Duality in Arithmetic Geometry and Applications to Discrete Logarithms

Gerhard Frey
IEM
University of Duisburg-Essen

IPAM
October 12, 2006

Contents

1 Geometric DL-systems and Bilinear Structures

Let ℓ be a prime number and G a group of order ℓ such that

- the elements in G are presented in a compact way i.e. by $O(log(\ell))$ bits
- the group composition $\oplus$ is easy to be implemented and very fast,i.e. has complexity $O(log(\ell))$.

- the discrete logarithm problem (DL-problem) i.e.:
  for randomly chosen elements $g_1, g_2 \in G$ *compute a number* $k \in \mathbb{Z}$ *such that* $[k]g_2 = g_1$
  is hard.

1.1 Bilinear Structures

Let $(A, \circ)$ be a DL-system.

Definition 1.1 *Assume that there are $\mathbb{Z}$-modules B and C and that a bilinear map*

$$Q : A \times B \to C$$

with

- *Q is computable in polynomial time*
- *$Q(.,.)$ is non-degenerate in the first variable. Hence, for random $b \in B$ we have $Q(a_1, b) = Q(a_2, b)$ iff $a_1 = a_2$.*

We call (A, Q) a DL-system with bilinear structure.

The importance of bilinear structures for cryptology was discussed in several lectures.

Remark 1.2 *One is used to describe bilinear maps on free modules by matrices whose entries consist of the values of the form on pairs of elements in fixed bases. For instance assume that A is a cyclic group with n elements with generator P_0. Then*

$$Q : A \times A \to \mathbb{Z}/n$$

is determined by $Q(P_0, P_0)$. Without further information the computation of $Q(P, Q)$ is equivalent with DL.

From the algebraic point of view there are pairings "everywhere".
But: Because of the condition about the computational complexity it is much harder to find DL-systems with bilinear structure.

Problem 1 *Find bilinear structures!*

One possibility is to use duality theorems of Arithmetic Geometry ie. from Algebraic Geometry and Algebraic Number Theory.

2 Dualities

For abelian groups A one has the Pontryagin Duality:
$A^* := \mathrm{Hom}(A, \mathbb{R}/\mathbb{Z})$.
For finite group schemes $\mathcal{A}$ defined over a field K one has the Cartier dual, ie. a group scheme $\widehat{\mathcal{A}} := \mathrm{Hom}_K(\mathcal{A}, G_m)$.
Etale group schemes correspond to Galois modules $A = \mathcal{A}(K_s)$ of G_K, the absolute Galois group of K.
If $\mathcal{A}$ and $\widehat{\mathcal{A}}$ are étale then

$$\widehat{\mathcal{A}}(K_s) = A(K_s)^*.$$

Let J be an abelian variety.
There exists a dual abelian variety $\widehat{J}$ such that

$$J[n] := ker(n \circ id_J)$$

is the Cartier dual to $\widehat{J}[n]$.
If n is prime to char(K) then $J[n]$ and $\widehat{J}[n]$ are étale.
In general $\widehat{J}$ is isogenous to J. For simplicity we shall assume from now on that J and $\widehat{J}$ can be identified (ie. J is principally polarized.)
This is the case if J is the Jacobian of a curve.
Consequence:
$J[n]$ is self-dual.
Explicitly, the duality is given by the Weil pairing.

2.1 Local and Global fields: Class Field Theory

Over special fields we get a much finer duality theory which involves the arithmetic of K.
Assume that K is a number field (global field). Let me state one of the most beautiful theories of Mathematics in four lines .

Theorem 2.1 *For* $0 \leq i \leq 3$ *we have a perfect duality of finite groups*

$$H^i_{et}(X, F) \times Ext^{3-i}_X(F, G_m)$$
$$\rightarrow H^3_{et}(X, G_m) = \mathbb{Q}/\mathbb{Z}.$$

Here, X is the spectrum of the ring of integers of a number field, the cohomology is with respect to the étale situs, and F is a constructible sheaf (ie. there is a finite set of points in X such that the pull back of F to ... $< X - \{x_1, \ldots, x_n\}$ and to $x_1, \ldots x_n$ is a locally constant abelian sheaf),for instance, it is the sheaf related to an étale group scheme.

