ANNALES MATHÉMATIQUES

BLAISE PASCAL

Gerhard Frey

On Bilinear Structures on Divisor Class Groups

Volume 16, n° 1 (2009), p. 1-26.

<http://ambp.cedram.org/item?id=AMBP_2009__16_1_1_0>

Publication éditée par le laboratoire de mathématiques
de l'université Blaise-Pascal, UMR 6620 du CNRS
Clermont-Ferrand — France

Annales mathématiques Blaise Pascal **16**, 1-26 (2009)

On Bilinear Structures on Divisor Class Groups

Gerhard Frey

Abstract

It is well known that duality theorems are of utmost importance for the arithmetic of local and global fields and that Brauer groups appear in this context unavoidably. The key word here is class field theory.

In this paper we want to make evident that these topics play an important role in public key cryptopgraphy, too. Here the key words are Discrete Logarithm systems with bilinear structures.

Almost all public key crypto systems used today based on discrete logarithms use the ideal class groups of rings of holomorphic functions of affine curves over finite fields $\mathbf{F}_q$ to generate the underlying groups. We explain in full generality how these groups can be mapped to Brauer groups of local fields via the Lichtenbaum-Tate pairing, and we give an explicit description.

Next we discuss under which conditions this pairing can be computed efficiently.

If so, the discrete logarithm is transferred to the discrete logarithm in local Brauer groups and hence to computing invariants of cyclic algebras. We shall explain how this leads us in a natural way to the computation of discrete logarithms in finite fields.

To end we give an outlook to a globalisation using the Hasse-Brauer-Noether sequence and the duality theorem ot Tate-Poitou which allows to apply index-calculus methods resulting in subexponential algorithms for the computation of discrete logarithms in finite fields as well as for the computation of the Euler totient function (so we have an immediate application to the RSA-problem), and, as application to number theory, a computational method to "describe" cyclic extensions of number fields with restricted ramification.

This report is based on a lecture given at the conference **Algèbre, Théorie des Nombres et leurs Applications, Université Mohammed I, Oujda**, at May 11, 2006. The author would like to thank the organizers for their support and the overwhelming hospitality which made the conference to an unforgettable experience.

Keywords: Discrete Logarithms, pairings, Brauer groups, Index-Calculus .

Math. classification: 11R65, 11R37, 11G20.

1. DL-systems and Bilinear Structures

1.1. DL-systems

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

- **i):** the elements in A are presented in a compact way, for instance by $O(log(\ell))$ bits,
- **ii):** it is easy to implement the group composition $\circ$ such that it is very fast, for instance has complexity $O(log(\ell))$, but
- **iii):** to compute, for randomly chosen elements $g_1, g_2 \in A$, a number $k \in \mathbf{Z}$ such that $g_2^k = g_1$ (the discrete logarithm problem (DL-problem)) is hard.

In the ideal case this complexity were $exp(O(\log(\ell)))$. This is obtained in black box groups, and, as we hope, in certain groups related to elliptic curves and abelian varieties.

In many cases one gets a weaker result: The complexity is subexponential, and this forces to take the parameters larger to get security.

Typical examples are systems related to the multiplicative group of quotients of rings of integers ("classical" DL).

A group $(A, \circ)$ satisfying conditions i),ii) and iii) is called a *DL*-system.

1.2. Bilinear Structures

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

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

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

with

- **i):** the group composition laws in A, B and C as well as the map Q can be computed rapidly (e.g. in polynomial time).
- **ii):** $Q(.,.)$ is non-degenerate in the first variable. Hence, for random $b \in B$ we have $Q(a_1, b) = Q(a_2, b)$ iff $a_1 = a_2$.

Then we call (A, Q) a *DL-system with bilinear structure.*

Remark 1.2. One is used to describe bilinear maps on free modules by matrices whose entries consist of the values of pairs of elements in fixed bases. This is not enough for our purposes.

For instance assume that $A = B$ is a cyclic group with n elements with generator P_0 and take $C = \mathbf{Z}/n$.

Choose $m \in \mathbf{Z}$ prime to n. Let

$$Q_m : A \times A \to \mathbf{Z}/n$$

be the pairing determined by $Q_m(P_0, P_0) := m + n\mathbf{Z}$.

Without further information the computation of $Q_m(P, Q)$ is equivalent with the Discrete Logarithm in A. So, though from the algebraic point of view pairings are "everywhere" it is much harder to find DL-systems with bilinear structure. One source is delivered by duality theorems in Arithmetic Geometry.

1.3. Some applications of bilinear structures

There are destructive aspects which may weaken DL-systems if they carry a bilinear structure.

Here is one.

: The DL-system $(A, \circ)$ is at most as secure as the discrete logarithm in $(C, \circ)$ [6].

And there are constructive aspects, for instance

: Tripartite Key Exchange [13],

: Identity Based Protocols [4], and

: Short Signatures [5].

For more information the interested reader is advised to visit *Paulo Barretos Pairing Based Crypto Lounge.*

2. Discrete Logarithms in class groups

Let O be an integral domain with quotient field F.

The group of invertible ideals of O is denoted by $I(O)$. Principal ideals are invertible ideals of the form $f \cdot O =: (f)$ with $f \in F^*$. They form a subgroup Princ(O) of $I(O)$.

The quotient group $I(O)$/Princ(O) is denoted by Pic(O).

2.1. Ideal classes of function rings

In the following we take for O the ring of holomorphic functions of an affine curve C_O defined over a field K.

We allow singularities of a restricted type interesting for cryptological applications:

We assume that there is only one singular point and that the conductor ideal $\mathfrak{m}$ of this point is square free.

Let $\widetilde{O}$ denote the ring of holomorphic functions on the desingularisation $\widetilde{C}$ of C_O.

Let C be the projective irreducible regular curve with affine part $\widetilde{C}$.

We extend scalars and interpret C_O as well as $\widetilde{C}$ and C as curves defined over the separable closure K_s of K with corresponding ring of holomorphic functions. [1]

We denote by T_∞ the set $C(K_s) \setminus \widetilde{C}(K_s)$ and we assume that there is an K-rational point P_∞ in T_∞.

By S we denote the set of points in $\widetilde{C}$ which correspond to the singular point on C_O.

The absolute Galois group $G_K := Aut_K(K_s)$ of K acts on the points of C_O, $\widetilde{C}$ and C as well as on T_∞ and S and on functions, ideals and ideal classes in a natural way.

