# Duality Theorems in Arithmetic Geometry and Applications

Gerhard Frey

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

FIELD INSTITUTE
COXETER LECTURES
September 24-27, 2006

# Contents

# Chapter 1

# Duality in Arithmetic Geometry

## 1.1 Bilinear structures

### 1.1.1 DL in Cyclic Groups

Take $n \in N$ and assume that

$$(\mathbb{Z}/n, +) \xrightarrow{f} \mathbb{N}$$

is given.
$A := \mathrm{Im}(\mathbb{Z}/n)$ becomes a group with the composition $\oplus$ by the rule:

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

$\oplus$ has to be given "in coordinates" of the elements of $A$ without using $f^{-1}$. The computation of $\oplus$ is required to be of polynomial time in $\log(n)$ and hence for $k \in \mathbb{Z}/n$ the evaluation of $k \cdot id_A =: k\circ$ requires polynomial time in $\log(n)$.

Let $P_0$ be a generator of $A$.
Define the discrete logarithm of $P$ with respect to the base $P_0$ by

$$\log_{P_0}(P) := k \in \mathbb{Z}/n \,\text{with}\, k \circ P_0 = P.$$

This function can serve (as we have learned from Diffie-Hellman, ElGamal and many others) as crypto primitive in many protocols of public key cryptography (key exchange, authentification, signatures and encryption).
The secret is the chosen element $k \in \mathbb{Z}/n^*$, the public key is $k \circ P_0$.
Crucial for security is the complexity of the evaluation of $\log_{P_0}$. If this is "large", we call $(A, \circ)$ a DL-system.

To define DL-systems requires only elementary "abstract" mathematics.
In order to find "strong groups"one has to look in rather sophisticated mathematical structures which we shall discuss in Chapter 2.
In fact, the realization of DL-systems used today is done in the frame of arithmetic geometry. Typically the cyclic groups are embedded into torsion groups in divisor classes resp. ideal classes of function rings of curves. Hence, by their very nature, they carry a lot of structure.
One aspect is duality as a major theme in arithmetic - and so - of the lectures.

### 1.1.2 Definition

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

**Definition 1.1.1** *Assume that there are $\mathbb{Z}$-modules $B$ and $C$ and a bilinear map*

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

*with*

- *$Q$ is computable in polynomial time*
- *$Q(.,.)$ is non-degenerate in the first variable. Hence, for random $b \in B$ we have $Q(a_1, b) = Q(a_2, b)$ iff $a_1 = a_2$ .*

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

**Remark 1.1.2** *If we need non-degeneracy in the second variable, too, we can replace $B$ by a quotient. But for computational reasons it may be better to have some "freedom" in the choice of the second argument.*

**Remark 1.1.3** *One is used to describe bilinear maps on free modules by matrices whose entries consist of the value of the form on pairs of elements in fixed bases. For instance, assume that $A$ is a cyclic group with $n$ elements with generator $P_0$. Then*

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

*is determined by $Q(P_0, P_0)$. Without further information the computation of $Q(P, Q)$ is equivalent with the discrete logarithm in $A$.*

### 1.1.3 Some Applications of Bilinear Structures

We begin with destructive aspects:

#### Transfer of DL

The DL-system $(A, \circ)$ is at most as secure as the discrete logarithm in $(C, \circ)$.
For take random $b \in B$ and $c_0 := Q(P_0, b)$.
Then the map

$$< P_0 > \to < c_0 >$$
$$P := n \circ P_0 \mapsto Q(P, b)$$

is a monomorphism, and the claim follows.

#### DDH

If we want to use a DL-system $(A, \circ)$ as crypto primitive for public key systems a necessary condition is the hardness of the discrete logarithm.
For many applications an even stronger condition is needed:

$$\text{For random triples } (P_1, P_2, P_3) \text{ decide whether}$$
$$\log_{P_0}(P_3) = \log_{P_0}(P_1) \log_{P_0}(P_2).$$

If the complexity of the two problems differs one speaks of a gap group. The identities

$$Q(P_1, P_2) = \log_{P_0}(P_1) \cdot \log_{P_0}(P_2) Q(P_0, P_0),$$
$$Q(P_3, P_0) = \log_{P_0}(P_3) Q(P_0, P_0)$$

show that bilinear structures with $A = B$ yield gaps.

### 1.1.4 Constructive Aspects

Since the following applications are discussed at many places I only list them. A first step to get more information is to visit **Paulo Barreto**s Pairing Based Crypto Lounge.
Bilinear structures are used for

- Tripartite Key Exchange
- Identity Based Protocols
- Short Signatures

From the algebraic point of view there are pairings "everywhere".
But: Because of the condition about the computational complexity it is much harder to find DL-systems with bilinear structure.

## 1.2 Class Field Theory

A natural source for pairings are duality theorems of Arithmetic Geometry. Their background is one of the most beautiful theories of Mathematics which I shall state in two lines.