I cannot explain this result in detail, not to speak of proving it. A nice reference is B. Mazur: Notes on étale cohomology of number fields; Ann. sci. ENS t.6, n^o 4 (1973),p.521-552.
I shall have to restrict myself to special cases and to state consequences.

2.2 DL-systems in Class Groups: Geometry Enters

The most important source for finding G are ideal or divisor class groups attached to curves C over finite fields $\mathbb{F}_q$.

Take O, an integral domain with quotient field F.
$A \subset F$ is an O-ideal
i.e. there is an element $f \in F^*$ with fA an ideal of O.
The invertible ideals form the *ideal group* of O.
Its quotient group modulo principal invertible ideals is denoted by $\mathrm{Pic}(O)$.

Problem 2 *Find suitable rings O such that for a large prime ℓ*

- $\mathbb{Z}/\ell$ *can be embedded into* $\mathrm{Pic}(O)$
- *the elements in* $\mathrm{Pic}(O)$ *can be described in a compact way*
- *the composition in the ideal class group has complexity* $O(\log(\ell))$.

2.3 Ideal Classes of Rings of Functions

We study one type of rings:
O the ring of holomorphic functions
of an (affine) curve C_O defined over a finite field $\mathbb{F}_q$ with q elements.
In general we allow **singularities** (leads to tori) as well as "missing points" **(localizations)**.
We assume that C_O has only one singular point P_{sing} and that its conductor is squarefree.
(Higher powers of prime ideals in the conductor change the ideal class group by unipotent groups and different singular points can be treated separately.)

To see the geometric picture better we extend scalars and interpret C_O as curve defined over $\overline{\mathbb{F}_q}$ with corresponding ring of holomorphic functions $\overline{O}$.
The Galois group of $\mathbb{F}_q$ acts on functions, ideals and ideal classes in a natural way.
We have the exact sequences of Galois modules

$$1 \to Princ_{\overline{O}} \to I(\overline{O}) \to \mathrm{Pic}(\overline{O}) \to 0$$

.

By the theory of Generalized Jacobians and using the Approximation Theorem we relate the Picard groups of such rings to the divisor class groups of the projective non singular curve C attached to C_O and so to the points of the Jacobian variety J_C of C.

Theorem 2.2 *We have the exact sequences of G_K-modules*

$$1 \to Princ_{\overline{O}} \to I_{\overline{O}} \to \mathrm{Pic}_{\overline{O}} \to 0$$

$$1 \to \mathcal{T}_S(K_s) \to \mathrm{Pic}(\overline{O}) \to \mathrm{Pic}(\overline{\widetilde{O}}) \to 0$$

and

$$0 \to \mathcal{C}_{T_\infty} \to J_C(K_s) \to \mathrm{Pic}(\overline{\widetilde{O}}) \to 0.$$

where $\mathcal{T}_S$ is a torus of dimension $\mid S \mid -1$ and $\mathcal{C}_T$ is the ideal class group with support in $T_\infty \setminus P_\infty$.

The isomorphism class of $\mathcal{T}_S$ is determined by its character group X, and this group is determined by the first homology group of the dual graph of C_O (Grothendieck) (with G_K-action). So Theorem 2.2 (applied to $K = \mathbb{F}_q$) gives a tool to realize discrete logarithms in subgroups of multiplicative groups of extension fields of $\mathbb{F}_q$ as subgroups of ideal class groups of rings of holomorphic functions of affine curves.

Problem 3 *Can this be made explicit for existing systems?*
And: Is security concerned (key word Weil descent)?