By the theory of Generalized Jacobians and using the Approximation Theorem we relate the ideal class groups of the rings of functions to the points of the Jacobian variety J_C of C by the following exact sequences of Galois modules.

Theorem 2.1. *We have the exact sequences of Galois modules*

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

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

and

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

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 $T_\infty \setminus P_\infty$.

For more details see [19] and [21].

[1] In the following $\bar{\ }$ always indicates that we are extending scalars to K_s.

3. **The Lichtenbaum pairing**

The sequences in Theorem 2.1 are exact G_K-module sequences and so we can apply Galois cohomology.[2]

3.1. **The regular "complete" case**

Assume first that C_O is regular and $T_\infty = \{P_\infty\}$.

From

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

we get the exact sequence

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

The map δ^1 can be given explicitly.

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

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

and choose

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

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 3.1. The *Lichtenbaum pairing*([14])

$$T_L : \mathrm{Pic}(O) \times H^1(G_K, \mathrm{Pic}(\overline{O})) \to H^2(G_K, K_s^*)$$

is defined in the following way:

Choose $D := \prod_{P \in C_O(K_s)} m_P^{z_P} \in \bar{D} \in \mathrm{Pic}(O)$ of degree 0 and the element $c \in H^1(G_K, \mathrm{Pic}(\overline{O}))$ such that $\delta^1(c)$ is presented by a cocycle $(f(\sigma_1, \sigma_2))$ prime to D.

[2] We shall need only very elementary facts from Galois cohomology. For definitions and properties we refer to [20] or [7], Appendix.

Then $T_L(\bar{D}, c)$ is the cohomology class of the cocycle

$$\zeta(\sigma_1, \sigma_2) = \prod_{P \in C_O(K_s)} f(\sigma_1, \sigma_2)(P)^{z_P}$$

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

Since $\mathrm{Pic}(\overline{O})$ is, as Galois module, isomorphic to $J_C(K_s)$ with J_C the Jacobian variety of C, we get the pairing

$$T_L : J_C(K) \times H^1(G_K, J_C(K_s)) \to H^2(G_K, K_s^*).$$

Example 3.2. Let L by a cyclic extension of K of degree n and let τ be a generator of $G(L/K)$. We denote by $\mathrm{Pic}(O_L)$ the ideal class group of the ring of holomorphic functions on $C \times L$, the curve obtained from C by base extension from K to L.

Let ζ be a 1-cocycle from $< \tau >$ into $\mathrm{Pic}(O_L)$ representing the cohomology class $z \in H^1(G(L/K), \mathrm{Pic}(O_L))$.

The cocycle condition implies that $\zeta(\tau^j) = \sum_{i=0}^{j-1} \tau^i c$ for $1 \leq j \leq n$ with $\zeta(\tau) = c$. Hence

$$Trace_{L/K}(c) = 0.$$

In other words: we can identify 1-cocycles from $G(L/K)$ to $\mathrm{Pic}(O_L)$ with elements $c \in \mathrm{Pic}(O_L)$ whose trace is equal to 0.

Now choose an ideal $D \in c$ and $D(\tau^j) := \sum_{i=0}^{j-1} \tau^i D$. Then

$$Trace_{L/K}(D) = (f_D) \text{ with } f_D \in F.$$

Hence $\delta^1(c)$ is presented by the cocycle

$$f(\tau^i, \tau^j) = 1 \text{ for } i + j < n$$

and

$$f(\tau^i, \tau^j) = (f_D) \text{ for } i + j \geq n.$$

Next choose in the ideal class $a \in \mathrm{Pic}(O)$ an ideal $A \in I(O)$ with $A = \prod_{P \in C_O(K_s)} m_P^{z_P}$ prime to the set of zeroes and poles of f_D and of degree 0, ie. $\sum z_P = 0$.

Then $T_L(a, z) \in H^2(G(L/K), L^*)$ is presented by the cocycle

$$\eta(\tau^i, \tau^j) = 1 \text{ for } i + j < n$$

and

$$\eta(\tau^i, \tau^j) = \prod_{P \in C_O(K_s)} f_D(P)^{z_P} \in K^* \text{ for } i + j \geq n.$$

This is a cocycle defining a cyclic algebra with center K and splitting field L, see Example 5.8.

3.1.1. The Lichtenbaum-Tate pairing

Take $n \in \mathbf{N}$ prime to $\mathrm{char}(K)$. By using the Kummer sequence

$$0 \to J_C[n](K_s) \to J_C(K_s) \xrightarrow{n} J_C(K_s) \to 0$$

the Lichtenbaum pairing induces the "Lichtenbaum pairing modulo n"

$$T_{L,n} : J_C(K)/nJ_C(K) \times H^1(G_K, J_C(K_s))[n] \to H^2(G_K, K_s^*)[n].$$

The Tate pairing [22]**.** Let $\mathcal{A}$ be an abelian variety with dual abelian variety $\widehat{\mathcal{A}}$ [17].

Then $\mathcal{A}[n]$, the kernel of $n \circ id_{\mathcal{A}}$, is dual to $\widehat{\mathcal{A}}[n]$, and the pairing is made explicit by the Weil pairing w_n.

The cup product composed with w_n induces a pairing

$$w_n^1 : H^1(G_K, \mathcal{A}[n](K_s)) \times H^1(G_K, \widehat{\mathcal{A}}[n](K_s)) \to H^2(G_K, K_s^*).$$

Using the Kummer sequence for $\mathcal{A}$

$$0 \to \mathcal{A}(K)/n\mathcal{A}(K) \xrightarrow{\delta^0} H^1(G_K, \mathcal{A}[n](K_s)) \to H^1(G_K, \mathcal{A}(K_s))[n] \to 0$$

and the corresponding one for $\widehat{\mathcal{A}}$ one maps $\mathcal{A}(K)$ and $\widehat{\mathcal{A}}(K)$ to the group $H^1(G_K, \mathcal{A}[n])$ resp. $H^1(G_K, \widehat{\mathcal{A}}[n])$.

Fact:
$\delta^0(\mathcal{A}(K))$ is orthogonal with respect to w_n^1 to $\delta^0(\widehat{\mathcal{A}}(K))$.

Hence w_n^1 induces the *Tate pairing*

$$T_n : \mathcal{A}(K)/n \cdot \mathcal{A}(K) \times H^1(G_K, \widehat{\mathcal{A}}(K_s))[n] \to H^2(G_K, K_s^*).$$

Theorem 3.3. ***(Lichtenbaum)***[14]

For Jacobian varieties the pairing $T_{L,n}$ is up to a sign equal to the Tate pairing T_n.

