

Arithmetical Aspects of Brauer Groups and Applications to Discrete Logarithms

Gerhard Frey

Institute for
Experimental Mathematics
University of Duisburg-Essen
frey@exp-math.uni-essen.de

Algebraic Methods in Cryptography

Bochum

Nov. 17, 2005

Contents

1	Discrete Logarithms in Class Groups	2
1.1	DL-systems in Class Groups	4
1.2	Ideal Classes of Function Rings	6
2	Cohomology	8
2.1	Notations and Definitions	8
2.1.1	The relevant cohomology groups	9
2.2	The Long Cohomology Sequence	12
3	The Lichtenbaum Pairing	13
4	\mathfrak{p}-adic Lifting	16
4.1	Theorem of Tate-Lichtenbaum	20
5	Brauer Groups	21
5.1	Definition	21
5.2	Cyclic Algebras	22
5.3	Brauer Groups of Local Fields	23

5.3.1	The Tamely Ramified Case	23
5.3.2	The Unramified Case:Invariants	25
6	Globalization of Brauer Groups	28
6.1	The Local-Global Relation	28
6.2	Application to Ring Class Num- bers	31
6.3	Computation of the Classical DL	34
6.4	Description of Cyclic Extensions	35
7	Index-Calculus in Global Brauer Groups	36
7.1	Example: $K = \mathbb{Q}$	37
8	Relations related to Abelian Varieties	38
8.1	Finding Sparse Relations	38
8.2	Lifting Local Pairings	40
8.2.1	A Challenge for Heuristics	41

1 Discrete Logarithms in Class Groups

There is a large family of practically used (or usable) public key cryptosystems that rely on crypto primitives based on hard computational problems in easily “implemented” groups.¹

In this section we shall concentrate to the **Discrete Logarithm Problem (DLP)** in groups G whose order is divided by a large prime number ℓ .

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

¹This includes RSA.

1.1 DL-systems in Class Groups

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 ideals is denoted by $\text{Pic}(O)$.

Find suitable rings O such that for a large prime ℓ

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

1.2 Ideal Classes of Function Rings

We study one type of rings:

\mathcal{O} the ring of holomorphic functions

of an (affine) curve $C_{\mathcal{O}}$ 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**).

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 $C_{\mathcal{O}}$ and so to the points of the Jacobian variety J_C of C .

We can 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

$$1 \rightarrow \text{Princ}_{\overline{O}} \rightarrow I(\overline{O}) \rightarrow \text{Pic}(\overline{O}) \rightarrow 0$$

.

Observation and Warning: In this general setting it is not true that by taking Galois invariant elements this sequence yields the corresponding sequence of ideal groups attached to O .

To see what is happening, and to connect the sequence with Brauer groups one has to use **Galois Cohomology**.

2 Cohomology

2.1 Notations and Definitions

Let G be a (pro-)finite group.

Example 2.1 K be any field, K_s its separable closure

$G := G_K = \text{Aut}_K(K_s)$ its absolute Galois group.

All maps from G into another topological space M will be assumed to be continuous with respect to the Krull topology on G . From now on we assume that M has the discrete topology.

2.1.1 The relevant cohomology groups

$$H^0(G, M) := M^G = \{m \in M; \sigma m = m \text{ for all } \sigma \in G\}.$$

Definition 2.2 *1-cocycles are maps*

$$c^1 : G \rightarrow M$$

with

$$c^1(\sigma\tau) = c^1(\sigma) + \sigma c^1(\tau).$$

1-coboundaries are maps

$$b^1 : G \rightarrow M$$

with

$$b^1(\sigma) = \sigma \cdot m - m$$

for a fixed $m \in M$ and for all $\sigma \in G$.

$$H^1(G, M) = \{1\text{-cocycles}\} / \{1\text{-coboundaries}\}$$

2-cocycles are maps

$$c^2 : G \times G \rightarrow M$$

with

$$\sigma c^2(\tau, \mu) - c^2(\sigma\tau, \mu) + c^2(\sigma, \tau\mu) - c^2(\sigma, \mu) = 0.$$

2-coboundaries are maps

$$b^2 : G \times G \rightarrow M$$

such that there exists

$$f : G \rightarrow M$$

with

$$b^2(\sigma, \tau) = \sigma f(\tau) - f(\sigma\tau) + f(\sigma).$$

$$H^2(G, M) = \{2\text{-cocycles}\} / \{2\text{-coboundaries}\}$$

Let U be a closed subgroup of G .

Every G -module M is in a natural way a U -module.

