rank $A_i = 2^{n_i}$

Trace$_A(1^2) = n$:
$1 \in A_i$, trace$_{A_i}(1^2) = 2^{m_i} = \begin{cases} 1 \text{ if } i \text{ even} \\ 2 \text{ if } i \text{ odd} \end{cases}$ (mod squares).

$$\Rightarrow q_{A_i} \cong \langle 1 \rangle \oplus \psi_i \quad \text{if } m_i \text{ even}$$
$$\cong \langle 2 \rangle \oplus \psi_i \quad \text{if } m_i \text{ odd}$$

Since $\langle 2, 2 \rangle = \langle 1, 1 \rangle$, we have proven the proposition

Returning to our formula: $(n=3)$.

$3 = 1+2$, $h=2$, $m_1=0$, $m_2=1$. Σm_i odd.

so $q_A \cong x^2 + 2y^2 + az^2$ with $(a) = (2d)$

$\Rightarrow q_A \cong x^2 + 2y^2 + 2dz^2$

One can check $w_2(q_A) = (2, 2d) = (2, d)$ and $\varphi^* s_3 = 0$

$\Rightarrow w_2(q_A) = \varphi^* s_3 + (2)(d)$.

Now given q_A, consider $2q_A$, q_A a twist of Σx_i^2; $G_k \to S_n \to O_n(k)$

If one considers $2q_A$, $2q_A(e_i - e_j) = 4 \equiv 1$ (modulo squares). Then can lift $O_n(k)$ to $\widetilde{O_n}$

q a quadratic form of rank n

$q = \Sigma a_i x_i^2$

$$w_1(2q) = w_1(q) + n(2)$$
$$w_2(2q) = w_2(q) + n'(2)\, w_1(q)$$

for $n' = n-1$

In general, $w_2(\lambda q) = w_2(q) + n'(\lambda)\, w_1(q) + n''(-1)(\lambda)$

with $n'' = n(n-1)/2$

Lecture 8 — October 11

$w_2(q_A)$: Let A be an étale algebra of rank n over k. Let q_A be the trace form of A.

In the split case, $A = k \times \dots \times k$ (n times). For $x = (x_1, \dots, x_n)$, $x^2 = (x_1^2, \dots, x_n^2)$ and $q_A = tr(x^2) = x_1^2 + \dots + x_n^2 = \langle 1, 1, \dots, 1 \rangle = q^{split}$

View the general case as being given by a twist $\alpha \in H^1(k, \mathrm{Aut}\, k^n) = \mathrm{Hom}(G_k, S_n)$. Let $\varphi: G_k \to S_n$ be the associated map, q_A = twist of q^{split} by the image of α in $H^1(k, O(q^{split})) = H^1(k, O_n)$

Recall that for a functor (with suitable good properties), F, and X an object,
$$F(_\alpha X) = {}_\alpha(FX) \quad \text{where } {}_\alpha X \text{ is the twist of } X \text{ by } \alpha.$$

Now $2q_A$ is the α-twist of $2q^{split}$. To compute $w_2(q_A)$, consider.
$$1 \to \pm 1 \to \tilde{O}(2q^{split}) \to O(2q^{split}) \to 1$$
$$O(2q^{split}) = O(q^{split})$$

Lemma: $S_n \subset O_n(k)$ is contained in the image of $\tilde{O}(2q^{split})(k)$.

Proof: The transposition of i, j corresponds to the reflection with respect to $\frac{e_i - e_j}{2}$. Now $2q^{split}(e_i - e_j) = 4 = 1$ (modulo squares). These are exactly the elements which lift to $\tilde{O}(2q^{split})$.

Note that $\tilde{S}_n \subset \tilde{O}(2q^{split})(k)$.

$$w_2(2q_A) = w_2(2q^{split}) + w_1(2q^{split})\,\delta_1(\alpha) + \delta_2(\alpha)$$

Now $\delta_1(\alpha) \in H^1(k)$, $G_k \to S_n \to O(2q^{split}) \xrightarrow{\det} \{\pm 1\}$ (composite: signature) and clearly $\delta_1(\alpha) = (d)$.

If $1 \to C \to \tilde{G} \to G \to 1$ is a central extension, $\alpha = (\alpha_s)$ a 1-cocycle with values in G. Let $(\tilde{\alpha}_s)$ be a lifting. $\delta_2(\alpha)$ is defined by $(s,t) \mapsto \tilde{\alpha}_s\, {}^s\tilde{\alpha}_t\, \tilde{\alpha}_{st}^{-1}$. Here $G = O(2q^{split})$

The $\tilde{\alpha}_s$ are in $\tilde{S}_n \subset$ rational points of $\tilde{O}(2q^{split})$. Hence $\delta_2(\alpha)$ is given by $(s,t) \mapsto \tilde{\alpha}_s \tilde{\alpha}_t \tilde{\alpha}_{st}^{-1}$

One has $\delta_2(\alpha) = \varphi^* s_n$

We have $\quad w_2(2q_A) = w_2(q_A) + n'(z)\, w_1(q_A), \quad n' = n-1$

$\quad\quad w_2(2q_A) = w_2(2q_A^{split}) + w_1(2q_A^{split})(d) + e^* s_n$

$\Rightarrow \quad w_2(q_A) + n'(z)(d) = n(z)(d) + e^* s_n$

$\Rightarrow \quad \boxed{w_2(q_A) = (z)(d) + e^* s_n}$

Because $(-1), (z)$ play a role in the proof and $\mathbb{Q}(\sqrt{-1}, \sqrt{2}) = \mathbb{Q}(\mu_8)$, one expects that there exists a proof based on the eighth roots of unity.

Suppose one considers the trace form $Tr(ax^2)$ for $a \in A^*$.

let $s_n' = (-1)^n s_n$, $\quad s_n' \in H^2(S_n')$.

$$G_k \xrightarrow{\varphi'} S_n' \qquad \text{Then}$$
$$\searrow^{\varphi} \quad \downarrow$$
$$S_n$$

$$w_2(\text{form } Tr(ax^2)) = \varphi'^*(s_n') + (z)(d)$$

(see CMH paper on $Tr(x^2)$)

Now we consider how $w_1(q_A)$, $w_2(q_A)$ determine q_A.

Theorem: If k is a number field, and if the archimedean behavior of A is known, then $w_1(q_A)$, $w_2(q_A)$ determine q_A.

One has $k \otimes \mathbb{R} \cong \mathbb{R}^{r_1} \otimes \mathbb{C}^{r_2}$. Fix an embedding $\psi: k \hookrightarrow \mathbb{R}$.

$A \otimes_\psi \mathbb{R} = \mathbb{R}^{r_1(\psi)} \otimes \mathbb{C}^{r_2(\psi)}$

$(q_A)_\psi$ has $r_1(\psi) + r_2(\psi)$ positive signs, $r_2(\psi)$ negative signs $\Rightarrow (q_A)_\psi = r_1\langle 1\rangle + r_2\langle \text{hyperbolic} \rangle$ planes

Knowing q_A determines $r_1(\psi)$. Over $\mathbb{R}$, one knows $q_A \iff$ one knows $r_1(\psi)$ (Borchardt, Crelle, 1857).

Jacobi applied this to $Tr(x^2)$, $A = \mathbb{R}[x]/(f(x))$. The signature determines the number of real roots of f.

let $f = x^n + a_1 x^{n-1} + \dots + a_n$, $\quad A = k[x]/(f(x))$. A has basis $1, x, \dots, x^{n-1}$

$Tr(x_i x_j) = \begin{pmatrix} x_{11} & x_{12} & \cdots \\ \vdots & & \\ \cdot & & \end{pmatrix}$. Let $d_1 = x_{11}$ Assume that the $d_i \neq 0$

$$d_2 = \begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix} \neq 0$$

$\vdots$

Then $w_2 = \sum_{i=1}^{n-1} (d_i)(-d_{i+1})$ and $r_2 =$ the number of sign changes in the d_i

Theorem: A quadratic form over a number field is determined by w_1, w_2 and its signature

---

Example: A_5-extensions.

Let k be a field (infinite); $\operatorname{disc}(q_A)$, 5 squares in k, for a 5-dimensional étale algebra A given by $G_k \xrightarrow{\varphi} A_5 \subset S_5$

Then the following properties are equivalent:

(1) $q_A \simeq \langle 1,1,1,-1,-1\rangle$

(2) $A \simeq K[x]/(f(x))$, where $f(x)$ is a polynomial of the form $f(x) = x^5 + a_1x^4 + \dots + a_5$, with $a_1 = a_2 = 0$

(3) $\varphi^* s_n = (-1,-1) \in H^2(k)$

(4) A comes from the Klein construction (to be defined).

A is $5 = 2^2+1$ dimensional. Hence by the proposition proved last time, $q_A = \langle 1\rangle + \langle 1\rangle + \psi_3$, for ψ_3 a form in 3 variables. ψ_3 is determined by w_1, w_2 so one needs to check that ψ_3 and $\langle 1,-1,-1\rangle$ have the same invariants. $w_1(\psi_3) = w_1(q_A) = 0 = w_1(\langle 1,-1,-1\rangle)$ and $w_2(q_A) = \varphi^* s_n$, $w_2(\psi_3) = (-1,-1)$. Hence (1) $\Longleftrightarrow$ (3).

(2') There is a non-zero element $a \in A$ with $\operatorname{Tr}(a) = \operatorname{Tr}(a^2) = 0$

Clearly (2) $\Rightarrow$ (2'). We leave (2') $\Rightarrow$ (2) as an exercise.

Now one has $A = k\cdot 1 \oplus A_0$, where A_0 consists of elements of trace 0, and thus $q_A = \langle n\rangle \oplus q_{A_0}$. But $n = 5$ is a square and $q_A = \langle 1\rangle \oplus q_{A_0}$

(2') holds $\Longleftrightarrow$ q_{A_0} represents zero $\Longleftrightarrow$ $q_{A_0} = \langle 1\rangle + \langle -1\rangle + \theta_2$

But θ_2 is a form of dimension 2, with discriminant -1; hence θ_2 is a hyperbolic form, $\theta_2 = \langle 1\rangle + \langle -1\rangle$, $q_{A_0} = \langle 1\rangle + \langle 1\rangle + \langle -1\rangle + \langle -1\rangle$

So (2') $\Longleftrightarrow$ (1). We have proven

$$(1) \Longleftrightarrow (2') \Rightarrow (2)$$
$$(1) \Rightarrow (3)$$

Lecture 9

October 16

Klein's quintic construction:

The idea is to describe a curve Y of genus 0 over K on which $G = A_5$ acts faithfully with $X = Y/A_5$ having genus 0.

Over K_s, $Y \simeq \mathbb{P}_1$ and there is an action of A_5 (faithful) $\iff \exists$ an embedding $A_5 \xrightarrow{\phi} PGL_2(K_s)$.
Let $x \in A_5$ have order 5 and $\phi(x) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ has order 5 in $PGL_2(K_s)$
Then $m(x) \overset{\text{def}}{=} \dfrac{(\operatorname{Tr}\phi(x))^2}{\det \phi(x)} = \dfrac{(\alpha+\delta)^2}{\alpha\delta - \beta\gamma}$

satisfies a quadratic equation. One finds $m(x) = \frac{3+\sqrt{5}}{2}$ and hence $m(x)$ generates $K(\sqrt{5})$.

We want the action of G to be defined over K. Hence we require $\sqrt{5} \in K$.

Let Y be the curve corresponding to the standard quaternion algebra $(-1,-1)$. In characteristic $p>0$, $(-1,-1)$ is split and $Y \cong \mathbb{P}^1$. We look for an embedding $A_5 \hookrightarrow PSL_2(\mathbb{F}_q)$ with $\sqrt{5} \in \mathbb{F}_q$.

Examples: $p=2$: $\sqrt{5} \in K$ requires $\mathbb{F}_4 \subset K$. $A_5 \xrightarrow{\sim} SL_2(\mathbb{F}_4) \subset PSL_2(K)$

$p=3$: We have $\mathbb{F}_9 \subset K$. $A_5 \hookrightarrow PSL_2(\mathbb{F}_9) \cong A_6$ since A_5 can be embedded in A_6 as a transitive subgroup through its action on the 6 5-Sylow subgroups of A_5.

$p=5$: $\sqrt{5} \in \mathbb{F}_5 \subset K$. and $A_5 \cong PSL_2(\mathbb{F}_5)$ gives the embedding.

The Quadric Construction of the Klein Covering

Let Q be a quadric in $\mathbb{P}_3$. The variety of lines on Q has dimension 1 and has two irreducible components (over K_s), both of genus 0.
If the discriminant of Q is a square, the action of G_K on these components is trivial. Otherwise, it is given by the action of G_K on $\sqrt{d}$.
Hence the variety of lines is a disjoint union of 2 curves of genus 0 when d is a square and two conjugate curves (a curve over $K\sqrt{d}$) when d is not a square.

Klein's example: Let H be the hyperplane $\Sigma x_i = 0$ in $\mathbb{P}_4$. Let Q be the quadric $\Sigma x_i^2 = 0$ in $\mathbb{P}_4$ and let Q_2 be the quadric $Q \cap H$ in $\mathbb{P}_3$. Since $(d) = (5) = (i)$ since $\sqrt{5} \in K$, A_5 preserves each component. (S_K interchanges the components according to the signature map).

For ch. $K \neq 2,3,5$, Y = component of Q_2 has ramification at three points with degrees 2, 3, and 5.

$$\downarrow$$

$$X$$

In ch. $K = 2,3,5$, there is wild ramification.

Modular Description of the Construction.

Let char $k = 0$. Let M_5 be the set of modular functions of level 5 over $\mathbb{Q}(\mu_5)$. M_5 can be viewed as the set of $\mathbb{Q}$-functions on the moduli space of elliptic curves E with a specified basis for the 5-division points. In other words, M_5 consists of functions defined over $\mathbb{Q}(\mu_5)$ on the upper half plane invariant under

$$\Gamma(5) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv 1 \mod 5 \right\}$$

Hence $GL_2(\mathbb{F}_5)$ acts on the field M_5, with the action on $\mathbb{Q}(\mu_5)$ given by $\det: GL_2(\mathbb{F}_5) \longrightarrow \mathbb{F}_5^* \cong Gal(\mathbb{Q}(\mu_5)/\mathbb{Q})$.
It is clear that -1 acts trivially $((E, e_1, e_2) \longmapsto (E, -e_1, -e_2))$.
We have $\mathbb{F}_5^* \subset GL_2(\mathbb{F}_5)$ and $PGL_2(\mathbb{F}_5) = GL_2(\mathbb{F}_5)/\mathbb{F}_5^*$.
Let $k|_5$ = fixed field of M_5 under $\mathbb{F}_5^*/\{\pm 1\}$

Then $PGL_2(\mathbb{F}_5)$ and $PGL_2(\mathbb{F}_5) \cong S_5$

$k|_5$ — A_5

$\mathbb{Q}(\sqrt{5})$

$\mathbb{Q}$

Choose Y to be the curve over $\mathbb{Q}(\sqrt{5})$ with function field $k|_5$.
Then the action of A_5 is the one described before.

Let L/k be étale of degree 5. Assume it is a field. Let L^{gal} = Galois closure of L/k. Now $Gal(L^{gal}/k) \subset S_5$. Assume $disc\ L/k = 5$ and 5 is a square in k.

Theorem: L^{gal} <u>can be obtained by the Klein construction</u>

$\iff$ $q_L|_L$ = <u>trace form attached to</u> L

$\cong \langle 1\rangle \oplus \langle 1\rangle \oplus \langle 1\rangle \oplus \langle -1\rangle \oplus \langle -1\rangle$

$\iff$ $w_2(q_L) = (-1)(-1)$

$\iff$ <u>There exists a defining equation of the form</u>

$$x^5 + ax^2 + bx + c = 0.$$

Lecture 10

G Galois algebra

$G = A_5$, K a field, $\sqrt{5} \in K$, (disc) = (1)

When does this come from the Klein construction?

Y curve of genus 0 $\longleftrightarrow$ $(-1,-1)$
$\downarrow G$
$X = \mathbb{P}^1$ ramified in 3 points.

Let Λ be a P torsor.
(e.g. $\varphi: G_K \to G$)

Last time, we had the criterion:

The Galois twist of Y by Λ has a rational point ($\simeq \mathbb{P}_1$).

Given $\varphi: G \to A_5$, one has $a_5 \in H^2(A_5, \mathbb{Z}/2\mathbb{Z})$, $a_5 \neq 0$
$\varphi^* a_5 \in H^2(G_K) = H^2(K)$

We need to show: Λ comes from Klein construction $\iff \varphi^* a_5 = (-1,-1)$

Two proofs will be given:

Proof #1: Y can be described as one of the two curves of lines on the quadric $Q: \sum x_i = 0$, $\sum x_i^2 = 0$

Let $A^{split} = K \times K \times K \times K \times K$. Interpret A as an x s.t. $tr(x) = 0$, $tr(x^2) = 0$.
Twisting by Λ (or P or φ), gives a five-dimensional étale algebra L
Q^L: $\mathrm{Tr}\, x = 0$, $\mathrm{Tr}\, x^2 = 0$.

Λ
|
L
5 |
K
) A_5

L = fixed algebra of $A_4 \subset A_5$.

We want Q^L to have a rational line.
($\iff$ $Y_{twisted}$ has a rational point)

$\iff$ the vector space defined in L/K by $\mathrm{Tr}\, x = 0$ contains a 2-dim. subspace on which $\mathrm{Tr}(x^2) = 0$

$\iff$ $\mathrm{Tr}(x^2)$ (on $\mathrm{Tr}(x) = 0$) is hyperbolic $\langle 1\rangle + \langle -1\rangle + \langle 1\rangle + \langle$

Now $L = K \perp (\mathrm{Tr}\ x = 0)$

$q_L = \langle 1 \rangle \oplus \nearrow$

Hence.

$\iff q_L \cong \langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle 1 \rangle \oplus \langle -1 \rangle \oplus \langle -1 \rangle.$

Proof #2: Y curve of genus 0., action of A_5, invariant $(-1,-1)$

Take any A_5- Galois algebra Λ. Let $Y_\Lambda = Y^{\text{twist}}$

Lemma: The invariant in $Br_2 K = H^2(K)$ of Y_Λ is $(-1,-1) + \varphi^*_{a_S}$

Intuitive idea: $\mathbb{P}^1 \overset{\text{twist}}{\longmapsto} Y \longmapsto Y_\Lambda$
$(-1,-1)$ $\quad\quad$ Λ

Formula for composition in LN 5, p I-72.

Explanations on Twists

Let π be a profinite group. Let $1 \to C \to B \to A \to 1$ be an exact sequence of groups with π-action. Let $C \subset$ center(B). Recall there is a map:

$$H^1(\pi, A) \xrightarrow{\Delta} H^2(\pi, C)$$

Let a_s be a 1-cocycle with values in A. If $a \in A$, $x \mapsto a x a^{-1}$ acts on B, C. In other words, choose $b \in B$, $b \mapsto a$. $x \longmapsto b x b^{-1}$ One has:

$$1 \to C \to {}_aB \to {}_aA \to 1$$

and ${}_a\Delta : H^1(\pi, {}_aA) \longrightarrow H^2(\pi, C)$.

There is a bijection: $\tau_a : H^1(\pi, {}_aA) \xrightarrow{\sim} H^1(\pi, A)$ given by

$$(a'_s) \longmapsto a'_s a_s$$

On the level of cocycles τ_a transforms $s \longmapsto a'_s$ into $s \longmapsto a'_s a_s$ (values in A). Remember ${}_aA = A$. Only the action of π changes. ${}^{\Delta}x = a_s {}^{s}x\, a_s^{-1}$

One checks: $a'_{st}\, a_{st} \overset{?}{=} a_s'\, a_s{}^{s}(a_t'\, a_t) = a_s'\, a_s{}^{s}a_t'\, {}^{s}a_t$

$\| $

$a_s'\, {}^{s}(a_t')\, a_{st} = a_s'\, a_s\, {}^{s}a_t'\, a_t^{-1}$.

Let $x \in H'(\pi_1, A)$. $\Delta_a x \in H'(\pi, C)$.

$x \longmapsto \tau_a x \in H'(\pi, A)$

One has the formula $\Delta_u(x) = \Delta(\tau_a x) - \Delta(a)$ which can be checked by a trivial calculation LN 5, p. I-72

Consider $1 \to \pm 1 \to SL_2(K_5) \to \underbrace{PSL_2(K_5)}_{A} \to 1$

$\pi = G_k$.

Take $a \in H'(\pi, A) \subset Br_2(K)$; $a = (-1,-1)$. The twisted exact sequence is

$$1 \to \pm 1 \to SL(H) \to PGL(H) \to 1$$

for H the quat. algebra $(-1,-1)$

Let $x = \varphi^* a_5$, corresponding to the A_5-Galois algebra.

$x \in H'(\pi, {}_a A)$

$x : G_k \to A_5 \to PGL(H)$

$\Delta(a) = (-1,-1)$ is pretty clear by construction

$\Delta(\tau_a x)$ = the invariant of Y_{twisted}

$\Delta_a(x) = \varphi^* a_5$

Hence the lemma

Theorem: Assume k has no quadratic extensions. Then any A_5-extension of k is obtained by Klein's construction.

Theorem: Assume k has no quadratic extensions, nor cubic extensions. Then any quintic equation can be put in the form $x^5 + ax + b = 0$.

Proof: Need to find x with $\operatorname{tr} x = 0$, $\operatorname{tr} x^2 = 0$, $\operatorname{tr} x^3 = 0$; to do that, (plane, quadric, cubic)

choose a line on the quadric, and intersect it with the cubic.

Back to the $Tr(x^2)$ theorem:

$\varphi: G_k \to S_n$, $\quad w_2(q_L) = \varphi^* s_n + (2)(d)$

Then:

$\varphi^*(s_n) = 0 \iff \varphi$ can be lifted to $\tilde{\varphi}: G_k \to \tilde{S}_n$

$$\begin{array}{ccc} \tilde{G} & \subset & \tilde{S}_n \\ \downarrow & & \downarrow \\ G & \subset & S_n \end{array}$$

(L is a field $\Leftrightarrow$ G is transitive on $[1,n]$)

Case ①: $\tilde{G}$ is a split extension $\Rightarrow \varphi^* s_n = 0$

No information except that $w_2(q_L) = (2)(d)$

Case ②: $\tilde{G}$ is not split: $\tilde{\varphi}$ is then onto:

Get an $\tilde{L}/k$, Galois gp $\tilde{G}$

(then the embedding problem is solvable)

$$\begin{array}{c} \tilde{L} \\ | \\ L \\ | \\ G \\ | \\ k \end{array} \qquad \tilde{G}$$

Now consider groups $G: H^1 = H^2 = 0$. (e.g. $SL_2(\mathbb{F}_8)$, J_1, Monster)

$\Rightarrow w_2(q_L) = w_1(q_L) = 0$

Suppose k is a number field and totally imaginary. Any étale algebra L/k with G such that $H^1 = H^2 = 0$ has a trace form isomorphic to $\langle 1\rangle \oplus \langle 1\rangle \oplus \dots \oplus \langle 1\rangle$. (This follows from the $Tr(x^2)$ theorem since the w_1, w_2 of the trace form are then 0.)

More generally, assume for every $k \hookrightarrow \mathbb{R}$, L is split $/\mathbb{R}$, $L \cong \mathbb{R} \times \dots \times \mathbb{R}$.

Over $\mathbb{Q}$, one knows very few examples of a totally real Galois extension with Galois groups a simple (non abelian) group

Mostre: O.K. for A_n, $n \geq 5$

La Macchia: $PSL_2(\mathbb{F}_7)$

Finite Simple Groups:

	Order	Group
×	60	$A_5 = SL_2(\mathbb{F}_4)$
×	168	$PSL_2(\mathbb{F}_7) = SL_3(\mathbb{F}_2)$
×	360	$A_6 = PSL_2(\mathbb{F}_9)$
?	504	$SL_2(\mathbb{F}_8)$
?	660	$PSL_2(\mathbb{F}_{11})$

If you drop totally real assumption, then the rigidity method gives 25 sporadic groups $/\mathbb{Q}$ (M_{23} is missing) but none are totally real.

