Contents

1 The Brauer Group **3**

1.1 Definition and First Properties of Brauer Groups 3

1.2 Brauer Groups of Local Fields . . . 7

1.2.1 Invariants 7

1.3 The Local-Global Relation 13

1.3.1 Localization 13

1.4 Application to Ring Class Numbers . 21

1.5 Computation of the Classical DL . . 25

1.6 Description of cyclic extensions . . 27

2 Index-Calculus in Global Brauer Groups **29**

3 Construction of Elements in the Brauer Group **39**

3.1 Pairings with Dirichlet Characters . 39

3.2 Pairings with Principal Homogenous Spaces 42
3.3 Cassel's Pairing 44

1 The Brauer Group

In the last Lecture we have motivated the importance of the second cohomology group of the multiplicative group of local fields.

1.1 Definition and First Properties of Brauer Groups

Let K be a field.

Definition 1.1 *The Brauer group of K is the cohomology group*

$$H^2(G_K, K_s^*).$$

It is denoted by

$$\mathrm{Br}(K).$$

$\mathrm{Br}(K)$ is a torsion group.

One can interpret its elements as classes of simple K-algebras with center K.
The addition in the cohomology group corresponds to the tensor product.
The unit element in $\mathrm{Br}(K)$ corresponds to the class of full matrix algebras.
Let L be an extension field of K, A an algebra representing $c \in \mathrm{Br}(K)$.

$A \otimes_K L$ represents

$$c_L = \mathrm{res}_{K/L}(c).$$

Recall that for Galois extensions L/K the inflation map from $H^2(G(L/K), L^*)$ to $H^2(G_K, K_s^*)$ is injective and that the kernel of the restriction map $\mathrm{res}_{K/L}$ is equal to $H^2(G(L/K), L^*) := \mathrm{Br}(L/K)$, the relative Brauer group.

Assume that L/K is a cyclic extension of degree n with $G(L/K) =< \tau >$. Algebras corresponding to elements in $H^2(G(L/K), L^*)$ are called *cyclic* algebras.

Recall: We get all cyclic algebras split be L as cohomology classes of cocycles in the following way:
For $a \in K^*$.
define $f_{\tau,a} : G \times G \to L^*$ by

$$f_{\tau,a}(\tau^i, \tau^j) = \begin{cases} a & : \quad i+j \geq n \\ 1 & : \quad i+j < n \end{cases}$$

For two elements a, a' the cocycles $f_{\tau,a}$ and $f_{\tau,a'}$ are in the same cohomology class if and only if $a \cdot a'^{-1} \in N_{L/K}L^*$.
We denote the corresponding class of cyclic algebras by

$$(L, \tau, a \cdot N_{L/K}L^*).$$

We get $\mathrm{Br}(L/K) \cong K^*/N_{L/K}(L^*)$.
Note that this isomorphism depends on the choice of τ!

1.2 Brauer Groups of Local Fields

1.2.1 Invariants

Let L_u be the unique unramified extension of K of degree n.
$G(L_u/K) =< \phi_q >$ where ϕ_q is the lift of the Frobenius automorphism of $\mathbb{F}_q$.
Let $c \in \mathrm{Br}(K)$ be split by L_U.
Since both L_u and ϕ_q are canonically given we can characterize c in a canonical way by

$$(L_u, \phi_q, a \cdot N_{L_u/K}(L_u^*)).$$

Since

$$N_{L_u/K}(L_u^*) \cong < \pi > / < \pi^n >$$

with π an uniformizing element of K the class of c is uniquely determined by $w_{\mathfrak{p}}(a)$ mod n.

Definition 1.2 *Let* $c \in H^2(G(L_u/K), L_u^*)$ *be given by the triple* (L_u, ϕ_q, a).
Then $v(a) \in \mathbb{Z}/n\mathbb{Z}$ *is the* invariant $\mathrm{inv}_K(c)$ *of* c.

It is obvious that the discrete logarithm in $H^2(G(L_u/K), L_u^*)$ is computable in polynomial time if the elements in this group are given in the "canonical" way, i.e. as cyclic algebras with automorphism ϕ_q.