For $0 \leq i \leq 3$ we have a perfect duality of finite groups

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

Here, $X$ is the spectrum of the ring of integers of a number field, the cohomology is with respect to the étale situs, and $F$ is a constructible sheaf (eg. there is a finite set of points in $X$ such that the pull back of $F$ to $X - \{x_1, \ldots, x_n\}$ and to $x_1, \ldots x_n$ is a locally constant abelian sheaf). I cannot explain this result in detail, not to speak of proving it. A nice reference is B. Mazur: Notes on étale cohomology of number fields; Ann. sci. ENS t.6, $n^o$ 4 (1973),p.521-552.
I shall have to restrict myself to special cases and to state consequences.

## 1.3 Dual Groups

### 1.3.1 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] Define $\mathbb{Z}^{(S)}$ as the group of functions $h$ from $S$ to $\mathbb{Z}$ for which $h(z) = 0$ for almost all $z \in \mathbb{Z}$.
$S$ is embedded into $\mathbb{Z}^{(S)}$ by sending $s$ to $f_s$ with $f_s^{-1}(1) = \{s\}$ and $f_s^{-1}(0) = S \setminus \{s\}$.
$\mathbb{Z}^{(S)}$ is the free abelian group generated by $S$.
A function $f$ from $S$ to $C$ can be extended "linearly" (and then is denoted again by $f$) to $\mathbb{Z}^{(S)}$ by

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

By this construction we map $F(S,C)$ to $\mathrm{Hom}(\mathbb{Z}^{(S)}, C)$.
We get the evaluation pairing

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

by

$$Q(g_0, f) \mapsto f(g_0).$$

### 1.3.2 Pairings in the World of Homomorphisms

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

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

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

$D$ is linear and non-degenerate in the second argument. As function of the first argument, it is a group homomorphism.
Since $C$ is assumed to be abelian every homomorphism vanishes on the commutator subgroup $S'$ of $S$, and hence $D$ gives rise to a pairing

$$D : S/S' \times \mathrm{Hom}(S, C) \to C.$$

## The algebraic duality theorem

Take a topological group $S$ and $C = \mathbb{R}/\mathbb{Z}$ 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.
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 $S/S'$ 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:
Assume that $S$ is abelian.
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

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

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

## 1.4 Arithmetical Duality

We add more structure to $S$.
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 all subgroups of $G$ which have finite index. We define a functor

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

sending $L$ to $M^{G_L}$.

**Example 1.4.1** *Take $M = K_s^*$.*
*The corresponding functor is called $G_m$. It has a 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 $K$ the set of $R$-rational points of $G_m$ is*

$$G_m(R) = R^*,$$

*the group of invertible elements in $(R, \cdot)$.*
*$G_m$ is an affine curve with coordinate ring*

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

This example is generalized in the following way.
Assume that $\mathcal{A}$ is an étale commutative group scheme defined over $K$.
Then $A = \mathcal{A}(K_s)$ is a $G_K$-module and the corresponding functor is represented by $\mathcal{A}$. 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.
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 $\mathrm{Hom}_K(A, B)$.

## 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 1.4.2** *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 group schemes of 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 $n$.
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 $\mu_n$ 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 only 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 $\mu_n$ is isomorphic to $\mathbb{Z}/n$. Assume that we can compute the duality pairing fast. Then this does not imply that we can transfer the discrete logarithm from $A$ to $\mathbb{Z}/n$. We only transfer it to the multiplicative group of $K$.

The negative aspects of some of these items can be repaired by using "derived" pairings.

### 1.4.1 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 $\beta^G$ 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 $H^*$ 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 $\delta^n$ such that there is an exact sequence of $G$-modules

$$\dots \xrightarrow{\delta^{n-1}} H^n(G, A) \xrightarrow{\alpha^{(n)}}$$

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

$H^n(G, M)$ is a quotient of the group of $n$-cocycles $C^n(G, A) \subset F(G^n, A)$ satisfying a combinatorial condition modulo the subgroup of $n$-coboundaries $B^n(G, A)$.
Relevant examples for us:

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

We shall need the connecting homomorphisms $\delta^n$ only for $n = 0, 1$.
**Definition of $\delta^0$:** For $c \in C^G$ choose $b \in B$ with $\beta(b) = c$.
For all $\sigma \in G$ the element $\sigma(b) - b$ lies in $A$.
$\delta^0(c)$ is the class of the cocycle
$$\zeta : \sigma \mapsto \sigma(b) - b.$$

**Definition of $\delta^1$:** Take $c \in H^1(G, C)$ and represent it by the cocycle
$$\zeta : G \to C.$$
For every $\sigma \in G$ choose $b(\sigma) \in B$ with $\beta(b(\sigma)) = \zeta(\sigma)$.
For $\sigma, \tau \in G$ define
$$\delta(\sigma, \tau) := \sigma(b(\tau)) + b(\sigma) - b(\sigma\tau)$$
which is, as $\zeta$ is a cocycle, in $A$.
Take $\delta^1(c)$ as class of $\delta(\sigma, \tau)$ in $H^2(G, A)$.