E. Bayer, H. Lenstra Jr. American Journal

G Galois algebra Λ. Interested in Trace form $\mathrm{Tr}(x^2)$ on Λ.
Quadratic form, invariant under G.

ex: Λ split $= \underbrace{K \times \dots \times K}_{G}$. The quadratic form is $\sum x_i^2$, G acts transitively, freely on the indices.
Call this a unit or standard G-quadratic form.

By G-quadratic form, have V, q, G, q non-degenerate, q invariant by G.
Here $\dim V = G$. There is in V a vector $v \neq 0$, such that the gv ($g \in G$) make up a basis of V. (gv) is a normal basis, and

$$q(gv, g'v) = \begin{cases} 0 & \text{if } g \neq g' \\ 1 & \text{if } g = g' \end{cases}$$ orthonormal basis

Terminology to use is self-dual normal basis (SNB). "base normale autoduale"

General question: decide when Λ has an SNB basis?

In coding theory, G cyclic order n, $\Lambda/K = \mathbb{F}_{q^n} / \mathbb{F}_q$. (char $\neq 2$)

Λ has an SNB basis $\iff$ n is odd

[BL] If Λ has an SNB basis after an odd degree extension of K, it has one over K.

Cor: If G has odd order, an SNB exists.

If G has even order, examples exist where an SNB doesn't exist.

S 2 Sylow of G: ① $|S| = 2$ SNB exists $\iff$ d is a square
② S type $(2,2)$, G no qt of order 2.
Then $x \in H^2(G)$, $x \neq 0$. $\varphi : G_K \to G$,
$\varphi^* x \in H^2(K)$ is zero $\iff$ SNB exists
③ S type $(2,2,2)$, G no quotient of order 2,
Then $H^1(G) = H^2(G) = 0$, $H^3(G) \ni x$, $x \neq 0$.
$\varphi^* x \in H^3(K)$ is zero $\iff$ SNB exists

Lecture 11

10/25/90

Bayer-Lenstra Theory

Let G be a finite group, Λ a G-Galois algebra (with action on the left) over K. For $\lambda \in \Lambda$, define $tr_\Lambda(\lambda) = \sum_{g \in G} g\lambda \in K$.

We are interested in the existence of a self-dual normal basis*; a K-basis of Λ given by $\{gv\}_{g \in G}$ for some $v \in \Lambda$, with

$$q_\Lambda(gv, g'v) = Tr(gv \cdot g'v) = \begin{cases} 0 & \text{if } g \neq g' \\ 1 & \text{if } g = g' \end{cases} \qquad (*)$$

One consequence of a SNB is the following:

Proposition: Let $H \subset G$. Let Λ^H be the subalgebra fixed by H. If Λ has an SNB, then the trace form of Λ^H is the "unit quadratic form" ($\cong \langle 1 \rangle \oplus \dots \oplus \langle 1 \rangle$)

Proof #1: Assume we have a v with property $(*)$, $\{gv\}$ a SNB. Then $w_g = \sum_{h \in H} h(gv)$ for $g \in H\backslash G$ is a basis for Λ^H.
Calculation shows it is an ortho~~normal~~ basis for the trace form of Λ^H.

Proof #2: (in characteristic 0). The proposition doesn't depend on the algebra structure. It is enough to prove it for the free G-quadratic form.
Let $\Lambda = \underbrace{K \times \dots \times K}_{\#G \text{ copies}}$ be split with the obvious action. Then the proposition is trivial.

Remark: Let K_s be the separable closure of K. Let $\Lambda_s = \Lambda \otimes_K K_s$.
$\Lambda_s \cong \underbrace{K_s \times \dots \times K_s}_{\#G \text{ copies}}$ is split and Λ_s has an SNB.
(choose $v = (1, 0, 0, \dots)$)

* base normale autoduale ("belle base")

Let (V, q_V) be a quadratic space with the G-action preserving q_V. Assume V has a SNB. What is $\mathrm{Aut}(V)$?

By assumption, we have v with property (*). Let u be an automorphism of (V, G_v, q_v). Then

$$w = uv = \sum_{g \in G} x_g \, gv, \quad x_g \in K.$$

$$g'w = \sum_{g'' \in G} x_{g''} \, g'g''v$$

and $$q_V(w, g'w) = \sum_{\substack{g', g'' \\ g = g'g''}} x_g x_{g''} = \sum_{g} x_g x_{g'^{-1}g} = \begin{cases} 0 & g' \neq 1 \\ 1 & g' = 1 \end{cases}$$

More generally, $A = K[G]$ is an algebra with involution $g^* = g^{-1}$

$$\left(\sum x_g g\right)^* = \sum x_g g^{-1}$$

$$U_G(K) = U(A) = \{a \mid a \in A, \ a^* a = 1\}$$

$$a^* a = 1 \iff \left(\sum x_g g\right)\left(\sum x_{g''} g''^{-1}\right) = 1$$

$$\iff \begin{cases} \sum x_g^2 = 1 \\ \sum_g x_g x_{yg} = 0 \quad \text{for } y \neq 1 \end{cases}$$

For $x, y \in V$, define $\Phi(x,y) = \sum_{g \in G} q_V(x, gy) \cdot g \in A = K[G]$

We have $\Phi(sx, y) = s\,\Phi(x,y)$

$\Phi(x, sy) = \Phi(x,y)\, s^*$

$\Phi(x,y)$ is a Hermitian form since $\Phi(y,x) = \Phi(x,y)^*$

V is free of rank 1 as a $K[G]$ module. of the standard G-quad. form

It is now clearer that the automorphism group is the unitary group of $A = K[G]$.

Hence for a Galois G-algebra Λ, the G-trace form of Λ is obtained via a Galois twist by an element $\alpha_\Lambda \in H^1(K, U_G)$

What is α_Λ? Λ is defined up to automorphism by $G \longrightarrow U_G(K)$.

Then $G_K \longrightarrow G \longrightarrow U_G(K)$ is homomorphism defining α.

In order to understand the trace form of Galois G-algebras, we just need to understand the cohomology of U_G relative to $A = K[G]$ and the $\alpha_\Lambda \in H^1(K, U_G)$.

Example: Take $H \subset G$, $X = G/H$. O_X the orthogonal group with respect to the quadratic form $\sum_{x \in X} t_x^2$.

We have $U_G \longrightarrow O_X$
$A \longrightarrow M_\Lambda(K)$

$\alpha_\Lambda \in H^1(K, U_G) \longrightarrow o_\Lambda \in H^1(O_X)$ Trace form Λ^H

In particular, if $\alpha_\Lambda = 1$, so is o_Λ : this gives a third proof of the prop. on p. 11-1.

We can get a few results on SNBs using cohomology

Theorem: Assume $\operatorname{cd} K \leq 1$ (i.e. $H^i(G_K, \text{finite module}) = 0$ for $i \geq 2$, or in other words, $Br(K') = 0$ for K'/K a finite extension. $K = \mathbb{C}(T)$, $\mathbb{C}((T))$, or a finite field are examples).
If G has no quotient of order 2, then any G-Galois algebra has an SNB basis.

Note: It is a ~~property~~ theorem of Steinberg that $\operatorname{cd} K \leq 1 \Rightarrow H^1(K, T) = 0$ for every connected affine group T. We want to apply this to U_G but U_G is not connected.

Let A be an algebra with an involution, radical r: $0 \to r \to A \to A/r \to 0$
$1 \to N \to U_A \to U_{A/r} \to 1$

N is unipotent (separable extension of $\mathbb{G}_a$'s) and $H^1(U_A) \cong H^1(U_{A/r})$

A/r decomposes into a product of algebras of type:
① $S \times S^\circ$ with $(x, y) \mapsto (y, x)$ under the involution
② a simple algebra, stable under involution.

In ①, $U_{S \times S^\circ} \cong GL_S$ and $H^1(GL_S) = 0$
In ②, $S = M_n(D)$ for a division algebra D. One can prove that the involution of S is compatible with an involution of D
Now the unitary (orthogonal) group of a hermitian (or skew-symmetric) form over a division algebra with involution is connected except for the standard orthogonal groups where there is a quotient of

As a consequence, U_A / U_A^0 is a group of type $(2,2,\cdots,2)$

The image of $G \to U_G(K)$ is in $U_G^0(K)$ and the cocycle α_n comes from some α_n^0 in $H^1(K, U_G^0)$, which is zero by Steinberg's theorem. Hence an SNB exists.

We have one more theorem of the same type:

Theorem 1: Assume K is a totally imaginary number field. Assume $G = (G,G)$ and $H^2(G, \mathbb{Z}/2\mathbb{Z}) = 0$. Then any G-Galois algebra has an SNB.

Examples: G = Monster group, $\tilde{A}_n$, J_n, $SL_2(\mathbb{F}_8)$, $SL_n(\mathbb{F}_q)$ except finitely many)

Theorem: (Kneser) (for T a classical group) If K is totally imaginary, T is a connected, simply connected linear group, then $H^1(K,T) = 0$

For $T = G_2, \cdots, E_7$, and E_8 (due to Chernousov), it is much harder. There is no general proof known.

Proof of Theorem 1: Consider the diagram

$$\begin{array}{ccccc} \tilde{U}_G' & & \tilde{U}_G^0 & & \\ \downarrow & & \downarrow & & \\ U_G' & \subset & U_G^0 & \subset & U_G \end{array}$$

with $\tilde{U}_G'$, $\tilde{U}_G^0$ universal covers of U_G', U_G^0 (U_G', U_G^0 are semisimple groups)

U_G' = commutator subgroup of U_G^0

If we can prove:

Claim: $G \to U_G(K)$ has its image in $U_G'(K)$ and lifts to $\tilde{U}_G'(K)$

then we are done, since the cohomology class is 0 by Kneser's theorem.

We have already seen that the image lies in $U_G^0(K)$. Since $G = (G,G)$, the image lies in $U_G'(K)$.

Now $1 \to C \to \tilde{U}_G' \to U_G' \to 1 \Rightarrow \tilde{U}_G'(k) \to U_G'(k) \xrightarrow{\delta} H^1(k, C)$ (*)
$H^1(k, C)$ is abelian but $U_G'(k)$ has no abelian quotient so the map can be lifted pointwise to $\tilde{U}_G'(k)$. But if $\tilde{G}$ is the inverse image of G in (*), we have the exact sequence $1 \to C \to \tilde{G} \to G \to 1$.
C is of type $(2,2,\cdots,2)$ and $H^2(G, \mathbb{Z}/2\mathbb{Z}) = 0$ so the extension splits and the map comes from a map into $\tilde{U}_G'(k)$. Then $H^1(k, \tilde{U}_G'(k)) = 0$ and a SNB exist

Remark: The theorem is also true if $H^1(G, \mathbb{Z}/2\mathbb{Z}) = 0$ (instead of $G = (G, G)$) but the proof is more difficult.

Bayer-Lenstra Theorem:

(char $k \neq 2$) Let A be an algebra with involution, U_A its unitary group (as an algebraic group, it is smooth for char $k \neq 2$). Let k' be a finite extension of k of odd degree. Then $H^1(k, U_A) \longrightarrow H^1(k', U_A)$ is injective.

(i.e. Springer's theorem is true for unitary groups)

There is a Witt group $W(A)$ attached to hermitian modules (projective A-modules). The hyperbolic modules are ~ 0. M is hyperbolic if $\exists N \subset M$, direct factor of M as a module, such that $N = N^\perp$. We have:

THM: k'/k odd extension $\Rightarrow W_k(A) \longrightarrow W_{k'}(k' \otimes_k A)$ is injective.

Let $k' = k(x)$. Define $s: k' \to k$ by $\begin{cases} s(1) = 1 \\ s(x^i) = 0 \quad 1 \leq i \leq n-1 \end{cases}$

s defines a map $W_{k'} \longrightarrow W_k$ such that:

Lemma: (Scharlau) $W_k \longrightarrow W_{k'} \xrightarrow{s} W_k$ is the identity.
A formal computation shows that the same is true for $W_k(A)$ (since it is a W_k-module).
As in the orthogonal case, we also have

THM: (Witt Simplification Theorem): M, M', N hermitian modules.
$M \oplus N \cong M' \oplus N \Rightarrow M \cong M'$ as hermitian modules

The idea of the proof is similar to what we did earlier. One reduces to the semisimple and then the simple case. Then one has the classical Witt theorem for hermitian forms with A a matrix algebra over a division algebra. See Scharlau's book for the details.

Back to Bayer-Lenstra's theorem.

Now let M_1, M_2 be two hermitian A-modules with $M_i' = k' \otimes_k M_i$. If $M_1' \sim M_2'$, then M_1 and M_2 are the same in the Witt group. Then $M_1 \oplus$ hyperbolic $\cong M_2 \oplus$ hyperbolic. (Krull-Remak-Schmidt) shows that the hyperbolics are isomorphic as A-modules, One then and then as hermitian modules.

Cor 1: Let Λ be a G-Galois algebra, k'/k an extension of odd degree. If an SNB exists for $k' \otimes_k \Lambda$, it exists for Λ.

Cor 2: If G has odd order, then an SNB exists for Λ.

Pf: $G_{k'} \to G$ so the image has odd order and the kernel H has odd index in $G_{k'}$. It corresponds to k' / k odd extension. By base change to k', we get a split Galois algebra with a SNB. Then by Cor 1, we have an SNB for Λ.

Lecture 12

10/30/90

Let G be a group, $A = K[G]$ with involution $*$ $(g^* = g^{-1})$, U_G the unitary group associated to A.
Take Λ to be a G-Galois algebra defined by $G \to U_G(K)$. Then the composition $G_K \to G \to U_\alpha(K)$ defines a 1-cocycle $\alpha_\Lambda \in H^1(K, U_G)$.
We saw last time that $\alpha_\Lambda = 0 \iff$ a SNB exists

Examples: ① $G = A_4$. It is a semi-direct product of C_3 and a normal subgroup of type $(2,2)$ i.e. $\{(1), (12)(34), (13)(24), (14)(23)\}$

Let K be a field, char $\neq 0$, $\sqrt{-3} \notin K$. From the exact sequence
$$1 \longrightarrow (2,2) \longrightarrow A_4 \longrightarrow C_3 \longrightarrow 1,$$

a representation of C_3 gives a representation of A_4.

A has a quotient $\cong K[C_3] \cong K \times K(\sqrt{-3})$
(involution is trivial; involution interchanges $\sqrt{-3}$ and $-\sqrt{-3}$)

A_4 acts on four letters doubly transitively.

$$A \longrightarrow M_3(K) \text{ and}$$

$A = M_3(k) \times K \times K(\sqrt{-3})$. We get an involution on $M_3(k)$ since there is a non-degenerate quadratic form and one gets an involution from the quadratic form.

Then $U_G = O_3(h) \times (\pm 1) \times T$ since the involution preserving the quadratic form h is $O_3(h)$; on K, $uu^* = 1$ implies $u^2 = 1$ and $u = \pm 1$; and on $K(\sqrt{-3})$, $uu^* = 1$ if and only if $u \in T = \{\alpha \in K(\sqrt{-3}) \mid N\alpha = 1\}$

Now α_Λ is the 1-cocycle given by $G_k \to G \to U_G(K)$.
Claim: α_Λ is given by $(\sigma_\Lambda, 0, 0)$ in $U_G(K)$.

Since A_4 has no non-trivial characters of order 2, α_Λ is given by $(\sigma_\Lambda, 0, *)$. Also $A_4 \to T$ factors as $A_4 \to C_3 \to T(k)$. By extending the base field, it is easy to see that $H^1(K, T_k)$ is killed by 2.

But the image of the cohomology class under $C_3 \to T_k$ shows that the cohomology class is killed by 3. Hence the image must be 0 and $\alpha_\Lambda = (c_\Lambda, 0, 0)$, for $c_\Lambda \in H^1(K, O_3(h))$

We have $c_\Lambda = 1 \iff$ The quadratic form h, twisted by c_Λ, is $\cong h$
$\iff$ The quadratic form $\langle 1 \rangle \oplus h$ twisted by c_Λ is $\cong \langle 1 \rangle \oplus h$
$\iff$ The quadratic form $x_1^2 + \dots + x_4^2$ twisted by c_Λ is $\cong x_1^2 + \dots + x_4^2$

For $A^3 \subset A^4$, $E = \Lambda^{A_3}$ is an étale algebra of rank 4 over K. Let q_E = the trace form of E. Then $c_\Lambda = 1 \iff q_E = \langle 1 \rangle \oplus \dots \oplus \langle 1 \rangle$

We have $\operatorname{disc}(q_E) = (1)$, $w_2(q_E) = \varphi^* a_4$ where $\varphi: G_k \to A_4$ is associated with q_E and $a_4 \in H^2(A_4, \mathbb{Z}/2\mathbb{Z})$ is a canonical class.

Now $c_\Lambda = 1 \iff \varphi^* a_4 = 0 \in H^2(k) \iff \varphi$ can be lifted to $\tilde{\varphi}: G_k \to \tilde{A}_4$
$\iff \Lambda$ comes from an $\tilde{A}_4$ - Galois algebra.

So we have reduced the problem for trace forms to a question about whether we can lift:

$$\begin{array}{ccc} ? & \to & \tilde{A}_4 \leftarrow \text{quaternion algebra} \\ & & \downarrow \\ G_k & \to & A_4 \quad \text{type } (2,2) \end{array}$$

② $G = A_5$. K char 0 and $\sqrt{5} \notin K$. The table of irreducible characters of A_5 over $\mathbb{C}$ is:

$x = \frac{1+\sqrt{5}}{2}$

$x' = \frac{1-\sqrt{5}}{2}$

	(1)	(12)(34)	(123)	(12345) 5A	(13524) 5B
1	1	1	1	1	1
χ_1	3	-1	0	x	x'
χ_2	3	-1	0	x'	x
ω_4	4	0	1	-1	-1
ω_5	5	1	-1	0	0

Thus $A = k[G] \cong k \times M_3(k(\sqrt{5})) \times M_4(k) \times M_5(k)$
For each factor, the involution $*$ is associated with an invariant quadratic form. Then $U_G \cong O_1 \times O_3 \times O_4 \times O_5$

The cohomology class α_Λ has four components, but only the O_3, O_4, and O_5 components are interesting.

The O_4 component of α_Λ vanishes

$\iff$ the trace form of the quintic etale algebra E_5 defined by Λ is the $\langle 1\rangle \oplus \dots \oplus \langle 1\rangle$ form

$\iff$ the map $\varphi: G_k \to A_5$ defining Λ lifts to $\tilde{\varphi}: G_k \to \tilde{A}_5$

Fact: The O_4 component vanishes $\Rightarrow$ the O_3, O_5 components vanish.

Let $D = (-1,-1)$ over $k(\sqrt{5})$. We view D^* as an algebraic group of dimension 4. Then $D^*/\mathbb{G}_m \cong SO_3$

$$\begin{array}{ccccc} & \tilde{\varphi} \nearrow & \tilde{A}_5 & \longrightarrow & D^*(k(\sqrt{5})) \\ & & \downarrow & & \downarrow \\ G_k & \xrightarrow{\varphi} & A_5 & \longrightarrow & SO_3(k(\sqrt{5})) \end{array}$$

Assume the O_4 component is zero. Then we can lift the map $A_5 \to O_3$ to $\tilde{A}_5 \to D^*$

But $H^1(\ ,D^*) = 0$ so the O_3 component must be 0.

Similarly, one shows that the O_5 component vanishes.

Finally, we note that one can relate q_6 (trace form for $G = A_6$) and q_5. We have:

Theorem: $q_6 \cong 2(\langle 1\rangle \oplus q_5) \cong \langle 2\rangle \oplus 2q_5$

If $q_5 = \langle 1\rangle \oplus \dots \oplus \langle 1\rangle$, then $q_6 = \langle 2\rangle \oplus \dots \oplus \langle 2\rangle$.
But $\langle 2\rangle \oplus \langle 2\rangle = \langle 1\rangle \oplus \langle 1\rangle \Rightarrow q_6 = \langle 1\rangle \oplus \dots \oplus \langle 1\rangle$

Reminder of Group Theory: Fusion in the center of a p-Sylow group.

Let G be a finite group, S a p-Sylow. Let $N = N_G(S)$ be the normalizer of S in G.

Lemma: A, B subsets contained in $Z(S)$. Let $g \in G$ with $gAg^{-1} = B$. Then there is an $n \in N$ with $nan^{-1} = gag^{-1}$ for every $a \in A$.

Remark: The lemma is also true with finite group G replaced by compact Lie group
Sylow subgroup " " Maximal Torus
N/S " " Weyl group (if G connected)

Proof: n should be of the form $\begin{cases} n = gx \\ n \in N \end{cases}$ where x commutes with elements of A.

Let $C_A = \{x \mid x \in G,\ xa = ax \text{ for all } a \in A\}$
We need $gxSx^{-1}g^{-1} = S$ or $xSx^{-1} = g^{-1}Sg$
Since $S \subset C_A$, S is a Sylow group of C_A. $g^{-1}Sg$ is also a Sylow subgroup of C_A. Hence, by the Sylow theorems, there is a $x \in C_A$ with the correct form.

Idea:

"He who Controlleth Fusion Doth Control Cohomology"

Cohomology:

Assume S is abelian, N = the normalizer of S. Let A be a G-module killed by a power of p, and with trivial action of G.

The restriction map $H^i(G, A) \xrightarrow{\text{Res}} H^i(S, A)$ is injective.
N acts on $H^i(S, A)$ with S acting trivially. Hence, N/S acts on $H^i(S, A)$. Note that N/S has order prime to p.
The image of Res is contained in the invariants of N/S in $H^i(S, A)$.

Theorem: (S abelian): $\text{Res}: H^i(G, A) \longrightarrow H^i(S, A)^{\text{invariants of } N/S}$ is an isomorphism.

Recall the definition of a "stable" element of $H^i(S,A)$. We say $x \in H^i(S,A)$ is stable if for every P, Q subgroups of S and any $g \in G$ with $gPg^{-1} = Q$, one has $ig: \mathrm{Res}_Q(x) \xrightarrow{\text{conjugation by } g} \mathrm{Res}_P(x)$

$\uparrow$ in $H^i(Q,A)$ $\qquad$ $\uparrow$ in $H^i(P,A)$

Fact: The image of restriction is the set of stable elements.

To prove the theorem, we need to show that for S abelian, the stable elements are those invariant by N. The stable elements are invariant by N. Conversely, by replacing $g \in G$ by an $n \in N$ having the same effect (by the lemma), we see that an invariant element is also stable.

Let $p=2$, S an abelian group of type $(2,2,\cdots,2)$, $|S| = 2^r$. In other words, S is a vector space over $\mathbb{F}_2$ of dimension r. The cohomology modulo 2 of S is a polynomial algebra over $\mathbb{F}_2$ generated by $x_1, \cdots, x_r$.
We have: $H^1(S) = \mathrm{Hom}(S, \mathbb{F}_2) \cong$ dual of S, dimension $= r$
$H^*(S) = \mathrm{Sym}\ H^1(S)$

For $f \in H^i(S)$, f is a $\left\{\begin{matrix}\text{negligible} \\ \text{vanishing}\end{matrix}\right.$ class if the restriction to every subgroup of order 2 is 0.
If $f = f(x_1, \cdots, x_r)$ is homogeneous of degree i, f is negligible if and only if $f(\varepsilon_1, \cdots, \varepsilon_r) = 0$ for all $(\varepsilon_1, \cdots, \varepsilon_r) \in \mathbb{F}_2^r$

Theorem1: The graded ideal of negligible polynomials is generated by the $x_i x_j (x_i + x_j)$

Theorem 2 Let q be the power of a prime. The graded ideal of polynomials in $\mathbb{F}_q[x_0, \cdots, x_n]$ which vanish on $\mathbb{P}_n(\mathbb{F}_q)$ is generated by $x_i^q x_j - x_i x_j^q$ for $i<j$.

Lemma: (the affine case) The ideal of polynomials in n variables which vanish on $\mathbb{F}_q^n$ is generated by $x_i^q - x_i$.

