Duality Theorems in Arithmetic Geometry and Applications in Data Security

Gerhard Frey

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

WS 07/08

Contents

Chapter 1

Crypto Primitives and Protocols

1.0.1 Preambula

To ensure a safe environment for data exchange and data storage is a very complex task involving problems from quite different areas like engineering and computer science but also "human factors" and legal problems, and as a small but crucial component, mathematics. It is the task of mathematics to provide the particles called crypto primitives around which cryptographic protocols are developed. To estimate the security of these protocols is a difficult problem which is impossible if one cannot trust the primitives.

In the following lecture we shall try to discuss one special but most important family of crypto primitives based on the discrete logarithm problem in groups. We shall describe how deep methods from arithmetical geometry and especially the interaction between Galois theory and algebraic geometry over special fields can be used to construct them and to give estimates (or hints) for their reliability.

The basic ideas go back to Diffie and Hellman. The main aim is the construction of a function f mapping the natural numbers $\mathbb{N}$ (or, in practice, a finite subset of $\mathbb{N}$) to a finite set A of $\mathbb{N}$ satisfying some "functional equations" and with the most important properties:

- The function f can be evaluated rapidly at every element of $\mathbb{N}$ but

- for randomly chosen $y \in A$ the effort needed to compute $x \in \mathbb{N}$ with $f(x) = y$ is very large, in the ideal case the brute force method " TRY" should be the best strategy.

So we have to find functions f together with algorithms to evaluate them with a proven small complexity, and we have to estimate the probability for finding the inverse images by proposing possible "attacks". In contrast to the first task in almost all cases the second one cannot be solved in a satisfactory way. What we can get are estimates for this complexity from above which will lead to reject some functions f and the statement that " to our best knowledge" other functions are safe "in the moment".

Since the security of the whole crypto system depends on this rather vague statement we would feel much better if we could use for f a *one way function* in the sense of information theory, or a *trap door one way function* (for the definition cf. [21]).
But since we even don't know whether such functions exist we have to use what we have and to be very sensitive to new developments in technology (e.g. "quantum computers" (cf. [26])) and to new results in mathematics. We refer to the rather spectacular progress in recent years in factorizing numbers (by sieve methods in number fields), in counting points on curves over finite fields (cf. [1] and the references therein) and in applying index-calculus methods to Discrete Logarithm Systems ([14] and [7]).

1.0.2 Exponential and Discrete Logarithm Systems

Let A be a finite subset of $\mathbb{N}$. For normalization reasons we shall assume that $1 \in A$.
Let

$$e : \mathbb{N} \times A \to A$$

be a function satisfying a *functional equation*:
For all $n_1, n_2 \in \mathbb{N}$ one has

$$e(n_1, e(n_2, 1)) \;=\; e(n_1 \cdot n_2, e(1, 1)).$$

This is enough to organize a **key exchange:**
Two parties M_1, M_2 want to agree on a common *secret key* based on e. The

communication uses a public channel.

Key exchange scheme: [1]

i) M_i chooses (as randomly as possible) a number n_i which never leaves the secure environment of M_i.

ii) M_i sends $y_i := e(n_i, 1)$.

iii) M_1 computes $e(n_1, y_2)$, M_2 computes $e(n_2, y_1)$.

Since

$$e(n_1, y_2) = e(n_1, e(n_2, 1)) = e(n_1 n_2, e(1, 1)) = e(n_2, e(n_1, 1)) = e(n_2, y_1)$$

M_1 and M_2 share the common key

$$S = e(n_1 n_2, e(1, 1)).$$

It is obvious that the secrecy of S depends on the secrecy of n_i and so on the difficulty to compute n_i from the knowledge of $y_i = e(n_i, 1)$.

So we *assume* that the function $e(n, a)$ as function of the first variable behaves like a one way function. Then we call

$$(e : \mathbb{N} \times A \to A; e(1, 1))$$

an *exponential system with base point* $e(1, 1)$.

For many applications one needs more "structure". For instance the *signature* of a message m can use a scheme of *ElGamal type* if we have a rapidly computable function

$$\oplus : A \times A \to A$$

which we require to be *associative*. In other words we require that A is a semigroup.

Using this associativity we define in the usual way for $n \in \mathbb{N}$ and $a \in A$

$$n \circ a$$

as the $n - 1$ fold application of $\oplus$ to a.

[1] We do not go into details of how this protocol has to be refined in order to become as secure as its primitive, the function e.

Remark 1.0.1 *Of course the actual computation of $n \circ a$ uses the well known method of (for instance) developing n in the binary system and then "adding and doubling" accordingly. This bounds the number of compositions $\circ$ by $2 \log n$. Several variants can be used to accelerate and sometimes precalculations speed up even more.*

Use this to define

$$e : \mathbb{N} \times A \to A$$

by

$$e(n, a) := n \circ a.$$

Obviously the function e satisfies the functional equation:
For all $n_1, n_2 \in \mathbb{N}$, $a \in A$ we have

$$e(n_1, e(n_2, a)) = e(n_1 n_2, a)$$

and especially

$$e(n_1, e(n_2, 1)) = e(n_1 n_2, e(1, 1)).$$

Signature

Let e be as above.
e satisfies a second functional equation

$$e(n_1, a) \oplus e(n_2, a) = e(n_1 + n_2, a).$$

This equation is used for signature schemes of El Gamal type. We shall give one variant:

Aim: M wants to sign a message m in such a way that everybody can check the authenticity of m but no one can fake the contents of m or the name of M.

To *initialize* the system M chooses, again randomly and secretly, his **private key** $x \in \mathbb{N}$ and publishes his **public key** $Y := e(x, 1)$.
This number Y identifies M in public.

Signing a message M uses, in addition to the DL-system, a (publicly known) *hash function* h which maps $\mathbb{N}$ to a set of numbers of bounded size. It has

to have properties similar to those of one way functions. Especially it has to be impossible in practice to construct a number z such that $h(z)$ is a given value. (For hash functions cf. [21].)

Signature 1 *M chooses a second random number k and computes*

$$s := h(m)x + h(e(k,1))k.$$

The signed message consists of

$$(m, e(k,1), s)$$

To check the authenticity of (M, m) one computes

$$S = e(s,1), P = e(h(m), Y)), H = e(h(e(k,1)), e(k,1)).$$

Now the functional equations of e imply:

$$S = P \oplus H$$

if the signature is authentic. Otherwise it is rejected.

It is obvious that the security of the signature depends on the quality of $e(.,1)$ as one-way function, but it is easily seen that this is not enough.

Logarithms

Definition 1.0.2 *The notation is as above.*
For given a in A and $b \in \{n \circ a, n \in \mathbb{N}\}$ the **logarithm of b with respect to** *a is a number $\log_a(b) := n_b \in \mathbb{N}$ with $n_b \circ a = b$.*

Complexity Hierarchy

To have a more precise statement on the complexity of algorithms we measure it by the function

$$L_p(\alpha, c) := \exp(c(\log p)^\alpha (\log\log p)^{1-\alpha})$$

with $0 \leq \alpha \leq 1$ and $c > 0$.

The *best case* for a cryptosystem is $\alpha = 1$ – then one has *exponential complexity*, this means that the complexity of solving the DLP is exponential in the binary length of the group size $\log p$. The *worst case* is when $\alpha = 0$ – then the system only has *polynomial complexity*. For $0 < \alpha < 1$ the complexity is called *subexponential*.

Definition 1.0.3 *The notation is as above. Let C be a positive real number.*

$$(\oplus : A \times A \to A, 1)$$

is a **Discrete Logarithm System (DL-systems) of exponential security** *C if for random elements $a, b \in A$ the computation of $\log_a(b)$ has (probabilistic) complexity [2] $\geq e^{C \cdot \log(|A|)}$.*

So DL-systems with exponential security C with C not too small give rise to exponential systems. We hope that we can find DL-systems with exponential security $1/2$.

But there are important examples which have only sub exponential security. This does not mean that we cannot use these systems but we have to choose larger parameters.

1.0.3 Algebraic DL-Systems

Let $(G, \times)$ be a finite group.
For our purposes the way how to present the group elements and the composition law is essential.

Definition 1.0.4 *A* **numeration** *(A, f) of G is a bijective map*

$$f : G \to A$$

where A is a finite subset of $\mathbb{N}$ containing 1.
A **presentation** *of an abstract finite group G is an embedding of G into a group with numeration.*

[2] In the whole paper the measure for complexity is the number of needed bit-operations.

Assume that (A, f) is a numeration of the finite group G and that $g_0 \in G$ with $f(g_0) = 1$ is given.

Define

$$\oplus : A \times A \to A$$

by

$$a_1 \oplus a_2 := f(f^{-1}(a_1) \times f^{-1}(a_2)).$$

Then for $n \geq 1$ we have

$$e(n, a) = f(n \circ f^{-1}(a))$$

as one sees easily by induction.
Especially we get: $e(n, 1) = f(n \circ g_0)$.

We want to make one thing completely clear: We require that $\oplus$ is rapidly computable *without* the knowledge of f^{-1} and that we can think of G as an abstract group (i.e. we look at it up to isomorphisms) but the security and the efficiency of the DL-System based on $\oplus$ will depend crucially on f.

We can refine our signature scheme 1:

Signature 2 *Let n be the order of G. Let (A, f) be a numeration of G and $e(.,.)$ as above. The signature procedure of a sender M and a message m is as described in Subsection 1.0.2 except that we replace in the equation of 1 all numbers by their smallest positive residue modulo n:*
The signature of m given by M is $(m, e(k, 1), s)$ with

$$s \equiv h(m)x + h(e(k, 1))k \ mod \ n$$

and $x, k, s, h(.) \in \{0, \cdots, n-1\}$.

1.0.4 The Diffie-Hellman Problems

Computational Diffie-Hellman problem

$$\text{For random } a \in A \text{ to compute}$$

$$\log_{a_0}(a) \text{ (CDH)}$$

is hard.
For many applications an even stronger condition is needed:
Decision **Diffie-Hellman problem**

$$\text{For random triples } (a_1, a_2, a_3) \text{ decide whether}$$

$$\log_{a_0}(a_3) = \log_{a_0}(a_1) \log_{a_0}(a_2).$$

$$\text{(DDH)}$$

1.0.5 Examples

Example 1:

We take a prime number p and the set $G := \mathbb{Z}/p$ together with its addition. Hence we deal with "the" group with p elements.
As numeration we take the map

$$f : G \to \{1, \cdots, p\}$$

given by

$$f(r + p\mathbb{Z}) := [r]_p$$

where $[r]_p$ is the smallest positive representative of the class of r modulo p. The function $\oplus$ is given by

$$r_1 \oplus r_2 = [r_1 + r_2]_p$$

which is easy to compute from the knowledge of r_i.

What about security? We can assume that $a \in \{1, \cdots, p-1\}$ and $b = e(n, a) = [na]_p$. To determine n we have to solve the equation

$$b = na + kp$$

with $k \in \mathbb{Z}$. But by using the *Euclidean algorithm* this task is done in $O(\log(p))$ operations in $\mathbb{Z}$ and so n is computed very rapidly. Hence the complexity to compute the DL is polynomial (even linear).
We can generalize the example easily to subgroups in the additive group of fields of characteristic p or to subspaces of vector spaces over $\mathbb{Z}/p$.

Example 2: Again we take $G = \mathbb{Z}/p$. In addition we choose a prime q such that p divides $q-1$. As it is well known this implies the existence of an element $\zeta \neq 1$ in $\mathbb{Z}/q$ with $\zeta^p = 1$ (i.e. ζ is a primitive p-th root of unity). Now define for $1 \leq i \leq p$ the number $z_i := [\zeta^i]_q$ and for $\bar{i} = i + p\mathbb{Z} \in G$

$$f(\bar{i}) := [z_i - z_1 + 1]_q.$$

Then f defines an injection of G into $\{1, \cdots q\}$ with $f(1 + p\mathbb{Z}) = 1$. Let A denote the image of f.

Using the addition in G we get for $a_i = f(x_i + p\mathbb{Z}) \in A$

$$a_1 \oplus a_2 = [[\zeta^{x_1+x_2}]_q - z_1 + 1]_q.$$

As stressed above it is important that one can compute $a_1 \oplus a_2$ without knowing x_1 and x_2. For this purpose we use the rules for addition and multiplication in $\mathbb{Z}/p$ and get:

$$a_1 \oplus a_2 = [(a_1 + z_1 - 1)(a_2 + z_1 - 1) - z_1 + 1]_q$$

and

$$e(n, 1) = n \circ 1 = [z_1^n - z_1 + 1]_q.$$

What about security in this system? For fixed a and random $b \in A$ we have to find n in $\mathbb{N}$ with

$$b = e(n, a) = n \circ a = [a^n - z_1 + 1]_q.$$

Essentially this means that for one fixed p-th root of unity and one random p-th root of unity in the multiplicative group of $\mathbb{Z}/q$ one has to determine the exponent needed to transform the fixed root of unity into the random element. This explains the name "discrete logarithm" introduced above.