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

Because of continuity one gets

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

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

**Consequence:**
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 $K$.
The inflation and the restriction maps are related. A special case is the very useful sequence

$$0 \to H^1(G/U, M^U) \overset{\mathrm{inf_{U/G}}}{\to} H^1(G,M) \overset{\mathrm{res}_U}{\to} H^1(U,M).$$

In particular,

$$H^1(G,M) = \bigcup_{U} H^1(G/U, M^U).$$

We can generalize this statement to the second cohomology group under special assumptions on $M$.

**Lemma 1.4.3** *Assume that $M$ is a $G$-module such that for all $U < G$ one has $H^1(U,M) = 0$.*
*Then*

$$\mathrm{inf_{U/G}} : \mathrm{H^2(G/U, M^U)} \to \mathrm{H^2(G,M)}$$

*is injective.*

**Example 1.4.4** *Take $G = G_K$ and $M = K_s^*$.*
*Hilbert's Theorem 90 implies that for all $L/K$ one has $H^1(G_L, L_s^*) = 0$.*
*Hence*

$$H^2(G_K, K_s^*) = \bigcup_{L} \mathrm{inf_{G_L/G_K} H^2(G(L/K, L^*))}$$

*where $L$ runs over all 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 $\Gamma$ 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 $A(= \mathcal{A}(K_s))$.
So we can embed Galois cohomology into a much wider and flexible frame as it is done in the fundamental duality theorem of class field theory.

## Pairings in Cohomology

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

$$A \bigotimes B$$

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

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

$$\to H^{p+q}(G, A \bigotimes B)$$

with functorial properties with respect to cohomology functors (especially $\delta^n$, this implies uniqueness).
$\cup^{p,q}$ is called the cup product.
Explicit formulas can be found for instance in the book of Cartan-Eilenberg.
Now assume that there is a $G$-pairing

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

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

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

**Example 1.4.5** *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). As part of the long exact sequence we have the exact sequence

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

Duality implies

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

Fact: $\delta^0(J(K)/nJ(K))$ is isotrop w.r.t $E^{1,1}$ and so $E^{1,1}$ induces the Tate-pairing

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

### 1.4.2 The Local Case

We apply the fundamental duality theorem

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

to the special case that $X = Spec(O_K)$ and $O_K$ is the ring of integers in a local field $K$, ie. $K$ is a finite algebraic extension of a $p$-adic field $\mathbb{Q}_p$ or a power series field over a finite field.
$F$ is assumed to be a finitely generated Galois module. $Spec(O_K)$ is a one-dimensional schema with a closed point corresponding to the maximal ideal $\mathfrak{p}$ (or, to $Spec(k)$ where $k$ is the residue field of $\mathfrak{p}$) and a generic point corresponding to $Spec(K)$ as open subscheme of $X$.
Galois modules over $X$ consist of a generic fiber, ie. 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 1.4.6** *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 $0 \le i \le 2$ the cohomology groups $H^i(G_K,A)$ are finite and the evaluation pairing induces non-degenerate pairings*

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

**Corollary 1.4.7** *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.*

We shall discuss computational aspects (at least for Jacobian varieties) in the next chapter in detail.
5

Etale cohomology sees the unramified part of cohomology.
Let $I$ be the inertia group of $K$.
A $G_K$-module is unramified if $I$ acts trivially on $A$.
This allows to see $A$ as $\widehat{Z}$-module, and the cohomology $H^n(\widehat{\mathbb{Z}}, A)$ is called $H^n_{nr}(K, A)$.
Let $A$ be finite.

- $H^1_{nr}(K, A)$ can be identified with a subgroup of $H^1(G_K, A)$. Its order is equal to the order of $A^{G_K}$.
- $H^n_{nr}(G_K, A) = 0$ for $n \geq 2$.
- $H^1_{nr}(K, A)$ is orthogonal to $H^1_{nr}(K, \widehat{A})$.

### 1.4.3 Global Situation

Now let $K$ be a global field. In this case étale cohomology shows its full strength. An important method is to study global objects by passing to local ones. So let $\Sigma_K$ 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 $G_{K_\mathfrak{p}}$.
We have restriction maps

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

Define

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

The key questions are: Describe the kernel and the cokernel of $f_n$!
Consequences of the duality theorem: 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 celebrated 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

$$0 \to Br(K) \stackrel{\sum \rho_\mathfrak{p}}{\to} \sum Br(K_\mathfrak{p}) \to \mathbb{Q}/\mathbb{Z} \to 0$$

  is exact.