We see that $\mathbb{F}_q[x]/(x^q - x) \cong \{\text{all } \mathbb{F}_q\text{- functions on } \mathbb{F}_q\}$

and $\mathbb{F}_q[x_1, \cdots, x_n]/(x_1^q - x_1, \cdots, x_n^q - x_n) \cong \{\text{all } \mathbb{F}_q\text{- functions on } \mathbb{F}_q^n\}$

Proof of Theorem 2: The argument is by induction on n. Let $\mathcal{A}$ be the ideal generated by the $x_i^q x_j - x_i x_j^q$. Modulo $\mathcal{A}$, any monomial is congruent to a monomial $x_0^{i_0} \cdots x_n^{i_n}$ where either $i_0 = 0$ or $i_1 \leq q-1, \ldots, i_n \leq q-1$. Any f can be written as

$$f \equiv \varphi_0(x_1, \ldots, x_n) + x_0 \varphi_1(x_1, \ldots, x_n) + \cdots + x_0^\alpha \varphi_\alpha + \cdots$$

where φ_α is homogeneous of degree $i - \alpha$.
If $\alpha \geq 1$, then the exponents are at most $q-1$.
Assume $f = 0$ on $\mathbb{P}_n(\mathbb{F}_q)$.

$f = 0$ on $x_0 = 0 \Rightarrow \varphi_0 \in \mathcal{A}$ by induction, so we may assume $\varphi_0 = 0$
Let $x_0 = 1$. Then $f = \varphi_1 + \cdots + \varphi_\alpha + \cdots$ with φ_α of degree $i - \alpha$.
Since $f = 0$, by affine lemma, all the coefficients must be zero since the monomials $x_1^{i_1} \cdots x_n^{i_n}$ are linearly independent and $i_j \leq q-1$ for all j. Hence $f \equiv 0$ modulo $\mathcal{A}$

Lecture 13

November 1

Let G be a finite group with S, the 2-Sylow subgroup of G, an elementary abelian group $\cong (\mathbb{Z}/2\mathbb{Z})^r$. Let N be the normalizer of S in G.

Recall: The cohomology modulo 2 is given by:

$$H^*(S) = \operatorname{Sym} H^1(S) \cong \mathbb{F}_2[x_1, \dots, x_r]$$
$$H^*(G) = N\text{-invariant part of } H^*(S)$$

$\alpha \in H^i(S)$ is negligible $\iff$ the restriction of α to every cyclic group of S of order 2 is 0

$\iff \alpha(\varepsilon_1, \dots, \varepsilon_r) = 0$ for every $(\varepsilon_i) \in \mathbb{F}_2^r$

$\iff \alpha$ is an element of the ideal generated by $x_i^2 x_j + x_i x_j^2$

Note that a cohomology class is $H^*(G)$ is negligible if its restriction to $H^*(S)$ is negligible.

Now consider a G-Galois algebra L over K. Up to isomorphism, L is given by $\varphi_L : G_K \to G$ (with φ_L defined up to conjugacy). Hence we have $\varphi_L^* : H^*(G) \to H^*(G_K) = H^*(K)$. For $z \in H^*(G)$, write z_L for $\varphi_L^*(z)$.

Theorem: If z is negligible in $H^*(G)$, then $z_L = 0$.

Proof: There exists an extension K'/K of odd degree such that $\varphi_L(G_{K'}) \subset S$. Since $H^*(K) \to H^*(K')$ is injective, it is enough to prove $z_L = 0$ after base extension.

Assume $\varphi_L(G_K) \subset S$. $z|_S \in H^*(S)$ and the pullback by $\varphi_L : G_K \to S$ gives $z_L = \varphi_L^*(z|_S)$. Hence it is enough to prove that $\varphi_L^*(x_i^2 x_j + x_i x_j^2)$ is zero. More generally, we show that $\varphi_L^*(x^2 y + x y^2) = 0$ for all $x, y \in H^1(S)$.

Let $\xi \in \varphi_L^*(x)$, $\eta \in \varphi_L^*(y)$, $e = (-1) \in H^1(K)$. We have $\xi \cdot \xi = e \cdot \xi$, $\eta \cdot \eta = e \cdot \eta$.

Then $0 = 2e\,\xi \cdot \eta = e\xi\eta + \xi e \eta$

$= \xi^2 \cdot \eta + \xi \cdot \eta^2$, which is what we needed to show to prove the theorem.

From above, we have $H^i(S)/H^i_{negl}(S) \cong \{$Polynomials f (homogeneous): $S \to \mathbb{F}_2$ of degree $i\} = \mathrm{Pol}\, f_i(S)$

$H^i(G)/H^i_{negl}(G) \cong N$-invariant part of $\mathrm{Pol}\, f_i(S)$

If $i = r = \mathrm{rank}\, S$, there is a canonical element in $H^i(G)/H^i_{negl}(G)$

Let $f(s) = \begin{cases} 0 & \text{if } s = \text{neutral element} \\ 1 & \text{otherwise.} \end{cases}$

Claim: This is a polynomial function of degree r on S.

Proof: Consider the polynomial $f = \prod_{i=1}^{r} (1+x_i) + 1$.

If all the $x_i = 0$, then $f = 0$ (modulo two).
If one of the x_i is not 0, then $f = 1$
Write $f = \sigma_1 + \sigma_2 + \dots + \sigma_r$ with σ_i the elementary symmetric functions.
If we let

$$\left.\begin{aligned} \tilde{\sigma}_1 &= x_1^r + \dots + x_r^r \\ \tilde{\sigma}_2 &= x_1^{r-1} x_2 + \dots + x_{r-1}^{r-1} x_r \\ &\vdots \\ \tilde{\sigma}_r &= x_1 \cdots x_r \end{aligned}\right\} \begin{array}{l}(\text{exponents are chosen in any} \\ \text{manner that gives a homogeneous} \\ \text{polynomial of degree } r)\end{array}$$

then since σ_i and $\tilde{\sigma}_i$ take the same values,
$\tilde{\sigma}_1 + \dots + \tilde{\sigma}_r$ is the desired polynomial.

Hence $z = f \in H^r(G)/H^r_{negl}(G)$ and $z_L \in H^r(K)$. If L is a G-Galois algebra, z_L is well-defined in $H^r(K)$.

Theorem: (Bayer-Serre): Let G be a finite group whose 2-Sylow subgroup is elementary abelian of order 2^r. Let L be a G-Galois algebra over K and $z_L \in H^r(K)$ its invariant. Then

(a) If L has an SNB, then $z_L = 0$
(b) Assume N acts transitively on $S - \{\text{neutral elt}\}$ and $r \le 3$.
Then $z_L = 0 \Rightarrow$ an SNB exists
(This holds for all r if some standard conjectures are true).

Remarks: 1) $r=1$: $z \in H^1(G)$ corresponds to $G \xrightarrow{\text{onto}} \{\pm 1\}$.

It is a well-known fact that if the 2-Sylow subgroup of G has order 2, then G has a quotient of order 2. (G is the semi direct product of C_2 and a group of odd order).

[If $n=2m$ with m odd, G acts via

$$G \longrightarrow S_n \longrightarrow \{\pm 1\}.$$

If σ acts by m transpositions, m odd $\Rightarrow$ sign $\sigma = -1$ and the composition gives z.]

Now $G_K \xrightarrow{\varphi_L} G \xrightarrow{z} \{\pm 1\}$. Hence

$$\varphi_L^*(z)=0 \iff \text{Image } G_K \text{ has odd order}$$

$$\Updownarrow$$

L is split by an odd degree extension of K.

Suppose $C_2 = \{\pm 1\} = G/I$, $|I|$ odd; and let L^I be a quadratic algebra over K. Recall that the trace form of a quadratic algebra is $\langle 1\rangle \oplus \langle 1\rangle \oplus \cdots \oplus \langle 1\rangle \iff$ the quadratic algebra is split.
If $L^I = K(\sqrt{d})$, the trace form is $\langle 2\rangle + \langle 2d\rangle$. Last time, we saw that L has an SNB $\Rightarrow L^I$ has a unit quadratic form $\Rightarrow L^I$ is split. (which is equivalent to $\varphi_L(G_K) \subset I$).

2) $r=2$: The Sylow group S is of type $(2,2)$, $\mathrm{Aut}(S) = GL_2(\mathbb{F}_2) = S_3$.
Hence N/S is a subgroup of $S_3 = \mathrm{Aut}(S)$ of odd order (1 or 3).
If $N/S = \{1\}$, then $H^*(G) = H^*(S)$ and $H^1(G) \cong (2,2)$. This is an uninteresting case for SNB bases.
If N/S acts by an element of order 3, then it acts transitively and (b) of the theorem applies. Then an SNB exists $\iff z_L = 0$ with $z \in H^2(G)$.
z is the cohomology class in $H^2(G)$ corresponding to the unique nontrivial central extension $\tilde{G} \to G$. $\tilde{S}$ is a central extension of a $(2,2)$ group in which every nontrivial element of S gives an element of order 4 in $\tilde{S}$. Then $\tilde{S}$ = quaternion group of eight elements.

$$\begin{array}{ccc} \tilde{S} & \subset & \tilde{G} \\ \downarrow & & \downarrow \\ S & \subset & G \end{array}$$

Examples of such groups are A_4, A_5 and $PSL_2(\mathbb{F}_q)$ when $q \equiv \pm 3 \pmod 8$.
Then a SNB exists iff the lifting problem to $SL_2(\mathbb{F}_q)$ is solvable.

3) $r=3$: $S = (\mathbb{F}_2)^3$ and $Aut(S) = SL_3(\mathbb{F}_2)$ has order $168 = 2^3 \cdot 3 \cdot 7$
$= G_{168} = PSL_2(\mathbb{F}_7)$.
N/S maps to a subgroup of odd order in G_{168}.

Assume the order of N/S is greater than 1.
If the order is 7, then $\mathbb{F}_8 \cong (\mathbb{F}_2)^3$ additively, and
$\mathbb{F}_8^* \cong C_7$, and the action is transitive. Hence (b) of Thm applies.
If the order is 21, then $\mathbb{F}_8$ is acted on by $\mathbb{F}_8^*$ and C_3 by conjugation. Again (b) of the Thm applies.
If the order is 3, then there exists a non-trivial invariant element of $H^1(S)$, hence a hom. $G \xrightarrow{\text{out}} C_2$.

Examples: ① Let $G = SL_2(\mathbb{F}_8)$. The 2-Sylow is $\begin{pmatrix} 1 & \mathbb{F}_8 \\ 0 & 1 \end{pmatrix}$. The normalizer is the Borel-subgroup $\begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix}$. The action of N is of order 7.
$H^1 = H^2 = 0$ and $H^3(G)/H^3_{ngl}(G)$ has dimension 1.

② $G = J_1$, the first Janko group., $S \cong \mathbb{F}_2^3$.
The action of N is of order $3 \cdot 7$. $H^1 = H^2 = 0$ and the dimension of $H^3(G)/H^3_{ngl}(G) = 1$.

In both of these examples, the rigidity methods can construct families of extensions: E regular extensions with Galois group G.
E
$|\ G$
$\mathbb{Q}(T)$
There are 3 ramification points:
9,9,9 for $SL_2(\mathbb{F}_8)$
2,3,5 for J_1
For any point $P \in \mathbb{P}_1(K)$ distinct from ramification points, one gets a G-Galois algebra L/K depending on P from the map $T \hookrightarrow t \in K$.

In both cases, the z_L invariant in $H^3(K)$ of the Galois algebra L_p is $(-1)(-1)(-1)$

Cor: An SNB exists for such an algebra $L_p \iff -1$ is a sum of 4 squares
$\iff -1$ is a sum of 7 squares
$\iff x_1^2 + \dots + x_8^2$ represents 0

[$x_1^2 + \dots + x_8^2 = 0 \Rightarrow x_1^2 + \dots + x_4^2 = (-1)(x_5^2 + \dots + x_8^2)$
$\Rightarrow (-1)$ is a sum of 4 squares since a product of sums of 4 squares is a sum of 4 squares.]

Lecture 14

November 6

Exercise: If $z \in H^i(G)$ is not negligible, there exists a G-Galois algebra L over $\mathbb{R}$ such that $z_L \neq 0$ in $H^i(\mathbb{R})$.

Hint: Choose $C \subset G$, cyclic of order 2, $z|_C \neq 0$. Then $\varphi: Gal(\mathbb{C}/\mathbb{R}) \xrightarrow{\sim} C$ and we get $G_{\mathbb{R}} \to G$ defining a G-Galois algebra L over $\mathbb{R}$ with $z_L \neq 0$

There is a p-variant of this situation. Let p be a prime $\neq 2$. Let $z \in H^i(G)$

def: z is p-negligible $\iff z_L = 0$ for every G-Galois algebra L over K of char. p.

Exercise: If $p \equiv 1 \ (4)$, the negligible classes of $H^*(S)$ are those of the ideal generated by x^2, $x \in H^1(S)$. It is clear that the x^2 are negligible since $x^2 = (-1)(x) = 0$ (-1 is a square mod p). The negligible classes of $H^*(G)$ are the N-invariant ones of $H^*(S)$.
If $p \equiv -1 \ (4)$, the negligible classes of $H^*(S)$ are the elements of the ideal generated by x^3, $x \in H^1(S)$. The elements of the ideal are negligible since $(-1)(-1) = 0 \Rightarrow x^3 = (-1)(x)(x) = (-1)(-1)(x) = 0$

In order to show that these ideals include all negligible classes, one looks at the local fields $\mathbb{F}_p((t_1))((t_2)) \cdots ((t_r))$. It is easy to calculate the cohomology modulo 2 and determine the form of all negligible classes

---

Recall that last time, we showed that there is a canonical element in $H^r(S)$ given by $f(z) = \begin{cases} 0 & x = \text{neutral element} \\ 1 & \text{otherwise} \end{cases}$; that f is a homogeneous polynomial of degree r.

Another way to prove this is to identify S with $\mathbb{F}_{2^r}$. The norm map $N: \mathbb{F}_{2^r} \to \mathbb{F}_2$ is homogeneous of degree r and is 1 for non-zero elements. Note that the norm map is dependent upon a choice of identification.

Exercise: For which r can one make the polynomial invariant by $Aut(S)$? (One can only do this for $r \leq 2$.)

Exercise: Let $S \subset G$, N act transitively on $S - \{o\}$. We saw last time that a SNB for $L \Rightarrow z_L = 0$. Then we have $H^i(G) \to H^i(K)$ is 0 for $i \geq 1$.
Hint: The image of $H^i(G) \to H^i(K)$ is 0 if $1 \leq i \leq r-1$ and is generated by $e^{i-r} z_L$ if $i \geq r$ (where $e = (-1)$).

Is it true for all G (with any 2-Sylow) that a SNB $\Rightarrow H^i(G) \to H^i(K)$ is 0 ?

We refer to books by Scharlau and Lam for some facts concerning quadratic forms.

Notation: If f is a quadratic form $/K$, $m \in \mathbb{Z}^+$,

$$m \otimes f \overset{\text{def}}{=} \underbrace{f \oplus f \oplus \dots \oplus f}_{m \text{ times.}}$$

Proposition: (Scharlau Chapter 2, §6):

1. If m is odd, $m \otimes f_1 \cong m \otimes f_2 \Rightarrow f_1 \cong f_2$.
2. If m is odd, then m is not a zero divisor in $W(K)$

Idea of Proof: $m \otimes f_1 \cong m \otimes f_2 \Rightarrow m \cdot (f_1 - f_2) = 0$ in $W(K)$
$\Rightarrow f_1 = f_2$ in $W(K)$ (assuming 2.)
$\Rightarrow f_1 \oplus h_1 \cong f_2 \oplus h_2$ for h_1, h_2 hyperbolics.
But f_1, f_2 have the same rank $\Rightarrow h_1, h_2$ have the same rank
$\Rightarrow h_1 \cong h_2 \Rightarrow f_1 \cong f_2$ by Witt simplification.

To prove 2., the idea is to reduce the proof to the field extension of K where the sum of any two squares is a square. Then the calculation of $W(K)$ is easy.

Proposition: If q is a quadratic form of odd rank, q is not a zero-divisor in $W(K)$. (Equivalently, $q \otimes f_1 \cong q \otimes f_2 \Rightarrow f_1 \cong f_2$).

I feel there should be a proof of ~~there are still cases to prove~~ this proposition via root systems. This is vexing since the proposition says $O(n) \xrightarrow[\otimes q]{} O(nm)$ is injective on

$$H^1(k, O(n)) \longrightarrow H^1(k, O(mn))$$

definition: Given q, m an odd integer ≥ 1, q is divisible by m if there exists q_0 such that $q \simeq m \otimes q_0$ and q_0 is unique.

Proposition: Let k'/k be an extension of odd degree. Let $m \geq 1$ be odd. Let q be a quadratic form over k and $q_{k'}$ the k'-form it defines. $q_{k'}$ divisible by m (over k') $\Longrightarrow$ q is divisible by m.

Remark: $W(k) \to W(k')$ is an injection. It is "split" since there is a retraction s_* as follows. Assume $k' = k(\alpha)$. Choose $s: k' \to k$ such that
$$\begin{cases} s(1) = 1 \\ s(\alpha^i) = 0 \text{ for } 1 \leq i \leq \deg k'/k - 1 \end{cases}$$
The Scharlau transfer $s_*: W(k') \to W(k)$ is a retraction. Hence $s_*(q_{k'}) \simeq q$. If $q_{k'} = m \cdot x$, then $q_k = m$ (retraction of x) in $W(k)$. in $W(k')$.

Induction for Galois Algebras

Given $G_1 \xrightarrow{i} G_2$, we want to construct a map from G_1-Galois algebra L_1 to a G_2-Galois algebra L_2

There are various definitions:

① L_1 corresponds to T_1 a G_1-torsor and there exists a unique G_2-torsor T_2 with $T_1 \xrightarrow{i^T} T_2$ such that $i^T(t_1 g_1) = i^T(t_1)\, i(g_1)$

② K_s-points of L_1: $\Omega_1 = T_1(K_s)$. Ω_1 has right action of G_1 and left action of G_k. Let $\Omega_2 = \Omega_1 \times^{G_1} G_2$ with $(\omega g_1, g_2) \sim (\omega, g_1 g_2)$

③ L_2 is characterized by the algebra homomorphism $L_2 \xrightarrow{\pi} L_1$ commuting with action of G

④ (Up to isomorphism) L_2 is given by $G_k \to G \xrightarrow{i} G_2$

There is an analogy with induced representations. We consider the two cases $\left\| \begin{array}{l} i \text{ onto} \\ i \text{ injective} \end{array} \right.$. If i onto, $G_2 \cong G_1/I$, and $L_2 = L_1^I$ (Equivalently, $T_2 = T_1/I$)

If i injective, we can describe L_2 by

$$L_2 = \{ f \mid f : G_2 \longrightarrow L_1 \text{ such that } f(g_1 g_2) = g_1 f(g_2) \}.$$

The G_2-action is given by $(g_2 f)(s) = f(s g_2)$. One must check that this gives a G_2-Galois algebra with the desired properties.

~

Quadratic Form attached to a G-Galois algebra

Let G be a finite grap, $|G| = 2^r \cdot m$ with m odd. If S is 2-Sylow, $|S| = 2^r$. Let L be a G-Galois algebra over K. Let q_L be the trace form of L. It is a quadratic form of rank $2^r m$.

Theorem: q_L is divisible by m.

First step: Let $\varphi : G_K \longrightarrow G$ be attached to L. There exists K'/K extension of odd degree such that $\varphi(G_{K'}) \subset S$. By the proposition, we may hence assume that $\varphi(G_K) \subset S$. In other words, the Galois algebra is induced by an S-Galois algebra L_S over K. (Caution: this is not functorial!). Let q_L° = trace form of L_S.

Claim: $q_L \cong m \otimes q_L^\circ$

Second Step: Let $i : G_1 \longrightarrow G_2$ be an injection. By the description (4) of L_2, we have $L_2 = \bigoplus_{g \in G_2/G_1} g L_1$. There is an idempotent π in L_2 which is G_1 invariant with $\pi L_2 \cong L_1$, and $g\pi \cdot \pi = 0$ if $g \in G_1$. The $(g\pi)_{g \in G_2/G_1}$ are independent idempotents with sum 1.

With this description, it is pretty easy to calculate the trace. q_{L_2} is the orthogonal direct sum of the trace forms of the gL_1.

Remark: If L has an SNB, then q_L° is a unit form. This can be seen since L has an SNB $\Rightarrow$ $q_L \cong \langle 1 \rangle \oplus \cdots \oplus \langle 1 \rangle$ ($2^r m$ times) and by division by m, $q_L^\circ \cong \langle 1 \rangle \oplus \cdots \oplus \langle 1 \rangle$ 2^r times.

Pfister Forms:

Definition: Let q be a quadratic form on V (over K). q is multiplicative if for all $x \in V_{K'}$ with $q_{K'}(x) \neq 0$ for K'/K any extension, the forms $q_{K'}$ and $q_{K'}(x)\, q_{K'}$ are equivalent.

($\Rightarrow$ the non-zero elements of K' represented by q make a subgroup of K'^*).

Definition: An r-Pfister form is a form

$$\langle\langle \alpha_1, \cdots, \alpha_r \rangle\rangle \overset{\text{def}}{=} (\langle 1 \rangle \oplus \langle \alpha_1 \rangle) \otimes \cdots \otimes (\langle 1 \rangle \oplus \langle \alpha_r \rangle).$$

Fact: A Pfister form representing 0 is totally hyperbolic

Theorem: (Pfister) Let q be an anisotropic form (i.e. q does not represent 0). Then the following are equivalent:

① q is a Pfister form

② q is multiplicative (over every extension of K)

One result of the theorem is that if $\alpha = q(x_1, \cdots, x_{2^r})$

$\beta = q(y_1, \cdots, y_{2^r})$,

then $\alpha\beta = q(z_1, \cdots, z_{2^r})$ where the z_i are linear in x_i, y_i but not bilinear if $r \geq 4$.

Theorem: (Arason) Journal of Algebra 36 (1975). Let $q = \langle\langle \alpha_1, \cdots, \alpha_r \rangle\rangle$. Then $(-\alpha_1) \cdots (-\alpha_r) \in H^r(K)$ depends only on q. In other words if $\langle\langle \alpha_1, \cdots, \alpha_r \rangle\rangle \cong \langle\langle \beta_1, \cdots, \beta_r \rangle\rangle$ then the products are equal in $H^r(K)$ (also in $k_r^M(K)$).

Note: For $r \leq 4$, the class determines the Pfister group.

11/8/90

Lecture 15

November 8

Definition: Let q be anisotropic. q is a multiplicative form if there exists $z_1, \cdots, z_n \in k(x_1, \cdots, x_n, y_1, \cdots, y_n)$ with
$q(z_1, \cdots, z_n) = q(x_1, \cdots, x_n)\, q(y_1, \cdots, y_n)$.

We can use Pfister's theorem that an anisotropic form is a Pfister form $\iff$ it is multiplicative to prove:

Theorem: Let k'/k be an odd degree field extension; q a quadratic form on k. q is a Pfister form over $k \iff q_{k'}$ is a Pfister form over k'

Proof: If q is isotropic, q is Pfister $\iff q$ is hyperbolic
$\iff q_{k'}$ is hyperbolic $\iff q_{k'}$ is Pfister

If q is anistropic, then $q(x_1, \cdots, x_n)\, q(y_1, \cdots, y_n) \in k(x,y)$ is represented by q over $k'(x,y)$. Since $k'(x,y) / k(x,y)$ has odd degree, by Springer's theorem, it is represented by q over $k(x,y)$. Hence q multiplicative $\Rightarrow q$ Pfister. The $(\Rightarrow)$ is trivial.

