Explicit Arithmetic of Brauer Groups

Ray Class Fields and Index Calculus

Dissertation zur Erlangung des Grades
eines Doktors der Naturwissenschaften

Dem Fachbereich 6
(Mathematik und Informatik)
der Universität Gesamthochschule Essen
vorgelegt von

Kim Nguyen
aus Köln am Rhein

Essen, 2.Juli 2001

Acknowledgments

First of all I would like to thank my supervisor, Prof. Dr. Dr.h.c. Gerhard Frey, for suggesting this research topic to me. During the last three years he has guided me through sometimes difficult times. His enthusiasm, his knowledge and his understanding were invaluable to me.

I would also like to thank the SIEMENS AG, Munich, for making this research possible through a research scholarship.

Many thanks to Prof. Dr. H.–G. Rück (University Kassel) for many fruitful discussions.

Several people have read parts of this thesis at various times: Dr. Markus Holder, Annegret Weng, Dr. Markus Wessler. Many thanks to them. All errors are mine.

Thanks to all the members of the Institute for providing such nice and relaxed working conditions. Especially, many thanks to my room mate Annegret.

Prof. Dr. Edlyn Teske (CACR, University of Waterloo, Canada), Prof. Dr. Kumar Murty (University of Toronto, Canada) and Prof. Dr. H.–G. Rück (University of Kassel, Germany) gave me the possibility to speak about results from this thesis at their universities, for which I am very grateful.

The computations in this thesis were performed using the MAGMA and KANT packages. Special thanks goes to the two groups providing these excellent tools.

Thanks to the members and the musical directors of the Kettwiger Bach Ensemble (Wolfgang Kläsener) and the Essener Kantorei (Eckhard Manz) for making my time in Essen an enjoyable musical experience.

Finally I would like to thank my parents for all their love and understanding. This work is dedicated to them.

Erklärung

Ich habe diese Arbeit selbstständig verfasst und dabei keine anderen als in der Literaturliste angegebenen Hilfsmittel verwendet.

Essen, 2.7.2001

(Kim Nguyen)

Tag der Disputation: 18.12.2001
Vorsitzender: Prof. Dr. J. Herzog
1. Gutachter: Prof. Dr.Dr.h.c. G. Frey
2. Gutachter: Prof. Dr. H. Stichtenoth

Ergänzte Version vom 18.1.2002

Abstract

In this thesis we examine the arithmetic of Brauer groups of local and global fields. Although Brauer groups are well studied from a theoretical point of view, no one has yet addressed the question of making this theory explicit.

We propose to do exactly this in the case of relative Brauer groups.

Let L/K be a local extension of degree l. Then the invariant map induces an isomorphism $Br(L/K) \simeq \mathbb{Z}/l\mathbb{Z}$. The first natural question is to compute this invariant map explicitly for a given element $A \in Br(K/L)$. In doing this we show that this problem is intimately related to the arithmetic of the underlying finite field.

This motivates the following approach: calculate a local invariant map at a ramified place $\mathfrak{p}$ via the Hasse–Brauer–Noether local–global principle by relating it to the invariant map at other (unramified) places $\mathfrak{q} \neq \mathfrak{p}$. We show that – using the concept of smoothness – this leads to algorithms which are known as index calculus methods in order to compute the discrete logarithm in finite fields.

Moreover we show how this approach links the question of solving the discrete logarithm in finite fields to the problem of solving discrete logarithms in the Galois group of certain global extensions.

In order to apply the local global principle, we need to construct or at least prove the existence of global extensions with prescribed ramification and order. Except in the cases of $K = \mathbb{Q}$ and K an imaginary quadratic field we provide results about extensions of this kind in the case that K is a CM field.

Using these results we are able to modify a well known algorithm in the case of discrete logarithms in certain subgroups of $\mathbb{F}_{p^n}$.

We also give an interpretation of the function field sieve in the setting of Brauer groups. This interpretation explains a notable difference between number field sieve and function field sieve.

Finally we link the discrete logarithm problem on abelian varieties to the arithmetic of Brauer groups using the Tate pairing.

Contents

Chapter 1

Cryptographic Systems based on Discrete Logarithms

Before introducing Brauer groups, we briefly explain which kind of cryptographical applications we are interested in.

1.1 Introduction

Formally a crypto system is described by the following parameters:

- A set $\mathcal{P}$ of plain texts.
- A set $\mathcal{C}$ of cypher texts.
- A set $\mathcal{K}$ of keys.
- A family of encryption functions $\mathcal{E} = \{E_k : \mathcal{P} \to \mathcal{C}, k \in \mathcal{K}\}$.
- A family of decryption functions $\mathcal{D} = \{D_k : \mathcal{C} \to \mathcal{P}, k \in \mathcal{K}\}$.

Given an encryption key $e \in \mathcal{K}$ the encryption process is applying the function E_e to a plain text p. The decryption process is applying the function D_d, where d is a suitable decryption key, to the cypher text $c = E_e(p)$.

In order to guarantee the decryption process to succeed, we want that:
For each $e \in \mathcal{K}$ there exists at least one $d \in \mathcal{K}$ such that for all $p \in \mathcal{P}$ the equation $D_d(E_e(p)) = p$ holds.

In a symmetric crypto system the decryption key d is easily computable from the encryption key e. Therefore, both e and d have to be kept secret.

In an asymmetric crypto system d can only be computed from e with a very large (not feasible) computational effort.
In this case the encryption key e can be made public and only the decryption key d has to be kept secret. We call a system like this a public–key crypto system.

For the construction of public–key crypto systems the construction of one–way functions is of great importance. Here a one–way function is understood to be a function f whose inverse is hard to compute (for a more precise definition of this see for example [Gol01, Chapter 2]).

One possibility to construct one–way functions is to consider an Abelian group G together with an efficiently computable group operation $(G, +)$ and consider the hardness of the following problem:

Given two elements $g \in G$ and $h \in \langle g \rangle$, find $n \bmod |\langle g \rangle|$ such that $g^n = h$ if such n exists. We call this the discrete logarithm problem in G.

Once we have convinced ourselves that the discrete logarithm problem in a group G is hard, this can be seen as strong evidence for the fact that the function

$$f : \mathbb{Z} \to G, \quad n \mapsto n \cdot g$$

for $g \in G$ is likely to be a one–way function.

Here are some instances of the discrete logarithm problem used in cryptography:

- The discrete logarithm in the multiplicative group of a finite field $\mathbb{F}_q$ (or in cyclic subgroup of this group) (first proposed by Diffie and Hellman [DH76]).
- The discrete logarithm in the group of rational points of an elliptic curve (or more general in the Jacobian of a hyperelliptic curve) over a finite field $\mathbb{F}_q$ (simultaneously proposed by Koblitz [Kob87] and Miller [Mil85] in the year 1985 in the case of elliptic curves and in the year 1989 by Koblitz [Kob89] in the case of hyperelliptic curves).

1.2 Discrete Logarithms in Finite Fields

When considering the discrete logarithm in finite fields we can distinguish two cases:

- The discrete logarithm problem in the full multiplicative group $\mathbb{F}_q^\times$.
- The discrete logarithm problem in subgroups of $\mathbb{F}_q^\times$.

We will deal with the second case. Hence let $k = \mathbb{F}_q$ be a finite field satisfying $l|q-1$, meaning that the l–th roots of unity are contained in k.

We can then consider the discrete logarithm problem in the group of l–th roots of unity: given two non trivial l–th roots of unity ζ_0 and $\zeta_1 \in \langle\zeta_0\rangle$, determine $n \bmod l$ such that $\zeta_1 = \zeta_0^n$ holds.

The difficulty of this problem relies critically on the assumption that to solve a discrete logarithm in μ_l means essentially solving a discrete logarithm in $\mathbb{F}_q^\times$. It seems that the only possibility to attack the discrete logarithm directly in the cyclic subgroup is to use generic methods which have exponential complexity depending on the order of the subgroup. The subexponential methods used in order to compute the discrete logarithm have complexity varying with q not with l.

Hence the Digital Signature Standard as proposed by NIST chooses l to be about 160 bit and q to be a also prime and of size about 1000 bit such that $l|q-1$. While the discrete log in a finite field of size 160 bit is certainly not secure no one seems to be able to compute discrete logarithms in fields of size much larger than 280 bits in reasonable time (see [JL01]), so at the moment 1000 bit can be viewed as secure.

Shoup [Sho97] has proven that the discrete logarithm in a group of prime order l can not be solved in less than $O(\sqrt{l})$ operations, as long as only generic algorithms are allowed. This means that you are only allowed to use the group operations for computations in the algorithm.

It is therefore not surprising that the most effective methods to solve the discrete logarithm problem in finite fields make extensive use of lifting techniques: avoiding generic algorithms means that the source for extra information about relations in the group must be obtained from outside the group.

For example one may make use of the fact that we can lift the finite field to a global field. We are then able to lift the group elements to the larger object and construct relations in this larger object. Upon reduction to the finite field this yields relations in the original group obtained without generic methods. Having collected enough relations, one can then hope to solve the original discrete logarithm problem by applying linear algebra to the system of relations. This approach is known as index calculus.

We will give a new description of index calculus using the theory of Brauer groups or equivalently cyclic Galois cohomology. By this we show how to link the discrete logarithm problem in finite fields to certain discrete logarithms in class groups of global field extensions.

Chapter 2

Brauer Groups

The following brief introduction to the theory of Brauer groups is modeled after [Ker90]. Let K be a field, let $\overline{K}$ be a separable closure of K and G the Galois group $Gal(\overline{K}/K)$. Then $\overline{K}^\times$ is a G–module in a natural way. Hence we can consider the Galois cohomology of $\overline{K}^\times$ (a short introduction to Galois cohomology is given below).

We want to study the properties of $H^2(G, \overline{K}^\times)$. It is a classical result that this is equivalent to classifying finite simple central algebras over the field K. Using this interpretation we will be able to give a complete classification in the case that K is a local field. It will be the aim of the following chapters to examine to which extent this classification can be made completely explicit.

2.1 Algebras over Fields

An algebra over a field K is a ring A, together with a K–vectorspace structure satisfying

$$(\lambda a)b = a(\lambda b) = \lambda(ab)$$

for $\lambda \in K$ and $a, b \in A$. The dimension A is given by the dimension of A viewed as a K–vectorspace. An algebra in which every element $a \neq 0$ is invertible is called skew field or division algebra over K.

A K–algebra homomorphism $f : A \to B$ is a K–linear ring homomorphism $A \to B$.

An ideal I of a K–algebra A is an ideal of the underlying ring. A K–algebra A is called simple, if A does not contain any ideals except (0) and A.

Theorem 2.1.1 (Wedderburn structure theorem) *Let A be a finite simple K–algebra. Then there exists exactly one $n \geq 1$ and up to K-algebra isomorphism exactly one skew field D over K such that $A \simeq M_n(D)$.*

If A is a ring and B a subring of A, then

$$Z_A(B) = \{a \in A | ab = ba \; \forall b \in B\}$$

is the centralisor of B in A. Let $Z(A) := Z_A(A)$ denote the centralisor of A in A, this is also called the center of A. Let A be a K–algebra, we can assume $K \subset A$. Obviously we have $K \subset Z(A)$. In the case of $K = Z(A)$ we call A central.

The automorphisms of a finite central simple algebra A have a particularly simple form:

Theorem 2.1.2 (Skolem–Noether) *Let A be a finite simple central algebra, then every K–algebra automorphism $\phi : A \to A$ is an inner automorphism, meaning that there is a unit $u \in A$ such that $\phi(a) = uau^{-1}$ for all $a \in A$.*

Given two K–algebras A and B, $A \otimes_K B$ is a K–algebra with unity element $1 \otimes 1$. Multiplication is defined via

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$$

for a_1, a_2 in A and b_1, b_2 in B. The center of $A \otimes_K B$ is given by $Z(A) \otimes_K Z(B)$. Hence, if A and B are central K–algebras, so is $A \otimes B$.

In the following we shall be considering central simple algebras over a field K.
Two algebras A and B are called equivalent ($A \sim B$), if there exist $r, s \in \mathbb{N}$, such that $A \otimes_K M_r(K) \simeq B \otimes_K M_s(K)$.

The Brauer group of a field K is defined as the set of equivalence classes

$$[A] = \{B | \, B \, \text{finite, central, simple}, B \sim A\}$$

implying

$$Br(K) = \{[A], A \,\text{finite, central, simple}\}.$$

Here multiplication is defined as follows: $[A] \times [B] = [A \otimes B]$, this is welldefined. Properties of the tensor product imply that multiplication is associative and commutative, the unity element is given by $1_{Br(K)} = [K]$.

Let A^{opp} be the oppositional algebra of A, meaning that we have $A^{opp} = A$ as K–vektorspaces with the multiplication in A^{opp} given by

$$A^{opp} \times A^{opp} \to A^{opp}, a \times b \mapsto ba,$$

where the product on the right hand side is the one in A. Then $[A][A^{opp}] = [K] = 1_{Br(K)}$. Hence $Br(K)$ is indeed a group.

Let L be an arbitrary algebraic field extension of K and A be a K–algebra, then $A \otimes_K L$ is a L–algebra, more precisely there is a group homomorphism

$$res_{L/K} : Br(K) \to Br(L), [A] \mapsto [A \otimes_K L].$$

A field extension L of K is called splitting field of A, if $[A] \in ker(res_{L/K})$. We call $Br(L/K) = ker(res_{L/K})$ the relative Brauer group of K with respect to L.

If L/K is a splitting field of A, this is equivalent to saying that there is an algebra $\tilde{A}$ equivalent to A containing L with dimension $\dim_K(\tilde{A}) = [L : K]^2$.

Let D be a finite central skewfield over K and L its maximal subfield. Then D is split by L and we have $\dim_K(D) = [L : K]^2$.

Let A be a finite central simple K–algebra. Then there exists a splitting field of A, which is of finite dimension over K as well as Galois.
It turns out that the Brauer group $Br(K)$ can be described only in terms of relative Brauer groups:

$$Br(K) = \bigcup_{\substack{L/K \\ \text{finite, Galois}}} Br(L/K).$$

Hence we can concentrate on the study of $Br(L/K)$ with L finite Galois over K.

2.2 Examples

Theorem 2.2.1 *Let k be a finite field. Then $Br(k) = 1$.*

Proof:
Let D be a finite central skew field over k, then each element of D is contained in a maximal subfield of D. But all maximal subfields have the same degree $\sqrt{\dim_k(D)}$ over k.
Since k is a finite field, all extension fields of given degree are k–isomorphic. But now the theorem by Skolem–Noether (Theorem 2.1.2) says that these fields are of the form xLx^{-1} with $x \in D^\times$ and a fixed maximal subfield L. Hence

$$D^\times = \bigcup_{x \in D^\times} xLx^{-1}.$$

But if a finite group G is the union of all the conjugates of a subgroup H, it follows that $G = H$ whence $D = L$.
Therefore D is commutative, thus $D = k$, since D is central over k. Therefore $Br(k) = 1$. □

Theorem 2.2.2 *Let K be algebraically closed. Then $Br(K) = 1$.*

Proof:
Let D be a finite division algebra over K, then we have to show:
D is split by K.
Let E be a commutative subalgebra of D. Then E is an integral domain and hence finite algebraic over K. Therefore $E = K$, since K is algebraically closed.
Now consider the subalgebra $K[a]$ for $a \in D$, then $a \in K$, hence $D = K$. Also D is split by K, hence: $Br(K) = 1$. □

Theorem 2.2.3 *Is K real closed, then $Br(K) \simeq \mathbb{Z}/2\mathbb{Z}$.*

Proof:
This is the statement of the celebrated theorem by Frobenius, saying that the Hamiltonians are the only proper skew field of finite dimension over a real closed field K.

2.3 Galois Cohomology

In the following we give a (very) short introduction to the basics of Galois cohomology, more details can be found for example in [Neu69, Teil I] (in German) or in [Ser64].

Let G be a finite group.

Definition 2.3.1 *A discrete G–module is an Abelian group M with an action of G in such a way that for all $a, b \in M$ and $\sigma, \tau \in G$:*

1. $1a = a \ \forall a \in M$
2. $\sigma(a + b) = \sigma a + \sigma b \ \forall \sigma \in G, a, b \in M$
3. $(\sigma\tau)a = \sigma(\tau a) \ \forall \sigma, \tau \in G, a \in M$.

Let A be a G–module, then we denote by A_q the set of q–cochains, that is the set of maps

$$x : \underbrace{G \times \cdots \times G}_{\text{q–times}} \to A.$$

By $(\partial_1 x)(\sigma) = \sigma x - x$ for $x \in A_0 = A$ and in general by $(\partial_q x)(\sigma_1, \ldots, \sigma_q) = \sigma_1 x(\sigma_2, \ldots, \sigma_q) + \sum_{i=1}^{q-1}(-1)^i x(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_q) + (-1)^q x(\sigma_1, \ldots, \sigma_{q-1})$ for $x \in A_{q-1}, q \geq 1$ we define maps $\partial_q : A_{q-1} \to A_q$, which satisfy $\partial_{q+1} \circ \partial_q = 0$. Now define q–cocycles Z_q and q–coboundaries R_q by

$$Z_q = \ker(\partial_{q+1}) \subset A_q, \quad R_q = \mathrm{Im}(\partial_q) \subset A_q.$$

Since $\partial_{q+1} \circ \partial_q = 0$ we have $R_q \subset Z_q$, hence we can consider the quotient:

Definition 2.3.2 *The factor group*

$$H^q(G, A) = Z_q / R_q, \ q \geq 1.$$

is called the cohomology group of dimension q of the G–module A.
For $q = 0$ we define $H^0(G, A) = A^G = \{a \in A : \sigma a = a \ \forall \sigma \in G\}$.

In arithmetical applications especially the cohomology groups of lower dimension are important. It turns out that we can give algebraic interpretations of these groups.

In the case of $q = 1$ the 1–cocycles are the functions $x : G \to A$ satisfying $\partial_2 x = 0$, hence

$$x(\sigma\tau) = \sigma x(\tau) + x(\sigma), \quad \sigma, \tau \in G.$$

Therefore the 1–cocycles are also known as crossed homomorphisms. The 1–coboundaries are the functions

$$x(\sigma) = \sigma a - a, \sigma \in G, \text{ for an } a \in A$$

In the case that the action of G on A is trivial we obviously get $H^1(G, A) = Hom(G, A)$.

In the case of $q = 2$ the 2–cocycles are the functions satisfying $\partial_3 x = 0$, hence

$$x(\sigma\tau, \rho) + x(\sigma, \tau) = \sigma x(\tau, \rho) + x(\sigma, \tau\rho), \quad \sigma, \tau, \rho \in G.$$

The 2–coboundaries satisfy

$$x(\sigma, \tau) = \sigma y(\tau) - y(\sigma\tau) + y(\sigma)$$

with a 1–cochain $y : G \to A$.

The following theorem is most important in the subsequent computations:

Theorem 2.3.3 *Let*

$$0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$$

be an exact sequence of G–modules, then we have a long exact sequence

$$0 \to A^G \xrightarrow{i_0} B^G \xrightarrow{j_0} C^G \xrightarrow{\delta_1} H^1(G, A) \xrightarrow{i_1} H^1(G, B) \to \cdots,$$

which is called exact cohomology sequence.

Here the δ–map has the following explicit realization:
Let $c_q \in H^q(G, C)$ be given, then we can represent c_q by a q–cocycle $C_q : G^q \to C$. Since $j : B \to C$ is surjective, we can find a q–cochain B_q with values in B, such that $j(B_q) = C_q$. Now we have $0 = \partial C_q = \partial j(B_q) = j(\partial B_q)$, hence B_q is in the kernel of j_{q+1}. Therefore there exists a q–cochain A_{q+1} satisfying $\partial B_q = i(A_{q+1})$. Now

$$0 = \partial\partial B_q = \partial i(A_{q+1}) = i(\partial A_{q+1}),$$

whence $\partial A_{q+1} = 0$, since i is injective. It follows that A_{q+1} is a q–cocycle. If a_q is the class of A_q in $H^{q+1}(G, A)$, we define $\delta_q(c_q) = a_q$.

Now let K be a perfect field, $\overline{K}$ an algebraic closure of K and $G = Gal(\overline{K}/K)$ the Galois group of $\overline{K}$ over K. Then G is the inverse limit of the groups $Gal(L/K)$, where L runs through all finite Galois extensions L of K. G has the structure of a pro–finite group, the basis of one of the topology of G is given by all the normal subgroups of G with finite index.

A G–module is then defined to be an Abelian group A with a continuous action of G, meaning that the map $G \times A \to A$ is continuous if G is considered in the pro–finite and A in the discrete topology.

Example: $\overline{K}$ as well as $\overline{K}^{\times}$ together with the natural action of G can be considered as G–modules, since for every $x \in \overline{K}$ the extension $K(x)/K$ is finite.

For a pro–finite group G and a G–module M we can also define cohomology groups $H^q(G, M)$ for $q \geq 0$ by restricting the cochains to continuous maps $G^q \to M$.

In the case of $G = Gal(\overline{K}/K)$ we have

$$H^q(G, M) \simeq \lim_{\rightarrow} H^q(Gal(L/K), M),$$

where L/K runs through all finite Galois extensions of K.

2.4 The Connection between Algebras and Galois Cohomology

We now consider algebras with the following special property:
A finite central simple algebra A over K is called a crossed product, if A contains a field L Galois over K such that $\dim_L(A) = \dim_K(L)$.

Each finite central simple algebra A is split by a finite Galois extension of K, but this is equivalent to saying that A is at least equivalent to a crossed product over K.

The great advantage of dealing with crossed products is that they have a remarkable simple structure:

Let A be a crossed product, then we can find for each $\sigma \in G = Gal(L/K)$ a unit $u_\sigma \in A$ such that $\{u_\sigma\}_{\sigma \in G}$ is a basis of A as a L left vectorspace and furthermore

$$u_\sigma x = \sigma(x) u_\sigma \ \forall x \in L, \forall \sigma \in G,$$
$$u_\sigma u_\tau = f(\sigma, \tau) u_{\sigma\tau} \ \forall \sigma, \tau \in G,$$

where $f : G \times G \to L^\times$ is a 2–cocycle.

Given on the other hand a 2–cocycle $f \in H^2(G, L^\times)$ with values in a Galois extension L/K of degree n, we can form the n^2–dimensional K–vectorspace

$$(L, G, f) = \bigoplus_{\sigma \in G} L u_\sigma,$$

where multiplication of two elements of (L, G, f) is given by

$$(\sum_{\sigma \in G} x_\sigma u_\sigma)(\sum_{\tau \in G} y_\tau u_\tau) = \sum_{\sigma, \tau \in G} x_\sigma \sigma(y_\tau) f(\sigma, \tau) u_{\sigma\tau}$$

with $x_\sigma, y_\tau \in L$. Now (L, G, f) is a finite central simple algebra with unity element $f(1,1)^{-1} u_1$, which is split by L. (L, G, f) is called crossed product of L and G with respect to f.

Two crossed products of the form (L, G, f) and (L, G, g) are isomorphic as K–algebras if and only if f and g differ by a 2–coboundary.

Theorem 2.4.1 *We have $Br(L/K) \simeq H^2(G, L^\times)$.*

Proof:
Consider two crossed products (L, G, f) and (L, G, g) with f and g normed (that is $f(1,1) = g(1,1) = 1$), then we have

$$(L, G, f) \otimes (L, G, g) \sim (L, G, fg).$$

For each 2–cocycle g there exists a normed 2–cocycle $\tilde{g}$, which is cohomologous to g.

Is follows that the map

$$\alpha : H^2(G, L^\times) \to Br(L/K), [f] \mapsto (L, G, f)$$

is a well defined group homomorphism.
α is surjective, since each finite central simple algebra A over K which is

split by L is equivalent to such an algebra B with $L \subset B$ and $\dim_L(B) = n$. Also there is a 2–cocycle with $B \simeq (L, G, f)$.

α is also injective: if f is a 2–cocycle with $(L, G, f) \sim K$, we deduce $(L, G, f) \simeq M_n(K)$, since $\dim_K((L, G, f)) = n^2$.
Now consider the crossed product of L and G with respect to the trivial 2–cocycle 1, we obtain $(L, G, 1) = \oplus_\sigma L v_\sigma$ with $v_\sigma v_\tau = v_{\sigma\tau}$ and $v_\sigma x = \sigma(x) v_\sigma \, \forall \sigma \in G, x \in L$.
By $\phi : (L, G, 1) \to End_K(L), \phi(x v_\sigma) = x\sigma(y)$ we define a K–algebrahomomorphism, which is obviously injective, since $(L, G, 1)$ is simple.
Comparing dimensions this implies that ϕ is also surjective, hence $(L, G, 1) \simeq M_n(K) \simeq (L, G, f)$, meaning that f is cohomologous to 1. □

In the following we will only consider the case that L/K is a cyclic Galois extension of degree $[L : K] = n$. In this case we can restrict ourselves to the following simple type of 2–cocycles:
Let $G = Gal(L/K) =< \sigma >$. For $a \in K^\times$ we consider the map

$$f_{\sigma,a} : G \times G \to L^\times,$$

given by

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

Obviously $f_{\sigma,a}$ is a normed 2–cocycle. Let (L, σ, a) be the crossed product $(L, G, f_{\sigma,a})$ and set $u = u_\sigma$. Then obviously $u^i = u_{\sigma^i}$ for $i = 1, \ldots, n-1$ whence

$$(L, \sigma, a) = \bigoplus_{i=0}^{n-1} L u^i,$$

with

$$u^n = a, \text{ and } ux = \sigma(x)u, \forall x \in L.$$

It turns out that every crossed product is isomorphic to an algebra of the form (L, σ, a).

Lemma 2.4.2 *Let f be a normed 2–cocycle, then*

$$(L, G, f) \simeq (L, \sigma, a) \textit{ with } a = \prod_{m=0}^{n-1} f(\sigma^m, \sigma) \in K^\times.$$

Proof:
We have $(L,G,f) = \oplus_{i=0}^{n-1} Lv_{\sigma^i}$ with $v_1 = 1$ and $v_{\sigma^i}x = \sigma^i(x)v_{\sigma^i}$ for $x \in L$. Furthermore $v_{\sigma^i}v_{\sigma^j} = f(\sigma^i,\sigma^j)v_{\sigma^{i+j}}$ for $0 \le i,j \le n-1$.
Now

$$v_\sigma^2 = v_\sigma v_\sigma = f(\sigma,\sigma)v_{\sigma^2},$$

also

$$v_\sigma^3 = f(\sigma,\sigma)v_{\sigma^2}v_\sigma = f(\sigma,\sigma)f(\sigma^2,\sigma)v_{\sigma^3},$$

and in general

$$v_\sigma^i = (\prod_{j=1}^{i-1} f(\sigma^j,\sigma))v_{\sigma^i}$$

for $i = 2,\dots,n-1$. Considering v_σ^n we obtain $v_\sigma^n = av_{\sigma^n} = a$. Therefore $(L,G,f) = \oplus_{i=0}^{n-1} Lv_\sigma^i$, since $\prod_{j=0}^{i-1} f(\sigma^j,\sigma) \in L^\times$ for $i = 2,\dots,n-1$. Also we have $v_\sigma^n = a$ and $v_\sigma x = \sigma(x)v_\sigma$ for all $x \in L$. Hence$(L,G,f) \simeq (L,\sigma,a)$. Since $a = v_\sigma^n$ lies in the center of (L,G,f), we have $a \in K$. □

The following theorem shows that the relative Brauer group $Br(L/K)$ can be described completely in terms of the ground field K:

Theorem 2.4.3 *Let L/K be Galois with cyclic Galois group $G =< \sigma >$ of order n. Then the map $\phi : a \mapsto (L,\sigma,a)$ induces an isomorphism*

$$K^\times/N_{L/K}(L^\times) \xrightarrow{\sim} Br(L/K).$$

Proof:
(L,σ,a) is split by L, thus $[(L,\sigma,a)] \in Br(L/K)$. Since $f_{\sigma,a}f_{\sigma,b} = f_{\sigma,ab}$ we also have $\phi(a)\phi(b) = \phi(ab)$. Let A be a finite central simple algebra split by L, then there exists a normed 2–cocycle f such that $A \sim (L,G,f)$. But then there exists also $a \in K^\times$ such that $(L,G,f) \sim (L,\sigma,a)$, whence $A \sim (L,\sigma,a)$. Therefore ϕ is surjective.

It remains to show:

$$(L,\sigma,a) \simeq (L,\sigma,1) \Leftrightarrow a \in N_{L/K}(L^\times).$$

Set $(L,\sigma,a) = \bigoplus_i Lu^i$ and $(L,\sigma,1) = \bigoplus_i Lv^i$ together with the usual rules. Suppose $a = N_{L/K}(y)$ with $y \in L^\times$, then consider $\tilde{u} = y^{-1}u$. It follows

$$\begin{aligned}\tilde{u}^n &= y^{-1}uy^{-1}u\cdots y^{-1}u = y^{-1}\sigma(y^{-1})u^2y^{-1}\cdots y^{-1}u = \cdots \\ &= (\prod_{i=0}^{n-1}\sigma^i(y^{-1}))u^n = N_{L/K}(y^{-1})a = a^{-1}a = 1.\end{aligned}$$

Furthermore we have

$$\tilde{u}x = y^{-1}ux = y^{-1}\sigma(x)u = \sigma(x)y^{-1}u = \sigma(x)\tilde{u}.$$

Therefore $(L, \sigma, a) \simeq (L, \sigma, 1)$.
Consider a K–algebra automorphism $\phi : (L, \sigma, a) \overset{\simeq}{\to} (L, \sigma, 1)$, applying Skolem–Noether (2.1.2) there exists α such that $x \times 1 = \alpha\phi(x)\alpha^{-1}$ for all $x \in L$. Now consider $w = \alpha\phi(u)\alpha^{-1}$, then we obtain $w^n = a$ as well as $wxw^{-1} = \sigma(x)$ and $wx = \sigma(x)w$ $\forall x \in L$. Considering $y = wv^{n-1}$, where the v was used to define the trivial algebra $(L, \sigma, 1)$, we obtain

$$yx = wv^{n-1}x = w\sigma^{n-1}(x)v^{n-1} = \sigma(\sigma^{n-1}(x))wv^{n-1} = xy.$$

Therefore $y \in Z_{(L,\sigma,1)}(L) = L$. Furthermore

$$\begin{aligned} a &= w^n = yvyv \cdots yv = y\sigma(y)v^2yv \cdots yv = \cdots \\ &= y\sigma(y)\sigma^2(y) \cdots \sigma^{n-1}(y)v^n = N_{L/K}(y)v^n = N_{L/K}(y) \end{aligned}$$

since by definition of $(L, \sigma, 1)$ we have that $v^n = 1$. □

2.5 Brauer Groups of Local Fields

Let K be a local field, meaning there exists a discrete valuation v on K, K is complete with respect to v and the residue class field k of K with respect to v is a finite field.