## 1.5 From Curves to Arithmetic

### 1.5.1 Evaluation of Functions

We return to arbitrary fields $K$.
Let $C$ be a (projective absolutely irreducible regular) curve defined over $K$ with function field $F$.
Let $L$ be an extension field of $K$, $C_L$ the curve obtained by constant extension to $L$ and $F_L = F \cdot L$ the function field of $C_L$. The set of points of $C$ rational over $L$ is denoted by $C(L)$.
The field $F_{K_s}$ is a Galois extension of $F$ with Galois group $G_K$.
$G_K$ is acting in a natural way on $C(K_s)$ and the set of $G_L$-invariant points is $C(L)$. The set $C(K_s)$ is the disjoint union of (finite) $G_K$-orbits. Each orbit corresponds to a place $\mathfrak{p}$ of $F$, ie. a class of equivalent valuations on $F$ which are trivial on $K$.
Let $S$ be a set of places of $F$ and $C_S \subset C(K_s)$ the set of points which occur in orbits attached to $S$.
Let $F_{K_s,S}$ be the subgroup of functions in $F_{K_s}^*$ which have neither zeroes nor poles in points of $C_S$. Note that $F_{K_s,S}$ is a $G_K$-module.

We can evaluate $f \in F_{K_s,S}$ at points $P \in C_S$ and the map

$$Q : C_S \times F_{K_s,S} \to K_s^*$$

$$Q(P, f) := f(P)$$

is $G_K$-equivariant and linear in the second argument.

By $D_S$ we denote the free abelian group generated by $C_S$. It is the group of divisors of $C$ with support in $S$. It is a $G_K$-module with action induced by the action of $G_K$ on points of $C$. If $S$ is the set of all places of $F$ we call $D_S =: D_C$ the divisor group of $C$.
By linear extension we get a Galois pairing

$$Q : D_S \times F_{K_s,S} \to K_s^*.$$

**Remark 1.5.1** *One defines a "partial" map*

$$D_C \times F_{K_s}^* \dashrightarrow K_s^*$$

*for pairs $(D, f)$ where the set of zeros and poles of $f$ is disjoint to the support of the divisor $D$.*

### 1.5.2 Induced pairings in cohomology: The Lichtenbaum Pairing

Motivated by the duality theorems we are interested in the case that $p+q = 2$. It is not difficult to see that $H^1(G_K, D_S) = H^1(G_K, D_C) = 0$.
Thus an interesting pairing is

$$Q : H^0(G_K, D_S) \times H^2(G_K, F_{K_s,S}) \to H^2(G_K, K_s^*).$$

An element $c \in H^2(G_K, F_{K_s,S})$ is represented by

$$(f(\sigma, \tau) \in F_{K_s,S}; \sigma, \tau \in G_K),$$

$H^0(G_K, D_S)$ consists of divisors $D$ which are sums of Galois orbits of points on $C$ with support in $S$.

$$Q(D, c) \text{ is the class of the cocycle } (f(\sigma, \tau)(D)).$$

### Pairings on Divisor Classes

Let $S'$ be the complement of $S$ in the set of places of $F$. To $g \in F^*_{K_s,S'}$ we can associate the principal divisor

$$(g) = \sum_{P \in C(K_s)} v_P(g) \cdot P$$

where $v_P$ is the normed valuation in $P$.
These principal divisors form a $G_K$-submodule of $D_S$ denoted by $P_S$ which is contained in $D^0_S$, the group of divisors of degree 0 in $D_S$ consisting of all divisors for which the coefficients add up to 0. If $S$ consists of all places we denote by $P_C$ the subgroup of principal divisors in $D^0_C$, the group of divisors of degree 0. Restricting the evaluation pairing we get a pairing

$$E_S : P_S \times F_{K_s,S} \to K_s^*$$

with $E_S((g), f) = f((g))$. We can interchange the role of $f$ and $g$ by replacing $S$ with its complement $S'$ in the set of places of $F$ and get $E_{S'}((f), g) = g((f))$.

**Theorem 1.5.2**

$$E_S((g), f) = E_{S'}((f), g)$$

This is the fundamental Reciprocity law of **Weil**.
Define the divisor class group of degree 0, $\mathrm{Pic}^0_S$, by the exact sequence

$$0 \to P_S \to D^0_S \to \mathrm{Pic}^0_S \to 0$$

and $\mathrm{Pic}^0_C$ by

$$0 \to P_C \to D^0_C \to \mathrm{Pic}^0_C \to 0.$$

**Remark 1.5.3**

- *$(f) \in P_S$ determines $f$ up to a constant.*

  *For $D \in D^0_S$*

  $$(f)(D) := f(D)$$

  *is well defined, and we get an evaluation pairing*

  $$P_S \times D^0_{S'} \to K_s^*$$

  *with $S'$ the complement of $A$ in the set of places of $F$.*

- *Given a finite set $S_0$ of places and $c \in \mathrm{Pic}^0_C$ we find a divisor $D \in c$ prime to $S_0$.*

Again take $S'$ as complement of $S$ in the set of places of $F$. We use the exact sequence

$$0 \to P_{S'} \to D^0_{S'} \to \mathrm{Pic}^0_{S'} \to 0$$

to get an injection

$$\delta^1 : H^1(G_K, \mathrm{Pic}^0_{S'}) \to H^2(G_K, P_{S'}).$$

Weil's reciprocity theorem yields that

$$Q \mid (P_S \times \delta^1(H^1(G_K, \mathrm{Pic}^0_{S'})) = 0$$

and so we get a pairing

$$L_S : (\mathrm{Pic}^0_S)^{G_K} \times H^1(G_K, \mathrm{Pic}^0_{S'}) \to H^2(G_K, K_s^*).$$