To state the next theorem, we need the following terminology:

$(\alpha_1, \cdots, \alpha_n)$ and $(\beta_1, \cdots, \beta_n)$ are 2-neighbors if $\alpha_i = \beta_i$ for $i \neq j, k$ and $\langle\langle \alpha_j, \alpha_k \rangle\rangle$ and $\langle\langle \beta_j, \beta_k \rangle\rangle$ are equivalent

Theorem (Arason): $\langle\langle \alpha_1, \cdots, \alpha_n \rangle\rangle$ is isomorphic to $\langle\langle \beta_1, \cdots, \beta_n \rangle\rangle$
$\iff$ There is a sequence $\gamma^{(\lambda)} = (\gamma_1^{(\lambda)}, \gamma_2^{(\lambda)}, \cdots, \gamma_n^{(\lambda)})$ with $\gamma^{(\lambda)}, \gamma^{(\lambda+1)}$ 2-neighbors and $\gamma^{(0)} = \alpha$, $\gamma^{(n)} = \beta$ for some n

Corollary: If $q = \langle\langle \alpha_1, \cdots, \alpha_r \rangle\rangle$ is a Pfister form, the element $(-\alpha_1) \cdots (-\alpha_r)$ of $k_r^M(K)$ (hence of $H^r(K)$) depends only on q. (Because $\langle\langle \alpha, \beta \rangle\rangle \simeq \langle\langle \gamma, \delta \rangle\rangle \Rightarrow (-\alpha)(-\beta) = (-\gamma)(-\delta)$ in $H^2(K)$.)

Arason and others (Math. Ann.(*) 1986) have shown that a Pfister form is determined by its invariant in $H^r(k)$ for $r \leq 4$.

(*) J.K. Arason, R. Elman, B. Jacob – Fields of cohomological 2-dimension three, Math. Ann. 274 (1986), 649–657.

Recall our situation: G is a finite group, its 2-Sylow subgroup S is elementary abelian with normalizer N. Let $|G| = 2^r \cdot m$, m odd.

If L is a G-Galois algebra / K, we showed last time that $q_L \cong m \otimes q_L^\circ$ where q_L° has rank 2^r.

Theorem: If r is even, q_L° is an r-Pfister form
If r is odd, $2q_L^\circ$ is an r-Pfister form.

Example: let $G = C_2$, $L = K(\sqrt{d})$, $q_L = 2x^2 + 2dy^2 = 2\langle\langle d \rangle\rangle$

From the above theorem, we only need to prove this after an odd degree field extension. Hence we can assume that L is induced by an S-Galois algebra L_S and $q_L^\circ = q_{L_S}$. We have:

Theorem: Let L be an S-Galois algebra.
(a) If r is even (resp. odd), q_L (resp. $2q_L$) is a Pfister-form
(b) The cohomology class of the Pfister form in (a) in $H^r(K)$ is $e^r + z_L$, $e = (-1)$, z the canonical class (modulo negligibles) in $H^r(S)$

Proof: Identify S with $S_1 \times S_2 \times \dots \times S_r$ with $S_i = C_2$ for all i.
L can be written as $L = L_1 \otimes \dots \otimes L_r$ with L_i a S_i-Galois algebra. Each $L_i = K(\sqrt{\alpha_i})$ and thus $L = K(\sqrt{\alpha_1}) \otimes \dots \otimes K(\sqrt{\alpha_r})$.
One has $q_L \cong \bigotimes_i q_{L_i} \cong 2^r \langle\langle \alpha_1, \dots, \alpha_r \rangle\rangle$, which proves (a).

The invariant is $(-\alpha_1)\cdots(-\alpha_r) = \prod_{i=1}^{r} (e + (\alpha_i))$

$= e^r + e^{r-1} o_1 + \dots + o_r$; with o_i the symmetric functions in $x_i = (\alpha_i)$

$= e^r + \tilde{o}_1 + \dots + \tilde{o}_r$ with $\tilde{o}_1 = x_1^r + \dots + x_r^r$, $\tilde{o}_2 = x_1^{r-1} x_2 + \dots$, $\vdots$

$= e^r + z_L$

Remark: If q_L° is the unit form (e.g. if L has an SNB), then $q_L^\circ \cong \langle\langle 1, \dots, 1 \rangle\rangle$ and its cohomology invariant is both e^r and $e^r + z_L$. Hence $z_L = 0$.

More Group Theory

Lemma: Let H be a finite group, acting on a vector space V over $\mathbb{F}_q$. The number of orbits of H on V equals the number of orbits of H on the dual V^* of V.

In general if H is a finite group acting on a finite set Ω, we have:

Burnside's Lemma (Proved by Frobenius ~1880): The number of orbits of H in Ω is $\frac{1}{|H|} \sum_{h \in H} |\Omega^h|$

(where Ω^h is the subset of Ω fixed by h).

Hence to prove the lemma, we only need to show that $h \in GL(V)$ fixes the same number of elements in V and V^*. We are reduced to proving

Lemma: If s is an automorphism of a vector space V,

$$\dim \ker (s-1)_V = \dim \operatorname{Coker} (s-1) = \dim \ker ({}^t s - 1)_{V^*}$$

Proof: Counting dimensions in the exact sequence

$$0 \to \ker (s-1)_V \to V \xrightarrow{s} V \to \operatorname{Coker} (s-1) \to 0$$

gives $\dim \ker (s-1)_V = \dim \operatorname{Coker} (s-1)$ $\left(= \dim \ker ({}^t s - 1)_{V^*}\right)$

2 It is not true that the action of H on V is isomorphic to the action of H on V^*.

Example: $V = \mathbb{F}_2^3$, $S = SL_3(\mathbb{F}_2)$. $\begin{pmatrix} * & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$ is a parabolic subgroup

$\begin{pmatrix} * & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}$ acts on V^* but the actions are not isomorphic.

Quadratic Spaces

Let V be a vector space with a quadratic form q and an action of a group H under which q is invariant. Call this a "H-quadratic space" for V.

If $H \subset H'$, V a H-quadratic space, we can define $V' = \mathrm{Ind}_H^{H'} V$ by $V' = \bigoplus_{g \in H'/H} gV$. We transport q by g to gV, $q_{V'} = \bigoplus_{g \in H'/H} q_{gV}$ (orthogonal sum)

The resulting form $q_{V'}$ is invariant by G.

Structure of an S-quadratic space:

The characters of S, $S^* = \mathrm{Hom}(S, \{\pm 1\}) \simeq H^1(S)$.
Every V with an S-action can be split $\bigoplus_{\chi \in S^*} V_\chi$

$$\text{with } V_\chi = \{ v \mid v \in V,\ sv = \chi(s)v \text{ for all } s \in S \}$$

V_χ is a quadratic space with $V_\chi \perp V_\psi$ if $\chi \neq \psi$.

Hence, any S-quadratic space is isomorphic to a collection of quadratic spaces indexed by S^*.

Also, given a S-quadratic space V, W a quadratic space, $W \otimes V$ is a S-quadratic space in a natural way.

Conversely, if L_χ is a one-dimensional S-quadratic space, we can write $L_\chi \cong V_\chi \otimes I_\chi$, with V_χ a quadratic space of dimension 1 and I_χ the S-quadratic space of dimension 1 given by

- $I_\chi = k$ as a vector space
- $q(x,y) = xy$ the quadratic form on I_χ
- S acts by χ.

Back to our situation:

Let L be a G-Galois algebra

Theorem: Let S, the 2-Sylow subgroup of G, be elementary abelian. Let the normalizer of S, N, act transitively on $S-\{1\}$. Then the following are equivalent:

1. An SNB exists for L
2. The Pfister form q_L^0 (resp. $2q_L^0$) is the unit form
3. q_L^0 is the unit form
4. q_L is the unit form

Proof: (2) $\Leftrightarrow$ (3) If r is even, there is nothing to prove.
If r is odd, then (3) $\Rightarrow$ (2) since $\langle 2\rangle \otimes \langle 2\rangle \cong \langle 1\rangle \oplus \langle 1\rangle$

(3) $\Leftrightarrow$ (4) has already been proved (by division)
(1) $\Rightarrow$ (2) has also been proved already.

To finish the proof, we may assume 2, 3, and 4, and that $L = \mathrm{Ind}_S^G L_S$, L_S a S-Galois algebra. Hence $L_S \cong \langle 1\rangle \oplus \cdots \oplus \langle 1\rangle$.
To show that 2,3,4 $\Rightarrow$ (1), we need only prove:

Proposition: $\mathrm{Ind}_S^N L_S$ has an SNB

Note: L_S will not in general have an SNB

Proof: By the structure of a S-quadratic space, we have

$$L_S = \bigoplus_{\chi \in S^*} L_\chi \quad \text{with } \dim L_\chi = 1$$

Then $\mathrm{Ind}_S^N L_S = \bigoplus_{\chi \in S^*} \mathrm{Ind}_S^N L_\chi$.

We could then write $L_\chi = V_\chi \otimes I_\chi$, with V_χ a quadratic space of dimension 1.

If χ is conjugate to χ_0 by N, $\mathrm{Ind}_S^N I_\chi \cong \mathrm{Ind}_S^N I_{\chi_0}$

Let Ω be an orbit of N is S^*. One finds that

$$\bigoplus_{\chi \in \Omega} \mathrm{Ind}_S^N(L_\chi) \cong \bigoplus_{\chi \in \Omega} V_\chi \otimes \mathrm{Ind}_S^N I_{\chi_0} \quad \text{for any } \chi_0 \in \Omega$$

This isomorphism is of N- quadratic spaces.

In general, if V is a S-quadratic space, $V = \bigoplus_{\chi \in S^*} V_\chi$, let $V_\chi = Q_\chi \otimes I_\chi$ with Q_χ a quadratic space.
let $Q_\Omega = \bigoplus_{\chi \in \Omega} Q_\chi$ for Ω, an orbit of N in S^*.
Then $\mathrm{Ind}_S^N V = \bigoplus_\Omega Q_\Omega \otimes \mathrm{Ind}_S^N I_{x_\Omega}$, $x_\Omega \in \Omega$

Proposition: Let V, V' be two S-quadratic spaces. If $Q_\Omega \cong Q'_\Omega$ for every orbit Ω of N is S^*, then $\mathrm{Ind}_S^N V \cong \mathrm{Ind}_S^N V'$ as N-quadratic spaces.

Proof: $\mathrm{Ind}_S^N V \cong \bigoplus_\Omega Q_\Omega \otimes \mathrm{Ind}_S^N I_{x_\Omega}$, where $x_\Omega \in \Omega$

$\cong \mathrm{Ind}_S^N V'$

To finish the proof of the theorem, let $V = L_S$, $V' = \mathrm{Ind}_{\{1\}}^S \langle 1 \rangle$.
Since V' has an SNB, so does $\mathrm{Ind}_S^N V'$.
Thus if we can show $Q_\Omega \cong Q'_\Omega$ (for every orbit Ω), we are done.

Now N acts transitively on $S - \{0\}$ so there are two orbits on S and on S^*. (*)
Orbit 1: $\Omega_1 = \{0\}$, Q_{Ω_1} has dimension 1, with basis "1" such that $q_L^0(1,1) = 2^r$.
Same thing for Q'_{Ω_1}

Orbit 2: $\Omega_2 = S^* - \{0\}$. ; $Q_{\Omega_1} \oplus Q_{\Omega_2} = q_{L_S} \cong \langle 1 \rangle \oplus \cdots \oplus \langle 1 \rangle$ by hypothesis
(and same in the split case).
But then $Q_{\Omega_1} \oplus Q_{\Omega_2} \cong Q'_{\Omega_1} \oplus Q'_{\Omega_2}$ and since $Q_{\Omega_1} \cong Q'_{\Omega_1}$,

By witt simplification, $Q_{\Omega_2} \cong Q'_{\Omega_2}$.

Hence by the proposition $\mathrm{Ind}_S^N V \cong \mathrm{Ind}_S^N V'$ has an SNB.

(*) The number of orbits on S and on S^* is the same by the theorem "More Group Theory" of p. 15.3.

Lecture 16

11/13/90

Assume G is a finite group with 2-Sylow S of type $(2,2)$ and with the normalizer of S, N, acting nontrivially on $S-\{0\}$. Hence N acts by an automorphism of order 3. (Equivalently, we could say $H^1(G)=0$).

We have seen that $\dim H^2(G)=1$. If x,y is a basis of $H^1(S)$, then x^2+xy+y^2 is invariant by N and gives the unique non-zero element z of $H^2(G)$. Hence z corresponds to a nontrivial extension of G by C_2:

$$1 \longrightarrow C_2 \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$$

We have seen that the inverse image $\tilde{S}$ of S in $\tilde{G}$ is isomorphic to Q_8 the quaternion group of order 8.

This situation happens for $G = A_5, A_6, PSL_2(\mathbb{F}_p)$ for $p \equiv \pm 3 \ (8)$
[Here $\tilde{G} = SL_2(\mathbb{F}_p)$].

If L is a G-Galois algebra over K and $z_L \in H^2(K)$ is the corresponding cohomology element, we have proved that the following are equivalent:

(a) L has an SNB
(b) $z_L = 0$
(c) $\varphi: G_K \to G$ can be lifted to $\tilde{\varphi}: G_K \to \tilde{G}$

Assume (a), (b), and (c) hold. Then there exists a $\tilde{G}$-Galois algebra $\tilde{L}$ over K such that $\tilde{L}^{C_2} \simeq L$ (by (c)). Note that $\tilde{L}$ is not unique; there can be many liftings.

Question: Does $\tilde{L}$ always (sometimes) have an SNB? The answer is { Yes and No }
More precisely:

Theorem: There is at least one choice of $\tilde{L}$ such that $\tilde{L}$ has an SNB.

Let M be a Q_8-Galois algebra and q_M its trace form. Let C_2 be the center of Q_8. Write $C_2 = \{1, \sigma\}$. Then

$$M = M^+ \oplus M^- \quad \text{with} \quad M^+ = \{n \mid \sigma n = n\} = M^{C_2}$$
$$M^- = \{n \mid \sigma n = -n\}$$

($\dim B$ over M^+, $\dim 4$ over M^-)

Thus M^{C_2} is a $Q_8/C_2 \simeq (2,2)$ Galois algebra

$$G_K \longrightarrow Q_8 \twoheadrightarrow (2,2)$$

Lemma: The quadratic form of $\mathbf{M}^+$ is $\langle 1\rangle\oplus\langle 1\rangle\oplus\langle 1\rangle\oplus\langle 1\rangle = \langle 1,1,1,1\rangle$.

Proof: From last time, $q_{\mathbf{M}^+} = \langle\langle \alpha, \beta\rangle\rangle$. Since M^+ lifts to a Galois Q_8-algebra, $z_{M^+} = 0$, $(-\alpha)(-\beta) = e^2 = (-1)(-1)$. Hence $\langle\langle \alpha, \beta\rangle\rangle \cong \langle\langle 1,1\rangle\rangle$ and $\langle\langle \alpha, \beta\rangle\rangle = \langle 1\rangle\oplus\langle 1\rangle\oplus\langle 1\rangle\oplus\langle 1\rangle$

Now $q_{\mathbf{M}} = q_{\mathbf{M}}^+ \oplus q_{\mathbf{M}}^-$, with $q_{\mathbf{M}}^+ =$ 2×trace form of $\mathbf{M}^+$ (viewed as $(2,2)$-Galois alg
$= 2\otimes(\langle 1\rangle\oplus\langle 1\rangle\oplus\langle 1\rangle\oplus\langle 1\rangle) \cong \langle 1\rangle\oplus\langle 1\rangle\oplus\langle 1\rangle\oplus\langle 1\rangle$

Lemma: $q_{\mathbf{M}}^-$ is isomorphic to $\langle a\rangle\otimes(\langle 1\rangle\oplus\langle 1\rangle\oplus\langle 1\rangle\oplus\langle 1\rangle)$ for some $a\in k^*$, where $a\in k^*/\mathbf{N}D^*$ is well-defined $(D = (-1,-1))$.

Parenthesis on $k^*/$ sum of four squares. $= k^*/[4]$

By theorems of (Jacob, Rost, Arason), $k^*/[4] \xrightarrow{\phi} H^3(k)$

is well-defined, and: $a\in k^* \longmapsto (a)(e)(e)$, $e = (-1)$

Theorem: ϕ is injective.

In general, for every quaternion algebra D (corresponding to $d\in H^2(k)$), we have

$$k^*/\mathbf{N}D^* \hookrightarrow H^3(k)$$
$$a \longmapsto (a)d$$

If $a\in k^*$ is a sum of four squares, then $\langle\langle 1,1,a\rangle\rangle \cong \langle\langle 1,1,1\rangle\rangle$
$\Rightarrow (-1)(-1)(-a) = (-1)(-1)(-1) \Rightarrow (-1)(-1)(a) = 0$.
Conversely, since a 3-Pfister form is determined by the cohomology class in $H^3(k)$, $(-1)(-1)(a) = 0 \Rightarrow \langle\langle 1,1,a\rangle\rangle \cong \langle\langle 1,1,1\rangle\rangle$.
Then $a\cdot(\text{unit form}) \cong (\text{unit form}) \Rightarrow a$ is a sum of 4 squares.

As an example, consider $k = \mathbb{R}$, $H^3(\mathbb{R})$ is cyclic of order 2, generated by e^3. We have $\mathbb{R}/[4] \simeq C_2$

The same thing is true for $k = \mathbb{Q}$, but less obvious. One needs to know that $H^3(\mathbb{Q}) = H^3(\mathbb{R})$. (In general, $H^i(\mathbb{Q}) = H^i(\mathbb{R})$ for $i \geq 3$).

Corollary to Lemma: $q_M \cong \langle\langle 1,1,a \rangle\rangle$

We still have to prove the lemma. This is very easy by the following remarks.

Remark: Let D be the standard quaternions on K.
We have $Q_8 \hookrightarrow D^*$
$\sigma \longmapsto (-1)$
$K[Q_8] \xrightarrow{\text{onto}} D$ with $D \cong K[Q_8]/(1+\sigma)K[Q_8]$
$\cong K[Q_8]/K[Q_8]^+$

Any Q_8-space on which σ acts by -1 is a D-module.
M^- is a free left D-module of rank 1.

Sublemma: $q_L(dx, y) = q_L(x, d^* y)$ for $d \in D$, $d^* = \bar{d}$ = conjugate of d
$x, y \in M^-$

Pf: Check it for $d = q \in Q_8$. Then $d^* = q^{-1}$ since an element of Q_8 has norm 1.
Then $q_L(qx, y) = q_L(q^{-1}qx, q^{-1}y) = q_L(x, q^{-1}y)$ □

Now $q_L(dx, dx) = q_L(x, N(d)x) = N(d)\, q_L(x,x)$.
Choose any $x \neq 0$. x is a D-basis of M^-. Put $\alpha = q_L(x,x) \in M^-$.

Then $q_L(dx, dx) = \alpha N(d)$

Hence to q_N^- we have attached $a \in k^*/[4]$.

q_M = unit form $\iff$ the q_M^- invariant is trivial in $k^*/[4]$
$\iff$ cohomological invariant is zero in $H^3(k)$

Now let H be any finite group with $|H| = 8 \cdot m$, m odd, and with the 2-Sylow group $\cong Q_8$. Let L_H be an H-Galois algebra. Let $q_{L_H} \cong m \otimes q^0_{L_H}$, $q^0_{L_H}$ a form of rank 8.

Proposition: (a) $q^0_{L_H}$ is a 3-Pfister form which can be represented by $\langle\langle 1,1,a\rangle\rangle$ for some well-defined $a \in k^*/|4|$

(b) If q_{L_H} is the unit form (esp. if an SNB exists.), then the invariant is trivial.

Proof: We can choose k'/k an odd degree extension such that over k', L_H is induced by a Q_8-Galois algebra with trace form $q^0_{L_H}$. It remains to prove:

Lemma: If a quadratic form over k has a 3-Pfister form of type $\langle\langle 1,1,a'\rangle\rangle$, $a' \in k'^*$, then it is a 3-Pfister form over k of type $\langle\langle 1,1,a\rangle\rangle$, $a \in k^*$.

Proof: By an induction argument, we may assume $k(a') = k'$.
Scharlau's transfer $s: k' \to k$ $\Big|$ $s(1) = 1$, $s(a'^i) = 0$ $1 \le i < [k':k] = m$

gives $s_*(\langle 1\rangle) = \langle 1\rangle$ in the Witt ring $W(k)$
$s_*(\langle a'\rangle) = \langle Na'\rangle$ " " " "

Hence $s_*(\langle\langle 1,1,a'\rangle\rangle) = \langle\langle 1,1,Na'\rangle\rangle$ in $W(k)$ $\square$.

By the corollary above, $q^0_{L_H} \cong \langle\langle 1,1,a'\rangle\rangle$ over k'. Hence $q^0_{L_H} \cong \langle\langle 1,1,a\rangle\rangle$ over k by the lemma which proves (a).

If q_{L_H} is the unit form, then $\langle\langle 1,1,a\rangle\rangle \cong \langle\langle 1,1,1\rangle\rangle$ and $(-1)(-1)(a) = 0$ as we saw before. Hence (b).

(Open) Question: If the invariant is trivial, is there an SNB?

<u>Theorem</u>: <u>Assume</u> $G \cong H/\{1,\theta\}$, $H \cong \tilde{G}$; <u>If the</u> <u>invariant $a \in k^*/\boxed{4}$ of</u> $\tilde{L}$ <u>is trivial, then an SNB exists</u>.

<u>Proof</u>: By going to an odd degree extension k' of K, we can assume $\tilde{L}$ is induced by a Q_8-Galois algebra $\mathbf{M}$.

$$\tilde{L} = \mathrm{Ind}_{Q_8}^{\tilde{G}} \mathbf{M} = \underbrace{\mathrm{Ind}_{Q_8}^{G} \mathbf{M}^+}_{= \tilde{L}^+} \oplus \underbrace{\mathrm{Ind}_{Q_8}^{G} \mathbf{M}^-}_{= \tilde{L}^-}$$

<u>Claim 1</u>: $\tilde{L}^+ \cong \hat{L}^+_{split}$ as a $\tilde{G}$-quadratic space.

<u>Proof</u>: $\tilde{L}^+ = L$ as G-Galois algebra.
Then by our assumptions on L (L has an SNB), $\tilde{L}^+ \cong \tilde{L}^+_{split}$.

<u>Claim 2</u>: $\mathbf{M}^- \cong \mathbf{M}^-_{split}$ as a Q_8-quadratic space.

<u>Proof</u>: Both are quaternion ~~algebras~~ modules of rank 1 with a hermitian form. By the hypothesis on a, both forms are isomorphic to $\langle 1\rangle \oplus \langle 1\rangle \oplus \langle 1\rangle \oplus \langle 1\rangle$ with the standard action. Hence the claim.

<u>Claim 2</u>: $\Rightarrow$ $\tilde{L}^- \cong \tilde{L}^-_{split}$ as a $\tilde{G}$-quadratic space

Then $\tilde{L} = \tilde{L}^+ \oplus \tilde{L}^- \cong \tilde{L}_{split}$ and $\tilde{L}$ has an SNB.

*6 Now for a given $\tilde{L}$, the obstruction for an SNB is given by $a \in k^*/\boxed{4}$.
If
$$\begin{array}{ccccc} C_2 & \longrightarrow & \tilde{G} & \longrightarrow & G \\ & & \tilde{\varphi} \nwarrow & & \uparrow \varphi \\ & & & & G_k \end{array}$$
, and $\tilde{\varphi}$ corresponds to $\tilde{L}$, we can change $\tilde{L}$ by $\varepsilon : G_k \longrightarrow C_2$ by replacing $\tilde{\varphi}$ by $\varepsilon\tilde{\varphi}$.
let $\varepsilon \in H^1(k)$ corresponds to $\lambda \in k^*/(k^*)^2$. One has to check that $\tilde{\varphi} \longmapsto \varepsilon\tilde{\varphi}$ changes $a \longmapsto a\lambda \in k^*/\boxed{4}$. If we choose ε to correspond to $\lambda = a$, $a\lambda = a^2 = 0$ in $k^*/\boxed{4}$. Hence we have a lifting.

Galois Cohomology For Function Fields

Let $K(T)$ be the field of functions on $\mathbb{P}_1$ over K. We want to compare the Galois cohomology of K and $K(T)$.

We can consider $\alpha \in H^i(K(T))$ as a "function" on $\mathbb{P}_1$ and study its poles, residues, and values outside poles.

Ex: $(-1, T) \in H^2(K(T))$. has poles at $T=0, T=\infty$ with residue $\cdot(-1)$.

$\|$

$(-1)(T)$ For $T \neq 0, \infty$, we have values in $H^i(K')$

A "function" with no poles comes from $H^i(K)$.

We will apply this theory to $K = \mathbb{Q}$, $H^2(\mathbb{Q}(T))$, and conside the specialization of an element.