Let D be a finite dimensional skew field over K, then the discrete valuation v of K can be extended uniquely to a valuation v_D of D. This valuation is given in terms of v by $v_D(x) = (1/n)v_K(N_{D/K}(x))$. Here n is the degree of D over K, the norm of an element d of D/K is defined in the usual way as the determinant of the K–linear map $x \mapsto dx$.

Let R_D be the valuation ring of D and $\mathfrak{p}$ its maximal ideal. We have $k_{\mathfrak{p}} = R_D/\mathfrak{p}$.

By definition of v_D there exists a divisor e of $n = [D : K]$ such that $v(D^\times) = (1/e)\mathbb{Z}$, e is called the ramification index of D.

A finite extension L/K is called unramified if the ramification index e of L over K equals 1 and the associated extension of residue class fields is separable.

If L/K is an arbitrary extension of local fields of degree n, then the associated extension of residue class fields is a finite extension of degree f (f is called residue class degree). The fundamental relationship between the degree n of the extension and the corresponding residue class and ramification degree is given by $n = ef$.

Fixing a separable closure $\overline{K}$ of K, for each number n there exists exactly one unramified extension K_n of K of degree n in $\overline{K}$ which is Galois with cyclic Galois group. Set $q = |k|$, then the Galois group $Gal(K_n/K)$ has a canonical generator, the Frobenius automorphism $\sigma_{\mathfrak{p}}$, which induces the automorphism of residue class fields given by $x \mapsto x^q$.

It follows from the above remarks that it is enough to study the relative Brauer group $Br(L/K)$ for L/K finite and Galois. We first examine the case that L/K is unramified and then show that each element of $Br(K)$ is split by an unramified extension of K.

With respect to Theorem 2.4.3 the study of $Br(L/K)$ is equivalent to the study of the Norm map $N_{L/K}$ in an unramified extension L/K.

Lemma 2.5.1 *Let K be a local field and L a cyclic unramified extension of K of finite degree. Then every unit $u \in U_K$ is the Norm of a unit of L, hence the norm map $N_{L/K} : U_L \to U_K$ is surjective.*

Proof:(following [Ser79, Chapter V,§2])
Consider the higher principal units $U_L^m = 1 + \mathfrak{p}_L^m$ respectively $U_K^m = 1 + \mathfrak{p}_K^m$, we can then introduce filtrations on U_L and U_K of the form

$$\cdots U_L^{m+1} \subset U_L^m \subset \cdots U_L^2 \subset U_L^1 \subset U_L$$

and

$$\cdots U_K^{m+1} \subset U_K^m \subset \cdots U_K^2 \subset U_K^1 \subset U_K$$

respectively.

We now examine the norm map on this filtrations:
Set $x = 1 + y$ with $y \in \mathfrak{p}_L^n$. Then $\sigma(x) = 1 + \sigma(y)$ for all $\sigma \in G$, furthermore $\sigma(y) \in \mathfrak{p}_L^n$. Hence

$$N_{L/K}(x) = \prod_{\sigma \in G}(1 + \sigma(y)) \equiv 1 + \sum_{\sigma \in G} \sigma(y) \bmod \mathfrak{p}_L^{2n}. \tag{2.1}$$

Since L/K is unramified, we have $\mathfrak{p}_L^n \cap K = \mathfrak{p}_K^n$, therefore $N_{L/K}(x) \equiv 1 \mod \mathfrak{p}_K^n$.

By passage to the quotient the norm map induces maps $N_n : U_L^n/U_L^{n+1} \to U_K^n/U_K^{n+1}$ which we now examine. We first remark that U_L/U_L^1 can be identified with the multiplicative group of the residue class field l, for $n > 1$ we can identify U_L^n/U_L^{n+1} with $\mathfrak{p}_L^n/\mathfrak{p}_L^{n+1}$ which is a one dimensional vectorspace Ω_L^n over l. Since L/K is unramified, we can identify Ω_L^n with $\Omega_K^n \otimes_K l$.

The map N_i can now be described as follows:
for $i = 0$ the map $N_0 : l^\times \to k^\times$ is just the norm map of the extension of residue class fields l/k.
Due to (2.1) $N_i : l \otimes_K \Omega_K^n$ for $i \geq 1$ is just the map $1 \otimes Tr_{L/K}$.

Since in any separable extension the trace map is surjective, again due to (2.1) we obviously have that $N_n : U_L^n/U_L^{n+1} \to U_K^n/U_K^{n+1}$ is surjective.

We now use the following fact:
Assume that we have bijections $U_L \simeq \lim_{\to} U_L/U_L^n$ as well as $U_K \simeq \lim_{\to} U_K/U_K^n$.
Then the surjectivity of the maps $N_n : U_L^n/U_L^{n+1} \to U_K^n/U_K^{n+1}$ implies the surjectivity of $N : U_L \to U_K$.

It remains to check whether these conditions are satisfied in our situation.

For $n \geq 1$ it follows from the observations made above that the map N_n is surjective.
For $n = 0$ we have to consider the norm map $N_0 : l^\times \to k^\times$ which is surjective, since k is a finite field. Therefore the map $N : U_L \to U_K$ is also surjective.$\square$

For crossed products defined with respect to an unramified extension of K we can now give the following classification:

Theorem 2.5.2 *Let K_n/K be the unique unramified extension of K of degree n, let σ be the Frobenius automorphism, then the map*

$$\Theta : \mathbb{Z} \to Br(K_n/K), k \mapsto [(K_n/K, \sigma, \pi^k)],$$

where π is a uniformizing element of K, induces an isomorphism

$$\Theta_n : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} Br(K_n/K).$$

Proof:
By $k \mapsto (K_n/K, \sigma, \pi^k)$ we define a group homomorphism inducing a map $\mathbb{Z}/n\mathbb{Z} \to Br(K_n/K)$.

This induced homomorphism is surjective, since an element of $Br(K_n/K)$ has the form $(K_n/K, \sigma, a)$ with $a \in K^\times$. Decompose $a = u\pi^k$ with a unit u, it follows that

$$A \sim (K_n/K, \sigma, u) \otimes_K (K_n/K, \sigma, \pi^k) \sim (K_n/K, \sigma, \pi^k),$$

since every unit of K is a norm of an unramified extension K_n/K, hence the algebra belonging to u is trivial.

If on the other hand we have $[(K_n/K, \sigma, \pi^k)] = 1$ in $Br(K_n/K)$, we know that $\pi^k = N_{K_n/K}(y)$ with $y \in K_n^\times$. Hence

$$nv_{K_n}(y) = v_K(N_{K_n/K}(y)) = v_K(\pi^k) = k,$$

and thus $k \equiv 0 \bmod n$. We have proven Θ_n to be both injective and surjective, hence Θ_n is a bijection as claimed. $\square$

Theorem 2.5.3 *For given $m, n \in \mathbb{N}$ the following diagram commutes:*

$$\begin{array}{ccc} \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \to & \frac{1}{mn}\mathbb{Z}/\mathbb{Z} \\ \downarrow & & \downarrow \\ Br(K_n/K) & \to & Br(K_{mn}/K). \end{array} \tag{2.2}$$

Hence we get

Theorem 2.5.4 *Let K be a local field. Then we have an isomorphism*

$$\Theta : \mathbb{Q}/\mathbb{Z} \simeq Br(K) \textit{ with } \Theta(k/n \bmod \mathbb{Z}) = [(K_n/K, \sigma_n, \pi^k)],$$

for $n \in \mathbb{N}$ and $0 \leq k \leq n$, where σ_n denotes the Frobenius element of K_n/K.

Proof:
We have $\mathbb{Q}/\mathbb{Z} = \cup_{n\in\mathbb{N}} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, furthermore $Br(K) = \cup_{n\in\mathbb{N}} Br(K_n/K)$. For the relative Brauer group we have an isomorphism $\Theta_n : \mathbb{Z}/n\mathbb{Z} \simeq Br(K_n/K)$, also $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \simeq Br(K_n/K)$. From the commutativity of (2.2) we get an isomorphism $\mathbb{Q}/\mathbb{Z} \simeq Br(K)$. $\square$

Definition 2.5.5 *The inverse of* Θ^{-1} *from Theorem 2.5.4 is called invariant map.*

$$inv : Br(K) \to \mathbb{Q}/\mathbb{Z}, [A] = [(K_n/K, \sigma_n, \pi^k)] \mapsto inv(A) = \frac{k}{n} \bmod \mathbb{Z}.$$

Instead of using the original definition of the invariant map, it is sometimes convenient to use the map $n \cdot \text{inv}$ for an algebra A with $[A]^n = 1$ instead. By abuse of language we will refer to both of these maps as invariant map.

2.6 The Brauer Group of a Global Field

Let K be a number field, i. e. a finite algebraic extension of $\mathbb{Q}$. Let S denote a system of representatives of the places $\mathfrak{p}$ of K. Besides the non–archimedean places $\mathfrak{p}$ for which the completion $K_\mathfrak{p}$ of K with respect to $\mathfrak{p}$ is a local field, we also have to consider the archimedean primes for which $K_\mathfrak{p}$ is either equal to $\mathbb{C}$ or to $\mathbb{R}$.

For the local Brauer groups we have the following results:

- If $\mathfrak{p}$ is an archimedean place we have that $K_\mathfrak{p}$ is a local field and $Br(K_\mathfrak{p}) \simeq \mathbb{Q}/\mathbb{Z}$.
- Is $\mathfrak{p}$ a real place we have $K_\mathfrak{p} \simeq \mathbb{R}$ and
$$Br(K_\mathfrak{p}) \simeq \mathbb{Z}/2\mathbb{Z} \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}.$$
.
- If $\mathfrak{p}$ is a complex place we have $K_\mathfrak{p} \simeq \mathbb{C}$ and $Br(K_\mathfrak{p}) = 1$.

The embeddings $K \hookrightarrow K_\mathfrak{p}$ induce a group homomorphism $Br(K) \to \oplus_\mathfrak{p} Br(K_\mathfrak{p})$.

The most important statement about Brauer groups of global fields is the fact that the global elements are completely described by the image in the local Brauer groups:

Theorem 2.6.1 (Hasse–Brauer–Noether) *There is an exact sequence*

$$0 \to Br(K) \to \oplus_{\mathfrak{p}\in S} Br(K_\mathfrak{p}) \to \mathbb{Q}/\mathbb{Z} \to 0, \tag{2.3}$$

where the last map is given by $(A_\mathfrak{p})_{\mathfrak{p}\in S} \mapsto \sum_{\mathfrak{p}\in S} inv(A_\mathfrak{p})$.

In the following chapters this exact sequence will play a major role both in a theoretical as well as a practical sense.

2.7 Discrete Logarithms in Finite Fields

Let $k = \mathbb{F}_q$ be a finite field satisfying $l|q-1$, meaning that the l–th roots of unity are contained in k.

We can then consider the discrete logarithm problem in the group of l–th roots of unity: given two non trivial l–th roots of unity ζ_0 and $\zeta_1 \in \langle\zeta_0\rangle$, determine n mod l such that $\zeta_1 = \zeta_0^n$ holds.

As we have pointed out before (see 1.2), the question whether the embedding of this group of order l into the larger group $\mathbb{F}_q^\times$ essentially gives the same security as considering the discrete logarithm in $\mathbb{F}_q^\times$ is essential for the security of the Digital Signature Algorithm (DSA).

Therefore it is interesting to consider this question in the context of Brauer groups, since they give an approach especially suited for this discrete logarithm problem.

Let K be a local field with residue class field $k = \mathbb{F}_q$, let L/K be a ramified cyclic Galois extension of degree l with $l \neq char(k)$ and $Gal(L/K) = \langle\sigma\rangle$.

In this situation we get the following description of the relative Brauer group $Br(L/K)$:

Lemma 2.7.1 *Let K be a finite extension of $\mathbb{Q}_p$ with residue class field k. Let L/K be a ramified extension of prime degree $l \neq p$ implying that the group μ_l of l–th roots of unity is contained in $K^\times$. Then we have $Br(L/K) \simeq k^\times/(k^\times)^l \simeq \mu_l(k)$.*

Proof:(for further details see [Ser79, V.,§3.])
We have $Br(L/K) \simeq K^\times/N_{L/K}(L^\times)$ according to theorem 2.4.3. Hence we have to examine the norm map of the ramified extension L von K.

Each element of K can be written in the form $u \cdot \pi^i$ with $u \in U_K$ and $i \in \mathbb{Z}$. Since L/K is ramified, π_K is a norm.Therefore we can restrict our attention to the groups of units U_L of L.

Consider the filtrations

$$\cdots U_L^i \subset U_L^{i-1} \subset \cdots U_L^1 \subset U_L$$

and

$$\cdots U_K^i \subset U_K^{i-1} \subset \cdots U_K^1 \subset U_K,$$

where we put $U_L^i = 1 + \mathfrak{p}_L^i$ and $U_K^i = 1 + \mathfrak{p}_K^i$ for $i \geq 1$.

Since L/K is tamely ramified (we have $l \neq p$), all quotients U_K^i/U_K^{i+1} for $i \geq 1$ are killed by the norm map ([Ser79, V, Proposition 5 and Corollaries]), only the case $U_L/U_L^1 \to U_K/U_K^1$ remains to be examined. We have $U_L/U_L^1 \simeq l^\times$ and $U_K/U_K^1 \simeq k^\times$. Since L/K is ramified we have $l = k$. The image of U_L/U_L^1 under the norm map therefore is $k^{\times l}$. Hence we have

$$K^\times/N_{L/K}(L^\times) \simeq k^\times/k^{\times l}.$$

We have an isomorphism

$$k^\times/k^{\times l} \simeq \mu_l$$

given by

$$x \bmod k^{\times l} \mapsto x^{\frac{q-1}{l}}.$$

$\square$.

From Theorem 2.4.3 and Lemma 2.7.1 we get $\mu_l(k) \xrightarrow{\sim} Br(L/K)$, since $l \neq char(k)$. Here the map is given by $\zeta \mapsto (L, \sigma, \zeta) \in Br(L/K)$.

Hence we can solve the discrete logarithm problem in the cyclic subgroup $\mu_l \subset \mathbb{F}_q^\times$ as follows:
Given two l–th roots of unity ζ_0 and ζ_1 with $\zeta_1 = \zeta_0^n$ we choose an extension K of $\mathbb{Q}_p$ with $k = \mathbb{F}_q$ as well as a ramified Galois extension L/K of degree l with $Gal(L/K) = \langle\sigma\rangle$. Now forming the cyclic algebras $A_0 = (L/K, \sigma, \zeta_0)$ and $A_1 = (L/K, \sigma, \zeta_1)$, the discrete logarithm problem is solved if we are able to compute $\mathrm{inv}(A_0)$ and $\mathrm{inv}(A_1) = n \cdot \mathrm{inv}(A_0)$. Thus n can be obtained by computing

$$\mathrm{inv}(A_1)/\mathrm{inv}(A_0) \bmod l.$$

Hence we are lead to this computational task:
Given a cyclic algebra $A = (L/K, \sigma, \zeta)$ defined over a tamely ramified extension of prime degree l compute the invariant of this algebra as an element of $Br(K)$.

Chapter 3

Local Computation of Invariants

In the previous section we showed the importance of the invariant map of the theory of Brauer groups for cryptographic applications.

This section will be concerned with the explicit calculation of this map over local fields. As shown in the previous section the case of an algebra defined over a tamely ramified extension of a local field K is of special interest.

3.1 Unramified Extensions

Let K be a local field complete with respect to a discrete valuation $\mathfrak{p}$, let $k_{\mathfrak{p}}$ denote the residue class field of K with respect to $\mathfrak{p}$. Assume $k_{\mathfrak{p}} = \mathbb{F}_q$.

In the following we will assume that $l|(q-1)$ holds, meaning that the l–th roots of unity are contained in K.

Now let L/K be an unramified extension of prime degree l, since we assumed that the l–th roots of unity are contained in K by Kummer theory there exists an $\alpha \in K^*/K^{*l}$ such that $L = K(\alpha^{1/l})$.

The field extension L/K is cyclic Galois, assume $Gal(L/K) = \langle\sigma\rangle$.
Consider an element of order l inside $Br(K)$ given by the two–cocycle

$$\phi(\sigma^i, \sigma^j) = \begin{cases} \beta & : \quad i+j \geq l \\ 1 & : \quad i+j < l. \end{cases}$$

Let U_L and U_K denote the groups of unity of L and K respectively. As we have noted before (see Theorem 2.5.1) in an unramified extension L/K each element of U_K is a norm coming from a unity of L. Let π be a prime element then we can assume that β is of the form $\beta = \pi^n$. Hence we get:

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

If σ is the Frobenius element $\sigma_{\mathfrak{p}}$, the invariant map can be computed immediately since by definition $\mathrm{inv}(\phi(\sigma_{\mathfrak{p}}^i, \sigma_{\mathfrak{p}}^j)) \equiv n \bmod l$.
Suppose $\sigma^k = \sigma_{\mathfrak{p}}$, then we obtain:

$$(L, \sigma, \pi^n) \simeq (L, \sigma^k, \pi^{nk}) \simeq (L, \sigma_{\mathfrak{p}}, \pi^{nk}).$$

Hence we get $\mathrm{inv}(\phi(\sigma^i, \sigma^j)) \equiv nk \bmod l$.

Therefore in this case we have reduced the computation of the invariant map to the problem of describing the relation between a generator σ of the Galois group $Gal(L/K)$ and the Frobenius element $\sigma_{\mathfrak{p}}$ of the extension L/K, i.e. solving a discrete logarithm in the Galois group of L/K.

Since we are in the situation of Kummer extensions, this can be accomplished as follows:
Recall that σ acts on $\gamma = \alpha^{1/l}$ via $\sigma(\gamma) = \zeta_l \gamma$ with a primitive l–th root of unity ζ_l.
Let $\overline{x}$ denote the reduction of an element $x \in K$ in the residue class field $k_{\mathfrak{p}} = \mathbb{F}_q$.

The Frobenius automorphism acts on elements of the extension $l_{\mathfrak{p}}/k_{\mathfrak{p}}$ by raising to the q–th power: $\sigma_{\mathfrak{p}}(\overline{x}) = \overline{x}^q$. Hence the action of the Frobenius on $\overline{\gamma}$ is given by

$$\sigma_{\mathfrak{p}}(\overline{\gamma})/\overline{\gamma} = \overline{\gamma}^q/\overline{\gamma} = \overline{\alpha}^{q/l}/\overline{\alpha}^{1/l} = \overline{\alpha}^{\frac{q-1}{l}}. \tag{3.1}$$

In order to describe σ as a power of the Frobenius we have to solve the discrete logarithm $(\overline{\alpha}^{\frac{q-1}{l}})^k = \overline{\zeta_l}$ in $\mathbb{F}_q$.

3.2 Tamely Ramified Extensions

We have seen before (see 2.7) that the case of a two–cocycle defined over a tamely ramified extension L/K of prime degree l is especially interesting.

Note that we only consider the case $l \neq \mathrm{char}(k_{\mathfrak{p}})$.
We keep the assumptions on K from the previous section, especially assume $\zeta_l \in K^\times$ (otherwise an extension of the described type would not exists). For technical reasons also suppose that $\zeta_{l^2} \notin K$ holds.

Let $Gal(L/K) = \langle \sigma \rangle$ be cyclic of order l, consider an element of order l in the Brauer group $Br(K)$ given by the two–cocycle

$$\phi(\sigma^i, \sigma^j) = \begin{cases} \beta & : \quad i+j \geq l \\ 1 & : \quad i+j < l \end{cases}$$

with $\beta \in K^*/N_{L/K}(L^*)$.

Since we have $l \neq \mathrm{char}(k_{\mathfrak{p}})$ we see that L/K is tamely ramified, hence (see Theorem 2.7.1) we have $K^*/N_{L/K}(L^*) = k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*l} \simeq \langle \zeta_l \rangle$. Therefore we can assume that $\beta \in \langle \zeta_l \rangle$ holds.

In order to compute the invariant of the algebra given by ϕ, we consider the following situation:
Let L/K be cyclic and tamely ramified of prime degree l. Let K_l/K be the unramified extension of degree l, assume $Gal(K_l/K) = \langle \sigma_{\mathfrak{p}} \rangle$ where $\sigma_{\mathfrak{p}}$ denotes the Frobenius automorphism.

$$\begin{tikzcd}
 & K_lL & \\
L \arrow[ur] & & K_l \arrow[ul] \\
 & K \arrow[ul, "\langle \sigma \rangle"', "\text{ramified}"] \arrow[ur, "\langle \sigma_{\mathfrak{p}} \rangle", "\text{unramified}"'] &
\end{tikzcd}$$

This diagram gives us the following diagram in Galois cohomology:

$$\begin{tikzcd}
 & H^2(K_lL/K, (K_lL)^*) & \\
H^2(L/K, L^*) \arrow[ur, "\mathrm{infl}_L^{K_lL}"'] & & H^2(K_l/K, K_l^*) \arrow[ul, "\mathrm{infl}_{K_l}^{K_lL}"']
\end{tikzcd}$$

Our task can be described as follows:

We have to find a cocycle ψ in $H^2(K_l/K, K_l^*)$ such that the inflation $\hat{\psi} = \mathrm{infl}_{K_l}^{K_lL}(\psi)$ differs from the inflation $\hat{\phi} = \mathrm{infl}_L^{K_lL}(\phi)$ only by a coboundary.

The inflations of the two cocycles can be described explicitly as follows:
Set $Gal(L/K) = \langle \sigma \rangle$ and $Gal(K_l) = \langle \sigma_{\mathfrak{p}} \rangle$, hence we have $Gal(LK_l) = \langle \sigma, \sigma_{\mathfrak{p}} \rangle$.

We then get

$$\hat{\phi}(\sigma^i\sigma_{\mathfrak{p}}^j, \sigma^r\sigma_{\mathfrak{p}}^s) = \phi(\sigma^i, \sigma^r) \quad \text{with} \quad 1 \leq i, j, r, s \leq l$$

and

$$\hat{\psi}(\sigma^i\sigma_{\mathfrak{p}}^j, \sigma^r\sigma_{\mathfrak{p}}^s) = \psi(\sigma_{\mathfrak{p}}^j, \sigma_{\mathfrak{p}}^s) \quad \text{with} \quad 1 \leq i, j, r, s \leq l.$$

Now $\hat{\psi}$ is cohomologous to $\hat{\phi}$ iff there is a map $\theta : Gal(LK_l/K) \to (LK_l)^*$ such that:

$$\hat{\phi}(z_1, z_2) = \hat{\psi}(z_1, z_2)\theta(z_2)\theta(z_1z_2)^{-1}\theta(z_1)^{z_2}$$

for all $z_1, z_2 \in Gal(LK_l/K)$.
It turns out that the function θ is already determined by its values $\theta(\sigma)$ and $\theta(\sigma_{\mathfrak{p}})$.
Some basis properties of θ are summed up in the following lemma:

Lemma 3.2.1 *1.* $\theta(1) = 1$.

2. $\beta = N_{LK_l/K_l}(\theta(\sigma))$.

3. $\pi^{-n} = N_{LK_l/L}(\theta(\sigma_{\mathfrak{p}}))$.

4. $\theta(\sigma\sigma_{\mathfrak{p}}) = \theta(\sigma_{\mathfrak{p}})\theta(\sigma)^{\sigma_{\mathfrak{p}}} = \theta(\sigma)\theta(\sigma_{\mathfrak{p}})^{\sigma}$.

Proof:
1.: Trivial.
2.: We have

$$\theta(\sigma)\theta(\sigma^{i+1})^{-1}\theta(\sigma^i)^{\sigma} = \hat{\phi}(\sigma^i, \sigma)\hat{\psi}(\sigma^i, \sigma)^{-1}, \tag{3.2}$$

and furthermore $\hat{\phi}(\sigma^i, \sigma) = \phi(\sigma^i, \sigma) = 1$ for $i < l-1$ and $\hat{\psi}(\sigma^i, \sigma) = \psi(1, 1) = 1$.
Hence using (3.2) we immediately get

$$\theta(\sigma^{i+1}) = \theta(\sigma)\theta(\sigma^i)^{\sigma}. \tag{3.3}$$

Now we conclude inductively for $i < l - 1$:

$$\theta(\sigma^{i+1}) = \theta(\sigma)\theta(\sigma)^{\sigma} \cdots \theta(\sigma)^{l-2}, \tag{3.4}$$

For $i = l-1$ we get:

$$\begin{aligned}\theta(\sigma)\theta(\sigma^l)^{-1}\theta(\sigma^{l-1})^{\sigma} &= \theta(\sigma)\theta(\sigma^{l-1})^{\sigma} \\ &= \hat{\phi}(\sigma^{l-1},\sigma)\hat{\psi}(\sigma^{l-1},\sigma)^{-1} \\ &= \phi(\sigma^{l-1},\sigma)\psi(1,1) \\ &= \beta.\end{aligned} \tag{3.5}$$

Using (3.4) we obtain:

$$\beta = \theta(\sigma)\theta(\sigma)^{\sigma}\cdots\theta(\sigma)^{\sigma^{l-1}}. \tag{3.6}$$

Since L/K is cyclic Galois with $Gal(L/K) = \langle\sigma\rangle$ it follows that

$$x = \prod_{i=0}^{l-1}\theta(\sigma)^{\sigma^i} = N_{L/K}(\theta(\sigma)). \tag{3.7}$$

3.: Considering $\theta(\sigma_{\mathfrak{p}})$ we can conclude analogous to **2.** that

$$\theta(\sigma_{\mathfrak{p}}^{i+1}) = \theta(\sigma_{\mathfrak{p}})\theta(\sigma_{\mathfrak{p}})^{\sigma_{\mathfrak{p}}}\cdots\theta(\sigma_{\mathfrak{p}})^{i}\,\text{for}\, i < l-1 \tag{3.8}$$

holds.

From $\hat{\phi}(\sigma_{\mathfrak{p}}^{l-1},\sigma_{\mathfrak{p}}) = \phi(1,1)$ and $\hat{\psi}(\sigma_{\mathfrak{p}}^{l-1},\sigma_{\mathfrak{p}}) = \psi(\sigma_{\mathfrak{p}}^{l-1},\sigma_{\mathfrak{p}}) = \pi^n$ we get

$$\pi^{-n} = \prod_{i=0}^{l-1}\theta(\sigma_{\mathfrak{p}})^{\sigma_{\mathfrak{p}}^i} = N_{K_l/K}(\theta(\sigma_{\mathfrak{p}})), \tag{3.9}$$

since K_l/K is cyclic Galois with $Gal(K_l/K) = \langle\sigma_{\mathfrak{p}}\rangle$.

4.: Considering $\theta(\sigma\sigma_{\mathfrak{p}})$ we obtain

$$\hat{\phi}(\sigma,\sigma_{\mathfrak{p}}) = \phi(\sigma,1) = 1 = \phi(1,\sigma) = \hat{\phi}(\sigma_{\mathfrak{p}},\sigma) \tag{3.10}$$

and

$$\hat{\phi}(\sigma,\sigma_{\mathfrak{p}}) = \phi(1,\sigma_{\mathfrak{p}}) = 1 = \phi(\sigma_{\mathfrak{p}},1) = \hat{\phi}(\sigma_{\mathfrak{p}},\sigma), \tag{3.11}$$

using (3.2) we obtain

$$\theta(\sigma_{\mathfrak{p}})\theta(\sigma\sigma_{\mathfrak{p}})^{-1}\theta(\sigma)^{\sigma_{\mathfrak{p}}} = \theta(\sigma)\theta(\sigma\sigma_{\mathfrak{p}})^{-1}\theta(\sigma_{\mathfrak{p}})^{\sigma}, \tag{3.12}$$

hence

$$\theta(\sigma_{\mathfrak{p}})\theta(\sigma)^{\sigma_{\mathfrak{p}}} = \theta(\sigma)\theta(\sigma_{\mathfrak{p}})^{\sigma}. \tag{3.13}$$

□

Using these elementary properties of θ we can now proceed to find a suitable coboundary transforming the cocycle ϕ into the cocycle ψ. Here it is most important to choose L/K and K_l/K carefully. This has to be done in such a way that the operation of σ and $\sigma_{\mathfrak{p}}$ in 3.2.1[4.] can be related to each other.

