Tatra Mt. Math. Publ. **33** (2006), 199–227

Tatra Mountains
Mathematical Publications

ON THE RELATION BETWEEN BRAUER GROUPS AND DISCRETE LOGARITHMS

Gerhard Frey

ABSTRACT. In this article we want to make evident that Brauer groups of local and global fields play an important role in public key cryptography. In the first section we show that all ideal class groups resp. divisor class groups attached to curves over finite fields $\mathbb{F}_q$ taken into consideration for DL-systems can be mapped to such Brauer groups via the Tate-Lichtenbaum pairing. It is well known that this pairing applied to elements of order n can be computed with complexity polynomial in $|\mathbb{F}_q(\mu_n)|$ where μ_n is the group of roots of unity of order n. The image under this map leads to cyclic algebras over local fields with residue field $\mathbb{F}_q(\mu_n)$.

In the next section we study such algebras and explain the connection with discrete logarithms in finite fields as well as with elements in the Brauer group over global fields. This leads to a possibility to apply index-calculus methods described in the third section. As a result we get subexponential algorithms for the computation of discrete logarithms in finite fields as well as for the computation of the Euler totient function.

For the convenience of the reader we list the needed definitions and results about Galois cohomology groups in an appendix.

1. Discrete logarithms in ideal class groups

The aim of this section is to show that Brauer groups of local fields play a key role in cryptosystems based on discrete logarithms in ideal class groups of rings attached to curves over finite fields.

2000 Mathematics Subject Classification: 11R65, 11R37, 11R31.
Keywords: discrete logarithms in ideal class groups, Lichtenbaum pairing, invariants of local Brauer groups, index-calculus in global Brauer groups.

This article is based on a lecture given at the conference *WartaCrypt 2004*. The author would like to thank the organizers of the conference for generous support, an interesting program and last but not least for a very inspiring and pleasant atmosphere, and T. Lange for fruitful discussions on questions related to this work.

1.1 Realization of DL-systems

First we recall the definition of DL-systems.

1.1.1. Discrete logarithms.

Public key cryptosystems rely on one-way functions as crypto primitives. It is the task of mathematics to construct candidates f for such functions and to analyze possible attacks, i.e., to discuss the possibility of algorithms with low complexity which compute the inverse of f. In practice one uses nowadays two types of such primitives. In the RSA system the underlying mathematical problem is the computation of the Euler totient function φ which is, for given $m \in \mathbb{N}$, the number of elements in $\{1, \ldots, m\}$ which are prime to m. We shall come to this problem in Subsection 2.4.

Another elegant way to solve the main tasks of public key cryptography is to use discrete logarithms. We recall the definition in the cryptographically relevant situation.

Let ℓ be a prime number and G a group of an order ℓ such that the elements in G can be stored in a computer in a compact way (i.e., using only $O(\log(\ell))$ bits), and such that the group composition $\oplus$ is given by an algorithm which is easy to be implemented and which is very fast, i.e., has complexity $O(\log(\ell))$.

The discrete logarithm problem (for short called DLP) is: for randomly chosen elements $g_1, g_2 \in G$ compute a number $k \in \mathbb{Z}$ such that $[k]g_2 = g_1$.

The group G is cryptographically suitable[1] if the computation of discrete logarithms has a large complexity which makes the computation infeasible. In the ideal case this complexity would be $\exp(O(\log(\ell)))$. By generic methods (cf. [2]) we see that the DL can be computed in any group G with complexity $\exp O(1/2\log(\ell))$, and for black box groups one cannot do better. But there is no black box group available in the real world and so we have to look for groups G for which it can be hoped that the discrete logarithm is hard enough to provide the wanted security level. It is convenient to introduce the following function as a measure for complexities.

Definition 1.1. For $x \in \mathbb{N}$, $c \in \mathbb{R}_{>0}$ and $\alpha \in [0,1]$ define

$$L_x(\alpha, c) := \exp\Big(c\big(\log(x)\big)^{\alpha}\big(\log\log(x)\big)^{1-\alpha}\Big).$$

For $\alpha = 0$ we get that $L_x(0, c) = O(\log(x))$ is "polynomial" in $\log(x)$, and for $\alpha = 1$ we get that $L_x(1, c)$ is "exponential" in $\log(x)$. If $\alpha \in (0,1)$ we call $L_x(\alpha, c)$ *subexponential.*

[1] In this paper we shall not discuss protocols and more refined security issues which can be found in [1].

In our context we assume that x is closely related to ℓ, the order of G. So we are looking for groups G in which addition is polynomial in $\log(\ell)$ and the computation of the DL is exponential but in many cases we shall have to be content with a subexponential complexity. The purpose of the paper is to explain the structural background of this fact.

Remark 1.2. If the DLP has only subexponential complexity it does not mean that the system is insecure. It only means that the parameters of the system, and especially the size of p has to be chosen larger than in black box groups.

1.1.2 DL-systems in class groups.

Let O be a commutative noetherian ring with unit element 1 without zero divisors. Two ideals A, B of O can be multiplied:

$$A \cdot B = \left\{ \Sigma a_i \cdot b_i : a_i \in A,\, b_i \in B \right\}.$$

Clearly—is associative.

We generalize the notion of ideals slightly. Let F be the quotient field of O and $M \subset F$. The set M is an O-ideal if M is an O-module, and if there is an element $f \in F^*$ with $fM \subset O$. If we can take $f = 1$, then M is an ideal of O in the usual sense. We can multiply ideals in this generalized sense by using the definition made above for usual ideals. The ideal M is called invertible if there is an ideal M' with $M \cdot M' = O$. The set $I(O)$ of invertible ideals is a commutative group called the *ideal group* of O.

Definition 1.3. Let M_1, M_1 be elements of $I(O)$. M_1 is *equivalent* to M_2 ($M_1 \sim M_2$) if there is an element $f \in F^*$ with

$$M_1 = f \cdot M_2 .$$

$\mathrm{Pic}(O)$ is the set of equivalence classes of invertible ideals of O, it is an abelian group called the *ideal class group* of O.

The idea is to find suitable rings O such that $\mathbb{Z}/\ell$ can be embedded into $\mathrm{Pic}(O)$, the elements in $\mathrm{Pic}(O)$ can be described in a compact way, and the composition in the ideal class group has the complexity $O(\log(\ell))$.

There are only two types of rings O used today:

1. O is an order or a localization of an order in a number field, or
2. O is the ring of holomorphic functions of a curve defined over a finite field $\mathbb{F}_q$ with q elements.

We shall restrict ourselves to the second case but we remark that most of the consideration done in the following have analogues for the number field case.

1.2 Ideal classes of function rings

Let K be a field and F/K a (conservative) function field of one variable over K. Let C_O be an absolutely irreducible curve defined over K with function field F and let O be the ring of holomorphic functions on C_O. We assume that $\mathrm{Quot}(O) = F$ and so C_O is an affine curve. Let $\widetilde{C_O}$ be its desingularization with ring of holomorphic functions $\tilde{O}$. So O is contained in $\tilde{O}$ and $\tilde{O}$ is a Dedekind domain. There is a unique projective irreducible regular curve C with function field F containing $\widetilde{C_O}$ as an affine part. To see the geometric situation in terms of points better, we enlarge the ground field from K to K_s, the separable closure of K. For simplicity we assume that all singular points on C_O become rational over K_s. (In most applications K is perfect and so K_s is equal to the algebraic closure of K.) We denote by $\overline{C}$ the projective curve defined over K_s and obtained by constant field extension from K to K_s from C. Its function field is $\overline{F} = FK_s$.

The integral closure of O (resp. $\tilde{O}$) in $\overline{F}$ is denoted by $\overline{O}$ (resp. $\overline{\tilde{O}}$), it is the ring of holomorphic functions of the curve $\overline{C_O}$ (resp. $\overline{\widetilde{C_O}}$) obtained from C_O (resp. $\widetilde{C_O}$) by constant field extension.

The set of points rational over K_s of $\overline{C}$ contains the finite set T_∞ consisting of points not lying on $\overline{\widetilde{C_O}}$. Let S be the set of points on $\overline{\widetilde{C_O}}$ which correspond to singular points on $\overline{C_O}$. The Galois group G_K acts on points of $\overline{C}$. The sets T_∞ and S are mapped by G_K into themselves.

We assume from now on that there is a K-rational point $P_\infty \in T_\infty$. The singularities of $\overline{C_O}$ are reflected by the conductor $\mathfrak{m}_{\overline{O}}$ of $\overline{\tilde{O}}/\overline{O}$. In geometric language $\mathfrak{m}_{\overline{O}}$ corresponds to a divisor also denoted by $\mathfrak{m}_{\overline{O}}$ on $\overline{C}$ with support in S (cf. [6]). For cryptographical purposes it is sufficient to assume that the singular points are ordinary double points, and so $\mathfrak{m}_{\overline{O}} = \sum_{P \in S} P$.