The pairing $T_{L,n}$ is called the *Lichtenbaum-Tate pairing.*

3.2. **The regular affine case**

A first application of Theorem 3.3 is the definition of the Lichtenbaum-Tate pairing pairing when T_∞ contains more than one element.

We want to define a pairing for $\mathrm{Pic}(O)$ with $H^1(G_K, \mathrm{Pic}(\overline{O}))$ which generalizes the pairing $T_{L,n}$ defined for the complete case.

Using the sequence

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

we map, as above, $H^1(G_K, \mathrm{Pic}(\overline{O}))$ to

$$\delta^1(H^1(G_K, \mathrm{Pic}(\overline{O}))) \subset H^2(G_K, \mathrm{Princ}(\overline{\mathrm{O}}))\,.$$

But the map from $\bar{F}$ to $\mathrm{Princ}(\overline{\mathrm{O}})$ has as kernel the group of functions U_{T_∞} which have no poles and zeroes outside of T_∞. Hence the evaluation of elements of the image of δ^1 at points on $C \setminus T_\infty$ is not well defined.

On the other side $H^0(G_K, \mathrm{Pic}(\overline{O}))$ is, in general, not equal to $\mathrm{Pic}(O) = \varphi(\mathrm{Pic}(O_{P_\infty}))$, and we can use the exact sequence

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

For simplicity we assume that $\mathcal{C}_{T_\infty}$ is finite.(This is the interesting case for cryptography and the general case can be treated, too.)

We apply an isogeny ψ to J_C with $\mathcal{C}_{T_\infty} = \mathit{kernel}(\psi)$. By doing this we leave the world of Jacobian varieties. We achieve that $\mathrm{Pic}(\overline{O})$ is as G_K-module isomorphic to the K_s-rational points of an abelian variety. Using Theorem 3.3 we switch to the Tate pairing. In addition we have to use the functoriality of the Weil pairing with respect to isogenies. Finally we get

Proposition 3.4. *For natural numbers prime to char(K) the Tate-Lichtenbaum pairing induces a pairing $T_{L,n}$ with*

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

3.3. **The singular case**

To make things not too complicated we assume that $T_\infty = \{P_\infty\}$. We recall the exact sequence

$$1 \to \mathcal{T}_S(K_s) \to \mathrm{Pic}(\overline{O}) \to \mathrm{Pic}(\overline{O}_{P_\infty}) \to 0.$$

Here $\mathcal{T}_S$ is a torus determined by the conductor $\sum_{P\in S} m_P$ and $\mathrm{Pic}(\overline{O}_{P_\infty}) = J_C(K_s)$.

From this sequence we get the exact sequence

$$1 \to \mathcal{T}_S(K) \to \mathrm{Pic}(O) \to J_C(K_s) \to H^1(G_K, \mathcal{T}_S(K_s))$$

and since $H^1(G_K, \mathcal{T}_S(K_s)) = 0$ by Hilbert's theorem 90 we have the exact sequence

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

as well as

$$0 \to H^1(G_K, \mathrm{Pic}(\overline{O})) \to H^1(G_K, J_C(K_s)).$$

We can restrict the boundary map δ^1 to $H^1(G_K, \mathrm{Pic}(\overline{O}))$ and we get a pairing as above but we cannot expect to get any information about $\mathcal{T}_S(K)$.

3.4. Conclusion

Let O be the ring of holomorphic functions of an affine curve C_O defined over K.

Theorem 3.5. *For all n prime to char(K) we have defined the Tate-Lichtenbaum pairing*

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

Hence one can suspect that DL-systems based on divisor class groups of rings of holomorphic functions on curves over finite fields are endowed with a bilinear structure. (Note that in this case $\mathrm{Pic}(O)$ is finite and so $\mathrm{Pic}(O)[n]$ is isomorphic to $\mathrm{Pic}(O)/n\,\mathrm{Pic}(O)$.)

But recall that one *needs*

i): $T_{L,n}$ is non-degenerate,

ii): one can compute efficiently in $H^2(G_K, K_s^*)[n]$, and

iii): $T_{L,n}$ can be computed rapidly (for instance, in polynomial time).

One sees immediately that i) is not satisfied (over any field K) if C_O has singularities, or (for any curve C) if K is a finite field which is the interesting case for cryptography since in this case $H^2(G_K, (\mathbf{F}_q)_s) = 0$.

In the next section we shall describe how to overcome these difficulties.

4. $\mathfrak{p}$-adic lifting

We begin with O being the ring of holomorphic functions of an affine curve over a finite field $\mathbf{F}_q$.

We want to replace finite fields by *local fields* K with residue field $\mathbf{F}_q$, maximal ideal $m_{\mathfrak{p}}$ and normalized valuation $w_{\mathfrak{p}}$, and geometric objects defined over $\mathbf{F}_q$ by objects lifted in such a way that no information and no efficiency is lost.

4.1. Lifting of Galois groups

Let ϕ_q be the Frobenius automorphism which acts by exponentiation by q and which generates topologically $G_{\mathbf{F}_q}$.

The maximal unramified extension of K is denoted by K_{nr}.

There is a canonical lift of ϕ_q to K_{nr} also called the Frobenius automorphism and denoted by ϕ_q, and this automorphism generates topologically the Galois group of K_{nr}/K. (For computational aspects of this lifting see [1].)

Algebraic extensions of K_{nr} are totally ramified. Let n be a natural number prime to p, π a *uniformizing* element of K, i.e. $w_{\mathfrak{p}}(\pi) = 1$.

$L_n := K_{nr}(\pi^{1/n})$ is the unique ramified extension of K_{nr} cyclic of degree n.

Choose a primitive n-th root of unity ζ_n and denote by τ_n the generator of $G(L_n/K_{nr})$ which maps $\pi^{1/n}$ to $\zeta_n \cdot \pi^{1/n}$.

Special case: *Assume* that $n \mid (q-1)$. Then $K(\pi^{1/n})$ is Galois over K, τ_n and ϕ_q commute and the maximal tamely ramified extension of K whose Galois group has exponent dividing n is the subfield of L_n fixed by ϕ_{q^n}.