Theorem 3.2.2 *Let K be a local field with $\zeta_l \in K$ and $\zeta_{l^2} \notin K$. Let π be an element of K such that $v(\pi) = 1$.*
Let K_l/K be unramified of degree Grad l over K with Frobenius automorphism $\sigma_{\mathfrak{p}}$ generating $Gal(K_l/K)$.
Realize $K_l = K(\alpha^{1/l})$ as a Kummer extension. Fix the l–th root of unity ζ defining the action of $\sigma_{\mathfrak{p}}$ on $\alpha^{1/l}$:

$$\sigma_{\mathfrak{p}}(\alpha^{1/l}) = \zeta\alpha^{1/l}.$$

Let $L = K(\pi^{1/l})/K$ be cyclic ramified of degree l ($l \neq char(k_{\mathfrak{p}})$) and $Gal(L/K) = \langle\sigma\rangle$. Here σ is defined by $\sigma(\pi^{1/l}) = \zeta\pi^{1/l}$.
Let $\phi \in H^2(\langle\sigma\rangle, L^*)$ be given by

$$\phi(\sigma^i, \sigma^j) = \begin{cases} \zeta^m & : \quad i+j \geq l \\ 1 & : \quad i+j < l. \end{cases}$$

Let $\psi \in H^2(K_l/K, K_l^*) = H^2(\langle\sigma_{\mathfrak{p}}\rangle, K_l^*)$ be given by

$$\psi(\sigma_{\mathfrak{p}}^i, \sigma_{\mathfrak{p}}^j) = \begin{cases} \pi^n & : \quad i+j \geq l \\ 1 & : \quad i+j < l. \end{cases}$$

Then ϕ and ψ are cohomologous in $H^2(Gal(LK_l/K), (LK_l)^\times)$ if

$$n \equiv -tm \bmod l$$

with $t \equiv (q-1)/l \bmod l$.

Corollary 3.2.3 *The element of $Br(K)$ given by ϕ has invariant*

$$-tm \bmod l$$

.

Proof: We first compute $\theta(\sigma)$ and $\theta(\sigma_{\mathfrak{p}})$. Lemma 3.2.1[4.] gives a relation between these elements and the action of $\sigma, \sigma_{\mathfrak{p}}$ on them. It turns out that the invariant can be computed from this relation.

Lemma 3.2.1[1.] implies that $\beta = N_{LK_l/K_l}(\theta(\sigma))$. Since we have $\zeta \in K$ and $\zeta_{l^2} \notin K$, an unramified extension of degree l over K is defined by $\zeta^{1/l}$. Since this extension is uniquely determined we have $\zeta^{1/l} \in L$. Hence from $\beta = \zeta^m$ we get $\beta = ((\zeta^m)^{1/l})^l = N_{LK_l/K_l}((\zeta^m)^{1/l})$. Therefore we have:

$$N_{LK_l/K_l}\left(\frac{\theta(\sigma)}{(\zeta^m)^{1/l}}\right) = 1.$$

Hilbert 90 implies that

$$\theta(\sigma) = (\zeta^m)^{1/l} x_1^{\sigma - 1} \tag{3.14}$$

with $x_1 \in (LK_l)^*$ holds.

Now consider LK_l/L instead of LK_l/K_l. Since we have $(\pi^{-n})^{1/l} \in L$ it follows that

$$N_{LK_l/L}((\pi^{-n})^{1/l}) = ((\pi^{-n})^{1/l})^l = \pi^{-n},$$

hence we obtain

$$\theta(\sigma_{\mathfrak{p}}) = (\pi^{-n})^{1/l} x_2^{\sigma_{\mathfrak{p}} - 1} \tag{3.15}$$

with $x_2 \in (LK_l)^*$.

It follows from 3.2.1[4.] that

$$\theta(\sigma_{\mathfrak{p}})\theta(\sigma)^{\sigma_{\mathfrak{p}}} = \theta(\sigma)\theta(\sigma_{\mathfrak{p}})^{\sigma}. \tag{3.16}$$

The action of the Frobenius $\sigma_{\mathfrak{p}}$ on $\zeta^{1/l}$ is given by raising to the $q = p^f$–th power. Hence we get

$$\theta(\sigma)^{\sigma_{\mathfrak{p}}} = ((\zeta^m)^{1/l} x_1^{\sigma-1})^{\sigma_{\mathfrak{p}}} = \zeta^{mq/l} x_1^{\sigma_{\mathfrak{p}}\sigma - \sigma_{\mathfrak{p}}}. \tag{3.17}$$

The action of σ on $\pi^{1/l}$ is given by $\sigma(\pi^{1/l}) = \zeta\pi^{1/l}$, hence we get

$$\theta(\sigma_{\mathfrak{p}})^{\sigma} = ((\pi^{-n})^{1/l} x_2^{\sigma_{\mathfrak{p}}-1})^{\sigma} = \zeta^{-n}(\pi^{-n})^{1/l} x_2^{\sigma\sigma_{\mathfrak{p}} - \sigma}. \tag{3.18}$$

Inserting (3.14) and (3.15) in (3.16), we get

$$((\pi^{-n})^{1/l} x_2^{\sigma_{\mathfrak{p}}-1})\theta(\sigma)^{\sigma_{\mathfrak{p}}} = ((\zeta^m)^{1/l} x_1^{\sigma-1})\theta(\sigma_{\mathfrak{p}})^{\sigma}. \tag{3.19}$$

Now considering (3.17) and (3.18) we obtain

$$(\pi^{-n})^{1/l} x_2^{\sigma_{\mathfrak{p}}-1} \zeta^{mq/l} x_1^{\sigma\sigma_{\mathfrak{p}} - \sigma_{\mathfrak{p}}} = (\zeta^m)^{1/l} x_1^{\sigma-1} \zeta^{-n} (\pi^{-n})^{1/l} x_2^{\sigma\sigma_{\mathfrak{p}} - \sigma}. \tag{3.20}$$

At this point we use the fact that both extensions L/K and K_l/K are defined in such a way, that both the operation of σ and of $\sigma_{\mathfrak{p}}$ on appropriate primitive elements are described by the same l–th root of unity ζ.
Equivalently this gives

$$\zeta^{-n-m(q-1)/l} = x_1^{\sigma\sigma_{\mathfrak{p}} - \sigma_{\mathfrak{p}} - \sigma + 1} x_2^{\sigma_{\mathfrak{p}} - \sigma\sigma_{\mathfrak{p}} + \sigma_{\mathfrak{p}} - 1} = (\frac{x_1}{x_2})^{(\sigma-1)(\sigma_{\mathfrak{p}}-1)}. \tag{3.21}$$

Now inserting $x = (\frac{x_1}{x_2})^{\sigma-1}$ we can write (3.21) in the form

$$x^{\sigma_{\mathfrak{p}}} = \zeta^{-n-m(q-1)/l}x. \tag{3.22}$$

We now proceed by rewriting this relation in such a form that we can solve for n in this equation.

To do this we first try to change x in such a way that the new element is fixed by $\sigma_{\mathfrak{p}}$, hence does not lie in LK_l but in K_l.

Hence we want to find an element $c \in LK_l$ such that $c^{\sigma_{\mathfrak{p}}}/c = \zeta^{n+tm}$ holds. We have $(\zeta^{1/l})^{\sigma_{\mathfrak{p}}}/\zeta^{1/l} = \zeta^{(q-1)/l}$. The fact that $\zeta_l \in K$ and $\zeta_{l^2} \notin K$ implies $l|(q-1)$ and $(q-1)/l \not\equiv 0 \bmod l$. Therefore we can compute $((q-1)/l)^{-1} \bmod l$.

We now have

$$((\zeta^{1/l})^{-((q-1)/l)^{-1}n-m})^{\sigma_{\mathfrak{p}}-1} = \zeta^{-n-m(q-1)/l}. \tag{3.23}$$

Hence for $x/((\zeta^{1/l})^{-((q-1)/l)^{-1}n-m})$ we have

$$(x/((\zeta^{1/l})^{-((q-1)/l)^{-1}n-m}))^{\sigma_{\mathfrak{p}}} = x/((\zeta^{1/l})^{-((q-1)/l)^{-1}n-m}). \tag{3.24}$$

Thus we have

$$x = (\frac{x_1}{x_2})^{\sigma-1} = (\zeta^{1/l})^{-((q-1)/l)^{-1}n-m)}x_L \tag{3.25}$$

with $x_L \in L$.

Now applying the norm with respect to LK_l/K_l to equation (3.25) we get:

$$1 = (\zeta)^{-((q-1)/l)^{-1}n-m}N_{L/K}(x_L), \tag{3.26}$$

since $(\frac{x_1}{x_2})^{\sigma-1}$ is in the kernel of the norm map.

Hence we have $\zeta^{-n-m(q-1)/l} \in N_{L/K}(L^*)$. We have that $\zeta \notin N_{L/K}(L^*)$ holds since otherwise this would imply $\zeta_{l^2} \in K$ contrary to our assumptions. Whence

$$n \equiv -m(q-1)/l \bmod l \tag{3.27}$$

as claimed. □

Chapter 4

Local–global–methods

4.1 Introduction

In Chapter 3 we introduced methods from Galois cohomology of local fields in order to compute the invariant of an element of $Br(K_\mathfrak{p})$ for a local field $K_\mathfrak{p}$.

We will now show how we can make use of local–global methods in order to calculate the invariant map at a given place of a global field K.

Let S be a set of non–equivalent places of K, let $K_\mathfrak{p}$ for $\mathfrak{p} \in S$ denote the completion of K with respect to $\mathfrak{p}$. For each place $\mathfrak{p}$ we have an invariant map $\mathrm{inv}_\mathfrak{p} : Br(K_\mathfrak{p}) \to \mathbb{Q}/\mathbb{Z}$.

As explained in Chapter 2 the celebrated theorem by Hasse, Brauer and Noether gives a relationship between the Brauer group $Br(K)$ of the global field K and the Brauer groups $Br(K_\mathfrak{p})$ of the completions of K.

Theorem 4.1.1 *We have a short exact sequence*

$$0 \to Br(K) \to \bigoplus_{\mathfrak{p} \in S} Br(K_\mathfrak{p}) \overset{\sum inv_\mathfrak{p}}{\to} \mathbb{Q}/\mathbb{Z} \to 0, \tag{4.1}$$

where $Br(K) \to \oplus_{\mathfrak{p} \in S} K_\mathfrak{p}$ *is given by* $A \mapsto \oplus_\mathfrak{p}(A \otimes K_\mathfrak{p})$ *and the map*

$$\oplus_{\mathfrak{p} \in S} K_\mathfrak{p} \overset{\sum inv_\mathfrak{p}}{\to} \mathbb{Q}/\mathbb{Z}$$

is defined by

$$\oplus_{\mathfrak{p}}(A \otimes K_{\mathfrak{p}}) \mapsto \sum_{\mathfrak{p} \in S} inv_{\mathfrak{p}}(A \otimes K_{\mathfrak{p}}).$$

This can be interpreted in the following way: the local invariants of a given global element A of $Br(K)$ determine this element completely. Furthermore these local invariants satisfy the equation $0 = \sum_{\mathfrak{p} \in S} \mathrm{inv}_{\mathfrak{p}}(A \otimes K_{\mathfrak{p}})$ in $\mathbb{Q}/\mathbb{Z}$.

4.2 Explicit Computation of Invariants

Consider a local field $K_{\mathfrak{p}}$ and an element $A_{\mathfrak{p}}$ of $Br(K_{\mathfrak{p}})$. For the sake of simplicity we will assume that $A_{\mathfrak{p}}$ is of prime order l in $Br(K_{\mathfrak{p}})$. Our task is to compute $\mathrm{inv}(A_{\mathfrak{p}})$ efficiently.

Furthermore assume that $A_{\mathfrak{p}} \in Br(K_{\mathfrak{p}})$ is given in the form $A_{\mathfrak{p}} = (L_{\mathfrak{p}}/K_{\mathfrak{p}}, \sigma, a_{\mathfrak{p}})$. Here $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ is a cyclic extension of degree l, σ is a generator of the Galois group $G_{\mathfrak{p}} = Gal(L_{\mathfrak{p}}/K_{\mathfrak{p}})$ and $a_{\mathfrak{p}} \in K_{\mathfrak{p}}^*/N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^*)$.

In order to use local–global methods we have to lift the given local algebra $A_{\mathfrak{p}}$ to a global algebra A. Then the relation given by the Hasse–Brauer–Noether theorem shows that the invariant at $\mathfrak{p}$ – which we are interested in – can be recovered from the knowledge of the invariants at all other places $\mathfrak{q} \neq \mathfrak{p}$ for which we have $\mathrm{inv}_{\mathfrak{q}}(A) \neq 0$.

Assume that the prime ideal $\mathfrak{q}$ is unramified in L/K. Also assume that the global lift A is given now as a global cyclic algebra of the form $(L/K, \sigma, a)$. From the definition of the invariant map, we know that the explicit calculation of the invariant of A at the place $\mathfrak{q}$ is related to two problems:

- Computing $v_{\mathfrak{q}}(a)$, the $\mathfrak{q}$–adic valuation of a.
- Computing an integer $f_{\mathfrak{q}}$ such that $\sigma^{f_{\mathfrak{q}}}$ is the Frobenius $\sigma_{\mathfrak{q}}$ at $\mathfrak{q}$.

While the first task is easy to solve (see for example [Coh96, Algorithm 4.8.17]), the second task is much more difficult. Indeed, we have seen in Chapter 3.1 that this question is directly related to solving a discrete logarithm problem in a finite field, at least in the case that we deal with a local Kummer extension.

Note, however, that the Hasse–Brauer–Noether theorem predicts the existence of a global algebra A which has non trivial invariant exactly at two places $\mathfrak{p}$ and $\mathfrak{q}$, where $\mathfrak{p}$ is the place we are interested in and $\mathfrak{q}$ is any other place of K. Therefore, theoretically we should be able to relate the problem of calculating the invariant at $\mathfrak{p}$ to a task as easy as possible. However the statement of the theorem is simply an existence statement. We will show in the following what kind of techniques one might use in order to explicitly construct such algebras.

4.3 Explicit Construction of Global Algebras

In order to construct a global lift of the local algebra $A_{\mathfrak{p}}$, we first construct a global cyclic extension L of K with prescribed local behavior at the place $\mathfrak{p}$.

The easiest way to do this is to use Kummer theory. Thus we assume, that K contains the l–th roots of unity and that we have $L = K(\alpha^{1/l})$ with $\alpha \in K^\times/K^{\times l}$.

The local behavior of such a Kummer extension can be described as follows (see [Coh00, Theorem 10.2.9]):

Theorem 4.3.1 *Let K be a number field, l a prime such that $\zeta_l \in K$ holds and $L = K(\alpha^{1/l})$ with $\alpha \in K^\times/K^{\times l}$. Let $\mathfrak{q}$ be a place of K. Set $e = v_{\mathfrak{q}}(l)$.*

1. *If $(v_{\mathfrak{q}}(\alpha), l) = 1$ holds, then $\mathfrak{q}$ is ramified.*
2. *If $(v_{\mathfrak{q}}(\alpha), l) = l$ and $\mathfrak{q} \nmid l$ holds, we have that*
   - *$\mathfrak{q}$ splits completely, if the congruence $x^l \equiv \alpha \bmod \mathfrak{q}$ has a solution.*
   - *$\mathfrak{q}$ is inert, if the congruence $x^l \equiv \alpha \bmod \mathfrak{q}$ has no solution.*
3. *If $(v_{\mathfrak{q}}(\alpha), l) = l$ and $\mathfrak{q}|l$ hold, we have that*
   - *$\mathfrak{q}$ splits completely, if the congruence $x^l \equiv \alpha \bmod \mathfrak{q}^{el+1}$ has a solution.*
   - *$\mathfrak{q}$ is inert, if the congruence $x^l \equiv \alpha \bmod \mathfrak{q}^m$ has a solution for $m = el$ but not for $m = el + 1$.*

- $\mathfrak{q}$ *is ramified, if the congruence* $x^l \equiv \alpha \bmod \mathfrak{q}^{el}$ *has no solution.*

The Galois group G of the global extension L/K is given by $G_\mathfrak{p} = \langle\sigma\rangle$, here σ is determined by $\sigma(\alpha^{1/l}) = \zeta_l \alpha^{1/l}$ for a fixed l–th root of unity ζ_l.
Lifting a local cyclic algebra to a global one is easy:
we simply have to choose an element $a \in K$ which lifts $a_\mathfrak{p} \in K_\mathfrak{p}$. Then the global cyclic algebra $(L/K, \sigma, a)$ coincides locally at $\mathfrak{p}$ with the given algebra $A_\mathfrak{p}$.
This means that A has invariant $\mathrm{inv}_\mathfrak{p}(A_\mathfrak{p})$ at $\mathfrak{p}$. Let $res_\mathfrak{q} : Br(K) \to Br(K_\mathfrak{q})$ denote the restriction map for a place $\mathfrak{q}$ of K given by $A \mapsto A \otimes K_\mathfrak{q}$, then we also have $\mathrm{inv}_\mathfrak{q}(A_\mathfrak{q}) = \mathrm{inv}_\mathfrak{q}(res_p(A))$. In the following we will identify $\mathrm{inv}_\mathfrak{q}(A) = \mathrm{inv}_\mathfrak{q}(A \otimes K_\mathfrak{q})$.

In order to make use of the Hasse–Brauer–Noether theorem we now have to determine the places $\mathfrak{q} \neq \mathfrak{p}$ of K for which the global algebra A has a non–trivial invariant.

We first note that $\mathrm{inv}_\mathfrak{q}(A)$ is automatically trivial if $\mathfrak{q}$ splits completely in L/K since in this case $L_\mathfrak{Q} = K_\mathfrak{q}$ holds (here $\mathfrak{Q}$ denotes an extension of $\mathfrak{q}$ to L).

If $\mathfrak{q}$ is inert in L/K, the invariant is trivial if $l | v_\mathfrak{q}(a)$ holds.

In the tamely ramified case $\mathfrak{q} \not| l$, to which we restrict our attention, we see that the invariant is trivial if a has an order prime to l in the residue class field $k_\mathfrak{q}^\times$ of $K_\mathfrak{q}$. Hence the l–th root of unity associated to a in $k_\mathfrak{q}^\times$ is the trivial one.

local behavior		condition for trivial invariant
ramified	$\mathfrak{q} \not| l$	$\overline{a} = 1$ in $k_\mathfrak{q}^* / k_\mathfrak{q}^{*l}$
unramified	$\mathfrak{q}$ inert	$l \| v_\mathfrak{q}(a)$
unramified	$\mathfrak{q}$ completely split	automatically

4.4 Efficient Methods for Calculating Invariants

We now describe in an example how it is possible to explicitly construct a global algebra relating the computation of the invariant map at a ramified place $\mathfrak{p}$ to computations at unramified places $\mathfrak{q}$ of small norm. Since we only succeeded to do this using (global) Kummer theory, it is immediately clear that this approach is not going to work for cryptographic instances. The study of the occurring problems leads to the development of a method working without Kummer theory. This will be explained in detail in the next chapter.

Consider the following global Kummer extension with especially simple ramification structure:
Choose an element α of K such that $\alpha\mathfrak{o}_K = \mathfrak{p}$, then from theorem 4.3.1 we see that in $K(\alpha^{1/l})/K$ ramification can only occur for $\mathfrak{q} = \mathfrak{p}$ or for $\mathfrak{q}$ such that $\mathfrak{q}|l$.
In the following we will assume that this is the case.

Example 4.4.1

We give an example for the case $l = 13$.
First we have to construct a global extension $L/K = \mathbb{Q}(\zeta_{13})$ with prescribed ramification. Consider the element

$$\alpha = -2\zeta^{11} + 2\zeta^{10} - \zeta^8 - \zeta^7 - 4\zeta^5 + \zeta^4 + \zeta^3 - \zeta^2 \in \mathbb{Q}(\zeta_{13}).$$

We have $\alpha\mathfrak{o}_{\mathbb{Q}(\zeta_{13})} = \mathfrak{p}$ with $\mathfrak{p}|263$. It is checked easily using theorem 4.3.1 that all places $\mathfrak{q}$ with $\mathfrak{q}|13$ split completely in L/K. Hence L/K is ramified exactly at $\mathfrak{p}$.
Now consider the algebra given by

$$A_{\mathfrak{p}} = (L_{\mathfrak{p}}/K_{\mathfrak{p}}, \sigma, a_{\mathfrak{p}} = 193z^2 + 100z + 67).$$

Here $K_{\mathfrak{p}}/\mathbb{Q}_{263}$ is an extension of degree 3 over $\mathbb{Q}_{263}$ obtained by adjoining the 13–th roots of unity to $\mathbb{Q}_{263}$. We have that $K_{\mathfrak{p}}/\mathbb{Q}_{263}$ is unramified, the extension of residue class fields is given by $k = \mathbb{F}_{263}(z)/\mathbb{F}_{263}$, where z satisfies the irreducible equation $z^3 + 25z^2 + 229z + 262 = 0$ over $\mathbb{F}_{263}$.

Furthermore we note that $|k| = 263^3 = 18191447$.
It is easily seen that $a_{\mathfrak{p}}$ indeed corresponds to a non trivial element in $k^\times/k^{\times l}$, hence describes a non trivial algebra. The naive lift leads for example to the algebra

$$A = (L/\mathbb{Q}(\zeta_{13}), \sigma, a = 193\zeta^2 + 100\zeta + 67).$$

Factoring the norm of a shows that $a\mathfrak{o}_K$ is divided by a prime ideal $\mathfrak{q}$ lying over 449359464893. Since the corresponding local extension $L_{\mathfrak{q}}/K_{\mathfrak{q}}$ is inert, we have to compute a discrete logarithm in $\mathbb{F}_{449359464893}$. Hence this naive lifting approach does not lead to a simplification of the original problem.

4.5 Experimental Results

We now describe an experimental approach which aims at producing global algebras with non trivial invariants at primes of small norm.

To this end we proceed as follows:
Besides A we also consider the element

$$A^i = \underbrace{A \otimes A \otimes \cdots \otimes A}_{i\,\text{times}} \quad (1 < i < l)$$

of $Br(K_{\mathfrak{p}})$ which is given by $(L_{\mathfrak{p}}/K_{\mathfrak{p}}, \sigma, a^i)$. Obviously we have: $\mathrm{inv}_{\mathfrak{p}}(A^i) = i * \mathrm{inv}_{\mathfrak{p}}(A)$.
Given a relation involving $\mathrm{inv}_{\mathfrak{p}}(A)$ as well as one involving $\mathrm{inv}_{\mathfrak{p}}(A^i)$, we can subtract these two relations from each other, thus gaining a relation containing $(i-1)\mathrm{inv}_{\mathfrak{p}}(A)$. If we find two such relations containing a common term belonging to a prime of large norm this term cancels out. Thus we can hope to construct a relation involving only terms belonging to places of small norm besides a multiple of $\mathrm{inv}_{\mathfrak{p}}(A)$.

The constructing of these relations is easy:
Given $a_{\mathfrak{p}}$ in $k_{\mathfrak{p}}$ which is non trivial in $k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*l}$, this means that $a_{\mathfrak{p}}^{(p^f-1)/l} \neq 1$ holds in $k_{\mathfrak{p}}$.

In order to construct global liftings a of $a_{\mathfrak{p}}$ giving the same algebra and hence the same invariant locally at $\mathfrak{p}$ we proceed as follows:
Consider powers of $a_{\mathfrak{p}}$ of the form $a_{\mathfrak{p}}^n$ in $k_{\mathfrak{p}}$, where $n \equiv 1 \bmod l$ holds. Then

we get $(a^n_{\mathfrak{p}})^{(p^f-1)/l} = a_{\mathfrak{p}}^{(p^f-1)/l}$. Hence the different a^n_p describe indeed the same local algebra at $\mathfrak{p}$.

Lifting the different elements $a^n_{\mathfrak{p}}$ to global elements a_n, we obtain the desired global algebras $A_n = (L/K, \sigma, a_n)$ with prescribed invariant at $\mathfrak{p}$.

We again consider the local algebra from example 4.4.1.

Here we had $K_{\mathfrak{p}} = \mathbb{Q}_{263}(\zeta_{13})$ and $k_{\mathfrak{p}} \simeq \mathbb{F}_{263}(z)$, where z satisfied the equation $z^3 + 25z^2 + 229z + 262 = 0$. Let $\mathfrak{p}$ be a fixed place of $\mathbb{Q}_{263}(\zeta_{13})$ lying over $p = 263$.
Consider also the element $a_{\mathfrak{p}} = 193z^2 + 100z + 67$ in $k_{\mathfrak{p}}$ which belongs to a non trivial invariant at $\mathfrak{p}$.

Following the procedure explained above we constructed 50.000 relations involving $\mathrm{inv}_{\mathfrak{p}}(A)$ and $2\mathrm{inv}_{\mathfrak{p}}(A)$ respectively. Since $|k_{\mathfrak{p}}| = 18.191.446$, we searched for relations having in common a place of norm greater than 100.000.

Amongst the 50.000 relations we found 32 pairs which had in common a term belonging to a place of large norm. However, even if one such term cancels out, it is of course possible that some other terms belonging to places of high norm remain, in which case the new relation is not useful. However, if this is not the case, we have found a good relation relating the invariant at the place $\mathfrak{p}$ to the calculation of discrete logarithms in finite fields of small norm.

Amongst the 32 pairs we were able to find 5 good pairs.

Results in the case $\mathrm{inv}_{\mathfrak{p}}(A)$–$2\mathrm{inv}_{\mathfrak{p}}(A)$		
Number of relations	Number of pairs	Number of good pairs
50.000	32	5

Good pairs	
Number	finite fields involved
1	**(53,1)**,**(157,1)**,**(313,1)**,**(937,1)**,**(29173,1)**,**(31357,1)**,**(37571,1)**
2	**(53,1)**,**(937,1)**,**(31357,1)**,**(37571,1)**
3	(131,1),**(157,1)**,**(521,1)**,**(677,1)**,**(2731,1)**,(4421,1)
4	**(2,12)**,**(3,4)**,**(859,1)**
5	**(3823,1)**,**(13417,1)**,**(14717,1)**,**(20333,1)**,**(38351,1)**,**(79301,1)**

Here (p, f) denotes the finite field $\mathbb{F}_{p^f}$, the bold entries denote those places which are inert in the global extension L/K.

Some further 50.000 relations involving $3\mathrm{inv}_{\mathfrak{p}}(A)$ made some more comparisons possible.

Results in the case $\mathbf{inv}_{\mathfrak{p}}(A)$–$3\mathbf{inv}_{\mathfrak{p}}(A)$		
Number of relations	Number of pairs	Number of good pairs
50.000	42	16

Good pairs	
Number	finite fields involved
1	**(5227,1)**,**(38923,1)**
2	**(2,12)**,**(2731,1)**
3	**(2,12)**,**(2731,1)**
4	**(2731,1)**
5	**(2,12)**,**(2731,1)**
6	**(2,12)**,**(313,1)**,**(2731,1)**,**(31357,1)**
7	**(2731,1)**
8	**(313,1)**,(31513,1),**(31357,1)**
9	**(313,1)**,**(2731,1)**,**(31357,1)**
10	**(2731,1)**
11	**(2,12)**,**(313,1)**,(1483,1),**(31357,1)**,**(96487,1)**
12	**(2731,1)**
13	**(2731,1)**
14	**(2,12)**,**(5227,1)**,**(38923,1)**
15	**(2731,1)**
16	**(313,1)**,**(2731,1)**,**(31357,1)**

Here it is worth noticing that in four cases all but one term canceled out, hence relating the computation of the desired invariant at $\mathfrak{p}$ to a term belonging to place of very small norm (2731). Thus we have reduced a discrete logarithm in $\mathbb{F}_{263^3}$ to one in $\mathbb{F}_{2731}$.

Finally the data for the last comparison:

Results in the case $2\mathbf{inv}_{\mathfrak{p}}(A)$–$3\mathbf{inv}_{\mathfrak{p}}(A)$		
Number of relations	Number of pairs	Number of good pairs
50.000	12	1

Good pairs	
Number	finite fields involved
1	**(2,12)**,(131,1),(521,1),(677,1),(4421,1)

We can draw the following conclusions from these computational experiments:

- The proposed local–global technique indeed yields relations which relate the computation of the invariant map at the ramified place $\mathfrak{p}$ to the discrete logarithm problem in small finite fields.
- The explicit construction of global algebras using Kummer theory is only possible, if the l–th roots of unity are contained in the global ground field K.
  But this of course implies that for larger l the global field K can no longer be handled efficiently because of $\mathbb{Q} \subset \mathbb{Q}(\zeta_l) \subset K$. Hence the proposed method can not deal with values of l which are of cryptographic interest.

The key to overcome this problems is to find a completely different way of dealing with global cyclic extensions with prescribed ramification. This will be discussed at length in the next chapter.

Chapter 5

Global Class Field Theory

In the previous chapter we described explicit methods to construct global cyclic algebras with prescribed ramification. It turned out that the central problem is to have a good description of the local properties of the global field over which we want to construct the cyclic algebra.

As we already remarked at the end of the last chapter, the fact that we used Kummer theory to construct cyclic extensions makes is impossible to apply these ideas in a general context, since we can not deal efficiently with the global field $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ for l large.

We therefore turn to a more theoretical approach to this problem. Recall that the description of Abelian extensions of global number fields with restricted ramification lies at the heart of global class field theory.

We will first give a summary of class field in a general sense. Extensive examples will then be given for the two easiest cases.

5.1 Moduli and Ray Class Groups

We fix a base field K. Our goal is to describe the Abelian extension of K with prescribed ramification. We first introduce some terminology.