Lemma 1.3 *Assume that* τ *is another generator of* $G(L_u/K)$ *and* c *is given by the triple* (L_u, τ, a). *Let* $f \in \mathbb{Z}$ *be such that* $\tau^f = \phi_q$.
Then $\mathrm{inv}(c) = f \cdot w_{\mathfrak{p}}(a) \bmod n$.

Hence the computation of the invariant of c leads to a discrete logarithm problem in $G(L_u/K)$.

Example 1.4 *Assume that* $L_u = K(\alpha)$ *with* $\alpha \in U(K)$ *such that* $\tau(\alpha) = \beta \cdot \alpha$ *with* $\beta \in K$.
Then $\tau^f = \phi_q$ *if and only if* $\beta^f \equiv \alpha^q$ *modulo the maximal ideal of* K. *So we have to solve a discrete logarithm problem in* $\mathbb{F}_q$.

By the duality theorem we know that $\mathrm{Br}(K)[n]$ is cyclic. Hence every element of c in $\mathrm{Br}(K)[n]$ (resp. every central simple algebra A over K) is equivalent to a cyclic algebra split by L_u. So we can associate to c (resp. A) its invariant and we get an isomorphism

$$\mathrm{inv}_K : \mathrm{Br}(K)[p] \to \mathbb{Z}/p.$$

The discrete logarithm in $\mathrm{Br}(K)[n]$ would be trivial if we could compute invariants.

The application of the Tate-Lichtenbaum pairing leads to cyclic algebras split by ramified extensions.

Assume that $n \mid q-1$.

Take $L_n = K(\pi^{1/n})$ and $\tau \in G(L_n/K)$ with

$$\tau(\pi^{1/n}) = \zeta_n \pi^{1/n}.$$

Since π is a norm element and τ acts trivially on the residue field of K the class c is determined by a triple

$$(L_n, \tau, \zeta_n^k).$$

Let M_n be the composite of L_n and L_u. It is a Galois extension with Galois group $< \tau, \phi_q >$.
To compute the invariant of C we have to find a number ℓ such that

$$\inf_{M/L_n}(c) = inf_{M/L_u}((L_u, \phi_q^{\ell}, \pi_q)).$$

This can be worked out in an explicit way, and as result we see that again we have to compute a discrete logarithm in $\mathbb{F}_q$.

1.3 The Local-Global Relation

We go one step further and lift local fields to global fields.
K be a global field, i.e. K is either a finite algebraic extension of $\mathbb{Q}$ or a function field of one variable over a finite field $\mathbb{F}_q$.

1.3.1 Localization

Let v be a non-archimedean valuation on K. Let $\tilde{v}$ be an extension of v to K_s with decomposition group $G_{\tilde{v}}$ which will be identified with G_{K_v}, the Galois group of the completion of K at v. K_v depends only on the place, ie the equivalence class $\mathfrak{p}$ of the valuation v and hence is denoted by $K_{\mathfrak{p}}$.

The decomposition group of v (or more precisely, of a chosen extension of v), depends up to conjugation only on $\mathfrak{p}$ and is denoted by $G_{\mathfrak{p}}$.
The set of all places of K is denoted by Σ_K.
A G_K-module M has (by restriction) a natural structure as $G_{\mathfrak{p}}$-module and so we have restriction maps

$$\rho_{\mathfrak{p}} : H^n(G_K, M) \to H^n(G_{\mathfrak{p}}, M)$$

of cohomology groups.
If M is a $G_{\mathfrak{p}}$-submodule of $M_{\mathfrak{p}}$ we can interpret cochains with value in M as cochains with value in $M_{\mathfrak{p}}$. Combining this with $\rho_{\mathfrak{p}}$ we get maps (again denoted by $\rho_{\mathfrak{p}}$) from $H^n(G_K, M)$ in $H^n(G_{\mathfrak{p}}, M_{\mathfrak{p}})$.