4.2. Lifting of curves

Let O be the ring of holomorphic functions of an affine curve C_O defined over $\mathbf{F}_q$, with one singular point and corresponding desingularized curve $\tilde{C}$. Let $S \subset \tilde{C}(\mathbf{F}_{q_s})$ be the set of points associated with the singular point on C_O defining the conductor $\mathfrak{m}_O = \sum_{P \in S} m_P$ of the singularity. We embed $\tilde{C}$ into the projective nonsingular curve C. The set T_∞ is defined as $C(\mathbf{F}_{q_s}) \setminus \tilde{C}(\mathbf{F}_{q_s})$.

We denote by g_0 the genus of C. We state the following (rather elementary) facts from the reduction theory of curves respectively abelian varieties.

Theorem 4.1. *(1) There is a projective absolutely irreducible* nonsingular *curve C^l over K and a Galois invariant set ${T_\infty}^l \subset C^l(\overline{K})$ with*

- *The genus of C^l is equal to $g_0+ \mid S \mid -1$.*
- *$C^l \setminus {T_\infty}^l$ modulo the maximal ideal of K is equal to C_O.*
- *The Jacobian of C^l extends to its Néron model J_{C^l} over the spectrum $Spec(O_K)$, the ring of integers of K, whose connected component $J^0 := J^0_{C^l}$ is a semi-abelian variety which has as special fiber the generalized Jacobian of $C_O \cup T_\infty$.*
- *The set ${T_\infty}^l$ is G_K-invariant. It is mapped bijectively to T_∞.*

We assume from now on that n is prime to q and to the number of connected components of the special fiber of J_{C^l}.

(2) Denote by O^l the ring of holomorphic functions on $C^l \setminus {T_\infty}^l$.

- $\mathrm{Pic}(O^l)/[n]\,\mathrm{Pic}(O^l)$ *and* $\mathrm{Pic}(O)/[n]\,\mathrm{Pic}(O)$ *are canonically isomorphic.*
- *There is a torus $\mathcal{T}^l_S$ defined over K of dimension $\mid S \mid -1$ with reduction $\mathcal{T}_S$ such that the elements of order n in $\mathcal{T}^l_S$ are mapped to the elements of order n in $\mathcal{T}_S$ and we have the exact sequence of finite abelian groups*

$$1 \to \mathcal{T}^l_S(U_K)/(\mathcal{T}^l_S(U_K))^n \to \mathrm{Pic}(O^l)/[n]\,\mathrm{Pic}(O^l) \to \mathrm{Pic}(\tilde{O})/[n]\,\mathrm{Pic}(\tilde{O}) \to 0$$

where U_K are the units with respect to the valuation of K.

(3) For $T_\infty = \{P_\infty\}$ we get that $J_{C^l}(K)/[n]J_{C^l}(K)$ is canonically isomorphic to $\mathrm{Pic}(O)/[n]\,\mathrm{Pic}(O)$.

(4) The set ${T_\infty}^l$ can be chosen such that the subgroup $\mathcal{C}_{{T_\infty}^l}$, the subgroup of divisor classes generated by divisors of degree 0 *with support in ${T_\infty}^l$, is isomorphic to $\mathcal{C}_{T_\infty}$. So we get the exact sequence*

$$0 \to (\mathcal{C}_{T_\infty}/[n]\mathcal{C}_{T_\infty})^{G_K} \to J_{C^l}(K)/[n]J_{C^l}(K) \to \mathrm{Pic}(O)/[n]\,\mathrm{Pic}(O) \to 0.$$

Moreover there is an isogeny ψ of J_{C^l} defined over K with kernel isomorphic to $\mathcal{C}_{T_\infty}$ such that $\mathrm{Pic}(O)/[n]\,\mathrm{Pic}(O)$ *is isomorphic to $\psi(J_{C^l}(K))/[n]\psi(J_{C^l}(K))$.*

Theorem 4.1 enables us to study all crypto systems based on ideal classes of curves over finite fields by using cohomology theory of local fields.

In most instances the situation will be rather simple. The curve C will be either non-singular (good reduction) or will have genus equal to zero (the toric case).

The set of missing points will often consist (e.g. in the case of C_{ab}-curves) of one point and so the group $\mathcal{C}_{T_\infty}$ is the trivial group.

The lift of curves in the toric case leads to the interesting theory of Mumford curves.

Remark 4.2. It is important that all interesting objects can be lifted over K. This is so since n is prime to q and we are in the étale world.

The next important observation is that the finite modules defined over $\mathbf{F}_q$ can be lifted to unramified Galois modules over K which play a special role in the cohomology theory of local fields [15].

Connected components and ramification. In Theorem 4.1 we have assumed that n is prime to the number of connected components of the special fiber of the Jacobian of the lifted curve. This is a very mild condition. On the one hand we have many choices for the construction of C^l and we can do it such that this number is very small. On the other side the assumption is not really necessary; it only simplifies the formulation of Theorem 4.1 (which is long enough as it is). In certain cases it may be even desired to have an appropriate number of components which deliver torsion points on J_{C^l} which are not coming from points on $\mathrm{Pic}(O)$.

If, after the lifting, we extend K by a ramified extension L and if there was a singularity on C_0 then the group of connected components of the semi-abelian group scheme over O_L will be multiples of the ramification index, and so there is a ramified part of the torsion group of J_{C^l} if there are singular points on C_O. This makes the cohomology theory of Galois modules attached to torsion points much richer.

The Tate elliptic curve. Instead of proving the statements of Theorem 4.1 we give a simple but important example.

Example 4.3. We begin with the affine curve

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

defined over $\mathbf{F}_q$ and corresponding to

$$O = \mathbf{F}_q[X,Y]/(Y^2 + XY - X^3).$$

We have $T_\infty = \{P_\infty\}$ where P_∞ corresponds to the point $(0,1,0)$ on the projective curve

$$Y^2Z - XYZ = X^3.$$

There is one singular point $(0,0)$ on C. This point corresponds to two points (we have two different tangents at this point) on the desingularization. It follows that $\mathrm{Pic}(O)$ is isomorphic to $\mathbf{F}_q^*$.

Let K be a local field with residue field $\mathbf{F}_q$ and uniformizing element π, $k \in \mathbf{N}$.

