Quadratic forms and Galois Cohomology

R. Parimala

Department of Mathematics and Computer Science
Emory University

May 22, 2013

Fields Institute, Toronto

Classical invariants

We begin by recalling the classical invariants of quadratic forms.

Let k be a field, $\mathrm{char}(k) \neq 2$ and q a nondegenerate quadratic form over k.

Dimension mod 2 : $\dim_2(q) = n \pmod 2 \in \mathbb{Z}/2\mathbb{Z}$

Discriminant : $\mathrm{disc}(q) = (-1)^{n(n-1)/2} \det(A_q) \in k^*/k^{*2}$

Clifford invariant :

$$c(q) = \begin{cases} [C(q)] \in {}_2\mathrm{Br}(k), & \text{if } \dim(q) \text{ even} \\ [C_0(q)] \in {}_2\mathrm{Br}(k), & \text{if } \dim(q) \text{ odd.} \end{cases}$$

These classical invariants take values in the Galois cohomology groups.

Galois cohomology

$$H^n(k,\mathbb{Z}/2\mathbb{Z}) = \varinjlim_{L/k \text{ finite Galois}} H^n(\mathrm{Gal}(L/k),\mathbb{Z}/2\mathbb{Z})$$

n=0 $H^0(k,\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$

n=1 $H^1(k,\mathbb{Z}/2\mathbb{Z}) = k^\times/k^{\times 2}$ (Kummer isomorphism)

$(a) \in H^1(k,\mathbb{Z}/2\mathbb{Z})$ denotes the square class of $a \in k^\times$

n=2 $H^2(k,\mathbb{Z}/2\mathbb{Z}) = {}_2\mathrm{Br}(k)$

The cup product $(a).(b)$ represents the quaternion algebra with generators i, j and relations $i^2 = a$, $j^2 = b$, $ij = -ji$.

Milnor's conjecture

Milnor (1970) proposed 'successive' higher invariants for quadratic forms which could determine the isomorphism class of a quadratic form up to planes.

Definition

An *n-fold Pfister form* is a quadratic form isomorphic to $\langle\langle a_1, \cdots, a_n \rangle\rangle = \langle 1, -a_1 \rangle \otimes \langle 1, -a_2 \rangle \otimes \cdots \otimes \langle 1, -a_n \rangle$.

$P_n(k)$ = Set of isomorphism classes of n-fold Pfister forms.

The assignment

$$e_n(\langle\langle a_1, \ldots, a_n \rangle\rangle) = (a_1) \cdot (a_2) \cdot \cdots \cdot (a_n) \in H^n(k, \mathbb{Z}/2\mathbb{Z})$$

is well-defined on $P_n(k)$.

Milnor conjecture

$I(k) =$ ideal of even dimensional forms in $W(k)$.

$I^n(k) = I(k)^n$ is generated by $P_n(k)$.

Conjecture (Milnor,1970)

The map e_n extends to a homomorphism

$$e_n \colon I^n(k) \to H^n(k, \mathbb{Z}/2\mathbb{Z})$$

which is onto with kernel $I^{n+1}(k)$.

Equivalently, there is an isomorphism

$$(e_n) \colon \bigoplus_{n \geq 0} I^n(k)/I^{n+1}(k) \longrightarrow \bigoplus_{n \geq 0} H^n(k, \mathbb{Z}/2\mathbb{Z})$$

of the graded Witt ring and the graded Galois cohomology ring.

Milnor Conjecture

Milnor conjecture as stated above is a consequence of the two conjectures of Milnor relating Milnor ring K_*F with the mod 2 Galois cohomology ring and the graded Witt ring.

Milnor conjecture for $n = 2$ is a theorem of Merkurjev (1981) which is the first major breakthrough for a general field.

Milnor conjecture is a theorem due to Voevodsky (2003) and Orlov-Vishik-Voevodsky (2007).

Milnor Conjecture

The conjecture, together with Arason-Pfister Hauptsatz $\cap_{n\geq 1} I^n(k) = 0$, gives a complete classification of quadratic forms by their Galois cohomological invariants.

u-invariant

We shall discuss how a good understanding of the generation of the Galois cohomology group by symbols leads to bounding the u-invariant of the underlying field.