By restricting cocycles one gets

restriction homomorphisms

$$\text{res}_U : H^n(G, M) \rightarrow H^n(U, M).$$

If U is a normal subgroup we have the inflation map induced by the quotient map

$$\text{inf}_{G/U} : H^n(G/U, M^U) \rightarrow H^n(G, M).$$

Example 2.3 *We can compute cohomology groups of G_K acting on M by computing the cohomology groups of the finite quotients $G(L/K)$ of G_K acting on M^{G_L} and then using the inflation map.*

2.2 The Long Cohomology Sequence

Assume that

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

is an exact sequence of G -modules.

For $n \geq 0$ the maps α resp. β induce (by composition with cocycles) homomorphisms $\alpha^n : H^n(G, A) \rightarrow H^n(G, B)$ resp.

$$\beta^n : H^n(G, B) \rightarrow H^n(G, C).$$

There is an explicitly given “boundary map” $\delta^n : H^n(G, C) \rightarrow H^{n+1}(G, A)$.

FACT

$$\begin{aligned} \dots H^n(G, A) &\xrightarrow{\alpha^n} H^n(G, B) \xrightarrow{\beta^n} H^n(G, C) \\ &\xrightarrow{\delta^n} H^{n+1}(G, A) \xrightarrow{\alpha^{n+1}} H^{n+1}(G, B) \rightarrow \dots \end{aligned}$$

is exact.

3 The Lichtenbaum Pairing

\mathcal{O} resp. $\overline{\mathcal{O}}$ are defined as above but associated to curves over arbitrary K .

Assume first that $C_{\mathcal{O}}$ regular and $C \setminus C_{\mathcal{O}} = \{P_{\infty}\}$.

From

$$1 \rightarrow (\overline{F}) \rightarrow I(\overline{\mathcal{O}}) \rightarrow \text{Pic}(\overline{\mathcal{O}}) \rightarrow 0$$

we get

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

Explicit description:

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

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

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

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*

$$T_L : \text{Pic}(O) \times H^1(G_K, \text{Pic}(\bar{O})) \rightarrow H^2(G_K, K_s^*)$$

is defined in the following way:

Choose $A := \prod_{P \in C_O} m_P^{z_P} \in \bar{D} \in \text{Pic}(O)$ of degree 0 and

$c \in H^1(G_K, \text{Pic}(\bar{O}))$ 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:

$$T_L : \text{Pic}(O) \times H^1(G_K, \text{Pic}(\bar{O})) \rightarrow H^2(G_K, K_s^*).$$

4 \mathfrak{p} -adic Lifting

We want to apply the pairing to the situation in section 1.2, i.e. \mathcal{O} is the ring of holomorphic functions of an affine curve over a finite field \mathbb{F}_q .

We encounter two difficulties:

- over *any* field K the first cohomology group of tori is trivial (Hilbert 90), and so we do not get a non-trivial pairing on the torus part of Generalized Jacobians reflecting the singularities
- $H^2(G_{\mathbb{F}_q}, \overline{\mathbb{F}_q}^*) = 0$.

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

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 assume that C_O has only ordinary double points in the set S (regarded as point set on the desingularisation) as singularities, and that a set T_∞ of points are “missing” on C_O .

Fact 4.1 1. $\exists C^l/K$ and $T_\infty^l \subset (C^l(K_s))$
with

- $g(C^l) = g_0 + |S| - 1$.
- $C^l \setminus T_\infty^l \pmod{m_K} = C_O$.
- T_∞^l is G_K -invariant and mapped bijectively to T_∞ .

2. $O^l :=$ ring of holomorphic functions
on $C^l \setminus T_\infty^l$
 \tilde{O} its normalization
 n prime to q .

- $\text{Pic}(O^l)/[n]\text{Pic}(O^l)$ is canonically isomorphic to $\text{Pic}(O)/[n]\text{Pic}(O)$.
- \exists a torus T_S/K of dimension $|S| - 1$ and an exact sequence

$$1 \rightarrow T_S^l(U_K)/(T_S^l(U_K))^n \rightarrow \text{Pic}(O^l)/[n]\text{Pic}(O^l) \rightarrow \text{Pic}(\tilde{O})/[n]\text{Pic}(\tilde{O}) \rightarrow 0$$

with U_K the units of K

.

SO: Fact 4.1 enables us to lift all crypto systems based on ideal classes of curves over finite fields to such systems over local fields.

Interesting examples: Mumford curves.

Example 4.2

$$C_O : Y^2 + XY = X^3 / \mathbb{F}_q$$

We have $T_\infty = \{(0, 1, 0)\}$. There is one singular point $(0, 0)$ on C_O corresponding to 2 points on the desingularization

So $\text{Pic}(O) \cong \mathbb{F}_q^$.*

K local field with residue field \mathbb{F}_q and uniformizing element π .