We apply this to $M = K_s^*$, $M_{\mathfrak{p}} = K_{\mathfrak{p},s}^*$ and $n = 2$ and get for all $\mathfrak{p} \in \Sigma_K$ the restriction map

$$\rho_{\mathfrak{p}} : \mathrm{Br}(K) \to \mathrm{Br}(K_{\mathfrak{p}}).$$

The kernel of this map consists of the classes of simple algebras with center K which become isomorphic to full rings of matrices after tensorizing with $K_{\mathfrak{p}}$.
In terms of invariants this means:
for $c \in \mathrm{Br}(K)$ define $\mathrm{inv}_{\mathfrak{p}}(c) := \mathrm{inv}_{K_{\mathfrak{p}}}(\rho_{\mathfrak{p}}(c))$.
Then the kernel of $\rho_{\mathfrak{p}}$ consists of the set
$\{c \in \mathrm{Br}(K);\ \mathrm{inv}_{\mathfrak{p}}(c) = 0\}$.

Recall:

Theorem 1.5 *Let K be a global field and $n \in \mathbb{N}$ odd and prime to $char(K)$. Then the sequence*

$$0 \to \mathrm{Br}(K)[n] \xrightarrow{\oplus_{\mathfrak{p}\in\Sigma_K} \rho_{\mathfrak{p}}} \bigoplus_{\mathfrak{p}\in\Sigma_K} \mathrm{Br}(K_{\mathfrak{p}})[n] \xrightarrow{\Sigma_{\mathfrak{p}\in\Sigma_K} \mathrm{inv}_{\mathfrak{p}}} \mathbb{Z}/n \to 0$$

is exact.

Trivial but useful is

Corollary 1.6 *Let T be a finite set of places of K. For each $\mathfrak{p} \in T$ let $A_{\mathfrak{p}}$ be a given cyclic algebra corresponding to $c_{\mathfrak{p}} \in \mathrm{Br}(K_{\mathfrak{p}})[n]$.*
For every cyclic algebra A over K of order n with

$$A \bigotimes K_{\mathfrak{p}} \cong A_{\mathfrak{p}}$$

for $\mathfrak{p} \in T$
we get

$$-\sum_{\mathfrak{p} \in \Sigma_K \setminus T} \mathrm{inv}_{\mathfrak{p}}(\rho_{\mathfrak{p}}(A)) = \sum_{\mathfrak{p} \in T} \mathrm{inv}_{\mathfrak{p}}(A_{\mathfrak{p}}).$$

Remark 1.7 *For the existence of lifts A of $A_{\mathfrak{p}}$ we need* existence theorems *for cyclic extensions of K with* restricted *ramification, and such results are delivered by* global class field theory *(in an explicit way e.g. by CM theory).*

Let $\mathfrak{m}$ be an ideal in O_K, the ring of integers of K. We *assume* that there is a cyclic extension L of odd degree n of K unramified outside of $T_{\mathfrak{m}}$, the set of places dividing $\mathfrak{m}$.
Let τ be a generator of $G(L/K)$.
For $\mathfrak{p} \notin T_{\mathfrak{m}}$ let $\phi_{\mathfrak{p}}$ be a Frobenius automorphism at $\mathfrak{p}$ in $G(L/K)$, and $f_{\mathfrak{p}}$ so that

$$\tau^{f_{\mathfrak{p}}} = \phi_{\mathfrak{p}}.$$

For $a \in K^*$ define the cyclic algebra A by (L, τ, a). Using Theorem 1.5 and Lemma 1.3 we get

Proposition 1.8 *For all $\mathfrak{p} \in \Sigma_K$ there are numbers $f_\mathfrak{p}$ such that for all elements $a \in K^*$ we have*

$$\sum_{\mathfrak{p} \in T_\mathfrak{m}} \mathrm{inv}_\mathfrak{p}(A) f_\mathfrak{p} \equiv -\left(\sum_{\mathfrak{p} \notin T_\mathfrak{m}} w_\mathfrak{p}(a)) f_\mathfrak{p} \bmod n \right)$$

where $w_\mathfrak{p}$ is the normed valuation in $\mathfrak{p}$.