We will see Mestre's construction of Galois extensions of $\mathbb{Q}(T)$ with Galois groups $6.A_6, 6.A_7$.

Lecture 17

11/15/90

Spectral Sequence of Group Extensions

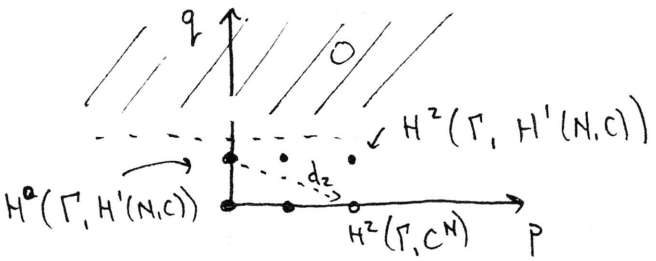
Let G be a profinite group, N a normal subgroup (closed), $\Gamma = G/N$
Let C be a G-module and assume:

$$H^i(N, C) = 0 \quad \text{for all } i \geq 2.$$

The Spectral Sequence gives:

$$H^p(\Gamma, H^q(N, C)) \Longrightarrow H^\cdot(G, C).$$

For $q \geq 2$, $H^p(\Gamma, H^q(N,C)) = 0$ and we have the diagram



$d_i = 0$ for $i \geq 3$ in this situation

$d_2 : H^i(\Gamma, H^1(N,C)) \longrightarrow H^{i+2}(\Gamma, C^N)$.

From the spectral sequence, we have the exact sequence

$$\longrightarrow H^i(\Gamma, C^N) \longrightarrow H^i(G, C) \longrightarrow H^{i-1}(\Gamma, H^1(N,C)) \xrightarrow{d_2} H^{i+1}(\Gamma, C^N) \longrightarrow$$

$$\uparrow \text{ map given by}$$

$$\alpha \longmapsto G \to \Gamma \xrightarrow{\alpha} C^N \to C$$

[This just says that $H^i(G,C)$ is filtered $0 \subset A \subset H^i(G,C)$
with $A = H^i(\Gamma, C^N)/\operatorname{Im} d_2$
$H^i(G,C)/A = \operatorname{Ker} d_2$ on $H^{i+1}(\Gamma, H^1(N,C))$.]

Remark: We can deduce the spectral sequence of group extensions from the spectral sequence in topology. The cohomology of G equals the (topological) cohomology of BG and one uses the fibering

BG
| fiber BN
$B\Gamma$

Special Case: Now we assume:

(1) N acts trivially on C
($\Rightarrow C^N = C$, $H^1(N, C) = \operatorname{Hom}(N, C)$)

(2) G is the semi-direct product of Γ by N
($\Rightarrow H^i(\Gamma, C) \hookrightarrow H^i(G, C)$ is split)

(2) $\Rightarrow d_2 = 0$ and the exact sequence breaks into pieces

$$0 \to H^i(\Gamma, C) \longrightarrow H^i(G, C) \xrightarrow{r} H^{i-1}(\Gamma, H^1(N,C)) \longrightarrow 0$$

What is the homomorphism r?

Group cohomology is the right derived functor of $C \longrightarrow C^G$. But we can write $C \longrightarrow C^G$ as the composition of $C \longrightarrow C^N$ and $C \longrightarrow C^{G/N}$. Then by general nonsense, we can derive the spectral sequence. However, we have no idea what the maps in the exact sequence are. In Hochschild-Serre (Transactions of the AMS, 1953), we have an explicit recipe for computing $r(\alpha)$, $\alpha \in H^i(G,C)$. **Namely:**

Claim: There exists a cocycle $f(s_1, \cdots, s_i)$ on G representing α such that
(1) $f(s_1, \cdots, s_i) = 0$ if one of the $s_j = 1$ "f is normalized"
(2) $f(s_1, s_2 n_2, \cdots, s_i n_i) = f(s_1, s_2, \cdots, s_i)$ for all $s_j \in G$, $n_2, \cdots, n_i \in N$

Then $r(f)$ is the $i-1$ cochain g on Γ given by
$g(\gamma_1, \cdots, \gamma_{i-1})(n) = f(n, g_1, \cdots, g_{i-1})$, where the g_j are representatives of γ_j in G.
$g(\gamma_1, \cdots, \gamma_{i-1})$ is a $i-1$ cochain in $\mathrm{Hom}(N, C)$

Example. $i=2$ $\alpha \in H^2(G,C)$. α corresponds to some extension $E = E_\alpha$ of G by C:

$$1 \longrightarrow C \longrightarrow E_\alpha \xrightarrow{\pi} G \longrightarrow 1$$
$$\cup$$
$$N \simeq N$$

If the restriction of α to N is trivial, there exists a section $N \longrightarrow E_\alpha$ which is a homomorphism.

Let $G = \Sigma \cdot N$ with Σ a system of representatives. Lift Σ to Σ_E in E. Then $\Sigma_E N$ defines a section (set-theoretic) of $E = C(\Sigma_E N)$. Let $\sigma: G \to E$ be the map corresponding to $\Sigma_E N$

$$\sigma(gn) = \sigma(g)\sigma(n), \quad g \in G, \ n \in N$$

Then α defines a cocycle f by

$$\boxed{\sigma(s)\,\sigma(t) = f(s,t)\,\sigma(st)} \quad ; \quad \sigma(1) = 1$$

Now $\sigma(s)\,\sigma(tn) = f(s,tn)\,\sigma(stn)$

$\Rightarrow \sigma(s)\,\sigma(t)\sigma(n) = f(s,tn)\,\sigma(st)\sigma(n)$

$\Rightarrow \sigma(s)\,\sigma(t) = f(s,tn)\,\sigma(st) \Rightarrow f(s,tn) = f(s,t)$

We then find r by $r(\alpha)(\lambda)(n) = f(n,\lambda)$.

Formula for cup-products

Now let $C_1 \times C_2 \to C$ be a homomorphism of Γ-modules.

let $\alpha_1 \in H^i(G, C_1)$, $\beta_2 \in H^j(\Gamma, C_2) \longmapsto \alpha_2 = \pi_j^* \beta_2 \in H^j(G, C_2)$

$\alpha = \alpha_1 \cdot \alpha_2 \in H^{i+j}(G, C)$, $r(\alpha) \in H^{i+j-1}(\Gamma, \mathrm{Hom}(N, C))$

Claim: $r(\alpha_1 \cdot \alpha_2) = r(\alpha_1) \cdot \beta_2$

We have the pairing $\mathrm{Hom}(N, C_1) \times C_2 \longrightarrow \mathrm{Hom}(N, C)$

$r(\alpha_1) \times \beta_2 \longmapsto r(\alpha_1) \cdot \beta_2$.

Recall $f \cup g(\sigma_1, \cdots, \sigma_i, \sigma_{i+1}, \cdots, \sigma_{i+j}) = f(\sigma_1, \cdots, \sigma_i)^{\sigma_1 \cdots \sigma_i} g(\sigma_{i+1}, \cdots, \sigma_{i+j})$

We can check the claim if the effect of r on cup-products using this.

Local Cohomology

Let K be a local field, complete with discrete valuation v. Let k be the residue field. Assume k is perfect.

Let $\bar{k}$ be some algebraic closure of k, K_{nr} the maximal unramified extension of K (inside K_s). We have

$$G_K \left(\begin{array}{c} K_s \\ | \\ \end{array} \right) N \qquad \text{with } N = \mathrm{Gal}(K_s / K_{nr})$$

$$\left. \begin{array}{c} | \\ K_{nr} \\ | \end{array} \right) \Gamma \qquad \Gamma = \mathrm{Gal}(\bar{k}/k)$$

$$K$$

Fact: N has cohomological dimension 1.

N is the inertia group and there is an exact sequence

$1 \to P \to N \to I \to 1$ with P a profinite p group

I a tame ramification group

We have $I = \varprojlim_{(n,p)=1} I_n$, $I_n \cong \mu_n(\bar{k}) = \mu_n(K_s)$ $\left(\cong \prod_{\ell \neq p} \mathbb{Z}_\ell\right)$

Let $K_{nr}^{(n)}$ be the unique cyclic extension of degree n of K_{nr}.

$K_{nr}^{(n)}$ can be obtained by extracting an nth root of a uniformizing element.

Then $I_n \cong \mathrm{Gal}(K_{nr}^{(n)}) \xrightarrow{\sim} \mu_n$. If π_n is a uniformizing element of $K_{nr}^{(n)}$, this map is given by $s \in \mathrm{Gal}(K_{nr}^{(n)}) \longmapsto \frac{s\pi_n}{\pi_n} = \xi \in \mu_n(\bar{k})$.

In the limit, $I_{\ell^\infty} \cong \mathbb{Z}_\ell(1)$, so that $I = \prod_{\ell \neq p} \mathbb{Z}_\ell(1)$.

Now assume C is finite with order prime to p. C is killed by some n.
$\mathrm{Hom}(N, C) = \mathrm{Hom}(\mu_n, C) = C(-1)$. $(= \mu_n(-1) \otimes C)$

Claim: $H^i(\Gamma, C) \to H^i(G, C)$ is injective for all i
(We could assume this instead of the assumption that $G = N \rtimes \Gamma$)

Example of computation of $r: H^2(G, C) \to H^1(\Gamma, C(-1))$ when $C = \mu_n$, $(n,p)=1$.

$H^2(G, \mu_n) = Br_n(K)$

$\mathrm{Hom}(C, \mu_n) = C(-1) = \mathbb{Z}/n\mathbb{Z}$.

$$r : Br_n(K) \longrightarrow \mathrm{Hom}(\Gamma, \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Hom}(\Gamma, \tfrac{1}{n}\mathbb{Z}/\mathbb{Z})$$
$$\cap$$
$$\mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z}).$$

Now Witt showed:

$$0 \to Br(k) \to Br(K) \xrightarrow{r_{Witt}} \mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z}) \to 0$$

Theorem: $r = -r_{Witt}$

Recall that if $a \in K^*$, $\chi \in \mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z})$, then $\alpha \cdot \delta\chi \in Br_n(K)$
since $\alpha = (a) \in H^0(G_K, K_S^*)$
$\chi \in H^1(G_K, \mathbb{Q}/\mathbb{Z})$ and $\alpha \cdot \delta\chi \in H^2(G_K, K_S^*)$

Thus we have an explicit way of getting elements in the Brauer group. Start with $\gamma \in \mathrm{Hom}(\Gamma, \mathbb{Z}/n\mathbb{Z})$, lift to G. This gives an unramified character $\chi \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$. Then for $\alpha \in k^*$, $\alpha \cdot \delta\chi \in Br_n K$.
We have:

Theorem: $r(\alpha \cdot \delta\chi) = -r(\alpha) \cdot \gamma$, $r(\alpha) \in \mathbb{Z}$.

Lecture 18

11/20/90

We will need two lemmas to prove the theorem stated last time.

Lemma: If k has characteristic $p>0$, $\Gamma = \mathrm{Gal}(k_s/k)$, then $\mathrm{cd}_p \Gamma \leq 1$

Proof: In general, one has the exact sequence of algebraic groups:
$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{G}_a \xrightarrow{\wp} \mathbb{G}_a \to 0$ with $\wp z = z^p - z$. Applying this to k_s, we have $0 \to \mathbb{Z}/p\mathbb{Z} \to k_s \xrightarrow{\wp} k_s \to 0$ and the long exact cohomology sequence:

$$0 = H^{i-1}(\Gamma, k_s) \to H^i(\Gamma, \mathbb{Z}/p\mathbb{Z}) \to H^i(\Gamma, k_s) = 0 \quad \text{for } i \geq 2$$

shows that $H^j(\Gamma, \mathbb{Z}/p\mathbb{Z}) = 0$ for $j \geq 2$. Hence $\mathrm{cd}_p \Gamma \leq 1$

Note: If $\Gamma' \subset \Gamma$ is a closed subgroup, $\mathrm{cd}_p \Gamma' \leq 1$ by the same argument

Lemma: Let $1 \to P \to E \to \Gamma \to 1$ be an exact sequence of profinite groups with P a pro-p-group and $\mathrm{cd}_p \Gamma \leq 1$. Then $E = P \cdot \Gamma$ (semi-direct product)

Proof: This is proven in LNS, I-23, by a "dévissage" argument.

Now recall the situation from last time. K is a local field, complete with respect to valuation v. Assume the residue field k is perfect. Let K_s the separable closure of K, K_{nr} the maximal unramified extension of K in K_s, and $\bar{k}$ the algebraic closure of k. Let $G = \mathrm{Gal}(K_s/K)$, N = the inertia group $= \mathrm{Gal}(K_s/K_{nr})$ and $\Gamma = G/N = \mathrm{Gal}(\bar{k}/k)$.

If $\mathrm{char}\, k = p > 0$, let P be the largest pro-p-subgroup of N. (= wild ramification group)
Then $I_k = N/P = \prod_{\ell \neq p} \mathbb{Z}_\ell(1) = \mathrm{Gal}(K_t/K_{nr})$ = the tame ramification group.

From last time, we need to prove:

Theorem: The extension $1 \to N \to G \to \Gamma \to 1$ splits

Remarks: 1) If $\mathrm{char}\, k = 0$, $P = \{1\}$, $N = I_t$ and the theorem is easier to prove.
2) If k is finite, then $\Gamma = \hat{\mathbb{Z}}$ and we have an obvious lifting given by lifting the topological generator 1 of $\hat{\mathbb{Z}}$.

Now let π be a uniformizing element in K.

Claim: We can define $\pi_n \in K_s$ for every n prime to π such that $\pi_1 = \pi$, $\pi_{nm}^n = \pi_m$ for all (n,m)

In other words, it is possible to choose the n^{th} roots of π in a coherent manner. Let S_n = the n^{th} roots of π in K_s, $|S_n| = n$. Consider the map $S_{mn} \to S_n$, $z \longmapsto z^m$. This defines a projective system and $\varprojlim S_n \neq \emptyset$. A point in $\varprojlim S_n$ is exactly the sequence $\{\pi_n\}$ we desire. Hence the claim is proven.

Now choose such a sequence (π_n). Let $K_n = K(\pi_n)$, $K_\infty = \bigcup_n K_n$.
Let H be a subgroup of G which fixes K_∞.

K_s
| H
K_∞
|
K

Claims: ① $G = H \cdot N$
② $H \cap N = P$

Note: If $\mathrm{char}\, k = 0$, then $P = \{1\}$ and ① + ② $\Rightarrow$ G is a semi-direct product of H and N. Hence the theorem.
In general, ① and ② $\Rightarrow$ G/P is a semi-direct product of Γ and $I_t = N/P$.

Now since K_n is totally ramified of degree n over K, $K_{nr} \cap K_\infty = K$ and $G = H \cdot N \Rightarrow$ ①. One has $K_{nr} \cdot K_n = K_{nr}(\pi^{1/n})$ and $K_{nr} \cdot K_\infty = K_t$.
Then $P = H \cap N \Rightarrow$ ②.

Proof of the Theorem: By the lemma, $0 \to P \to H \xrightarrow{\varepsilon} \Gamma \to 1$ and the inclusion $H \subset G$ gives the desired lifting $\Gamma \to G$. Hence G is a semi-direct product.

We saw last time that the theorem implies that:

$$0 \to H^i(\Gamma, C) \to H^i(G, C) \to H^{i-1}(\Gamma, C(-1)) \to 0 \quad \text{is exact.}$$

with C a finite Γ-module of order prime to p and

$$C(-1) = \mathrm{Hom}(\mu_n, C) = \mathbb{Z}/n\mathbb{Z}(-1) \otimes_{\mathbb{Z}} C \quad \text{for } (n,p)=1,\ nC = 0,$$

with $$\mathbb{Z}/n\mathbb{Z}(d) = \begin{cases} \mu_n^{\otimes d} & \text{if } d \geq 0 \\ \text{dual of } \mu_n^{\otimes -d} & \text{if } d < 0 \end{cases}$$

More intrinsically, we could give $C(-1)$ by

$$C(-1)_\ell = \mathbb{Z}_\ell(-1) \otimes_{\mathbb{Z}_\ell} C_\ell \quad \text{with} \quad \mathbb{Z}_\ell(d) = \varprojlim \mu_{\ell^n}^{\otimes d}$$

Note that $\mathbb{Z}_\ell(d)$ is a free $\mathbb{Z}_\ell$-module of rank 1.

We now study the map r ("residue map") in detail.

Computation of r for $i=2$, $C=\mu_n$

We have $C(-1)=\mathbb{Z}/n\mathbb{Z}$, $H^2(G,C)\cong Br_n(K)$, and $H^1(\Gamma, C(-1)) = \mathrm{Hom}(\Gamma, \mathbb{Z}/n\mathbb{Z})$. Let $\varphi \in \mathrm{Hom}(\Gamma, \mathbb{Z}/n\mathbb{Z})$ and lift it to $\chi \in \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$. For $\alpha \in K^*$, $\alpha \cdot \delta\chi \in Br_n(K)$ and we have:

$$r(\alpha \cdot \delta\chi) = -v(\alpha)\cdot\varphi$$

Earlier in the course, we have proven $\alpha\cdot\delta\chi = -(\alpha)\cdot\chi$ where $(\alpha) \in H^1(G,\mu_n) = K^*/(K^*)^n$. From last time $r(\alpha\cdot\delta\chi) = -r((\alpha)\cdot\chi)$ $= -r((\alpha))\cdot\varphi$. Hence we need to show $r((\alpha)) \equiv v(\alpha)$ modulo n.

It is enough to prove $r((\alpha)) \equiv v(\alpha) \pmod n$ for all uniformizing elements π. Let $\alpha = \pi$. Then $r((\pi)) \in H^0(\Gamma, \mathbb{Z}/n\mathbb{Z})$. Now $(\pi) \in H^1(G,\mu_n)$ is given by $s \in G \longmapsto \frac{s\pi^{1/n}}{\pi^{1/n}} \in \mu_n$. Our identification $C(-1) = \mathbb{Z}/n\mathbb{Z}$ then proves $r((\alpha)) \equiv v(\alpha)$ modulo n.

Now since k is perfect, we have the exact sequence

$$0 \to Br_n(k) \to Br_n(K) \xrightarrow{r} \mathrm{Hom}(\Gamma, \mathbb{Z}/n\mathbb{Z}) \to 0$$

This is a specific case of a theorem of Witt. Witt proved that having chosen a uniformizing element π of K, then $Br(K) \cong Br(k) \times \mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z})$ and $0 \to Br(k) \to Br(K) \xrightarrow{r_{witt}} \mathrm{Hom}(\Gamma, \mathbb{Q}/\mathbb{Z}) \to 0$.
This relates to the exact sequence above since

Theorem: $r_{witt} = -r$

By the construction of Witt, $r_{witt}(\pi\cdot\delta\chi) = \varphi$. Hence $r(\pi\cdot\delta\chi) = -r_{witt}(\pi\cdot\delta\chi) = -\varphi$
By Witt's results, every element of $Br_n(K)$ is the sum of an element in $Br(k)$ and $\pi\cdot\delta\chi$, for some χ.

Remark: The residue map $r: H^i(G,C) \to H^{i-1}(\Gamma, C(-1))$ also makes sense when K is not complete(*), but still has a discrete valuation v. Let w be an extension of v to K_s (w is not discrete). Let G_w be the decomposition group, ($G_w = \{s \in G_K \mid s(w) = w\}$. Let $\hat{K}$ be the completion of K. Then $G_w = Gal(\hat{K}_s/\hat{K})$ and $Gal(\hat{K}_s/\hat{K}) \longrightarrow G_w \subset G_K$. Hence,

$$H^i(G_K, C) \to H^i(G_{\hat{K}}, C) \xrightarrow{r} H^{i-1}(\Gamma, C(-1))$$

(*) Allowing of course that the inertia group acts trivially on C.

Special case: $C = \mathbb{Z}/2\mathbb{Z} = \mu_2$. We can give a direct description of r.

$r: H^2(G_K, C) \to H^1(\Gamma, C(-1))$.

$Br_2(K) \xrightarrow{r} k^*/(k^*)^2$

By Mercuriev's theorem, $Br_2(K)$ is generated by (f,g), $f,g \in K^*$.

Formula:

① If $f \in K^*$ has valuation n for v, $g \in K^*$ has valuation 0, and $\tilde{g}$ is the image of g in k^*, then $r((f,g)) = (\tilde{g}^n) \in k^*/(k^*)^2 = \begin{cases} 1 & \text{if } n \text{ even} \\ (\tilde{g}) & \text{if } n \text{ odd} \end{cases}$

② Every (f,g) is a sum of (f_i, g_i) where the g_i's are units (i.e. $v(g_i) = 0$)

By choosing π to be a uniformizing element, it is enough to calculate r for $(\pi,\pi) = (\pi,-1)$, $(\pi, \text{unit}) = (\text{unit}, \pi)$, and $(\text{unit}, \text{unit})$. Then the formulas apply and we can calculate r. We can describe the kernel of r by the following lemma.

Lemma: Let $C = \mathbb{Z}/2\mathbb{Z}$, $\alpha \in Br_2(K)$ such that $r(\alpha) \in k^*/(k^*)^2$ is trivial. Then α is a sum of (f_i, g_i) for f_i, g_i v-units of K.

Proof: By Mercuriev's, $\alpha = \sum (a_j, b_j)$ for $a_j, b_j \in K^*$. Choose π a uniformizing element, $a_j = \pi^{n_j} c_j$ with c_j, d_j v-units.
$b_j = \pi^{m_j} d_j$

Then $\alpha = (\pi, h) + \sum_\lambda (e_\lambda, f_\lambda)$ for e_λ, f_λ, h v-units in K^*.

By the formulas, $r(\alpha) = 0 \iff \tilde{h}$ is a square.
If K is complete, then h is a square and we are done. If K is not complete,

Lemma: There exists a v-unit u such that $v(hu^2 - 1)$ is 1.

Proof: If $v(h-1)$ is >1, then replace h by $h(1+\pi)^2$. $(1+\pi)^2 \equiv 1 + 2\pi \mod \pi^2$
Hence $v(h-1) = v((h-1) + 2\pi h + \pi^2 h) = 1$.

Let u be as in the lemma. Replace h by hu^2. Then $v(h-1) = 1$ and $h - 1 = \pi u'$, u' a unit. $0 = (h, 1-h) = (h, \pi u') = (h,\pi) + (h, u')$
Hence $(h,u') = (h,\pi)$ and α can be written in the desired form.

Lecture 19

11/27/90

As last time, let k have valuation v, perfect residue field $\mathbb{k}$, let $G = G_k$, $\Gamma = \mathrm{Gal}(\bar{\mathbb{k}}/\mathbb{k}) = G_{\mathbb{k}}$, C a finite G-module (unramified action) with order prime to $\mathrm{char}\,\mathbb{k}$. Consider the residue map $r: H^i(G,C) = H^i(K,C) \longrightarrow H^{i-1}(\Gamma, C(-1)) = H^{i-1}(\mathbb{k}, C(-1))$. We want to give criteria for the residue to be trivial.

Proposition: Let Φ be a finite group, $\varphi: G \to \Phi$ a homomorphism, and let C be a finite Φ-module of order prime to $\mathrm{char}\,\mathbb{k}$. Assume the inertia subgroup I of G is such that $\varphi(I)$ acts trivially on C. Then if $\alpha \in H^i(\Phi, C)$, $\varphi^*\alpha \in H^i(G,C)$ and we have $e \cdot r(\varphi^*(\alpha)) = 0$ with $e = |\varphi(I)|$.

Cor: If e is prime to $|C|$, then the residue of $\varphi^*(\alpha)$ is 0.

To prove the proposition, we may assume that k is complete. The following lemma will be useful for the proof.

Lemma: Let K'/K be a finite extension. Let $\mathbb{k}'$ be the residue field of K'. The diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^i(\mathbb{k}, C) & \longrightarrow & H^i(K, C) & \xrightarrow{r} & H^{i-1}(\mathbb{k}, C(-1)) & \longrightarrow & 0 \\ & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow e\cdot\mathrm{Res} & & \\ 0 & \longrightarrow & H^i(\mathbb{k}', C) & \longrightarrow & H^i(K', C) & \longrightarrow & H^{i-1}(\mathbb{k}', C(-1)) & \longrightarrow & 0 \end{array}$$

is commutative, where Res denotes the restriction maps in cohomology that arise from $G_{K'} \subset G_K$ and e is the ramification index of K'/K.