Remark 1.4. $\mathfrak{m}_{\overline{O}}$ is invariant under the action of G_K and so it corresponds to an ideal in $\tilde{O}$ which is equal to the conductor of $\tilde{O}/O$.

Denote by $\overline{U_{T_\infty}}$ the functions in $\overline{F}$ which have no zeros or poles outside of T_∞. These functions are called T_∞-units. By $\overline{F_S^1}$ we denote the functions $f \in \overline{F}$ for which $f(P) = 1$ for all $P \in S$. Obviously both sets of functions are invariant under the natural G_K-action. The sets of fixed functions U_{T_∞} resp. F_S^1 lie in F. For a given integrally closed subring $R \subset \overline{F}$ with $\mathrm{Quot}(R) = \overline{F}$ and a function $f \in \overline{F}$ we denote by $(f)_R$ the ideal $f \cdot R$. For $H \subset \overline{F}$ we define $(H)_R = \{(f)_R \colon f \in H\}$. If it is clear which ring R is meant, we ease the notation and write (H) for $(H)_R$. The set $\left(\overline{F}^*\right)_R$ is called the group of principal ideals of R and is denoted by Princ_R.

EXAMPLES 1.5.

1. Take for R the ring $\overline{O_{P_\infty}}$ of meromorphic functions on $\overline{C}$ which have no poles outside of P_∞.
   Take $f \in \overline{F}^*$. For a point $P \in C$ denote by $v_P(f)$ the order of vanishing of f at P, i.e., the order of zero if f in P if f is holomorphic, and the negative of the order of the pole of f at P else. Let m_P be the ideal of functions in $\overline{O_{P_\infty}}$ which vanish at P. Then $(f)_R = \prod_{P \in C \setminus \{P_\infty\}} m_P^{v_P(f)}$.
2. We continue to take $R = \overline{O_{P_\infty}}$. Take the set of T_∞-units $\overline{U_{T_\infty}}$. It is well known that $(\overline{U_{T_\infty}})_R =: (\overline{U_{T_\infty}})$ is a $\mathbb{Z}$-sublattice in the group of ideals $\mathcal{D}_{T_\infty}$ in $I(\overline{O_{P_\infty}})$ generated by the ideals m_P corresponding to points $P \in T_\infty \setminus \{P_\infty\}$. Define
$$\mathcal{C}_{T_\infty} := \mathcal{D}_{T_\infty} / (\overline{U_{T_\infty}}).$$
3. Take for R the ring $\tilde{\overline{O}}$ and $f \in \overline{F}^*$. Then $(f)_R = \prod_{P \in C \setminus T_\infty} (m_P \cdot \tilde{\overline{O}})^{v_P(f)}$.

By definition we have the exact sequence of Galois modules
$$1 \to \mathrm{Princ}_R \to I(R) \to \mathrm{Pic}(R) \to 0,$$
and by using the approximation theorem we get the exact sequence of G_K-modules
$$0 \to \mathcal{C}_{T_\infty} \to \mathrm{Pic}(\overline{O_{P_\infty}}) \to \mathrm{Pic}(\tilde{\overline{O}}) \to 0.$$
Next we want to describe $\mathrm{Pic}(\overline{O})$. Let $I'(\overline{O})$ be the group generated by ideals of $\overline{O}$ which are prime to $\mathfrak{m}_{\overline{O}}$. Then $(\overline{F_S^1})$ is contained in $I'(\overline{O})$ and we get the exact sequence of G_K-modules
$$1 \to (\overline{F_S^1}) \to I'(\overline{O}) \to \mathrm{Pic}(\overline{O}) \to 0.$$
Using the approximation theorem for functions in $\overline{F}$ we get:

1. In every class $c \in \mathrm{Pic}(\tilde{\overline{O}})$ there is an ideal which is prime to S. So we have a natural surjective map $\varphi\colon \mathrm{Pic}(\overline{O}) \to \mathrm{Pic}(\tilde{\overline{O}})$ which is G_K-invariant.
2. The kernel of φ is in a canonical way isomorphic to $\prod_{P \in S} (K_s^*)_P / \Delta(K_s^*)$ where G_K acts on $\prod_{P \in S} (K_s^*)_P$ by $\sigma(\ldots, x_P, \ldots) = (\ldots, \sigma(x_P)_{\sigma(P)}, \ldots)$ and $\Delta(K_s^*)$ is the diagonal embedding.

A more geometric way to express this is

PROPOSITION 1.1. *There is a torus T_S of dimension $|S|-1$ defined over K such that we have the exact sequence of G_K-modules*

$$1 \to T_S(K_s) \to \mathrm{Pic}(\overline{O}) \to \mathrm{Pic}(\tilde{\overline{O}}) \to 0\,.$$

Remark 1.6. The isomorphism class of T_S is determined by its character group X, and this group is determined by the set S as G_K-set. So Proposition 1.1 (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.

In Proposition 1.1 we have described the relation between ideal classes of rings $\overline{O}$ and their desingularization $\tilde{\overline{O}}$. Now we investigate the relation between $\mathrm{Pic}(\tilde{\overline{O}})$ and the points on the Jacobian variety J_C of C. Divisors D of $\overline{C}$ (or of $\overline{F}$) are formal sums with integer coefficients

$$D = \sum_{P \in \overline{C}} z_P \cdot P$$

with almost all $z_P = 0$. Using formal addition the set of divisors forms a group denoted by $\mathcal{D}$. The degree of D is $\deg(D) = \sum_{P\in\overline{C}} z_P$. The subgroup $\mathcal{D}^0$ consists of the divisors of $\overline{C}$ of degree 0. It contains the group of principal divisors (f) attached to functions $f \in \overline{F}^*$ in the following way:

$$(f) = \sum_{P \in C(\overline{K})} v_P(f) P\,,$$

where $v_P(f)$ is as above the order of zero or the negative of the order of pole of f in the point P. The quotient is the divisor class group of degree 0 of $\overline{C}$ (or of $\overline{F}$) denoted by $\mathrm{Pic}^0(\overline{C})$. The connection to the ideal class groups considered above is given by

LEMMA 1.1. *There is a natural group isomorphism from $\mathcal{D}^0$ to $I(\overline{O_{P_\infty}})$ given by the map φ_{P_∞} sending the divisor $D = \sum_{P\in\overline{C}} z_P \cdot P$ to the ideal $\prod_{P\in\overline{C}\setminus\{P_\infty\}} m_P^{z_P}$. In this way, φ_{P_∞} maps principal divisors of $\overline{F}K$ to $\mathrm{Princ}_{\overline{O_{P_\infty}}}$ and induces an isomorphism between $\mathrm{Pic}^0(\overline{C})$ and $\mathrm{Pic}(\overline{O_{P_\infty}})$ which is compatible with the action of G_K.*

To prove this lemma we observe that every ideal M of $\overline{O_{P_\infty}}$ is given in a unique way as $M = \prod_{P\in\overline{C}\setminus\{P_\infty\}} m_P^{z_P}$ and the inverse image of M under φ is

$$D = \sum_{P\in\overline{C}\setminus\{P_\infty\}} z_P \cdot P - \left(\sum_{P\in\overline{C}\setminus\{P_\infty\}} z_P \right) \cdot P_\infty\,.$$

Corollary 1.1. *We have the exact sequence of G_K-modules*

$$0 \to \mathcal{C}_{T_\infty} \to J_C(K_s) \to \operatorname{Pic}(\overline{\tilde{O}}) \to 0\,.$$

1.3 The Lichtenbaum pairing

We continue to work with rings O resp. $\overline{O}$ as in Subsection 1.2. We begin with the case that $S = \emptyset$ and $T_\infty = \{P_\infty\}$ and so $\overline{O} = \overline{O_{P_\infty}}$. In this case we have that $\operatorname{Pic}(\overline{O})$ is as G_K-module isomorphic to $J_C(K_s)$. We use the exact sequence

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

and get as a part of the long exact cohomology sequence the exact sequence

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

We remark that $I(\overline{O})$ is a direct sum of copies of G_K-submodules isomorphic to $\mathbb{Z}[\overline{G}]$ with $\overline{G}$ a finite quotient group of G_K and so $H^1\big(G_K, I(\overline{O})\big) = 0$. The same remark applies to the more general ideal groups we were looking at in Subsection 1.2. So the map δ^1 is injective. As described in the appendix it is given explicitly by the following rule: Take $c \in H^1\big(G_K, \operatorname{Pic}(\overline{O})\big)$ and represent it by a cocycle

$$\zeta\colon G_K \to \operatorname{Pic}(\overline{O}) \quad \text{with} \quad \zeta(\sigma) = \bar{D}(\sigma)\,,$$

where $\bar{D}(\sigma)$ is an ideal class with a (chosen) representative $D(\sigma) \in I(\overline{O})$. Then for all $\sigma_1, \sigma_2 \in G_K$ the ideal

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

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

$$\gamma\colon (\sigma_1, \sigma_2) \mapsto \big(f(\sigma_1, \sigma_2)\big)\,.$$

We have some choices. For instance we can change $D(\sigma)$ by a principal ideal. So for a given ideal $A \in I(O)$ we can and will choose $D(\sigma)$ such that the $\overline{O}$-ideals $\sigma_1 D(\sigma_2)$ and $A \cdot (\overline{O})$ are relatively prime for all $\sigma_1, \sigma_2 \in G_K$. As a result the function $f(\sigma_1, \sigma_2)$ has neither zeros nor poles in points $P \in C$ for which the ideal m_P occurs with non-zero multiplicity z_P in $A\overline{O} = \prod_{P \in C \setminus P_\infty} m_P^{z_P}$.