2.4 Pairings in Cohomology

Let A and B be two $G-$modules, where G is a profinite group (eg. $G = G_K$). The tensor product (over $\mathbb{Z}$)

$$A \bigotimes B$$

becomes, in a natural way, a G-module. We have a natural (and functorial) homomorphism $\cup^{0,0}$
from $A^G \bigotimes B^G$ to $(A \bigotimes B)^G$.
Fact: $\cup^{0,0}$ induces a unique family of homomorphisms, *the cup product*,

$$\cup^{p,q} : H^p(G, A) \times H^q(G, B)$$

$$\rightarrow H^{p+q}(G, A \bigotimes B)$$

with functorial properties with respect to cohomology functors.

Assume that there is a G-pairing

$$Q : A \times B \to C.$$

Q defines a G-homomorphism ϕ_Q from $A \bigotimes B$ to C by sending $a \otimes b$ to $Q(a, b)$. Hence we get a bilinear pairing

$$Q^{p,q} = \phi_Q^{(p+q)} \circ \cup^{p,q}.$$

Example 2.3 *The evaluation pairing induces a pairing*

$$E^{p,q} : H^p(G_K, A) \times H^q(G_K, \widehat{A}) \to H^{p+q}(G_K, K_s^*).$$

If $A = \mathcal{A}(K_s)$ we can interpret this as a pairing between étale cohomology groups:

$$\mathcal{E}^{p,q} : H^p_{et}(Spec(K), \mathcal{A}) \times H^q_{et}(Spec(K), \widehat{\mathcal{A}}) \to H^{p+q}_{et}(Spec(K), G_m).$$

2.4.1 The Tate Pairing

Let J be an abelian variety (principally polarized for simplicity). We have the long exact sequence

$$0 \to J(K)/nJ(K) \xrightarrow{\delta^0}$$

$$H^1(G_K, J[n](K_s)) \to H^1(G_K, J(K_s))[n] \to 0$$

yielding

$$E^{1,1} : H^1(G_K, J[n](K_s)) \times H^1(G_K, J[n](K_s)) \to H^2(G_K, K_s^*).$$

Fact: $J(K)/nJ(K)$ is isotrop w.r.t $E^{1,1}$ and so $E^{1,1}$ induces the Tate-pairing

$$T_n : J(K)/n \cdot J(K) \times H^1(G_K, J(K_s))[n] \to H^2(G_K, K_s^*).$$

2.4.2 The Lichtenbaum Pairing

O resp. $\overline{O}$ are defined as above but associated to curves over arbitrary K.
Assume first that C_O regular and
$C \setminus C_O = \{P_\infty\}$.
From

$$1 \to (\overline{F}) \to I(\overline{O}) \to \mathrm{Pic}(\overline{O}) \to 0$$

we get

$$0 = H^1(G_K, I(\overline{O})) \to H^1(G_K, \mathrm{Pic}(\overline{O})) \xrightarrow{\delta^1} H^2(G_K, (\overline{F})).$$

Explicit description:
Take $c \in H^1(G_K, \mathrm{Pic}(\overline{O}))$ and represent it by a cocycle

$$\zeta : G_K \to \mathrm{Pic}(\overline{O}) \text{ with } \zeta(\sigma) = \bar{D}(\sigma)$$

$$D(\sigma) \in \bar{D}(\sigma) \in Pic(\overline{O}).$$

The ideal

$$A(\sigma_1, \sigma_2) = \sigma_1 D(\sigma_2) \cdot D(\sigma_1) \cdot D(\sigma_1 \cdot \sigma_2)^{-1}$$

is a principal ideal $(f(\sigma_1, \sigma_2))$ and $\delta^1(c)$ is the cohomology class of the $2-cocycle$

$$\gamma : (\sigma_1, \sigma_2) \mapsto (f(\sigma_1, \sigma_2)).$$

We have some choices.
As result we can assume that the function $f(\sigma_1, \sigma_2)$ has neither zeros nor poles in finitely many given points $P \in C$.