Then

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

is the affine part of an elliptic curve with reduction equal to C. It is a Tate curve with period Q with $w_{\mathfrak{p}}(Q) = k$. The number of connected components in the special fiber is equal to k. The group of rational points $E(K)$ is isomorphic to $K^*/ < Q >$, and we get the exact sequence

$$1 \rightarrow U_K \rightarrow E(K) \rightarrow \mathbf{Z}/k\mathbf{Z} \rightarrow 0,$$

and all the assertions of the Theorem 4.1 can be checked immediately.

5. Local duality

We state the local version of the fundamental duality theorem for (finite) Galois modules (cf. [22] and [15])[3].

Let K be a local field and A a finite G_K-module of order n prime to the characteristic of the residue field of K. Let $\widehat{A}$ be the Cartier dual $\mathrm{Hom}(A, \mu_n)$ of A (where μ_n is the Galois module consisting of the n-th roots of unity in K_s).

Theorem 5.1. *(Duality Theorem of Tate) For $0 \leq i \leq 2$ the cohomology groups $H^i(G_K, A)$ are finite and the evaluation pairing induces nondegenerate pairings*

$$H^i(G_K, A) \times H^{2-i}(G_K, \widehat{A}) \rightarrow H^2(G_K, K_s^*).$$

[3] The reader will find a nice introduction to the number theoretical background in [12]

We apply this to $A = \mathbf{Z}/n$. Its dual is μ_n. We get for $i = 0$ a non-degenerate pairing

$$\mathbf{Z}/n \times H^2(G_K, \mu_n) \to H^2(G_K, K_s^*).$$

The Kummer sequence for K_s^* and Hilbert's theorem 90 imply that

$$H^2(G_K, \mu_n) = H^2(G_K, K_s^*)[n]$$

and hence it follows

Corollary 5.2. $H^2(G_K, \mu_n) = H^2(G_K, K_s^*)[n] \overset{inv}{\cong} \mathbf{Z}/n.$

We shall make this isomorphism "inv" explicit (which does not mean "computable"!).

The interesting consequence of the duality theorem in our context is

Theorem 5.3. ***(Tate-Lichtenbaum)*** *Let K be a local field, C_O an affine regular curve over K with ring of holomorphic functions O.*

For every natural number n the Lichtenbaum-Tate pairing

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

is non-degenerate.

This result encourages to investigate the modules $H^1(G_K, \mathrm{Pic}(\overline{O}))[n]$ and $H^2(G_K, K_s^*)[n]$.

5.1. $H^1(G_K, \mathrm{Pic}(\overline{O}))[n]$

We recall that $\mathrm{Pic}(\overline{O})$ is G_K-isomorphic to $\mathcal{A}(K_s)$ where $\mathcal{A}$ is an abelian variety defined over K and isogenous to J_C. Moreover $\mathcal{A}$ extends to a group scheme over the rings of integer of K, its *Néron model* whose connected component of the unity is a semi-abelian variety.

We continue to assume that n is prime to the characteristic of the residue field of K and to the number of connected components of the special fiber of $\mathcal{A}$[4].

It follows that $H^1(G(K_{nr}/K), \mathrm{Pic}(O_{K_{nr}})) = 0$.

Hence via restriction of cocycles we can embed $H^1(G_K, \mathrm{Pic}(\overline{O}))$ into $H^1(G_{K_{nr}}, \mathrm{Pic}(\overline{O}))$, and the image is contained in the subgroup of elements which are ϕ_q-invariant (ϕ_q acts by conjugation on $G_{K_{nr}}$).

[4] It can be interesting to study what happens if the last condition is not satisfied.

It is known that elements in $H^1(G_K, Pic(\overline{O}))[n]$ are split by extensions of exponent n, and so $H^1(G_K, Pic(\overline{O}))[n]$ can be considered as subgroup of $H^1(G(L_n/K_{nr}), \mathrm{Pic}(O_{K_{nr}}))$ with $L_n := K_{nr}(\pi^{1/n})$.

We state this as a lemma.

Lemma 5.4. *Let O be the ring of holomorphic functions of a regular affine curve, and let $\mathcal{A}$ be an abelian variety with $\mathcal{A}(K_s) \cong_{G_K} \mathrm{Pic}(\overline{O})$. Assume that $n \in \mathbf{N}$ is prime to the characteristic of the residue field of K and to the number of connected components of the Néron model of $\mathcal{A}$.*

Then $H^1(G_K, Pic(\overline{O}))[n]$ can, via restriction, be identified with the subgroup of $H^1(G(K_{nr}(\pi^{1/n})/K_{nr}), \mathrm{Pic}(O_{K_{nr}(\pi^{1/n})}))[n]$ which is invariant under the action of ϕ_q.

We recall that $G(L_n/K_{nr}) =< \tau_n >$ with $\tau_n(\pi^{1/n}) = \zeta_n \cdot \pi^{1/n}$.

Hence the Frobenius automorphism ϕ_q acting by conjugation on τ sends τ to τ^q. (q is the value of the cyclotomic character applied to ϕ_q.)

Using this one can determine $H^1(G_K, Pic(\overline{O}))[n]$ in all concrete cases. Here are two examples.

First assume that J_C and hence $\mathcal{A}$ has good reduction. This is true if the affine curve C_O is the lift of a regular curve over $\mathbf{F}_q$. In this case

$$\mathcal{A}[n] := \mathcal{A}(K_s)[n] = \mathcal{A}(L_n)[n] = \mathcal{A}(K_{nr})[n]$$

and hence

$$H^1(G_K, Pic(\overline{O}))[n] = Hom_{<\phi_q>}(< \tau >, \mathcal{A}[n]).$$

Proposition 5.5. *Let K be a local field with residue field $\mathbf{F}_q$. We assume that O is the ring of holomorphic functions of a regular affine curve which is the lift of a regular curve over $\mathbf{F}_q$.*

Let n be prime to q. Let $\mathrm{Pic}(O)[n]^{(q)}$ be the subgroup in $\mathrm{Pic}(\overline{O})[n]$ consisting of elements c with $\phi_q(c) = q \cdot c$.

Then $H^1(G_K, Pic(\overline{O}))[n]$ is isomorphic to $\mathrm{Hom}(< \tau >, \mathrm{Pic}(O)[n]^{(q)})$, and so, non-canonically since depending on the choice of τ, to $\mathrm{Pic}(O)[n]^{(q)}$.