Assume that $\sum_{P \in C \setminus P_\infty} z_P = 0$. Then $\prod_{P \in C \setminus P_\infty} f(\sigma_1, \sigma_2)(P)^{z_P}$ is defined and independent of the choice of $f(\sigma_1, \sigma_2)$ in its divisor class.

Definition 1.7. The *Lichtenbaum pairing* (cf. [3])

$$T_L\colon \operatorname{Pic}(O_{P_\infty}) \times H^1\big(G_K, \operatorname{Pic}(\overline{O_{P_\infty}})\big) \to H^2(G_K, K_s^*)$$

is defined in the following way: In the class $\bar D \in \operatorname{Pic}(O)$ choose an ideal A such that $A\overline{O} = \prod_{P \in C\setminus P_\infty} m_P^{z_P}$ with $\sum_{P\in C\setminus P_\infty} z_P = 0$. For the class $c \in H^1\big(G_K, \operatorname{Pic}(\overline{O_{P_\infty}})\big)$ make choices as described above such that for all $\sigma_1, \sigma_2 \in G_K$ the class $\delta^1(c)$ is presented by a cocycle $\big(f(\sigma_1,\sigma_2)\big)$ prime to A. Then

$T_L(\bar D, c)$ is the cohomology class of the cocycle $\zeta(\sigma_1,\sigma_2) = \prod_{P\in C\setminus P_\infty} f(\sigma_1,\sigma_2)(P)^{z_P}$.

Remark 1.8. There is a close connection of the Lichtenbaum pairing with the *Tate pairing* which uses the duality of the group of torsion points on Jacobian varieties (via the Weil pairing) to get for all natural numbers n a pairing

$$T_n\colon J_C(K)/nJ_C(K) \times H^1\big(G_K, J_C(K_s)\big)[n] \to H^2(G_K, K_s^*)[n]\,.$$

Lichtenbaum proves in [3] that the pairing T_L induces "on the level modulo n" the Tate pairing up to a sign. We shall denote the resulting pairing T_n as *Tate-Lichtenbaum pairing.* The Tate pairing is defined in a more general frame. In fact it is a pairing defined for abelian varieties A with dual abelian variety $\hat A$ and mapping $A(K)/nA(K) \times H^1\big(G_K, \hat A(K_s)\big)[n]$ to $H^2(G_K, K_s^*)[n]$. For the definition see [1].

We can use this remark to see what is happening if T_∞ is not equal to $\{P_\infty\}$, but contains more elements. In Subsection 1.2 we have found the exact sequence

$$0 \to \mathcal{C}_{T_\infty} \to \operatorname{Pic}(\overline{O_{P_\infty}}) \xrightarrow{\varphi} \operatorname{Pic}(\overline{\tilde O}) \to 0\,.$$

We want to define an analogue of the Lichtenbaum pairing for $\operatorname{Pic}(\tilde O)$ resp. $H^1\big(G_K, \operatorname{Pic}(\overline{\tilde O})\big)$, but we encounter two difficulties. First it is not true in general that $H^0\big(G_K, \operatorname{Pic}(\overline{\tilde O})\big)$ is equal to the group $\operatorname{Pic}(\tilde O) = \varphi\big(\operatorname{Pic}(O_{P_\infty})\big)$ in which we want to realize a DL-system. Secondly the map from $\bar F$ to $\operatorname{Princ}_{\overline{\tilde O}}$ has the group of functions U_{T_∞} as a kernel. Hence we cannot evaluate the image of $\delta^1\colon H^1\big(G_K, \operatorname{Pic}(\overline{\tilde O})\big) \to H^2(G_K, \operatorname{Princ}_{\overline{\tilde O}})$ at points on $C \setminus T_\infty$. To overcome these difficulties we look at the sequence

$$H^1(G_K, \mathcal{C}_{T_\infty}) \to H^1\big(G_K, \operatorname{Pic}(\overline{O_{P_\infty}})\big) \xrightarrow{\varphi} H^1\big(G_K \operatorname{Pic}(\overline{\tilde O})\big)\,.$$

We would like to lift elements from $H^1\big(G_K \operatorname{Pic}(\overline{\tilde O})\big)$ to $H^1\big(G_K, \operatorname{Pic}(\overline{O_{P_\infty}})\big)$ and then use the Lichtenbaum recipe from above. The kernel $\mathcal{C}_{T_\infty}$ of φ is a finitely generated $\mathbb{Z}$-module. A straightforward computation shows that the interesting case that the $\mathcal{C}_{T_\infty}$ is finite. We denote its order by n. We can interpret $\mathrm{Pic}(\overline{\tilde{O}})$ as the group of K_s-rational points of the abelian variety $A = J_C/\mathcal{C}_{T_\infty}$ which is defined over K and isogenous to J_C. There is a map $\psi\colon A \to J_C$ with $\mathcal{C}'_{T_\infty} = \mathrm{kernel}(\psi) = \varphi(J_C[n])$. So we have a map

$$\psi^1\colon H^1(G_K, A(K_s)) \to H^1(G_K, J_C(K_s))$$

whose kernel is a quotient of $H^1(G_K, \mathcal{C}'_{T_\infty})$. We use now the fact that the Lichtenbaum pairing restricted to elements of order n in $H^1(G_K, J_C(K_s))$ resp. $A(K)/nA(K)$ is the Tate pairing and the functoriality of the Weil pairing to get

Lemma 1.2. *The group $\varphi(J_C(K))$ is orthogonal to the image of $H^1(G_K, \mathcal{C}'_{T_\infty})$ in $H^1(G_K, A(K_s))[n]$ under the Tate pairing.*

Corollary 1.2. *The Lichtenbaum pairing induces a pairing, also denoted by T_L from $\mathrm{Pic}(\tilde{O}) \times \psi^1(H^1(G_K, \mathrm{Pic}(\overline{\tilde{O}})))$ to $H^2(G_K, K_s^*)$.*

To come to the most general situation we have to do the last step and allow singularities in the set S. To make things not too complicated we assume that $T_\infty = \{P_\infty\}$. We recall the exact sequence

$$1 \to T_S(K_s) \to \mathrm{Pic}(\overline{O}) \to \mathrm{Pic}(\overline{O_{P_\infty}}) \to 0\,,$$

where T_S is a torus determined by the conductor $\sum_{P\in S} P$ and $\mathrm{Pic}(\overline{O_{P_\infty}}) = J_C(K_s)$. From this sequence we get the exact sequence

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

and since $H^1(G_K, T_S(K_s)) = 0$ by Hilbert's Theorem 90 we have the exact sequence

$$1 \to T_S(K) \to \mathrm{Pic}(O) \to J_C(K_s) \to 0$$

as well as

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

We can apply δ^1 to $H^1(G_K, \mathrm{Pic}(O))$ and we get a pairing as above but we cannot expect to get any information about $T_S(K)$. We shall show in the next subsection how one can overcome this difficulty in the case relevant for cryptography.

1.4 The Tate-Lichtenbaum pairing for Picard groups of curves over finite fields

The interesting case for applications in cryptography is that the ground field is a finite field $\mathbb{F}_q$ with $q = p^d$. The Galois group $G_{\mathbb{F}_q}$ is generated as a topological group by ϕ_q, the Frobenius automorphism of $\mathbb{F}_q$, acting by exponentiation by q.

From our point of view the disappointing fact is that all cohomological groups $H^n(G_{\mathbb{F}_q}, M)$ are trivial for $n > 1$ and so the Lichtenbaum pairings considered in Subsection 1.3 are trivial. The way out is *to lift* our objects to local fields K with residue field $\mathbb{F}_q$ and normed valuation $w_{\mathfrak{p}}$ and their separable closures which are either fields of Laurent series with coefficients in $\overline{\mathbb{F}_q}$ or the algebraic closure of the unramified extension of $\mathbb{Q}_p$ of degree d. 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. This automorphism generates the Galois group of K_{unr}/K as a topological group. Algebraic extensions of K_{unr} are totally ramified. We are interested in *tamely* ramified extensions. Let n be a natural number prime to p. Then there is exactly one tamely ramified extension L_n of K_{unr} of degree n given explicitly by $L_n = K_{\mathrm{unr}}(\pi^{1/n})$ where π is an element in K with $w_{\mathfrak{p}}(\pi) = 1$. (Such elements are called *uniformizing elements* of K.) So L_n/K_{unr} is cyclic. We choose a primitive nth root of unity ζ_n and denote by τ_n the generator of the Galois group of L_n/K_{unr} which maps $\pi^{1/n}$ to $\zeta_n \cdot \pi^{1/n}$. It follows that L_n is a Galois extension of K whose group is generated by ϕ_q and τ_n. If we assume that $\zeta_n \in K$, or equivalently, 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}. The converse statement holds, too. In particular, there is a totally and tamely ramified extension of K cyclic of degree n if and only if $\zeta_n \in K$.