Definition

$u(k) := \max\{\dim(q) \mid q \text{ anisotropic quadratic form over } k\}$

Symbol length

An element of the form $(a_1) \cdot (a_2) \cdots (a_n)$ in $H^n(k, \mathbb{Z}/2\mathbb{Z})$ is called an *n-symbol*.

Definition

n-symbol length of k is bounded by N if every element $\zeta \in H^n(k, \mathbb{Z}/2\mathbb{Z})$ is a sum of at most N symbols.

If k is a number field, n-symbol length of k is 1 for all n.

u-invariant and symbol length

Proposition

Suppose k is a field with $H^n(k, \mathbb{Z}/2\mathbb{Z}) = 0$ for $n \geq n_0$ and the i-symbol length of F is bounded for $i < n_0$. Then $u(k) < \infty$.

If i-symbol length is at most r, every $\zeta \in H^i(k, \mathbb{Z}/2\mathbb{Z})$ is the invariant of a quadratic form in $I^i(k)$ of dimension at most $r2^i$.

Thus given any quadratic form q over k, by subtracting successively quadratic forms of bounded dimensions in I^i, one can bring q into $I^{n_0}(k)$. This group is zero because $H^{n_0}(k, \mathbb{Z}/2\mathbb{Z}) = 0$.

u-invariant and symbol length

The converse is also true.

Theorem (Saltman)

If $u(k)$ is finite, the i-symbol length is bounded for all i.

$i = 3$ There is a generic quadratic form $\tilde{q}$ of dimension $2m$ in I^3! Thus $e_3(\tilde{q})$ is a sum of bounded number of symbols. In particular over any field k, any form q in $I^3(k)$ of dimension at most $2m$ has bounded 3- symbol length.

$i \geq 4$ There is no generic quadratic form q of given dimension in I^i. Saltman proves that there exist finitely many generic types in H^i, one of which would specialise to $e_i(q)$ for a given quadratic form q in $I^i(k)$ of dimension $2m$.

Function fields of p-adic curves

Let us look at some special classes of fields of arithmetic interest.

Let K be a p-adic field. Then $u(K) = 4$.

Let F be the function field of a curve over K.

Question (Kaplansky)

Is $u(F) = 8$?

Function fields of p-adic curves

The first finiteness results for $u(F)$ were as late as 1997.

Theorem (Merkurjev, Hoffmann-Van Geel)

$u(F) \leq 22$ for $p \neq 2$.

A key ingredient in their proof is the following period-index bound of Saltman.

Function fields of p-adic curves

Theorem (Saltman)

Let A be a central simple algebra over F of index coprime to p. Then index(A) divides period$(A)^2$.

In particular, every 2-torsion element in $Br(F)$ has index at most 4, hence a tensor product of two quaternion algebras (if $p \neq 2$). i.e 2-symbol length of F is at most 2.

Theorem (Parimala-Suresh)

If $p \neq 2$, then every element in $H^3(F, \mathbb{Z}/2\mathbb{Z})$ is a symbol.

The above symbol length bounds brought down the bound for the u-invariant to 12.

Function fields of p-adic curves

Let F be function field in one variable over a p-adic field.

Theorem (Parimala-Suresh 2007)

If $p \neq 2$, $u(F) = 8$.

Theorem (Heath-Brown, Leep 2010)

For all p, $u(F) = 8$.

The method of proof of Heath-Brown and Leep is very different from Galois cohomological methods.

Techniques of Saltman

Let K be a p-adic field.

Let X/K be a smooth projective geometrically integral curve over K.

$F = K(X)$.

Let $\mathscr{O}$ be the ring of integers in K.

Let κ be the residue field of K.

Techniques of Saltman

Let $\mathscr{X} \to \mathscr{O}$ be a regular proper model of X.

Let $\mathscr{X}_0 \to \kappa$ be the special fiber of $\mathscr{X}$.