Then

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

is a Tate elliptic curve with reduction C and period Q with $w_{\mathfrak{p}}(Q) = 1$.

$$E(K) \cong K^* / \langle Q \rangle \cong U_K.$$

4.1 Theorem of Tate-Lichtenbaum

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

Theorem 4.3 (Tate, Lichtenbaum)

For every natural number n the pairing

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

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

5 Brauer Groups

5.1 Definition

Let K be a field.

Definition 5.1 *The Brauer group of K is the cohomology group $H^2(G_K, K_S^*)$. It is denoted by $\text{Br}(K)$. The elements of $\text{Br}(K)$ with order dividing n are denoted by $\text{Br}(K)[n]$.*

5.2 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 is a generator of $G(L/K)$ and take a in K^* .

The map $f_{\sigma,a} : G \times G \rightarrow L^*$, given by

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

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

5.3 Brauer Groups of Local Fields

K a local field with residue field \mathbb{F}_q .

5.3.1 The Tamely Ramified Case

Let L_n a totally ramified cyclic extension L_n of degree n of K . We remark that this implies that K contains the n -th roots of unity.

Let τ be a fixed generator of $G(L_n/K)$. Since $K^* N_{L_n/K}(L_n^*) \cong \mathbb{F}_q^*/\mathbb{F}_q^{*n}$ elements $c \in H^2(G(L_n/K), L_n^*)$ are determined by elements in $\mathbb{F}_q^*/\mathbb{F}_q^{*n}$.

It is worthwhile to state a consequence.

Proposition 5.2 *Let n be a natural number dividing $q - 1$.*

The discrete logarithm in the group of elements of order dividing n in ideal class groups attached to curves over \mathbb{F}_q is transferred by the Tate-Lichtenbaum pairing to the discrete logarithm in $\mathbb{F}_q^/\mathbb{F}_q^{*n}$.*

5.3.2 The Unramified Case: Invariants

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

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

$c \in H^2(G(L_u/K), L_u^*)$ is canonically given by $(\phi_q, a \cdot N_{L_u/K}(L_u^*))$.

Since

$$K^*/N_{L_u/K}(L_u^*) \cong \langle \pi \rangle / \langle \pi^n \rangle$$

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

Definition 5.3 $w_{\mathfrak{p}}(a) \in \mathbb{Z}/n\mathbb{Z}$ is the invariant $\text{inv}_K(c)$ of c .

The key result of local class field theory is:

Theorem 5.4 *Every element of c in $\text{Br}(K)[n]$ is given by a cyclic algebra split by L_u . So we can associate to c (resp. A) its invariant and we get an isomorphism*

$$\text{inv}_K : \text{Br}(K)[n] \rightarrow \mathbb{Z}/n.$$

Corollary 5.5 *Assume that L_n is tamely ramified and cyclic of order n . Then*

$$\begin{aligned} H^2(G(L_n/K), L_n^*) &= \text{Br}(K)[n] \\ &= H^2(G(L_u/K), L_u^*) \xrightarrow{\text{inv}_K} \mathbb{Z}/n. \end{aligned}$$

RESULT:

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

However, it turns out that even for cyclic algebras this is equivalent to computing the discrete logarithm in \mathbb{F}_q .

6 Globalization of Brauer Groups

6.1 The Local-Global Relation

We go one step further and extend local fields to global fields.

So 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 $\rho_{\mathfrak{p}}$.

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

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

Theorem 6.1 *Let K be a global field and $n \in \mathbb{N}$ odd and prime to $\text{char}(K)$.*

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

is exact.

We shall use an obvious consequence:

Corollary 6.2 *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. For all elements $a \in K^$ we have*

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

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

6.2 Application to Ring Class Numbers

Assume that the ideal \mathfrak{m} of O_K is given in a way which gives no information about the prime ideals dividing it. For simplicity we assume that \mathfrak{m} is square free .

We want to compute $h(\mathfrak{m})$, the order of the ideal class group of the order in K with conductor \mathfrak{m} .

$$K_{\mathfrak{m}} := \{a \in K; w_{\mathfrak{p}}(a - 1) \geq 1\}$$

for all $\mathfrak{p} \in T_{\mathfrak{m}}$.

Define the linear equation

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

Proposition 6.3 *Take any subset*

$$R \subset K_{\mathfrak{m}}$$

and an odd prime number l .

If $l \mid h(\mathfrak{m})$ then the system of linear equations

$$\mathcal{L}_R$$

given by

$$\{L_a; a \in R\}$$

has a non-trivial solution modulo l .

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.

Example 6.4 Take $K = \mathbb{Q}$, $m \in \mathbb{N}$.