Next we lift the curves which gave the geometric background for the ideal class groups we are interested in. We begin with the observation that the study of the discrete logarithm in the elements of order n in finite abelian groups M is equivalent with the study of the discrete logarithm in $M/[n]M$, the group obtained by taking the quotient of M by the image obtained by scalar multiplication by n.

We recall the definitions in Subsection 1.2 for the case that the ground field is $\mathbb{F}_q$. We began with the ring O which is the ring of holomorphic functions of an affine curve C_O defined over $\mathbb{F}_q$. There was a set of singular points S defining the conductor $\mathfrak{m}_O = \sum_{P \in S} P$ and the corresponding desingularized curve $\tilde{C}$ embedded in the projective nonsingular curve C. The set T_∞ was defined as $C(\overline{\mathbb{F}_q}) \setminus \tilde{C}(\overline{\mathbb{F}_q})$. We denote by g_0 the genus of C. We state the following (rather elementary) facts from the reduction theory of curves resp. abelian varieties.

Theorem 1.1. *1. There is a projective absolutely irreducible nonsingular curve C^l defined over K and a set T^l_∞ of points in $C^l(\overline{K})$ with the following properties.*

- *The genus of C^l is equal to $g_0 + |S| - 1$.*

- *The reduction of the affine curve $C^l \setminus T^l_\infty$ modulo the maximal ideal of K is equal to C_O.*
- *There is a K-rational point P^l_∞ which is mapped to P_∞*
- *The set T^l_∞ is G_K-invariant. It is mapped bijectively to T_∞.*

2. Denote by O^l the ring of holomorphic functions on $C^l \setminus T^l_\infty$. For all numbers n prime to q we get

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

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

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

3. For $T_\infty = \{P_\infty\}$ we get that

$$J_{C^l}(K)/[n]J_{C^l}(K) \text{ is canonically isomorphic to } \operatorname{Pic}(O)/[n]\operatorname{Pic}(O)\,.$$

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

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

Moreover, there is an isogeny φ from J_{C^l} over K with kernel isomorphic to $\mathcal{C}_{T_\infty}$ such that $\operatorname{Pic}(O)/[n]\operatorname{Pic}(O)$ is isomorphic to $\varphi\big(J_C(K)\big)/[n]\varphi\big(J_C(K)\big)$.

Theorem 1.1 enables us to study all crypto systems based on ideal classes of curves over finite fields by using the cohomology theory of local fields. In practice the situation will be much simpler. For instance the curve C will be either nonsingular (the case of good reduction) or will have genus equal to zero (the toric case). Moreover the set of missing points will consist in important cases (e.g., in the case of C_{ab}-curves) of just 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. Instead of proving the statements of Theorem 1.1 we give the simplest example for these curves.

Example 1.9. Let p be odd. We begin with the affine curve

$$C_O\colon Y^2 + XY = X^3$$

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

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

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 2 points (we have two different tangents at this point) on the desingularization. It follows that $\mathrm{Pic}(O)$ is isomorphic to $\mathbb{F}_q^*$. Let K be a local field with residue field $\mathbb{F}_q$ and uniformizing element π. Then

$$C^{\,l} := E\colon Y^2 - XY = X^3 + \pi$$

is the affine part of an elliptic curve with reduction equal to C. It is a Tate curve with period Q with $w_{\mathfrak{p}}(Q) = 1$. The group of rational points $E(K)$ is isomorphic to $K^*/\langle Q\rangle \cong U_K$, and all the assertions of the Theorem 1.1 can be checked immediately.

Next we apply the Lichtenbaum pairing (see Definition 1.7) to the divisor class group of $C^{\,l}$ (or, equivalently, to $\mathrm{Pic}(O^{\,l})$) and get the pairing

$$T_L\colon\ \mathrm{Pic}(O^l_{P^l_\infty}) \times H^1(G_K, \mathrm{Pic}(\overline{O^l_{P^l_\infty}})) \to H^2(G_K, K_s^*)\,.$$

For numbers n prime to q this pairing induces a pairing

$$T_n\colon\ \mathrm{Pic}(O^l_{P^l_\infty})/[n]\,\mathrm{Pic}(O^l_{P_\infty{}^l}) \times H^1(G_K, \mathrm{Pic}(\overline{O^l_{P_\infty{}^l}}))[n] \to H^2(G_K, K_s^*)[n]\,.$$

Theorem 1.2. *The Tate-Lichtenbaum pairing T_n is nondegenerate.*

Corollary 1.3. *Assume that D_n is a cyclic subgroup of $\mathrm{Pic}(O^l_{P^l_\infty})/[n]$ $\mathrm{Pic}(O^l_{P_\infty{}'^l})$. Then there is an element $c \in H^1(G_K, \mathrm{Pic}(\overline{O^l_{P^l_\infty}}))[n]$ such that the restriction $T_n\big|_{D_n\times\{c\}}$ is a monomorphism. Hence the discrete logarithm in D_n is transferred to the discrete logarithm in $H^2(G_K, K_s^*)[n]$ with costs arising from the complexity of computing $T_n\big|_{D_n\times\{c\}}$.*

Using the results stated in Theorem 1.1 and the discussions in Subsection 1.7 we get

Theorem 1.3. *The discrete logarithm in ideal classes of rings of holomorphic functions of affine curves C is transferred to $H^2(G_K, K_s^*)$ by the Tate-Lichtenbaum pairings T_n.*

Remarks 1.10.

1. By lifting curves from finite fields to local fields we get the nontriviality of cohomology groups involved in the pairings as well as a smoothing of the curve. We do not loose information about the torus part of the ideal class groups. The reason is that we have ramified extensions at hand.

2. Of course the practical value of Corollary 1.3 depends on two assumptions: the pairings T_n have to have low computational complexity *and* the discrete logarithm in $H^2(G_K, K_s^*)$ has to be weak enough. The first task needs (at least today) the assumption that $n \mid (q-1)$. The reason is that only in this case we have ramified extensions cyclic of degree n defined over K. The second assumption will be discussed in the following sections.
3. We do not go into details about the explicit computation of the Tate-Lichtenbaum pairing but refer to [1].

2. The Brauer group

In the last Section we have motivated the importance of the second cohomology group of the multiplicative group of local fields. Now we want to study these groups in detail.

2.1 Definition and first properties of Brauer groups

Let K be a field.

Definition 2.1. The *Brauer group* of K is the cohomology group $H^2(G_K, K_s^*)$. It is denoted by $\mathrm{Br}(K)$. The elements of $\mathrm{Br}(K)$ with order dividing n are denoted by $\mathrm{Br}(K)[n]$.

By definition $\mathrm{Br}(K)$ consists of the classes of 2-cocycles of G_K with values in K_s^* modulo 2-coboundaries. One can interpret these classes as classes of simple K-algebras with center K. The addition in the cohomology group corresponds to the tensor product. The unit element in $\mathrm{Br}(K)$ corresponds to the class of full matrix algebras. Let L be a separable extension field of K, and let A be an algebra representing an element $c \in \mathrm{Br}(K)$. Then $A \otimes_K L$ represents a class c_L in $\mathrm{Br}(L)$. It is not difficult to see that $c_L = \mathrm{res}_{K/L}(c)$.

As a consequence of Hilbert's Theorem 90 we get that for Galois extensions L/K the inflation map from $H^2\big(G(L/K), L^*\big)$ to $H^2(G_K, K_s^*)$ is injective and that the kernel of the restriction map $\mathrm{res}_{K/L}$ is $H^2\big(G(L/K), L^*\big)$. So we can study the Brauer group of K by looking at classes of simple K-algebras A with center K, for with $A \otimes_K L$ is a full matrix algebra for some finite Galois extensions L of K.

It is especially interesting to look at the case that L/K is a cyclic extension of degree n which we assume from now on. Algebras corresponding to elements in $H^2\big(G(L/K), L^*\big)$ are called *cyclic* algebras. It is a general fact that (Tate) cohomology groups of cyclic groups are periodic with period 2 and so $H^2\big(G(L/K), L^*\big) \cong K^*/N_{L/K}(L^*)$. This isomorphism is made explicit in the following way: Let σ be a generator of $G(L/K)$ and take a in K^*. The map $f_{\sigma,a}\colon G\times G\to L^*$, given by

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

is a 2-cocycle and its class determines an element in $\mathrm{Br}(K)[n]$. For two elements a, a' 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 $(L,\sigma,a\cdot N_{L/K}L^*)$. We remark that the relative Brauer group $\mathrm{Br}(L/K)$ can be described completely in terms of the ground field K.