Indeed to our knowledge at present a system based on this numeration is quite safe though for all constants C there is a number p_0 such that for all primes $p \geq p_0$ the corresponding DL-system it not of exponential security C. The best known method to compute the discrete logarithm is "subexponential" (cf. [1]). The suggested size of p is at least 2048 bits.

1.0.6 Generic Systems

In the examples in the last subsection we already had more structure available than necessary for us: The set A was the image of the numeration f of a *finite cyclic group* G. This will be so in the following sections, too.

This seems to be reasonable: The part of the numeration we use for key exchange and signatures is given by the numeration of the group generated by $f^{-1}(1)$. But it would be interesting to study whether one can win security by generating this numeration by a more complicated group like a general matrix group.

Next we used in the signature scheme 2 the order of G. There are crypto systems which are based on the assumption that one cannot compute this order or that one can compute it only by using a secret trapdoor function (RSA-like systems). Here we do not enter into these very interesting discussions but assume that the order of G and even its prime factorization are given.
An easy application (by some people called "Pohlig-Hellman attack") of the Chinese remainder theorem and p-adic expansion shows that the security of the discrete logarithm attached to G and so a forteriori of the cryptographic schemes is reduced to the difficulty to compute the DL in the subgroups of G with prime order. Hence we have to restrict ourselves to cyclic groups of order p where p is a prime number which is sufficiently large.

We can formulate the mathematical task to be solved more precisely now:
We have to find numerations f of groups $\mathbb{Z}/p$ with p large enough which satisfy:

- Time needed (probabilistically) for the computation of the logarithm in $f(\mathbb{Z}/p)$ is **exponential in log(p).**

- Time needed to write down the elements and to execute the composition $\oplus$ is **polynomial in $\log(p)$.**

But having decided to use the algebraic structure "group" in the construction of the crypto primitive "DL" we have added a lot of structure to our system. So it is important which methods are available to attack crypto systems which use "just" groups and the resulting DL-problems. For a very interesting discussion of different types of information which can weaken the protocols we refer to [19].
Of course the worst case is that the discrete logarithm can be computed.
Here the amazing fact is that we can do much better than brute force attacks: The Baby-Step-Giant-Step method of Shanks as well as the ρ- and Λ-methods of Pollard work in every finite group. All of them have time-complexity $O(p^{1/2})$ and the methods of Pollard need very little storage space (for more details cf. [21]).

These attacks give a first upper bound for the optimal exponential complexity of the Discrete Logarithm in finite groups: The constant $C = 1/2$ is the best one can hope for, and so we are forced to choose p of a size near to 10^{80} instead of 10^{40}.

1.0.7 The Index-Calculus Attack

In reality we shall have to use a concrete presentation of our group. In many examples there are elements in G which are easier to deal with, and this gives rise to the index-calculus attack.

The principle of index-calculus methods in abelian groups G is to find a "factor base" consisting of relatively few elements and to compute G as $\mathbb{Z}-$module given by the free abelian group generated by the base elements modulo relations.
As next step one has to prove that with high probability every element of G can be written (fast and explicitly) as a sum of elements in the factor base.
The important task in this method is to balance the number of elements in the factor base to make the linear algebra over $\mathbb{Z}$ manageable and to guarantee "smoothness" of arbitrary elements with respect to this base. Typically successes give rise to algorithms for the computation of the DL in G which have **subexponential** complexity and so, for large enough order of G, the

DL-systems have a poor exponential security.

The effectiveness of this approach is the reason for the large numbers of bits required for safe RSA-systems and for DL-systems based on the multiplicative group of finite fields (Example 2 in the Subsection 1.0.5).

In [7] one finds a very nice discussion of the index-calculus attack in a rather general frame. The results found there explain why it is so effective in many cases.

1.1 Bilinear Structures

1.1.1 Definition

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

Definition 1.1.1 *Assume that there are abelian groups A', B and a map*

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

satisfying the following requirements

- *Q is computable in polynomial time (this includes that the elements in B need only $O(\log \mid A \mid)$ space)*
- *for all $n_1, n_2 \in \mathbb{N}$ and random elements $a_1, a_2' \in A \times A'$ we have*

$$Q(n_1 \circ a_1, n_2 \circ a_2') = n_1 \cdot n_2 \circ Q(a_1, a_2')$$

- *$Q(.,.)$ is non degenerate. Hence, for random $a' \in A'$ we have $Q(a_1, a') = Q(a_2, a')$ iff $a_1 = a_2$.*

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

Remark 1.1.2 *One is used to describe bilinear maps on free modules by matrices with entries equal to the values on pairs of base vectors. This does not help in our context. For instance take $A = B$ as cyclic group with n elements and generator P_0 and $C := \mathbb{Z}/n$.*
For $m \in \mathbb{Z}$ prime to n define

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

by $Q_m(P_0, P_0) := m + n\mathbb{Z}$.
Without further information the computation of $Q_m(P, Q)$ is equivalent with the Discrete Logarithm in A. So bilinear maps are easy to be defined but it is much more difficult to find DL-Systems with bilinear structure. As we shall see one possibility is to use Duality Theorem from Arithmetic Geometry.

Example:

1.)Let V be a vector space over $\mathbb{F}_p$ with bilinear map ϕ which maps $V \times V$ to a $\mathbb{F}_p$ vector space W .
Take $a_0 \in V$, $A =< a_0 >$ and

$$< a_0 >^{\perp} := \{v \in V \text{ with } \phi(a_0, v) = 0_V\}.$$

Take $a_0' \in V \setminus < a_0 >^{\perp}$, $A' :=< a_0' >$, $B := \phi(< a_0 >, < a_0' >)$ und $Q = \phi_{|A \times A'}$.

2.) A little more general:
Let $\varphi : V \to V'$ be a (computable(!)) linear map and

$$\phi' : V \times V' \to W$$

bilinear. Define

$$\phi := \phi' \circ (id_V \times \varphi)$$

and then proceed as in example 1.

1.1.2 Applications

In the following we always assume that the DL-system $(A, \circ)$ has a bilinear structure

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

Transfer of DL

The DL-system $(A, \circ)$ is at most as secure as the system $(B, \circ)$.

For take random $a' \in A'$
and denote $b_0 := Q(a_0, a')$.

Then the map

$$< a_0 > \rightarrow < b_0 >$$

$$a := n \circ a_0 \mapsto Q(a, a')$$

is a monomorphism of numerated groups, and the claim follows.

DDH

Assume that

$$A = A'$$

and hence

$$Q(a_0, a_0) \neq 0.$$

Then for all triples $(a_1, a_2, a_3) \in < a_0 >$ one can decide in polynomial time (in $\log(p)$ whether

$$\log_{a_0}(a_3) = \log_{a_0}(a_1) \cdot \log_{a_0}(a_2)$$

holds. For we can use the identities

$$Q(a_1, a_2) = \log_{a_0}(a_1) \cdot \log_{a_0}(a_2) Q(a_0, a_0),$$

$$Q(a_3, a_0) = \log_{a_0}(a_3) Q(a_0, a_0).$$

Tripartite Key Exchange

The following is a nice idea of A. Joux (ANTS 4).
Parties P_1, P_2, P_3 want to create a common secret.
We assume that we have A with bilinear structure Q on $A \times A$.
Each partner P_i chooses a secret number s_i and publishes

$$a_i := s_i \circ a_0.$$

Hence every partner can compute

$$s_1 \circ Q(a_2, a_3) = s_2 \circ Q(a_1, a_3) = s_3 \circ Q(a_1, a_2),$$

the common secret. **(Semantical) Security** needs

1. hardness of the (computational) DL problem in A
2. hardness of the following problem called Bilinear Diffie-Hellman-Problem (BDH):
   For $(a, a_1 = n_1 \circ a, a_2 = n_2 \circ a, a_3 = n_3 \circ a)$ compute
   $n_1 n_2 n_3 \circ Q(a, a)$.

Identity based Protocol

This is an old dream (of Shamir):
One wants to send an encrypted message to a certain person without building up a public key environment but by the **use of one's identity** and some trusted institution TA which **computes a secret key** and the related public one (and the public key does not give information about the identity!)

We shall assume that $A =< a_0 >$ and $A' = A$.

We shall explain an idea of **Franklin and Boneh:** how to use it to come nearer to the dream. We have a sender Q who wants to transmit a message m to the receiver P. We shall assume that $m \in (\mathbb{Z}/2)^n$.

Q uses the service of TA.

Setup:
There are two publicly known hash functions

$$G : \mathbb{N} \to A$$

and

$$H : B \to (\mathbb{Z}/2)^n.$$

TA chooses s, the master key, and publishes $a_{pub} := s \circ a_0$.
Generation of keys:
P sends (after authentification) an element $ID \in (\mathbb{Z}/2)^n$ representing his identity to TA.
P (or TA, or the sender) computes

$$a_{ID} := G(ID) \in A$$

and then as
"public key" of P

$$b_{ID} := Q(a_{ID}, a_{pub}).$$

TA generates the **"private key"**

$$s_{ID} := s \circ a_{ID}$$

of P.

Encryption:
The message is $m \in (\mathbb{Z}/2)^n$.
Q chooses r randomly and computes
$r \circ a_0$ and $r \cdot b_{ID}$
and sends the ciphertext
$C := (r \cdot a_0, m \oplus H(r \cdot b_{ID}))$.

Decryption:
Let (U, V) be a cyphertext.
P computes
$T := H(Q(s_{ID}, U))$.
Then $m = V \oplus T$.

Proof:
Since $V = m \oplus H(r \cdot b_{ID})$ we have to show that $Q(s_{ID}, U) = r \cdot b_{ID}$.
But

$$Q(s_{ID}, U) = Q(s \circ a_{ID}, r \cdot a_0)$$

$$= rsQ(a_{ID}, a_0) = r \cdot Q(a_{ID}, s \circ a_0) = r \cdot b_{ID}.$$

(Semantical) Security
needs again the hardness of (BDH).

Work to do:
Assume that TA has done the original setup and has published
$A, B, Q, G, H, a_0, a_{pub}$.
To serve P it has to perform one scalar multiplication in A (with fixed argument a_0).
The **sender** has to compute b_{ID} by one application of Q with one argument $(= a_{pub})$ independent of P,one scalar multiplication in A of a fixed element (a_0) and one scalar multiplication in B with argument depending on ID.
P has to get his private key from TA and to compute Q (with one argument independent of the message and the sender).
In all cases precomputation is possible to accelerate the computation.
Advantage:
For the **sender:** He can send a message to a receiver who does not have a public key system before. (But he has to be sure that there is a TA which will communicate with P.)
For the **receiver** P**:** He has not to have a public or private key but only a ID before a message comes. So for instance TA could become active **after** a message arrives.
Big disadvantage:
TA knows everything since it has the master key s.
One case is interesting:

P is his own TA and creates different public keys with one master key and different identities, e.g. on laptops.

"The Gap"

The last application we mention is the construction of DL-systems in which (DDH) is weak (of polynomial complexity) but (CDH) is believed to be subexponentially hard.
The groups are points of order ℓ in supersingular elliptic curves E over fields $\mathbb{F}_q$ of odd degree over the prime field. The curves E have to be chosen in such a way that the order of $E/(\mathbb{F}_q)$ is not a smooth number.
Explicit examples have been given by A. Joux and K. Nguyen.

Chapter 2

Duality in Arithmetic

2.1 Dual Groups

2.1.1 Pairings in the world of functions

Let S be a (non-empty) set and C an abelian group.

$$F(S,C) := \{f : S \to C\}$$

becomes, in a natural way, an abelian group, and the evaluation map

$$S \times F(S,C) \to C$$

is non-degenerate and $\mathbb{Z}$-linear in the second argument.[1] The group $F(S,C)$ is in a natural way isomorphic to C^S.
The restricted product $C^{(S)}$ consists of all functions g_0 with the property that $g_0(s) = 0_C$ for almost all $s \in S$.
It is obvious that $C^{(S)}$ is a subgroup of $F(S,C)$.

Example 2.1.1 *$\mathbb{Z}^{(S)}$ is the group of functions g_0 from S to $\mathbb{Z}$ for which $g_0(s) = 0$ for almost all $s \in S$.*
S is embedded into $\mathbb{Z}^{(S)}$ by sending s to f_s with $f^{-1}(1) = \{s\}$ and $f^{-1}(0) =$

[1] In many contexts both S and C are endowed with a topology. In this case we tacitly assume that all functions are continuous.

$S \setminus \{s\}$.
$\mathbb{Z}^{(S)}$ *is the free abelian group generated by* S.