Corollary 5.6. *The assumptions are as in the Proposition 5.5.*

- **i):** *If $\zeta_n \in K$ then $H^1(G_K, Pic(\overline{O}))[n]$ is isomorphic to $\mathrm{Pic}(O)[n]$.*
- **ii):** *Let L be any extension field of K totally ramified of degree n. Then $H^1(G_K, \mathrm{Pic}(\overline{O}))[n]$ is equal to the kernel of the restriction map from G_K to G_L.*

For general curves C_O it is more complicated to describe the result. One reason is that the torus part of the special fiber of J_C need not be split. A complete treatment is possible in principle but not in the frame of this survey. So we restrict ourselves to take as rings O the holomorphic functions on Tate elliptic curves given by affine equations

$$E_Q : Y^2 + XY = X^3 + Q.$$

with $w_{\mathfrak{p}}(Q) = m \in \mathbf{N}$.

Since only one point is missing we get that $\mathrm{Pic}(\overline{O})$ is Galois isomorphic to $E_Q(K_s)$.

We assume that n is prime to m. Then $E_Q(K)$ contains elements of order n iff $\zeta_n \in K$, and hence by duality $H^1(G_K, E_Q(K_s))[n] \neq 0$ iff $\zeta_n \in K$, and in this case it is cyclic of order n.

So we assume that $\zeta_n \in K$.

We take a special cyclic extension of degree n, namely $L_Q := K(Q^{1/n})$. By Tate's theory this field is equal to $K(E_Q[n])$.

Proposition 5.7. *Let τ be a generator of $G(L_Q/K)$, let $P \in E_Q[n]$ be any point of order n which is not K-rational, and let ζ be the cocycle from $< \tau >$ to $E_Q[n]$ determined by $\zeta(\tau) = P$.*

Then $H^1(G_K, E_Q(K_s))[n]$ is cyclic of order n and generated by the class of ζ.

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

For the moment let K be any field of characteristic prime to n.

The second cohomology group of K_s^* plays a very important role in the arithmetic of K and is called the *Brauer group* Br(K) of K.

Its elements can be identified with classes of central simple algebras with center K. The group composition is the tensor product, and the trivial class consists of all algebras which are isomorphic to full matrix algebras over K (for details see [18]).

Because of Hilbert's theorem 90 one sees that for L/K Galois the inflation map from $H^2(G(L/K), L^*)$ to Br(K) is injective.

For any L/K the restriction map from Br(K) to Br(L) corresponds to base field extension applied to algebras, and its kernel consists of the classes of algebras which become, after tensoring with L, isomorphic to full matrix algebras. In this case L is called a splitting field of K.

Example 5.8. Cyclic algebras Assume that L/K is cyclic extension of degree n.

$H^2(G(L/K), L^*)$ consists of classes of *cyclic* algebras with 2-cocycles given in the following way: let σ be a generator of $G(L/K)$ and take a in K^*. The map $f_{\sigma,a} : G \times G \to L^*$, given by

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

defines a 2-cocycle. The cocycles $f_{\sigma,a}$ and $f_{\sigma,a'}$ 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 $(L, \sigma, a \cdot N_{L/K}L^*)$.

Recall that a cyclic algebra occurred in Example 3.2 as result of the Lichtenbaum-Tate pairing.

5.2.1. Brauer groups of local fields

Let K be a local field with residue field $\mathbf{F}_q$, and let n be prime to q.

Because of the local duality theorem we know already that $\mathrm{Br(K)[n]} \cong \mathbf{Z}/\mathrm{n}$.

5.2.2. The unramified case: the invariant

Let L_u be the unique unramified extension of K of degree n. It is cyclic.

$G(L_u/K)$ has as canonical generator a lift of the Frobenius automorphism ϕ_q of $\mathbf{F}_q$.

Elements $c \in H^2(G(L_u/K), L_u^*)$ are represented by cyclic algebras.

We use Example 5.8 and represent c by a triple $(L_u, \phi_q, a \cdot N_{L_u/K}(L_u^*))$.

Since

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

the class of c is uniquely determined by $w_{\mathfrak{p}}(a) \bmod n$.

Definition 5.9. $w_{\mathfrak{p}}(a) \in \mathbf{Z}/n\mathbf{Z}$ is the *invariant* $\mathrm{inv}_K(c)$ of c.

Proposition 5.10. **i):** $\mathrm{Br(K)[n]} = \mathrm{inf_{L_u/K_s}(H^2(G(L_u/K), L_u^*))}$.

ii): *The map*

$$\mathrm{inv}_K : Br(K)[n] \to \mathbf{Z}/n$$

is defined as follows:

For $c \in \mathrm{Br(K)[n]}$ *take* $c_0 \in H^2(G(L_u/K), L_u^*)$ *with* $\inf_{L_u/K_s}(c_0) = c$ *and represent* c_0 *by the triple* $(L_u, \phi_q, a \cdot N_{L_u/K}(L_u^*))$.

Then $\mathrm{inv}_K(c) := w_{\mathfrak{p}}(a) \mod n$ *is well defined, determines* c *uniquely, and defines an isomorphism*

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

Remark 5.11. Though the invariant is defined in a seemingly very explicit way for cyclic algebras split by unramified extensions it may be difficult to compute it even in this case. To see this assume that τ is another generator of $G(L_u/K)$ and the cyclic algebra representing c is given by the triple

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

We know that there exists $k \in \mathbf{Z}$ with $\tau^k = \phi_q$. Then

$$\mathrm{inv}_K(c) = k \cdot w_{\mathfrak{p}}(a) \mod n.$$

So we have to determine k, and this is a discrete logarithm problem.

For example, assume that $\zeta_n \in K$ and $L_u = K(\zeta_{n^2})$. Then $\tau(\zeta_{n^2}) = \zeta_\tau \zeta_{n^2}$.

Hence k has to satisfy

$$\zeta_\tau^k \cdot \zeta_{n^2} = \zeta_{n^2}^q,$$

i.e.

$$\zeta_\tau^k = \zeta_{n^2}^{q-1}$$

which is a discrete logarithm problem in $\mathbf{F}_q^*$.

5.2.3. **The tamely ramified case**

Let L_n a totally ramified Galois extension L_n of degree n of K. It follows that L_n/K is cyclic and that K contains the n-th roots of unity.

Let τ be a fixed generator of $G(L_n/K)$.