Definition 5.1.1 *A modulus* $\mathfrak{m}$ *in* K *is a pair* $(\mathfrak{m}_0, \mathfrak{m}_\infty)$ *where* $\mathfrak{m}_0$ *is an integral ideal and* $\mathfrak{m}_\infty$ *is a set of real embeddings of* K *into* $\mathbb{C}$*. We write this*

formally as $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$.
We define $(\mathfrak{o}/\mathfrak{m})^\times = (\mathfrak{o}/\mathfrak{m}_0)^\times \times \mathbb{F}_2^{\mathfrak{m}_\infty}$.
If $\mathfrak{m}$ *and* $\mathfrak{n}$ *are two moduli, we say that* $\mathfrak{n}$ *divides* $\mathfrak{m}$ *(*$\mathfrak{n}|\mathfrak{m}$*) if* $\mathfrak{m}_0 \subset \mathfrak{n}_0$ *and* $\mathfrak{n}_\infty \subset \mathfrak{m}_\infty$.
If $\mathfrak{a}$ *is a nonzero fractional ideal of* K *we say that* $\mathfrak{a}$ *is coprime to* $\mathfrak{m}$ *if* $v_\mathfrak{p}(\mathfrak{a}) = 0$ *for all* $\mathfrak{p}|\mathfrak{m}$. *Equivalently we can write* $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$ *with* $\mathfrak{b}$ *and* $\mathfrak{c}$ *integral ideals coprime to* $\mathfrak{m}_0$ *in the usual sense.*
The set of ideals coprime to $\mathfrak{m}$ *forms a group denoted by* $I_\mathfrak{m}(K)$. *If* $\alpha \in K^\times$ *we say that* α *is coprime to* $\mathfrak{m}$ *if the corresponding principal ideal* $\alpha\mathfrak{o}_K$ *is.*

Recall that the class group of K is defined via the long exact sequence

$$1 \to U(K) \to K^\times \to I(K) \to Cl(K) \to 1$$

where $U(K)$ denotes the groups of units in $K^\times$ and $I(K)$ denotes the set of fractional $\mathfrak{o}_K$–ideals. We now want to find a way to replace I_K with $I_\mathfrak{m}(K)$ in this definition.

Definition 5.1.2 *Let* $\mathfrak{m}$ *be a modulus in* K.
For $\alpha \in K^\times$ *we say that*

$$\alpha \equiv 1 \bmod \mathfrak{m}$$

if for all $\mathfrak{p}$ *dividing* $\mathfrak{m}_0$ *we have* $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}_0)$ *and for all embeddings* $\sigma_i \in \mathfrak{m}_\infty$ *we have* $\sigma_i(\alpha) > 0$. *We write* $K_\mathfrak{m}^\times$ *for the group of such* α.

Let $P_\mathfrak{m}(K)$ denote the set of fractional principal ideals of $\mathfrak{o}_K$ that can be written in the form $\alpha\mathfrak{o}_K$ with $\alpha \in K_\mathfrak{m}^\times$. It is clear that $P_\mathfrak{m}(K)$ is a subgroup of $I_\mathfrak{m}(K)$ called ray group of $\mathfrak{m}$.

Now consider an element $\mathfrak{a}$ of $P_\mathfrak{m}(K)$. If $\mathfrak{a} = \alpha\mathfrak{o}_K = \beta\mathfrak{o}_K$ with $\alpha, \beta \in K_\mathfrak{m}^\times$ this is equivalent to saying that α/β is a unit in $K_\mathfrak{m}^\times$. These units form a subgroup of $U(K)$ which will be denoted by $U_\mathfrak{m}(K) = U(K) \cap K_\mathfrak{m}^\times$. We therefore have the following exact sequence

$$1 \to U_\mathfrak{m}(K) \to K_\mathfrak{m}^\times \to P_\mathfrak{m}(K) \to 1.$$

We are now ready to define the ray class group $Cl_\mathfrak{m}(K)$ in an analogous way to $Cl(K)$ via the exact sequence

$$1 \to P_\mathfrak{m}(K) \to I_\mathfrak{m} \to Cl_\mathfrak{m}(K) \to 1.$$

The finiteness of the ray class group and a formula to calculate its cardinality follows from the following statement.

Theorem 5.1.3 *We have an exact sequence*

$$1 \to U_{\mathfrak{m}}(K) \to U(K) \to (\mathfrak{o}_K/\mathfrak{m})^\times \to Cl_{\mathfrak{m}}(K) \to Cl(K) \to 1. \tag{5.1}$$

Hence the ray class group is finite. Also we know that

$$h_{\mathfrak{m}}(K) = h(K)\frac{|(\mathfrak{o}_K/\mathfrak{m})^\times|}{[U(K) : U_{\mathfrak{m}}(K)]} \tag{5.2}$$

where $h(K)$ and $h_{\mathfrak{m}}(K)$ denote the cardinality of the class group of K and the ray class group of $K_{\mathfrak{m}}$ respectively.

In order to be able to formulate the main theorem of global class field theory we now introduce the notion of a congruence subgroup.

Definition 5.1.4 *A group of fractional ideals C such that*

$$P_{\mathfrak{m}}(K) \subset C \subset I_{\mathfrak{m}}(K)$$

is called a congruence subgroup for the modulus $\mathfrak{m}$. In order to indicate the modulus to which C corresponds, we introduce the notation $(\mathfrak{m}, C)$ for a congruence subgroup modulo $\mathfrak{m}$.

Note that we can also consider the set of classes $\overline{C} = C/P_{\mathfrak{m}} \subset Cl_{\mathfrak{m}}$, so we can consider a congruence subgroup as a subgroup of the ray class group $Cl_{\mathfrak{m}}$.

It is natural to ask when, given $(\mathfrak{m}_1, C_1)$ and $(\mathfrak{m}_2, C_2)$, we have that $Cl_{\mathfrak{m}_1}/\overline{C_1} \simeq Cl_{\mathfrak{m}_2}/\overline{C_2}$ holds. To answer this question we introduce an equivalence relation between congruence subgroups:

Definition 5.1.5 *We say that two congruence subgroups $(\mathfrak{m}_1, C_1)$ and $(\mathfrak{m}_2, C_2)$ are equivalent ($(\mathfrak{m}_1, C_1) \sim (\mathfrak{m}_2, C_2)$) if*

$$I_{\mathfrak{m}_2} \cap C_1 = I_{\mathfrak{m}_1} \cap C_2.$$

One checks that this is indeed an equivalence relation and that we have $I_{\mathfrak{m}_1}/C_1 \simeq I_{\mathfrak{m}_2}/C_2$ as claimed.

A further notion is that of the conductor of a congruence subgroup. In order to introduce this we first define the GCD (greatest common divisor) of two congruence subgroups. If $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are two moduli, we define the greatest common divisor $\mathfrak{n} = gcd(\mathfrak{m}_1, \mathfrak{m}_2)$ of $\mathfrak{m}_1$ and $\mathfrak{m}_2$ by taking the sum of the corresponding integral ideals and the intersection at the places of infinity. Clearly, if $\mathfrak{n}$ is defined thus, it is the largest modulus dividing both $\mathfrak{m}_1$ and $\mathfrak{m}_2$, hence the terminology.

Theorem 5.1.6 *Let $(\mathfrak{m}_1, C_1)$ and $(\mathfrak{m}_2, C_2)$ be two congruence subgroups such that $(\mathfrak{m}_1, C_1) \sim (\mathfrak{m}_2, C_2)$. Let $\mathfrak{n} = gcd(\mathfrak{m}_1, \mathfrak{m}_2)$. Then there exists a unique congruence subgroup C modulo $\mathfrak{n}$ such that $(\mathfrak{n}, C) \sim (\mathfrak{m}_1, C_1) \sim (\mathfrak{m}_2, C_2)$. C is given by $C = C_1 P_{\mathfrak{n}} = C_2 P_{\mathfrak{n}}$. We call the congruence subgroup $(C, \mathfrak{n})$ the GCD of the congruence subgroups $(\mathfrak{m}_1, C_1)$ and $(\mathfrak{m}_2, C_2)$.*

Now consider an equivalence class $\mathcal{C}$ of congruence subgroups. Then there exists a congruence subgroup $(\mathfrak{f}, C_{\mathfrak{f}})$ in $\mathcal{C}$ called the conductor of the class $\mathcal{C}$ such that each member of $\mathcal{C}$ is of the form $(\mathfrak{f}\mathfrak{a}, C_{\mathfrak{f}} \cap I_{\mathfrak{f}\mathfrak{a}})$ for any modulus $\mathfrak{a}$ of K.

We can now define the conductor of a congruence subgroup:

Definition 5.1.7 *Given a congruence subgroup $(\mathfrak{m}, C)$ we consider the class $\mathcal{C}$ of congruence subgroups equivalent to $(\mathfrak{m}, C)$. Call $\mathfrak{f}$ the conductor of $(\mathfrak{m}, C)$, if $(\mathfrak{f}, C_{\mathfrak{f}})$ is the conductor of $\mathcal{C}$.*
Call any given modulus $\mathfrak{f}$ a conductor if there exists a congruence subgroup of conductor equal to $\mathfrak{f}$.

5.2 Abelian Extensions of K

Having explained the structure of the ray class group of a given modulus $\mathfrak{m}$ of K, we now proceed to explain how this structure controls the arithmetic of Abelian extensions of K with ramification controlled by $\mathfrak{m}$.

Recall from algebraic number theory the notion of the conductor of an extension L/K. It is given by

$$\mathfrak{f}_0 = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}},$$

where $n_{\mathfrak{p}} \in \mathbb{N}_0$ is given by a local condition at $\mathfrak{p}$. More precisely we have $n_{\mathfrak{p}} > 0$ exactly if $\pi_{K_{\mathfrak{p}}}$ is a norm locally at $\mathfrak{p}$ in the extension $L_{\mathfrak{p}}/K_{\mathfrak{p}}$. Hence $\mathfrak{f}_0$ contains exactly those primes $\mathfrak{p}$ which ramify in L/K.

Let $\mathfrak{f}_\infty$ be the set of real places of K ramified in L. We define the conductor of L/K to be the modulus $\mathfrak{f}(L/K) = \mathfrak{f}_0\mathfrak{f}_\infty$.

Definition 5.2.1 *Let L/K be an Abelian extension and $\mathfrak{m}$ a modulus of K. Then $\mathfrak{m}$ is called suitable for the extension L/K if $\mathfrak{m}$ is a multiple of the conductor $\mathfrak{f}$ of L/K.*

Now we define a group homomorphism from $I_{\mathfrak{m}}$ (the group of fractional ideals coprime to $\mathfrak{m}$), to the absolute Galois group G of L/K. More precisely for

$$\mathfrak{a} = \prod_{\mathfrak{p}|\mathfrak{a}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

we define the Artin map to be

$$Art_{L/K}(\mathfrak{a}) = \prod_{\mathfrak{p}|\mathfrak{a}} \sigma_{\mathfrak{p}}^{v_{\mathfrak{p}}(\mathfrak{a})}$$

where $\sigma_{\mathfrak{p}}$ denotes the Frobenius at $\mathfrak{p}$ inside G as usual.

Theorem 5.2.2 (Artin reciprocity) *The Artin map is a surjective group homomorphism from $I_{\mathfrak{m}}$ to G. Moreover the kernel of the Artin map $A_{\mathfrak{m}}(L/K)$ is a congruence subgroup modulo $\mathfrak{m}$, hence the Artin map can be viewed as a surjective map from $Cl_{\mathfrak{m}}$ to G.*

The fundamental equivalence of studying the structure of $Cl_{\mathfrak{m}}(K)$ and of studying Abelian extensions of K is now given by the celebrated Tagaki Existence theorem

Theorem 5.2.3 *If $(\mathfrak{m}_1, A_{\mathfrak{m}_1}(L_1/K)) \sim (\mathfrak{m}_2, A_{\mathfrak{m}_2}(L_2/K))$, then L_1 and L_2 are K–isomorphic.*
Conversely, given any congruence subgroup $(\mathfrak{m}, C)$ then there exists an Abelian extension L/K, unique up to K–isomorphism, such that $\mathfrak{m}$ is a suitable modulus for L/K and $C = A_{\mathfrak{m}}(L/K)$.

The arithmetic properties of the Abelian extension L/K corresponding to $(\mathfrak{m}, C)$ are as follows:

Theorem 5.2.4 *The Artin map induces a canonical isomorphism from $Cl_{\mathfrak{m}}/\overline{C}$ to $Gal(L/K)$.*
The conductor $\mathfrak{f} = \mathfrak{f}(L/K)$ of the Abelian extension is equal to the conductor of the corresponding congruence subgroup.
The places of K that ramify in L are exactly the divisors of $\mathfrak{f}$.

Thus we see that the existence of an extension of K of degree l which is ramified exactly at one place $\mathfrak{p}$ is completely determined by the structure of the ray class group modulo $\mathfrak{m} = \mathfrak{p}\mathfrak{m}_\infty$.

Therefore global class field theory establishes the existence of a global extension with prescribed ramification, or more precisely gives criteria to determine whether such an extension exists.

We can now return to the question we want to address, namely how to relate the invariant at ramified places with the invariant at other places. As we pointed out before, this can be done using the local-global principle coming from the Hasse–Brauer–Noether theorem.

However in order to make this explicit we now need to examine the possibilities we have to describe the local properties of the Galois group of the extension L/K contained in the ray class field $K_{\mathfrak{m}}/K$.

As before, let σ denote a generator of the global Galois group $Gal(L/K)$, for $\mathfrak{q}$ unramified in L/K denote the Frobenius automorphism by $\sigma_{\mathfrak{q}}$. Define $f_{\mathfrak{q}}$ by $\sigma^{f_{\mathfrak{q}}} = \sigma_{\mathfrak{q}}$.

Recall again that the existence of a global field extension L/K of degree l implies that there is a relation coming from a global cyclic algebra $(L/K, \sigma, a)$ of the form

$$\sum_{\mathfrak{p}\,\text{ramified}} \text{inv}_{\mathfrak{p}}(a) + \sum_{\mathfrak{q}\,\text{unramified}} f_{\mathfrak{q}} v_{\mathfrak{q}}(a) \equiv 0 \bmod l.$$

The approach of the last section was to restrict the ramification to one place and to try to eliminate all places of large norm.

We now propose to do the following:

1. Establish the existence of an extension of degree l ramified at $\mathfrak{p}$.

2. Fix a set $\mathfrak{Q}$ of (unramified) primes $\mathfrak{q}$ of K.

3. Generate relations of the form

$$\sum_{\mathfrak{p}\,\text{ramified}} \mathrm{inv}_{\mathfrak{p}}(a) + \sum_{\mathfrak{q}\,\text{unramified},\mathfrak{q}\in\mathfrak{Q}} f_{\mathfrak{q}} v_{\mathfrak{q}}(a) \equiv 0 \bmod l.$$

4. Solve the resulting homogeneous system of linear equations for the $\mathrm{inv}_{\mathfrak{p}}(a)$ and the $f_{\mathfrak{q}}$.

It should be worth noticing at this point that in performing these computations we actually solve two problems at once:

- We provide algorithms for the computation of discrete logarithms in finite fields.

- These algorithms will also compute discrete logarithms between a fixed generator σ and Frobenius automorphisms $\sigma_{\mathfrak{q}}$ inside the Galois group of certain subfields of ray class fields.

- The theory of Brauer groups shows that describing the Galois group of ray class fields is intimately linked to solving the discrete logarithm in finite fields.

We will now examine two cases in which the global class field theory is especially well understood, namely the cases of the rationals $K = \mathbb{Q}$ and of imaginary quadratic fields $K = \mathbb{Q}(\sqrt{D}), D < 0$.

Chapter 6

Two Examples

6.1 The Case $K = \mathbb{Q}$

The global class field theory of $\mathbb{Q}$ is completely determined by the celebrated theorem of Kronecker and Weber:

Theorem 6.1.1 (Kronecker–Weber) *Every Abelian extension $K/\mathbb{Q}$ of $\mathbb{Q}$ is contained in a suitable cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.*

The following lemma shows why this theorem is of special interest for us:

Corollary 6.1.2 *There exists an Abelian extension $K/\mathbb{Q}$ of degree l ramified exactly at p iff $l|p-1$ holds. If it exists it is uniquely determined.*

Proof: Obviously the fact that K is ramified exactly at p implies that for each cyclotomic extension $\mathbb{Q}(\zeta_n)$ containing K we have that $p|n$. Hence $\mathbb{Q}(\zeta_p)$ is the smallest cyclotomic extension containing K. The extension $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ has degree $p-1$ hence there exists an intermediate field of $\mathbb{Q}(\zeta_p)$ of degree l over $\mathbb{Q}$ iff $l|p-1$ holds.

Since $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois and $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic K is uniquely determined. $\square$

Note that therefore $\mathbb{Q}(\zeta_p)$ is the ray class field of $\mathbb{Q}$ for the modulus $\mathfrak{m} = (p)\infty$, since $\mathbb{Q}$ has one real embedding. Also we see that the ray class group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Note that in this case the cardinality of the ray class group is given by $\phi((p))$, since the units of $\mathbb{Z}$ are just $\{+1, -1\}$, therefore $U_{\mathfrak{m}}(\mathbb{Q}) = \{+1\}$ and hence $[U(\mathbb{Q}) : U_{\mathfrak{m}}(\mathbb{Q})] = 2$, which cancels out with the contribution from the real embedding in (5.2).

Hence we know how to compute an extension of $\mathbb{Q}$ of prime degree l which is ramified exactly at p:
consider the extension $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$, set $\langle\sigma\rangle = Gal(\mathbb{Q}(\zeta_p/\mathbb{Q}))$ and consider the fixed field K of $\langle\sigma^l\rangle$ inside $\mathbb{Q}(\zeta_l)$.

Thus we have ascertained the existence of an extension of degree l ramified exactly at one place. However our task was not only to construct such an extension but also to describe its Galois group locally at all unramified places. We will do this by studying the relative Brauer group $Br(K/\mathbb{Q})$.

Let $K/\mathbb{Q}$ be an extension of degree Grad l ramified exactly at p. Let $\langle\sigma\rangle = Gal(K/\mathbb{Q}) = G$ be the Galois group of $K/\mathbb{Q}$, consider a global algebra A of the form $A = (K/\mathbb{Q}, \sigma, a)$.

If a can be factored in the form $a = \prod q^{n_q}$ the theorem by Hasse–Brauer–Noether leads to a relation of the form

$$\mathrm{inv}_p(a) + \sum_{q \neq p} f_q n_q \equiv 0 \bmod l. \tag{6.1}$$

We now have to choose a suitable set $\mathfrak{Q}$ of unramified primes which we allow in (6.1). More precisely we have to find a way to control the primes occurring in the factorization of a, since otherwise each new equation is likely to introduce new indeterminates to the system. The easiest way to handle this problem is to restrict our attention to relations of the form (6.1) containing only terms related to small primes. Hence the notion of smoothness of natural numbers comes up in a natural way.

We now note the following similarity between the algorithm we proposed and a classical algorithm from computational number theory which also makes use of the smoothness property:

Fix a generator g of the multiplicative group $\mathbb{F}_p^\times$. Note that $a = \prod q^{n_q}$ can be viewed as an element of $\mathbb{F}_p^\times$ via the natural reduction map. Hence we can consider the logarithm of a to the basis g, which is defined to be the uniquely determined natural number $x \bmod p-1$ such that $a \equiv g^x \bmod p$ holds.

Write $x = \log_g(a)$. Obviously we have that $\log_g(ab) = \log_g(a) + \log_g(b)$. Hence the factorization $a = \prod q^{n_q}$ leads to the equation

$$\log_g(a) \equiv \log_g(\prod q^{n_q}) \equiv \sum \log_g(q^{n_q}) \equiv \sum n_q \log_g(q) \bmod p-1,$$

hence

$$\log_g(a) - \sum n_q \log_g(q) \equiv 0 \bmod p-1. \tag{6.2}$$

Observe the total similarity between (6.1) and (6.2). Indeed, (6.1) can be recovered from (6.2) by reducing equation (6.2) modulo l (this is possible since we assumed that $l|(p-1)$).

Hence the proposed method to compute the local properties of the Galois group of $K/\mathbb{Q}$ has reproduced the classical index calculus algorithm to compute discrete logarithms in prime fields $\mathbb{F}_p$ (see [COS86]). We briefly recall this algorithm.

Starting with an element x of $\mathbb{F}_p^\times$ we want to compute the discrete logarithm $\log_g(x)$. In order to do this we compute x^{exp} for random exp and lift this to $\overline{x^{exp}} \in \mathbb{Z}$. If this lift is smooth of the form

$$\overline{x^{exp}} = \prod_{q \in S} q^{n_q},$$

we obtain a relation of the form

$$exp \cdot \log_g(x) = \sum_{q \in S} n_q \log_g(q) \bmod p-1.$$

If we collect enough relations of this sort we can solve the resulting system of linear equations for $\log_g(x)$ and $\log_g(q)$.

In the case of Brauer groups we can proceed exactly like this, a smooth lift leads to a relation

$$exp \cdot \mathrm{inv}_p(x) + \sum_{q \in S} n_q f_q \equiv 0 \bmod l.$$

So instead of computing $\log_g(x)$ and $\log_g(q)$, we compute $\mathrm{inv}_p(x)$ and f_q.

Algorithm 1 Computation of local properties of $K/\mathbb{Q}$
Input: $x \in \mathbb{F}_p$
Output: $inv_p(x)$,f_q

1. $A := [0]$

2. $x :=$ `lift of` ζ_0 `to` $\mathbb{F}_p^\times$

3. **while** `Rang`$(A) < |S| - 1$ **do** $exp :=$ `random element of` $[1, p-1]$
   $\overline{x^{exp}} =$ `lift of` x^{exp} `to` $\mathbb{Z}$
   if `smooth`$(\overline{x^{exp}})$ **then** $Relation = ($`exp`$,$`factorization`$(\overline{x^{exp}}))$
   $A :=$ `Include`$(A, Relation)$ **end while**

4. `vector:=element of` $Ker(A)$

5. **Output** `vector`

Note that in order to compute the discrete logarithm of y with respect to x in the cyclic subgroup of order l inside $\mathbb{F}_p^\times$ we simply need to compute $\mathrm{inv}_p(y)$ and $\mathrm{inv}_p(x)$ and we can do so by lifting $x^{exp_1}y^{exp_2}$ to $\mathbb{Z}$ and storing the smooth relations obtained from this for random exp_1 and exp_2.
We can then obtain $\mathrm{inv}_p(x)$ and $\mathrm{inv}_p(y)$ by computing a vector in the kernel of the resulting relation matrix. We need to assume that the matrix has maximal rank in order to be sure to obtain non trivial values for $\mathrm{inv}_p(x)$ and $\mathrm{inv}_p(y)$ from the one vector we compute. The discrete logarithm is then obtained via computing

$$\mathrm{inv}_p(y)/\mathrm{inv}_p(x) \bmod l.$$

The complexity estimates found in [COS86] also apply to the problem of computing local properties of the Galois group of $K/\mathbb{Q}$. More precisely we obtain the following:

Theorem 6.1.3 *Consider an extension $K/\mathbb{Q}$ of degree l ramified exactly at p such that $l|(p-1)$. Let σ be a generator for the Galois group of $K/\mathbb{Q}$. Then the computation of the exponents f_q such that σ^{f_q} equals the Frobenius σ_q at q for $q \leq L_p(\frac{1}{2}, \rho)$ for $\rho \in \mathbb{R}^+$ has heuristic complexity*

$$L_p\left(\frac{1}{2}, \rho + \frac{1}{\rho} + o(1)\right).$$

Here L denotes the complexity theoretic function given by

$$L_N(\alpha, \beta) = \exp(\beta(\log N)^\alpha(\log\log N)^{1-\alpha}).$$

Note that we need not consider any primes q in the relation (6.2) for which we have $l|log_g(q)$ if we are interested in computing the f_q. This corresponds to the case that q splits completely in $K/\mathbb{Q}$:
We know from the decomposition law for cyclotomic fields that the order of the residue class field of q is given by the order of q mod $p-1$. Hence q splits completely in $K/\mathbb{Q}$ iff this order is prime to l. But this means that $l|\log_g(q)$.

Since we solve a homogeneous system of equations the solution is only determined up to multiplication of a scalar from $\mathbb{F}_l^\times$.
This reflects the fact that we have not fixed a generator σ of the Galois group $Gal(K/\mathbb{Q})$ and that σ^i for $1 \leq i \leq l-1$ is also a generator.

6.2 Example

Consider the extension of degree 37 of $\mathbb{Q}$ which is ramified exactly at $p = 10^{15} + 37$. Therefore the computation of the local properties of $Gal(K/\mathbb{Q})$ corresponds to solving discrete logarithms in the cyclic subgroup of order 37 in $\mathbb{F}_p^\times$ where $p = 10^{15} + 37$. In order to check the correctness of our computations we compute a discrete logarithm as well as the exponents f_q for the primes up to 1009. Hence consider the elements $x_0 = 23$ and $x_1 = 57$ of $\mathbb{F}_p$, these can be viewed as liftings of the 37–th roots of unity $\zeta_0 = 627390197251587$ and $\zeta_1 = 312088005699472$ to $\mathbb{F}_p$.

As factor basis S we choose the first 169 primes up to 1009 and search for elements $23^{k_1}57^{k_2}$ in $\mathbb{F}_p^\times$ for which the lifts to $\mathbb{Z}$ factor over S (here n_1 and n_2 are random numbers from the interval $[1, p]$). After collecting 200 smooth lifts it turned out, that three primes can be eliminated from the factor basis since they did not appear in any of the relations. Furthermore the prime 743 can be eliminated since it splits completely in the cyclic extension $K/\mathbb{Q}$ of degree 37 ramified exactly at p. The relation matrix built from 200 columns of the form

$$\sum_{q_i \in S} n_i f_i + k_1 \mathrm{inv}_p(\zeta) + k_2 \mathrm{inv}_p(\zeta^n) = 0 \tag{6.3}$$

in 167 indeterminates turned out to have rank 166. The kernel of the matrix is generated by the vector

$(1, 8, 31, 20, 32, 18, 23, 7, 29, 25, 5, 36, 11, 12, 7, 9,$
$14, 32, 4, 14, 27, 14, 35, 35, 12, 34, 5, 27, 19,$
$17, 17, 15, 15, 20, 22, 16, 2, 33, 15, 35, 26, 34,$
$34, 6, 23, 4, 5, 12, 11, 33, 33, 29, 10, 33, 30, 15, 1,$
$3, 2, 5, 20, 28, 6, 28, 3, 20, 9, 29, 23, 18, 30, 26, 20,$
$4, 6, 24, 1, 27, 9, 17, 14, 25, 14, 7, 13, 13, 2, 19, 13,$
$6, 9, 21, 4, 31, 1, 27, 23, 18, 24, 19, 4, 12, 29, 13, 27,$
$10, 7, 14, 5, 28, 1, 31, 14, 2, 28, 28, 4, 35, 15, 31, 19,$
$6, 19, 9, 10, 2, 5, 12, 36, 34, 24, 34, 10, 8, 30, 28, 11,$
$35, 11, 33, 26, 34, 25, 24, 1, 21, 34, 27, 18, 7, 9, 26, 25,$
$19, 29, 2, 15, 30, 26, 3, 5, 22, 17, 13, 21, 8, 22)$

The two last entries correspond to the two invariants. Since we have $22/8 = 12$ in $\mathbb{Z}/37\mathbb{Z}$, the solution of the discrete logarithm is 12. Indeed we have

$$627390197251587^{12} = 312088005699472$$

in $\mathbb{F}_{10^{15}+37}$.

6.3 The Case of Imaginary Quadratic Fields

We now turn to the simplest example of number fields, namely quadratic extensions of the rationals. Here, the case of imaginary quadratic fields is especially easy.

Theorem 6.3.1 *Let $K = \mathbb{Q}(\sqrt{-D})$ with $D > 0$, D squarefree and $D \neq -1, -3$ be an imaginary quadratic field. Let $\mathfrak{m}$ be a modulus associated to the ideal $\mathfrak{a}$. Then the order of the ray class group modulo $\mathfrak{m}$ is given by*

$$h_{\mathfrak{m}}(K) = h(K)\frac{\phi(\mathfrak{a})}{2}. \tag{6.4}$$

Proof: Since K is imaginary quadratic, K does not have a real embedding, hence no real places. Also, the group of units of $\mathfrak{o}_K$ is equal to $\{+1, -1\}$. Hence the the index of $U_{\mathfrak{m}}(K)$ in $U(K)$ is equal to two. □

Corollary 6.3.2 *Let $\mathfrak{p}$ be a prime ideal of K. Assume that $l | N_{K/\mathbb{Q}}(\mathfrak{p}) - 1$ with $l \neq 2$ prime. Also assume that $(l, h(K)) = 1$. Then there exists an extension L/K ramified exactly at $\mathfrak{p}$.*

Note that the assumption $(l, h(K)) = 1$ is needed in order to assure that we obtain an extension which is not contained in the Hilbert class field of K and hence would be unramified.

Fix an extension of degree l over K ramified exactly at a prime $\mathfrak{p}$, set $Gal(L/K) = \langle\sigma\rangle$. Again we want to describe $Gal(L/K)$ locally, that is find the relation between σ and $\sigma_{\mathfrak{q}}$ for a prime $\mathfrak{q}$ of K which is inert in L/K.

We can make use of the arithmetic of $K/\mathbb{Q}$ in order to get information about the exponents $f_{\mathfrak{q}}$ we are interested in:

Consider the global cyclic algebra $(L/K, \sigma, q)$ where q is a rational prime, which leads to a relation

$$\mathrm{inv}_{\mathfrak{p}}(q) + \sum_{\mathfrak{q}|q} f_{\mathfrak{q}} \equiv 0 \bmod l.$$

But $\mathrm{inv}_{\mathfrak{p}}(q)$ corresponds to the local cyclic algebra $(L_{\mathfrak{p}}/K_{\mathfrak{p}}, \sigma, q)$, where q now has to be viewed in $k_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times l} \simeq \mathbb{F}_{p^2}^{\times}/\mathbb{F}_{p^2}^{\times l}$.