A function f from S to C can be extended "linearly" to $\mathbb{Z}^{(S)}$ to by

$$F : g_0 \mapsto \sum_{s \in S} g_0(s) \circ f(s).$$

Then $F \in Hom(\mathbb{Z}^{(S)}, C))$.
We get the pairing

$$Q : \mathbb{Z}^{(S)} \times F(S, C) \to C$$

by

$$Q(g_0, f) \mapsto F(g_0) = \sum_{s \in S} g_0(s) \circ f(s).$$

An important special case is that $C = \mathbb{Z}$.
For *fixed* $f \in F(S, \mathbb{Z})$ we define

$$\deg_f : \mathbb{Z}^{(S)} \to \mathbb{Z}$$

by

$$\deg_f(g_0) := Q(g_0, f) = \sum_{s \in S} g_0(s) f(s) = F(g_0).$$

Take $f \equiv 1$. In this case we denote $\deg_f$ by deg and its kernel by $\mathbb{Z}^{(S)0}$, the subgroup of elements of degree 0.

2.1.2 Pairings in the World of Homomorphisms

Now assume that S is an abelian group.
By restricting from $F(S, C)$ to $\mathrm{Hom}(S, C)$, the group of homomorphisms from S to C the evaluation map gives rise to a map

$$D : S \times Hom(S, C) \to C.$$

D is a pairing that is non-degenerate in the second argument.

The algebraic duality theorem

Take $C = \mathbb{R}/\mathbb{Z}$ with the discrete topology.
Functions from S to $\mathbb{R}/\mathbb{Z}$ are continuous if they are locally constant. For a homomorphism from S to $\mathbb{R}/\mathbb{Z}$ this means that its kernel is open.
Example:
If S is compact then a function is locally constant iff its image is finite.

The (topological) group $\mathrm{Hom}(S, \mathbb{R}/\mathbb{Z})$ is called the Pontryagin dual S^* of S.
If S is locally compact (finite) then S^* is locally compact (finite).
If S is compact then S^* is discrete.
The group $\mathbb{R}/\mathbb{Z}$ has a very special property: It is an injective $\mathbb{Z}$-module.
For injective

$$\iota : S_1 \hookrightarrow S$$

the restriction map

$$\iota^* : \mathrm{Hom}(S, \mathbb{R}/\mathbb{Z}) \to \mathrm{Hom}(S_1, \mathbb{R}/\mathbb{Z})$$

is surjective.
Consequence: The pairing

$$D : S \times S^* \to \mathbb{R}/\mathbb{Z}$$

is non-degenerate in both variables.
We have an embedding of S into $(S^*)^*$, and if S is compact (finite) then $S \cong (S^*)^*$in a canonical way (by evaluating functions).

2.2 Arithmetical Duality

Let K be a field of characteristic $p \geq 0$.
For simplicity we shall assume in the following that group orders are prime to p.
Let K_s be the separable closure of K and $G_K = \mathrm{Aut}_K(K_s)$ the absolute Galois group of K. This is a topological group with profinite topology and hence it is compact.

A Galois module M is a discrete $\mathbb{Z}$-module with continuous G_K-action. In particular, this implies that

$$M = \bigcup_U M^U$$

where U runs over subgroup of G which have finite index. The Galois module M determines a functor

$$\mathcal{M} : \{ \text{ fields between } K \text{ and } K_s\}$$

$$\mapsto \{ \text{ Abelian groups } \}$$

sending L to M^{G_L}.

Example 2.2.1 *Take $M = K_s^*$.*
The corresponding functor is called G_m.
It has a further nice property: It is representable.
This means: There is a scheme,also denoted by G_m, defined over K such that for commutative algebras R over K we have

$$G_m(R) = R^*, \text{ the group of}$$

$$\text{invertible elements in } (R, \cdot).$$

It is the spectrum of the coordinate ring

$$K[X, Y]/(XY - 1).$$

This example is generalized in the following way.
Assume that $\mathcal{A}$ is a commutative group scheme defined over K.
Then $A = \mathcal{A}(K_s)$ is a G_K-module. **Caution:** In general, $\mathcal{A}$ is not determined by $\mathcal{A}(K_s)$.

But this is so if $\mathcal{A}$ is smooth (i.e. reduced).
If $\mathcal{A}$ is a finite commutative group scheme with order prime to p then it is smooth and even **étale** over K.

Remark 2.2.2 *A finite Galois module is always represented by an (affine) étale commutative group scheme, and conversely, the K_s-rational points of a finite étale commutative group scheme are a finite Galois module.*

Remark 2.2.3 *Let A, B be G_K-modules. Then*

$$\mathrm{Hom}(A, B)$$

is a G_K-module in a natural way: For $\varphi \in \mathrm{Hom}(A, B)$ and $\sigma \in G_G$ define

$$\sigma(\varphi) = \varphi^\sigma := \sigma \circ \varphi \circ \sigma^{-1}.$$

The subgroup of G_K-invariant homomorphisms (ie $\sigma \circ \varphi = \varphi \circ \sigma$) is denoted by $\mathrm{Hom}_K(A, B)$.
If $\mathcal{A}, \mathcal{B}$ are étale group schemes defined over K we denote by $Hom(\mathcal{A}, \mathcal{B})$ the homomorphisms of the group schemes.
To

$$\phi \in Hom(\mathcal{A}, \mathcal{B})$$

there is associated a homomorphism

$$\varphi : \mathcal{A}(K_s) \to \mathcal{B}(K_s)$$

in $\mathrm{Hom}_K(A(K_s), B(K_s))$.
For finite étale commutative group schemes and all fields L between K and K_s we get a one-to-one correspondence between $Hom(\mathcal{A}_L, \mathcal{B}_L)$ and $\mathrm{Hom}_L(A(K_s), B(K_s))$.

Galois Duality

A pairing between the G_K-modules A, B in a G_K-module C is a $\mathbb{Z}$-bilinear map

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

with

$$Q(\sigma \circ a, \sigma \circ b) = \sigma Q(a, b)$$
$$\text{for all } (a, b, \sigma) \in A \times B \times G_K.$$

The key example is that $C = K_s^*$ and $B = \mathrm{Hom}(A, K_s^*) := \widehat{A}$, the Cartier dual of A.

Theorem 2.2.4 *The evaluation pairing $A \times \widehat{A} \to K_s^*$ is a non-degenerate Galois pairing. If $\mathcal{A}$ is a finite étale group scheme with order prime to p then $\widehat{\mathcal{A}} := Hom(\mathcal{A}, G_m)$ is the Cartier dual of $\mathcal{A}$ and $\widehat{\mathcal{A}(K_s)} = \widehat{\mathcal{A}}(K_s)$.*

$G_m(K_s)_{tor}$ is (non-canonically) isomorphic as abstract group to $(\mathbb{R}/\mathbb{Z})'_{tor}$, where $'$ means that we restrict ourselves to elements of order prime to p.
For finite étale group schemes with order prime to p we get

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

Key Examples

1. Take $A = \mu_n$, the group of roots of order dividing n with (as always,) n prime to p.
   Then $\mathcal{A} = ker(n \circ id_{G_m}) =: G_m[n]$ and we have the Kummer sequence

   $$1 \to G_m[n] \to G_m \to G_m \to 1$$

   of group schemes yielding the exact sequence of Galois modules

   $$1 \to \mu_n \to K_s^* \to K_s^* \to 1.$$

   The Cartier dual of $G_m[n]$ is the constant group scheme $\mathbb{Z}/n$ (with trivial Galois action) since every endomorphism of μ_n is an exponentiation.

2. Let $\mathcal{A}$ be be an abelian variety defined over K. Take

   $$\mathcal{A}[n] := ker(n \circ id_{\mathcal{A}}).$$

   Again we have a Kummer sequence

   $$0 \to \mathcal{A}[n] \to \mathcal{A} \to \mathcal{A} \to 0$$

   yielding the exact sequence

   $$0 \to \mathcal{A}(K_s)[n] \to A(K_s) \to A(K_s) \to 0$$

   of Galois modules.
   There is an abelian variety $\widehat{\mathcal{A}}$ dual to $\mathcal{A}$ such that, in a canonical way, $\widehat{(\mathcal{A}[n])}$ is isomorphic to $\widehat{\mathcal{A}}[n]$.
   In particular, we get a non-degenerate Galois pairing between the points of order dividing n of $\mathcal{A}(K_s)$ and $\widehat{\mathcal{A}}(K_s)$.
   An important special case is that $\mathcal{A}$ is principally polarized (eg., $\mathcal{A}$ a Jacobian of a curve). Then $\mathcal{A}$ is isomorphic to $\widehat{\mathcal{A}}$, and so $\mathcal{A}[n]$ is self-dual.

Computational Aspects

- In general it is not clear how to compute the evaluation pairing fast.
- In special cases (ie. if $\mathcal{A}$ is a subscheme of an abelian variety) there is an explicit and fast evaluation function, the Weil pairing.
- But even in this case one has to deal with objects in large extension fields L of K in general (eg., $L = K(\mathcal{A}[n](K_s))$ even though one is interested in the group of K-rational points. In general it is not true that the restriction of the pairing to $\mathcal{A}(K) \times \mathcal{A}(K)$ is non-degenerate.
- Caution: Assume that the exponent of A is n and that K contains the n-th roots of unity hence μ_n is isomorphic to $\mathbb{Z}/n$. Assume that we can compute the duality fast (E.g. take $A = \mu_n$) . Then this does not imply that we can transfer the discrete logarithm from A to $\mathbb{Z}/n$ but only to the multiplicative group of K.

Some of the items can be repaired by using "derived" pairings.

2.2.1 Galois Cohomology and Induced Pairings

In this section we take G as profinite group. Of course $G = G_K$ is the motivating example.

Galois Cohomology

Let A, B, C be G-modules such that

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

is exact. Then

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

is exact but in general β^G is not surjective: the functor

$$H^0(G, .)$$

sending A to A^G is left-exact but not right-exact.
To repair this "defect" one notes that there are "enough" injective modules and uses either a general machinery or an explicit construction to show that there is one derived cohomology functor H^* $(H^n(G,A), n = 0 \dots i, \dots)$ with

1.
$$H^0(G,A) = A^G$$

2. The exact sequence
$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$
induces maps $\alpha^{(n)}$, $\beta^{(n)}$ and δ^n such that there is an exact sequence of G-modules
$$\dots \xrightarrow{\delta^{n-1}} H^n(G,A) \xrightarrow{\alpha^{(n)}}$$
$$H^n(G,B) \xrightarrow{\beta^{(n)}} H^n(G,C) \xrightarrow{\delta^n} H^{n+1}(G,A) \dots$$

First take a standard projective resolution (*chain complex*) of $\mathbb{Z}$ (regarded as G-module with trivial action) and then take the cohomology of the complex obtained by replacing a module P_i by $Hom(P_i, A)$ (cochain complex) to define $H^n(G,A)$.

Remark 2.2.5 *Since $Hom_G(\mathbb{Z}, A) = A^G$ we can see Galois cohomology as derived from the Hom-functor:*

$$H^n(G,A) = Ext^n(\mathbb{Z}, A).$$

$H^n(G,M)$ is a quotient of the group of n-cocycles $\zeta(\sigma_1, \dots, \sigma_n) \in C^n(G,A) \subset F(G^n, A)$ satisfying a combinatorial condition modulo the subgroup of n-coboundaries $B^n(G,A)$.

Example 2.2.6 *1. 1-cocycles are maps*
$$c^1 : G \to A$$

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

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

1-*coboundaries are maps*

$$b^1 : G \to A$$

such that there exists an element $a \in A$ with

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

for all $\sigma \in G$.

2. 2-*cocycles are maps*

$$c^2 : G \times G \to A$$

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

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

$2-$*coboundaries are maps $b^2 : G \times G \to A$ such that there exists a function $f : G \to A$ with $b^2(\sigma, \tau) = \sigma f(\tau) - f(\sigma\tau) + f(\sigma)$.*

$\alpha \in Hom(A, B)$ induces by composition elements $\alpha'^{(n)} \in Hom(C^n(G, A), C^n(G, B))$ which map coboundaries to coboundaries and so induce $\alpha^{(n)} \in Hom(H^n(G, A), H^n(G, B))$. The maps δ^n are given in a very explicit way. We shall see examples soon.
For closed subgroups U of G we can restrict functions from G^n to A to functions of U^n to A and get

$$\mathrm{res}_U : H^n(G, A) \to H^n(U, A).$$

For normal closed subgroups $U < G$ we can compose the quotient map

$$G \to G/U$$

with cocycles and get the inflation map

$$inf_{G/U} : H^n(G/U, A^U) \to H^n(G, A).$$

Because of continuity one gets

$$H^n(G, A) = \lim_{\to U} inf_{G/U}(H^n(G/U, A^U)$$

where U runs over normal subgroups of G of finite index.