Since $K^*/N_{L_n/K}(L^*) \cong \mathbf{F}_q^*/\mathbf{F}_q^{*n}$ elements $c \in H^2(G(L_n/K), L_n^*)$ are determined by triples

$$(L_n, \tau, a \in \mathbf{F}_q^*/\mathbf{F}_q^{*n}).$$

Proposition 5.12. *Assume that* $a_1, a_2 \in \mathbf{F}_q$ *are given.*

Then

$$a_1^k \equiv a_2 \mod \mathbf{F}_q^{*n} \textit{ iff } \mathrm{inv}_K((L_n, \tau, a_1 \cdot \mathbf{F}_q^{*n})) = k \cdot \mathrm{inv}_K((L_n, \tau, a_2 \cdot \mathbf{F}_q^{*n})).$$

Corollary 5.13. *The computation of discrete logarithms in the multiplicative group of finite fields is equivalent with the computation of invariants of cyclic algebras split by ramified extensions.*

5.2.4. **The Frobenius case**

The most important case for applications is that $c \in \mathrm{Br(K)}$ is represented as algebra split by an extension L of K which is totally ramified of degree n but which becomes Galois only after adjoining the n-th roots of unity. This is exactly the situations which occurs when one applies the Lichtenbaum-Tate pairing.

At the moment a description useful for algorithmic purposes is only available if one restricts c to $K(\zeta_n)$ and then uses the results obtained for cyclic ramified extensions over $K(\zeta_n)$ instead of K. Hence one has to pass to a field which will be, in general, much larger than K!

It is a challenge to do better.

5.3. **The pairing**

Having information about the groups involved in the Lichtenbaum-Tate pairing we give this pairing now in an explicit way, first over local fields, and then, in order to apply it to cryptography, over finite fields.

5.3.1. **Explicit description of the Lichtenbaum-Tate pairing**

The pairing over local fields. We continue to assume that K is a local field with residue field $\mathbf{F}_q$.

Though the general case is interesting we restrict ourselves to the case that the curve C has good reduction (hence is the lift of a nonsingular curve C_0 over $\mathbf{F}_q$) and that only one point "at infinity" is missing on C_O. So we have a non-degenerate pairing

$$T_{L,n} : J_C(K)/nJ_C(K) \times H^1(G_K, J_C(K_s))[n] \to \mathrm{Br(K)[n]}.$$

Let k be the smallest number with

$$q^k \equiv 1 \mod n.$$

k is called the "embedding degree".

Define $K(\zeta_n) := K_n$. It is a local field with residue field $\mathbf{F}_{q^k}$.

We choose a uniformizing element $\pi \in K$ and define $L := K_n(\pi^{1/n})$ and take τ as generator of $G(L/K_n)$.

As seen in Subsection 5.1 we can identify $H^1(G_K, J_C(K_n))[n])$ with the group of homomorphisms $\varphi \in \mathrm{Hom}(G_K, J_C(K_n)[n])$ with $\varphi(\tau) = P$ and $\phi_q(P) = q \circ P$.

Hence we are in the situation described already in Example 3.2 and have only to repeat the construction made there.

Take $c \in H^1(G_K, J_C(K_s))$ and corresponding φ with $\varphi(\tau) = P$.

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

Then $T_{L,n}(\overline{Q}, c)$ is the class of cyclic algebra $(L, \tau, f_P(Q) \cdot N_{L/K_n}(L^*))$.

As seen in Subsection 5.2.3 we can interpret $T_{L,n}$ as pairing with values in $\mathbf{F}^*_{q^k}/(\mathbf{F}^*_{q^k})^n$. Hence we get a pairing

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

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

The pairing over finite fields. We can look at the result above modulo $m_{\mathfrak{p}}$ and get an explicit description of the Tate-Lichtenbaum pairing in the case of good reduction which only uses objects attached to the curve modulo $m_{\mathfrak{p}}$.

Theorem 5.14. *Assume that C is a projective irreducible non-singular curve define over $\mathbf{F}_q$. Then we get a pairing*

$$T_n : J_C(\mathbf{F}_q) \times J_C(\overline{\mathbf{F}_q})[n]^{(q)} \rightarrow \mathbf{F}^*_{q^k}/(\mathbf{F}^*_{q^k})^n$$

which is non-degenerate on the right side and has radical $nJ_C(\mathbf{F}_q)$ on the left side.

5.3.2. **Evaluation**

To get a bilinear structure on class groups of rings attached to holomorphic functions on curves over finite fields there is a last step to be done. One has to show that the computation of the pairing is fast.

To compute T_n one has to evaluate a divisor D on C defined over $\mathbf{F}_q$ by a function f_P contained in the function field $F \cdot \mathbf{F}_{q^k}$.

A naive approach is, because of the high degrees needed in practice, not possible.

The way out was found by *V. Miller* [16] for elliptic curves (applied to the Weil pairing). The general method uses as background the theory of Mumford‘s Theta groups which describe extensions of (finite subgroups of) abelian varieties by linear groups. It was developed in [10], for elliptic curves we refer to [9].

The basic step for the computation is: for given positive divisors A_1, A_2 of degree g find a positive divisor A_3 of degree g and a function h on C such that

$$A_1 + A_2 - A_3 - gP_0 = (h).$$

One has to repeat such an step $O(\log(n))$ times and one has to compute in $\mathbf{F}_{q^k}$.

For more details and shortcuts we refer to [1] (and many publications in recent time).

6. Bilinear structures on divisor classes

Let O be the ring of holomorphic functions of an affine curve over a finite field $\mathbf{F}_q$.

Let n be a number prime to q, and let k be the smallest number such that $n \mid q^k - 1$.

Theorem 6.1. *The Lichtenbaum-Tate pairing induces a bilinear structure on* $\mathrm{Pic}(O)$ *of complexity* $O(k \cdot log(q))$ *with value group* $\mathrm{Br(K)}$.

Corollary 6.2. *The discrete logarithm in* $\mathrm{Pic}(O)$ *is reduced to the discrete logarithm with costs* $O(k \cdot log(q))$ *in* $\mathrm{Br(K)}$ *and hence to the computation of invariants in* $\mathrm{Br(K)}$*, or alternatively, to the computation of discrete logarithms in* $\mathbf{F}^*_{q^k}/\mathbf{F}^{*n}_{q^k}$.

To apply these results (and to have a bilinear structure in the strong sense) it is necessary that k is not too big.

In particular, for the constructive applications it is necessary to have an embedding degree $\sim 12 \cdot g$. It is a very nice problem in computational number theory to find such k. For elliptic curves see for example [2] and [3].

But for $g > 1$ nearly nothing is known if J_C is not supersingular.