Proposition 2.1. *Let L/K be Galois with cyclic Galois group $G=\langle\sigma\rangle$ of order n. Then the map $\phi\colon a\mapsto(L,\sigma,a)$ induces an isomorphism*

$$\overline{\phi}\colon K^*/N_{L/K}(L^*)\xrightarrow{\sim}\mathrm{Br}(L/K)\,.$$

2.2 Brauer groups of local fields

In Section 1 we have seen that the discrete logarithm in the group of elements of order dividing n in ideal class groups of curves defined over finite fields $\mathbb{F}_q$ is linked via the Tate-Lichtenbaum pairing to the discrete logarithm in $\mathrm{Br}(K)[n]$ with K a local field with normed valuation v and residue field $\mathbb{F}_q$. To compute this pairing explicitly one needs, at least at present, that K contains the nth roots of unity. In this case the result of the pairing is a cyclic algebra of order n attached to "the" totally ramified extension L_n of degree n of K (see [1]) i.e., it is given by a cocycle c whose class is determined by a triple $\bigl(L_n,\tau,a\cdot N_{L_n/K}(L_n^*)\bigr)$ where τ is a generator of $G(L_n/K)$. It is easy to check that $K^*/N_{L_n/K}(L_n^*)\cong\mathbb{F}_q^*/\mathbb{F}_q^{*n}$ and so, having fixed τ, the class of c is determined by an element in $\mathbb{F}_q^*/\mathbb{F}_q^{*n}$.

Theorem 2.1. *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 $\mathbb{F}_q^*/\mathbb{F}_q^{*n}$.*

By taking $n=q-1$ we see that the discrete logarithm in $\mathbb{F}_q^*$ is transferred to the discrete logarithm in $H^2\bigl(G(L_{q-1}/K),L_{q-1}^*\bigr)$. This is a cyclic group of order $q-1$, and a key result of class field theory of K is that $\mathrm{Br}(K)[n]$ is cyclic of order n (cf. Theorem 2.2). Hence $H^2\bigl(G(L_{q-1}/K),L_{q-1}^*\bigr)=\mathrm{Br}(K)[q-1]$.

Question 2.2. *Can one find in an effective way in a given class of algebras in $\mathrm{Br}(K)[n]$ a cyclic algebra split by L_n?*

2.2.1 Invariants.

From now on we assume n to be fixed with $n \mid q-1$. Let L_u be the unique unramified extension of K of degree n. Its Galois group over K has as a canonical generator a lift of the Frobenius automorphism of $\mathbb{F}_q$ which we denote by ϕ_q. Assume that c is given by a cocycle corresponding to a cyclic algebra split by L_u. Since now both L_u and ϕ_q are canonically given we can characterize c in a canonical way by a triple $\left(L_u,\, \phi_q,\, a \cdot N_{L_u/K}(L_u^*)\right)$. Since $U(K)$ is in the image of the norm map we get that $K^*/N_{L_u/K}(L_u^*) \cong \langle\pi\rangle/\langle\pi^n\rangle$ where π is a uniformizing element of K. So the class of c is uniquely determined by $v(a) \bmod n$.

Definition 2.3. Let $c \in H^2\left(G(L_u/K), L_u^*\right)$ be given by the triple (L_u, ϕ_q, a). Then $v(a) \in \mathbb{Z}/n\mathbb{Z}$ is the *invariant* $\operatorname{inv}_K(c)$ of c.

It is obvious that the discrete logarithm in $H^2\left(G(L_u/K), L_u^*\right)$ 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 2.1. *Assume that τ is another generator of $G(L_u/K)$, and c is given by the triple (L_u, τ, a). Let $f \in \mathbb{Z}$ be such that $\tau^f = \phi_q$. Then $\operatorname{inv}(c) = f \cdot v(a) \bmod n$.*

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

Example 2.4. Assume that $L_u = K(\alpha)$ with $\alpha^n \in U(K)$ such that $\tau(\alpha) = \beta\cdot\alpha$ with $\beta \in K$. Then $\tau^f = \phi_q$ if and only if $\beta^f \equiv \alpha^{q-1}$ modulo the maximal ideal of K. So we have to solve a discrete logarithm problem in $\mathbb{F}_q$.

Theorem 2.2. *Every element of c in $\operatorname{Br}(K)[n]$ (resp. every central simple algebra A over K) is equivalent to a cyclic algebra split by L_u. So we can associate to c (resp. A) its invariant and we get an isomorphism*

$$\operatorname{inv}_K\colon\ \operatorname{Br}(K)[n] \to \mathbb{Z}/n\,.$$

Corollary 2.1. *Assume that $n \mid (q-1)$. Then*

$$H^2\left(G(L_n/K), L_n^*\right) = \operatorname{Br}(K)[n] = H^2\left(G(L_u/K), L_u^*\right).$$

The discrete logarithm in $\operatorname{Br}(K)[n]$ would be trivial if we could compute invariants. We have already seen that even for cyclic algebras split by unramified extensions this is as difficult as computing the discrete logarithm in $\mathbb{F}_q$. If c is split by a totally ramified extension, the situation is even more complicated but it can be verified that discrete logarithms in $\mathbb{F}_q$ have to be computed again. Details can be found in [5].

2.3 The local-global relation

We go one step further and lift 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 $\mathbb{F}_q$.

2.3.1 Localization.

Let v be a non-archimedean valuation on K. Let $\tilde{v}$ be an extension of v to K_s. Let $K_{(\tilde{v})}$ be the Henselization of K with respect to $\tilde{v}$, i.e., $K_{(\tilde{v})}$ is the smallest subfield of K_s containing K over which Hensel's lemma holds for all polynomials, or equivalently, the restriction of $\tilde{v}$ to $K_{(\tilde{v})}$ has exactly one extension (namely $\tilde{v}$) to K_s. The Galois group $G_{K_{(\tilde{v})}}$ is characterized by

$$G_{K_{(\tilde{v})}} = \{\sigma \in G_K : \sigma \text{ acts continuously on } K_s \text{ w.r.to the topology induced by } \tilde{v}\}.$$

For shortness we denote $G_{K_{(\tilde{v})}}$ by $G_{\tilde{v}}$ or, whenever $\tilde{v}$ is fixed, by G_v. Changing $\tilde{v}$ induces a conjugation of $G_{K_{(\tilde{v})}}$ with an element in G_K. The group G_v is called the decomposition group of $\tilde{v}$ resp. v.

Remark 2.5. Let K_v be the completion of K with respect to the topology induced by v on K. First we observe that it is equal to the completion of $K_{(\tilde{v})}$ with respect to the valuation $\tilde{v}|_{K_{(\tilde{v})}}$. Next we can and will identify $G_{\tilde{v}}$ with G_{K_v}, since every automorphism on K_s which is continuous with respect to the topology induced by $\tilde{v}$ has a unique continuous extension to the completion of K_s which fixes K_v and which maps the algebraic closure of K_v onto itself. This identification is canonical if $\tilde{v}$ is chosen which we shall assume in future.

The field K_v is called the localization of K at v. In fact K_v depends only on the equivalence class $\mathfrak{p}$ of the valuation v and hence is denoted by $K_{\mathfrak{p}}$. This equivalence class is called a (non-archimedean) *place* of K. The decomposition group of v (or more precisely, of a chosen extension of v), depends up to conjugation only on $\mathfrak{p}$ and is denoted by $G_{\mathfrak{p}}$. The set of all places of K is denoted by Σ_K. A G_K-module M has (by restriction) a natural structure as a $G_{\mathfrak{p}}$-module and so we have restriction maps

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

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

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

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

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

We have the most important exact sequence due to Hasse–Brauer–Noether.

Theorem 2.3. *Let K be a global field and $n \in \mathbb{N}$ odd and prime to* $\mathrm{char}(K)$. *Then the sequence*

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

is exact.

For a proof see [4]. A trivial, but useful consequence of Theorem 2.3 is

Corollary 2.2. *Let T be a finite set of places of K. For each $\mathfrak{p} \in T$ let $A_\mathfrak{p}$ be a given cyclic algebra corresponding to $c_\mathfrak{p} \in \mathrm{Br}(K_\mathfrak{p})[n]$. For every simple algebra A with center K of order n in $\mathrm{Br}(K)$ with $A \bigotimes K_\mathfrak{p} \cong A_\mathfrak{p}$ for $\mathfrak{p} \in T$ we get*

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

Remark 2.6. For the existence of *cyclic* lifts A of $A_\mathfrak{p}$ we need *existence theorems* for cyclic extensions of K with prescribed ramification, and such results are delivered by *global class field theory* (in an explicit way, e.g., by CM theory).