Example 2.2.7 *We can compute cohomology groups of G_K acting on A by computing the cohomology groups of the finite quotients $G(L/K)$ of G_K acting on A^{G_L} where L runs over finite Galois extensions of K.*

Etale Cohomology around the Corner Take $X = Spec(K)$. Etale (connected) covers of X are separable extension fields L of K with the induced map

$$Spec(L) \to Spec(K).$$

They define the "open" sets of the étale topology of $Spec(K)$. Galois modules A define sheaves via the section functor

$$\Gamma(Spec(L), A) := A^{G_L}.$$

The functor Γ is left-exact and there are enough flask sheaves (injective modules) and so we get a sheaf cohomology $H^n_{et}(X, A)$ resp. $H^n_{et}(X, \mathcal{A})$ which is nothing but the Galois cohomology of $A(= \mathcal{A}(K_s))$.
In general we have to begin with a scheme X replacing $Spec(K)$ and abelian sheaves with respect to unramified covers T of S, e.g. $\mathcal{A}(T) := Hom(Spec(T), \mathcal{A})$ for a smooth commutative group scheme $\mathcal{A}$ defined over S. As functor Γ take again $\mathcal{A}(S)$. The functor Γ is left-exact and there are enough flask sheaves and so we get a sheaf cohomology $H^n_{et}(X, \mathcal{A})$.
So we can embed Galois cohomology into a much wider and flexible frame.

Pairings in Cohomology

Let A and B be two $G-$modules.
The tensor product (over $\mathbb{Z}$)

$$A \otimes B$$

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

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

with functorial properties with respect to cohomology functors (especially δ^n, this implies uniqueness).
$\cup^{p,q}$ is called the cup product.
Explicit formulas can be found, eg., in the book of Cartan-Eilenberg. There the existence is proved by defining a product on the level of cochaines.
Now assume that there is a G-pairing

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

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

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

Example 2.2.8 *The evaluation pairing induces a pairing*

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

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

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

The Tate Pairing

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

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

yielding

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

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

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

2.3 Duality for Local and Global Fields

2.3.1 Class Field Theory

One of the most fascinating objects in number theory is class field theory ruling over the extensions of number fields which are Galois with abelian

Galois groups. The essentials of this theory are formulated in a very elegant way by a fundamental duality theorem involving étale cohomology. For a nice introduction we refer to B. Mazur's paper [20].
Let O be a ring of integers of a number field and $X = \mathrm{Spec(O)}$, let F be a constructible abelian sheaf (i.e. there are finitely many points $\{x_1, \ldots, x_n\}$ such that the pullback of F to $X \setminus \{x_1, \ldots, x_n\}$ and to $\{x_1, \ldots, x_n\}$ is locally constant.
With G_m we denote the group scheme attached to the multiplicative group.

Theorem 2.3.1 *For $0 \leq i \leq 3$ we have a perfect pairing*

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

of finite groups.

From this pairing we get duality theorems both for local fields (e.g. finite algebraic extensions of $p-$adic fields) and for global fields (here we consider finite algebraic extensions of $\mathbb{Q}$).

2.3.2 Duality over Local Fields

We apply Theorem 2.3.1 to finite Galois modules A over local fields K with residue field $\mathbb{F}_q$. We assume that the order of A is prime to q. In the language of Subsection 2.3.1 we interpret O_K, the ring of integers of K, as localization of the ring of integers of a number field, and look at abelian sheaves F trivial outside of $Spec(O_K)$.
$Spec(O_K)$ is a one-dimensional scheme with a closed point corresponding to the maximal ideal $\mathfrak{p}$, i.e. to $Spec(\mathbb{F}_q)$, and a generic point corresponding to $Spec(K)$ as open subscheme of X.
Galois modules over X consist of a generic fiber, i.e. a Galois module over G_K, a special fiber, which is a Galois module over the residue field, and a reduction map.
Etale neighborhoods are given by unramified extensions of O_K, by Galois extensions of K and by Galois extensions of k.
The duality theorem takes care of these data. Restricting to the generic fiber we come home to Galois cohomology.
We get the *Duality Theorem of Tate*:

Theorem 2.3.2 *1. $H^3_{et}(X, G_m)$ is isomorphic (in a natural way) to the Brauer group $H^2(G_K, K_s^*) = \mathrm{Br(K)}$ and hence this group is isomorphic to $\mathbb{Q}/\mathbb{Z}$.*

2. Let A be a finite G_K-module with Cartier dual $\widehat{A}$.
Then for $0 \leq i \leq 2$ the cohomology groups $H^i(G_K, A)$ are finite and the evaluation pairing induces non-degenerate pairings

$$H^i(G_K, A) \times H^{2-i}(G_K, \widehat{A}) \to \mathrm{Br(K)}.$$

As a consequence of this duality theorem Tate proves in [30]

Theorem 2.3.3 *Let J be an abelian variety (for simplicity principally polarized). The Tate pairing*

$$T_n : J(K)/nJ(K) \times H^1(G_K, J(K_s))[n] \to \mathrm{Br(K)}$$

is a non-degenerate pairing.

2.3.3 Duality over Global Fields

If we would like to get equivalent results like in the local case we would have to replace the multiplicative group by the idele group of K.
Here we restrict ourselves to cite consequences of the duality theorem.
Let K be a global field, i.e. either a finite extension of $\mathbb{Q}$ or a function field of one variable over a finite field. To simplify we shall assume that K is a number field but the function field case can be treated analogously and is very interesting (key word: function field sieve).
An important method in Number Theory is to relate global objects to local ones.
Let Σ_K be the set of all places of K (including archimedean places). For $\mathfrak{p} \in \Sigma_K$ we denote by $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$. We choose an extension $\tilde{\mathfrak{p}}$ of $\mathfrak{p}$ to K_s and identify the decomposition group of $\tilde{\mathfrak{p}}$ with $G_{K_\mathfrak{p}}$.
Let A be a G_K-module.
We have restriction maps

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

Define

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

The key questions are: Describe the kernel and the cokernel of f_n!
Here are consequences of Theorem 2.3.1(cf.[24]).
Assume that A is finite.

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

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

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

  (Here G_K is replaced by K, and $\prod'$ is the restricted product with respect to the unramified cohomology.)
- The Hasse-Brauer-Noether Sequence:
  For all natural numbers n the sequence

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

  is exact.

Chapter 3

Pairings on Class Groups of Curves

DL-systems in Class Groups

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

$$A \cdot B = \{\Sigma a_i \cdot b_i; a_i \in A, b_i \in B\}.$$

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

Definition 3.0.4 *Let M_1, M_1 be elements of $I(O)$.*
M_1 is equivalent to M_2 ($M_1 \sim M_2$) if there is an element $f \in F^*$ with

$$M_1 = f \cdot M_2.$$

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

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

There are only two types of rings O used today:

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

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

3.0.4 Ideal Classes of Function Rings

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

(resp. $\widetilde{C_O}$) by constant field extension.

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

We assume from now on that there is a K-rational point $P_\infty \in T_\infty$. The singularities of $\overline{C_O}$ are reflected by the conductor $\mathfrak{m}_{\overline{O}}$ of $\overline{\tilde{O}}/\overline{O}$. In geometric language $\mathfrak{m}_{\overline{O}}$ corresponds to a divisor also denoted by $\mathfrak{m}_{\overline{O}}$ on $\overline{C}$ with support in S (cf. [27]). For cryptographical purposes it is sufficient to look at the case that there is at most one singular point on C_O and that its conductor is square free, hence equal to $\mathfrak{m}_{\overline{O}} = \sum_{P\in S} P$. We shall assume this from now on.

Remark 3.0.5 *$\mathfrak{m}_{\overline{O}}$ is invariant under the action of G_K and so it corresponds to an ideal in $\tilde{O}$ which is equal to the conductor of $\tilde{O}/O$.*

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

Examples 3.0.6 *1. Take for R the ring $\overline{O_{P_\infty}}$ of meromorphic functions on $\overline{C}$ which have no poles outside of P_∞.*
Take $f \in \overline{F}^*$. For a point $P \in \overline{C}$ denote by $v_P(f)$ the order of vanishing of f at P, i.e. the order of zero if f in P if f is holomorphic, and the negative of the order of the pole of f at P else. Let m_P be the ideal of functions in $\overline{O_{P_\infty}}$ which vanish at P. Then $(f)_R = \prod_{P\in\overline{C}\setminus\{P_\infty\}} m_P^{v_P(f)}$.

2. *We continue to take* $R = \overline{O_{P_\infty}}$. *Take the set of* T_∞*-units* $\overline{U_{T_\infty}}$. *It is well known that* $(\overline{U_{T_\infty}})_R =: (\overline{U_{T_\infty}})$ *is a* $\mathbb{Z}$*-sublattice in the group of ideals* $\mathcal{D}_{T_\infty}$ *in* $I(\overline{O_{P_\infty}})$ *generated by the ideals* m_P *corresponding to points* $P \in T_\infty \setminus \{P_\infty\}$. *Define*

$$\mathcal{C}_{T_\infty} := \mathcal{D}_{T_\infty}/(\overline{U_{T_\infty}}).$$

3. *Take for* R *the ring* $\overline{\tilde{O}}$ *and* $f \in \overline{F}^*$. *Then* $(f)_R = \prod_{P \in \overline{C} \setminus T_\infty} (m_P \cdot \overline{\tilde{O}})^{v_P(f)}$.

By definition we have the exact sequence of Galois modules

$$1 \to \mathrm{Princ_R} \to \mathrm{I(R)} \to \mathrm{Pic(R)} \to 0.$$

Using the approximation theorem we get the exact sequence of G_K-modules

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

Next we want to describe $\mathrm{Pic}(\overline{O})$.
Let $I'(\overline{O})$ be the group generated by ideals of $\overline{O}$ which are prime to $\mathfrak{m}_{\overline{O}}$. Then $(\overline{F_S^1})$ is contained in $I'(\overline{O})$ and we get the exact sequence of G_K-modules

$$1 \to (\overline{F_S^1}) \to I'(\overline{O}) \to \mathrm{Pic}(\overline{O}) \to 0.$$

Using the approximation theorem for functions in $\overline{F}$ we get:

1. In every class $c \in \mathrm{Pic}(\overline{\tilde{O}})$ there is an ideal which is prime to S. So we have a natural surjective map $\varphi : \mathrm{Pic}(\overline{O}) \to \mathrm{Pic}(\overline{\tilde{O}})$ which is G_K-invariant.

2. The kernel of φ is in a canonical way isomorphic to $\prod_{P \in S} (K_s^*)_P / \Delta(K_s^*)$ where G_K acts on $\prod_{P \in S} (K_s^*)_P$ by $\sigma(\dots, x_P, \dots) = (\dots, \sigma(x_P)_{\sigma(P)}, \dots)$ and $\Delta(K_s^*)$ is the diagonal embedding.

A more geometric way to express this is

Proposition 3.0.7 *There is a torus* T_S *of dimension* $\mid S \mid -1$ *defined over* K *such that we have the exact sequence of* G_K*-modules*

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

Remark 3.0.8 *The isomorphism class of T_S is determined by its character group X, and this group is determined by the set S as G_K-set. So Proposition 3.0.7 (applied to $K = \mathbb{F}_q$) gives a tool to realize discrete logarithms in subgroups of multiplicative groups of extension fields of $\mathbb{F}_q$ as subgroups of ideal class groups of rings of holomorphic functions of affine curves.*

In Proposition 3.0.7 we have described the relation between ideal classes of rings $\overline{O}$ and their desingularization $\overline{\tilde{O}}$.
Now we investigate the relation between $\mathrm{Pic}(\overline{\tilde{O}})$ and the points on the Jacobian variety J_C of C.
Divisors D of $\overline{C}$ (or of $\overline{F}$) are formal sums with integer coefficients

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

with almost all $z_P = 0$. Using formal addition the set of divisors forms a group denoted by $\mathcal{D}$. Recall the discussion in Subsection 2.1.1 to see that $\mathcal{D} = \mathbb{Z}^{(\overline{C}(K_s))}$ and D corresponding to the function $g_0 : P \mapsto z_P$.
The degree of D is $\deg(D) = \sum_{P \in \overline{C}} z_P$. This is consistent with the definition in Subsection 2.1.1.
The subgroup $\mathcal{D}^0$ consists of the divisors of $\overline{C}$ of degree 0. It contains the group of principal divisors (f) attached to functions $f \in \overline{F}^*$ by

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

The quotient is the divisor class group of degree 0 of $\overline{C}$ (or of $\overline{F}$) denoted by $\mathrm{Pic}^0(\overline{C})$.
The connection to the ideal class groups considered above is given by

Lemma 3.0.9 *There is a natural group isomorphism from $\mathcal{D}^0$ to $I(\overline{O_{P_\infty}})$ given by the map φ_{P_∞} sending the divisor $D = \sum_{P \in \overline{C}} z_P \cdot P$ to the ideal $\prod_{P \in \overline{C} \setminus \{P_\infty\}} m_P^{z_P}$.*
This way, φ_{P_∞} maps principal divisors of $\overline{F}K$ to $\mathrm{Princ}_{\overline{O_{P_\infty}}}$ and induces an isomorphism between $\mathrm{Pic}^0(\overline{C})$ and $\mathrm{Pic}(\overline{O_{P_\infty}})$ which is compatible with the action of G_K.