Let $\mathscr{X}^1$ be the set of codimension one points of $\mathscr{X}$.

$x \in \mathscr{X}^1$, $\mathscr{O}_{\mathscr{X},x}$ is a discrete valuation ring with field of fractions F and residue field $\kappa(x)$

Techniques of Saltman

Let A be a central simple algebra over F of exponent $\ell \neq p$.

Then A is unramified at x if there exists an Azumaya algebra $\mathscr{A}$ over $\mathscr{O}_{\mathscr{X},x}$ such that $[\mathscr{A} \otimes_{\mathscr{O}_{\mathscr{X},x}} F] = [A]$.

The unramified condition can be tested by the residue map

$$\partial_x : H^2(F, \mu_\ell) \to H^1(\kappa(x), \mathbb{Z}/\ell\mathbb{Z})$$

A is unramified at x if and only if $\partial_x(A) = 0$.

A is *unramified on $\mathscr{X}$* if for every $x \in \mathscr{X}^1$, $\partial_x(A) = 0$.

By purity A is unramified on $\mathscr{X}$ if and only if $A = \mathscr{A} \otimes_{\mathscr{O}_{\mathscr{X}}} F$ for some Azumaya algebra $\mathscr{A}$ on $\mathscr{X}$.

Techniques of Saltman

Theorem (Grothendieck)

$Br(\mathscr{X}) = 0$

Thus a finite extension L over F splits $A \Leftrightarrow A \otimes_F L$ is unramified on a regular proper model of L over $\mathscr{O}$.

Given a central simple algebra A over F, Saltman proves that there exist $f, g \in F^*$ such that $A \otimes F(\sqrt[\ell]{f}, \sqrt[\ell]{g})$ is unramified on a regular proper model of $F(\sqrt[\ell]{f}, \sqrt[\ell]{g})$.

Degree three cohomology

One can define unramified elements in $H^n(F, \mu_\ell^{\otimes 2})$ with respect to a model $\mathscr{X}$ as elements which belong to the image of $H^n_{\text{et}}(\mathscr{O}_{\mathscr{X},x}, \mu_\ell^{\otimes 2}) \to H^n(F, \mu_\ell^{\otimes 2})$ for every $x \in \mathscr{X}^1$.

Unramified elements are precisely the elements of the kernel of the residue maps.

Theorem (Kato)

$H^3_{nr}(F/\mathscr{X}, \mu_\ell^{\otimes 2}) = 0.$

Kato's result was used in the proof that every element in $H^3(F, \mathbb{Z}/2\mathbb{Z})$ is a symbol.

The bad characteristic case

Let F be the function field of a p-adic curve.

For $\ell = p$, it remained open whether there were bounds for the index in terms of the period for the p-torsion elements in $Br(F)$.

For $\ell = p = 2$, $u(F) = 8 \Rightarrow$ for any element in ${}_2\mathrm{Br}(F)$ is a sum of at most three symbols (index divides 8).

If $A \sim H_1 \otimes \cdots \otimes H_n$, H_i quaternion algebras, there is a quadratic form q of dimension $2n + 2$ such that $e_2(q) = A$.

$q \simeq q_1 \perp planes$, $\dim(q_1) = 8$

$[A] = e_2\,(q_1) =$ tensor product of three quaternion algebras

The bad characteristic case

Theorem (Parimala-Suresh)

Let F be a function field in one variable over a p-adic field and A a central simple algebra over F. Then the index of A divides the square of its period.

In fact, one has the following more general statement.

The bad characteristic case

Let κ be a field of characteristic p.

p-rank(κ) is n if $[\kappa : \kappa^p] = p^n$.

Theorem (Parimala-Suresh)

Let K be a complete discrete valued field with residue field κ and F a function field in one variable over K. Suppose that p-rank$(\kappa) = n$. Then for any central simple algebra A over F of exponent p, index(A) divides p^{2n+2}.

In particular if κ is perfect, index(A) divides p^2.

The method of proof

There are two main ingredients in the proof of the above theorem.