Let $\mathfrak{m}$ be an ideal in O_K, the ring of integers of K. We *assume* that there is a cyclic extension L of odd degree n of K 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 $a \in K^*$ define the cyclic algebra A given by the triple (L, τ, a). Using Theorem 2.3 and Lemma 2.1 we get

Proposition 2.2. *For all $\mathfrak{p} \in \Sigma_K$ there are numbers $f_\mathfrak{p}$ such that for all elements $a \in K^*$ we have*

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

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

2.4 Application to ring class numbers

We want to apply Proposition 2.2 to the following problem: 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 squarefree (this is the relevant case for practical purposes). We want to compute the order $\varphi(\mathfrak{m})$ of the ring class group of O_K with module $\mathfrak{m}$, i.e., the number of elements in the ideal class group of the order in K with conductor $\mathfrak{m}$. Define $K_{\mathfrak{m}}$ as a subgroup in K^* consisting of the elements $a \in K^*$ prime to $\mathfrak{m}$ and for which $\sum_{\mathfrak{p}\in T_{\mathfrak{m}}} \mathrm{inv}_{\mathfrak{p}}\big(\rho_{\mathfrak{p}}(A)\big) = 0$ for all cyclic algebras A corresponding to a which are split by extensions of K with conductor $\leqslant \mathfrak{m}$. A subset of $K_{\mathfrak{m}}$ are the elements a in K for which $w_{\mathfrak{p}}(a-1) \geqslant 1$ for all $\mathfrak{p} \in T_{\mathfrak{m}}$.

Proposition 2.3.

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

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

   has a non-trivial solution modulo l.

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

Remark 2.7. There are reasonable bounds for the size of $\varphi(\mathfrak{m})$ in terms of the norm of $\mathfrak{m}$, and so knowing a number whose prime divisors include the prime divisors of $\varphi(\mathfrak{m})$ one can determine a power of this number which is a multiple of $\varphi(\mathfrak{m})$. In most applications (e.g., to RSA-like schemes) this is already sufficient. In many concrete cases it will be possible to determine $\varphi(\mathfrak{m})$ in the situation of Proposition 2.3 exactly.

Example 2.8. Take $K = \mathbb{Q}$. First $\Sigma_{\mathbb{Q}}$ is identified with the primes l in $\mathbb{Z}$. For $m \in \mathbb{N}$ the function $\varphi(m)$ is the classical Euler totient function. The global class field theory of $\mathbb{Q}$ is completely determined by the theorem of Kronecker and Weber.

Theorem 2.4. (Kronecker–Weber) *Every abelian extension $K/\mathbb{Q}$ of $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. The class group with respect to the conductor $m\mathbb{Z}$ has order $\varphi(m)$. There exists an extension $L/\mathbb{Q}$ of prime degree l with conductor dividing m if and only if $l \mid \varphi(m)$.*

We now assume that the prime number ℓ divides $\varphi(m)$, and consider a global algebra A of the form $A = (L/\mathbb{Q}, \sigma, a)$ corresponding to this extension with a prime to m. To be explicit we choose a random number $1 < k < m$ and assume that the exponentiation of mth roots of unity by k induces σ on L. For $a = \prod p^{n_p}$ the theorem by Hasse–Brauer–Noether leads to a relation of the form

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

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

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

2.5 Computation of the classical DL

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

Proposition 2.4. *Let $k \in \mathbb{Z}$. Then $\zeta^k = \zeta_1$ if and only if*

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

This proposition is an immediate consequence of Proposition 2.2. Recall that we have already seen that the discrete logarithm in Brauer groups of local fields is (at least if we deal only with cyclic algebras) transferred to the discrete logarithm in their residue fields. Proposition 2.4 shows that we can compute the discrete logarithm in finite fields if we can compute the numbers $f_{\mathfrak{p}}$ at least for divisors of lifts of ζ and ζ_1. Section 3 will be devoted to outline certain possibilities to reach this aim.

2.6 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 (at least in theory) is to find polynomials (maybe monic over the ring of integers O_K) which define L, and then the decomposition of these polynomials modulo the places of K gives all the information necessary for studying the arithmetic of L. In practice this method is working only for small degrees of

L/K and definitely not for degrees of the size which occur in cryptography (e.g., $\ell \sim 10^{60}$). If we could compute for a given extension L, and a given prime $\mathfrak{p}$ of O_K the number $f_\mathfrak{p}$ in an effective way, 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.

3. Index-calculus in global Brauer groups

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

For simplicity we restrict ourselves in the following to the case $K = \mathbb{Q}$ and so $\mathbb{F}_q = \mathbb{F}_p$. It is obvious that we can extend our considerations to all number fields in which we have a fairly explicit arithmetic at hand which allows to compute principal ideals with only "small" prime divisors.

The congruence (1) can be seen as a solution of a system of linear equations relating the indeterminates f_p for p prime to m and $\mathrm{inv}_\mathfrak{p}(A)$ for $p \mid m$. The basic task is to compute f_p and for this we use cyclic algebras with trivial invariants at primes dividing m. At the other primes we want to have $w_\mathfrak{p}(a) \neq 0$ outside of in a certain distinguished set which is on the one hand big enough such that many elements a satisfying the local conditions can be found, and which is on the other hand small enough to make linear algebra feasible. The key concept is the notion of smooth numbers. Let B be a natural number.

Definition 3.1. A number $n \in \mathbb{N}$ is *B-smooth* if all prime numbers dividing n are bounded by B.

The following result states how many smooth numbers are to be expected.

Theorem 3.1. (Theorem of Canfield–Erdös–Pomerance) *Let x, y be natural numbers which grow asymptotically such that (for some fixed $\varepsilon \in]0,1[$) we have*

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

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

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

asymptotically for $x \to \infty$.

EXAMPLE 3.2. Assume that $y = L_x(1/2, c)$. Then $u = \left(\frac{\log x}{c^2 \log\log x}\right)^{1/2}$ and so we can take $\varepsilon = 1/2 - \delta$ with $\delta > 0$ and small. We get

$$\begin{aligned}\psi(x,y)/x \sim u^{-u} &= \exp\big((\log u)(-u)\big)\\ &= \exp(1/2 \log\log x - 1/2 \log\log\log x)\left(\left(-\frac{\log x}{c^2 \log\log x}\right)^{1/2}\right)\\ &\sim \exp\left(\frac{-1}{2c}\log x^{1/2} \log\log x^{1/2}\right) = L_x(1/2, -1/2c)\,.\end{aligned}$$

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

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

An algorithm for $K = \mathbb{Q}$. Choose a smoothness bound B and compute the factor basis S consisting of the primes less than or equal to B. Let d be the smallest number $\geqslant \sqrt{m}$. For $\delta \in L := [0, \ldots, l_0]$ take $a_1(\delta) := d + \delta$, $a_2(\delta) :=$ $c_0 + 2\delta \cdot d + \delta^2$ ($\equiv a^2$ modulo m) with $c_0 = d^2 - m$. We get a linear equation of the type described in Proposition 2.3

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

Assume that for $\delta \in L$ both $a_1(\delta)$ and $a_2(\delta)$ are B-smooth. Then we get a relation in which the coefficient of f_p is $\neq 0$ only if q is in the factor base. To find such $\delta \in L$ we can use sieves.

Relations arising from quadratic fields. We are interested in cyclic extensions L of odd degree ℓ with a conductor m over $\mathbb{Q}$ and a generator τ of $G(L/\mathbb{Q})$. The composite of such an extension with a quadratic extension field K of $\mathbb{Q}$ has the same properties. So we can use cyclic algebras over K given by a triple $A = (L/K, \tau, c)$ with $c \in K^*$. For places $\mathfrak{p} \in \Sigma_K$ we have numbers $f_\mathfrak{p}$ with $\tau^{f_\mathfrak{p}} = \phi_\mathfrak{p}$. If $p \in \mathfrak{p}$ is not split in K, then $f_\mathfrak{p} = 2f_p$. Otherwise we get $f_p = f_\mathfrak{p}$ for $p \in \mathfrak{p}$.

We need the sum of the invariants of A taken over all places dividing m to be zero. This is certainly the case if c is prime to m, and if the norm of c is congruent to 1 modulo m (i.e., $w_p\big(N_{K/\mathbb{Q}}(c) - 1\big) \geqslant w_p(m)$ for $p \mid m$). If we assume that all primes dividing m are split in K, and that the class number of K is prime to ℓ, we get that there is an extension cyclic of degree ℓ, and unramified outside of m if and only if $\ell \mid \varphi(m)$. So we can use relations by cyclic algebras over K for our system of equations of the type described in Proposition 2.3.