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

Corollary 3.0.10 *We have the exact sequence of G_K-modules*

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

3.1 The Lichtenbaum Pairing

3.1.1 The Regular Complete Case

Let C be an absolutely irreducible non-singular projective curve defined over K with function field F with a $K-$rational point P_∞ (for simplicity). By $\overline{C}$ we denote the curve obtained from C by extending scalars to K_s. The function field of $\overline{C}$ is $\overline{F} = F \cdot K_s$.
G_K is acting in a natural way on $\overline{F}$ and $\overline{C}(K_s)$ with fixed sets F and $C(K)$. We apply the discussions in Subsection 2.1.1 to subsets $T \subset \overline{C}(K_s)$ which are assumed to be G_K-invariant, and interpret $\overline{F}_T \in \overline{F}$, defined as the group of functions on $\overline{C}$ *without* zeroes and poles in T, as Galois invariant subset in $F(T, K_s^*)$, the set of all maps from T to K_s^*.
The evaluation pairing

$$E_T : \mathbb{Z}^{(T)} \times \overline{F}_T \to K_s$$

is a Galois pairing inducing (for $p + q = 2$) a pairing

$$E_T^{p,q} : H^p(G_K, \mathbb{Z}^{(T)}) \times H^q(G_K, \overline{F}_T) \to \mathrm{Br(K)}.$$

Since C is assumed to be regular we can identify $\mathbb{Z}^{(T)}$ with the group $\overline{D}_T$ of divisors on $\overline{C}$ with support in T. For $T = \overline{C}(K_s)$ we get $\overline{\mathcal{D}}$, the divisor group of $\overline{C}$.
It is easy to see that $H^1(G_K, \overline{D}_T) = 0$.
In this paper we shall be interested in

$$E_T := E_T^{0,2} : H^0(G_K, \mathbb{Z}^{(T)}) \times H^2(G_K, \overline{F}_T) \to \mathrm{Br(K)}$$

where $H^0(G_K, \mathbb{Z}^{(T)}) := D_T$ can be identified with the group of K-rational divisors on C with support in T (Caution: This is not the free abelian group generated by K-rational points on C!).

Key Example

We assume that L/K is a cyclic extension of order n with Galois group $G =< \tau >$.
Because of Hilbert's Theorem 90 the inflation from $H^2(G, (F{\cdot}L)_T)$ to $H^2(G_K, \overline{F}_T)$ is injective.
We have the following explicit description of $H^2(G, (F \cdot L)_T)$: every cohomology class c contains a cocycle given by

$$\zeta_f(\tau^i, \tau^j) := 1 \text{ if } i + j < n$$

$$\zeta_f(\tau^i, \tau^j) := f \text{ if } i + j \geq n$$

with $f \in F_T$. ζ_f lies in the same class as ζ_g iff

$$f \cdot g^{-1} \in \mathrm{Norm}_{F \cdot L/F}(F \cdot L).$$

Hence the restriction of E_T to $D_T \times H^2(G_K, (F \cdot L)_T)$ is given by

$$(D, c) \mapsto [f(D)]$$

where $[f(D)]$ is the inflation of the class of the cocycle $\zeta(\tau^i, \tau^j)$ with

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

and

$$\zeta(\tau^i, \tau^j) = f(D) \text{ if } i + j \geq n.$$

This cocycle is a factor system for a cyclic algebra split by L.

The Brauer Group of C

We would like to extend the pairing E_T to a pairing with $\overline{F}^*$ as domain for the second argument. The idea is to use that for a given finite set S of points on the projective non-singular $\overline{C}$ and a given K-rational divisor D on C we can always find a function $h \in F$ with principal divisor (h) such that $D + (h)$ is prime to S.
Beginning with $c \in H^2(G_K, \overline{F}^*)$ we represent c by a cocycle ζ determined by finitely many functions $f(\sigma, \tau)$ as values. This is possible since because of continuity there is a finite Galois extension L/K such that c is the inflation

of an element $c^0 \in H^2(G(L/K), F \cdot L)$. Let S be the finite set of points on $\overline{C}$ which occur as zeroes of these functions, and take $T = \overline{C} \setminus S$.
Next, for given K-rational divisor D on C we choose a function $h \in F$ such that $D_h := D + (h)$ is, as divisor on C, prime to S. So $D_h \in D_T$ and $E_T(D_h, c)$ is an element in Br(K).
But this element may depend on the choice of h!
The question is: Let $h \in F$ be a function such that the principal divisor (h) is in D_T. Is the class of the cocycle ζ_0 given by

$$\zeta_0(\sigma, \tau) := f(\sigma, \tau)((h)); \sigma, \tau \in G(L)$$

trivial?
We use Weil's reciprocity law and get

$$f(\sigma, \tau)((h)) = h((f(\sigma, \tau))$$

and, since h is invariant under G_K, the class of ζ_0 is trivial if the class of

$$\zeta_1 : G(L/K) \times G(L/K) \to \overline{\mathcal{D}}$$

given by

$$\zeta_1(\sigma, \tau) = (f(\sigma, \tau))$$

in $H^2(G_K, \overline{\mathcal{D}})$ is trivial.

Definition 3.1.1 *The Brauer group* Br(C) *of C is the kernel of the map*

$$\alpha : H^2(G_K, \overline{F}^*) \to H^2(G_K, \overline{\mathcal{D}})$$

induced by sending a function f on $\overline{C}$ to its principal divisor (f).

By the discussion above we see that we can define a pairing from $\mathcal{D} \times$ Br(C) in Br(K) by using appropriate pairings E_T and changing elements in $\mathcal{D}$ by principal divisors. By definition the resulting pairing depends only on the divisor class of the K-rational divisors on C and so get

Proposition 3.1.2 *Let C be a non-singular absolutely irreducible curve over K with divisor class group* Pic(C).
Then the evaluation map induces a pairing

$$E : \text{Pic}(C) \times \text{Br(C)} \to \text{Br(K)}.$$

In many cases one is interested in $\mathrm{Pic}^0(C)$.We observe that the evaluation of a function f at a divisor of degree 0 depends only on (f), and so E induces a pairing, also denoted by E, from $\mathrm{Pic}^0(C) \times \overline{\mathrm{Br}}(C)$ where $\overline{Br}(C)$ is the image of Br(C) in $H^2(G_K, \mathrm{Princ}(\overline{\mathrm{C}}))$ induced by the map $f \mapsto (f)$.

Corollary 3.1.3 *The evaluation pairing induces a pairing*

$$E : \mathrm{Pic}^0(C) \times \overline{\mathrm{Br}}(C) \to \mathrm{Br(K)}.$$

It remains to describe elements in $\overline{\mathrm{Br}}(C)$.
We use the exact G_K-module sequence

$$0 \to \mathrm{Princ}(\overline{\mathrm{C}}) \to \overline{\mathcal{D}}^0 \to \mathrm{Pic}^0(\overline{\mathrm{C}}) \to 0$$

and get (since $H^1(G_K, \overline{\mathcal{D}}^0) = 0$)

$$0 \to H^1(G_K, \mathrm{Pic}^0(\overline{C})) \xrightarrow{\delta^1} H^2(G_K, \mathrm{Princ}(\overline{\mathrm{C}})) \to \mathrm{H}^2(\mathrm{G_K}, \overline{\mathcal{D}}^0))$$

where δ^1 is the connecting homomorphism from $H^1(G_K, \mathrm{Pic}^0(\overline{C}))$ to $H^2(G_K, \mathrm{Princ}(\overline{\mathrm{C}}))$ resulting from cohomology.
It follows that $\overline{\mathrm{Br}}(C) = \delta^1(H^1(G_K, \mathrm{Pic}^0(\overline{C})))$.

Proposition 3.1.4 *Let C be a non-singular absolutely irreducible projective curve.*
The evaluation pairing between points and functions on C induces a pairing

$$T_L : \mathrm{Pic}^0(C) \times H^1(G_K, \mathrm{Pic}^0(\overline{C})) \to \mathrm{Br(K)}.$$

This pairing is called the *Lichtenbaum pairing.*

Explicit Pairing Since for computational purposes it is important to describe the pairing explicit we do this here.
Take $c \in H^1(G_K, \mathrm{Pic}^0(\overline{C}))$, represent it by a cocycle

$$\zeta : G_K \to \mathrm{Pic}^0(\overline{C}) \text{ with } \zeta(\sigma) = \bar{D}(\sigma)$$

and choose

$$D(\sigma) \in \bar{D}(\sigma).$$

The divisor

$$A(\sigma_1, \sigma_2) = \sigma_1(D(\sigma_2)) + D(\sigma_1) - (D(\sigma_1 \cdot \sigma_2))$$

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

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

For $c \in H^1(G_K, \mathrm{Pic}^0(\overline{C}(K_s))$ choose $D_0 := \sum_{P \in \overline{C}(K_s)} z_P \cdot P \in \bar{D}_0 \in \mathrm{Pic}^0(C)$ such that $\delta^1(c)$ is presented by a cocycle $(f(\sigma_1, \sigma_2))$ prime to D_0.
Then $T_L(\bar{D}_0, c)$ is the cohomology class of the cocycle

$$\zeta(\sigma_1, \sigma_2) = \sum_{P \in \overline{C}(K_s)} f(\sigma_1, \sigma_2)(P)^{z_P}$$

in $H^2(G_K, K_s^*) = \mathrm{Br(K)}$.

Example

We give the analogue of Example 3.1.1 for the Lichtenbaum pairing.

Example 3.1.5 *Let L/K be cyclic of degree n and $G(L/K) =< \tau >$.*
By $\mathrm{Pic}^0(C_L)$ we denote the divisor class group of degree 0 of $C \times L$.
Let ζ be a 1-cocycle from $< \tau >$ into $\mathrm{Pic}^0(C_L)$ representing the cohomology class $c \in H^1(G(L/K), \mathrm{Pic}^0(C_L))$.
ζ is determined by the value $\zeta(\tau) =: z$ since the cocycle condition implies that $\zeta(\tau^j) = \sum_{i=0}^{j-1} \tau^i z$ for $1 \leq j \leq n$. In particular,we get

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

Choose a divisor $D \in z$ and $D(\tau^j) := \sum_{i=0}^{j-1} \tau^i D$. Then

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

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

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

and

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

Next choose in the divisor class $\bar{D}_0 \in \mathrm{Pic}^0(C)$ *a divisor* D_0 *with* $D_0 = \sum_{P \in \overline{C}(K_s)} z_P \cdot P$ *prime to the set of zeroes and poles of* f_D.
Then $T_L(\bar{D}_0, c) \in H^2(G(L/K), L^*)$ *is presented by the cocycle*

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

and

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

This is a cocycle defining a cyclic algebra with center K *and splitting field* L.

Comparison Theorem

We have defined two pairings attached to Jacobian varieties, namely the Tate pairing T_n which uses crucially the Weil pairing on torsion points of the Jacobian of order n, and the Lichtenbaum pairing T_L which uses evaluation of functions on the curve. A priori, no number n appears in the latter pairing but we can look at it modulo n and get for all natural numbers prime to $\mathrm{char}(K)$

$$T_{L,n} : \mathrm{Pic}^0(C)/n \cdot Pic^0(C) \times H^1(G_K, \mathrm{Pic}^0(\overline{C}))[n] \to \mathrm{Br(K)[n]}.$$

Lichtenbaum proves in [18]

Theorem 3.1.6 *Up to a sign, the pairing* $T_{L,n}$ *is equal to* T_n.

We shall call $T_{L,n}$ the Lichtenbaum-Tate pairing. For most purposes its interpretation by evaluation of functions on C is used.

3.1.2 The Non-complete Case

We can use Theorem 3.1.6 to see what is happening if T_∞ is not equal to $\{P_\infty\}$ but contains more elements.
In Subsection 3.0.4 we have found the exact sequence

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

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

To overcome these difficulties we look at the sequence

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

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

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

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

Lemma 3.1.7 *The group $\varphi(J_C(K))$ is orthogonal to the image of $H^1(G_K, \mathcal{C}'_{T_\infty})$ in $H^1(G_K, A(K_s))[n]$ under the Tate pairing.*

Corollary 3.1.8 *The Lichtenbaum pairing induces a pairing, also denoted by T_L from* $\mathrm{Pic}(\tilde{O})/n\mathrm{Pic}(\tilde{O}) \times \psi^1(H^1(G_K, \mathrm{Pic}(\overline{\tilde{O}})))[n]$ *to* $\mathrm{Br(K)[n]}$.