1.4 Application to Ring Class Numbers

Apply Proposition 1.8 to the following problem:
For $\mathfrak{m} < O_K$ compute the order $\varphi(\mathfrak{m})$ of the ring class group of O_K with module $\mathfrak{m}$, i.e. the order of the ideal class group of the order in K with conductor $\mathfrak{m}$.
Define

$$K_{\mathfrak{m}} = \{a \in K^* \text{ with } \sum_{\mathfrak{p} \in T_{\mathfrak{m}}} \text{inv}_{\mathfrak{p}}((L, \tau, a)) = 0\}$$

for all cyclic extensions of K with conductor $\leq \mathfrak{m}$.
A subset (?) of $K_{\mathfrak{m}}$ are the elements a in K for which

$$w_{\mathfrak{p}}(a-1) \geq 1;\ \mathfrak{p} \in T_{\mathfrak{m}}.$$

Proposition 1.9 *1. Take any subset* $R \subset K_{\mathfrak{m}}$ *and an odd prime number* ℓ. *If* $\ell \mid \varphi(\mathfrak{m})$ *then the system of linear equations* $\mathcal{L}_{\mathcal{R}}$ *given by* $\{L_a;\, a \in R\}$ *with*

$$L_a : \sum_{\mathfrak{p} \in \Sigma_K \setminus T_{\mathfrak{m}}} w_{\mathfrak{p}}(a) X_{\mathfrak{p}} = 0$$

has a non-trivial solution modulo l.

2. Assume that we find R *such that the number of variables* $X_{\mathfrak{p}}$ *occurring with non-zero coefficient in at least one of the equations in* $\mathcal{L}_R$ *is equal to the rank of* $\mathcal{L}_R$ *then* l *divides the determinant of the system, and so the odd prime divisors of* $\varphi(\mathfrak{m})$ *are a subset of the prime divisors of the determinant.*

Example 1.10 *Take* $K = \mathbb{Q}$.
For $m \in \mathbb{N}$ *the function* $\varphi(m)$ *is the classical Euler totient function. The global class field theory of* $\mathbb{Q}$ *is completely determined by the theorem of Kronecker and Weber.*
We now assume that the prime number ℓ *divides* $\varphi(m)$ *and consider a global algebra* A *of the form* $A = (L/K, \sigma, a)$ *corresponding to this extension with a prime to* m. *To be explicit we choose a random number* $1 < k < m$ *and assume that the exponentiation of* m*-th roots of unity by* k *induces* σ *on* L.

For $a = \prod p^{n_p}$ *the theorem by Hasse–Brauer–Noether leads to a relation of the form*

$$\sum_{p|m} \mathrm{inv}_p A + \sum_{\gcd(p,m)=1} n_p f_p \equiv 0 \bmod \ell \tag{1}$$

with $f_p \in \mathbb{Z}$ *such that* $p \equiv k^{f_p} \bmod m$.

Assume moreover that $a = r/s$ *with* $r, s \in \mathbb{Z}$ *and* $\gcd(r,s) = 1$ *such that* $m \mid (r-s)$. *Then*

$$\sum_{\gcd(p,m)=1} n_p f_p \equiv 0 \bmod \ell. \tag{2}$$

1.5 Computation of the Classical DL

Let $\mathfrak{m} = \mathfrak{p}_0$ be a prime ideal of the ring of integers O_K of K with residue field $\mathbb{F}_q$. We assume that ℓ is a prime number dividing $q-1$ and that there is a cyclic extension of K of degree ℓ totally ramified at $\mathfrak{p}_0$. For instance this is the case if the class number of K is prime to ℓ.
Let ζ and ζ_1 be two ℓ-th roots of unity which are the reduction modulo $\mathfrak{p}_0$ of two integers a and a_1 in O_K.