I. Kato's filtration

II. Harbater-Hartmann-Krashen patching.

Kato's filtration

Let (K, ν) be a complete discrete valued field with $\text{char}(K) = 0$ and $\text{char}(\kappa) = p$.

Let R be the valuation ring of ν and π a parameter.

$U_0 =$ units in R, $U_i = \{u \in U_0 \mid u \equiv 1 \ mod\ \pi^i\}$

Suppose K contains a primitive p^{th} root of unity ζ.
For $a, b \in K^*$, let (a, b) denote the cyclic algebra of degree p with generators x, y and relations $x^p = a$, $y^p = b$, $xy = \zeta yx$

Kato's filtration

$br(K)_0 = {}_p\mathrm{Br}(K)$

$br(K)_i =$ subgroup of ${}_p\mathrm{Br}(K)$ generated by $\{(u, a) \mid u \in U_i, a \in K^*\}$.

Kato's filtration is finite: $br(K)_n = 0$ for $n \geq N = \frac{\nu(p)p}{p-1}$.

Kato's filtration

Let Ω^1_κ be the module of differentials of κ.

Let $K_2(\kappa)$ be the Milnor K-group and $k_2(\kappa) = K_2(\kappa)/pK_2(\kappa)$.

There are surjective homomorphisms:

$$\rho_0 : k_2(\kappa) \oplus \kappa^*/\kappa^{*p} \to br(K)_0/br(K)_1$$

defined by $\rho_0((a,b) + (c)) = (\tilde{a}, \tilde{b}) + (\pi, \tilde{c})$

$$\rho_i : \Omega^1_\kappa \oplus \kappa \to br(K)_i/br(K)_{i+1}, i \geq 1$$

defined by $\rho_i(x\frac{dy}{y}, z) = (1 + \tilde{x}\pi^i, \tilde{y}) + (\pi, 1 + \tilde{z}\pi^i)$.

Here $\tilde{}$ denote the lifts in R.

Kato's filtration

Let $\{y_1, \cdots, y_n\}$ be a p-basis of κ. Then $\{dy_i \mid 1 \leq i \leq n\}$ is a basis of Ω^1_κ and $\{dy_i \wedge dy_j \mid 1 \leq i < j \leq n\}$ is a basis of Ω^2_κ.

We note that $k_2(\kappa)$ is isomorphic to a subgroup of Ω^2_κ.

Using the surjections ρ_i, one can modify a given element $\zeta \in {}_p\mathrm{Br}(K)$ by a bounded number of symbols to fit it into $br(K)_{N+1} = 0$.

This leads to the fact that index(ζ) divides p^{2n+1} (In fact, if $n \geq 1$, index(ζ) divides p^{2n}).

HHK patching

Let K be a complete discrete valued field with residue field κ.

Let X be a smooth projective geometrically integral curve over K with function field F.

Let $\mathscr{X} \to Spec(\mathscr{O})$ be a regular proper model of X.

Let $\mathscr{X}_0 \to Spec(\kappa)$ be the special fiber.

For $x \in \mathscr{X}_0$, let $\hat{\mathscr{O}}_{\mathscr{X},x}$ denote the completion of the local ring $\mathscr{O}_{\mathscr{X},x}$ at x.

Let F_x be the field of fraction of $\hat{\mathscr{O}}_{\mathscr{X},x}$.

HHK patching

Theorem (Harbater-Hartmann-Krashen.)

For any $\alpha \in Br(F)$,

$$index(\alpha) = lcm(index(\alpha_{F_x}) \mid x \in \mathscr{X}_0)$$

Thus it suffices to bound the indices of $\alpha \otimes_F F_x$ for all $x \in \mathscr{X}_0$ for a suitable model $\mathscr{X}$ of F.

The method of proof

For any $x \in \mathscr{X}_0$ corresponding to an irreducible component of $\mathscr{X}_0$, F_x is a complete discrete valued field and Kato's filtration gives bounds for α_{F_x}.

For a closed point x of $\mathscr{X}_0$, one has to do some further work to get bounds.