Assume that q is trivial in this quotient, hence we have $\mathrm{inv}_{\mathfrak{p}}(q) \equiv 0 \bmod l$. From this it follows that $f_{\mathfrak{q}_1} \equiv -f_{\mathfrak{q}_2} \bmod l$ if q splits in K or $f_{\mathfrak{q}} \equiv 0 \bmod l$ if q is inert. Hence we get

Lemma 6.3.3 *Assume that q is inert in $K/\mathbb{Q}$, i. e. $(q) = \mathfrak{q}$. Then we have $f_{\mathfrak{q}} = 0$ if the order of q in $k_{\mathfrak{p}}$ is prime to l.*
Assume that q splits in $K/\mathbb{Q}$, i. e. $q = \mathfrak{q}\overline{\mathfrak{q}}$, then we have $f_{\mathfrak{q}} \equiv -f_{\overline{\mathfrak{q}}} \bmod l$ exactly if the order of q in $k_{\mathfrak{p}}$ is prime to l.

Corollary 6.3.4 *Assume that $l|p+1$. Then we have:*
$f_{\mathfrak{q}} = 0$ if $q\mathfrak{o}_K = \mathfrak{q}$.
$f_{\mathfrak{q}} \equiv -f_{\overline{\mathfrak{q}}} \bmod l$ if $q\mathfrak{o}_K = \mathfrak{q}\overline{\mathfrak{q}}$.

6.3.1 The Case of $l|p+1$

In this case we can make use of Corollary 6.3.4 in when describing the Galois group $Gal(L/K)$ locally.

Consider the relation coming from the algebra $(L/K, \sigma, a)$ for $a \in K$. Write

$$a\mathfrak{o}_K = \prod_{q\,\mathrm{inert}} \mathfrak{q}^{m_{\mathfrak{q}}} \prod_{q\,\mathrm{split}} \mathfrak{q}^{n_{\mathfrak{q}}}\overline{\mathfrak{q}}^{n_{\overline{\mathfrak{q}}}},$$

hence

$$\mathrm{inv}_{\mathfrak{p}}(a) \equiv \sum_{q\,\mathrm{inert}} f_{\mathfrak{q}} m_{\mathfrak{q}} + \sum_{q\,\mathrm{split}} (\mathfrak{q} n_{\mathfrak{q}} + \overline{q} n_{\overline{\mathfrak{q}}}) \bmod l. \tag{6.5}$$

Due to Lemma 6.3.3 we know that we have $f_{\mathfrak{q}} \equiv 0 \bmod l$ for q inert in K. Furthermore, due to Lemma 6.3.3 in the situation $q = \mathfrak{q}\overline{\mathfrak{q}}$ in K it is enough to compute $f_{\mathfrak{q}}$ since then $f_{\overline{\mathfrak{q}}}$ is also known.
Therefore we can modify a relation of the form

$$\mathrm{inv}_{\mathfrak{p}}(a) + \sum_{q\,\mathrm{inert}} f_{\mathfrak{q}} m_{\mathfrak{q}} + \sum_{q\,\mathrm{split}} (f_{\mathfrak{q}} n_{\mathfrak{q}} + f_{\overline{q}} n_{\overline{\mathfrak{q}}}) \equiv 0 \bmod l \tag{6.6}$$

by

- Removing all inert primes.
- Replacing $f_{\mathfrak{q}} n_{\mathfrak{q}} + f_{\overline{q}} n_{\overline{\mathfrak{q}}}$ by $f_{\mathfrak{q}}(n_{\mathfrak{q}} - n_{\overline{\mathfrak{q}}})$.

Thus (6.6) can be rewritten in the form

$$\mathrm{inv}_{\mathfrak{p}}(a) + \sum_{q\,\mathrm{split}} (f_{\mathfrak{q}}(n_{\mathfrak{q}} - n_{\overline{\mathfrak{q}}})) \equiv 0 \bmod l.$$

Again this computation reproduces an algorithm for computing discrete logarithms, now in $\mathbb{F}_{p^2}^{\times}$ originally proposed by ElGamal in [ElG85]. However we can modify this algorithm, since instead of using all the split primes up to a certain norm, we use only one prime from each pair.

Here is an overview of the algorithm:

Algorithm 2 DL in cyclic subgroup of order l in $\mathbb{F}_{p^2}$, $l|p+1$.
Input: $\mathbb{Q}(\sqrt{-D})$, D `square free,` $D \neq -1, -3$. $a, b \in \mathbb{F}_{p^2}$
Output: n `such that` $(a^{(p^2-1)/l})^n = b^{(p^2-1)/l}$.

1. `Generate rational factorbase` $S_{rational}$ `of rational primes` $p \leq B$.
2. `Generate algebraic factorbase` $S_{algebraic}$ `containing one prime ideal` $\mathfrak{q}$ `of the the decomposition` $q = \mathfrak{q}\overline{\mathfrak{q}}$ `for rational` q `that splits in` K.
3. `Compute` $x = a^{n_a} b^{n_b}$ `in` $\mathbb{F}_{p^2}$.

4. Lift x to an element $\overline{x}$ in K.

5. If $N_{K/\mathbb{Q}}(\overline{x})$ is B-smooth, factor

$$\overline{x}\mathfrak{o}_K = \prod_{s\,\texttt{inert}} \mathfrak{s}^{n_\mathfrak{s}} \prod_{q\,\texttt{split}} \mathfrak{q}^{n_\mathfrak{q}}\overline{\mathfrak{q}}^{n_{\overline{\mathfrak{q}}}}$$

.

6. Store relation $(n_a, n_b, n_\mathfrak{q} - n_{\overline{\mathfrak{q}}})_{\mathfrak{q}\in S_{algebraic}}$.

7. Once enough relations are collected ($> |S_{algebraic}| + 2$), build the relation matrix A.

8. Compute $v = ker(A)$.

9. Output $v_2/v_1 \bmod l$.

Although the rational factorbase $S_{rational}$ contains all primes up to B, the algebraic factorbase $S_{algebraic}$ is generated from $S_{rational}$ by omitting all inert primes (one half of the primes in $S_{rational}$) and by selecting only one of the two prime ideals lying over a split rational prime q. Hence the algebraic factorbase has exactly half the size of the rational factorbase which means that:

1. We only have to find halve as much relations in order to obtain a relation matrix of maximal rank.

2. The linear algebra becomes easier since the resulting matrix is considerably smaller. If we assume the complexity of the linear algebra to be quadratic in the size of factorbase, this would give a factor of four.

ElGamal gives the following complexity estimate which also carries over to our modification.

Theorem 6.3.5 *Let K be an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, let $\mathfrak{p}$ be the prime ideal lying over the inert rational prime number p, assume $l|p+1$.*
Let L/K be the extension of K of degree l ramified exactly at $\mathfrak{p}$, let σ be a generator of $Gal(L/K)$. Then the computation of the exponents $f_\mathfrak{q}$ such that $\sigma^{f_\mathfrak{q}}$ equals the Frobenius $\sigma_\mathfrak{q}$ at $\mathfrak{q}$, where the norm of $\mathfrak{q}$ is bounded by $L_p(1/2, \sqrt{4/3})$ has heuristic complexity

$$L_p(1/2, \sqrt{48} + o(1)).$$

6.3.2 Example

As an example consider the discrete logarithm inside the cyclic subgroup of order 19 insider $\mathbb{F}_{151^2}$. We use the global numberfield $K = \mathbb{Q}(\sqrt{-31})$ which has class number $h(K) = 3$. Since $19|151+1$ we can use the above mentioned modifications.
As factorbase S we choose the primes $\mathfrak{q}_{2,1}, \mathfrak{q}_{5,1}$ and $\mathfrak{q}_{7,1}$ lying above $2, 5$ and 7 respectively. We want to solve the discrete logarithm problem in the subgroup of order 19 given by the two 19–th roots of unity related to $3z+1$ and $40z+80$, where z denotes a root of $x^2 + 31$ over $\mathbb{F}_{151^2}$.We collect the following smooth relations:

$$\begin{aligned}
(3z+1)^1 = (3z+1) \text{ and } (3\sqrt{-31}+1)\mathfrak{o}_K &= \mathfrak{p}_{2,1}^1\mathfrak{p}_{2,2}^2\mathfrak{p}_{5,1}^1\mathfrak{p}_{7,1}^1 \\
(3z+1)^{156} = (6z+102) \text{ and } (6\sqrt{-31}+102)\mathfrak{o}_K &= \mathfrak{p}_{2,1}^6\mathfrak{p}_{2,2}^2\mathfrak{p}_3^1\mathfrak{p}_{5,1}^1 \\
(3z+1)^{170} = (128z+128) \text{ and } (128\sqrt{-31}+128)\mathfrak{o}_K &= \mathfrak{p}_{2,1}^{11}\mathfrak{p}_{2,2}^8 \\
(3z+1)^{181} = (12z+116) \text{ and } (12\sqrt{-31}+116)\mathfrak{o}_K &= \mathfrak{p}_{2,1}^3\mathfrak{p}_{2,2}^6\mathfrak{p}_{5,2}^1\mathfrak{p}_{7,1}^1 \\
(3z+1)^{253} = (12z+52) \text{ and } (12\sqrt{-31}+52)\mathfrak{o}_K &= \mathfrak{p}_{2,1}^3\mathfrak{p}_{2,2}^7\mathfrak{p}_{7,2}^1
\end{aligned}$$

Using the described modifications we obtain the following system of linear equations mod19:

$$\begin{aligned}
\mathrm{inv}_{\mathfrak{p}}(3z+1) - f_2 + f_5 + f_7 &\equiv 0 \bmod 19 \\
156\mathrm{inv}_{\mathfrak{p}}(3z+1) + 4f_2 + f_5 &\equiv 0 \bmod 19 \\
170\mathrm{inv}_{\mathfrak{p}}(3z+1) + 3f_2 &\equiv 0 \bmod 19 \\
181\mathrm{inv}_{\mathfrak{p}}(3z+1) - 3f_2 - f_5 + f_7 &\equiv 0 \bmod 19 \\
253\mathrm{inv}_{\mathfrak{p}}(3z+1) - 4f_2 - f_7 &\equiv 0 \bmod 19
\end{aligned}$$

As a solution we obtain $\mathrm{inv}_{\mathfrak{p}}(3z+1) \equiv 1, f_2 \equiv 13, f_5 \equiv 1, f_7 \equiv 11 \bmod 19$.
Now since

$$(40\sqrt{-31}+80)\mathfrak{o}_K = \mathfrak{p}_{2,1}^3\mathfrak{p}_{2,2}^3\mathfrak{p}_{5,1}^2\mathfrak{p}_{5,2}^1\mathfrak{p}_{7,2}^1$$

From this smooth factorisation we obtain the relation $\mathrm{inv}_{\mathfrak{p}}(40z+80)+f_5-f_7 \equiv 0 \bmod 19$, which gives $\mathrm{inv}_{\mathfrak{p}} \equiv 10 \bmod 19$. Hence the solution of the discrete logarithm problem should be 10.
In order to check this the two 19–th roots of unity associated to $3z+1$ and $40z+80$ are $136z+24$ and $69z+36$, indeed we have that

$$(136z+24)^{10} = 69z+36$$

as claimed.
Note that although the class group of the global numberfield we used is non trivial,we were able to obtain our relations without considering any obstruction problems.

6.3.3 The Case of $l|p-1$

While the case of $l|p+1$ can only appear in the case, that p is inert in $K/\mathbb{Q}$, the case that $l|p-1$ can be realized either with an inert or with a split prime p.

Consider first the case that p is inert, $p\mathfrak{o}_K = \mathfrak{p}$.

In this situation we have to include both inert and split primes in the algebraic factor base since we cannot use Lemma 6.3.3.

Hence from the global algebra $(L/K, \sigma, a)$ where L/K denotes the extension of degree l inside the ray class field belonging to $\mathfrak{p}$ we obtain relations of the form

$$\mathrm{inv}_{\mathfrak{p}}(a) + \sum_{q\,\text{inert}} f_{\mathfrak{q}} v_{\mathfrak{q}}(a) + \sum_{q\,\text{split}} f_{\mathfrak{q}} v_{\mathfrak{q}}(a) + f_{\bar{\mathfrak{q}}} v_{\bar{\mathfrak{q}}}(a) \equiv 0 \bmod l.$$

Since exactly one half of the elements in $S_{rational}$ will be inert in L/K and the other half will split in L/K, $S_{algebraic}$ will be of the size $N = 3/2|S_{rational}|$. Hence we do not obtain an advantage for computations in $\mathbb{F}_p^\times$, if we use this method.

Now consider the situation that $p = \mathfrak{p}_1\mathfrak{p}_2$, i. e. p splits in $K/\mathbb{Q}$, meaning that $f(x) = x^2 + D$ splits in the factors $(x - x_1)(x - x_2) \bmod p$. Note that when α denotes a global root of $f(x)$ generating $K/\mathbb{Q}$, the global element $a + b\alpha$ with $a, b \in \mathbb{Z}$ corresponds to the local element $a + bx_1$ and $a + bx_2$ in the residue class fields of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ respectively.

Let L/K be the ray class field of modulus $\mathfrak{m} = \mathfrak{p}_1$, hence L/K is ramified exactly at $\mathfrak{p}_1$. Then the relation coming from the global algebra $(L/K, \sigma, a+b\alpha)$ looks like this:

$$\mathrm{inv}_{\mathfrak{p}_1}(a + bx_1) + \sum_{\mathfrak{q}\neq\mathfrak{p}_1} f_{\mathfrak{q}} v_{\mathfrak{q}}(a + b\alpha) \equiv 0 \bmod l. \tag{6.7}$$

Assume that both $a + bx_1$ as well as $a + b\alpha$ are smooth meaning that the norm of $a + b\alpha$ is smooth with respect to an algebraic factor base S_2, and $a+bx_1 \in \mathbb{F}_p$ can be lifted to a smooth element of $\mathbb{Z}$ with respect to a rational factor base S_1. Set

$$a + bx_1 = \prod_{q \in S_1} q^{n_q}, \quad a + b\alpha = \prod_{\mathfrak{q} \in S_2} \mathfrak{q}^{n_\mathfrak{q}}.$$

Then the relation (6.7) can be rewritten in the form

$$\sum_{q \in S_1} n_q \mathrm{inv}_{\mathfrak{p}_1}(q) + \sum_{\mathfrak{q} \in S_2} f_\mathfrak{q} v_\mathfrak{q}(a + b\alpha) \equiv 0 \bmod l.$$

Our task is now to search for pairs $(a, b) \in \mathbb{Z}^2$ such that both $a + bx_1$ and $a + b\alpha$ are smooth. If we have collected enough of these pairs, we can solve the resulting system of relations of type (6.3.3) both for $\mathrm{inv}_{\mathfrak{p}_1}(q), q \in S_1$ and $f_\mathfrak{q}, \mathfrak{q} \in S_2$.

But this is exactly the situation of the generalization of the so called Gaussian integer sieve, which is one of the most effective method known for solving the discrete logarithm problem in prime fields $\mathbb{F}_p$ (see for example [eur98, 171–183]) .

Furthermore the proposed method is valid even in the case of non trivial class number. We will look at this phenomenon in greater detail in the next chapter.

Therefore we have demonstrated, that the classical index calculus approach as well as the more refined approach of the Gaussian integer method can both be interpreted as calculating local invariants of the Galois groups of ray class fields of certain number fields.

Chapter 7

Global Cyclic Extensions with Several Ramified Primes

In the preceding chapters we linked the arithmetic of extensions ramified exactly at one prime $\mathfrak{p}$ with the arithmetic of the underlying residue class field of $\mathfrak{p}$. It is a natural question to ask what happens if we allow more than one ramified prime.

We restrict this to the case of cyclic extensions of the rationals $\mathbb{Q}$. Therefore we study the relation between subfields L of the ray class field $K/\mathbb{Q}$ ramified at the primes $p_1, \dots, p_n$ and the arithmetic of the finite fields $\mathbb{F}_{p_i}$ respectively.

First we have to establish the existence of such an extension. Recall that by Kronecker–Weber (Theorem 6.1.1) an extension of $\mathbb{Q}$ of degree l ramified at p exists exactly in the case that $l|(p-1)$. More generally the extension $L_{p_1,\dots,p_n}/\mathbb{Q}$ of degree l ramified exactly at $p_1, \dots, p_n$ has to be contained in $\mathbb{Q}(\zeta_{p_1 \cdot p_2 \cdots p_n})$.

Assume that $L_{p_1,\dots,p_{n-1}}/Q$ is an extension of degree l ramified exactly at $p_1, \dots, p_{n-1}$ and $L_{p_n}/\mathbb{Q}$ of degree l is ramified at p_n. Then $L_{p_1,\dots,p_{n-1}} L_{p_n}/\mathbb{Q}$ is Galois of order l^2 over $\mathbb{Q}$. Fix a subgroup H of $G = Gal(L_{p_1,\dots,p_{n-1}} L_{p_n}/\mathbb{Q})$ of order l such that the fixed field L of H is contained neither in $L_{p_1,\dots,p_{n-1}}$ nor in L_{p_n}. This is possible since G has exactly $l+1$ distinct subgroups of order l. Then L has to be ramified exactly at $p_1, \dots, p_n$. Thus we have shown inductively the existence of a Galois extension of degree l ramified at prime p_i such that $l|(p_i - 1)$.

Again we want to study the local–global relation coming from a global algebra of the form $(L/\mathbb{Q}, \sigma, a)$ for $a \in \mathbb{N}$. Assume that a has the factorization

$$a = \prod_{i=1}^{n} p_i^{m_i} \prod_{q \in S} q^{n_q}$$

then we obtain a relation of the form

$$\sum_{i=1}^{n} \mathrm{inv}_{p_i}(a) + \sum_{q \in S} f_q n_q \equiv 0 \bmod l.$$

Note that due to the ramification properties of $L/\mathbb{Q}$ we now allow elements from a factor base S as well as the ramified primes p_i in the factorization of a.

We observe that again the knowledge of the exponents f_q relating the generator σ to the Frobenius automorphism σ_q at q is equivalent to obtaining a relation between discrete logarithm problems in $\mathbb{F}_{p_i}^{\times}$ for $i = 1, \ldots, n$.

First consider the non–cryptographic case that all primes p_i are small (meaning the discrete logarithm problem in all the fields $\mathbb{F}_{p_i}$ is easy to solve).

Fix a factorbase S of rational primes q, our aim is to compute the f_q. Consider a global algebra $(L/\mathbb{Q}, \sigma, a_0)$ where a_0 has the factorization

$$a_0 = \prod_{i=1}^{n} p_i^{m_{0,i}} \prod_{q \in S} q^{n_{0,q}}.$$

This leads to the relation

$$\sum_{i=1}^{n} \mathrm{inv}_{p_i}(a_0) + \sum_{q \in S} f_q n_{0,q} \equiv 0 \bmod l. \tag{7.1}$$

Suppose $a_1 \in \mathbb{N}$ has the factorization

$$a_1 = \prod_{i=1}^{n} p_i^{m_{1,i}} \prod_{q \in S} q^{n_{1,q}}$$

The relation induced by a second algebra $(L/\mathbb{Q}, \sigma, a_1)$ will contain factors of the form $f_q n_{1,q}$ as well as terms of the form $\mathrm{inv}_{p_i}(a_1)$. The crucial observation

is now that these invariants $\mathrm{inv}_{p_i}(a_1)$ can be related to $\mathrm{inv}_{p_i}(a_0)$ as follows:
First note that

$$\mathrm{inv}_{p_i}(a_1) = \mathrm{inv}_{p_i}(\prod_{j \neq i} p_j^{m_j} \prod_{q \in S} q^{n_{1,q}})$$

since in the local extension $L_{p_i}/\mathbb{Q}_{p_i}$ the prime element p_i is a norm.

Now we have $\mathrm{inv}_{p_i}(a_1) = n\mathrm{inv}_{p_i}(a_0)$, where n is the solution to the discrete logarithm problem

$$(\prod_{j \neq i} p_j^{m_{1,j}} \prod_{q \in S} q^{n_{1,q}})^{(p_i-1)/l} = ((\prod_{j \neq i} p_j^{m_{0,j}} \prod_{q \in S} q^{n_{0,q}})^{(p_i-1)/l})^n$$

in the l–th roots of unity inside $\mathbb{F}_{p_i}^{\times}$.

Using this approach, we need not search for relations:
Prescribe any exponents n_q for primes $q \in S$ thus obtaining

$$a = \prod_{q \in S} q^{n_q}.$$

Then relate the invariants of a at the ramified places p_i to relation (7.1) by solving the discrete logarithm problems in the fields $\mathbb{F}_{p_i}$. Thus the complexity of this calculation is determined by the complexity of solving the discrete logarithms in $\mathbb{F}_{p_i}^{\times}$ and from the following linear algebra. Hence we see that the complexity will be dominated in a subexponential way by the largest prime ramified in $L/\mathbb{Q}$.

What happens if we turn to the cryptographic interesting situation, namely that p_n (say) is so large that computing discrete logarithms in $\mathbb{F}_{p_n}^{\times}$ is no longer possible?

Obviously we cannot choose arbitrary elements

$$a = \prod_{i=1}^{n} p_i^{m_i} \prod_{q \in S} q^{n_q}$$

any longer in order to generate relations, since we now have to control the invariant inv_{p_n} at the ramified place p_n without computing discrete logarithms.

But by computing random powers of an element of $\mathbb{F}_{p_n}$ we can generate smooth relations while also controlling the invariant at p_n:
Fix $x \in \mathbb{F}_{p_n}^{\times}$ related to a l–th root of unity in $\mathbb{F}_{p_n}^{\times}$. Compute x^{exp} for random

exponents $1 \leq exp \leq \mathrm{Order}(x)$. Let $\overline{x^{exp}}$ be a lift of x^{exp} to $\mathbb{Z}$. We now keep the lift $\overline{x^{exp}}$ if it factors in the form

$$\overline{x^{exp}} = \prod_{i=1}^{n} p_i^{m_i} \prod_{q \in S} q^{n_q}.$$

Assume we look at two lifts

$$\overline{x^{exp_0}} = \prod_{i=1}^{n} p_i^{m_{0,i}} \prod_{q \in S} q^{n_{0,q}}$$

and

$$\overline{x^{exp_1}} = \prod_{i=1}^{n} p_i^{m_{1,i}} \prod_{q \in S} q^{n_{1,q}}$$

with relations

$$exp_0 \mathrm{inv}_{p_n}(x) + \sum_{i=1}^{n-1} \mathrm{inv}_{p_i}(\overline{x^{exp_0}}) + \sum_{q \in S} f_q n_{0,q} \equiv 0 \bmod l$$

and

$$exp_1 \mathrm{inv}_{p_n}(x) + \sum_{i=1}^{n-1} \mathrm{inv}_{p_i}(\overline{x^{exp_1}}) + \sum_{q \in S} f_q n_{1,q} \equiv 0 \bmod l$$

respectively, we again can compute the dependency between $\mathrm{inv}_{p_i}(\overline{x^{exp_1}})$ and $\mathrm{inv}_{p_i}(\overline{x^{exp_0}})$ by computing discrete logarithms in $\mathbb{F}_{p_i}^{\times}$ now for $i = 1, \ldots, n-1$.

Thus we are able to produce relations involving exactly $|S| + n$ terms as long as the computation of discrete logarithms in $\mathbb{F}_{p_i}$ for $i = 1, \ldots, n-1$ is feasible.

The complexity of this approach will be determined by

- the complexity of finding smooth relations
- the complexity of solving the discrete logarithms in $\mathbb{F}_{p_i}^{\times}$ for $i = 1, \ldots, n-1$.
- the complexity of solving the resulting system of linear equations.

How does this situation compare to the computation of discrete logarithms in $\mathbb{F}_{p_n}^{\times}$ using an extension with just one ramified prime?

Here we have to compare the suggested approach in the case of several ramified primes with the following modified version of our algorithm in the case of one ramified prime:

Instead of searching for relations involving primes below a certain bound B we also allow some extra primes $p_i, i = 1, \dots, n-1$ to occur in the factorizations of the lifts. Having collected enough relations of this sort, we then solve for the $f_q, q \in S$ and the $f_{p_i}, i = 1, \dots, n-1$.

Hence we see that

- In both algorithms a relation is kept, if it involves small primes less than B and some extra primes p_i. Hence the same smoothness condition holds in both algorithms.
- Since both types of relations contain $n + |S|$ unknowns, the number of operations in order to solve the resulting linear algebra problem will we be the same.
- Using just one ramified prime, we do not need to compute any discrete logarithms in the fields $\mathbb{F}_{p_i}$.

Hence if we are only interested in computing discrete logarithms in $\mathbb{F}_{p_n}$, we do not gain an advantage by allowing more than one prime to ramify.

Chapter 8

Constructing Global l–th powers and the DL problem

8.1 Introduction

We now review some ideas relating the construction of l–th powers in number fields to the discrete logarithm problem in finite fields ([AD93],[Sch93],[Sch99]) and then proceed to show how Brauer groups can be used in some instances to simplify this approach.

As a motivation consider the discrete logarithm problem in the cyclic subgroup of order l inside the multiplicative group of the prime field $\mathbb{F}_p^\times$. Suppose we are given elements a and b associated to l–th roots of unity ζ_a and ζ_b. In order to compute the discrete logarithm between ζ_a and ζ_b, we can proceed as follows:
Generate random pairs r, s and compute $c \equiv a^r b^s \bmod p$. Store the triple (r, s, c) if the lift of c to $\mathbb{N}$ factors over a factor base S. Now if we generate sufficiently many such triples $(r_i, s_i, c_i)_{i=1,\dots,z}$, we can find elements $e_1, \dots, e_z$ such that

$$\prod_{i=1}^{z} c_i^{e_i} = x^l$$

for some integer x. Indeed consider the factorizations $c_i = \prod_{j=1}^{|S|} p_j^{n_{j,i}}$, this gives

$$\begin{aligned}
\prod_{i=1}^{z} c_i^{e_i} &= \prod_{i=1}^{z} (\prod_{j=1}^{|S|} p_j^{n_{j,i}})^{e_i} = \prod_{i=1}^{z}\prod_{j=1}^{|S|} p_j^{n_{j,i}e_i} \\
&= \prod_{j=1}^{|S|}\prod_{i=1}^{z} p_j^{n_{j,i}e_i} \\
&= \prod_{j=1}^{|S|} p_j^{\sum_{i=1}^{z} n_{j,i}e_i}.
\end{aligned}$$

Now this is an l–th power exactly if $\sum_{i=1}^{z} n_{j,i}e_i \equiv 0 \bmod l$ for all j, where $j = 1, \dots, |S|$.

Hence we have to find a non trivial solution to the system of linear equations

$$\begin{aligned}
n_{1,1}e_1 + n_{1,2}e_2 + \dots + n_{1,z}e_z &\equiv 0 \bmod l \\
\vdots \quad &\vdots \quad \vdots \\
n_{|S|,1}e_1 + n_{|S|,2}e_2 + \dots + n_{|S|,z|}e_z &\equiv 0 \bmod l.
\end{aligned}$$

If we have obtained enough smooth lifts, that is if we have $z > |S|$, a non-trivial solution exists, and we can find it by linear algebra modulo l.

Thus we obtain that

$$a^{k_a} b^{k_b} \equiv x^l \bmod p$$

where $k_a = \sum_{i=1}^{z} e_i r_i$ and $k_b = \sum_{i=1}^{z} e_i s_i$ and x is an element of $\mathbb{F}_p^\times$. Note that the solution to the discrete logarithm problem is now given by $-k_a/k_b \bmod l$ assuming that k_b is invertible modulo l.

Now consider what happens if we want to generalize this idea to the more general case of extension fields $\mathbb{F}_{p^n}$.

Let K be number field of degree n over $\mathbb{Q}$, let p be an inert prime in K meaning $p\mathfrak{o}_K = \mathfrak{p}$. We can then represent $\mathbb{F}_{p^n}$ as $\mathfrak{o}_K/\mathfrak{p}\mathfrak{o}_K$, where $\mathfrak{o}_K$ is the ring of integers in K.

Assume that we are given a and b in $\mathbb{F}_{p^n}$. We want to solve the discrete logarithm associated to the two l–th roots of unity ζ_a and ζ_b defined by $a^{(p^n-1)/l}$ and $b^{(p^n-1)/l}$ (assuming l divides $p^n - 1$).

Again we generate random pairs r, s and compute $c = a^r b^s$ in $\mathbb{F}_{p^n}$. Now note that due to the isomorphism $\mathfrak{o}_K/\mathfrak{p}\mathfrak{o}_K \simeq \mathbb{F}_{p^n}$ we can lift c to an element of

$\mathfrak{o}_K$. We keep the triple (r, s, c) only if $c\mathfrak{o}_K$ factors over a factorbase S of (algebraic) primes of K.

Assume we are able to find enough of these triples, i. e. $(r_i, s_i, c_i)_{i=1,\dots,z}$. Again we are able to compute integers e_i such that

$$(\prod_{i=1}^{z} c_i^{e_i})\mathfrak{o}_K = I^l$$

where I denotes some ideal of $\mathfrak{o}_K$. But now we can not apply the same argument as in the case of prime fields above, since the ideal I need not be a principal ideal.

Thus we are lead to consider the following number theoretical problem:

Definition 8.1.1 *Set*

$$V_l = \{\alpha \in K \,|\, v_{\mathfrak{p}}(\alpha) \equiv 0 \bmod l \,\forall\, \mathfrak{p}\}.$$

Then the problem to decide whether an element in $V_l/K^{\times l}$ ss trivial is called **obstruction problem**.