Proof: From

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & \Gamma & \longrightarrow & 1 \\ & & \cup & & \cup & & \cup & & \\ 1 & \longrightarrow & N' & \longrightarrow & G' & \longrightarrow & \Gamma' & \longrightarrow & 1 \end{array}$$

, we have the diagram (of restriction maps)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^i(\Gamma, C) & \longrightarrow & H^i(G, C) & \longrightarrow & H^{i-1}(\Gamma, H^1(N, C)) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^i(\Gamma', C) & \longrightarrow & H^i(G', C) & \longrightarrow & H^{i-1}(\Gamma', H^1(N', C)) & \longrightarrow & 0 \end{array}$$

Looking at the cochains, the commutativity of this diagram is obvious. Now $H^1(N,C) = \mathrm{Hom}(N^{ab}, C)$. Then a trivial calculation shows

$$\begin{array}{ccc} \mathrm{Hom}(N^{ab}, C) & & \mathrm{Hom}(N'^{ab}, C) \\ \| & & \| \\ \mathrm{Hom}\left(N^{ab}, \prod_{\ell \neq p} \mathbb{Z}_\ell(1)\right) & \xrightarrow{e} & \mathrm{Hom}\left(N'^{ab}, \prod_{\ell \neq p} \mathbb{Z}_\ell(1)\right) \end{array}$$

Remark: If you consider the Corestriction maps, one has the diagram:

$$\begin{array}{ccccccccc} 0 & \to & H^i(\Gamma', C) & \to & H^i(G', C) & \to & H^{i-1}(\Gamma', H^i(N', C)) & \to & 0 \\ & & \downarrow e\cdot \mathrm{Cor} & & \downarrow \mathrm{Cor} & & \downarrow \mathrm{Cor} & & \\ 0 & \to & H^i(\Gamma, C) & \to & H^i(G, C) & \to & H^{i-1}(\Gamma, H^i(N, C)) & \to & 0 \end{array}$$

Commutativity of the first square is straight-forword, but I haven't proved the commutativity of the second square.

Remark on the Spectral Sequence for Group Extensions:

Suppose $(G:G') = n = ef$, $(H:H') = e$, $(G/H : G'/H') = f$

$$\begin{array}{ccccccccc} 1 & \to & H & \to & G & \to & G/H & \to & 1 \\ & & \cup & & \cup & & \cup & & \\ 1 & \to & H' & \to & G' & \to & G'/H' & \to & 1 \end{array},$$

then Cor (should be) compatible with the spectral sequence.

$$\begin{array}{ccc} H^i(G/H, H^i(H)) & \Rightarrow & H^i(G) \\ \uparrow \mathrm{Cor} & & \uparrow \mathrm{Cor} \\ H^i(G'/H', H^i(H')) & \Rightarrow & H^i(G') \end{array}$$

Now back to the proof of the proposition. Assume that we have proven the following lemma

Lemma: With notations as in the proposition, there is an open subgroup G' of G of index e such that $\varphi|_{G'}$ is unramified (i.e. $\varphi(I \cap G') = \{1\}$).

Remark: This is equivalent to finding k'/k, $[k':k] = e$ such that k'/k is totally ramified

Proof of Prop: Now $\varphi^*\alpha|_{G'} = \varphi'^*\alpha$, $\begin{array}{ccc} G' & \xrightarrow{\varphi'} & \Phi \\ & \searrow \quad \nearrow & \\ & \Gamma & \end{array}$

Hence $\varphi'^*\alpha$ comes from $H^i(\Gamma', C) = H^i(k', C)$ and the residue is zero. Since k'/k is totally ramified, $k = k'$ and the Restriction map is the identity. $e\cdot r(\varphi^*\alpha) = 0$ in $H^i(k, C)$.

Proof of Lemma: Let $G = I \cdot \Gamma$ be the semi-direct decomposition of G. Call I' the kernel of $I \to G \xrightarrow{\varphi} \Phi$. I' has index e in I. I' is invariant in G. Let $G' = I' \cdot \Gamma$ (it is well-defined). One checks that G' works.

Cohomology of $k(T)$

Again, assume k perfect, $\Gamma = \mathrm{Gal}(\bar{k}/k)$, C a Γ-module, finite with order prime to char k. One wants to relate the cohomology of k and that of $K = k(T)$. We view K as the field of functions on the projective line. By abuse of notation, we write $K\bar{k} = \bar{k}(T)$.

One has $1 \to N \to G_K \to \Gamma \to 1$,

$$G_K \left(\begin{array}{c} \bar{K} \\ | \; N \\ K\bar{k} \\ | \; \Gamma \\ K \end{array} \right.$$

More generally, let X be a projective, smooth curve $/k$, absolutely irreducible (i.e. k = "field of constants") let $K = k(X)$ = field of rational functions f on X. Again one has

$$1 \to N \to G_K \to \Gamma \to 1,$$

$$G_K \left(\begin{array}{c} \bar{K} \\ | \; N \\ \bar{k}(X) \\ | \; \Gamma \\ K \end{array} \right.$$

In general, one asks
1) Is G_K a semi-direct product?
2) Is $\mathrm{cd}\, N \le 1$?

① If X has a rational point $/k$, then $1 \to N \to G_K \to \Gamma \to 1$ splits.

Proof: Choose a rational point of X. It defines a valuation v of K which one extends to $\bar{K}$. Let w be an extension of v. Note that the residue field of v on K is k, of $\tilde{v}$ on $\bar{k}\cdot K$ is $\bar{k}$, and of w on $\bar{K}$ is $\bar{k}$.
Let $D = D_w$ = the decomposition group of w.
Then

$$\begin{array}{ccc} D_w & \xrightarrow{\text{onto}} & \mathrm{Gal}(\bar{k}/k) \\ \cap & & \| \\ G_K & \longrightarrow & \Gamma \end{array}$$

commutes. By local theory, we can lift Γ in D_w, hence in G_K.

② By Tsen's theorem, $\mathrm{cd}\, N = 1$

Theorem: (Tsen) $\bar{k}(x)$ is C_1.

definition: If F is a field, F is $C_1 \Leftrightarrow$ Every homogeneous polynomial over F in more indeterminates than its degree has a non-trivial zero.

It is known that F $C_1 \Rightarrow \mathrm{cd}\, G_F \le 1$

Proposition: (Tsen) If k is algebraically closed, then $k(T)$ is C_1.

Proof: Let $\varphi = \sum c_\alpha X^\alpha$, $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, $|\alpha| = d$. By multiplying by a scalar, we can assume $c_\alpha \in k[T]$. Write $X_i = x_i(T)$, a polynomial of some large degree $N-1$. Since each x_i has N coefficients, there are nN indeterminates and less than $dN+c$ equations where $c = \sup \deg c_\alpha$. Since $nN \geq dN+c$ for N large enough, there is a solution for the coefficients of $x_i(T)$ by the lemma:

Lemma: If $g_j(Y_1, \cdots, Y_m)$ are polynomials, $j = 1, \cdots, m'$, $g_j(0, \cdots, 0) = 0$, $m' < m$, then there is a non-trivial zero.

Proof: Consider the intersection of the hypersurfaces g_j. It is an algebraic variety over an algebraically closed field and has infinitely many points.

Proposition: If K is C_1, any finite extension is C_1.

Proposition: If K is C_1, $Br\, K = 0$.

Proof: The norm form of a division algebra of degree d has degree d and d^2 variables.

Proposition: If K is C_1, $cd\, G_K \leq 1$

For the proofs of these propositions, see LN5 or Corps Locaux.

Remark: (The principle of another proof that $cd\, N = 1$) In characteristic 0, we know the structure of N. Extensions (finite) are ramified at a finite set of places. If we denote such sets by S, we have $N = \varprojlim \pi_1(X-S)^{alg}$.

Lemma: $\pi_1(X-S)$, if $S \neq \emptyset$, is a free-profinite group

This is proved by going to $\mathbb{C}$ and comparing with the topological fundamental group.

Then $cd\, \pi_1(X-S) \leq 1$ and hence $cd\, N \leq 1$.

Now consider a conic without a point. Let X be a conic, $C = \mathbb{Z}/2\mathbb{Z}$. This corresponds to $\alpha \in Br_2 k = H^2(\Gamma, C)$. It is easy to see that α is in the kernel of $H^2(\Gamma, C) \longrightarrow H^2(G, C)$. Hence the map $H^0(\Gamma, H^1(N, C)) \xrightarrow{\delta} H^2(\Gamma, C)$ has image $\{0, \alpha\}$.

Arason has proved that $\ker \{ H^3(k, \mathbb{Z}/2\mathbb{Z}) \longrightarrow H^3(K, \mathbb{Z}/2\mathbb{Z}) \}$ is the set $\alpha \cdot x$, for $x \in H^1(k, \mathbb{Z}/2\mathbb{Z})$. Is this true for H^i, $i > 3$?

Let $\underline{X}$ = closed points of X. By abuse of notation, we write $X = \underline{X}$.
Let K_v be the completion of K at v. For $\alpha \in H^i(K, C)$, we have $\alpha_v \in H^i(K_v, C)$, and $r_v(\alpha) = r_v(\alpha_v) \in H^{i-1}(k(v), C(-1))$.

Theorem: Let $\alpha \in H^i(K, C)$. Then

1. α has only finitely many poles. (i.e. $r_v(\alpha) = 0$ for all v but a finite number.)
2. (Residue formula) $\sum_{v \in \underline{X}} \mathrm{Cor}_{k}^{k(v)} r_v(\alpha) = 0$ in $H^{i-1}(k, C(-1))$
3. If $\alpha \in H^i(k, C)$, then α has no pole. (all its residues are zero). Conversely, if α has no pole and the genus is 0, $(K \simeq k(T))$, then $\alpha \in H^i(k, C)$.

Cor: $(K = k(T))$. If $\alpha \in H^i(K, C)$ has no pole and vanishes at one rational point (i.e. $\alpha(v) = 0$ for some v with $k(v) = k$) then $\alpha = 0$.

Lecture 20

11/29/90

We are interested in regular extensions of $\mathbb{Q}(T)$ with Galois group G. Consider a central extension $1 \to C \to G \to A_n \to 1$.

Theorem: (Mestre) *G is the Galois group of a regular extension of $\mathbb{Q}(T)$. Hence it is a Galois group over any number field.*

definition: A central extension $1 \to \Gamma \to \hat{H} \to H \to 1$ is a universal central extension if for $1 \to C \to E \to H \to 1$ a central extension, there exists $\varphi: \Gamma \to C$, such that $E = \hat{H} \times C / \Gamma$ where $\Gamma \to \hat{H} \times C$, $\gamma \mapsto (\gamma, \varphi(\gamma)^{-1})$

Note: Γ can be shown to be $H_2(H, \mathbb{Z})$.

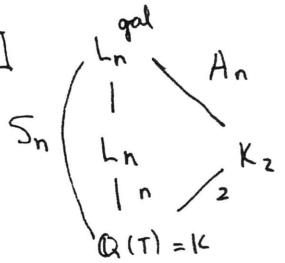
When $H = (H, H)$, Schur showed that there is a universal central extension of H. For A_n, Schur proved that $\hat{A}_n = 2 \cdot A_n$ for $n \neq 6, 7$, $\hat{A}_n = 6 \cdot A_n$ for $n = 6, 7$. If G is a central extension of A_n, then G is a quotient of $\hat{A}_n \times C$. Hence by reduction it is enough to show that $\hat{A}_n \times C$ is a Galois group. C is abelian and we know it is a Galois group. So it is enough to show that $\hat{A}_n$ is a Galois group. For $n \neq 6, 7$, this was shown by Mestre in Journal of Algebra, June 1990. Today, Mestre will show how to do it for $\hat{A}_6$ ($\hat{A}_7$ is similar). The construction consists of two steps:

① Construct an extension K_n ($n = 6, 7$) of $K = \mathbb{Q}(T)$ with Galois group A_n.

② From ①, we have $G_K \xrightarrow{\varphi} A_n$ (surjective). $1 \to C_6 \to \hat{A}_n \to A_n \to 1$ corresponds to $\alpha \in H^2(A_n, C_6)$. One can define $\varphi^*(\alpha) \in H^2(K, C_6)$. $\varphi^*(\alpha)$ is the obstruction to lifting $\varphi: G_K \dashrightarrow \hat{A}_n \downarrow A_n$.

We must show that $\varphi^*(\alpha) = 0$.

n=6



One constructs a degree n extension L_n/K with Galois closure L_n^{gal}, Galois group S_n. We want K_2/K to be a quadratic extension contained in L_n^{gal} with K_2 a purely transcendental extension of $\mathbb{Q}$, $K_2 = \mathbb{Q}(t)$. Then L_n^{gal}/K_2 will be an extension with Galois group A_n.

Details of the construction: Let $L_n = \mathbb{Q}(X)$ for some X, $k = \mathbb{Q}(T)$.
Let $T = \frac{P(X)}{Q(X)}$ where P is a monic polynomial of degree 6
Q is a polynomial of degree 5, no multiple roots,
and $(P, Q) = 1$.
$\mathbb{Q}(T) \subset \mathbb{Q}(X)$ gives a map $\mathbb{P}' \longrightarrow \mathbb{P}'$. Since Q has no multiple roots, there is no ramification at ∞. $T = P(X)/Q(X) \Rightarrow \frac{dT}{dX} = (P'Q - Q'P)/Q^2$.

Mestre can show that P, Q can be chosen such that $P'Q - Q'P = R^4(X)\, S(X)$, with $R(X) = X^2 + r$, $r, s \in \mathbb{Q}$, Hence the index of ramification is 5 at the $S(X) = X^2 + s$ $r \neq s$ zeros of R, 2 at the zeros of S.
One checks that the Hurwitz genus formula holds: $2 \cdot 0 - 2 = 6(2 \cdot 0 - 2) + (4+4+1+1)$

Let L_n = the root field of the irreducible polynomial $P(X) - TQ(X) = 0$.
Let $K_2 = k(\sqrt{\operatorname{disc}_X P(X) - TQ(X)})$. The only possible ramification is of degree 2 and occurs at the zeros of S. Since the discriminant is a square in K_2, it is easy to see that both zeros ramify. By the Hurwitz formula, K_2 has genus 0. Assume $\operatorname{disc}_X Q(X)$ is a square. The curve given by K_2 is of the form $z^2 = \operatorname{disc}_X P(X) - TQ(X)$. If we take $T = \infty$, we have $z^2 = \operatorname{disc} Q(X)$ and a rational point exists since $\operatorname{disc}_X Q(X)$ is a square. Hence $K_2 = \mathbb{Q}(t)$.

Let $\beta_2 = W_2(\operatorname{Tr}(x^2))$ form on $L_n/\mathbb{Q}(t)$. β_2 comes from a class $\beta_2(T)$ on $\mathbb{Q}(T)$. By the theorem of Lecture 19, $\beta_2(T)$ has at most two poles, corresponding to the points of 2-ramification. Hence, β_2 has no poles on $\mathbb{Q}(t)$. Since $K_2 = \mathbb{Q}(t)$, from the residue theorem, $\beta_2(t)$ is constant (i.e. $\in H^2(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z})$) and we can evaluate it at a point. Mestre will show it is 0 for $T = \infty$

Since 3 is prime to the ramification degree, $\beta_2(t)$ is constant by the corollary of last lecture. We calculate it at $T = \infty$. The Galois group of fiber is contained in A_5. But $\alpha \in H^2(A_6, \mathbb{Z}/3\mathbb{Z})$ is zero when restricted to a subgroup $H \subset A_6$ unless $9 \mid [H:1]$. Hence $\beta_3(t) = 0$.

① Constructing P, Q, R, S:

We want to construct P, Q, R, S with degrees $6, 5, 2, 2$ respectively such that they are all monic polynomials and $P'Q - Q'P = R^4 S$. Let $Q(x)$ have the form $X(x^4 - ax^2 + b)$ for $a, b \in \mathbb{Q}$. We solve for P, R, S in the following forms:

$$P(x) = x^6 + p_2 x^4 + p_4 x^2 + p_6$$
$$R(x) = x^2 + r$$
$$S(x) = x^2 + s$$

Proposition: There exists (P, R, S) such that $P'Q - Q'P = R^4 S$ $\iff$ $9a^2 - 100b$ is a square in $\mathbb{Q}$.

Suppose $Q(x) = x(x^4 - ax^2 + b)$. $P'Q - Q'P = R^4 S$ has a solution $\iff$ the residue of $\left(\frac{P}{Q}\right)' = (P'Q - Q'P)/Q^2 = R^4 S / Q^2$ is always zero. (Then integration gives P)

Now if F, G are 2 polynomials, the residue of F/G^2 at a simple root a of G is given by $\dfrac{(F'G' - FG'')(a)}{G'(a)^3}$ (*).

If $R(x) = x^2 + r$, $S(x) = x^2 + s$, $F(x) = f(x^2)$, $f(x) = (x+r)^4(x+s)$, $G(x) = x\,g(x^2)$, and $g(x) = x^2 - ax + b$, one has

$$(F'G' - FG'')(x) = 2x\left[\left(2x^2 g'(x^2) + g(x^2)\right) f'(x^2) - f(x^2)\left(3g'(x^2) + 2x^2 g''(x)\right)\right]$$

and the residue of $R^4 S / Q^2$ at $X = 0$ is 0.

We now derive conditions for the residue to be c at the other roots of $Q(x)$. The residue is 0 at the other roots of $Q(x)$

$$\iff \left((4R'S + RS')Q' - RSQ''\right)(a) = 0 \quad \text{for } a \text{ with } Q(a) = 0$$

This is equivalent to $Q(x) \mid (4R'S + RS')Q' - RSQ''$

$$x^4 - ax^2 + b \mid (4R'S + RS')Q' - RSQ'' \implies \begin{aligned} 3a^2 + (s - 5r)a - 10(rs + b) &= 0 \\ (rs - b)a + 2b(r - s) &= 0 \end{aligned}$$

Hence $s = b(a - 2r)/(ar - 2b)$

and $5(a^2 - 4b)r^2 + 3a(4b - a^2)r + 5b(a^2 - 4b) = (a^2 - 4b)(5r^2 - 3ar + 5b) = 0$

Since Q has no multiple roots, $a^2-4b \neq 0$ and $5r^2-3ar+5b=0$.
To be able to choose r to be rational, one needs $9a^2-100b$ to be a square. Then for one of the two values of r (since we assume $a^2 \neq 100b/9$), $ar-2b$ is non-zero and s exists. Hence the proposition.

② The Discriminant and Trace Form.

To calculate the discriminant of $Q(x)$, we use the lemma:

Lemma: Let $f(x)$ be a polynomial, $g(x)=f(x^2)$. Then $\Delta(g) = 2^{2n}\Delta^2(f)\sigma_n$, where σ_n is the product of the roots of f, $\deg f = n$.

Proof: By definition, $\Delta(g) = (-1)^{2n(2n-1)/2} \prod_{\substack{x_j, \\ g(x_j)=0}} g'(x_j) = (-1)^n \prod_{\substack{x_j \\ g(x_j)=0}} 2x_j f'(x_j^2)$

$$= (-1)^n \prod_{\substack{x_i \\ f(x_i)=0}} -2^2 x_i f'(x_i)^2 = 2^{2n}\sigma_n \cdot \Delta^2(f).$$

The discriminant of x^2-ax+b is a^2-4b and by the lemma, $\Delta(x^4-ax^2+b) = 2^4(a^2-4b)^2 b$. Now $\Delta(x(x^4-ax^2+b)) = 2^4(a^2-4b)^2 b^3$.
Hence $\operatorname{disc}(Q(x))$ is a square $\iff$ b is a square.

To calculate W_2 (trace form), we use the method mentioned in Lecture 8.
If q is a quadratic form with matrix M, and d_i are the principal minors of order i of M, $W_2(q) = \sum_{i=1}^{n-1} (d_i, -d_{i+1})$

Let $q = \operatorname{Tr}_{A/\mathbb{Q}}(x^2)$, $A = \mathbb{Q}(x)/(Q)$, $Q = x(x^4-ax^2+b)$.

One has $M = \begin{pmatrix} 4 & 0 & 2a & 0 \\ 0 & 2a & 0 & * \\ 2a & 0 & 2a^2-4b & * \\ 0 & * & * & * \end{pmatrix}$ relative to the factor x^4-ax^2+b

since $\operatorname{Tr}(x^2) = \operatorname{Tr}(x)^2 - 2(-a) = 2a$
and $\operatorname{Tr}(x^4) - a\operatorname{Tr}(x^2) + 4b = 0$

and $d_1 \equiv 1 \pmod{\text{squares}}$
$d_2 \equiv 2a$ " "
$d_3 = 8a(2a^2-4b) - 8a^3 = 8a^3 - 32ab = 2a^3 - 8ab$
$d_4 = 1$

Then $W_2(q) = \underset{\overset{\shortparallel}{0}}{(1,-2a)} + (2a, -2a(a^2-4b)) + (2a(a^2-4b), -1)$

$= (2a, -(a^2-4b)) + (a^2-4b, -1)$

Since $9a^2 - 100b$ is a square, $9(a^2-4b) = (\text{a square}) + 64b$

$= \text{a sum of two squares}$ since b is a $\square$.

Hence $(a^2-4b, -1) = 0$. If we choose $a = 2$, then $W_2(q) = 0$

Let $w = \dfrac{6u}{5(1+u^2)}$. Then $9.2^2 - 100w^2 = \dfrac{900 + 1800u^2 + 900u^4 - 3600u^2}{5^2(1+u^2)^2}$

$= \dfrac{36(1-u^2)^2}{(1+u^2)^2} = \left(\dfrac{6(1-u^2)}{1+u^2}\right)^2$

Then $Q(X) = X(X^4 - 2X^2 + (6u/5(1+u^2))^2$ gives an infinite family of extensions $(u \neq 0, 1)$.

12/4/90

Lecture 21

Let k be a perfect field, X/k a smooth projective absolutely irreducible curve. Let $K = k(X)$, $\bar{k}$ = the algebraic closure of k. Let $L = \bar{k}\cdot K$, $G_K = Gal(\bar{K}/K)$, $G_k = Gal(\bar{k}/k) = \Gamma$, $1 \to N \to G_K \to \Gamma \to 1$.
Let C be a Γ-module, finite with order prime to the characteristic.

Assume that X has a rational point. Then we have the exact sequence

$$0 \to H^i(G_k, C) \to H^i(G_K, C) \xrightarrow{r} H^{i-1}(\Gamma, H^1(N, C)) \to 0$$

If $\underline{X}$ denotes the closed points of X, for $v \in \underline{X}$, $\alpha \in H^i(G_K, C)$, we can define $r_v(\alpha) \in H^{i-1}(k(v), C(-1))$.

Theorem: Let $\alpha \in H^i(G_K, C)$. 1. α has finitely many poles

2. (Residue formula) $\sum_{v \in \underline{X}} \mathrm{Cor}_{k}^{k(v)} r_v(\alpha) = 0$ in $H^{i-1}(k, C(-1))$

3. If $\alpha \in H^i(G_k, C)$ then α has no pole. If $\alpha \in H^i(K, C)$ has no pole and the genus of X is 0 then $\alpha \in H^i(k, C)$

The idea of the proof is to show that r is essentially the collection of r_v when the genus is 0.