The theorem of HHK together with these bounds leads to the required period-index bound for F.

The bad characteristic-u-invariant

The above period-index bounds lead surprisingly to the following

Theorem (Parimala-Suresh.)

Let K be a complete discrete valued field with residue field κ. Suppose $\mathrm{char}(K) = 0$, $\mathrm{char}(\kappa) = 2$ and κ is perfect. Let F be a function field in one variable over K. Then $u(F) = 8$.

This theorem recovers Heath-Brown/Leep result for function fields of dyadic curves.

Function fields over number fields

Let K be a totally imaginary number field.

$u(K) = 4$ (Hasse-Minkowski Theorem)

Let F be a function field in one variable over K

An open question

Is $u(F) < \infty$?

There are some conditional results due to Lieblich-Parimala-Suresh.

Function fields over number fields

To obtain the finiteness of the u-invariant, one tries to bound the 2 and 3-symbol lengths in F.

Note that $\mathrm{cd}(F) \leq 3$ and $H^4(F, \mathbb{Z}/2\mathbb{Z}) = 0$.

Function fields over number fields

Let K be a totally imaginary number field and $\mathscr{O}$ the ring of integers in K.

Let X be a smooth projective geometrically integral curve over K and F its function field.

Let $\mathscr{X} \to \mathscr{O}$ be a regular proper model of X.

The sharp difference between the local and the global cases:

$Br(\mathscr{X})$ is not necessarily zero!

Function fields over number fields

Thus to bound the 2-symbol length of F, one is led to the following questions:

1. Can one split the ramification of $\alpha \in H^2(F, \mu_\ell)$ in a bounded degree extension of F?
2. Can one bound the index of classes in ${}_\ell\mathrm{Br}(\mathscr{X})$?

Function fields over number fields

The first question has an affirmative answer.

Theorem (Lieblich, Parimala, Suresh)

Let $\alpha \in {}_\ell\mathrm{Br}(F)$. Then there exist $f, g, h \in F^*$ such that $\alpha \otimes F(\sqrt[\ell]{f}, \sqrt[\ell]{g}, \sqrt[\ell]{h})$ is unramified on any regular proper model over the ring of integers in K.

Thus the 2-symbol length of F is bounded if and only if indices of unramified classes are bounded for all finite extensions of F.

Function fields over number fields

We also have the following:

Theorem (Suresh)

For every $\beta \in H^3(F, \mathbb{Z}/2\mathbb{Z})$, there exists $f \in F^*$ such that $\beta = (f) \cdot \alpha$ with $\alpha \in H^2(F, \mathbb{Z}/2\mathbb{Z})$.

Thus 3-symbol length is bounded if 2-symbol length is bounded.

Thus $u(F) < \infty \Leftrightarrow$ every element in $Br(\mathscr{X})$ has bounded index for any regular proper model of every finite extension of F.

Conjecturally, for $\alpha \in {}_{\ell}\mathrm{Br}(\mathscr{X})$, index$(\alpha)$ divides ℓ^2.

Colliot-Thélène's conjecture

The Brauer Manin obstruction

Let X be a smooth projective variety over a number field K.

Ω_K = set of all places of K

$v \in \Omega_K$, K_v completion of K at v.

For $x_v \in X(K_v)$ and $\alpha \in Br(X)$, $\alpha(x_v) \in Br(K_v) \overset{inv_v}{\hookrightarrow} \mathbb{Q}/\mathbb{Z}$.

Further $\alpha(x_v) = 0$ for almost all $v \in \Omega_F$

Colliot-Thélène's conjecture

Reciprocity for $Br(K)$ yields : $x \in X(K)$, $\alpha \in Br(X)$,

$$\sum_v inv_v(\alpha(x)) = 0$$

Brauer-Manin set :

$$\left(\prod_v Br(X(K_v))\right)^{Br(X)} = \{(x_v) \mid \sum_v inv_v(\alpha(x_v)) = 0\}$$

Colliot-Thélène's conjecture

Brauer-Manin obstruction is the only obstruction to the Hasse principle for the existence of rational points on X if the following is true :

Brauer-Manin set is non-empty $\Rightarrow X(K) \neq \emptyset$.