Using Remark 1.5.3 we see that we can skip the subscript $S$ and hence get the Lichtenbaum pairing

$$L : (\mathrm{Pic}^0_C)^{G_K} \times H^1(G_K, \mathrm{Pic}^0_C) \to H^2(G_K, K_s^*).$$

**Example 1.5.4** *Let $E$ be an elliptic curve over $K$. Then the Lichtenbaum pairing is a $\mathbb{Z}$-bilinear map*

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

# Chapter 2

# Ideal Class groups with Bilinear Structure

At the end of the previous chapter we have defined the Lichtenbaum pairing in terms of divisor classes of function fields.
We want to regain and to generalize this pairing in terms of ideal class groups, and then use the Tate duality for local fields to get bilinear structures.

## 2.1 Ideal Class Groups

The most important source for finding candidates for DL-systems are ideal class groups attached to curves $C$ over finite fields $\mathbb{F}_q$.

### 2.1.1 Picard Groups

#### Curves and Rings

Let $K$ be a field and $C_O$ be an absolutely irreducible curve defined over $K$ with function field $F$ and with $O$ as ring of holomorphic functions on $C_O$.
We assume that $Quot(O) = F$ and so $C_O$ is an affine curve.
Note that we allow singularities.

Let $\widetilde{C_O}$ be the desingularization with ring of holomorphic functions $\tilde{O}$.
$\tilde{O}$ is a Dedekind domain, it is the integral closure of $O$.
The compactification of $\widetilde{C_O}$ is the a unique projective irreducible non-singular curve $C$ with function field $F$ containing $\widetilde{C_O}$ as affine part.

## Base Extension

As always, $K_s$ is the separable closure of $K$. For simplicity we assume that all singular points on $C_O$ become rational over $K_s$.
By overlining we denote objects obtained by base change from $K$ to $K_s$.
So $\overline{C} = C \times Spec(K_s)$ with function field $\overline{F} = FK_s$.
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. $\overline{\widetilde{C_O}}$).

**Definition 2.1.1** *$T_\infty = \overline{C}(K_s) \setminus \overline{\widetilde{C_O}}(K_s)$ is the set of "infinite points" of $C$. By $S \subset \overline{\widetilde{C_O}}(K_s)$ we denote the points which correspond to singular points on $\overline{C_O}$.*

$G_K$ acts on $\overline{C}(K_s)$ mapping $T_\infty$ and $S$ into themselves.
We assume that there is a $K$-rational point $P_\infty$ in $T_\infty$.
The conductor $\mathfrak{m}_{C_0}$ of $\tilde{O}/O$ is an ideal which reflects the singularities of $C_O$.
We assume that $C_O$ has only one singular point $P_{sing}$ and $\mathfrak{m}_{C_O} < \tilde{O}$ corresponds to $\prod_{P \in S} m_P$ where $m_P$ is the maximal ideal which correspond to the point $P \in C(K_s)$. In the ring $O$ is $\mathfrak{m}_{C_O}$ is the ideal of functions vanishing in $P_{sing}$.

**Remark 2.1.2** *This looks like a strong assumptions but higher powers of prime ideals in $\mathfrak{m}_{C_O}$ change the corresponding ideal class by linear unipotent groups which are irrelevant for cryptology, and different singular points can be treated separately.*

## Ideal Classes

To ease notation we denote the ring of holomorphic functions on $\overline{C} \setminus \{P_\infty\}$ by $\overline{O}_{P_\infty}$.

**Definition 2.1.3** *Let $R \subset \overline{F}$ be a subring, $f \in \overline{F}$. Then*

$$(f)_R := f \cdot R$$

*is the principal ideal attached to $f$ in $R$.*
*For $H \subset \overline{F}$ we define*

$$(H)_R = \{(f)_R; f \in H\}.$$

*$(\overline{F}^*)_R$ is the set of of principal ideals of $R$.*

*The group of invertible ideals in $R$ is denoted by $I_R$. Its intersection with $(\overline{F}^*)_R$ is the group of invertible principle ideals denoted by denoted by $Princ_R$. The Picard group $\mathrm{Pic}_R$ is defined by the exact sequence*

$$1 \to Princ_R \to I_R \to \mathrm{Pic}_R \to 0.$$

**Example 2.1.4** *Take for $R$ the ring $\overline{O}_{P_\infty}$ of holomorphic functions on $C(K_s)\setminus P_\infty$. For $P \in C(K_s)$ let $v_P$ be the normalized valuation with valuation ideal $m_P := \{g \in \overline{F};\, g(P) = 0\}$.*
*Then*

$$(f) = \prod_{P \in C(K_s)\setminus P_\infty} m_P^{v_P(f)}$$

*and $\mathrm{Pic}_{\overline{O}_{P_\infty}}$ is isomorphic to the divisor class group of degree 0, $\mathrm{Pic}^0_{\overline{C}}$, of $\overline{C}$. In particular, we can represent every divisor class of degree 0 of $\overline{F}$ (resp. ideal class of $\overline{O}_{P_\infty}$) by an ideal*

$$A = \prod_{P \in C(K_s)\setminus\{P_\infty\}} m_P^{z_P} \text{ with } \sum_{P \in C(K_s)\setminus\{P_\infty\}} z_P = 0.$$

If we take more than one point $P_\infty$ away from $C$ the ideal class group will become smaller. The reason is that we pass to a localisation of $\overline{O}_{P_\infty}$. This is described in the next proposition.