To come to the most general situation we have to do the last step and to allow singularities in the set S.

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

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

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

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

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

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

as well as

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

We can apply δ^1 to $H^1(G_K, \mathrm{Pic}(O))$ and we get a pairing as above but we cannot expect to get any information about $T_S(K)$. We shall show in the next subsection how one can overcome this difficulty in the case which is relevant for cryptography, namely that the ground field K is equal to a finite field $\mathbb{F}_q$.
A first trivial observation is that in this case all occurring Galois modules are torsion modules. We are interested in elements of order dividing n in $\mathrm{Pic}(O)$, which is, since this is a finite group, isomorphic to $\mathrm{Pic}(O)/n \cdot \mathrm{Pic}(O)$ which fits better into our frame. We want to apply the duality theorem 2.3.1 from Subsection 2.3.1. For this, it is convenient to work over local fields instead over finite fields. Moreover we shall see that the geometric situation can be made simpler.

3.1.3 p-adic Lifting

Assume that O is the ring of holomorphic functions of an affine curve C_O defined over $\mathbb{F}_q$ with corresponding projective curve C of genus g_0. We assume that C_O has only one singular point with square free conductor. Let S be the set of points on C corresponding to the singular point.
Let K be a local field with residue field $\mathbb{F}_q$.
We can lift C_O to an affine *non-singular* curve C_O^l defined over K embedded

in the projective curve C^l which is a lift of C such that all relevant data are preserved.
In particular, for n prime to q,

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

is canonically isomorphic to $\mathrm{Pic}(O)/[n]\mathrm{Pic}(O)$, the genus of C^l is

$$g_0 + \mid S \mid -1$$

and there exists a torus T_S/K of dimension $\mid S \mid -1$ and an exact sequence

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

with U_K the units of K.

Instead of a proof I give an example.

Example 3.1.9 *Take*

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

Then $T_\infty = \{(0,1,0)\}$, *the singular point* $(0,0)$ *corresponds to two points on the desingularization and* $\mathrm{Pic}(O) \cong \mathbb{F}_q^*$.
Take $K = \mathcal{W}(\mathbb{F}_q)$ *as field of Witt vectors over* $\mathbb{F}_q$ *and choose* $\pi \in K$ *with* $w_{\mathfrak{p}}(\pi) = 1$.
Then

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

is a Tate elliptic curve with

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

Chapter 4

Bilinear Structure on Class Groups

4.1 The Lichtenbaum-Tate Pairing over Local Fields

Motivated by the results of the last chapter we assume now that C_O is an affine curve *without singularities* defined over a local field K with residue field $\mathbb{F}_q$. By K_{nr} we denote the maximal unramified extension of K. The normalized valuation on K is denoted by $w_{\mathfrak{p}}$.
As always we assume that n is prime to q.
The fundamental result following from the local duality theorem is worthwhile to be stated again.

Theorem 4.1.1 ***(Lichtenbaum-Tate)*** *Let K be a local field, C_O an affine regular curve over K with ring of holomorphic functions O.*
For every natural number n the Lichtenbaum-Tate pairing

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

is non-degenerate.

As already said the group $\mathrm{Pic}(O)/n\mathrm{Pic}(O)$ is isomorphic to $\mathrm{Pic}(O)[n]$ and so in the center of our interest.

This motivates to discuss the other groups occurring in the Lichtenbaum-Tate pairing both from the theoretical and algorithmic point of view.

4.1.1 $H^1(G_K, \mathrm{Pic}(\overline{O}))[n]$

We assume (and this is so for all cryptographically interesting cases cf.[9]) that we can replace $\mathrm{Pic}(\overline{O})$ by $\mathcal{A}(K_s)$ where $\mathcal{A}$ is an abelian variety defined over K and isogenous to J_C.
$\mathcal{A}$ extends to a group scheme over O_K, its Néron model.
As always we assume that n is prime to q and to simplify the situation we assume in the whole section in addition that n is prime to the number of connected components of the special fiber of $\mathcal{A}$[1].
It follows that

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

Via restriction we embed $H^1(G_K, \mathrm{Pic}(\overline{O}))$ into $H^1(G_{K_{nr}}, \mathrm{Pic}(\overline{O}))$, and the image is equal in the subgroup of elements which are ϕ_q-invariant (ϕ_q acts by conjugation on $G_{K_{nr}}$). Let L_n be the unique extension of K_{nr} of degree n which is totally ramified. It is equal to $K_{nr}(\pi^{1/n})$ where π is a uniformizing element of K.
So $G(L_n/K_{nr}) =< \tau_n >$ with $\tau_n(\pi^{1/n}) = \zeta_n \cdot \pi^{1/n}$ for an n-th root of unity ζ_n. The Frobenius automorphism ϕ_q acts by conjugation on τ sending τ to τ^q since q is the value of the cyclotomic character applied to ϕ_q.
These datas are sufficient to describe $H^1(G_K, Pic(\overline{O}))[n]$ in all concrete cases. Here are two examples. First assume that J_C and hence $\mathcal{A}$ has good reduction. In this case $\mathcal{A}[n] := \mathcal{A}(K_s)[n] = \mathcal{A}(L_n)[n] = \mathcal{A}(K_{nr})[n]$ and hence

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

Definition 4.1.2 *Let* $\mathrm{Pic}(O)[n]^{(q)}$ *be the subgroup in* $\mathrm{Pic}(\overline{O})[n]$ *consisting of elements* c *with* $\phi_q(c) = q \cdot c$.

Proposition 4.1.3 *Assume that* O *is the ring of holomorphic functions of a regular affine curve with good reduction. Let* n *be prime to* q.
Then $H^1(G_K, Pic(\overline{O}))[n]$ *is isomorphic to* $\mathrm{Hom}(< \tau >, \mathrm{Pic}(O)[n]^{(q)})$, *and so, non-canonically since depending on the choice of* τ, *to* $\mathrm{Pic}(O)[n]^{(q)}$.

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

Corollary 4.1.4 i) *If $\zeta_n \in K$ then $H^1(G_K, Pic(\overline{O}))[n]$ is isomorphic to* $\mathrm{Pic}(O)[n]$.

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

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

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

with $w_{\mathfrak{p}}(Q) = m \in \mathbb{N}$.
Since only one point is missing we get that $\mathrm{Pic}(\overline{O})$ is Galois isomorphic to $E_Q(K_s)$.
We assume that n is prime to m. Then $E_Q(K)$ contains elements of order n iff $\zeta_n \in K$, and hence by duality

$$H^1(G_K, E_Q(K_s))[n] \neq 0 \text{ iff } \zeta_n \in K,$$

and in this case it is cyclic of order n.
So we assume that $\zeta_n \in K$.
We take a special cyclic extension of degree n, namely $L_Q := K(Q^{1/n})$. By Tate's theory this field is equal to $K(E_Q[n])$.

Proposition 4.1.5 *Let τ be a generator of $G(L_Q/K)$, let $P \in E_Q[n]$ be any point of order n which is not K-rational, and let ζ be the cocycle from $< \tau >$ to $E_Q[n]$ determined by $\zeta(\tau) = P$.*
Then $H^1(G_K, E_Q(K_s))[n]$ is cyclic of order n and generated by the class of ζ.

4.1.2 The Local Brauer Group

Cyclic Algebras

For the moment let K be any field of characteristic prime to n.
The elements in the Brauer group Br(K) of K can be identified with classes of central simple algebras with center K. The group composition is the tensor product, and the trivial class consists of all algebras which are isomorphic to full matrix algebras over K.

Because of Hilbert's theorem 90 one sees that for Galois extensions L/K the inflation map from $H^2(G(L/K), L^*)$ to Br(K) is injective.
For any L/K the restriction map from Br(K) to Br(L) corresponds to base field extension applied to algebras, and its kernel consists of the classes of algebras which become, after tensoring with L, isomorphic to full matrix algebras. In this case L is called a splitting field of K. We have been confronted at different places with the special case that L/K is cyclic of degree n, for instance in Example 3.1.5 as result of the Lichtenbaum-Tate pairing.
In this case $H^2(G(L/K), L^*)$ consists of classes of *cyclic* algebras with 2-cocycles given in the following way:
Let σ is a generator of $G(L/K)$ and take a in K^*.
The map $f_{\sigma,a} : G \times G \to L^*$, given by

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

The cocycles $f_{\sigma,a}$ and $f_{\sigma,a'}$ are in the same cohomology class if and only if $a \cdot a'^{-1} \in N_{L/K}L^*$. We denote the corresponding class of cyclic algebras by $(L, \sigma, a \cdot N_{L/K}L^*)$.

Invariants

Now we return to the case that K is a local field with residue field $\mathbb{F}_q$ and that n is prime to q.
Because of the local duality theorem we know already that Br(K)[n] $\cong \mathbb{Z}/n$.

The unramified case: the invariant Let L_u be the unique unramified extension of K of degree n. It is cyclic.
$G(L_u/K)$ has as canonical generator a lift of the Frobenius automorphism ϕ_q of $\mathbb{F}_q$.
We represent elements $c \in H^2(G(L_u/K), L_u^*)$ by a triple

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

Since

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

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

Definition 4.1.6 *$w_{\mathfrak{p}}(a) \in \mathbb{Z}/n\mathbb{Z}$ is the* invariant $\mathrm{inv_K(c)}$ *of c.*

The general case: the invariant From the paragraph it follows that

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

Definition 4.1.7 *The map*

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

is defined as follows:
For $c \in \mathrm{Br(K)[n]}$ take $c_0 \in H^2(G(L_u/K), L_u^*)$ with $\inf_{L_u/K_s}(c_0) = c$ and represent c_0 by the triple $(L_u, \phi_q, a \cdot N_{L_u/K}(L_u^*))$.
Then $\mathrm{inv_K(c) := w_{\mathfrak{p}}(a) \mod n}$ *is well defined and determines c uniquely.*

Though the invariant is defined in a seemingly very explicit way for cyclic algebras split by unramified extensions it may be difficult to compute it even in this case. To see this assume that τ is another generator of $G(L_u/K)$ and the cyclic algebra representing c is given by the triple $(L_u, \tau, a \cdot N_{L_u/K}(L_u^*))$. We know that there exists $k \in \mathbb{Z}$ with $\tau^k = \phi_q$. Then $\mathrm{inv_K(c) = k \cdot w_{\mathfrak{p}}(a)}$ mod n.
So we have to determine k, and this is a discrete logarithm problem.

The Tamely Ramified Case

The relation to Discrete Logarithms in finite fields becomes even more evident in the ramified case.
Let L_n a totally ramified Galois extension of degree n of K. It follows that L_n/K is cyclic and that $\mu_n \subset K$. Let τ be a fixed generator of $G(L_n/K)$. Since

$$K^*/N_{L_n/K}(L^*) \cong \mathbb{F}_q^*/\mathbb{F}_q^{*n}$$

the element $c \in H^2(G(L_n/K), L_n^*)$ is determined by the triple

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

Proposition 4.1.8 *For* $a_1, a_2 \in \mathbb{F}_q$

$$a_1^k \equiv a_2 \mod \mathbb{F}_q^{*n}$$

iff

$$k \cdot (\mathrm{inv_K}((\mathrm{L_n}, \tau, \mathrm{a_1} \cdot \mathbb{F}_\mathrm{q}^{*\mathrm{n}}))) \equiv \mathrm{inv}((\mathrm{L_n}, \tau, \mathrm{a_2} \cdot \mathbb{F}_\mathrm{q}^{*\mathrm{n}}))\ \textit{modulo}\ \mathrm{n}.$$

Hence the computation of Discrete Logarithms in $\mathbb{F}_q^*$ *is equivalent with the computation of invariants of cyclic algebras.*

The Frobenius Case

The most important case for applications is that $c \in \mathrm{Br(K)}$ is represented as algebra split by an extension L of K which is totally ramified of degree n and which becomes Galois only after adjoining the n-th roots of unity. This is exactly the situations which occurs when one applies the Lichtenbaum-Tate pairing.
A description useful for algorithmic purposes is, at the moment, only available if one restricts c to $K(\zeta_n)$ and then uses the results obtained for cyclic ramified extensions over $K(\zeta_n)$ instead of K. Hence one has to pass to a field which will be, in general, much larger than K!
It is a challenge to do better.