Note: $H^1(N, C) = \mathrm{Hom}(N, C) = \mathrm{Hom}(N^{ab}, C)$, where N^{ab} is the Galois group of the maximal abelian extension of $\bar{k}K$ (= function field of $X/\bar{k}$)
If S denotes any finite set of closed points on $X/\bar{k}$, one has

$$N^{ab} = \varprojlim_S \pi_1^{ab}(X_{/\bar{k}} - S)$$

To prove the theorem, one needs to describe $H^1(N, \mu_n)$

Step 1: Let D be the group of divisors on $X/\bar{k}$
Let D^0 be the subgroup of degree 0 divisors.
Let J be the Jacobian.
One has the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & L^*/\bar{k}^* & \to & D^0 & \to & J & \to & 0 \\ & & \downarrow n^{th}\text{ power} & & \downarrow \times n & & \downarrow \times n & & \\ 0 & \to & L^*/\bar{k}^* & \to & D^0 & \to & J & \to & 0 \end{array}$$

Since multiplication by n is injective on D^0 and J is divisible, the snake lemma gives:

$$0 \to J_n \to \underset{\substack{\| \\ H^1(N, \mu_n)}}{L^*/(L^*)^n} \to D^0/nD^0 \to 0$$

Step 2: Assume $nC = 0$. Then $C = \mu_n \otimes C(-1)$. By the following general fact, $H^1(N, C) = H^1(N, \mu_n \otimes C(-1)) = H^1(N, \mu_n) \otimes C(-1)$.

Fact: If T is an exact functor on the category of finite $\mathbb{Z}/n\mathbb{Z}$-modules, then $T(\mathbb{Z}/n\mathbb{Z})$ is projective. Hence $T(C) \approx C \otimes T(\mathbb{Z}/n\mathbb{Z})$

Note: Since $\mathrm{cd}\, N \leq 1$, $H^i(N, -)$ is an exact functor. (N acts trivially on C)

Step 3: Tensoring by $C(-1)$, one has $0 \to J_n \otimes C(-1) \to H^1(N, C) \longrightarrow D^0/nD^0 \otimes C(-1) \longrightarrow 0$
Since D^0/nD^0 is free, the original sequence splits and the tensoring by $C(-1)$ is exact.

Step 4: The exact sequence $0 \to D^0 \to D \to \mathbb{Z} \to 0$ induces $0 \to D^0/nD_0 \to D/nD \to \mathbb{Z}/n\mathbb{Z} \to$
Using a rational point of X, this sequence splits. Tensoring, we have the split exact sequence

$$0 \longrightarrow D^0/nD^0 \otimes C(-1) \longrightarrow D/nD \otimes C(-1) \longrightarrow C(-1) \longrightarrow 0 .$$

Suppose we have $v \in \underline{X}$, with degree d_v. Then over $\bar{k}$, v splits in d_v conjugate points $w_1, \dots, w_{d_v}$. The action of Γ on the w_i is transitive. Taking a linear combination of the w_i, one can form an induced Γ-module, denoted $\mathrm{Ind}_{\Gamma}^{\Gamma(v)} \mathbb{Z}/n\mathbb{Z}$. Hence one can write $D/nD = \bigoplus_{v \in \underline{X}} \mathrm{Ind}_{\Gamma}^{\Gamma(v)} \mathbb{Z}/n\mathbb{Z}$,
and $D/nD \otimes C(-1) = \bigoplus_{v \in \underline{X}} \mathrm{Ind}_{\Gamma}^{\Gamma(v)} C(-1)$

$$D_0/nD_0 = \ker \{ D/nD \otimes C(-1) \longrightarrow C(-1) \}$$

Step 5: By Shapiro's lemma, $H^{i-1}(\Gamma, D/nD \otimes C(-1)) = \bigoplus_{v \in \underline{X}} H^{i-1}(\Gamma(v), C(-1))$

Step 6: One has the sequence of maps:

$$H^i(G_k, C) \xrightarrow{r} H^{i-1}(\Gamma, H^1(N, C)) \longrightarrow H^{i-1}(\Gamma, D/nD \otimes C(-1)) \downarrow$$
$$\cdots\cdots\cdots \xrightarrow{r'} \bigoplus_v H^{i-1}(\Gamma_v, C(-i))$$

Claim: r' is given by $\bigoplus_v r_v$

Step 7: Since the exact sequence in Step 4 is split, we have that

$$H^{i-1}(\Gamma,\ D^0/nD^0 \otimes C(-1)) = \ker\left\{ \bigoplus_{v\in \underline{X}} H^{i-1}(\Gamma_v,\ C(-1)) \xrightarrow{\text{Cor}} H^{i-1}(\Gamma, C(-1)) \right\}$$

(Cor: $\uparrow$ onto)

Proof of the theorem: (1) By Step 6, it is clear that there are only finitely many poles.

(2) Now $H^i(G_k, C) \xrightarrow{r} H^{i-1}(\Gamma, H^1(N,C)) \to H^{i-1}(\Gamma, D^0/nD^0 \otimes C(-1))$, Hence by Step 7, the residue formula holds.

(3) Since $H^i(G_{k(t)}, C) \to H^i(G_k, C) \xrightarrow{r} H^{i-1}(\Gamma, H^1(N,C))$ gives the zero map, if α is constant, it has no poles. Conversely if X has genus 0, $J_n = 0$ and $H^1(N,C) \simeq D^0/nD^0 \otimes C(-1)$. Hence if α has no poles, we must have $r(\alpha) = 0$ and α is constant.

Now suppose X has genus ≥ 1, α an element of $H^i(G_K, C)$ without poles. Let $v \in \underline{X}$, $\alpha(v) \in H^i(k_v, C)$.

Theorem: "Abel" Let $\Delta = \sum n_v v \sim 0$. Then $\sum_v n_v \text{Cor}_k^{k_v} \alpha_v = 0$

Proof: Let $\Delta = (f)$, f a nonconstant function. We view f as defining a map $f: X \to \mathbb{P}^1$ with the extension of function fields $K/k(t)$. Let $\beta = \text{Cor}_{k(t)}^{k}(\alpha) \in H^i(k(t), C)$. Since α has no poles, neither does β. Since $k(t)$ has genus 0, β must be a constant and $\beta(0) - \beta(\infty) = 0$. Now consider $\beta(0)$. Since $\text{Cor}_L^{L'} \alpha = \bigoplus \epsilon_w \text{Cor}_L^{L'_w} \alpha_w$, when L is a local field, complete with valuation v, and $L' = \bigotimes_{w|v} L'_w$, w valuations lying above v, e_w the ramification index.

Then $\beta(0) - \beta(\infty) = 0 = \sum_v n_v \text{Cor}_{k(t)}^{k_v} \alpha_v$. Hence the theorem.

The theorem is useful in constructing a map $\varphi_\alpha : J_X(k) \to H^i(k, C)$ such that $\alpha(x) - \alpha(x_0) = \varphi_\alpha(x - x_0)$ where X is a curve, $x_0 \in X(k)$ is a basepoint, α has no pole and $J_X(k)$ is the Jacobian of X. If we construct φ_α, then after embedding $X \hookrightarrow J_X$ by $x \mapsto \text{Cl}(x - x_0)$, we have $\alpha(x) = \varphi_\alpha(x)$ for $x \in X \hookrightarrow J_X$.

To define φ_α on $J_X = (\text{divisors of degree } 0)/\text{principal divisors}$, one needs $\varphi_\alpha(\Delta) = 0$ if $\Delta = (f)$. Hence by the theorem it is clear that we define $\varphi_\alpha(\Delta = \sum n_v v) = \sum_v n_v \text{Cor}_k^{k_v} \alpha_v$. Then $\varphi_\alpha(x - x_0) = \alpha(x) - \alpha(x_0)$ as wanted.

The elements of $H^i(G_K, C)$ with no poles modulo the constants $\approx Ext^i(J_X, C)$. For $i=1$, this is Rosenlicht's theory of abelian extensions and isogenies. When the poles are contained in S, we use the generalized Jacobian.

Special Case: Let $\alpha \in H^i(k(T), C)$. Assume α has no pole on the affine line $Aff^1 = \mathbb{P}_1 - \{\infty\}$. Then α is constant (i.e. an element of $H^i(k, C)$)

Theorem: (Let k have characteristic 0). If $\alpha \in H^i(k(T_1, \dots, T_n), C)$ has no pole on Aff^n, then α is constant.

Note: Let X/k be a smooth algebraic variety, $K = k(X)$. Let v_Δ be the discrete valuation of K given by an irreducible divisor Δ. We say α has no pole at $\Delta \iff$ the residue at v_Δ of α is 0.

One says α has no pole on $X \iff$ no irreducible divisor $\Delta \subset X$ is a pole.

Proof: We induct on n. We've just seen that this holds for $n=1$.
Assume $n=2$, and we have the tower of function fields $k(T_1, T_2)$ / $k(T_1)$

We need to show that α has no pole on the affine line $Aff^1_{k(T_1)}$
The possible poles correspond to irreducible divisors which aren't vertical divisors.
By assumption, the residues are 0.

Special Case: $C = \mu_n$, $i=2$. $H^2(K, \mu_n) = Br_n K$. We have a Grothendieck style interpretation. Let X be a smooth variety $/k$, $K = k(X)$.
When $Pic\, X = 0$, the subgroup of elements without poles $= Br_n(X) \hookrightarrow H^2_{et}(X, \mu_n)$
One has $Br(\text{Affine space}) = Br(k)$ (i.e. $Br(k[T]) = Br(k)$).
There is an étale cohomology interpretation of our results.

Lecture 22

12/6/90

Given $\alpha \in H^i(G_K, C)$, we saw last time that $\sum_v \mathrm{Cor}\, \mathrm{res}_v(\alpha) = 0$ in $H^{i+1}(\Gamma, C(-1))$. Conversely, given $\beta_v \in H^{i-1}(\Gamma(v), C(-1))$ for all v such that

a) All but a finite number of the β_v are 0

b) $\sum \mathrm{Cor}\, \beta_v = 0$,

there exists $\alpha \in H^i(G_K, C)$ with $\mathrm{res}_v(\alpha) = \beta_v$. This was implicitly proved last time for any curve X with a rational point.

Example: Let $i=2$, $C = \mathbb{Z}/2\mathbb{Z}$. $H^2(K, C) = \mathrm{Br}_2 K$, $C(-1) = \mathbb{Z}/2\mathbb{Z}$, and $H^1(k(v), \mathbb{Z}/2\mathbb{Z}) = k(v)^*/(k(v)^*)^2$.

For $\alpha \in \mathrm{Br}_2 K$ and a pde v, one attaches $r_v(\alpha) \in k(v)^*/(k(v)^*)^2$. The residue formula implies that $\prod_v N_{k(v)/k}\, r_\alpha(v) = 1$ modulo squares. We note that one can prove this formula in an elementary manner by using Mercuriev's theorem and the formulas for r.

Exercise: Without using Mercuriev's theorem, prove that every element of $\mathrm{Br}_2 k(t)$ is the sum of an element of $\mathrm{Br}_2 k$ and symbols (f,g).
Hint: One can use symbols to construct elements with given poles and residues. Let $\alpha = ((t-\lambda_1)(t-\lambda_2), \beta)$ for $\lambda_1, \lambda_2 \in \mathbb{P}_1(k)$ and $\beta \in k^*/(k^*)^2$. α has residue β at λ_1, λ_2 and is 0 at ∞. Little is known about the minimal number of symbols needed.

One can use residues to check formulas. Consider the expression $(x,y) + (x+y, -xy)$. On Aff^2, the only poles can occur at $x=0$, $y=0$ or $x+y=0$. For $x=0$, the residue $= y(x+y) = y^2 =$ a square $= 1$. At $y=0$, the residue is also 0. At $x+y=0$, $x=-y$ so $-xy = y^2 \equiv 1$. Hence the expression has no poles and it must be a constant. We check it for $x=1, y=1$: $(2,-1) = 0$ so $(x+y) + (x+y, -xy) = 0$.

Exercise: If $x+y+z=0$, does $(x,y)+(y,z)+(z,x) = 0$? (No!) $[(x,y)+(y,z)+(z,x) = (-1, -xyz)]$

Check this by showing $xX^2 + yY^2 + zZ^2 \approx X^2 - Y^2 - xyzZ^2$

Killing Elements of $Br_2\, k(t)$.

Let $X' \xrightarrow{\pi} X$ be a finite morphism /k. Let k', K be the respective function fields. Let C be a Γ-module. One has $G_{k'} \hookrightarrow G_k$ and the restriction map $H^i(k, C) \longrightarrow H^i(k', C)$.

Assume X, X' are projective lines. Let $\alpha \in H^i(K, C) \longmapsto \alpha' \in H^i(k', C)$. We want to give conditions for $\alpha' = 0$. If v is a pole of X, let v' be a pole of X' lifting v. One has $r_v(\alpha) \in H^{i-1}(k(v), C(-1))$ and one defines $\lambda_{v'}(\alpha') = e_{v'/v} \cdot \mathrm{Res}_{k(v)}^{k(v')} r_v(\alpha)$

($e_{v'/v}$ ← ramification index.)

Suppose $i=2$, $C = \mathbb{Z}/2\mathbb{Z}$. If v is a pole of α, $r_v(\alpha) \in k(v)^*/(k(v)^*)^2$ gives a quadratic extension $l_v(\alpha)/k_v$.

$(*)_{v'/v}$: Statement: $r_{v'}(\alpha') = 0 \iff$ Either $e_{v'/v}$ is even or $k(v')$ contains $l_v(\alpha)$

Theorem: Assume ① $\alpha_v = 0$ at a rational point of X which can be lifted to a rational point of X'
② $(*)_{v'/v}$ is true for every v' above a pole v of α.
Then $\alpha' = 0$.

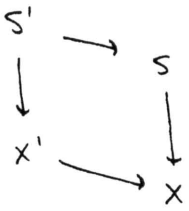
Proof: ② implies α' is constant. ① shows α' must $= 0$.

We can generalize the theorem to get:

Conjecture: Given any $\alpha \in Br_2(K)$, $K = k(T)$, k has characteristic 0, and a rational point x of $\mathbb{P}_1$ with $\alpha(x) = 0$, there is a covering $\pi: X' \to X$ with
(1) X' the projective line
(2) $\exists\, x' \in X'(k)$, $\pi x' = x$
(3) $\alpha' = \pi^* \alpha = 0$

There are at least two reasons to be interested in the above conjecture. The conjecture is related to constructing Galois groups of $\mathbb{Q}(T)$, and the unirationality of some conic bundles over $\mathbb{P}_1$.

Example: Let $P(t) = \prod (t - \lambda_i)$, $\lambda_i \in k$ distinct, be a polynomial of even degree. Let $\mu \in k^*$ not be a square and consider the surface $W: X^2 - \mu Y^2 - P(T) = 0$. If we fix t, we get a conic over $k(t)$. Let $\alpha = (\mu, P(T)) \in Br_2(K)$. α can be characterized by $\alpha(\infty) = 0$ (since $(\mu, T^{2m+\dots}) = (\mu, 1 + \frac{\alpha'}{T} + \dots) = (\mu, 1) = 0$ at $T = \infty$) and the poles of α are the λ_i with residue μ. Hence the fibers are nice except over λ_i



Suppose we have the conjecture. with X a curve of genus 0 with points satisfying

Suppose S' has trivial invariant, then S' is birational to $\mathbb{P}_1 \times \mathbb{P}_1$. Hence S is unirational (which means the image of a birational variety), and S has infinitely many fibers with rational points.
Conversely, if S is unirational, the conjecture above is true.

Question: Assume S is a surface / k that has a smooth rational point. If S is rational over $\bar{k}$, is it k-unirational?

~

We'll see next time that the conjecture implies that every 2-group is a Galois-group of a regular extension of $\mathbb{Q}(T)$.

Theorem (Mestre) The conjecture is true when $\sum_{v \text{ pde } d} \alpha \deg v \leq 4$

More precisely, we'll show that π may be chosen with $\deg \pi = 8$.

Proof: Choose coordinates so that $x = \infty$. We will choose $\pi: \mathbb{P}_1 \to \mathbb{P}_1$ with $\pi(\infty) = \infty$. Let $P(T) = T^4 + p_1 T^3 + \dots + p_4$ be a rational separable polynomial vanishing on the poles of α.
Let $\Lambda_P = k(T)/(P(T)) = \prod_{v \text{ irred divisor of } P} k(v)$. Then $r(\alpha)$ is an element of $\Lambda_P^* / (\Lambda_P^*)^2$.

Hence $r(\alpha)$ can be represented by $R(T)$, degree $R \leq 3$. We may assume $\deg R = 3$. By the residue theorem, $N_{\Lambda_P}(R)$ is a square.

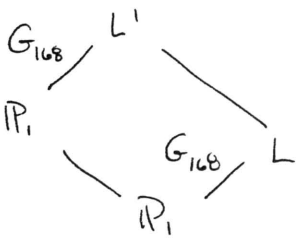
Let v be an indeterminate, $K(v)$ a curve of genus 1, $y^2 = P(T) + v^2 R(T)$, Y, T coordinates, $R = r_0 T^3 + r_1 T^2 + \dots + r_3$, $y^2 = T^4 + (p_1 + r_0 v^2) T^3 + \dots$
Above ∞, there are two points, $y = T^2 + \dots$, $Y = -T^2 + \dots$, so ∞ splits into two rational points. We will construct a rational point of this curve (but not above ∞). Let $t(v) \in K(v)$, $y(v) \in K(v)$, $y^2(v) = P(t(v)) + v^2 R(t(v))$

Euler knew that we could write $y^2 = t^4 + \alpha_1 t^3 + \dots + \alpha_4 = (t^2 + \beta_1 t + \beta_2)^2 + \beta_3 t + \beta_4$ with $\beta_1 = \alpha_1/2$, $\beta_2 = (\alpha_2 - \beta_1^2)/2$. Assume $\beta_3 \neq 0$. Then set $t = -\beta_4/\beta_3$. We have $y(v) = t^2(v) + \beta_1(v) t(v) + \beta_2(v)$. In general, one finds that $\beta_3(v)$ is a polynomial of degree 3 in v^2 and $\beta_4(v)$ is a polynomial in v^2 of degree 4.

By choosing k conveniently, one can arrange that $\beta_4(u)$, $\beta_3(u)$ are relatively prime. Then the map $\pi(u) = t(u) = -\beta_4(u) / \beta_3(u)$ has degree 8 and $\pi(\infty) = \infty$.

Let v' be a lift of v to k'. We need to show that r_v is a square in $k_v(v')$. We have $P = 0$ at v. Hence $y^2 = v^2 R(t)$ and $R(t_i)$ is a square. Hence $\# x = 0$ and the conjecture is proved.

Mestre was interested in $SL_2(\mathbb{F}_7) = \tilde{G}_{168}$ and wanted to show it occurs over $\mathbb{Q}(T)$ as a Galois group. La Macchia had constructed a two parameter family of seventh degree polynomials $f_{a,b}$ with Galois group G_{168}. Let $a = -1/4$, $b = T$, there is ramification of order 3 for ∞ and order 2 for four values of $b = T$. Then Σ deg poles $= 4$. We construct a $\mathbb{P}_1$ where the obstruction is 0. There are many choices for $\mathbb{P}_1$ and we can choose $\mathbb{P}_1$ disjoint from the extension L/K with $\mathrm{Gal}(L/K) = G_{168}$. Hence we have



and the obstruction is zero for $L/\mathbb{P}_1$.

Lecture 23

Let K be a field with char. $K = 0$ and assume that the conjecture of Lecture 22 is true for K. The conjecture has been proven for K a local field, complete (Henselian is enough) with a discrete valuation v. It is an open question whether it is true for $\mathbb{Q}$.

Theorem 1: *If K has the killing property and G is a finite 2-group, there is a Galois extension of $K(T)$, regular, with Galois group G and a completely split rational point.*

Theorem 2: *Assume K has the killing property and that $1 \to C_2 \to \tilde{G} \to G \to 1$ is an exact sequence. Assume we have a regular Galois extension of $K(T)$ with Galois group G and a completely split rational point. Then the same is true for $\tilde{G}$.*

By induction on $|G|$, one sees that Theorem 2 implies Theorem 1.

Proof of Thm 2: First, assume $\tilde{G} = G \times C_2$. Then we are done if we construct a quadratic extension L of $K(T)$ with a completely split rational point lying above our base point and L is disjoint from the G-extension. We can assume that the base point is 0 and then $L = K\left(T, \sqrt{(1-T/a)/(1-T/b)}\right)$ for a suitable choice of $a, b \in K^*$, $a \neq b$, is the desired extension.

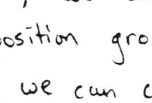
Now assume that the extension is not split. (Assume that the base point is 0.) We apply the following lemma.

Lemma: *If $L/K(T)$ is a regular Galois extension with group G and a base point, then there exists another such extension L' with the property that for every E, $L' \supsetneq E \supsetneq K(T)$, E has genus ≥ 1.*

Proof: The lemma follows from Hurwitz's theorem after a quadratic extension F of $K(T)$ with genus $F = 0$, F disjoint from L such that F makes the ramification of the G-extension worse.

By the lemma, we assume that $L/K(T)$ is a G-extension with a completely split rational point with no intermediate fields of genus 0. We then have an obstruction $\alpha \in H^2(G, C_2)$ corresponding to $1 \to C_2 \to \tilde{G} \to G \to 1$. By a suitable quadratic extension ($k' = K\left(T, \sqrt{(1-T/a)/(1-T/b)}\right)$ for suitable $a, b \in K^*$) we can kill α and k' has genus 0. Hence, $k'L/k'$ has Galois group G, and since $\alpha = 0$, we can lift the map $G_{k'} = G_{K(T)} \dashrightarrow \tilde{G}$.

If the decomposition group of the base point is not trivial, we can change the map by a quadratic twist,



to make it trivial.

Specialization of Elements of $Br_2\,\mathbb{Q}(T_1,\dots,T_n)$

Let $\alpha \in B_2 k = Br_2\,\mathbb{Q}(T_1,\dots,T_n)$. Choose an expression $\Sigma(f_i, g_i)$ for α with $f_i, g_i \in k^*$. If f_i, g_i are defined and are non-zero at $x \in Aff^n(\mathbb{Q})$, one has $\alpha(x) = \Sigma(f_i(x), g_i(x)) \in Br_2(\mathbb{Q})$. We are interested in how often $\alpha(x)$ is 0. ← independent of the expression for α

First Setting: Let x be an element of $Aff^n(\mathbb{Z}) = \mathbb{Z}^n$ such that $|x_i| \le X$ for all i, X a real number. Define $N(X) = N_\alpha(X)$ as the number of x's with $|x_i| \le X$ for all i such that $\alpha(x) = 0$. We can estimate the growth of $N(X)$ as $X \to \infty$.

Theorem 1: $N_\alpha(X) \ll \dfrac{X^n}{(\log X)^{d(\alpha)/2}}$ as $X \to \infty$,

where $d(\alpha)$ is the number of $\mathbb{Q}$-irreducible polar varieties of α on Aff^n.

A polar variety of α is a $\mathbb{Q}$-irreducible subvariety W of Aff^n of dimension $n-1$ which is a pole of α.

Second Setting: Take $x \in \mathbb{P}_n(\mathbb{Q})$. One says $Ht(x) \le X \iff$ x can be written $(x_0,\dots,x_n)$ with $x_i \in \mathbb{Z}$ for all i, not all $x_i = 0$ with $|x_i| \le X$ for all i. Let $N_{proj}(X)$ = number of x with $Ht(x) \le X$, $\alpha(x) = 0$. We have:

Theorem 2: $N_{proj}(X) \ll \dfrac{X^{n+1}}{(\log X)^{d_{proj}(\alpha)/2}}$

where $d_{proj}(\alpha)$ is the number of $\mathbb{Q}$-irreducible polar varieties of α in $\mathbb{P}_n$.

Theorem 2 is easily deduced from Theorem 1 applied to Aff^{n+1} and the image of α in $Br_2\,\mathbb{Q}(T_0,\dots,T_n)$.

We will prove Theorem 1 in the next lecture. Now we will see some of the consequences of the theorem.

Examples: (1) Let $n=1$, $\alpha = (-1, T)$. Then $N(X)$ is the number of integers t such that $|t| \le X$, $(-1, t) = 0$. Hence t is a sum of two squares. Theorem 1 implies that $N(X) \le C \cdot X/(\log X)^{1/2}$. It is a theorem of Landau that $N_\alpha(X) \sim cX/(\log X)^{1/2}$. More precisely, for any natural number n, we have

$$N_\alpha(X) = \frac{X}{\sqrt{\log X}} \left(c_0 + \frac{c_1}{\log X} + \cdots + \frac{c_n}{(\log X)^n} \right) + O\left(\frac{X}{(\log X)^{n+3/2}} \right)$$

where $c_0, c_1, \cdots, c_n$ are computable numbers.