We choose such $\varepsilon \in \mathbb{N}$ and $d \in \mathbb{Z}$ that d is not a square, d is prime to ε and $d \equiv \varepsilon^2 \bmod m$. To simplify matters we shall assume that ε is odd and d even. We denote by K_d the field $\mathbb{Q}(\sqrt{d})$. We take $u \in \mathbb{Z}$ with $\gcd(\varepsilon d, 1-u^4) = 1$. (This implies that u is even.) The element

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

has norm

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

and so we get

$$\sum_{\mathfrak{p}\in\Sigma_K} w_{\mathfrak{p}}\big(\varepsilon(1+u^2) + (1-u^2)\sqrt{d}\big) f_{\mathfrak{p}} \equiv \sum_{\mathfrak{p}\in\Sigma_K} w_{\mathfrak{p}}(2\varepsilon u) f_{\mathfrak{p}} \mod \ell\,.$$

Assume that $\mathfrak{p}$ is not split in K_d and prime to 2. If it would divide

$$\varepsilon(1+u^2) + (1-u^2)\sqrt{d}\,,$$

it would divide the conjugate of this element and so it would divide $\varepsilon(1+u^2)$ and so $(1-u^2)\sqrt{d}$. This contradicts the assumption that $\gcd\big(d\varepsilon, (1-u^4)\big) = 1$. By construction $\varepsilon(1+u^2) + (1-u^2)\sqrt{d}$ is prime to 2. By the same argument one sees that if p is split at most one extension of p can divide this expression. So the right hand side of our equation can be written as

$$\sum_{p\in\mathbb{P},\ p \text{ split in } K_d} w_p\big(\varepsilon^2(1+u^2)^2 - (1-u^2)^2 d\big) f_p\,.$$

Since $2\varepsilon(1+u^2) \in \mathbb{Z}$ we have that

$$\sum_{\mathfrak{p}\in\Sigma_K} w_{\mathfrak{p}}(2\varepsilon u) f_{\mathfrak{p}} = \sum_{p\in\mathbb{P}} w_p(2\varepsilon u) f_p$$

and so we get the equation

$$\sum_{p\in\mathbb{P}} \big(w_p\big(\varepsilon^2(1+u^2)^2 - (1-u^2)^2 d\big) - w_p(2\varepsilon u)\big) f_p \equiv 0 \mod \ell\,.$$

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

Remark 3.3. Of course there are other ways to find suitable equations, too. So it is not necessary to lift the local algebra to a global cyclic algebra, and abelian varieties or special elliptic curves could produce interesting lifts via the (global) Lichtenbaum pairing.

We do this search for relations till we have found $|S|$ $\mathbb{Z}$-linear independent equations which form a system of linear equations $\mathcal{L}$.

The linear algebra step. To **compute** $\varphi(m)$ we compute the determinant of $\mathcal{L}$. To do this efficiently one computes this determinant modulo small numbers by Wiedemann's algorithm and then uses the Chinese remainder theorem.

The performance of this algorithm depends as usual on two terms. First one has to find enough relations. One would expect that this can be done as efficiently as in the factorization algorithms but a thorough analysis has not been done yet. The second part is linear algebra which definitely will have to use fields with odd characteristic. But since they are of size $O(\log(m))$ one can hope that this is not too time consuming. This point of view is supported by new developments in special hardware for the linear algebra part.[2]

To **compute the discrete logarithm** modulo a prime p we can proceed as usual: for random $\overline{a} \in \mathbb{F}_p$ we take a lift $a \in \mathbb{Z}$ and raise it to small powers. We have a good chance that the residue modulo p of such a power is a smooth number. Then we can compute the invariant of the corresponding algebra and so the invariant of the cyclic algebra corresponding to a at p and use this for computing discrete logarithms. If the order of $\overline{a}$ is ℓ we have to treat our equations as equations over $\mathbb{Z}/\ell$.

Remark 3.4. The method described above to compute discrete logarithms unifies methods and results obtained by various authors (Coppersmith, ElGamal, Schirokauer, Adleman–Huang) including number field sieve methods and function field sieve methods. A detailed analysis can be found in [5].

4. Appendix: Cohomology groups

4.1 Definitions

Let G be a profinite group, i.e., G is the projective limit of its finite quotient groups. (So the case that G is finite is included.)

Example 4.1. Let K be a field, K_s its separable closure and $G_K = \mathrm{Aut}_K(K_s)$ its absolute Galois group. For a field L between K and K_s we have a natural injection of G_L into G_K.

[2]The author thanks R. Steinwandt and W. Geiselmann for hints and interest in this problem.

If L/K is a Galois extension, we get the exact sequence

$$1 \to G_L \to G_K \to G(L/K) \to 1\,,$$

where $G(L/K)$ is the Galois group of L/K.

So G_K is the projective limit of the groups $G(L/K)$ where L runs over the finite Galois extensions of K contained in K_s, and hence it is a profinite group.

Being a projective limit of finite groups G carries in a natural way the Krull topology and is compact in this topology. In future all maps from G into another topological space M will be assumed to be continuous with respect to this topology without further mentioning.

Let M be a $\mathbb{Z}$-module endowed with the discrete topology. M is a G-module if it is a $\mathbb{Z}[G]$-module and the operation is continuous. Let U be a closed subgroup of G. We define

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

We get

$$M = \bigcup_{L/K \text{ finite}} H^0(G_L, M)\,.$$

Examples for G_K-modules are K_s^* and, as a submodule, the group of roots of unity $\mu_n = \{x \in K_s^* \colon x^n = 1\}$. Another important family of G_K-modules consists of the K_s-rational points $\mathcal{A}(K_s)$ of abelian varieties $\mathcal{A}$ defined over K with submodules $\mathcal{A}[n](K_s) = \{P \in \mathcal{A}(K_s) \colon [n]P = 0\}$.

We have already defined the group $H^0(G, M)$. We shall now introduce higher cohomology groups $H^n(G, M)$. In fact we shall only need these groups for $0 \leqslant n \leqslant 2$, and we shall define them explicitly below.

In general, the group $H^n(G, M)$ is a quotient of the group of n-cocycles (i.e., of maps c from the n-fold cartesian product G^n to M satisfying a closedness condition) modulo the subgroup of n-coboundaries.

Definition 4.2.

1. 1-*cocycles* are maps

$$c^1 \colon G \to M$$

such that for all $\sigma, \tau \in G$ we have

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

They form a G-module $C^1(G, M)$. 1-*coboundaries* are maps

$$b^1 \colon G \to M$$

such that there exists an element $m \in M$ with

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

for all $\sigma \in G$. They form a G-module $B^1(G,M)$. The *first cohomology group* of M is

$$H^1(G,M) = C^1(G,M)/B^1(G,M).$$

2. 2-*cocycles* are maps

$$c^2 \colon G \times G \to M$$

such that for all $\sigma, \tau, \mu \in G$ we have

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

They form the G-module $C^2(G,M)$. 2-*coboundaries* are maps

$$b^2 \colon G \times G \to M$$

such that there exists a function $f \colon G \to M$ with

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

They form the G-module $B^2(G,M)$. The *second cohomology group* of M is

$$H^2(G,M) = C^2(G,M)/B^2(G,M).$$

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

$$\operatorname{res}_{G/U} \colon H^n(G,M) \to H^n(U,M).$$

Definition 4.3. Let L/K be an algebraic extension field. Take $G = G_K$ and $U = G_L$. Then $\operatorname{res}_{G_K/G_L}$ is denoted by $\operatorname{res}_{K/L}$.

Assume that U is a normal subgroup of G (e.g., L/K is a Galois extension and $U = G_L$, $G = G_K$), and that M_U is a G/U-module contained in a G-module M. By composition with the quotient map

$$\pi_U \colon G \to G/U$$

one transfers cochains ζ from $(G/U)^n$ to M_U to cochains $\zeta \circ \pi_U$ from G^n to M_U and then interprets them as cochains with target M. Obviously coboundaries are mapped to coboundaries. The induced map

$$\inf_{U/G} \colon H^n(G/U, M_U) \to H^n(G,M)$$

is called the *inflation map*. If $U = G_L$ we write often $\inf_{G_L/G_K} = \inf_{L/K}$ and call this map the inflation map from L to K.

Example 4.4. Let M be a G-module and U a normal subgroup of G. Then M^U is a G/U-module in a natural way and $\inf_{U/G} H^n(G/U, M^U)$ is a subgroup of $H^n(G,M)$, and (because we take only continuous cochains) we get

$$H^n(G,M) = \varinjlim_U \inf_{U/G} H^n(G/U, M^U)$$

over normal subgroups of G of finite index.

Take $G = G_K$ and M a G_K-module. Normal subgroups U of G_K of finite index correspond to Galois extension fields of K of finite degree. So 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}.