Proposition 1.11 *Let $k \in \mathbb{Z}$. Then $\zeta^k = \zeta_1$ if and only if*

$$k \left(\sum_{\mathfrak{p} \in \Sigma_K \setminus \{\mathfrak{p}_0\}} f_{\mathfrak{p}} w_p(a) \right)$$

$$\equiv \sum_{\mathfrak{p} \in \Sigma_K \setminus \{\mathfrak{p}_0\}} f_{\mathfrak{p}} w_p(a_1) \bmod \ell.$$

Recall that we have seen already that the discrete logarithm in Brauer groups of local fields is (at least if we deal only with cyclic algebras) transferred to the discrete logarithm in their residue fields. Proposition 1.11 shows that we can compute the discrete logarithm in finite fields if we can compute the numbers $f_{\mathfrak{p}}$ at least for divisors of lifts of ζ and ζ_1.

1.6 Description of cyclic extensions

How can one describe extension fields L of global fields K by objects defined over K?
A first answer is to use polynomials (maybe monic over the ring of integers O_K) which define L and then the decomposition of these polynomials modulo the places of K give all the information necessary for studying the arithmetic of L.
In practice this method is working only for small degrees of L/K and definitely not for degrees of the size which occur in cryptography (e.g. $\ell \sim 10^{60}$)).

Alternatively we could try to compute for a given extension L and a given prime $\mathfrak{p}$ of O_K the number $f_{\mathfrak{p}}$.
If we would succeed we would have a very satisfying description of the arithmetic of L. It would be much finer than a description of the splitting behavior of primes in L which alone characterizes L.

2 Index-Calculus in Global Brauer Groups

The results of the previous sections motivate the search for algorithms to determine the numbers $f_{\mathfrak{p}}$ which characterize the Frobenius automorphisms at places $\mathfrak{p}$ of K related to cyclic extensions with conductor dividing an ideal $\mathfrak{m}$.
The method to do this is an index-calculus algorithm of the type one is used to see in factorization algorithms. But we use the opportunity to stress that by computing the $f_{\mathfrak{p}}$ we get the φ-function and not the factorization of $\mathfrak{m}$.

To demonstrate the principle we take $K = \mathbb{Q}$ and so $\mathbb{F}_q = \mathbb{F}_p$.

The congruence (1) can be seen as solutions of a system of linear equations relating the indeterminates f_p for p prime to m and $\mathrm{inv}_p(A)$ for $p \mid m$. We use cyclic algebras with trivial invariants at primes dividing m.

At the other primes we want to have $w_p(a) \neq 0$ in a certain distinguished set big enough such that many elements a can be found, and small enough to make linear algebra feasible.

The key concept is the notion of smooth numbers.

Let B be a natural number.

Definition 2.1 *A number $n \in \mathbb{N}$ is B-smooth if all prime numbers dividing n are bounded by B.*

Theorem 2.2 *(Theorem of Canfield-Erdös-Pomerance)*
Let x, y be natural numbers which grow asymptotically such that (for some fixed $\epsilon \in]0,1[$) we have

$$(\log x)^{\epsilon} < u < (\log x)^{1-\epsilon}$$

with $u = \log x / \log y$.
Let $\psi(x,y)$ be the number of numbers $n < x$ which are y-smooth.
Then

$$\psi(x,y) = xu^{-u(1-o(1))}$$

asymptotically for $x \to \infty$.

Example 2.3 *We define the subexponential function*
$L_x(\alpha, c) := exp(c \log(x)^{\alpha} \cdot \log\log(x)^{1-\alpha})$.
Take $y = L_x(1/2, c)$. *Then*

$$\psi(x, y)/x \sim L_x(1/2, -1/2c).$$

Hence the heuristic probability to find a smooth number with smoothness bound $B = L_x(1/2, c)$ *in* $[1, x]$ *is* $L_x(1/2, -1/2c)$. *If we want to find* B *such numbers we have (again heuristically) to make* $\sim L_x(1/2, \frac{2c-1}{2c})$ *trials.*

We are now ready to state the most simple version of the index-calculus algorithm we have in mind.