If we want to use the following algorithm 3 in order to solve the discrete logarithm problem in the finite field $\mathbb{F}_{p^n}$, we have to find a way to deal with the obstruction problem.

Algorithm 3 Computing the DL in cyclic subgroups using l–th powers.
Input:
finite field $\mathbb{F}_{p^n}$, number field K, surjection $\phi : \mathfrak{o}_K \to \mathbb{F}_{p^n}$, $a, b \in \mu_l(\mathbb{F}_{p^n})$.
Output: m such that $a^m = b$.

1. `Choose a factorbase of (algebraic) primes` S.
2. `Generate` $c = a^{s_a} b^{s_b}$. `Lift` c `to` $\overline{c}$ `in` $\mathfrak{o}_K$ `via` ϕ. `Keep` $\overline{c}$ `if it is` S`--smooth.`
3. `Find more than` $|S|$ `smooth lifts` $\overline{c_1}, \dots, \overline{c_z}$.
4. `Compute` $e_i \in \mathbb{Z}/l\mathbb{Z}$ `such that` $(\prod_{i=1}^{z} \overline{c_i}^{e_i})\mathfrak{o}_K = I^l$.
5. `Decide if` $(\prod_{i=1}^{z} \overline{c_i}^{e_i})$ `is a` l`--th power in` K.
6. `If it is, return` $(-\sum e_i s_{a_i})/(\sum e_i s_{b_i}) \bmod l$.

8.2 Solutions for the Obstruction Problem

In the literature one can find two approaches to deal with the obstruction problem:
The first one uses the concept of character signatures ([AD93]), the second one uses a technique of Schirokauer based on p–adic logarithms ([Sch93, Proposition 3.10]).

We give a brief overview of the two techniques:

8.2.1 Character Signatures

The concept of character signatures was originally developed in the context of factoring and was adopted to index calculus by Adleman in [AD93].
Let K be a number field. Call an algebraic integer α generating an ideal of the form I^l an l–singular integer with respect to $\mathfrak{o}_K$.

Let σ, τ be two l–singular integers, call σ equivalent to τ ($\sigma \sim \tau$), if there exist $\alpha, \beta \in \mathfrak{o}_K$ such that $\alpha^l \sigma = \beta^l \tau$. Let $G(l)$ be the group of equivalence classes of l–singular integers with respect to $\sim$. It is a group of exponents dividing l with identity element $I(l) = \{\alpha^l | \alpha \in \mathfrak{o}_K\}$ and group operation $[\alpha][\beta] \mapsto [\alpha\beta]$. Let $Cl(K)[l]$ be the l–torsion inside the class group of K. Then $G(l)$ can be written in the form

$$G(l) \simeq U(K)/U(K)^l \oplus Cl(K)[l], \tag{8.1}$$

where $U(K)$ denotes the unit group of K.

We now introduce the notion of a character signature:
Consider prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_z$ of $\mathfrak{o}_K$, elements $n_1, \dots, n_z \in \mathfrak{o}_K$ and $\sigma \in \mathfrak{o}_K$. Assume that $(\sigma) + \mathfrak{p}_i = (1)$ for all i, $l | N(\mathfrak{p}_i) - 1$ and that n_i is a primitive l–th root of unity in $(\mathfrak{o}_K/\mathfrak{p}_i)^\times$.
Then the character signature of σ with respect to $< \mathfrak{p}_i, n_i >$ is $< e_1, \dots, e_z >$ where

$$\sigma^{(N(\mathfrak{p}_i)-1)/l} \equiv n_i^{e_i} \bmod \mathfrak{p}_i.$$

Assume that K is Abelian over $\mathbb{Q}$, then by Cebotarev it follows that for all prime ideals $\mathfrak{p}_i$ and $c \in G[l]$, there exists $\sigma \in \mathfrak{o}_K$ such that $[\sigma] = c$ and

$(\sigma) + \mathfrak{p}_i = (1)$.
Given $c \in G(l)$ and $< \mathfrak{p}_i, n_i >$, define the map θ by mapping c to the character signature of σ with respect to the $< \mathfrak{p}_i, n_i >$. The map θ is well defined on $G(l)$ and is a group homomorphism

$$\theta : G(l) \to \oplus_{i=1}^{z} \mathbb{Z}/l\mathbb{Z}.$$

How can these properties be used in order to solve the obstruction problem? Due to the finiteness of the class number and the fact that $U(K)$ is finitely generated we see from (8.1) that $G(l)$ is finitely generated as well. Let H be the number of generators of $C(l)$.

Recall that it is reasonably easy to construct l–singular elements $(\sigma_i)_{i=1,\dots,H}$ from the smooth liftings as described above. We now compute the character signatures θ_i of the elements σ_i and find elements b_i such that

$$\sum_i b_i \theta_i \equiv < 0, \dots, 0 > \bmod l.$$

Now Adleman argues that it is likely that the map $\theta : G(l) \to \oplus \mathbb{Z}/l\mathbb{Z}$ is an injection implying that these b_i are actually the same b_i needed in order to produce an element which is the identity element in $G(l)$. This in turn would imply that $\prod \sigma_i^{b_i} = \delta^l$ for $\delta \in \mathfrak{o}_K$. Hence our obstruction problem would be solved.

Note that you would need to compute rank$(G(l))$ many liftings in order to be able to apply this method, instead of just one as proposed in algorithm 3.

8.2.2 Schirokauers Approach

Schirokauer [Sch93] also uses characters to provide a solution to the obstruction problem. These are defined as follows.

Let K be a number field. Let l be rational prime which does not ramify in K. Let

$$\Gamma_1 = \{\gamma \in \mathfrak{o}_K | N_{K/\mathbb{Q}}(\gamma) \not\equiv 0 \bmod l\}.$$

For each prime ideal $\mathfrak{l}$ in $\mathfrak{o}_K$ dividing (l) let $\epsilon_{\mathfrak{l}} = |(\mathfrak{o}_K/\mathfrak{l})^\times|$ and let ϵ be the least common multiple of the $\epsilon_{\mathfrak{l}}$. Then for all $\gamma \in \Gamma_1$

$$\gamma^\epsilon \equiv 1 \bmod l.$$

Now define $\lambda_1 : \Gamma_1 \to l\mathfrak{o}_K/l^2\mathfrak{o}_K$ by

$$\lambda_1(\gamma) = (\gamma^\epsilon - 1) + l^2\mathfrak{o}_K.$$

For $i > 1$, let $\Gamma_i = \{\gamma \in \Gamma_{i-1} | \lambda_{i-1}(\gamma) = 0\}$, and let $\lambda_i : \Gamma_i \to l^{2^{i-1}}\mathfrak{o}_K/l^{2^i}\mathfrak{o}_K$ be the function given by $\lambda_i(\gamma) = (\gamma^\epsilon - 1) + l^{2^i}\mathfrak{o}_K$. For $1 \leq j \leq n$, let $\{b_j l^{2^{i-1}} + l^{2^i}\mathfrak{o}_K\}$ be a module basis for $l^{2^{i-1}}\mathfrak{o}_K/l^{2^i}\mathfrak{o}_K$ over $\mathbb{Z}/l^{2^{i-1}}\mathbb{Z}$. Then λ_i is given by the maps

$$\lambda_{i,j} : \Gamma_i \to \mathbb{Z}/l^{2^{i-1}}\mathbb{Z}$$

defined by the congruence

$$\gamma^\epsilon - 1 \equiv \sum_{j=1}^{n} \lambda_{i,j}(\gamma) b_j l^{2^{i-1}} \bmod l^{2^i}.$$

Since $\lambda_i(\gamma\gamma') = \lambda_i(\gamma) + \lambda(\gamma')$ and $\lambda_{i,j}(\gamma\gamma') = \lambda_{i,j}(\gamma) + \lambda_{i,j}(\gamma')$, these maps define homomorphisms on the group of units of $\mathfrak{o}_K$.

For any $\gamma \in K^\times$ and any prime ideal $\mathfrak{p}$ of $\mathfrak{o}_K$ let $\mathrm{ord}_\mathfrak{p}(\gamma)$ be the exponent to which $\mathfrak{p}$ divides the fractional ideal generated by γ. Now the relation between the maps λ_i and the obstruction problem comes from the following statement[Sch93]:

Theorem 8.2.1 *Let e be a positive integer, let ρ be the least integer such that $2^\rho > e$. Assume that the class number is not divisible by l and that the units in $\mathfrak{o}_K$ which are congruent to $1 \bmod l^{e+1}$ are l^e–th powers. Let $\gamma \in \Gamma_\rho$ be such that $\mathrm{ord}_\mathfrak{p}(\gamma) \equiv 0 \bmod l^e$ for all prime ideals $\mathfrak{p}$ in $\mathfrak{o}_K$ and $\lambda_\rho(\gamma) = 0$. Then γ is an l^e–th power in $\mathfrak{o}_K$.*

Note that both of the described techniques make use of certain more or less strong assumptions. We will now show how to avoid the obstruction problem in certain situations if we apply Brauer group techniques.
The central observation is that we only need to combine the global lifts in such a way that they generate a l–th power in the finite field k we consider. Brauer groups provide a technique to decide this from the global information we have. However we have to assume the existence of an extension of K with certain properties.

8.3 Application of Brauer Groups

We make the following fundamental assumption:

Main Assumption:
Assume that there exists a prime ideal $\mathfrak{p}$ of $\mathfrak{o}_K$ such that k is contained in the residue class field of $\mathfrak{p}$. Let $K_\mathfrak{p}$ be the ray class field of K belonging to the modulus $\mathfrak{m} = \mathfrak{p}$. Suppose that the order of $Cl_\mathfrak{m}(K)$ is divisible by l and that $(h(K), l) = 1$.

By the assumption we have that $l||Gal(K_\mathfrak{p}/K)|$. Since, by definition, $Gal(K_\mathfrak{p}/K)$ is Abelian, we can find a subgroup H of order $|Gal(K_\mathfrak{p}/K)|/l$, which fixes a Galois extension L/K of degree l. Since $(h(K), l) = 1$, this extension has to be ramified at $\mathfrak{p}$, since it can not be contained in the Hilbert class field of K.

We consider global algebras of the form $(L/K, \sigma, a)$. The following observation is crucial in this context:

Lemma 8.3.1 *Let $a \in K$ be an element of $V_l = \{\alpha \in K^\times \,|\, l|v_\mathfrak{q}(\alpha) \forall \mathfrak{q}\}$. Then under the assumption made above we know that $inv_\mathfrak{p}(a) \equiv 0 \bmod l$.*

Proof: Consider the relation coming from the global algebra $(L/K, \sigma, a)$. It is given by

$$\mathrm{inv}_\mathfrak{p}(a) + \sum_{\mathfrak{q} \neq \mathfrak{p}} f_\mathfrak{q} v_\mathfrak{q}(a) \equiv 0 \bmod l \tag{8.2}$$

as we have seen many times before.

Now observe that in (8.2) all terms involving the unramified places $\mathfrak{q}$ vanish, since by definition $a \in V_l$ implies that $l|v_\mathfrak{q}(a)$ for all $\mathfrak{q}$. Therefore (8.2) reduces to

$$\mathrm{inv}_\mathfrak{p}(a) \equiv 0 \bmod l,$$

as claimed. □

But this means that we can apply the construction described above without considering the obstruction problem at all.

To see this consider again the element $\prod_{i=1}^{z} c_i^{e_i}$ from the preceeding section. By construction this is an element of V_l, hence the preceding lemma tells us, that $\mathrm{inv}_\mathfrak{p}(\prod_{i=1}^{z} c_i^{e_i}) = 0$. But this can only happen, if the associated element in the finite field $\mathbb{F}_{p^n}$ becomes trivial in the quotient $\mathbb{F}_{p^n}^{\times}/\mathbb{F}_{p^n}^{\times l}$, hence is a l–th power. But this means that we have an equation

$$a^{k_a} b^{k_b} = x^l$$

in $\mathbb{F}_{p^n}$, where $k_a = \sum_{i=1}^{z} e_i r_i$ and $k_b = \sum_{i=1}^{z} e_i s_i$. If $k_b \not\equiv 0 \bmod l$, we have thus obtained the solution $-k_a/k_b \bmod l$ of the discrete logarithm problem.

Note that the methods from this and the preceding chapters differ significantly:
While the preceding chapter described how local properties of the Galois group of subfields of ray class fields can be used to solve the discrete logarithm problem, this chapter shows that the pure existence of such subfields implies that the obstruction problem is trivial.

However we still need to address the problem of how to ensure the existence of such a subfield. We will give a survey of computational methods to achieve this in the next section. Furthermore we will also give some theoretical results.

8.4 Computing the Degree of Ray Class Fields

The task of computing the order of the ray class group given the number field K and a modulus $\mathfrak{m}$ is a well studied one, there is number theoretic software available which is especially suited to do this (for example KANT and PARI). Of course, the strongness of the main assumption we had to make in order to apply the theory of Brauer groups is closely related to the complexity of the computations involved.

Recall that the ray class group was defined by the exact sequence (5.1)

$$1 \to U_{\mathfrak{m}}(K) \to U(K) \to (\mathfrak{o}_K/\mathfrak{m})^{\times} \to Cl_{\mathfrak{m}}(K) \to Cl(K) \to 1.$$

Via this sequence the task of determing the structure of $Cl_{\mathfrak{m}}(K)$ can be related to determing the structure of $U(K)$ and $Cl(K)$ as well as to making all these maps effectively computable.

More precisely we are only interested in determing the order of $Cl_{\mathfrak{m}}(K)$. Therefore it would suffice to compute the order of $Cl(K)$ and $U(K)/U_{\mathfrak{m}}(K)$.

The computation of the order of $(\mathfrak{o}_K/\mathfrak{m})^\times$ can be neglected.

We would even be satisfied with computing the index of $U(K)_\mathfrak{m}$ inside $U(K)$, since we only need to satisfy the condition that $(h(K), l)$ which is likely to be met for a prime l of cryptographic size.

The computation of the index of $U(K)_\mathfrak{m}$ inside $U(K)$ however is a highly nontrivial task. The only way of solving this problem in the general situation (see [Coh00, Chapter 4] and here especially [Coh00, 4.5, Exercise 1 and Algorithm 4.1.11]) is to apply general algorithms for computations in finite Abelian group which require the groups to be given in Smith Normal Form (SNF). Especially this means that we need to compute a system of fundamental units of K. Hence for arbitrary number fields this can not be accomplished without reasonable computational effort.

8.5 CM fields and their Ray Class Fields

Since determing whether a given number field K has a subfield of given order inside the ray class field of modulus $\mathfrak{m}$ can be a substantial computational problem, it would be nice to have general results about the degree of the ray class field for a given modulus $\mathfrak{m}$.

The main observation is that it will suffice to give estimates for the index $[U_K : U_{K,\mathfrak{m}}]$ from above, since this will give bounds for the degree of the ray class field from below.

When searching for examples for such bounds, we made some interesting observations in the case of cyclotomic fields. It turned out that these observations hold in the general case of CM fields.

We briefly recall some basic properties of CM fields.

A number field is called totally real if all its embeddings into $\mathbb{C}$ in fact lie in $\mathbb{R}$, it is called totally imaginary if none of its embeddings lies in $\mathbb{R}$. An element of a totally real field is called totally negative, if all its conjugates are negative.

Definition 8.5.1 *A number field K is called a CM field if K is a totally imaginary quadratic extension of a totally real number field K^+.*

Hence a CM field can be obtained from a totally real field K^+ by adjoining to K^+ the square root of a totally negative element of K^+.

Cyclotomic fields $K = \mathbb{Q}(\zeta_n)$ are CM fields, since their maximal real subfield is given by $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, and K is obtained by adjoining the square root of $\zeta_n^2 + \zeta_n^{-2} - 2$, which is totally negative, to K^+.

CM fields are especially interesting in our context, since much can be said about the structure of their unit groups without explicitly computing the fundamental units:

Theorem 8.5.2 *Let K be a CM field and let U be its unit group. Let U^+ be the unit group of the totally real subfield K^+ of K. Let W be the group of roots of unity in K. Then*

$$[U : WU^+] = 1 \; or \, 2.$$

Proof: Let $\phi, \psi : K \to \mathbb{C}$ be two embeddings of K. For $\alpha \in K$ we want to show that $\phi^{-1}(\overline{\phi(\alpha)}) = \psi^{-1}(\overline{\psi(\alpha)})$. First note that $\phi(K)/\phi(K^+)$ is quadratic, thus it is a normal extension, $\phi(K^+)$ is fixed by complex conjugation. Hence we have $\phi(K) = \overline{\phi}(K)$. Especially this implies that $\phi^{-1}(\overline{\phi})$ is defined. Now consider $\phi^{-1}(\overline{\phi})$ and $\psi^{-1}(\overline{\psi})$. Both are automorphisms of K and both fix K^+ since it is totally real. Hence both lie in $Gal(K/K^+)$. But since K is totally imaginary, neither of them can be the identity. Hence these automorphisms must be equal, since K/K^+ is quadratic.

Therefore we have established the existence of an automorphism of K induced by conjugation which is independent of the embedding into $\mathbb{C}$. For an element α of K it is therefore possible to speak of $\overline{\alpha}$. Furthermore, $|\alpha|^2 = \alpha\overline{\alpha}$ is also independent of the embedding. If ε is a unit, then $\varepsilon/\overline{\varepsilon}$ is an algebraic integer of absolute value 1. But this means that α has to be a root of unity (see [Was82, Lemma 1.6]).

Thus we can define a map $\phi : U \to W$ by $\phi(\varepsilon) = \varepsilon/\overline{\varepsilon}$. Consider the map $\psi : U \to W/W^2$ induced by ϕ. Since W is cyclic we have $|W/W^2| = 2$. Now we need to compute the kernel of ψ.

First note that for a totally real unit ε_1 and a root of unity ζ we have that

$$\phi(\varepsilon) = \phi(\zeta\varepsilon_1) = \frac{\zeta\varepsilon_1}{\overline{\zeta}\varepsilon_1} = \zeta^2,$$

since ε_1 is totally real. Hence $\varepsilon \in ker(\psi)$. Suppose on the other hand that $\phi(\varepsilon) = \zeta^2$. Then consider $\varepsilon_1 = \zeta^{-1}\varepsilon$. From $\zeta^2 = \varepsilon/\overline{\varepsilon}$ we see that $\zeta^{-1}\varepsilon$ has to be real. Thus $ker(\psi) = WU^+$. Hence $[U : WU^+]$ is bounded by $|W/W^2| = 2$. Furthermore, the index is equal to 2 exactly if $\phi(U) = W$ and equal to 1 exactly if $\phi(U) = W^2$. □

Corollary 8.5.3 *Let $K = \mathbb{Q}(\zeta_{p^n})$. Then $[U : WU^+] = 1$.*

Proof: See [Was82, Corollary 4.13].

How can this be used in order to give estimates for the index $[U : U_{\mathfrak{m}}]$?

Consider the case $\mathfrak{m} = \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of K lying over an inert rational prime p. The condition that u is in $U_{\mathfrak{p}}$ is that $v_{\mathfrak{p}}(u-1) \geq 1$. This can be reformulated as follows: u has to be an element of the principal $\mathfrak{p}$–units $U_{\mathfrak{p}}^1$, which means exactly that $u \equiv 1 \bmod \mathfrak{p}$.

Now assume that K is a CM field hence WU_{K^+} has index 1 or 2 in U_K. The Dirichlet unit theorem says that the free part of U_{K^+} is generated by $s = [K : \mathbb{Q}]/2 - 1$ fundamental units $u_1, \ldots, u_s$. Together with the roots of unity of K these constitute the full unit group of K. Now from the defining condition for $U_{\mathfrak{p}}$ we see that is enough to estimate the exponent n such that $u_i^n \in U_{\mathfrak{p}}^1$ for all i.

We now use the fact that the fundamental units are defined in the totally real field K^+. Recall that $\mathfrak{p}$ lies over an inert rational prime p. This implies that p will also be inert in K^+, let $\mathfrak{p}_+ = \mathfrak{p} \cap K^+$.
But then we know that $u_i^{1+p+p^2+\cdots+p^{m-1}} \in U_{\mathfrak{p}_+}^1$, since the global norm of the u_i in K^+ is 1, therefore the norm of the image of the u_i in the finite field $k_{\mathfrak{p}_+}$ has to be equal to 1 as well. But since $\mathfrak{p}|\mathfrak{p}_+$ this also implies $u_i^{1+p+p^2+\cdots+p^{m-1}} \in U_{\mathfrak{p}}^1$ or $(u_i^{1+p+p^2+\cdots+p^{m-1}})^2 \in U_{\mathfrak{p}}^1$ depending on the index of WU_{K^+} in U_K.

Let ζ be a non trivial element of W, then $\zeta^{|W|} \equiv 1 \bmod \mathfrak{p}$. Therefore we obtain the following estimate:

Theorem 8.5.4 *Let K be a CM field of degree n, let $m = n/2$ be the degree of its maximal totally real subfield K^+. Let $\mathfrak{p}$ be a prime ideal lying over an inert rational prime p. Then we have that*

$$[U_K : U_{K,\mathfrak{p}}] \leq |W|[U_K : WU_{K^+}](1 + p + p^2 + \cdots + p^{m-1}).$$

.

But this gives the estimate for the degree of the ray class field$K_{\mathfrak{p}}$ over K we wanted:

Corollary 8.5.5 *We have*

$$\frac{p^{2m}-1}{lcm(|W|,[U_K:WU_{K^+}](1+p+p^2+\cdots+p^{m-1}))}\,|\,[K_{\mathfrak{p}}:K].$$

Hence assume that $(l,h(K))=1$ *and* $(l,|W(K)|)=1$ *and* m *odd. Then there exists an extension of degree* l *over* K *which is ramified exactly at* $\mathfrak{p}$ *if*

$$l|(p^{m-1}-p^{m-2}+\cdots+1)$$

Note that for l of cryptographic size, the conditions $(l,h(K))=1$ and $(l,|W(K)|)=1$ are not very restrictive, since they are very likely to be satisfied. Furthermore, the degree of K over $\mathbb{Q}$ gives a bound for the size of $|W|$, since K has to contain the appropriate cyclotomic field.

The following table compares the estimate with the actual degree of the ray class field in the case of the cyclotomic field $K=\mathbb{Q}(\zeta_7)$ by computing the quotient of the actual degree of the ray class field ramified at an inert prime p (computed by KANT) and the estimate $2*7*(p^2+p+1)$ (note that in this case $U_K=WU_{K^+}$.

It seems that even with growing p the deviation from the estimate seems to be bounded.

Inert Prime	Quotient	Inert Prime	Quotient	Inert Prime	Quotient
17	1	577	1	1277	1
19	3	593	1	1279	1
31	1	607	3	1291	1
47	1	619	1	1307	1
59	1	647	1	1319	1
61	13	661	3	1321	1
73	3	677	1	1361	1
89	1	691	1	1433	1
101	1	719	1	1447	3
103	1	733	1	1459	3
131	1	761	1	1487	1
157	3	773	1	1489	3
173	1	787	1	1531	3
199	1	829	3	1543	3
227	1	857	1	1559	1
229	1	859	1	1571	1
241	1	887	1	1601	1
257	1	929	1	1613	1
269	1	941	1	1627	1
271	1	971	1	1657	3
283	1	983	1	1669	1
311	1	997	1	1697	1
313	3	1013	1	1699	1
353	1	1039	1	1741	3
367	3	1069	1	1753	1
383	1	1097	1	1783	1
397	1	1109	1	1811	1
409	1	1123	3	1823	1
439	3	1151	1	1867	1
467	1	1153	3	1879	1
479	1	1181	1	1907	1
509	1	1193	1	1949	1
521	1	1223	1	1951	1
523	1	1237	1	1979	13
563	1	1249	1	1993	1

8.6 Application of CM Fields in Index Calculus

We now consider the case that we use CM fields in order to compute discrete logarithms in the residue class fields of these number fields.

As we have seen before our approach using Brauer groups is especially suited to compute discrete logarithms in cyclic subgroups. This is of special interest to cryptography, since the idea of hiding a small subgroup inside the multiplicative group of a finite field as originally proposed by Schnorr, features in several crypto systems (DSA in the case of prime fields, XTR in the case of extension fields).

Consider the case of extension fields $k = \mathbb{F}_{p^n}$. Here it is important to use a subgroup that is not contained in a proper subfield of k, since otherwise we loose the security of the larger field we work in. Therefore either n should be prime, or we need to study the factorization of the polynomial $x^n - 1$ over $\mathbb{Z}$. The second case is exactly what happens in the case of XTR.

We look at the case that $n = 2m$ with m odd. Suppose we can lift k to a CM field K in which p is inert.

Thus we have to consider the factorization of $x^{2m} - 1$. It is given by

$$\begin{aligned} x^{2m} - 1 &= (x^m + 1)(x^m - 1) \\ &= (x-1)(x^{m-1} + x^{m-2} + \cdots + x + 1) \\ &\quad (x+1)(x^{m-1} - x^{m-2} + x^{m-3} - \cdots - x + 1). \end{aligned}$$

Consider l prime such that $l | p^{2m} - 1$. In order to decide whether the cyclic subgroup C of order l inside $\mathbb{F}_{p^{2m}}^\times$ is contained in a proper subfield of $\mathbb{F}_{p^{2m}}$, we have to consider the factors of $x^{2m} - 1$ separately.

- l must not divide $p - 1$, since otherwise C would be contained in $\mathbb{F}_p^\times$.
- l must not divide $p^{m-1} + p^{m-1} + \cdots + p + 1$, since otherwise l would divide $p^m - 1$, hence C would be contained in $\mathbb{F}_{p^m}^\times$.
- l must not divide $p + 1$, since otherwise l would divide $p^2 - 1$, hence C would be contained in $\mathbb{F}_{p^2}^\times$.

Thus we get

Lemma 8.6.1 *Let C be a cyclic subgroup of prime order l, then if C is not contained in a proper subfield of $\mathbb{F}_{p^{2m}}$ we have that*

$$l|(p^{m-1} - p^{m-2} + \cdots + (-1)^{m-1}).$$

We are now ready to apply all our computations to the following situation:

Assume p is inert in the CM field K of degree d over $\mathbb{Q}$. Consider the discrete logarithm in the cyclic subgroup C of order l in $\mathbb{F}_{p^d}$, where C is not contained in any subfield of $\mathbb{F}_{p^d}$. Suppose that $(l, h(K)) = 1$ and $(l, |W(K)|) = 1$, where $W(K)$ denotes the group of roots of unity inside K.

In this situation there exists an extension ramified precisely at $\mathfrak{p}|p$ of degree l, since l satisfies the conditions of Corollary 8.5.5. Thus we can solve the discrete logarithm in this subgroup using Algorithm 3 with trivial obstruction. Thus, the most interesting case from the cryptographical point of view coincides exactly with the case in which we can apply Brauer group techniques.

Note that this provides the first example of an obstruction free approach to index calculus while working in number fields of degree larger than 2 we are aware of.

Theorem 8.6.2 *Let K be a CM field of degree $d = 2m$, let p be a rational prime inert in K.*

Then the discrete logarithm in cyclic subgroups of order l in $\mathbb{F}_{p^d}$, where l satisfies the conditions of Lemma 8.5.5 can be solved using algorithm 3 without obstruction.

It is especially worth noticing that this technique does not carry over to the general case of discrete logarithms in the field $\mathbb{F}_{p^n}$. It only holds for the special case of the cyclic subgroup described above.

It should also be noted that the complexity of this obstruction free version of algorithm 3 will still be $L_{p^n}(1/2)$ as shown in [AD93]. This is due to the fact that the size of the factor base has to vary in subexponential complexity $L_{p^n}(1/2)$ in order to guarantee sufficiently many smooth elements.

8.7 The Number Field Sieve

In order to achieve a subexponential complexity of exponent 1/3 we have to lift $\mathbb{F}_{p^n}$ to a fixed number field F and then consider another extension K/F of degree d depending on both p and n. This is the basic idea of the number field sieve, which was originally invented for factoring integers, but was adopted to the discrete logarithm problem by Gordon ([Gor93]) and Schirokauer ([Sch93],[Sch99]).

We give a brief overview of Schirokauers version.
Given $\mathbb{F}_{p^n}$ he first finds the smallest prime r congruent to 1 mod n such that n is prime to $(r-1)/f$, where f is the order of p in $(\mathbb{Z}/r\mathbb{Z})^{\times}$. Then $\mathbb{Q}(\zeta_r)$ has a unique subfield F of degree n over $\mathbb{Q}$. Since $\mathfrak{o}_F/\mathfrak{p}\mathfrak{o}_F \simeq \mathbb{F}_{p^n}$ we can use this isomorphism to lift $\mathbb{F}_{p^n}$ to $\mathfrak{o}_F$.

This is in fact completely analogous to what we did in the preceding section.

Now on top of F a second number field K is defined. While in the classical method, the l–th power we seek is constructed only in the number field F, we now simultaneously compute one l–th power in F and one in K. The subexponential size of the factorbase is now determined by K.

The advantage in complexity over the classical index calculus is now gained by defining K/F in such a way that the degree d of K/F is given by

$$d = ((3n)^{1/3} + o(1))(\log p/\log\log p)^{1/3}.$$

Then the smoothness bound (and hence the size of the factor base) can be lowered to

$$B = L_{p^n}(1/3, (8n/9)^{1/3} + o(1)),$$

where in all this estimates n is assumed to be fixed and p varies.

We show that in principle it seems possible to give examples in which both F and K have no obstruction. However one should note that K is constructed in a very special way, so it is not quite clear if this construction can be modified in order to obtain the sort of extension we describe.

Suppose we look at the XTR situation, hence we work in a cyclic subgroup of order l inside $\mathbb{F}_{p^6}$, where l divides $p^2 - p + 1$.