4.1.3 Algorithmic Description of the Lichtenbaum-Tate Pairing

The Pairing over Local Fields

We continue to assume that K is a local field with residue field $\mathbb{F}_q$.
To make the situation not too complicated we discuss as example the case that the curve C has good reduction (hence is the lift of a nonsingular curve C_0 over $\mathbb{F}_q$) and that only one point "at infinity" is missing on C_O. So we have a non-degenerate pairing

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

Let k be the smallest number with $q^k \equiv 1 \mod n$. k is called the "embedding degree".
Define $K(\zeta_n) := K_n$. It is a local field with residue field $\mathbb{F}_{q^k}$.
We choose a uniformizing element $\pi \in K$ define $L := K_n(\pi^{1/n})$ and take τ as generator of $G(L/K_n)$.
As seen in Subsection 4.1.1 we can identify $H^1(G_K, J_C(K_n))[n]$ with group of homomorphisms

$$\{\varphi \in \mathrm{Hom}(G_K, J_C(K_n)[n]) \text{ with } \varphi(\tau) = P \text{ and } \phi_q(P) = q \circ P\}.$$

We use the explicit description of the Lichtenbaum pairing given in Example 3.1.5.
Take $c \in H^1(G_K, J_C(K_s))$ corresponding to φ with $\varphi(\tau) = P$ and $n \cdot P = (f_P)$.
Take $Q \in \overline{Q} \in J_C(K)$ such that $f_P(Q)$ is defined.
Then $T_{L,n}(\overline{Q}, c)$ is the class of cyclic algebra $(L, \tau, f_P(Q) \cdot N_{L/K_n}(L^*))$.
Hence we get a non-degenerate pairing

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

by the evaluation *modulo* $\mathfrak{p}$ of the functions f_P with $(f_P) = n \cdot P$ and $P \in J_C(K_s)[n]^{(q)}$ on $J_C(K)$.

4.1.4 The Pairing over Finite Fields

Now begin with a curve C_O defined over $\mathbb{F}_q$. Since we evaluate functions on a p-adic lift C^l of C_O *modulo the maximal ideal* $\mathfrak{p} \subset O_K$ we get an explicit

description of the Lichtenbaum-Tate pairing in the case of good reduction which only uses objects attached to the curve C_O. Using Corollary 3.1.8 we can generalize and get

Theorem 4.1.9 *Assume that C_O is an affine curve with one singular point over $\mathbb{F}_q$ whose conductor is square free. Let O be the ring of holomorphic functions O. Take n prime to q (and satisfying some "innocent" extra conditions).*
Then we get a non-degenerate pairing

$$T_n : \mathrm{Pic}(O)/n \cdot \mathrm{Pic}(O) \times J_{C^l}(K_s)[n]^{(q)} \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n$$

which is given by the evaluation modulo $\mathfrak{p}$ of a function f_P with $(f_P) = n \cdot P$ and $P \in J_{C^l}(K_s)[n]^{(q)}$ on $\mathrm{Pic}(O)$. If C_O is regular P and f_P can be replaced by their reduction modulo $\mathfrak{p}$, i.e by points and functions over $\mathbb{F}_q$, and we get a pairing

$$T_{n,0} : \mathrm{Pic}(O)/n \cdot \mathrm{Pic}(O) \times J_C(\mathbb{F}_{q_s})[n]^{(q)} \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n.$$

4.1.5 Evaluation

To get a bilinear structure on class groups of rings of holomorphic functions on curves over $\mathbb{F}_q$ there is a last step to be done. One has to show that the computation of the pairing is fast.

As we have seen in Subsection 4.1.4 one has to evaluate a function f_P contained in the function field $F \cdot \mathbb{F}_{q^k}$ at a divisor D on C defined over $\mathbb{F}_q$ to compute T_n.
A naive approach is, because of the high degrees needed in practice, not possible. The way to reduce the problem to a square-and-multiply algorithm in a group was found by *V. Miller* for elliptic curves (applied to the Weil pairing). The general method uses as background the theory of Mumford's Theta groups which describe extensions of (finite subgroups of) abelian varieties by linear groups.
The basic step for the computation is:
For given positive divisors A_1, A_2 of degree g find a positive divisor A_3 of degree g and a function h on C such that

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

Define the following *group law* on $\langle c\rangle \times K^*$: We begin with a divisor class c in $J_C(K_s)[n]$ and choose divisors $A_k \in k \circ c$. We assume that D is a K-rational divisor of degree O prime to all A_i. (In fact one can weaken this condition). Define

$$(i \cdot c, a_1) \circ (j \cdot c, a_2) := ((i+j) \cdot c, a_1 a_2 \cdot h_{i,j}(E)),$$

with $A_i + A_j - A_{i+j} - gP_0 = (h_{i,j})$. The assumptions on D guarantee that each $h_{i,j}(D) \in K^*$. The degree of $h_{i,j}$ is at most g. It can be easily seen by induction that $l \cdot (c,1) = (lc, h_{l-1}(D))$ where h_{l-1} is a function on C satisfying $lA - A_{l-1} - (l-1)gP_0 = h_{l-1}$. Hence the n-fold application gives the result $(0, f(D))$, where f is a function on C with $(f) = nA_1$.

Now we can use the group structure on $\langle c\rangle \times K^*$ and apply the square- and multiply algorithm to evaluate f at E in $O(\log(n))$ basic steps.

Corollary 4.1.10 *The Tate- Lichtenbaum pairing $e_{T,n}$ can be computed in $O(\log(n))$ basic steps over $\mathbb{F}_{q^k}$.*

CONSEQUENCE:
We can reduce the discrete logarithm in $J_C(K)/nJ_C(K)$ to the discrete logarithm in $Br(K)_n$ with the costs $O(log(\mid \mathbb{F}_{q^k}) \mid)$.

This result is of practical importance only if k is small. In general, the conditions that $\mathbb{F}_q$, contains ℓ-th roots of unity *and* that Pic^0_C has elements of order ℓ rational over $\mathbb{F}_q$ with ℓ in a cryptographically interesting range will not be satisfied at the same time.
Let $\chi(\phi_q)_C(T)$ be the characteristic polynomial of ϕ_q. Its zeroes $(\lambda_1, \ldots, \lambda_{2g})$ are integers in a number field K and they can and will be ordered such that $\lambda_i \lambda_{g+i} = q$ for $1 \le i \le g$.
Now assume that $\mathbb{F}_q$ contains ℓ-th roots of unity and so $q \equiv 1 \bmod \ell$. Then

$$(1-\lambda_i)(1-\lambda_{g+i}) \equiv 2 - (\lambda_i + \lambda_{i+g}) \bmod \ell.$$

So Pic^0_C has elements of order ℓ if and only if there is an eigenvalue λ_i of ϕ_q such that a prime ideal of K dividing (ℓ) divides *simultaneously* $(1-\lambda_i)$ and $(1-\lambda_{i+g})$.

For elliptic curves this yields

Proposition 4.1.11 *Let E be an elliptic curve defined over $\mathbb{F}_q$ and ℓ a prime such that ℓ divides $|E(\mathbb{F}_q)|$. Let ϕ_q be the Frobenius endomorphism acting on $E[\ell]$. The corresponding discrete logarithm in $E(\mathbb{F}_q)[\ell]$ can be reduced to the discrete logarithm in $\mathbb{F}^*_{q^k}[\ell]$ by the use of the Tate-Lichtenbaum pairing if and only if the characteristic polynomial of ϕ_q^k on E is congruent to $T^2 - q^k$ modulo ℓ.*

Avoiding elliptic curves with small k is easy. For randomly chosen elliptic curves k we can expect that k will be large.
But there is an important class of special elliptic curves for which k is always small: the *supersingular elliptic curves*. The crucial facts one uses are that the characteristic p of $\mathbb{F}_q$ divides the trace of the Frobenius acting on supersingular elliptic curves E and that their absolute invariant j_E lies either in $\mathbb{F}_p$ or in $\mathbb{F}_{p^2}$.

Let us discuss the easiest case in detail. We assume that $p > 3$ and $j_E \in \mathbb{F}_p$. Let E_0 be an elliptic curve defined over $\mathbb{F}_p$ with invariant j_E. Let $T^2 - aT + p$ be the characteristic polynomial of ϕ_p on E_0. One knows that $a = \lambda \cdot p$ with $\Lambda \in \mathbb{Z}$. By the estimate

$$|1 - \lambda \cdot p + p| \leq 2\sqrt{p} + (p+1) \text{ with } \lambda \in \mathbb{Z}$$

we get that $\lambda = 0$. Hence the eigenvalues λ_1, λ_2 of ϕ_p acting on E_0 satisfy

$$\lambda_1 = -\lambda_2 \text{ and } \lambda_1 \cdot \lambda_2 = p$$

and so $\lambda_i = \pm\sqrt{-p}$.
Assume now that $q = p^d$. Since E becomes isomorphic to E_0 over $\mathbb{F}_{q^2}$ the characteristic polynomial $\chi(\phi_{q^2}(T)$ of the Frobenius endomorphism on E over $\mathbb{F}_{q^2}$ is equal to

$$T^2 - (\lambda_1^{2d} + \lambda_2^{2d}) + q^2 = T^2 - 2\lambda_1^{2d} + \lambda_1^{4d})^2 = (T - \lambda_1^{2d})^2.$$

Since, by assumption, $E(\mathbb{F}_q)$ has elements of order ℓ we get that ℓ divides $(1 - \lambda_1^{2d})$.
Since $\lambda_1^2 = -\lambda_1 \cdot \lambda_2 = -p$ it follows that ℓ divides $1 - (-p)^d$. But this implies that $k = 1$ if d is even, and $k = 2$ if d is odd.

The other cases can be treated by similar considerations. As result we get

Proposition 4.1.12 *Let E be a supersingular curve over $\mathbb{F}_q$ with $q = p^d$. Assume that E has a $\mathbb{F}_q$-rational point of order ℓ.*
Let k be the smallest natural number such that $\ell | q^k - 1$.
Then $k \leq 6$.
If $j_E \in \mathbb{F}_p$ and $p > 3$ then $k \leq 2$.
If $p = 2$ then $k \leq 4$.

In general one has the

Theorem 4.1.13 *Let A be a supersingular abelian variety of dimension g over $\mathbb{F}_q$, then there exists an integer $k(g)$ such that, for all natural numbers r, the degree k is bounded by $k(g)$.*

One finds the number $k(g)$ in papers of S. Galbraith.

It is easy to implement the algorithm, and one can find it at many places including various tricks which speed up the pairing.
For the constructive applications it is necessary to have an embedding degree $\sim 12 \cdot g$. It is a very nice problem in computational number theory to find such k. For elliptic curves the situation is not so bad. But for $g > 1$ not much is known if J_C is not supersingular.
A successful approach to this problem could be interesting since one can speed up the computation of T_n by a factor g in interesting protocols.

4.1.6 Acceleration for Genus > 1

Let C be a (hyperelliptic) curve of genus g defined over $\mathbb{F}_q$ with a rational Weierstraß point which we take as point P_∞ at infinity. Let O be the ring of holomorphic functions on $C_O := C \setminus \{P_\infty\}$.
We recall that the addition law on

$$\mathrm{Pic}(O) \times \mathbb{F}_{q^k}$$

can be computed by Cantor's algorithm, or, more efficiently for $g \leq 4$, by explicit formulas.
There is a special subset in $\mathrm{Pic}(O) \times \mathbb{F}_{q^k}$ corresponding to points $P \in C_O(\mathbb{F}_{q^k})$.

It is well known that the additions of two ideal classes is considerably faster if one of the summands is in $C_O(\mathbb{F}_{q^k})$.

We look at the following situation which is desirable for cryptographic use. Assume that $n = \ell$ a prime number which does not divide q, and that there are exactly $\ell - 1$ elements of order ℓ in $\mathrm{Pic}(O)$.
Let k be as above, minimal with

$$\ell \mid q^k - 1.$$

For many cryptographic applications one needs a point $P \in \mathrm{Pic}(O)[\ell]$ and a point $Q \in \mathrm{Pic}(O \times \mathbb{F}_{q^k})$ with

$$T_\ell(Q, P) \neq 1.$$

Proposition 4.1.14 *(For q large enough we have:) For any random point $Q \in C(\mathbb{F}_{q^k})$ we get*

$$T_\ell(Q, P) \neq 1.$$

The proof and applications are given in [11].

Choosing Q according to the proposition will reduce the evaluation of the pairing by a factor g, and since for k large enough this evaluation is rather expensive it is worthwhile to do so.

Chapter 5

Globalization of Brauer Groups

In the previous chapter we have seen that DL-problems related with class groups of curves over $\mathbb{F}_q$ are, at least in principle, related with the computation of invariants of elements in the Brauer groups of local fields, and Proposition 4.1.8 states that this computation is equivalent with the computation with the classical Discrete Logarithm in finite fields. We try to go further by interpreting the local field as completion of a global field. The key tools for this are delivered by the global duality theorem and its consequences, in particular the Hasse-Brauer-Noether sequence for Brauer groups which we recall:

Theorem 5.0.15 *Let K be a global field and $n \in \mathbb{N}$ odd and prime to $char(K)$.*

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

is exact.

5.1 Reciprocity Laws

We use the sequence of Hasse-Brauer-Noether.