An algorithm for $K = \mathbb{Q}$ Choose a smoothness bound B and compute the factor basis S consisting of the primes less than or equal to B.
Let d be the smallest number $\geq \sqrt{m}$.
For $\delta \in L := [0, ..., l_0]$ take $a_1(\delta) := d + \delta$, $a_2(\delta) := c_0 + 2\delta \cdot d + \delta^2$ ($\equiv a^2$ modulo m) with $c_0 = d^2 - m$.

We get a linear equation of the type described in Proposition 1.9

$$L_\delta : \sum_{p \in \mathbb{P}} (2w_p(a_1(\delta)) - w_p(a_2(\delta)))X_p.$$

Assume that for $\delta \in L$ both

$$a_1(\delta) \text{ and } a_2(\delta)$$

are B-smooth. Then we get a relation in which the coefficient of f_p is $\neq 0$ only if q is in the factor base. To find such $\delta \in L$ we can use sieves.

Relations Arising from Quadratic Fields We are interested in cyclic extensions L of odd degree ℓ with conductor m over $\mathbb{Q}$ and generator τ of $G(L/\mathbb{Q})$. The composite of such an extension with a quadratic extension field K of $\mathbb{Q}$ has the same properties. So we can use cyclic algebras over K given by a triple $A = (L/K, \tau, c)$ with $c \in K^*$.

For places $\mathfrak{p} \in \Sigma_K$ we have numbers $f_{\mathfrak{p}}$ such that $\tau^{f_p} = \phi_{\mathfrak{p}}$.

If $p \in \mathfrak{p}$ is inert in K then $f_{\mathfrak{p}} = 2f_p$.

Else we get $f_p = f_{\mathfrak{p}}$ for $\mathfrak{p} \mid p$.

We need that the sum of the invariants of A taken over all places dividing m is zero. This is certainly the case if c is prime to m and if the norm of c is congruent to 1 modulo m. If we assume that all primes dividing m are split in K and that the class number of K is prime to ℓ we get that there is an cyclic extension cyclic of degree ℓ unramified outside of m if and only $\ell \mid \varphi(m)$. So we can use relations by cyclic algebras over K for our system of equations of the type described in Proposition 1.9.

Take odd $\epsilon \in \mathbb{N}$ and $d \in \mathbb{Z}\backslash\mathbb{Z}^2$, $\gcd(d,\epsilon) = 1$ and $d \equiv \epsilon^2 \bmod m$. We denote by K_d the field $\mathbb{Q}(\sqrt{d})$.
We take $u \in \mathbb{Z}$ with $\gcd(\epsilon d, 1-u^4) = 1$. (This implies that u is even.)
The element

$$c = \frac{1+u^2}{2u} + \frac{1-u^2}{2\epsilon u}\sqrt{d}$$

has norm

$$\frac{\epsilon^2(1+u^2)^2 - (1-u^2)^2 d}{4\epsilon^2 u^2} \equiv 1 \bmod m$$

and so we get

$$\sum_{\mathfrak{p}\in\Sigma_K} w_{\mathfrak{p}}(\epsilon(1+u^2) + (1-u^2)\sqrt{d}) f_{\mathfrak{p}} \equiv$$

$$\sum_{\mathfrak{p}\in\Sigma_K} w_{\mathfrak{p}}(2\epsilon u) f_{\mathfrak{p}} \mod \ell.$$

Straightforward calculations yield

$$\sum_{p \text{ split in } K_d} w_p(\epsilon^2(1+u^2)^2-(1-u^2)^2 d)$$

$$\equiv w_p(2\epsilon u))f_p \mod \ell.$$

Assume that both ϵu and $\epsilon^2(1+u^2)^2-(1-u^2)^2 d$ are B-smooth. Then we have found an equation of the wanted form.

3 Construction of Elements in the Brauer Group

We are looking for more methods to construct element in the Brauer group of number fields. The theoretical background for the success (or failure) is the duality theorem of Tate-Poitou.

3.1 Pairings with Dirichlet Characters

This method is due to **Huang-Raskind**. It uses the duality between $\mathbb{Z}/n$ and μ_n and leads to well known "symbols" in class field theory (cf. J.P. Serre: Corps locaux). $H^1(G_K, \mathbb{Q}/\mathbb{Z}) = Hom(G_K, \mathbb{Q}/\mathbb{Z})$ consists of Dirichlet characters of K.