**Proposition 2.1.5** *We have the exact sequence of $G_K$-modules*

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

*with*

$$\mathcal{C}_{T_\infty} =< m_P;\, P \in T_\infty \setminus P_\infty > /U_{T_\infty}.$$

*Here $U_{T_\infty}$ are the functions which have no zeros and poles outside of $T_\infty \setminus P_\infty$.*

Next we want to describe $\mathrm{Pic}(\overline{O})$.
The group of invertible ideals $I_{\overline{O}}$ in $\overline{O}$ is generated by ideals of $\overline{O}$ which are prime to $\mathfrak{m}_{C_O}$.
Let $\overline{F_S^1}$ denote the functions $f \in \overline{F}$ for which $f(P) = 1$ for all $P \in S$.
We get the exact sequence of $G_K$-modules

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

Now we use our assumption that we have *only one singular point on $C_O$ and that its conductor is squarefree.*
The approximation theorem for functions in $\overline{F}$ yields

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

   $$\varphi : \mathrm{Pic}(\overline{O}) \to \mathrm{Pic}(\tilde{\overline{O}})$$

   which is $G_K$-invariant.

2. The kernel of $\varphi$ 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 2.1.6** *There is a torus $\mathcal{T}_S$ of dimension $\mid S \mid -1$ defined over $K$ such that we have the exact sequence of $G_K$-modules*

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

**Remark 2.1.7** *The isomorphism class of $\mathcal{T}_S$ is determined by its character group $X$, and this group is determined by the first homology group of the dual graph of $C_O$ (Grothendieck) (with $G_K$-action). So Theorem 2.1.8 (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.*

Using that $\mathrm{Pic}_{\overline{O}_{P_\infty}} \cong_{G_K} J_C(K_s)$ and putting all pieces together we get

**Theorem 2.1.8** *We have the exact sequences of $G_K$-modules*

$$1 \to Princ_{\overline{O}} \to I_{\overline{O}} \to \mathrm{Pic}_{\overline{O}} \to 0$$

.

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

*and*

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

**Remark 2.1.9** *All the material of this section is to be found in* J-P. Serre: Corps de classes et groupes algébriques.

## 2.2 The Lichtenbaum Pairing for Ideal Class Groups

We continue to work with rings $O$ resp. $\overline{O}$ as above.

### 2.2.1 The non-singular complete case

We assume that $T_\infty = \{P_\infty\}$ and so $\overline{O} = \overline{O}_{P_\infty}$. We repeat, for the convenience of the reader, the definition of the Lichtenbaum pairing in the language of ideal classes. We use the exact sequence

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

and get as part of the long exact cohomology sequence

$$H^1(G_K, I_{\overline{O}}) \to H^1(G_K, \mathrm{Pic}_{\overline{O}}) \stackrel{\delta^1}{\to} H^2(G_K, (\overline{F})).$$

We remark that $I_{\overline{O}}$ is a direct sum of copies of $G_K$-submodules isomorphic to $\mathbb{Z}[\overline{G}]$ with $\overline{G}$ a finite quotient group of $G_K$ and so $H^1(G_K, I_{\overline{O}}) = 0$ and $\delta^1$ is injective. It is given by the following rule: Take $c \in H^1(G_K, \mathrm{Pic}_{\overline{O}})$ and represent it by a cocycle

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

where $\bar{D}(\sigma)$ is an ideal class. Choose an ideal $D(\sigma) \in I_{\overline{O}}$ lying in $c(\sigma)$.
Then for all $\sigma, \tau \in G_K$ the ideal

$$A(\sigma, \tau) = \sigma D(\tau) \cdot D(\sigma) \cdot D(\sigma\tau)^{-1}$$

is a principal ideal $(f(\sigma, \tau))$ with $f(\sigma, \tau) \in \overline{F}$ and $\delta^1(c)$ is the cohomology class of the $2-$*cocycle*

$$\gamma : (\sigma, \tau) \mapsto (f(\sigma, \tau)).$$

We note that, since $T_\infty$ is assumed to be $\{P_\infty\}$ the function $f(\sigma, \tau)$ is determined up to a constant by its ideal.
We have some choices. For instance we can change $D(\sigma)$ by a principal ideal. So for a given ideal $A \in I_O$ and all $\sigma \in G_K$ we can and will choose $D(\sigma)$ prime to $A\overline{O}$.
Hence $f(\sigma, \tau)$ has neither zeros nor poles in points $P \in C$ for which the ideal $m_P$ occurs with non-zero multiplicity $z_P$ in $A\overline{O} = \prod_{P \in C \setminus P_\infty} m_P^{z_P}$ and so the evaluation pairing

$$Q(\sum z_P \cdot P, f(\sigma, \tau))$$

is defined and gives a 2-cocycle in $H^2(G_K, K_s^*)$.