Definition 2.4 *The* Lichtenbaum pairing
$T_L : \mathrm{Pic}(O) \times H^1(G_K, \mathrm{Pic}(\overline{O})) \to H^2(G_K, K_s^*)$
is defined in the following way:
Choose $A := \prod_{P \in C_O} m_P^{z_P} \in \bar{D} \in \mathrm{Pic}(O)$ *of degree* 0 *and*
$c \in H^1(G_K, \mathrm{Pic}(\overline{O}))$ *such that* $\delta^1(c)$ *is presented by a cocycle* $(f(\sigma_1, \sigma_2))$ *prime to* A.
Then $T_L(\bar{D}, c)$ *is the cohomology class of the cocycle*

$$\zeta(\sigma_1, \sigma_2) = \prod_{P \in C \setminus P_\infty} f(\sigma_1, \sigma_2)(P)^{z_P}$$

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

Overcoming some technical problems one gets in the general case, too:
$T_L : \mathrm{Pic}(O) \times H^1(G_K, Pic(\overline{O}) \to H^2(G_K, K_s^*)$

3 Local Pairings

Note that both the Tate pairing and the Lichtenbaum pairing are defined over arbitrary fields. But they become useful only over fields with "strong" arithmetic.
A first candidate, from the point of view of cryptology, would be:

$$K = \mathbb{F}_q.$$

But, alas, the pairings are trivial. We have to replace finite fields by **local fields** K with residue field $\mathbb{F}_q$, maximal ideal $m_{\mathfrak{p}}$ and normalized valuation $w_{\mathfrak{p}}$.

3.1 Local Galois Theory

The maximal unramified extension of K is denoted by K_{unr}.
There is a canonical lift of ϕ_q to K_{unr} also called the Frobenius automorphism and denoted by ϕ_q.
Let π be an *uniformizing* element of K.
$L_n = K_{unr}(\pi^{1/n})$
is the unique ramified extension of K_{unr} cyclic of degree n.

Assume that $n \mid (q-1)$.
Then $K(\pi^{1/n})$ is Galois over K and the, up to twist with the unramified extension of degree n, unique totally tamely ramified extension of K of degree n.

3.2 Lifting of curves

O is the ring of holomorphic functions of an affine curve C_O defined over $\mathbb{F}_q$ with corresponding projective curve C of genus g_0. We assumed that C_O has only one singular point with squarefree conductor, and that a set T_∞ of points is "missing" on C_O.
We can lift C_O to an affine non-singular curve C_O^l defined over K embedded in the projective curve C^l which is a lift of C such that all relevant data are preserved.

In particular

$$\mathrm{Pic}(O^l)/[n]\mathrm{Pic}(O^l)$$

is canonically isomorphic to $\mathrm{Pic}(O)/[n]\mathrm{Pic}(O)$. and there exists a torus $\mathcal{T}/K$ of dimension
$\mid S \mid -1$ and an exact sequence

$$1 \to \mathcal{T}(U_K)/(\mathcal{T}(U_K))^n \to$$

$$\mathrm{Pic}(O^l)/[n]\mathrm{Pic}(O^l) \to \mathrm{Pic}(\tilde{O})/[n]\mathrm{Pic}(\tilde{O}) \to 0$$

with U_K the units of K.

Instead of a proof I give an example.

Example 3.1

$$C_O : Y^2 + XY = X^3$$

defined over $\mathbb{F}_q$ $T_\infty = \{(0,1,0)\}$, *the singular point* $(0,0)$ *corresponds to* 2 *points on the desingularization and* $\mathrm{Pic}(O) \cong \mathbb{F}_q^*$.
$K = \mathcal{W}(\mathbb{F}_q)$ *and* $w_{\mathfrak{p}}(\pi) = 1$.
Then

$$C^l := E : Y^2 + XY = X^3 + \pi$$

is a Tate elliptic curve with

$$E(K) \cong K^*/ < Q_E > \cong U_K.$$

3.3 Theorem of Tate-Lichtenbaum, and We Are Back in Number Theory

Let K be a local field, C_O an affine regular curve over K with ring of holomorphic functions O.