We use the Kummer sequence for the multiplicative group and map K^* to $H^1(G_K, \mu_n)$ (in fact, this is the original "Kummer theory". The cup product yields a pairing

$$K^* \times Hom(G_K, \mathbb{Z}/n) \to \mathrm{Br}(K)$$

sending (a, χ) to $< a, \chi >$.
By restriction we get local pairings (local symbols) and of course there is a reciprocity law for the invariant.

We look at the Dirichlet characters as test functions to get information about discrete logarithms at various places.
Hence we are interested in finding Dirichlet characters with prescribed ramification (see discussion above). The answer to this is given by the Tate-Poitou duality theorem.
One nice application is: Let K be a real quadratic field.
Under suitable conditions one proves the existence of a Dirichlet ramified at two given places. Applying $<,>$ to a unit of K one gets relations between the discrete logarithm at the two places. For details I refer to: Ming-Deh Huang and Wayne Raskind: Signature Calculus and Discrete Logarithm Problem, ANTS 2006.

3.2 Pairings with Principal Homogenous Spaces

Of course, one can try to do analogue things with abelian varieties instead of using the multiplicative group.
Hence one uses elements in $H^1(G_K, A(K_s)$ as test functions, and of course, the pairing is the Tate-Lichtenbaum pairing.
The situation is much more rigid. The duality theorem of Tate-Poitou predicts that there are not many suitable elements and our local description tells us that we get "very sparse" relations.

Assume that we have a Jacobian variety A (e.g. an elliptic curve) over a global field K with a point $P \in A(K)$ and that we have an element

$$\varphi \in H^1(G_K, A(K_s))[n].$$

Then $T_n(P, \varphi)$ is an element in $Br(K)[n]$ which is very sparse.

At all $\mathfrak{p}$ prime to $n \cdot cond(A)$ at which φ is unramified or at which the reduction of P lies in $nA(K_{\mathfrak{p}})$ the value of the local pairing is 0. Hence

$$\sum_{\mathfrak{p} \in S} inv_{\mathfrak{p}}(T_n(P, \varphi)) = 0$$

with

$$S = \{\mathfrak{p}; \mathfrak{p} \mid n \cdot cond(\varphi) \cdot cond(A)\}$$
$$\cap \{\mathfrak{p}; P \notin nA(K_{\mathfrak{p}})\}.$$

3.3 Cassel's Pairing

One of the complications occurring when we use $\varphi \in H^1(G_K, A(K_s))[n]$ for testing is that φ becomes trivial at many places.
This has a geometric interpretation. In a canonical way φ corresponds to a principal homogeneous space V_φ attached to A which becomes isomorphic to A over any field L with $V_\varphi(L) \neq \emptyset$.
So its restriction at $\mathfrak{p}$ becomes trivial iff V_φ has a $K_\mathfrak{p}$-rational point.
In the extreme case this happens at all places. Then φ is an element of the Tate-Shafarevich group $TS(A)$.

Hopefully this group is finite. But certainly its order cannot be bounded if we vary A.
For elliptic curves Heegner points and the corresponding Kolyvagin-Euler-systems are good candidate for yielding elements in $TS(A)$.
Cassels has used the Tate-Shafarevich group to define a very interesting skew symmetric pairing which is non-degenerate iff $TS(A)$ is finite. And then the order is a square!

Cassels' pairing is really a global object. To define it one has to leave the world of Brauer groups (which are good for local duality) and go to the second cohomology of idele classes, which is isomorphic to $\mathbb{Q}/\mathbb{Z}$ again.
Ideles (and so cocycles) have entries at all places of K coming from local fields, and so as result of the pairing we find again a collection of elements in local Brauer groups. But now the sum of invariants will not be 0 in general, but we are not far away!
So, besides of the great importance of Cassels' pairing for theory it could be an interesting object for cryptography, and I refer to ongoing work done by *K. Eisentrager, D. Jetchev and K.Lauter.*