Changing $A$ by a principal ideal does not change the cohomology class as we have seen in the first chapter (*Weil reciprocity*). Using the approximation theorem we see that we can change $A$ by a principal ideal such that $\sum_{P \in C \setminus P_\infty} z_P = 0$.
Then

$$Q(\sum z_P \cdot P, f(\sigma, \tau))$$

is defined and independent of the choice of $f(\sigma, \tau)$.

**Definition 2.2.1** *The* ***Lichtenbaum pairing***

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

*is defined in the following way.*

*Choose* $A$ *in* $\bar{P} \in \mathrm{Pic}_{O_{P_\infty}}$ *with* $A\overline{O}_{P_\infty} = \prod_{P \in C \setminus P_\infty} m_P^{z_P}$ *of degree* 0.
*Take* $c \in H^1(G_K, \mathrm{Pic}_{\overline{O}_{P_\infty}})$ *and represent* $\delta^1(c)$ *by* $(f(\sigma,\tau))$ *prime to* $A$.
*Then* $T_L(\bar{P}, c)$ *is the cohomology class of* $\zeta(\sigma,\tau) := Q(\sum z_P \cdot P, f(\sigma,\tau))$.

The following example is important for applications.

**Example 2.2.2** *Let* $L/K$ *be a cyclic extension with* $G(L/K) =< \tau >$ . *Take* $c \in H^1(< \tau >, \mathrm{Pic}_{\overline{O}_{P_\infty}^{G_L}})$ *with representing cocycle* $\zeta(\tau^i)$.
*The cocycle condition implies that* $\zeta(\tau^i) = \sum_{j=0\ldots i-1} \tau^j(\zeta(\tau))$ *and hence* $\sum_{j=0,\ldots n-1} \tau^j \zeta(\tau) = 0$.
*Choose* $D \in \zeta(\tau)$ *and* $L-$*rational and* $D(\tau^j) = \sum_{k=0\ldots j-1} \tau^k(D)$.
*It follows that*

$$\sum_{k=0\ldots n-1} \tau^k(D) = (f)_c$$

*with* $f_c \in F.L$, *the function field of* $C_L$.
*By applying the definition it is obvious that* $\delta^1(c)$ *is presented by the cocycle*

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

*and*

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

*Hence* $T_L(\bar{D}, c)$ *is (the inflation of) the class of the cocycle*

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

*and*

$$\zeta(\tau^i, \tau^j) = \prod f_c(P)^{z_P} \text{ if } i + j > n.$$

*This is an element in the subgroup* $H^2(G(L/K), L^*)$ *of* $H^2(G_K, K_s^*)$ *corresponding to a cyclic algebra (see third chapter).*

We still assume that we are in the complete non-singular case.

### The Tate-Lichtenbaum Pairing

Since $\mathrm{Pic}_{\overline{O}_{P_\infty}} = J_C(K_s)$ the Lichtenbaum pairing induces for every $n \in \mathbb{N}$ a pairing

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

We recall that we have defined the Tate pairing between these modules.

**Theorem 2.2.3** ***(Lichtenbaum)*** *Up to a sign the pairing $T_n$ is equal to the Tate pairing.*

We call the pairing $T_n$ the Tate-Lichtenbaum pairing.

## 2.2.2 The non-complete non-singular case

A first application of this theorem is the definition of the Lichtenbaum pairing when $T_\infty$ is contains more than one element.
We have the exact sequence

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

We want to define the Lichtenbaum pairing for $\mathrm{Pic}_O$ resp. $H^1(G_K, \mathrm{Pic}_{\overline{O}})$. But it is not true in general that $H^0(G_K, \mathrm{Pic}_{\overline{O}})$ is equal to $\mathrm{Pic}_O = \varphi(\mathrm{Pic}_{O_{P_\infty}})$. Moreover the map from $\bar{F}$ to $Princ_{\overline{O}}$ has as kernel the group of functions $U_{T_\infty}$. Hence we cannot evaluate the image of $\delta^1 : H^1(G_K, \mathrm{Pic}_{\overline{O}}) \to H^2(G_K, Princ_{\overline{O}})$ at points on $C \backslash T_\infty$. To overcome these difficulties we have to apply an isogeny $\psi$ to $J_C$ with $\mathcal{C}_{T_\infty} = kernel(\psi)$. Hence we have to leave the world of Jacobian varieties and to switch to the Tate pairing. In addition we have to use the functoriality of the Weil pairing with respect to isogenies. Finally we get

**Proposition 2.2.4** *The Lichtenbaum pairing induces a pairing, also denoted by $T_L$ from $\mathrm{Pic}_O \times \psi^1(H^1(G_K, \mathrm{Pic}_{\overline{O}}))$ to $H^2(G_K, K_s^*)$.*

### 2.2.3 The singular case

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

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

where $T_S$ is a torus determined by the conductor $\sum_{P\in S} m_P$ 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

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

We can restrict the boundary map $\delta^1$ to $H^1(G_K, \mathrm{Pic}_{\overline{O}})$ and we get a pairing as above but we cannot expect to get any information about $T_S(K)$. We shall show in the next Section how one can overcome this difficulty in the case which is relevant for cryptography.