Now suppose that K is a CM field of degree $6d$ with d odd and cyclic Galois group $G = \langle\sigma\rangle$. Consider the subfield F fixed by σ^d, it is of degree 6 over $\mathbb{Q}$ and is also a CM field (see [Shi97, 18.2. Lemma]).

Assume that p is inert in $K/\mathbb{Q}$, which implies that p is also inert in $F/\mathbb{Q}$. Therefore we know that the obstruction for constructing a l–th power in K is trivial, if $(h(F), l) = 1$.

From Corollary 8.5.5 we obtain that the degree of the ray class field of K ramified at $\mathfrak{P}|p$ is divided by $p^{3d}+1$. But since d is odd we have $p^3+1|p^{3d}+1$. but $(p^2-p+1)|p^3+1|p^{3d}+1$. Hence there exists an extension of degree l over K ramified exactly at $\mathfrak{P}$ if we assume $(h(K), l) = 1$. Thus the construction of l–th powers over K also has trivial obstruction.

Theorem 8.7.1 *Let $K/\mathbb{Q}$ be a CM field which is Galois with cyclic Galois group of order $2 \cdot 3 \cdot n$ with n odd. Let $F/\mathbb{Q}$ be the CM subfield of degree 6. Assume that p is inert in $K/\mathbb{Q}$ and that $l|p^2 - p + 1$.*

Then the construction of l–th powers both in F and in K is without obstruction, provided that $(h(K), l) = 1$, $(h(F), l) = 1$ and $(|W(K)|, l) = 1$, where $W(K)$ denotes the number of roots of unity inside K.

We conclude this discussion by remarking that subexponential algorithms of complexity $L_{p^n}(1/2, c)$ still play an important role in the theoretical analysis of discrete logarithms, since at present there is no subexponential algorithm of exponent $1/3$ available if both p and n vary in such a way that

$$(\log p)^{1/2} < n < (\log p)^2.$$

This reflects the fact that the number field sieve method for discrete logarithms has subexponential complexity $L_{p^n}[1/3, (64/9)^{1/3} + o(1)]$ as long as $n < (\log p)^{1/2-\epsilon}$ when $p^n \to \infty$ with $0 < \epsilon = o(1)$ [Sch99]. The function field sieve, which will be discussed later (see chapter 9), works well for $\log p < n^{1/2}$.

8.8 Extensions with Several Ramified Primes and the Obstruction Problem

In the preceding sections we showed how to overcome the obstruction problem by proving the existence of a subfield of the ray class field with exactly one ramified prime. However as we have seen such extensions need not exist. We now give some experimental results concerning the existence of such extensions if we allow more primes to ramify in this extension.

More precise we look at the following:
Consider $F/\mathbb{Q}$ of degree n, let K be an extension F. Consider a prime $\mathfrak{p}$ lying over p which is inert in $F/\mathbb{Q}$. Thus, F can be considered as a number field lifting $\mathbb{F}_{p^n}$. Consider $l|(p^n-1)$.

Now let $\mathfrak{P}$ be an prime ideal of $\mathfrak{o}_K$ lying over $\mathfrak{p}$. In order to prove the vanishing of the obstruction for K we would have to prove the existence of an extension of degree l ramified at $\mathfrak{P}$ over K.

Example:
Let $F = \mathbb{Q}(\zeta_7)$, let $p = 17$. Then p is inert in F, consider $\mathfrak{p} = 17\mathfrak{o}_K$. We have $13|(17^2-17+1)$. Since F is a CM field, there exists an extension of degree ramified at $\mathfrak{p}$.

Now consider F/K given by $x^2+\zeta_7+\zeta_7^{-1}$. It has the equation

$$x^{12}+2*x^{11}+x^{10}+10*x^9+10*x^8-10*x^7+13*x^6-2*x^5+20*x^4-52*x^3+60*x^2-32*x+8=0$$

over $\mathbb{Q}$.

$\mathfrak{p}$ splits into two distinct primes in K: $\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2$. However, a computation of the degree of the ray class field over K yields that the degree of $K_{\mathfrak{P}_i}$ over K is 2.

But if we consider the ray class field ramified at all primes lying over $\mathfrak{p}$ instead, this does contain a subfield of order 13. Hence we see that in principle by switching from one ramified prime to several ones it is possible to enforce the existence of an extension we look for.

In order to make use of this in cryptography, we have to take care that the extra primes we allow to ramify have considerably smaller norm than $\mathfrak{p}$. Of course we also want that $l|N_{K/\mathbb{Q}}(\mathfrak{q})-1$, since we want to enforce the existence of an extension of degree l inside the ray class field. By including primes $\mathfrak{q}$ with this property in the modulus, we hope to raise the powers of l in the enumerator of 5.2. Hopefully the index in the denominator of 5.2 will not grow in the same way. If this happens we may obtain a subfield of order l inside the ray class field.

Example: Consider F and K as above. Look at the ray class field $K_{\mathfrak{m}}$ belonging to the modulus $\mathfrak{m} = 53\mathfrak{P}_1$ consisting of all the primes lying above 53 in F as well as one prime $\mathfrak{P}_1$ lying over $\mathfrak{p} = 17\mathfrak{o}_F$ in K.

We have that the degree of the ray class field ramified at all primes lying above 53 has degree
$$[K_{53} : K] = 2^3 \cdot 13^2 \cdot 409^1.$$
However the degree of $K_{\mathfrak{m}}$ is given by

$$[K_{\mathfrak{m}} : K] = (2) \cdot (13) \cdot (2^2 \cdot 13) \cdot (2^2 \cdot 7 \cdot 13 \cdot 409),$$

where the decomposition in of the Galois group G of $K_{\mathfrak{m}}/K$ in cyclic subgroups is indicated by parentheses.

Especially we see that G contains three cyclic subgroups of order 13. Hence we know that there exists an extension L/K of degree 13 which is ramified both at $\mathfrak{P}_1$ and at all primes above 53 (note that K has class number 1, thus the Hilbert class field of K is just K).

Suppose in general that L/K is an extension of degree l ramified at $\mathfrak{P}$ as well as at prime ideals $\mathfrak{q}_i, i = 1, \ldots m$ such that $l | N_{K/\mathbb{Q}}(\mathfrak{q}_i) - 1$, furthermore $N_{K/\mathbb{Q}}(\mathfrak{q}_i)$ is considerably smaller than $N_{K/\mathbb{Q}}(\mathfrak{p})$.

Suppose we have constructed elements $a_i, i = 1, \ldots, m+1$ such that

$$v_{\mathfrak{q}}(a_i) \equiv 0 \bmod l \, \text{for all} \, \mathfrak{q} \, \text{unramified}.$$

Then these elements lead to relations

$$\mathrm{inv}_{\mathfrak{p}}(a_i) + \sum_{j=1}^{m} \mathrm{inv}_{\mathfrak{q}_j}(a_i) \equiv 0 \bmod l.$$

Using the assumption that $N_{K/\mathbb{Q}}(\mathfrak{q}_j)$ is considerably smaller than $N_{K/\mathbb{Q}}(\mathfrak{p})$ we can now relate $\mathrm{inv}_{\mathfrak{q}_j}(a_i)$ to $\mathrm{inv}_{\mathfrak{q}_j}(a_k)$ for $i \neq k$ by solving the discrete logarithm problem defined in the l–th roots of unity inside $k_{\mathfrak{q}_j}$. Let $\mathrm{inv}_{\mathfrak{q}_j}(a_k) = n_{j,k} \cdot \mathrm{inv}_{q_j}(a_1)$.

Thus we obtain a system of relations

$$\begin{aligned} \mathrm{inv}_{\mathfrak{p}}(a_1) + \sum_{j=1}^{m} \mathrm{inv}_{\mathfrak{q}_j}(a_1) &\equiv 0 \bmod l \\ \mathrm{inv}_{\mathfrak{p}}(a_2) + \sum_{j=1}^{m} n_{j,2}\mathrm{inv}_{\mathfrak{q}_j}(a_1) &\equiv 0 \bmod l \\ \cdots &\equiv 0 \bmod l \\ \mathrm{inv}_{\mathfrak{p}}(a_{m+1}) + \sum_{j=1}^{m} n_{j,m+1}\mathrm{inv}_{\mathfrak{q}_j}(a_1) &\equiv 0 \bmod l \end{aligned}$$

What happens to this system of equations if we switch from a_i to $a_i^{k_i}$? Because we deal with invariants at ramified places, we simply get $\mathrm{inv}_{\mathfrak{p}}(a_i^{k_i}) = k_i\mathrm{inv}_{\mathfrak{p}}(a_i)$ and $\mathrm{inv}_{q_j}(a_i^{k_i}) = k_i\mathrm{inv}_{q_j}(a_i)$.

Thus we get a new system of equations

$$\begin{aligned} k_1\mathrm{inv}_{\mathfrak{p}}(a_1) + \sum_{j=1}^{m} k_1\mathrm{inv}_{\mathfrak{q}_j}(a_1) &\equiv 0 \bmod l \\ k_2\mathrm{inv}_{\mathfrak{p}}(a_2) + \sum_{j=1}^{m} k_2 n_{j,2}\mathrm{inv}_{\mathfrak{q}_j}(a_1) &\equiv 0 \bmod l \\ \cdots &\equiv 0 \bmod l \\ k_{m+1}\mathrm{inv}_{\mathfrak{p}}(a_{m+1}) + \sum_{j=1}^{m} k_{m+1}n_{j,m+1}\mathrm{inv}_{\mathfrak{q}_j}(a_1) &\equiv 0 \bmod l \end{aligned}$$

Summing up all these equations gives

$$\sum_{j=1}^{m+1} k_j\mathrm{inv}_{\mathfrak{p}}(a_j) + \sum_{j=1}^{m+1} \mathrm{inv}_{\mathfrak{q}_j}(a_1)(\sum_{r=1}^{m} k_r n_{j,r}) \equiv 0 \bmod l. \tag{8.3}$$

Now we see that $\prod a_j^{k_j}$ will be an l–th power in $k_{\mathfrak{p}}$ exactly if the double sum in (8.3) vanishes, since in this case

$$0 \equiv \sum_{j=1}^{m+1} k_j\mathrm{inv}_{\mathfrak{p}}(a_j) \equiv \mathrm{inv}_{\mathfrak{p}}(\prod_{j=1}^{m+1} a_j^{k_j}) \bmod l + .$$

But this happens exactly if we have

$$\begin{aligned} k_1 n_{1,1} + k_2 n_{1,2} + \cdots + k_m n_{1,m} &\equiv 0 \bmod l \\ &\cdots \\ k_1 n_{m+1,1} + k_2 n_{m+1,2} + \cdots + k_m n_{m_1,m} &\equiv 0 \bmod l. \end{aligned}$$

This system of equations has more equations than indeterminates, hence there exists a non trivial solution $k_1, \ldots, k_m$, which will give us a perfect l–th power in $k_{\mathfrak{p}}$.

Thus introducing more than one ramified prime leads to another way of dealing with the obstruction problem in index calculus by applying the theory of Brauer groups.

Chapter 9

The Function Field Sieve

9.1 Class Field Theory of Function Fields

It was pointed out by Adleman in 1994 that the analogy between number fields and function fields can be used to generalize the number field sieve to the situation of global function fields [Adl94].

In the previous chapters we have discussed the theory of index calculus in global number fields at length. The main difficulty we had to overcome in order to apply the theory of Brauer groups was to establish the existence of extensions of given ramification and degree over a number field K. We were only able to prove general results about this in the case of CM fields.

It turns out that the situation is much easier in the case of function fields, since we are able to construct global function fields for which the degree of certain ray class fields is given by a completely explicit formula.

Let K be a global function field with full constant field $\mathbb{F}_q$. Let $\mathfrak{p}, \mathfrak{q}_0$ be two different places of K. Denote by $K_{\mathfrak{p}}^{\mathfrak{q}_0}$ the maximal extension over K which is ramified exactly at $\mathfrak{p}$ together with the property that $\mathfrak{q}_0$ splits completely in $K_{\mathfrak{p}}^{\mathfrak{q}_0}$. In this case we have the following (see [Aue99, 5.10] and [Hay79]):

Theorem 9.1.1 *The degree of $K_{\mathfrak{p}}^{\mathfrak{q}_0}$ over K is given by*

$$[K_{\mathfrak{p}}^{\mathfrak{q}_0} : K] = h(K)deg(\mathfrak{q}_0)\frac{q^{deg(\mathfrak{p})} - 1}{q - 1}. \tag{9.1}$$

Here $h(K)$ denotes the class number of K.

Therefore we have the following nice corollary:

Corollary 9.1.2 *Suppose $deg(\mathfrak{q}_0) = 1$. Also suppose that $(h(K), l) = 1$. Then there exists an extension L/K of degree l, which is ramified exactly at $\mathfrak{p}$, if l divides $\frac{q^{deg(\mathfrak{p})}-1}{q-1}$.*

The proof for this carries over directly from the case of number fields.

Now consider a place $\mathfrak{p}$ and a prime l dividing $\frac{q^{deg(\mathfrak{p})-1}}{q-1}$. We want to show how we can interpret the discrete logarithm in the subgroup of order l inside $\mathbb{F}_{q^{deg(\mathfrak{p})}}$ using the Brauer group of K.

In doing this we make extensive use of the fact that the theory of cyclic algebras over global function fields is completely analogous to the case of number fields (see [Roq99] for details).

In the number field case in order to translate the discrete logarithm into the setting of Brauer groups we needed the exact sequence from the Hasse–Brauer–Noether theorem and the explicit formulae for the invariant map in the unramified case. Both of these are available in the case of global function fields as well.

Let L/K be as above, let $\mathfrak{q}$ be an unramified prime. Then the local invariant of the cyclic algebra $A = (L/K, \sigma_{\mathfrak{q}}, a)$ is given by

$$\mathrm{inv}_{\mathfrak{q}}(a) = deg(\mathfrak{q}) v_{\mathfrak{q}}(a) \bmod l.$$

Consider the local extension $L_{\mathfrak{p}}/K_{\mathfrak{p}}$, which is ramified by definition of L/K. Since $[L_{\mathfrak{p}} : K_{\mathfrak{p}}] = l$ and $l | q^{deg(\mathfrak{p})} - 1$, it is a Kummer extension and therefore separable. Thus we obtain

$$Br(L_{\mathfrak{p}}/K_{\mathfrak{p}}) \simeq \mathbb{F}^{\times}_{q^{deg(\mathfrak{p})}} / \mathbb{F}^{\times l}_{q^{deg(\mathfrak{p})}}$$

exactly as in the case of number fields.

This shows that again we can use the Brauer group $Br(L/K)$ in order to relate the invariant at the ramified place $\mathfrak{p}$ to those at the unramified places.

9.2 Brauer Groups and the Function Field Sieve

Consider $R = \mathbb{F}_p[x]$ and an irreducible polynomial f of degree n. f defines a place $\mathfrak{p}$ of degree n in $Quot(R) = \mathbb{F}_p(x)$, we have $k_\mathfrak{p} \simeq \mathbb{F}_{p^n}$.

Let S/R be an extension given by $H(x, y) = 0$ where H is irreducible over R and has degree d in y. Define $K = Quot(S)$, assume that K has full constant field $\mathbb{F}_p$. Also assume that $\mathfrak{p}$ splits completely in K, hence we have $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_d$.

We now use a standard theorem due to Kummer, which phrases the decomposition of $\mathfrak{p}$ in terms of the reduction of $H(x, y)$ modulo f (see [Sti93, III.3.7.]).

Assume that y is integral over $\mathcal{O}_\mathfrak{p}$. $H(x, y)$ can then be viewed as an element in $\mathcal{O}_\mathfrak{p}[y]$. We have a canonical map $\mathcal{O}_\mathfrak{p}[y] \to k_\mathfrak{p}[y]$ which can be obtained as follows:
Assume $H(x, y)$ has the form

$$y^d + \sum_{i=0}^{d-1} y^i h_i(x)$$

where $h_i \in \mathcal{O}_\mathfrak{p}$. Let $\overline{h_i}$ be the reduction of h_i modulo f, hence $\overline{H(x, y)} \in k_\mathfrak{p}[y]$ where

$$\overline{H(x, y)} = y^d + \sum_{i=0}^{d-1} y^i \overline{h_i}(x).$$

Now the fact that $\mathfrak{p}$ splits completely in K is equivalent to the fact that $\overline{H(x, y)}$ splits in d linear factors $y - \overline{\gamma_i}$ with $\overline{\gamma_i} \in k_\mathfrak{p}$.

Let γ_i denote a lift of $\overline{\gamma_i}$ to $\mathcal{O}_\mathfrak{p}$. Then for $i = 1, \ldots, d$ there exist places $\mathfrak{P}_i$ of K such that $\mathfrak{P}_i | \mathfrak{p}$ and such that $(y - \gamma_i) \in \mathfrak{P}_i$.

Furthermore, in this situation the residue class field $k_{\mathfrak{P}_i} = \mathcal{O}_{\mathfrak{P}_i}/\mathfrak{P}_i$ is isomorphic to $k_\mathfrak{p}[y]/(y - \overline{\gamma_i})$.

We are now ready to apply the function field sieve to this setting:

Choose a place $\mathfrak{P}$ from the d places lying over $\mathfrak{p}$. Choose an element γ in $\mathcal{O}_\mathfrak{p}$ such that $(y - \gamma) \in \mathfrak{P}$.

Now search for coprime polynomials $r, s \in \mathbb{F}_p[x]$ such that both $ry+s$ and $r\gamma+s$ are B–smooth: here an element of $\mathbb{F}_p(x)$ is called B–smooth if it factors in irreducible elements of degree less than B. We call $ry+s$ B–smooth if the norm of $ry+s$ over $\mathbb{F}_p(x)$ is B–smooth.

Note that due to the choice of γ above, the reduction of $r\gamma+s$ to $k_{\mathfrak{p}}$ is exactly the image of $ry+s$ in the residue class field of K at $\mathfrak{P}$ (note that since $\mathfrak{p}$ splits in K, $k_{\mathfrak{P}}$ is isomorphic to $k_{\mathfrak{p}}$).

Choose l such that $l|(p^n-1)/(p-1)$. By Corollary 9.1.2 there exists an extension L/K ramified at $\mathfrak{P}$ if $(h(K), l) = 1$.

Define two factor bases: S_1 contains all irreducible polynomials g of $\mathbb{F}_p[x]$ of degree bounded by B. Let S_2 be the factorbase obtained from S_1 by computing all primes of K lying over elements of S_1.

Assume that $ry+s$ and $r\gamma+s$ are both B–smooth with factorization

$$ry+s = \prod_{\mathfrak{Q}\in S_2} \mathfrak{Q}^{n_{\mathfrak{Q}}}$$

and

$$r\gamma+s = \prod_{g\in S_1} g^{n_g}.$$

Consider the relation generated by the global cyclic algebra $(L/K, \sigma, ry+s)$. It looks like this:

$$\sum_{g\in S_1} n_g \mathrm{inv}_{\mathfrak{P}}(g) + \sum_{\mathfrak{Q}\in S_2} deg(\mathfrak{Q}) n_{\mathfrak{Q}} f_{\mathfrak{Q}} \equiv 0 \bmod l.$$

Here $f_{\mathfrak{Q}}$ as always denotes the element in $\mathbb{Z}/l\mathbb{Z}$ such that $\sigma^{f_{\mathfrak{Q}}} = \sigma_{\mathfrak{Q}}$, where $\sigma_{\mathfrak{Q}}$ is the Frobenius at $\mathfrak{Q}$.

Collecting enough of these relations, we will be able to solve for $\mathrm{inv}_{\mathfrak{P}}(f)$ and the $f_{\mathfrak{Q}}$.

In this setting $\mathrm{inv}_{\mathfrak{P}}(g)$ for $g \in S_1$ is related to the discrete logarithm in $k_{\mathfrak{p}}$ as follows:

By construction we have $k_{\mathfrak{P}} \simeq k_{\mathfrak{p}} \simeq F_p[x]/(f)$. Hence $\mathrm{inv}_{\mathfrak{P}}(g)$ is the invariant related to the l–th root of unity $(g \bmod f)^{(p^n-1)/l}$ in $k_{\mathfrak{P}}^{\times}/k_{\mathfrak{P}}^{\times l}$. In a first step we compute sufficiently many of these invariants. In order to compute the invariants of the l–th roots of unity associated to elements $\alpha_1, \alpha_2 \in \mathbb{F}_p[x]$, we search for random exponents a_1, a_2 such that

$$\alpha_1^{a_1}\alpha_2^{a_2} \equiv g_1 g_2 \cdots g_t \mod f$$

where the g_i are B–smooth. From two such smooth relations we are able to compute $\mathrm{inv}_{\mathfrak{P}}(\alpha_1)$ and $\mathrm{inv}_{\mathfrak{P}}(\alpha_2)$ which yields the solution to the discrete logarithm problem.

We have thus reproduced the situation of the function sieve algorithm as invented by Adleman and Huang. Especially this means that that if the parameters are chosen carefully this algorithm is expected to have heuristic subexponential complexity of the form $L_{p^n}(1/3)$.

9.3 Complexity Estimates for the Function Field Sieve

We will now show how the heuristic suxexponential complexity of $L_{p^n}(1/3)$ can be accomplished.

Recall that we considered an extension of the rational function field given by the polynomial $H(x, y)$.

More precisely, let $H(x, y)$ now be of degree

$$d = \lceil c_1^{-1} n^{1/3} (\log n)^{-1/3} (\log p)^{1/3} \rceil,$$

where c_1 is a constant to be determined later.

Assume we have that $H(x, \gamma) \equiv 0 \mod f$, where γ is of degree $d' = \lceil n/d \rceil$. Now choose $r, s \in \mathbb{F}_p[x]$ of degree bounded by

$$c_2 n^{1/3} (\log n)^{2/3} (\log p)^{-2/3},$$

where again c_2 is also to be determined later.

Now by the assumption on γ we have that the degree of $r\gamma + s$ is bounded by

$$(c_1 + o(1)) n^{2/3} (\log n)^{1/3} (\log p)^{-1/3}.$$

Next we have to compute the norm of $ry + s$, this is given by $r^d H(x, -s/r)$. Hence its degree is bounded by

$$(c_2/c_1 + o(1))n^{2/3}(\log n)^{1/3}(\log p)^{-1/3}.$$

Hence the degree of

$$(r\gamma + s)N(ry + s)$$

is bounded by

$$D = \lceil (c_1 + c_2/c_1 + o(1))n^{2/3}(\log n)^{1/3}(\log p)^{-1/3} \rceil.$$

We make the heuristic assumption that with randomly chosen r and s, the polynomial $(r\gamma + s)N(ry + s)$ is random with degree bounded by D.

Set $Q = p^D$, set the smoothness bound $b = \log_p(L_Q(1/2, 1/\sqrt{2}))$. Then the probability for a pair (r, s) to be b–smooth is at least

$$L_Q(1/2, -1/\sqrt{2} + o(1)),$$

where we have to assume, that $\log p < n^{1/2-\epsilon}$ with $0 < \epsilon = o(1)$ (see [AH99, page 10]). The number of elements in the factor bases is bounded by $L_Q(1/2, 1/\sqrt{2})$, thus $L_Q(1/2, \sqrt{2} + o(1))$ pairs (r, s) have to tried. Since there are

$$p^{2c_2 n^{1/3}(\log n)^{2/3}(\log p)^{-2/3}}$$

available this leads to the condition that

$$L_Q(1/2, \sqrt{2}) \leq p^{2c_2 n^{1/3}(\log n)^{2/3}(\log p)^{-2/3}}.$$

This can be seen to lead to the inequality

$$\frac{c_2 + c_1^2}{3c_1} \leq c_2^2.$$

Thus we have $c_1 = (2/3)^{1/3}$ and $c_2 = (4/9)^{1/3}$, which implies

$$D = (2(2/3)^{1/3} + o(1))n^{2/3}(\log n)^{1/3}(\log p)^{-1/3}$$

and

$$b = L_{p^n}[1/3, (4/9)^{1/3} + o(1)].$$

.

The relations obtained from doubly smooth pairs (r, s) form a system of sparse linear equation modulo l. The complexity of solving this system is $L_{p^n}[1/3, (32/9)^{1/3} + o(1)]$.

In the last step we have to relate the given elements α_1 and α_2 to elements in the factor base. To do this we have to consider the probability for a random $g \in \mathbb{F}_p[x]$ of degree less than n to be B–smooth. If we assume that $p^6 < n$ this is shown to be given by

$$L_{p^n}[1/3, (3/2)^{1/3}]$$

in [AH99, page 12]. Even if we do not use the sophisticated techniques used here, we obtain a subexponential complexity of exponent 1/3 (see [Adl94]).

9.4 A Comparison of NFS and FFS

The main observation of this chapter was that using a completely explicit formula for the extension degree of the ray class field $K_{\mathfrak{p}}^{\mathfrak{q}_0}$ of a global function field K we were able to ascertain the existence of an extension L of K of degree l ramified exactly at $\mathfrak{p}$ if $(h(K), l) = 1$ and $l|(p^n - 1)/(p - 1)$ holds. This is in contrast to the situation of global number fields, where it was not possible to establish the existence of such an existence of given degree. Especially this means that we are not able to give an obstruction free version of index calculus.

If one compares the treatment of NFS and FFS in the literature, one makes the following observation:
As we explained above, in the case of number fields the obstruction problems needs considerable attention. Adleman points out that

> In the number field sieve, the analog of the function field is a number field. When this number field has class number greater than 1 problems arise.
> When the number field sieve is used to factor integers, then these problems can be overcome efficiently with the use of singular integers and character signatures (*Remark: this was later generalized by Adleman to the case of discrete logarithms [AD93]*).

> When the class number is not 1 in the function field case similar problems arise. However, if $(h(K), (p^n - 1)/(p - 1)) = 1$ then these problems also can be efficiently overcome. The basic idea is to pretend that $h = 1$ and that all divisors are principle.

This observation ties in nicely with the class field theoretical observation we made above:
indeed in the case of $(h(K), (p^n - 1)/(p - 1)) = 1$ we can use Brauer groups in order to prove that an obstruction free index calculus exists, which implies that we can proceed exactly as if "all divisors are principle". Therefore the fundamental difference in the difficulty of overcoming the obstruction problem can be viewed as documenting the fundamental difference between the class field theory of function fields and global fields.

Chapter 10

Abelian Varieties and the Tate pairing

We have pointed out before (see chapter 1) that the discrete logarithm problem in finite fields is only one instance of the discrete logarithm problem on which a public key crypto system can be based. The most important alternative to finite fields seems to be the case of Abelian varieties over finite fields. The most prominent examples for this are elliptic curves over finite fields, although Jacobians of hyperelliptic curves also seem promising.

The discrete logarithm problem on Abelian varieties can be linked to the discrete logarithm problem in finite fields using pairings on these varieties. We give a description of this approach for elliptic curves over finite fields and show how we can describe this approach using Brauer groups.

10.1 The Tate Pairing and the Discrete Logarithm Problem on Elliptic Curves

Using the Tate pairing, Frey–Rück reduction ([FR94], for details concerning implementational details see also [FMR99]) allows to transfer the discrete logarithm problem in the group of rational points of an elliptic curve over $E/\mathbb{F}_q$ (with $q = p^f$) to a discrete logarithm problem in $\mathbb{F}_{q^k}$ with $k \geq 1$.

Theorem 10.1.1 *Let $E/\mathbb{F}_q$ be an elliptic curve, assume $l|q-1$, hence the group of l–th roots of unity μ_l is contained in $\mathbb{F}_q$. Then there exists a non–degenerate pairing*

$$\phi_l : E[l](\mathbb{F}_q) \times E(\mathbb{F}_q)/lE(\mathbb{F}_q) \to \mu_l.$$

The evaluation of the pairing is given as follows:
Consider $P \in E[l](\mathbb{F}_q)$ and $Q \in E(\mathbb{F}_q)$, choose D_P and D_Q divisors of prime support in the classes of $(P)-(O_E)$ respectively $(Q)-(O_E)$. Since $lP = O_E$ we know that lD_P is a divisor of a function f_{D_P}. Then the pairing is given by

$$\phi_l : (P,Q) \mapsto (f_{D_P}(D_Q))^{(q-1)/l} \in \mu_l(\mathbb{F}_q). \tag{10.1}$$

Given P and Q with $Q = nP$, choose a point $\tilde{P}$ satisfying $\phi_l(P,\tilde{P}) = \zeta_0 \in \mu_l, \zeta_0 \neq 1$ and calculate $\phi_l(Q,\tilde{P}) = \zeta_1$. Since ϕ_l is a non–degenerate pairing, we have that $\zeta_1 = \zeta_0^n$, hence the solution of the discrete logarithm problem in $\mathbb{F}_q$ also yields the solution of the discrete logarithm problem on the elliptic curve E.

The pairing (10.1) can be defined strictly over finite fields, however we can also use duality theory for Abelian varieties over local fields, which was how Frey and Rück proceeded. We recall this approach and show how it is linked to the arithmetic of Brauer groups we studied in the preceeding chapters.

Lift the elliptic curve $E/\mathbb{F}_q$ to a suitable curve E defined over an extension K of $\mathbb{Q}_p$.

Then we can consider the pairing [Tat57]:

$$H^1(G_K, E(\overline{K}))[l] \times E(K)/lE(K) \to H^2(G_K, \overline{K}^{\times})[l] \simeq \mathbb{Z}/l\mathbb{Z}.$$

In the following we consider the relation between the Tate pairing (according to Lichtenbaum [Lic69]) and the pairing (10.1). To do this we describe the image of the Tate pairing inside the Brauer group.