Theorem 3.2 ***(Tate, Lichtenbaum)*** *For every natural number n the pairing*

$$T_n : \mathrm{Pic}(O)/n\mathrm{Pic}(O) \times H^1(G_K, Pic(\overline{O}))[n] \rightarrow H^2(G_K, K_s^*)[n]$$

(with T_n induced by the Lichtenbaum pairing T_L)
is not degenerate.

Hence one can suspect that we get a bilinear structure in the cryptological sense.

Problem 4 *Can the pairing T_n be computed fast?*
And is $H^2(G_K, K_s^*)$ a group in the computational sense?

The answer is yes, if we assume that C is the lift of a curve C_0 which has no singularities (good reduction) In addition we need, at least at present,that K contains the n-th roots of unity , or equivalently

$$n \mid (q-1).$$

Assume that $n \mid (q-1)$. First Pic can be replaced by points on the Jacobian J_C.
$H^1(G_K, J_C(K_s))[n]$ is isomorphic to $\mathrm{Hom}(G_{L_n/K}, J_C(K)[n])$ where L_n is "the" ramified extension of degree n.
Take a generator τ of $G(L_n/K)$ and

$$\varphi(\tau) = P;\ P \in J_C(K)[n].$$

Let $nP = (f_P)$ and assume a representative of $Q \in J_C(K)$ is chosen such that $f_P(Q)$ is defined.
Then

$$T_n(P, Q)$$

is the class of of the cocycle

$$\zeta(\tau^i, \tau^j) = f_P(Q) \text{ for } i + j \geq n$$

and

$$\zeta(\tau^i, \tau^j) = 1 \text{ else.}$$

Moreover, we can change $f_P(Q)$ by a factor in N_{L/K_n} and use that $K_n^*/N_{L/K_n} \cong \mathbb{F}_q^*/(\mathbb{F}_q^*)^n$.
Hence we get a pairing

$$T_{n,0} : J_C(K) \times J_C(K_s)[n] \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^n$$

which is non-degenerate on the right side and has radical $nJ_C(K)$ on the left side.

Let k be the minimal number such that $n \mid q^k - 1$.
The number k is called the embedding degree. Using the result from above we get a pairing

$$T_{n,0} : J_C(K) \times J_C(K_s)[n][\chi_q] \to \mathbb{F}_{q^k}^* / (\mathbb{F}_{q^k}^*)^n$$

which is non-degenerate on the right side and has radical $nJ_C(K)$ on the left side.
Here $J_C(K_s)[n][\chi_q]$ is the subspace of $J_C(K_s)[n]$ on which ϕ_q acts by multiplication with q.

Using reduction we get

The discrete logarithm in ideal classes of rings of holomorphic functions of affine curves C over finite fields $\mathbb{F}_q$ is transferred to $H^2(G_K, K_s^*)$ with K a local field with residue field $\mathbb{F}_q$. .
If k is the embedding degree for n over $\mathbb{F}_q$ it is transferred to the discrete logarithm in $\mathbb{F}_{q^k}$.

It is annoying that we have to go through $\mathbb{F}_q(\zeta_n)$ to get an explicit description of the image of the Tate-Lichtenbaum pairing.
The direct output is a cocycle split by a generalized dihedral extension field of K.
We know that its restriction to the Galois group of an extension (non-Galois) of degree n becomes trivial.
By the local duality theorem (see next section) we know that it is equivalent to a cocycle c_u split by an unramified cyclic extension of of degree n of $\mathbb{F}_q$.

Problem 5 *Can one describe c_u?*

3.4 Invariants of Elements in $Br(K)$

Let K be a field.

Definition 3.3 *The Brauer group of K is the cohomology group*

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

It is denoted by

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

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 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

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

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.

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

Now let K be a local field.