Proposition 5.1.1 *Assume that we have a curve C_O defined over K with properties as above.*
Take $c \in \mathrm{Pic}(O)$ and $\varphi \in H^1(G_K, \mathrm{Pic}(\overline{O}))[n]$ with localizations $c_\mathfrak{p}$ respectively $\varphi_\mathfrak{p}$.
Then

$$\sum_{\mathfrak{p} \in \Sigma_K} inv_\mathfrak{p}(T_{L,n}(c, \varphi)) = 0.$$

Hence we have relations between local discrete logarithms modulo different places both on abelian varieties, e.g. elliptic curves, and in the multiplicative group.

The hope is that by these reciprocity laws we can compute discrete logarithms in geometrically defined groups A_q defined over $\mathbb{F}_q$ by first lifting them to groups $A_\mathfrak{p}$ over a local field $K_\mathfrak{p}$ with residue field $\mathbb{F}_q$, then lifting further to a global field K and finally passing to other places $\{\mathfrak{p}'\} \subset \Sigma_K$ where this computation is easier.
To realize this idea we have to find global geometric objects over K with given reduction modulo $\mathfrak{p}$ which are arithmetically accessible. And then we need "enough" test functions φ to exploit Proposition 5.1.1. This leads to hard problems in global number theory, and in the moment it is totally open whether anything useful will come out of this approach for abelian varieties.
The situation is much better if we look at the classical Discrete Logarithm in the multiplicative group of $\mathbb{F}_q$. Our global geometric object is the algebraic group G_m, and we are working with the duality theorem 2.3.1 with $p = q = 1$ (i.e. we use evaluation pairings with Dirichlet characters).
This approach is taken in the paper of Huang and Raskind in [15]. In the light of their results a realistic hope is that one can shift the computation of discrete logarithms in roots of unity of order n in arbitrary fields $\mathbb{F}_q$ with $n \mid q-1$ to fields $\mathbb{F}_{q'}$ with q' not much larger than n.
Here we give an obvious result.

Proposition 5.1.2 *Let $\mathfrak{m}$ be a divisor of K. We* assume *that there is a cyclic extension L of odd degree n of K which is unramified outside of the set $T_\mathfrak{m}$ of places in the support of $\mathfrak{m}$.*
Let τ be a generator of $G(L/K)$. For $\mathfrak{p} \notin T_\mathfrak{m}$ let $\phi_\mathfrak{p}$ be a Frobenius automorphism at $\mathfrak{p}$ in $G(L/K)$. By $f_\mathfrak{p}$ we denote a number for which $\tau^{f_\mathfrak{p}} = \phi_\mathfrak{p}$ holds.

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

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

where $w_{\mathfrak{p}}$ is the normalized valuation in $\mathfrak{p}$ and A is the cyclic algebra $(L, \tau, a \cdot N_{L/K}(L^*))$.

5.1.1 Application

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

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

and

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

5.1.2 Index-Calculus in Global Brauer Groups

Motivated by Proposition 5.1.2 we search for (heuristic) algorithms to determine the numbers $f_{\mathfrak{p}}$ which characterize the Frobenius automorphisms at places $\mathfrak{p}$ of K related to cyclic extensions with conductor dividing an ideal $\mathfrak{m}$.
A possible method to do this (with subexponential complexity) is an index-calculus algorithm of the type one is used to see in factorization algorithms.
A possible method to do this (with subexponential complexity) is an index-calculus algorithm of the type one is used to see in factorization algorithms.

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

The equations in Proposition 5.1.2 can be seen as a system of linear equations relating the indeterminates f_p for p prime to m and $\mathrm{inv_p(A)}$ for $p \mid m$. The basic task is to compute f_p and for this we use cyclic algebras with trivial invariants at primes dividing m.
At the other primes we want to have $w_p(a) \neq 0$ in a certain distinguished set which is on the one hand big enough such that many elements a satisfying the local conditions can be found, and which is on the other hand not small enough to make linear algebra feasible.

5.1.3 Smooth Numbers

The key concept is the notion of smooth numbers.
Let B be a natural number.

Definition 5.1.3 *A number $n \in \mathbb{N}$ is B-smooth if all prime numbers dividing n are bounded by B.*

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

Theorem 5.1.4 *(Theorem of Canfield-Erdös-Pomerance)*
Let x, y be natural numbers which grow asymptotically such that (for some fixed $\epsilon \in]0,1[$) we have

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

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

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

asymptotically for $x \to \infty$.

Example 5.1.5 *Assume that* $y = L_x(1/2, c)$. *Then*

$$\psi(x, y)/x \sim L_x(1/2, -1/2c).$$

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

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

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

Take $K = \mathbb{Q}$. We use the notation and assumptions of Proposition 5.1.2. The congruence in this proposition can be seen as solution of a system of linear equations relating the variables f_p for p prime to m and $\mathrm{inv_p(A)}$ for $p \mid m$. Note that the system is solvable modulo n since a cyclic extension unramified outside of m exists by assumption.
Let d be the smallest natural number $\geq \sqrt{m}$.
For small δ take $a_1(\delta) := d + \delta$, $a_2(\delta) := c_0 + 2\delta \cdot d + \delta^2$ with $c_0 = d^2 - m$.
Then at primes dividing m the invariants of the cyclic algebras attached to a_1^2 and a_2 are equal, and so for primes p prime to m the corresponding numbers f_p are solutions modulo n of the equations

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

We want to get equations with coefficients equal to 0 for $p > B$ for a certain convenient bound B[1], i.e. the numbers a_1 and a_2 have to be B-smooth. Let S be the number of primes $\leq B$.
Now choose a relatively small number L and search $\delta \leq L$ (using sieves) yielding such smooth pairs $(a_1(\delta), a_2(\delta))$.
Assume that we have found a system $\mathcal{L}$ of S $\mathbb{Z}$-independent equations.

Proposition 5.1.6 *$det(\mathcal{L})$ is a multiple of $\varphi(m)$.*

[1] B has to be large enough so that we can expect that not all primes $\leq p$ are split in L

In general this multiple will be rather big.
In a master thesis in Essen (2006) A. Timofeev did many experiments.
The nice result was that after applying the algorithm twice in all experiments the gcd of the two determinants was equal to $\varphi(m)$.

5.1.5 A Variant: Relations Arising from Quadratic Fields

We are interested in cyclic extensions L of odd degree ℓ with conductor m over $\mathbb{Q}$ and generator τ of $G(L/\mathbb{Q})$. The composite of such an extension with a quadratic extension field K of $\mathbb{Q}$ has the same properties. So we can use cyclic algebras over K given by a pair $A = (\tau, c)$ with $c \in K^*$. For places $\mathfrak{p} \in \Sigma_K$ we have numbers $f_\mathfrak{p}$ such that $\tau^{f_p} = \phi_\mathfrak{p}$. If $p \in \mathfrak{p}$ is inert in K then $f_\mathfrak{p} = 2f_p$. Else we get $f_p = f_\mathfrak{p}$ for $p \in \mathfrak{p}$.
We need that the sum of the invariants of A taken over all places dividing m is zero. This is certainly the case if c is prime to m and if the norm of c is congruent to 1 modulo m. If we assume that all primes dividing m are split in K and that the class number of K is prime to ℓ we get that there is an extension cyclic of degree ℓ and unramified outside of m if and only $\ell \mid \varphi(m)$. So we can use relations by cyclic algebras over K for our system of equations of the type described in Proposition 5.1.2.
We choose $\epsilon \in \mathbb{N}$ and $d \in \mathbb{Z}$ such that d is not a square, d is prime to ϵ and $d \equiv \epsilon^2 \bmod m$. To simplify matters we shall assume that ϵ is odd and d even. We denote by K_d the field $\mathbb{Q}(\sqrt{d})$.
We take $u \in \mathbb{Z}$ with $\gcd(\epsilon d, 1 - u^4) = 1$. (This implies that u is even.)
The element

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

has norm

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

and so we get

$$\sum_{\mathfrak{p}\in\Sigma_K} w_\mathfrak{p}(\epsilon(1+u^2) + (1-u^2)\sqrt{d}) f_\mathfrak{p}$$

$$\equiv \sum_{\mathfrak{p}\in\Sigma_K} w_\mathfrak{p}(2\epsilon u) f_\mathfrak{p} \mod \ell.$$

Some computations yield:

$$\sum_{p\in\mathbb{P};\ p\ split\ in\ K_d} w_p(\epsilon^2(1+u^2)^2-(1-u^2)^2d)f_p$$
$$-\sum_{p\in\mathbb{P};\ p\ split\ in\ K_d} w_p(2\epsilon u)f_p$$
$$\equiv 0 \mod \ell.$$

Assume that both ϵu and

$$\epsilon^2(1+u^2)^2-(1-u^2)^2d$$

are B-smooth. Then we have found an equation of the wanted form.

5.2 Construction of Elements in the Brauer Group of Global Fields

Motivated by the reciprocity laws and index-calculus, we are looking for more methods to construct elements in the Brauer group of global fields. The theoretical background for the success (or failure) is the duality theorem of Tate-Poitou. We can try to use

- Pairings with Dirichlet Characters [15]
- Pairings with Principal Homogenous Spaces with abelian varieties instead of using the multiplicative group. The arithmetic of abelian varieties predicts that this is much more difficult than using characters. Perhaps Euler systems attached to Heegner points could be interesting sources.
- As variant one could study Cassel's Pairing using Tate-Shafarevich groups and ending in the second cohomology group of the idele class group which is in fact the right global object from the point of view of class field theory.
- Instead of Brauer groups of curves one could try to use Brauer groups of higher dimensional varieties. Interesting beginnings for this can be found in [17].

Bibliography

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

[2] P. S. L. M. Barreto, B. Lynn, and M. Scott. *Constructing elliptic curves with prescribed embedding degrees*. In Security in Communication Networks – SCN 2002, volume 2576 of Lecture Notes in Comput. Sci., pages 257–267. Springer-Verlag, Berlin, 2003.

[3] P. S. L. M. Barreto and M. Naehrig. *Pairing-friendly elliptic curves of prime order*. preprint, 2005.

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

[5] D. Boneh, B. Lynn, and H. Shacham. *Short signatures from the Weil pairing*. In Advances in Cryptology – Asiacrypt 2001, volume 2248 of Lecture Notes in Comput. Sci., pages 514–532. Springer-Verlag, Berlin, 2002.

[6] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory* **22** (1976), 644–654.

[7] A. Enge and P. Gaudry. *A General Framework for Subexponential Discrete Logarithm Algorithms. Manuscript 19 pp (Febr. 2000).*

[8] G. Frey. *Applications of arithmetical geometry to cryptographic constructions*. In Finite fields and applications (Augsburg, 1999), pages 128–161. Springer, Berlin, 2001.

[9] G. Frey. *On the relation between Brauer groups and discrete logarithms.* Tatra Mt. Math. Publ., 33: 199-227, 2006

[10] G. Frey and T. Lange. *Mathematical background of public key cryptography.* In Séminaires et Congrès SMF: AGCT 2003, num.11 (2005), pages 41-74.

[11] G. Frey and T. Lange. *Fast Bilinear Maps from the Tate-Lichtenbaum Pairing on Hyperelliptic Curves.* In Proc. ANTS VII, LNCS 4076, pages 466-479. Springer, Berlin 2006.

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

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

[14] P. Gaudry. *A variant of the Adleman–DeMarrais–Huang algorithm and its application to small genera.* Laboratoire d' Informatique Preprint LIX/RR/99/04 (1999).

[15] M.-D. Huang and W. Raskind. *Signature calculus and discrete logarithm problems.* In Proc. ANTS VII, LNCS 4076. Springer, Berlin 2006.

[16] A. Joux. *A one round protocol for tripartite Diffie–Hellman.* In Proc.ANTS IV, LNCS 1838, pages 385–394. Springer, Berlin 2000.

[17] A. Kresch and Y. Tschinkel. *On the Arithmetic of Del Pezzo Surfaces of Degree 2.* Proc. LMS (3), 89, pages 545-569, 2004.

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

[19] U. Maurer and S. Wolf. *Lower Bounds on Generic Algorithms in Groups.* in: Advances in Cryptology-EUROCRYPT 98, K.Nyberg ed., LNCS 1403. Springer Verlag (1998), 72-84.

[20] B. Mazur. *Notes on étale cohomology of number fields.* Ann. sci. ENS t.6, n^o 4 ,pages 521-552, 1973.

[21] A. Menezes, P. van Oorschot and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press (1995).

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

[23] D. Mumford. *Abelian Varieties*. Oxford University Press 1970.

[24] Jürgen Neukirch. *Algebraic number theory*. Springer, 1999.

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

[26] P. W. Shor, Quantum Computing, *Doc.Math.J.DMV Extra Volume ICM I* (1998), 467–486.

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

[28] J.P. Serre. *Corps locaux*. Hermann, Paris, 1962.

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

[30] J. Tate. *WC-groups over* $\mathfrak{p}$*-adic fields*. Séminaire Bourbaki, Exposé 156, vol. 13, 1958.