Consider the two exact sequences

$$0 \to H(E) \to Div_0(E) \to Pic_0(E) \to 0, \tag{10.2}$$

where $Div_0(E)$ denotes the G_K–module of divisors of degree zero on the curve $E/\overline{K}$, $H(E)$ denotes the group of principal divisors and $Pic_0(E) = Div_0(E)/H(E)$ the Picard group of E, and

$$0 \to K^* \to \overline{K}(E) \to H(E) \to 0, \tag{10.3}$$

where $\overline{K}(E)$ denotes the function field of $E/\overline{K}$.

Since E has a K–rational point, we have $H^1(G_K, Div_0(K)) = 0$, hence the exact sequence (10.2) yields

$$\cdots \to 0 = H^1(G_K, Div_0(K)) \to H^1(G_K, E(\overline{K})) \xrightarrow{\delta} H^2(G_K, H(E)). \tag{10.4}$$

The exact sequence (10.3) gives another long exact sequence

$$\cdots \to H^2(G_K, \overline{K}(E)^*) \xrightarrow{\phi} H^2(G_K, H(E)) \to H^3(G_K, K^*) = 0, \tag{10.5}$$

since K has cohomological dimension two.

Let f_σ be an element of $H^1(G_K, E(\overline{K}))_l$. In order to calculate δf_σ, choose a lift $\hat{f}_\sigma$ of f_σ to $Div_0(E)$. Then we have

$$f_{\sigma,\tau} = (\delta f)_{\sigma,\tau} = \hat{f}_\tau^{\ \sigma} - \hat{f}_{\sigma\tau} + \hat{f}_\sigma \tag{10.6}$$

which is an element of $H^2(G_K, H(E))$.

According to (10.5) the map ϕ is surjective, hence there exists an element β in $H^2(G_K, \overline{K}(E)^*)$ with $\phi(\beta) = \delta(f_\sigma)$.
Let D_Q be an element of $Div_0(E)$ in the class of $(Q) - (0)$ and $f_{\sigma,\tau}$ be a two–cocycle in the class of β. If the support of $(f_{\sigma,\tau})$ and D_Q are coprime, we can define

$$c_{\sigma,\tau} = f_{\sigma,\tau}(D_Q) = \prod_{S \in E} f_{\sigma,\tau}(S)^{n_S} \text{ with } D_Q = \sum n_S S \tag{10.7}$$

which is a two–cocycle with values in $\overline{K}^\times$, hence defines a class $[c_{\sigma,\tau}]$ in $H^2(G_K, \overline{K}^\times)$, the Brauer group of K. In [Lic69] it is shown, that β always contains a two–cocycle coprime to D_P.

Consider now $\langle f, D_Q \rangle = [c_{\sigma,\tau}]$.
Lichtenbaum has proven in [Lic69], that

$$\begin{array}{rcl} \langle\ \ ,\ \rangle : H^1(G_K, E(\overline{K}))_l \times E(K)/lE(K) & \to & H^2(G_K, \overline{K}^*) \\ f_\sigma \times D_P & \mapsto & \langle f_\sigma, D_P \rangle = [c_{\sigma,\tau}] \end{array} \tag{10.8}$$

defines a pairing which is up to a sign equivalent to Tates original definition. Especially it is a non–degenerate and bilinear.

It turns out, that the pairing given by (10.8) can be evaluated very efficiently.

Crucial for this is the following observation

Lemma 10.1.2 *Suppose K contains the l–th roots of unity. Let π be a prime element of K and $\langle\tau\rangle$ the Galois group of the ramified extension $K(\pi^{1/l})/K$. Suppose that l is not equal to the characteristics of K and that E has good reduction* $\mathrm{mod}\pi_K$.
Then we have

$$H^1(G_K, E(\overline{K}))_l = Hom(\langle\tau\rangle, E(K)_l). \tag{10.9}$$

Proof:
Let K_u/K be the maximal unramified extension on K. Since l is not equal to the characteristic of $\overline{K}$ and E has good reduction, we obtain:

$$H^1(Gal(K_u/K), E(K_u))_l = H^2(Gal(K_u/K), E(K_u)) = 0. \tag{10.10}$$

With respect to the subgroup $H = Gal(\overline{K}/K_u) \subset Gal(\overline{K}/K)$ the inflation–restriction sequence gives

$$\begin{aligned} 0 \quad &\rightarrow \quad H^1(Gal(\overline{K}/K_u), E(\overline{K}))^{Gal(K_u/K)} \overset{infl}{\rightarrow} H^1(G_K, E(\overline{K})) \\ &\overset{res}{\rightarrow} \quad H^1(Gal(K_u/K), E(\overline{K}))^{Gal(\overline{K}/K_u)} = 0. \end{aligned}$$

Hence we have

$$H^1(Gal(\overline{K}/K_u), E(\overline{K}))_l^{Gal(K_u/K)} = H^1(G_K, E(\overline{K}))_l. \tag{10.11}$$

The exact sequence of $G/H = Gal(\overline{K}/K_u)$–modules

$$0 \rightarrow E(\overline{K})_l \rightarrow E(\overline{K}) \overset{l}{\rightarrow} E(\overline{K}) \rightarrow 0 \tag{10.12}$$

gives a long exact sequence

$$\begin{aligned} \cdots \rightarrow E(K_u) \overset{l}{\rightarrow} E(K_u) \rightarrow H^1(G(\overline{K}/K_u), E(\overline{K})_l) \quad &\rightarrow \quad H^1(G(\overline{K}/K_u), E(\overline{K})) \\ &\overset{l}{\rightarrow} \quad H^1(G(\overline{K}/K_u), E(\overline{K})) \rightarrow \cdots \end{aligned} \tag{10.13}$$

hence

$$E(K_u)/lE(K_u) \to H^1(G(\overline{K}/K_u), E(\overline{K})_l) \to H^1(G(\overline{K}/K_u), E(\overline{K}))_l \to 0. \tag{10.14}$$

But observe that $E(K_u)$ is l–divisible, since $l \neq char(\overline{K})$ and E has good reduction, hence $E(K_u)/lE(K_u) = 0$.
Combining this with (10.11) we obtain

$$H^1(G(\overline{K}/K_u), E(\overline{K}))_l = Hom(G(\overline{K}/K_u), E(\overline{K})_l)^{Gal(K_u/K)} \tag{10.15}$$

where we used the fact that, since E has good reduction, according to the criterion of Neron–Ogg-Shafarevich the action of $Gal(\overline{K}/K)$ on $E(\overline{K})$ is unramified. Hence the action of $Gal(\overline{K}/K_u)$ on $E(\overline{K})_l$ is trivial.
Each element of $Hom(G_{K_u}, E(\overline{K})_l)$ factors over the maximal l–quotient of G_{K_u}, and this is given by $Gal(K_u(\pi^{1/l})/K_u) = \langle\tau\rangle$.
Since τ commutes with all elements of $Gal(K_u/K)$, we obtain the result stated in the lemma. □

Let f_τ be an element of $H^1(G_K, E(\overline{K}))_l$. According to lemma 10.1.2 this means, that f_τ is given by $\tau \mapsto P$ with $P \in E(K)_l$.
In this case the associated two–cocycle $(\delta f)_{\tau^i,\tau^j}$ has a very special form:
lift f_τ according to $\hat{f}_{\tau^i} = (i - d*l)(P) - (i - d*l)(0)$ for $i = d*l + r$ and $r < l$ to $Div_0(E)$.

Now we proceed as in (10.6) and obtain for $i + j < l$

$$\delta f_{\tau^i,\tau^j} = i(P) - i(0) - ((i+j)(P) - (i+j)(0)) + j(P) - j(0) = 0 \tag{10.16}$$

and for $i + j > l$

$$\delta f_{\tau^i,\tau^j} = i(P) - i(0) - ((i+j-l)(P) - (i+j-l)(0)) + j(P) - j(0) = l(P) - l(0). \tag{10.17}$$

Therefore we have

$$(\delta f)_{\tau^i,\tau^j} = \begin{cases} 0 & : \; i+j < l \\ l(P) - l(0) & : \; i+j \geq l \end{cases} \tag{10.18}$$

Since $lP = O_E$ we know that $l(P) - l(0)$ is a principal divisor associated with the function f_P. Hence the image of the pairing in $H^2(G_K, \overline{K}^{\times})$ is given by the class of the two–cocycle

$$(\delta f)_{\tau^i,\tau^j}(D_Q) = \begin{cases} 1 & : \ i+j < l \\ f_P(D_Q) & : \ i+j \geq l, \end{cases} \tag{10.19}$$

defined over a ramified extension of degree l.

Considering the evaluation of the pairing the following observation is crucial: According to theorem 2.4.3 and 2.7.1 the value of $f_P(D_Q)$ has to considered in

$$K^{\times}/N_{L/K}(L^{\times}) \simeq k^{\times}/k^{\times l}.$$

Indeed it is shown in [FR94, p.872] that the values of the pairing obtained by lifting to the local field and then reducing to the finite field and of the pairing defined over the finite field coincide. Hence we obtain the two–cocycle describing the element in the Brauer group by computing the value of the pairing over the finite field.

Thus the description of the Tate pairing in terms of Brauer groups again leads us to the study of two–cocyles defined over ramified extensions of local fields. This was exactly the approach we discussed earlier when dealing with the discrete logarithm problem in finite fields. As we have shown this leads to well known index–calculus techniques solving the discrete logarithm problem in subexponential time.

Chapter 11

Application of the Tate pairing to the DHDP

11.1 Introduction

In this chapter[1] We will consider the security of various protocols on certain elliptic curves. Especially we will show that the Diffie Hellman decision problem is easy on some curves which was first observed by Frey. Furthermore we will make use of results of Maurer and Wolf in order to construct elliptic curves on which the Diffie Hellman decision problem is easy, but the discrete logarithm is hard and also equivalent to the Diffie Hellman problem. Thus we produce examples of cryptographic groups, in which the security of the Diffie Hellman decision problem is as low as possible, while the Diffie Hellman problem is hard.

Recall that in an (additive) group G we can pose the following problems (utilizing the Chinese remainder theorem we can assume G to have prime order without loss of generality):

- **The DL problem.** The DL (discrete logarithm) problem, is the problem given two group elements g and h, to find an integer n, such that $h = ng$ whenever such an integer exists.

[1] This chapter contains joint work with Antoine Joux [JN00].

- **The DH problem.** The DH (Diffie–Hellman) problem, is the problem given three group elements g, ag and bg, to find an element h of G such that $h = (ab)g$.

- **The DDH problem.** The DDH (decision Diffie–Hellman) problem, is the problem given four group elements g, ag, bg and cg, to decide whether $c = ab$ (modulo the order of g).

It is immediately clear that the solution of DH implies DDH and that the solution of DL implies DH. We first show how to apply the Tate pairing in order to solve the DDH on certain elliptic curves.

11.2 Diffie Hellman Decision Problem on elliptic Curves

Consider an elliptic curve E over a finite field k containing the l–th roots of unity together with the property that E has a k–rational torsion point P of order l.
Then the Tate pairing is defined in this situation and we can consider the value of $\langle P, P\rangle \in k^\times/k^{\times l} \simeq \mu_l$.

If this value is non trivial,$\langle P, P\rangle = \zeta_0$ say, the Tate pairing provides an easy solution to the DH decision problem:
Consider nP,mP as well as a point $Q \in \langle P\rangle$.
We want to decide whether $Q = nmP$ holds.

To decide this we evaluate the Tate pairing twice:
We first compute $\langle nP, mP\rangle = \langle P, P\rangle^{nm}$ and compare this to the value of $\langle P, Q\rangle$. If Q is indeed equal to nmP these two values coincide, since $\langle P, Q\rangle = \langle P, P^a\rangle = \zeta_0^a$. Hence $a \equiv nm \bmod l$ if $\zeta_0^a = \zeta_0^{nm}$.

Moreover this process will only take time polynomial in $\log q$, where $k = \mathbb{F}_q$, since the Tate pairing can be evaluated in $O(\log l)$ steps and the comparison can be done in $O(\log q)$ steps, since the value of the Tate pairing is an element of $\mathbb{F}_q^\times$.

Note that whenever k contains the l–th roots of unity, and $E(k)[l^2] = \langle P\rangle$ with P a point of order l, the Tate pairing for E/k will have the property that $\langle P, P \rangle \neq 1$. This condition is for example satisfied by all curves of trace 2 defined over a finite field k containing the l–th roots of unity, but not any roots of unity of l–power order.

If E is a supersingular curve over $\mathbb{F}_p$ the Tate pairing can be proven to be symplectic. Therefore we will have $\langle P, P \rangle = 1$ for every P, hence the Tate pairing can not be applied directly to the DH decision problem as outlined above.
But making use of our knowledge of the endomorphism ring of the curve E over $\mathbb{F}_p$ in some cases we will still be able to apply the Tate pairing.

Consider for example the curve $E : y^2 = x^3 + x$ over the field $k = \mathbb{F}_p$ where $p \equiv 3 \bmod 4$, which implies that E/k is supersingular. In this case we have that $|E| = p + 1$. Hence the full l–torsion group of E for $l \neq 2$ can not be defined over k, since otherwise we would have $l | p - 1$ and $l | p + 1$ and thus $l | p + 1 - p + 1 = 2$.

So we have $E(k)[l] = \langle P \rangle$ and $E(K)[l] = \langle P, Q \rangle$, where $K = \mathbb{F}_{p^2}$ and Q is defined over K. Now note that $p \equiv 3 \bmod 4$ implies that -1 is a quadratic nonresidue mod$p$, hence the endomorphism

$$\phi : (x, y) \mapsto (-x, i \cdot y),$$

where i is a root of $x^2 + 1 = 0$ in K, is not defined over k.

Thus we obtain that $\langle P, \phi(P) \rangle \neq 1$, and since ϕ is an endomorphism, we can now solve the DH decision problem in $\langle P \rangle$ by computing

$$\langle aP, \phi(bP) \rangle = \langle aP, b\phi(P) \rangle = \langle P, \phi(P) \rangle^{ab}$$

and

$$\langle cP, \phi(P) \rangle = \langle P, \phi(P) \rangle^{c}.$$

Note that we can solve the DH decision problem in the subgroup of order l over the ground field, although the pairing is not even defined over this field.

The application of endomorphisms in order to map a point from the ground field k to an extension field of k is only possible in the case of supersingular case, since only in this case the endomorphism ring is non commutative.

Here are some more supersingular curves with their respective endomorphisms (taken from [JN00]):

Field	Curve	Morphism	Conditions	Group order
$\mathbb{F}_p$	$y^2 = x^3 + ax$	$(x, y) \mapsto (-x, iy)$ $i^2 = -1$	$p \equiv 3 \pmod 4$	p+1
$\mathbb{F}_\mathfrak{p}$	$y^2 = x^3 + a$	$(x, y) \mapsto (\zeta x, y)$ $\zeta^3 = 1$	$p \equiv 2 \pmod 3$	p+1
$\mathbb{F}_{p^2}$	$y^2 = x^3 + a$	$(x, y) \mapsto (\omega \frac{x^p}{r^{(2p-1)/3}}, \frac{y^p}{r^{p-1}})$ $r^2 = a, r \in \mathbb{F}_{p^2}$ $\omega^3 = r, \omega \in \mathbb{F}_{p^6}$	$p \equiv 2 \pmod 3$	$p^2 - p + 1$

Table 11.1: Endomorphism on some supersingular curves

11.3 Results on the Equivalence of DH and DL

We have mentioned before that clearly DL implies DH. However Maurer and Wolf have proven that, assuming the existence of certain auxiliary groups, it is also possible to solve DL using only DH. We will now explain this result (see [MW99]).

Assume that we are given a group G of prime order p as well as a DH oracle for G. Assume also that we are also given an cyclic elliptic curve $E_{a,b}$ with generator P defined over $\mathbb{F}_p$ which has B–smooth group order. Maurer and Wolf show that in this case we can compute discrete logarithms in G in time $\sqrt{B}(\log p)^{O(1)}$.

So suppose we are given g^x, we want to compute x. First compute the group element g^{x^3+ax+b} from g^x. This can be done by $O(\log p)$ group operations and two calls to the DH oracle for G in order to compute g^{x^3} from g^x. If x^3+ax+b is a quadratic residue modulo p, then we can find a group element g^y such that $y^2 \equiv x^3 + ax + b \bmod p$ (otherwise replace g^x by g^{x+d} with random d). Note that we have done nothing else but computed a $\mathbb{F}_p$–rational point on the elliptic curve in the sense that we have computed $(g^x, g^y) = (g^x, g^{\sqrt{x^3+ax+b}})$ with $x, y \in \mathbb{F}_p$ where (x, y) is now a point on the elliptic curve $E_{a,b}$.

Given (g^{u_1}, g^{v_1}) and (g^{u_2}, g^{v_2}) where (u_i, v_i) are points on the elliptic curve $E_{a,b}$ we can compute (g^{u_3}, g^{v_3}) such that $(u_3, v_3) = (u_1, v_1) + (u_2, v_2)$ in $O(\log p)$ group operations in G and $O(\log p)$ calls to the DH oracle for G.
But now we can make use of the assumed smoothness of the group order of

E. Indeed let q be a prime factor of $|E_{a,b}|$. Given (g^x, g^y) compute (g^u, g^v) such that $(u, v) = (|E|/q)Q$ on E. Since we know a generator P of E we can compute the points $(u_i, v_i) = i(|E|/q)P$ on E for $i = 0, 1, \ldots, q-1$. From u_i, v_i we can obtain group elements in G simply by computing (g^{u_i}, g^{v_i}). Recall that our ultimate goal was to solve the discrete logarithm in G, which was transfered to E via (g^x, g^y), where $(x, y) = Q$ is a point on E.

Now suppose $Q = kP$, then we have $(g^u, g^v) = (g^{u_i}, g^{v_i})$ iff $k \equiv i \bmod q$. But this means that we can indeed compute k modulo the prime divisors of $|E|$ and recover k using Chinese remainder theorem. Once we know k, we can compute $Q = kP$. The solution to the discrete logarithm problem in G is then given by the first coordinate of Q.
Since we assumed the order of E to be B–smooth, it is now easy to see that these computations can be done in $O(\sqrt{B}(\log p)^3)$ operations and calls to the DH oracle.

This observation can be generalized to prove the following theorem:

Theorem 11.3.1 (Maurer,Wolf ([MW99])) *Let P be a fixed polynomial and let G be a cyclic group with generator g such that $|G|$ and its factorization $|G| = \prod_{i=1}^{s} p_i^{e_i}$ are known. If every prime factor p of $|G|$ greater than $B = P(\log|G|)$ is single, and for every such p a finite abelian group H_p with rank $r = O(1)$ is given that is defined strongly algebraically over $\mathbb{F}_p$ and whose order is B–smooth (and known), then breaking the Diffie–Hellman protocol for G with respect to g is probabilistic polynomial–time equivalent to computing discrete logarithms in G to the base g.*

Of course in order to turn into a rigorous proof of the equivalence of DH and DL, we would need a result on the distribution of smooth numbers in the Hasse interval $[p-2\sqrt{p}, p+2\sqrt{p}]$ (if we want to use elliptic curves as auxiliary groups). Since very little is known about this, the above argument only gives a strong heuristic argument for the equivalence of DH and DL. However, for a given group G with known order p if suffices to find a nice auxiliary group, for example an elliptic curve with smooth group order. We will show in the next section that this is indeed possible. Thus in special cases we can indeed construct groups with proven equivalence of DL and DH.

11.4 Separating DDH and DH

Now we want to apply the techniques described above in order to construct an elliptic curve with the properties that

- the DH decision problem can be solved in polynomial time using the techniques of section 11.2,
- the DH problem is polynomial–time equivalent to the DL using 11.3.

To do this we first construct a prime q of size 160 bit satisfying $q \equiv 3 \bmod 4$ such that $q+1$ is B–smooth, then the curve $E: y^2 = x^3 + x$ defined over $\mathbb{F}_q$ has smooth order $q+1$.
Now find a multiple lq of size 1024 bits such that $p = lq - 1$ is prime and satisfies $p \equiv 3 \bmod 4$, again this means that the curve $E: y^2 = x^3 + x$ defined over $\mathbb{F}_p$ has order lq.
Now consider the DH problem in the cyclic subgroup of $E(\mathbb{F}_p)$ of order q. Since $E/\mathbb{F}_p$ is supersingular, the q–th roots of unity are contained in $\mathbb{F}_{p^2}$ and we can apply the Tate pairing over this field to solve the DH decision problem. But since we have also constructed an elliptic curve with smooth order defined over $\mathbb{F}_q$, we can also apply Maurers result implying that on $E/\mathbb{F}_p$ the DH problem and the DL problem are polynomially equivalent.

Antoine Joux has indeed constructed a curve of this type (see the forthcoming preprint by Joux and myself[JN00]).

But we can also use the complex multiplication method in order to produce curves with the required properties.

Consider for example the prime

$$q = 2 \cdot 3^2 \cdot 5^2 \cdot 7^4 \cdot 11^4 \cdot 13^2 \cdot 17^2 \cdot 19^4 \cdot 23^4 \cdot 29^4 \cdot 41^4 \cdot 43^2 \cdot 47^2 \cdot 53^4 \cdot 59^2 \cdot 71^2 + 1.$$

By construction this prime splits in $\mathbb{Q}(\sqrt{-2})$ and hence gives rise to an elliptic curve given by the quadratic twist of $y^2 = x^3 + 4x^2 + 2x$ over $\mathbb{F}_q$ of trace 2. This curve has smooth group order $q-1$.

Now observe that the prime

$$\begin{aligned} p \;=\; & 1052027180309674701448197976576025733110067960564634771899656180613746430 \\ & 8594161644227333072555176902458828154778255387030653804798408032040744347 3 \\ & 1834051768223413568175716569369091530887708476713605295896792743 2 * q^2 + 1 \end{aligned}$$

also splits in $\mathbb{Q}(\sqrt{-2})$, so again will give us an elliptic curve $y^2 = x^3+4x^2+2x$ now over $\mathbb{F}_p$. Since $q^2|p-1$, this elliptic curve has a subgroup of order q. Also, it is checked easily that this curve possesses a q–torsion point P with the property that $\langle P, P\rangle \neq 1$.

11.5 Inverse Functions to the Tate Pairing

We will now consider the consequences the existence of an easily computable inverse to the Tate pairing would have.

An inverse to the Tate pairing is understood to be a group homomorphism $\phi : \mu_l \to E(\mathbb{F}_q)[l]$ such that $\langle \phi(\zeta), P_0\rangle = \zeta$ holds.

Consider $k = \mathbb{F}_p$ such that $l|p-1$, but k does not contain higher roots of unity of l–order. Let ζ_0 be a primitive l–th root of unity.

Now choose an elliptic curve E defined over $\mathbb{F}_p$ of Trace 2, that is $|E| = p-1$. Let P_0 be a fixed l–torsion point. We know that $\langle P_0, P_0\rangle = \zeta_0 \neq 1$ holds. But then we know that this must be true for each point of order l in $\langle P_0\rangle$, since for $P \in \langle P_0\rangle$, we have $P = nP_0$ with $1 \leq n < l$. It follows that

$$\langle P, P\rangle = \langle nP_0, nP_0\rangle = \langle P_0, P_0\rangle^{n^2} \neq 1.$$

Now we use this setting to solve the DH decision problem in the cyclic subgroup $\mu_l \subset \mathbb{F}_q^\times$ as follows:

Given $\zeta_0, \zeta_0^a, \zeta_0^b$ as well as ζ_0^c. We have to decide, whether $c = ab$ holds.

To do this we compute $\phi(\zeta_0) = P$, $\phi(\zeta_0^a) = P_a$,$\phi(\zeta_0^b) = P_b$ and $\phi(\zeta_0^c) = P_c$. We have so $P_a = aP, P_b = bP$ and $P_c = cP$.

But now we can apply the method described above in order to solve the DH decision problem on E. Hence we can determine in $O(\log p)$ operations, whether $c = ab$ holds on E and thus in μ_l.

So if one can find an inverse ϕ to the Tate pairing, which can be computed in $O(\log p)$ operations, we would be able to solve the DH decision problem in $\mathbb{F}_p$ in $O(\log p)$ operations.

The following points seem worth pointing out:

- At the moment the only method available to compute an inverse to the Tate pairing relies on the computation of sufficiently many discrete logarithms in $\mathbb{F}_p^\times$, hence has subexponential complexity.

- The construction of elliptic curves of trace 2 over arbitrary prime fields $\mathbb{F}_p$ seems to be a hard problem.

Menezes and Vanstone have pointed out, that the security of the XTR cryptosystem proposed by A. Lenstra and E. Verheul in 2000 is closely related to supersingular curves over $\mathbb{F}_{p^2}$.
Indeed choose a supersingular curve E over $\mathbb{F}_{p^2}$, then the Tate pairing is defined over an extension of degree 3, i. e. over $\mathbb{F}_{p^6}$. The points of order l on E, where l divides $p^2 - p + 1$ are mapped directly into the XTR subgroup of order l. Verheul [Ver00] has shown how by applying the Weil pairing with a special endomorphism the decision Diffie–Hellman problem can be solved on such a supersingular elliptic curve (the endomorphism is described in table 11.1).

He reasons that an efficiently computable embedding of the XTR subgroup into the group of points on a supersingular elliptic curve is not likely to exist since otherwise the decision DH in the XTR subgroup would be weak. If this reasoning is correct still remains to be seen.

Bibliography

[AD93] Leonard M. Adleman and Jonathan Demarrais. A subexponential algorithm for discrete logarithms over all finite fields. *Mathematics of Computation*, 61(203):1–15, 1993.

[Adl94] Leonard M. Adleman. The function field sieve. In *ANTS–I*, volume 877 of *LNCS*, pages 108–121. Springer, 1994.

[AH99] Leonard M. Adleman and Ming-Deh A. Huang. Function field sieve method for discrete logarithms over finite fields. *Information and Computation*, 151:5–16, 1999.

[Aue99] Roland Auer. *Ray Class Fields of Global Function Fields with Many Rational Places*. PhD thesis, Universität Oldenburg, 1999.

[Coh96] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Number 138 in Graduate Texts in Mathematics. Springer, 1996.

[Coh00] Henri Cohen. *Advanced Topics in Computational Number Theory*, volume 193 of *Graduate Text in Mathematics*. Springer, 2000.

[COS86] D. Coppersmith, A. Odlyzko, and R. Schroeppel. Discrete logarithms in GF(p). *Algorithmica*, 1:1–15, 1986.

[DH76] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, pages 644–654, 1976.

[ElG85] Taher ElGamal. A subexponential–time algorithm for GF(p^2). *IEEE Trans. Inform. Theory*, 31:473–481, 1985.

[eur98] *Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding*, volume 1403 of *Lecture Notes in Computer Science*. Springer, 1998.

[FMR99] Gerhard Frey, Michael Müller, and Hans-Georg Rück. The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. *IEEE Trans. Inform. Theory*, 45(5):1717–1719, 1999.

[FR94] Gerhard Frey and Hans-Georg Rück. A remark concerning m–divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 1994.

[Gol01] Oded Goldreich. *Foundations of Cryptography*. Cambridge University Press, 2001.

[Gor93] D. Gordon. Discrete logarithms using the number field sieve. *Siam J. Discrete Mathematics*, pages 124–138, 1993.

[Hay79] R.D. Hayes. Explicit class field theory in global function fields. *Stud.Alg.Number Th./Adv. Math. Suppl. Stud.*, 6:173–217, 1979.

[JL01] Antoine Joux and Reynald Lercier. Improvements on the general number field sieve for discrete logarithms in prime fields. *Mathematics of Computation*, 2001. accepted.

[JN00] Antoine Joux and Kim Nguyen. Separating decision diffie–hellman from diffie–hellman in cryptographic groups. Preprint, 2000.

[Ker90] Ina Kersten. *Brauergruppen von Körpern*, volume 6 of *Aspects of mathematics*. Vieweg, 1990.

[Kob87] Neal Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48, 1987.

[Kob89] Neal Koblitz. Hyperelliptic cryptosystems. *Journal of Cryptology*, 1:139–150, 1989.

[Lic69] Stephen Lichtenbaum. Duality theorems for curves over p–adic fields. *Invent. Math.*, 1969.

[Mil85] Victor Miller. Use of elliptic curves in cryptography. In *Abstracts for Crypto 85*, 1985.

[MW99] Ueli Maurer and Stefan Wolf. The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms. *SIAM Journal on Computing*, 28:1689–1721, 1999.

[Neu69] Jürgen Neukirch. *Klassenkörpertheorie*. Number 713/713a in BI Hochschulskripten. Bibliographisches Institut, 1969.

[Roq99] Peter Roquette. Class field theory in characteristic p, its origin and development, 1999.

[Sch93] Oliver Schirokauer. Discrete logarithms and local units. *Phil. Trans. R. Soc. London Ser. A*, 345:409–423, 1993.

[Sch99] Oliver Schirokauer. Using number fields to compute logarithms in finite fields. *Mathematics of Computation*, 69(231):1267–1283, 1999.

[Ser64] Jean-Pierre Serre. *Cohomologie Galoisienne*. Number 5 in Lecture Notes in Mathematics. Springer, 1964.

[Ser79] Jean-Pierre Serre. *Local Fields*. Number 67 in GTM. Springer, 1979.

[Shi97] Goro Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1997.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In *Advances in cryptology – Eurocrypt 1997*, volume 1233 of *LNCS*, pages 256–266, 1997.

[Sti93] Henning Stichtenoth. *Algebraic Functionfields and Codes*. Springer, 1993.

[Tat57] John Tate. WC–groups over p–adic fields. *Sem. Bourbaki*, 156:13 p., December 1957.

[Ver00] Eric Verheul. XTR is more secure than supersingular elliptic curve crypto systems. Preprint, 2000.

[Was82] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate texts in mathematics*. Springer, 1982.