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 $c \in$ 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 3.4 *Let* $c \in H^2(G(L_u/K), L_u^*)$ *be given by the triple* (L_u, ϕ_q, a).
Then $w_{\mathfrak{p}}(a) \in \mathbb{Z}/n\mathbb{Z}$ *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 3.5 *Assume that* τ *is another generator of* $G(L_u/K)$ *and* c *is given by the triple* (L_u, τ, a). *Let* $f_{\mathfrak{p}} \in \mathbb{Z}$ *be such that* $\tau^{f_{\mathfrak{p}}} = \phi_q$.
Then $\mathrm{inv(c)} = \mathrm{f_{\mathfrak{p}}} \cdot \mathrm{w_{\mathfrak{p}}(a)} \bmod \mathrm{n}$.

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

Example 3.6 *Assume that* $L_u = K(\alpha)$ *with* $\alpha \in U(K)$ *such that* $\tau(\alpha) = \beta \cdot \alpha$ *with* $\beta \in K$.
Then $\tau^{f_\mathfrak{p}} = \phi_q$ *if and only if* $\beta^{f_\mathfrak{p}} \equiv \alpha^{q-1}$ *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 Br(K)[n] is cyclic. Hence every representant of $c \in$ 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) the invariant of this representant and we get an isomorphism

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

The discrete logarithm in Br(K)[n] would be trivial if we could compute invariants.
BUT:
The discrete logarithm in Br(K)[n] even for cyclic algebras is equivalent with computing the discrete logarithm in $\mathbb{F}_q$.

The application of the Tate-Lichtenbaum pairing leads to cyclic algebras split by dihedral extensions composed by an unramified extension and a ramified extension of degree n.
We can reformulate **Problem 5** to

Problem 6 *Can one compute the invariants of algebras over local fields split by dihedral extensions "fast"?*

4 Globalisation

4.1 The Fundamental Theorems

We need more information and we get it by going from local fields to global fields.

Let 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 $\mathbb{F}_q$.

Let $\mathfrak{p}$ be a non-archimedean place of K with normalized valuation $w_{\mathfrak{p}}$.
Let $K_{\mathfrak{p}}$ be the completion of K with respect to $\mathfrak{p}$.

Its Galois group $G_{\mathfrak{p}}$ can be identified with a subgroup of G_K, namely the decomposition group of an extension $\tilde{\mathfrak{p}}$ of $\mathfrak{p}$ to K_s.
Restrictions maps to $G_{\mathfrak{p}}$ are denoted by $\rho_{\mathfrak{p}}$.
Let Σ_K be the set of all places of K.
Let A be a G_K-module and

$$f_n(A) : H^n(G_K, A) \stackrel{\prod \rho_{\mathfrak{p}}}{\longrightarrow} \prod_{\mathfrak{p} \in \Sigma_K} H^n(G_{K_{\mathfrak{p}}}, A).$$

The key questions are: Describe the kernel and the cokernel of f_n!

Assume that A is finite.

- The kernel of $f_1(A)$ is compact and dual to the kernel of $f_2(\widetilde{A})$. In particular, the kernel of $f_2(A)$ is finite.
- **Tate-Poitou**:We have an exact 9-term sequence

$$0 \to A^{G_K} \to \prod H^0(K_{\mathfrak{p}}, A) \to H^2(K, \widehat{A})^* \to H^1(K, A)$$

$$\to \prod{}' H^1(K_{\mathfrak{p}}, A) \to H^1(K, \widehat{A})^* \to H^2(K, A)$$

$$\to \sum H^2(K_{\mathfrak{p}}, A) \to H^0(K, \widehat{A})^* \to 0.$$

(Here G_K is replaced by K, and $\prod'$ is the restricted product with respect to the unramified cohomology.)

Sequence of **Hasse-Brauer-Noether**:

For $c \in \mathrm{Br(K)}$ define $\mathrm{inv}_{\mathfrak{p}}(\mathrm{c}) := \mathrm{inv}(\rho_{\mathfrak{p}}(\mathrm{c}))$.

Then the sequence

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

is exact.