Assume that $\ell \mid \varphi(m)$.

Let L be an extension of degree ℓ over \mathbb{Q} in $\mathbb{Q}(\zeta_m)$. We choose a random number k prime to m and take the generator σ of $G(L/K)$ induced by the exponentiation of ζ_m by k .

Let f_p such that $k^{f_p} \equiv p \pmod{m}$.

For $a = \prod p^{n_p}$ Theorem 6.1 yields

$$\sum_{p|m} \text{inv}_p A + \sum_{\gcd(p,m)=1} n_p f_p \equiv 0 \pmod{\ell} \quad (1)$$

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

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

6.3 Computation of the Classical DL

Let $\mathfrak{m} = \mathfrak{p}_0$ be a prime ideal of O_K with residue field \mathbb{F}_q and assume that there is a cyclic extension of K of degree ℓ totally ramified at \mathfrak{p}_0 .

Let ζ and ζ_1 be two ℓ -th roots of unity in \mathbb{F}_q that are the reduction modulo \mathfrak{p}_0 of two integers a and a_1 in O_K .

Proposition 6.5 *Let $k \in \mathbb{Z}$. Then $\zeta^k = \zeta_1$ if and only if*

$$k \left(\sum_{\mathfrak{p} \in \Sigma_K \setminus \{\mathfrak{p}_0\}} f_{\mathfrak{p}} w_{\mathfrak{p}}(a) \right) \equiv \sum_{\mathfrak{p} \in \Sigma_K \setminus \{\mathfrak{p}_0\}} f_{\mathfrak{p}} w_{\mathfrak{p}}(a_1) \pmod{\ell}.$$

6.4 Description of Cyclic Extensions

One of the main goals of algebraic number theory is the description of extension fields L of global fields K by objects defined over K . The most popular way to do this by giving polynomials fails if the degree of L is large. If we could compute for an extension L and a given prime \mathfrak{p} of O_K the number $f_{\mathfrak{p}}$ in an effective way for enough (*good estimate?*) \mathfrak{p} 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 .

7 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} .

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.

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

Take $K = \mathbb{Q}$. The congruence (1) can be seen as solution of a system of linear equations relating the variables f_p for p prime to m and $\text{inv}_p(A)$ 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 $c_0 = d^2 - m$.

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

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

8 Relations related to Abelian Varieties

The following is partly work in progress and mostly wishful thinking.

8.1 Finding 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 $\varphi \in H^1(G_K, A(K_s))[\ell]$. Then $T_\ell(P, \varphi)$ is an element in $Br(K)[\ell]$ which is very sparse.

At all places \mathfrak{p} prime to $\ell \cdot \text{cond}(A)$ at which a splitting field L of φ is unramified or at which the reduction of P lies in $\ell A(K_{\mathfrak{p}})$ the value of the local pairing is 0. Hence

$$\sum_{\mathfrak{p} \in S} \text{inv}_{\mathfrak{p}}(T_{\ell}(P \bmod \ell A(K_{\mathfrak{p}}), \varphi) = 0$$

with

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

Candidates for manageable A are elliptic curves with complex multiplication.

8.2 Lifting Local Pairings

Assume that we have $A_{\mathfrak{p}}$ over $K_{\mathfrak{p}}$ and $\varphi_{\mathfrak{p}} \in H^1(G_{\mathfrak{p}}, A_{\mathfrak{p}}(K_{\mathfrak{p},s}))$ and we want to compute the relative DL of two points $P_{\mathfrak{p}}, Q_{\mathfrak{p}}$.

We can try to lift the local data to global ones. If we succeed we have kind of “cohomological Xedni-algorithm”.

8.2.1 A Challenge for Heuristics

Assume that E is a CM-curve over \mathbb{Q} with two points $P, Q \in E(\mathbb{Q})$.

Assume that $\langle P, Q \rangle \pmod{\ell E(\mathbb{Q}_\ell)}$ is cyclic and that modulo a prime p the order of $\langle P, Q \rangle \pmod{\ell E(\mathbb{Q}_p)}$ is ℓ .

Assume that $[\mathbb{F}_p(\zeta_\ell) : \mathbb{F}_p] = \ell - 1$ (the “anti-MOV-case”).

Let P_ℓ be a point of order ℓ of E which is not rational over \mathbb{Q}_p , and assume that the class number of $\mathbb{Q}(P_\ell)$ is prime to ℓ (cf. Kummer regularity).

Then

$$P - kQ \in \ell E(\mathbb{Q}_p) \text{ iff } P - kQ \in \ell E(\mathbb{Q}_\ell).$$

Question 8.1 *How often can this situation occur?*