Let $a_n = 1$ if n is a sum of two squares, $a_n = 0$ otherwise. Then $N(X) = \sum_{n \le X} a_n$. If we let $f(s) = \sum a_n n^{-s}$,

we have $f(s) = \prod_{\substack{p=2 \\ \text{or } p \equiv 1 (4)}} \frac{1}{1-p^{-s}} \prod_{p \equiv 3 (4)} \frac{1}{1-p^{-2s}}$

and one finds that $f(s) \approx \zeta(s)^{1/2} L(s, \chi)^{1/2}$ where χ is the character attached to $\mathbb{Q}(i)$. Then $f(s)$ has "a pole of order $1/2$" at $s=1$. If we study the behavior of $f(s)$ well enough, we can estimate $N_\alpha(X)$, but this method doesn't give the correct values for c_i.

(2) Let $n=2$, $\alpha = (T_1, T_2)$. $N(X)$ equals the number of pairs $(t_1, t_2) \in \mathbb{Z} \times \mathbb{Z}$ such that $|t_1| \le X$, $|t_2| \le X$, $(t_1, t_2) = 0$. (In other words, the conic $x^2 - t_1 y^2 - t_2 z^2 = 0$ has a rational point). Theorem 1 says that $N(X) \ll X^2/\log X$ It is not known whether the bound is sharp. There is a lower bound for $N(X)$ however.

Theorem: $N(X) \gg X^2/(\log X)^2$

Proof: Choose t_1, t_2 to be primes congruent to 1 modulo 4. Then $(t_1, t_2) = 0 \iff \left(\frac{t_1}{t_2}\right) = 1 = \left(\frac{t_2}{t_1}\right)$. If we can assume that half of all such pairs have this property, then we have at least $\left(\frac{1}{2} \frac{X}{\log X}\right)^2 \cdot \frac{1}{2} = X^2/8(\log X)^2$, pairs. The assumption is valid since Heilbronn has shown that

$$\left| \sum_{t_1, t_2 \le X} \left(\frac{t_1}{t_2}\right) \right| \ll X^{2 - \frac{1}{4}}$$

(3): Let $n=3$, α the invariant of the conic $T_1x^2+T_2y^2+T_3z^2=0$. One has $\alpha=(-T_1T_2, -T_1T_3)$ and theorem 1 implies $N(X)\ll X^3/(\log X)^3$. One can prove that $N(X)\gg X^3/(\log X)^3$.

(4) Let $n=6$, α the invariant of the conic:

$$T_1x^2+T_2y^2+T_3z^2+T_4yz+T_5zx+T_6xy=0.$$

(Exercise: Calculate α !)

There is one pole. It is given by the equation, discriminant(conic) $=0$, which is irreducible over $\mathbb{C}$ and $\mathbb{Q}$. Theorem 1 implies $N(X)\ll X^6/\sqrt{\log X}$

(5) Let $n=2$, $\alpha=(-T_1T_2, T_1^3T_2+T_1T_2^3+T_2^4)$. Let $t=T_2/T_1$. Then $\alpha=(-t, t+t^3+t^4)$. Since $(t,-t)=0$, $\alpha=(-t, 1+t^2+t^3)$. Hence the possible poles occur at $t=0$, $t=\infty$ and a root of $1+t^2+t^3$. At $t=0$, the residue is 0 so there is no pole. At $t=\infty$, by the same reason, there isn't a pole. Hence there is one pole and we have $N_\alpha(X)\ll X^2/(\log X)^{1/2}$.

Problem: Is the estimate in theorem 2 for the exponent of $\log X$ optimal (assuming that $\alpha(x)=0$ for at least 1 value of $x\in\mathbb{P}_n(\mathbb{Q})$)

Special Case: On $\mathbb{P}_1$, if α vanishes at 1 point, does it vanish at infinitely many?

Lecture 24

12/6/90

Given $\alpha \in Br_2 \mathbb{Q}(T_1, \dots, T_n)$, suppose $\alpha = (f_i, g_i)$ for $f_i, g_i \in K^*$, with $K = \mathbb{Q}(T_1, \dots, T_n)$. If we have $x = (x_1, \dots, x_n) \in Aff^n(\mathbb{Q})$ and $f_i, g_i \in \mathcal{O}_x^*$, we can define $\alpha(x) = \sum (f_i(x), g_i(x)) \in Br_2 \mathbb{Q}$. Last time, we claimed that this is independent of our decomposition of α. In other words,

Lemma: Let K be the field of fractions of a regular local ring R with residue field k of characteristic $\neq 2$. Let f_i, g_i, f_i', g_i' be elements of R^*. If $\alpha = \sum (f_i, g_i) = \sum (f_i', g_i')$ in $Br_2 K$, then $\sum (\tilde{f}_i, \tilde{g}_i) = \sum (\tilde{f}_i', \tilde{g}_i')$ in $Br_2 k$ where if $a \in R^*$, $\tilde{a} \in k^*$ is its reduction.

First Proof: In "Le groupe de Brauer I, II, III" in "Dix exposés sur la cohomologique die schemas," Grothendieck proves:

$$Br\, R \longrightarrow Br\, K \quad \text{is injective since } R \text{ is regular.}$$

Then the reduction to $Br\, k$ is well-defined.

Note: If R is not regular, the map $Br\, K \longrightarrow Br\, K$ may not be injective. For example, let R, R' be rings such that $R \supset R'$, both have the same field of fractions K and they have residue fields ℓ, k where ℓ / k is a quadratic extension. One can choose R such that $\ell \subset K$. One can choose u, v in R' such that $(\tilde{u}, \tilde{v}) \neq 0$ in $Br_2 k$ but $(\tilde{u}, \tilde{v}) = 0$ in $Br_2 \ell$. Hence $(u, v) = 0$ in $Br_2 K$ and $Br_2 R' \longrightarrow Br_2 K$ is not injective.

Exercise: Give a direct proof of the lemma by inducting on the dimension. In dimension 1, complete R and use the exact sequence

$$0 \longrightarrow Br_2 k \longrightarrow Br_2 K \xrightarrow{r} k^*/(k^*)^2 \longrightarrow 0$$

For an arbitrary dimension, choose a uniformizing element $t \in R$. One shows that $\sum (f_i, g_i) = \sum (f_i', g_i')$ in $Br_2 k'$ with $k' = \text{Fract}\,(R/tR)$. Then by induction we are done.

Let U_α be the set of $x \in \mathrm{Aff}^n(\mathbb{Q})$ such that α can be written $\sum (f_i, g_i)$ with $f_i, g_i \in \mathcal{O}_x^*$. By the lemma, the value of $\alpha(x)$ is well-defined on U_α.

Let $V_\alpha = \mathrm{Aff}^n - \bigcup_{\substack{W_i \text{ polar} \\ \text{divisor of } \alpha}} W_i$. Then $V_\alpha \supset U_\alpha$.

In the "Purity Theorem", (theorem 6.1 of Brauer III), Grothendieck shows that if $x \in V_\alpha$, there exists a unique element $\alpha_x \in Br_2\, \mathcal{O}_x$ which gives α in $Br_2\, K$. The image of α in $Br_2\, k$ is defined as $\alpha(x)$.

Question: Does $U_\alpha = V_\alpha$? In other words, if $x \notin \bigcup_{\substack{W_i \\ \text{polar}}} W_i$, does there a decomposition of α as $\sum (f_i, g_i)$, $f_i, g_i \in \mathcal{O}_x^*$?

Answer: Yes. Lichtenbaum (Invent. Math. 87 (1988)) proves that for R a regular local ring of equal characteristic and the localization of a finitely-generated algebra over a field, $K_2 R \to Br_2 R$ is onto. Since $K_2 R$ is gen. by symbols, $U_\alpha = V_\alpha$.

Returning to the question of estimating integral points on a variety, we have the following **elementary lemma**:

Lemma: If V is any subvariety of $\mathrm{Aff}^n_{/\mathbb{Q}}$ of dimension d, the number of integral points of size $\leq X$ is $O(X^d)$ when $X \to \infty$.

of V

The proof of theorem 1 from last lecture is rather simple. We start with $\alpha \in Br_2 K$, $K = \mathbb{Q}(T_1, \ldots, T_n)$, W_i the polar varieties ($\mathbb{Q}$-irreducible) of α and $d(\alpha)$ the number of W_i. The idea of the proof is to use the sieve method.

For every prime p, we will define a subset $A(p)$ of $\left(\mathbb{Z}^n / p^2 \mathbb{Z}^n\right)$ such that if the reduction modulo p^2 of $x \in \mathbb{Z}^n$ lies in $A(p)$, then $\alpha(x) \neq 0$ in $Br_2 \mathbb{Q}_p$ (hence in $Br_2 \mathbb{Q}$).

To be more precise, for every i, choose P_i a polynomial in $\mathbb{Z}[T_1, \ldots, T_n]$ which gives the equation for W_i. We choose P_i to be irreducible in $\mathbb{Q}[T_1, \ldots, T_n]$. Then we have by Mercurier's theorem and the identity $(p_i, P_i) = (-1, P_i)$,

Lemma: One can choose polynomials U_i, V_j, W_j with coefficients in $\mathbb{Z}$, not divisible by P_i such that $\alpha = (P_i, U_i) + \sum_j (V_j, W_j)$

Let K_i be the field of fractions of $\mathbb{Q}[T_1, \dots, T_n] / P_i$ (i.e. the function field of W_i).

Let $p \neq 2$ (for $p=2$ we take $A(2) = \phi$). $Br_2(\mathbb{Q}_p)$ consists of two elements. Given (a,b), if $v_p(a) = 1$, $v_p(b) = 0$, then (a,b) is non-zero. If $v_p(a) = 1 = v_p(b)$, then $(a,b) = 0$ in $Br_2(\mathbb{Q}_p)$.

We define $A_i(p) \subset \mathbb{Z}^n / p^2 \mathbb{Z}^n$ as consisting of x such that

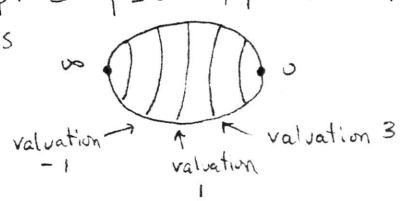
1. $P_i(x) \equiv 0 \pmod p$
   $P_i(x) \not\equiv 0 \pmod{p^2}$
2. $U_i(x) \not\equiv 0 \pmod p$, $U_i(x)$ not a quadratic residue mod p.
3. $V_j(x) \not\equiv 0 \pmod p$, $W_j(x) \not\equiv 0 \pmod p$.

By the lemma and the above remarks, we have

$$\alpha(x) = (P_i(x), U_i(x)) + \sum_j (V_j(x), W_j(x)) \neq 0 \quad \text{in } Br_2 \mathbb{Q}_p$$

Let $A(p) = \bigcup_i A_i(p)$

Example: Let $\alpha = (-1, T) \in Br_2(\mathbb{Q}(T))$. If $p \equiv 1 \ (4)$, there is no pole over $\mathbb{Q}_p$. If $p \equiv 3 \ (4)$, then $0, \infty$ are poles. One has



Outside the slices, the symbol is 0.

Notation: If E is a number field, p a prime, $r_p(E)$ is the number of prime ideals of $\mathcal{O}_E$ with norm p.

For each polar variety W_i, K_i the function field of W_i, and $L_i = K_i(\sqrt{\tilde{v}_i})$, where $\tilde{v}_i$ is the residue of α at W_i. Let E_i, F_i be the algebraic closure of $\mathbb{Q}$ in these fields.

Lemma: The number of solutions (mod p) of $P_i \equiv 0$ modulo p is $r_p(E_i) p^{n-1} + O(p^{n-3/2})$ for $p \to \infty$.

This follows from the Lang-Weil estimates applied to the hypersurface equation $P_i = 0$ modulo p.

Note that there are $r_p(E_i)$ absolutely irreducible varieties over $\mathbb{F}_p$.

Lemma: The number of x (mod p) with $P_i \equiv 0 \pmod p$ and $v_i(x)$ a quadratic residue modulo p is $\frac{1}{2} r_p(F_i) p^{n-1} + O(p^{n-3/2})$ for $p \to \infty$

Proof: One applies the Lang-Weil estimates to the subvariety of Aff^{n+1} defined by $P_i(x) = 0$ and $t^2 = v_i(x)$.

We can now begin estimating points:

Lemma: $|A_i(p)| = p^{2n-1}\left(r_p(E_i) - \frac{1}{2} r_p(F_i)\right) + O(p^{2n-3/2})$ for $p \to \infty$.

Proof: This follows from the above lemmas. Note that for each solution x of $P_i \equiv 0$ modulo p, there are p solutions $y_1, \dots, y_p$ modulo p^2 where $x \equiv y_i$ modulo p. If $P_i'(x) \not\equiv 0$ modulo p, then $P_i(y_i) \equiv 0 \pmod{p^2}$ for exactly one value of i. These y_i have density $\frac{1}{p^2}$ and can be ignored. If $P_i'(x) \equiv 0$ modulo p, the codimension of the intersection of $P_i \equiv 0$, $P_i' \equiv 0$ modulo p is at least two and the density of such x is at most $\frac{1}{p^2}$.

Lemma: $|A(p)| = \sum_i |A_i(p)| + O(p^{2n-2})$

If we let $r(p) = \sum_i \left\{ r_p(E_i) - \frac{1}{2} r_p(F_i) \right\}$, we have $|A(p)| = r(p) p^{2n-1} + O(p^{2n-3/2})$

To these estimates we can apply the sieve.

Statement of Sieve Theorem: Let $\Lambda = \mathbb{Z}^n$ and let $q_i > 1$ be integers with q_i and q_j relatively prime for $i \neq j$. For each q_i let $\Omega_i \subset \Lambda/q_i\Lambda$, and let $\frac{|\Omega_i|}{|\Lambda/q_i\Lambda|} = \frac{|\Omega_i|}{q_i^n} \geq w_i$.

Let X be a real number ≥ 1. Suppose $S \subset \Lambda$ and assume:
(1) "the archimedean condition" S is contained in $[0, X]^n$
(2) "the local condition" If $s \in S$, the reduction of s mod q_i is not in Ω_i.

Then $\boxed{|S| \leq (2X)^n / L(X^{1/2})}$ where $L(Y) = \sum_{q_J = \prod_{i \in J} q_i} \lambda(q_J)$ where $\lambda(q_J) = \prod_{i \in J} \frac{w_i}{1 - w_i}$

$q_J \leq Y$, J finite set.

For our situation, the q_i are the p_i^2.

Cor: If $q_i = p_i^2$, we have $|S| \leq (2X)^n \Big/ \sum_{\substack{q \text{ squarefree} \\ q \leq X^{1/4}}} \prod_{p \mid q} \frac{w_p}{1 - w_p}$

Lecture 25

12/18/90

Let $S \subset \mathbb{Z}^n$, $S = \{(t_i), t_i \in \mathbb{Z}, |t_i| \le X, \alpha \text{ defined at } t, \alpha(t) = 0\}$

We are proving that $|S| << \dfrac{X^n}{(\log X)^{d(\alpha)/2}}$ as $X \to \infty$.

Last time, we showed that $|S| \le (2X)^n \Big/ \sum_{q \le X^{1/4}} \prod_{p \mid q} \dfrac{\omega_p}{1-\omega_p}$

where $\omega_p = \frac{1}{p^{2n}} |A(p)| = \dfrac{a(p)}{p} + O\left(\dfrac{1}{p^{3/2}}\right)$ $\quad q$ squarefree

with $a(p) = \sum_i \left(r_p(E_i) - \frac{1}{2} r_p(F_i)\right)$

Now we must estimate $\sum \prod_{p \mid q} \omega_p/(1-\omega_p)$.

Let $f(s)$ be the Dirichlet series $\sum_{n \ge 1} a_n n^{-s}$ with $a_n = \begin{cases} 0 & \text{if } n \text{ is not square-free} \\ \prod_{p \mid n} \dfrac{\omega_p}{1-\omega_p} & \text{otherwise} \end{cases}$

Then $f(s) = \prod_p (1 - a_p p^{-s})$ with $a_p = \dfrac{a(p)}{p} + O(p^{-3/2})$

We will prove:

Theorem: $f(s)$ converges for $\mathrm{Re}(s) > 0$ and when $s \to 0$, $f(s) \sim \dfrac{c}{s^d}$, where $d = d(\alpha)$, $c > 0$.

Now if we let $A_X = \sum_{n \le X} a_n$, we want to estimate A_X. Together with the above theorem, the following Tauberian theorem finishes the proof of the estimate of $|S|$.

Tauberian Theorem (Hardy and Littlewood): (Hardy, Collected Papers, V. 6, p. 526 Thm 16) Let $f(s) = \sum_{n \ge 1} a_n n^{-s}$ convergent for $\mathrm{Re}(s) \ge 0$ with $a_n \ge 0$ and suppose that $f(s) \sim \dfrac{c}{s^d}$ as $s \to 0$.

Then $A_X \sim C (\log x)^d$ with $C = \dfrac{c}{\Gamma(1+d)}$

Example: Consider $\zeta(s+1) = \sum \frac{1}{n} n^{-s} = f(s)$. As $f(s) \sim \frac{1}{s}$ when $s \to 0$, $c = d = 1$ and $\sum \frac{1}{n} \sim (\log x)$.

Proposition: $f(s) = \left(\prod_i \zeta_{E_i}(s+1)\, \zeta_{F_i}(s+1)^{-1/2}\right) g(s)$ where $g(s)$ is holomorphic non-zero for $\mathrm{Re}(s) > -1/2$,

From the proposition, we have that $f(s)$ has "a pole of order $d(\alpha) - d(\alpha)/2 = d(\alpha)/2$" at $s = 0$.

Proof: For $s>1$, $\log \zeta_E(s) = -\sum_{\mathfrak{p}} \log(1-N\mathfrak{p}^{-s})$ is defined.

$$= \sum_p r_p(E)\, p^{-s} + \psi(s) \quad \text{with } \psi(s) \text{ a holomorphic function for } \mathrm{Re}(s) > 1/2.$$

Then $\log \zeta_E(s+1) = \sum_p \frac{r_p(E)}{p}\, p^{-s} + \psi(s+1)$,

with $\psi(s+1)$ holomorphic for $\mathrm{Re}(s) > -1/2$.

Hence $\sum_i \log \zeta_{E_i}(s+1)\, \zeta_{F_i}(s+1)^{-1/2} = \sum_p \cdot \frac{1}{p}\left(\sum_i r_p(E_i) - \frac{1}{2} r_p(F_i)\right) p^{-s} + h(s)$,

$h(s)$ hol. function for $\mathrm{Re}(s) > \frac{1}{2}$

and the proposition is proved.

~

Let $f(s) = \prod (1 + w_p p^{-s})$, with $w_p \geq 0$, $w_p = \frac{e(p)}{p} + O\left(\frac{1}{p^{1+\delta}}\right)$ for $\delta > 0$, $e(p) \geq 0$

One says $e(p)$ is a Frobenian function if there exists a Galois extension $E/\mathbb{Q}$ such that e_p depends only on Frob_p in $E/\mathbb{Q}$ (for large p)

One can define the mean value of a Frobenian function as $\lim_{x\to\infty} \left(\sum_{p\leq x} e(p)\right) / \pi(x)$. By the density theorem, this is the same as $\frac{1}{|G|} \sum_{g\in G} e(g)$ where e is regarded as a function on G.

If $e(p)$ is Frobenian, then f is holomorphic for $\mathrm{Re}(s) > 0$ and at $s=0$, $f \sim c/s^d$ with d = mean value of the Frobenian function

We can write $e_G = \sum_{\chi \text{ irred. char of } G} m_\chi \cdot \chi$ and let $f_1(s) = \prod L(\chi, s+1)^{m_\chi}$ for $\mathrm{Re}(s) > 0$

One has $f(s) = f_1(s)\, g(s)$, with g a holomorphic nonzero function for $\mathrm{Re}(s) > -\delta$.

Now $\zeta(s)$ has a simple pole at $s=1$, $L(\chi, s)$ is non-zero (no pole) at $s=1$ for $\chi \neq 1$. Hence, the mean value of the Frobenian function $= m_1$,

~

Finally, I'll give an example, due to Swinnerton-Dyer, of an element $\alpha \in Br_2\mathbb{Q}(T)$ for which "weak approximation" doesn't hold.

At ∞, "weak approximation" means that if $\alpha(t) = 0$ in $Br_2(\mathbb{R})$ for $t \in \mathbb{P}_1(\mathbb{R})$, then there exists $t_i \in \mathbb{P}_1(\mathbb{Q})$ such that $\{t_i\} \to t$ in $\mathbb{R}$ and $\alpha(t_i) = 0$ in $Br_2(\mathbb{Q})$

Let $\beta = (-1, 4T-7)$, $\gamma = (-1, T^2-2)$ and $\alpha = \beta+\gamma = (-1, (4T-7)(T^2-2))$

We have $\alpha(z) = (-1, (1)(z)) = (-1, z) = 0$ as we have seen before. One has the following:

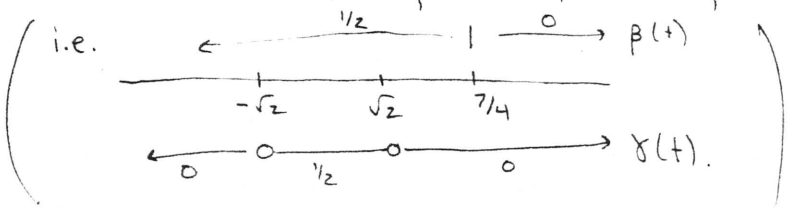
① Over every $\mathbb{Q}_p$ $(p \neq \infty)$ and for every $t \in \mathbb{P}_1(\mathbb{Q}_p)$, one has either $\beta(t) = 0$ or $\gamma(t) = 0$ in $Br_2\,\mathbb{Q}_p$

② Over $\mathbb{R}$, three of the four possible values for $\{\alpha(t), \beta(t)\}$ occur.

Recall that $Br_2\,\mathbb{R} = \{0, \frac{1}{2}\}$.

For $t > 7/4$, $\beta(t) = 0$, for $t < 7/4$, $\beta(t) = \frac{1}{2}$.
For $t > 2$, $\gamma(t) = 0$, $t < -2$, $\gamma(t) = 0$, and for $-2 < t < 2$, $\gamma(t) = \frac{1}{2}$.

i.e.



Claim: Let $-1/2 < t < 1/2$, $t \in \mathbb{Q}$. Then $\beta(t) \neq \gamma(t)$ in $Br_2(\mathbb{Q})$.
(Hence weak approximation doesn't hold.)

Suppose $\beta(t) = \gamma(t)$. Then at any prime p, by ①, one side is 0, hence so is the other. At ∞, by the diagram above, both sides are non-zero. But since the local invariants must sum to 0, this shows that such a t cannot exist.

Now let's check ① for $p \neq 2$.

(a) If $v_p(t) < 0$, then $\gamma(t) = (-1, T^2 - 2) = (-1, 1 - \frac{2}{t^2})$ and $1 - 2/t^2$ is a square in $\mathbb{Q}_p$. Hence $\gamma(t) = 0$.

(b) If $v_p(t) \geq 0$, then ① is satisfied except possibly when
$4t - 7 \equiv 0 \pmod{p}$ and $t^2 - 2 \equiv 0 \pmod{p}$.
Then $16t^2 - 32 \equiv 0 \pmod{p}$ and $p = 17$.
But -1 is a square in $\mathbb{Q}_{17}$ so the symbol is 0

The same logic is used for $p = 2$

(a) If $v(t) < 0$ then $\gamma(t) = 0$

(b) If $v(t) \geq 0$ then $\beta(t) = 0$ (since $4t - 7 \equiv 1 \pmod{4}$)

Finally, we can consider the same question for $Br_m(\mathbb{Q}(T_1, \cdots, T_n))$. The residue map has values in $H^1(\text{residue field}, \mathbb{Z}/m\mathbb{Z})$ which give cyclic extensions of degree e_i. One finds $|S| \ll \dfrac{X^n}{(\log X)^{\sum (1 - \frac{1}{e_i})}}$. Since there are only finitely many non-zero residues, $e_i = 1$ for almost all i

THE END