Example 4.5. Let $\mathcal{A}$ be an abelian variety defined over K. Then

$$H^n\big(G_K, A(K_s)\big) = \varinjlim_L \inf_{L/K} H^n\big(G(L/K), \mathcal{A}(L)\big)\,.$$

The inflation and the restriction maps are related. The background is given by spectral series. For many applications one uses the following exact sequence called inflation-restriction sequence

$$0 \to H^1(G/U, M^U) \xrightarrow{\inf_{U/G}} H^1(G,M) \xrightarrow{\mathrm{res}_{G/U}} H^1(U,M)$$

and refinements of this series (see [7]). In particular, that the inflation map is injective on the first cohomology groups and so we can interpret $H^1(G_K, M)$ as $\bigcup_L H^1\big(G(L/K), M^{G_L}\big)$ where L runs over finite Galois extensions of K. We can generalize this statement to the second cohomology group under special assumptions on M.

Lemma 4.1. *Assume that M is such a G_K-module that for all Galois extensions L of K one has $H^1(G_L, M) = 0$. Then for all such L we get that*

$$\inf_{L/K} \colon H^2\big(G(L/K), M^{G_L}\big) \to H^2(G_K, M)$$

is injective, and so $H^2(G_K, M) = \bigcup_L H^2\big(G(L/K), M^{G_L}\big)$ where L runs over all finite Galois extensions of K.

Assume that U is a subgroup of G of finite index. Let M be a G-module. Take $x \in M^U$ and define $\mathrm{trace}_{G/U}(x) = \sum_\beta \beta(x)$, where β runs over a system of representatives of G/H. (As an example take $G = G_K$, L a finite separable algebraic extension of K and for $\{\beta\}$ all K-embeddings of L into K_s.) It follows that $\mathrm{trace}_{G/U}(x) \in M^G$, and so the trace induces a map from $H^0(U,M)$ to $H^0(G,M)$. By general principles it follows that there is a unique family of maps from $H^n(U, M)$ to $H^n(G, M)$ for all n which extends the trace as cohomological functor called *corestriction* $\mathrm{cor}_{U/G}$ with

$$\mathrm{cor}_{U/G}\colon H^n(U, M) \to H^n(G, M)$$

and

$$\mathrm{cor}_{U/G} \circ \mathrm{res}_{G/U} = [G : U]\,\mathrm{id}\,.$$

Corollary 4.1. *Let m be a number prime to $[L : K]$. Then*

$$\mathrm{res}_{G/U|H^n(G,M)[m]}$$

is injective.

4.2 The long cohomology sequence

We assume that

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

is an exact sequence of G-modules. For $n \geqslant 0$ the maps α resp. β induce (by composition with cocycles) in a natural way homomorphisms $\alpha^n\colon H^n(G, A) \to H^n(G, B)$ resp. $\beta^n\colon H^n(G, B) \to H^n(G, C)$. Next we define homomorphisms $\delta^n\colon H^n(G, C) \to H^{n+1}(G, A)$ in the following way.

Let $c \in H^n(G, C)$ be represented by a cocycle ζ mapping $(\sigma_1, \ldots, \sigma_n) \in G^n$ to $\zeta(\sigma_1, \ldots, \sigma_n) \in C$. For all $(\sigma_1, \ldots, \sigma_n) \in G^n$ take $\overline{\zeta(\sigma_1, \ldots, \sigma_n)} \in B$ with $\beta\big(\overline{\zeta(\sigma_1, \ldots, \sigma_n)}\big) = \zeta(\sigma_1, \ldots, \sigma_n)$. Define the map $d^n\colon G^{n+1} \to B$ by

$$\begin{aligned} d^n(\zeta)(\sigma_1, \ldots, \sigma_n, \sigma_{n+1}) &= \sigma_1 \cdot \overline{\zeta(\sigma_2, \ldots, \sigma_{n+1})} + (-1)^{n+1}\overline{\zeta(\sigma_1, \ldots, \sigma_n)} \\ &\quad + \sum_{j=1}^{n} (-1)^j\, \overline{\zeta(\sigma_1, \ldots, \sigma_j \cdot \sigma_{j+1}, \ldots, \sigma_{n+1})}\,. \end{aligned}$$

By definition the map $\beta \circ d^n$ is the zero map, and so for every $(\sigma_1, \ldots, \sigma_{n+1}) \in G^{n+1}$ there is an element $a(\sigma_1, \ldots, \sigma_{n+1}) \in A$ with

$$\alpha\big(a(\sigma_1, \ldots, \sigma_{n+1})\big) = d^n(\zeta)(\sigma_1, \ldots, \sigma_{n+1})\,.$$

One checks by a straightforward computation that the map

$$a\colon G^{n+1} \to A$$

mapping $(\sigma_1, \ldots, \sigma_{n+1})$ to $a(\sigma_1, \ldots, \sigma_{n+1})$ is an $n+1$-cocycle and that its class modulo $n + 1$-coboundaries is determined by c and independent of all choices made. Define now $\delta^n(c)$ as class of a.

Theorem 4.1. *Assume that*

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

is an exact sequence of G-modules and $n \geqslant 0$. The (infinite) sequence of G-modules

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

is exact.

We shall need the connecting homomorphisms δ^n only for $n = 1, 2$.

4.3 The Kummer sequence

Assume that M is a G-module and $m \in \mathbb{N}$. Define

$$[m]\colon M \to M; \quad x \mapsto m \cdot x\,,$$

and $M[m] = \ker\bigl([m]\bigr)$. Assume that $[m]$ is surjective. Then we have the exact sequence of G-modules

$$0 \to M[m] \xrightarrow{\alpha} M \xrightarrow{\beta=[m]} M \to 0\,,$$

where α is the inclusion map. This sequence is called the *Kummer sequence* of M. On the cocycle level the maps α^n are induced by inclusion of $M[m]$ into M. So their image is contained in $H^n(G,M)[m]$. It is easy to see that $\beta^n = [m]$, and so we get from the long cohomology sequence the exact sequences

$$0 \to H^n(G,M)/[m]H^n(G,M) \xrightarrow{\delta^n} H^{n+1}\bigl(G, M[m]\bigr) \to H^{n+1}(G,M)[m] \to 0\,.$$

Example 4.6. Take $n = 0$. Then we have the exact sequence

$$0 \to M^G/\,[m]M^G \xrightarrow{\delta^0} H^1(G, M[m]) \to H^1(G,M)[m] \to 0\,.$$

The map δ^0 can be described explicitly. Take $x \in M^G$. There is an element $y \in M$ with $m \cdot y = x$. Define

$$\begin{aligned} &d^0(x)\colon G_K \to M[m]\,, \\ &\sigma \mapsto \sigma \cdot y - y\,. \end{aligned}$$

Then $\delta^0\bigl(x + [m]M^G\bigr)$ is the class of $d^0(x)$ in $H^1\bigl(G, M[m]\bigr)$.

EXAMPLES 4.7.

1. Take $M = K_s^*$ and $G = G_K$. Hence $[m]$ is exponentiation by m. We assume that m is prime to the characteristic of K. We get the Kummer sequence

$$1 \to \mu_m \to K_s^* \xrightarrow{[m]} K_s^* \to 1\,,$$

and the cohomology sequence

$$1 \to K^*/K^{*m} \xrightarrow{\delta^0} H^1(G_K, \mu_n) \to 1\,,$$

since Hilbert's Theorem 90 (see [7]) implies that $H^1(G_K, K_s^*) = 0$.

2. In the same situation take $n = 1$. Using Hilbert's Theorem 90 again we get: The inclusion $\mu_m \to K_s^*$ induces an isomorphism

$$H^2(G_K, \mu_m) \xrightarrow{\approx} H^2(G_K, K_s^*)[m]\,.$$

3. Take $M = \mathcal{A}(K_s)$ with $\mathcal{A}$ an abelian variety defined over K and m prime to the characteristic of K. We get the Kummer sequence

$$0 \to A(K_s)[m] \to A(K_s) \xrightarrow{[m]} A(K_s) \to 0$$

and the cohomology sequence

$$0 \to A(K)/mA(K) \xrightarrow{\delta} H^1\big(G_K, A(K_s)[m]\big) \to H^1\big(G_K, A(K_s)\big)[m] \to 0\,.$$

REFERENCES

[1] AVANZI, R.—COHEN, H.—DOCHE, C.—FREY, G.—LANGE, T.—NGUYEN, K.—VERCAUTEREN, F.: *The Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, Boca Raton, 2005.

[2] FREY, G.: *Applications of arithmetical geometry to cryptographic constructions*, in: Finite fields and applications (Augsburg, 1999), Springer-Verlag, Berlin, 2001, pp. 128–161.

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

[4] NEUKIRCH, J.: *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

[5] NGUYEN, K.: *Explicit arithmetic of Brauer groups, Ray class fields and index calculus*, PhD thesis, University Essen, 2001.

[6] SERRE, J. P.: *Groupes Algébriques et Corps de Classes*, Hermann, Paris, 1959.

[7] SERRE, J. P.: *Corps Locaux*, Hermann, Paris, 1962.

Received February 2, 2005

Institute for Experimental Mathematics
University of Duisburg-Essen
Ellernstrasse 29
G–45326 Essen
GERMANY

E-mail: frey@exp-math.uni-essen.de