A successful approach to this problem could be interesting since one can speed up the computation of T_n by a factor g in interesting protocols, see [8].

7. An Index-Calculus approach for the computation of invariants

In the previous chapters the role of Brauer groups of local fields was explained. In particular, the importance of invariants of elements in Br(K) for discrete logarithms was emphasized.

By passing from local fields to global fields we can again use the basic duality theorem of Tate, but now in a global version. For a precise formulation see [15].

So let K be a global field, i.e. K is either a finite algebraic extension of $\mathbf{Q}$ or a function field of one variable over a finite field $\mathbf{F}_q$.

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.

The restriction map to $G_{\mathfrak{p}}$ is denoted by $\rho_{\mathfrak{p}}$.

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

A consequence of the global duality theorem is the sequence of *Hasse-Brauer-Noether.*

Theorem 7.1. *Let K be a global field and $n \in \mathbf{N}$ odd and prime to $char(K)$.*

The sequence

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

is exact.

We shall use an obvious consequence:

Corollary 7.2. *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 the set $T_{\mathfrak{m}}$ of prime ideals 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 $G(L/K)$. By $f_{\mathfrak{p}}$ we denote a number for which $\tau^{f_{\mathfrak{p}}} = \phi_{\mathfrak{p}}$ holds. Then for all elements $a \in K^*$ we have

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

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

7.1. Applications

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

i): the order of ray class groups of K with conductor $\mathfrak{m}$, in particular Euler's totient function $\varphi(m)$

ii): the discrete logarithm in $\mathbf{F}_q^*$

and

iii): get a very subtle description of cyclic extensions of K.

More details can be found in [7].

7.2. 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 factorization algorithms.

7.3. Example: $K = \mathbf{Q}$

Take $K = \mathbf{Q}$. The congruence in Corollary 7.2 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 $q < B$. 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 $c_0 = d^2-m$.

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

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 $\mathbf{Z}$-independent equations and with n of the primes p occurring.

Proposition 7.3.

$$det(\mathcal{L})$$

is a multiple of $\varphi(m)$.

7.4. **Construction of elements in the Brauer group**

Motivated by index-calculus and for theoretical reasons, too, we are looking for more methods to construct elements in the Brauer group of number fields. The theoretical background for the success (or failure) is another consequence of the global duality theorem, namely the duality theorem of Tate-Poitou [15]. As methods to construct such elements of a very well controlled arithmetical nature one can try to use

i) pairings with Dirichlet Characters ([11]), or

ii) pairings with Principal Homogenous Spaces of abelian varieties instead of using the multiplicative group , or

iii) 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 corresponding to local Brauer group.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, *The Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC, Baton Rouge, 2005.

[2] P. S. L. M. Barreto, B. Lynn, and M. Scott, *Constructing elliptic curves with prescribed embedding degrees*, Security in Communication Networks – SCN 2002, volume 2576 of Lecture Notes in Comput. Sci.

(S.Cimato, C. Galdi, and G. Persiano, eds.), Springer-Verlag, Berlin, 2003, pp. 257–267.

[3] P. S. L. M. Barreto and M. Naehrig, *Pairing-friendly elliptic curves of prime order*, Selected Areas in Cryptography – SAC'2005, Lecture Notes in Comput. Sci. 3897 (B.Preneel and St.Tavares, eds.), Springer Verlag, Berlin, 2006, pp. 319–331.

[4] D. Boneh and M. Franklin, *Identity based encryption from the Weil pairing*, SIAM J. Comput. **32(3)** (2003), 586–615.

[5] D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, Advances in Cryptology – Asiacrypt 2001, Lecture Notes in Comput. Sci. 2248 (C.Boyd, ed.), Springer Verlag Berlin, 2002, pp. 514–532.

[6] G. Frey, *Applications of arithmetical geometry to cryptographic constructions*, Finite fields and applications (D. Jungnickel and H. Niederreiter, eds.), Springer, Berlin, 2001, pp. 128–161.

[7] G. Frey, *On the relation between Brauer groups and discrete logarithms*, Tatra Mt. Math. Publ. **33** (2006), 199–227.

[8] G. Frey and T. Lange, *Mathematical background of public key cryptography*, Séminaires et Congrès SMF: AGCT 2003 (Y. Aubry, ed.), SMF, 2005, pp. 41–74.

[9] G. Frey, M. Müller, and H. G. Rück, *The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems*, IEEE Trans. Inform. Theory **45(5)** (1999), 1717–1719.

[10] G. Frey and H. G. Rück, *A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves*, Math. Comp. **62** (1994), 865–874.

[11] M.-D. Huang and W. Raskind, *Signature calculus and discrete logarithm problems*, Proc. ANTS VII, LNCS 4076 (F.Hess, S.Pauli, and M.Pohst, eds.), Springer, Berlin, 2006, pp. 558–572.

[12] J.Neukirch, *Algebraic number theory*, Springer, Heidelberg, 1999.

[13] A. Joux, *A one round protocol for tripartite Diffie–Hellman*, Proc. ANTS IV, LNCS 1838 (W. Bosma, ed.), Springer, 2000, pp. 385–394.

[14] S. Lichtenbaum, *Duality theorems for curves over p-adic fields*, Invent. Math. **7** (1969), 120–136.

[15] B. Mazur, *Notes on étale cohomology of number fields*, Ann. sci. ENS **6** (1973), no. 4, 521–552.

[16] V.C. Miller, *The Weil Pairing, and Its Efficient Calculation*, J.Cryptology **17** (2004), 235–261.

[17] D. Mumford, *Abelian varieties*, Oxford University Press, Oxford, 1970.

[18] K. Nguyen, *Explicit Arithmetic of Brauer Groups, Ray Class Fields and Index Calculus*, Ph.D. thesis, University of Essen, 2001.

[19] J.P. Serre, *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.

[20] ______, *Corps locaux*, Hermann, Paris, 1962.

[21] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Heidelberg, 1993.

[22] J. Tate, *WC-groups over $\mathfrak{p}$-adic fields*, Séminaire Bourbaki; 10e année: 1957/1958. Textes des conférences; Exposés 152 à 168; 2e éd. corrigée, Exposé 156, vol. 13, Secrétariat mathématique, Paris, 1958.

Gerhard Frey
Institute for Experimental Mathematics
University of Duisburg-Essen
Ellernstrasse 29
45219 Essen
Germany
frey@iem.uni-due.de
sr@math.bu.edu