There are examples to show that the Brauer-Manin obstruction is not the only obstruction to HP for the existence of rational points.

Colliot-Thélène's conjecture

One can define in a similar way the Brauer-Manin obstruction to existence of zero-cycles of degree one on X.

Zero-cycles of degree one

$\sum_i n_i x_i$, x_i closed points of X such that $\sum n_i deg(x_i) = 1$

$x \in X(K)$, x is a zero-cycle of degree 1.

Conjecture (Colliot-Thélène)

Let X be a smooth projective variety over a number field. Then the Brauer-Manin obstruction is the only obstruction to Hasse principle for the existence of 0-cycles of degree one on X.

u-invariant

Theorem (M.Lieblich, Parimala, Suresh)

If CT-conjecture is true for unirational varieties X, then for all $\alpha \in {}_\ell\mathrm{Br}(F)$ unramified on a model $\mathscr{X}$ of $\mathscr{O}$, $\mathrm{ind}(\alpha)$ divides $\mathrm{period}(\alpha)^2$.

Corollary

Let K be a totally imaginary number field and F, a function field in one variable over K. If CT-conjecture holds, then $u(F) < \infty$.

Idea of the proof

Let K be a number field.

Let X be a smooth projective geometrically integral curve over K and F its function field.

$\mathscr{X} \to \mathscr{O}$: Regular proper model of X over the ring of integers $\mathscr{O}$ in K.

$\alpha \in {}_{\ell}\mathrm{Br}(\mathscr{X})$, $\alpha_K \in {}_{\ell}\mathrm{Br}(X)$,

$\tilde{\alpha} \in H^2_{ff}(\mathscr{X}, \mu_\ell)$, a lift of α.

$\tilde{\mathscr{C}}$: μ_ℓ-gerbe on $\mathscr{X}$ associated to α.

$\mathscr{C}$: μ_ℓ-gerbe on X which is the restriction of $\tilde{\mathscr{C}}$ to X.

Idea of the proof

$\mathscr{M}$: moduli stack of $\mathscr{C}$-twisted stable sheaves of rank ℓ and determinant 1.

M : moduli space of C-twisted stable sheaves of rank ℓ and determinant 1.

M is a smooth quasi projective variety over K.

$\mathscr{M}$ is a μ_ℓ-gerbe on M.

$Br(M)/Br(K)$ is generated by the class ζ of the μ_ℓ-gerbe $\mathscr{M}$

Idea of proof

Let M^{sc} be a smooth compactification of M.

$(M(\mathbb{A}(K)))^{Br(M)} \hookrightarrow (\prod_v M^{sc}(K_v))^{Br(M^{sc})}$

For all $v \in \Omega_K$, $\alpha_v = 0$ since $Br(\mathscr{X}_v) = 0$ and hence $\mathscr{M}(K_v) \neq \emptyset$.

In particular $M(K_v) \neq \emptyset$.

Further, for all $z_v \in M(K_v)$, $\zeta(z_v) = 0$

Hence $(M(\mathbb{A}(K)))^{Br(M)} \neq \emptyset$

$\Rightarrow (\prod_v M^{sc}(K_v)^{Br(M^{sc})}) \neq \emptyset$

Idea of proof

CT-Conjecture $\Rightarrow M^{sc}$ has a zero cycle of degree 1.

$\Rightarrow M$ has a zero-cycle of degree 1

$\Rightarrow \exists\ K'/K$ finite extension with $[K' : K]$ coprime to ℓ such that $M(K') \neq \emptyset \Rightarrow \mathscr{M} \times_M K' \in {}_\ell\mathrm{Br}(K')$ has index ℓ, k' being a number field.

$\Rightarrow \exists\ E/K'$, $[E : K'] = \ell$ and $\mathscr{M}(E) \neq \emptyset$.

$\Rightarrow \alpha_E$ has index ℓ.

$\Rightarrow \alpha$ has index ℓ^2.