4.2 Globalization of Algebras

Here is the main problem:

Problem 7 *Given an (finite) set S of places of K, and for each $\mathfrak{p} \in S$ an element $c_{\mathfrak{p}} \in \mathrm{Br}(\mathrm{K}_{\mathfrak{p}})[\mathrm{n}]$ represented by an algebra $A_{\mathfrak{p}}$.*
Can we find in an explicit way one (many) element(s) $c \in \mathrm{Br}(\mathrm{K})$ resp. algebras A with center K such that for all $\mathfrak{p} \in S$ we have

$$\mathrm{inv}_{\mathfrak{p}}(\mathrm{c}) = \mathrm{inv}(\mathrm{c}_{\mathfrak{p}})$$

resp

$$A \bigotimes K_{\mathfrak{p}} \sim A_{\mathfrak{p}}.$$

Especially interesting: the local splitting fields are dihedral extensions.

4.3 The Cyclic Case

We go back to the cyclic case.
Let $\mathfrak{m}$ be an ideal ($\mathfrak{m} = O_K$ allowed) in O_K, the ring of integers of K. We assume that there is a cyclic extension L of odd degree n of K which is unramified outside of $\mathfrak{m}$.
Let τ be a generator of $G(L/K)$. For $\mathfrak{p}$ prime to $\mathfrak{m}$ let $\phi_{\mathfrak{p}}$ be a Frobenius automorphism at $\mathfrak{p}$ in $G(L/K)$. By $f_{\mathfrak{p}}$ we denote a number for which $\tau^{f_{\mathfrak{p}}} = \phi_{\mathfrak{p}}$ holds.

Proposition 4.1 *For all elements* $a \in K^*$ *we have*

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

where $w_{\mathfrak{p}}$ *is the normalized valuation in* $\mathfrak{p}$ *and* A *is the cyclic algebra* (L, τ, a).

4.4 Applications

If we can compute (enough of) the numbers $f_{\mathfrak{p}}$ we can compute

- the order of the ideal class group of the order in K with conductor $\mathfrak{m}$, in particular Euler's totient function $\varphi(m)$
- the discrete logarithm in $\mathbb{F}_q^*$

and

- get a very subtle descriptions of of cyclic extensions of K

4.5 Index-Calculus in Global Brauer Groups

We 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 $\mathfrak{m}$.
A possible method to do this (with subexponential complexity) is an index-calculus algorithm of the type one is used to see in algorithms factoring numbers.

4.6 Example: $K = \mathbb{Q}$

Take $K = \mathbb{Q}$. The congruence in Proposition 4.1 can be seen as solution of a system of linear equations relating the variables f_p for p prime to m and $\mathrm{inv_p(A)}$ for $p \mid m$.
We want to use numbers a with $w_q(a) \neq 0$ only for $q < B$, ie. a is B-smooth. Let d be the smallest number $\geq \sqrt{m}$. For small δ take $a_1(\delta) := d+\delta$, $a_2(\delta) := c_0 + 2\delta \cdot d + \delta^2$ with $c_0 = d^2 - m$.

$$L_\delta : \sum_{p \in \mathbb{P}} (2w_p(a_1(\delta)) - w_p(a_2(\delta)))X_p = 0.$$

Now look for $\delta \in L$ (using sieves) such that both $a_1(\delta)$ and $a_2(\delta)$ are B-smooth for convenient B.

Assume that we have found a system $\mathcal{L}$ of n $\mathbb{Z}$-independent equations and with n of the primes p occurring.

Proposition 4.2 *$det(\mathcal{L})$ is a multiple of $\varphi(m)$.*

4.7 Construction of Elements in the Brauer Group

Motivated by index-calculus and for theoretical reasons, too, 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. We can try to use

- Pairings with Dirichlet Characters (**Huang-Raskind**)
- Pairings with Principal Homogenous Spaces with abelian varieties instead of using the multiplicative group (much more rigid)
- Cassel's Pairing using Tate-Shafarevich groups and ending in the second cohomology group of the idele class group which is the right global object instead of the Brauer group.

More details and problems are given in the lectures of Wayne Raskind, Ming-Deh Huang and Kirsten Eisentraeger!

Main Problem:

Motivate people from Computational Number Theory to look at Brauer groups as interesting arithmetical objects.