### 2.2.4 Conclusion

Let $O$ be the ring of holomorphic functions of an affine curve $C_O$ defined over $K$. For all $n$ prime to $\mathrm{char}(K)$ we have defined the Tate-Lichtenbaum pairing

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

## 2.3 Lifting

The interesting case for applications in cryptography is that $K = \mathbb{F}_q$ with $q = p^d$. In fact, all DL-systems with geometric background can be realized

as $G_K$-invariant subgroups of Galois submodules of some $\mathrm{Pic}_O$.
But over finite fields the Tate-Lichtenbaum pairing is trivial since

$$H^2(G_{\mathbb{F}_q}, \overline{\mathbb{F}_q}) = 0.$$

The way out is to switch to local fields as ground fields always taking care that this lifting is easy and that we do not loose either relevant information or fast operations. Then the local duality theorem will imply the non-triviality of the pairing, and, at the same time, we shall get information about the "torus part" related to singularities.

**Remark 2.3.1** *We recall that for point counting a similar procedure is most successful.*

So let $K$ be complete with respect to a normed valuation $w_{\mathfrak{p}}$ and with residue field $\mathbb{F}_q$.
Its separable closure is either a field of Laurent series with coefficients in $\overline{\mathbb{F}_q}$ or the algebraic closure of the unramified extension of $\mathbb{Q}_p$ of degree $d$.

### 2.3.1 Lifting the Galois Group

The maximal unramified extension of $K$ of $K$ is denoted by $K_{nr}$. There is a canonical lift (easily computable) of the Frobenius automorphism $\phi_q$ to $K_{nr}$ also called the Frobenius automorphism and denoted by $\phi_q$. This automorphism generates the Galois group of $K_{nr}/K$ as topological group. Algebraic extensions of $K_{nr}$ are totally ramified.
We are interested in *tamely* ramified extensions.
Let $n$ be a natural number prime to $p$. There is exactly one tamely ramified extension $L_n$ of $K_{nr}$ of degree $n$ given explicitly by $L_n = K_{nr}(\pi^{1/n})$ where $\pi$ is any of the elements in $K$ with $w_{\mathfrak{p}}(\pi) = 1$. (Such elements are called *uniformizing elements* of $K$.) So $L_n/K_{nr}$ is cyclic. We choose a primitive $n$-th root of unity $\zeta_n$ and denote by $\tau_n$ the generator which maps $\pi^{1/n}$ to $\zeta_n \cdot \pi^{1/n}$. It follows that $L_n$ is a Galois extension of $K$ whose group is generated by $\phi_q$ and $\tau_n$.
If we assume that $\zeta_n \in K$, or equivalently, that $n \mid (q-1)$ then $K(\pi^{1/n})$ is Galois over $K$, $\tau_n$ and $\phi_q$ commute and the maximal tamely ramified

extension of $K$ whose Galois group has exponent dividing $n$ is the subfield of $L_n$ fixed by $\phi_{q^n}$.

**Proposition 2.3.2** *There is a totally ramified extension of $K$ of degree $n$ if and only if $\zeta_n \in K$.*
*This extension is cyclic and, up to "twists " with unramified extensions, unique.*

Lifting gives more freedom, since in addition to unramified extensions we find ramified extensions, too.

### 2.3.2 Lifting of Curves

Let $O$ be the ring of holomorphic functions of an affine curve $C_O$ defined over $\mathbb{F}_q$, with singular points $S \subset \overline{C_O}(\mathbb{F}_{q_s})$ defining the conductor $\mathfrak{m}_O = \sum_{P \in S} m_P$ and the corresponding desingularized curve $\tilde{C}$ embedded in the projective nonsingular curve $C$. The set $T_\infty$ was defined as $C(\overline{\mathbb{F}_q}) \setminus \tilde{C}(\overline{\mathbb{F}_q})$.
We denote by $g_0$ the genus of $C$.
We state the following (rather elementary) facts from the reduction theory of curves resp. abelian varieties.[1]

**Theorem 2.3.3** *1. There is a projective absolutely irreducible* nonsingular *curve $C^l$ over $K$ and a Galois invariant set ${T_\infty}^l \subset C^l(\overline{K})$ with*

- *The genus of $C^l$ is equal to*

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

- *$C^l \setminus {T_\infty}^l$ modulo the maximal ideal of $K$ is equal to $C_O$.*
- *The Jacobian of $C^l$ extends to a scheme $J_{C^l}$ over $Spec(O_K)$, the ring of integers of $K$, whose connected component $J^0 := J^0_{C^l}$ is a semi-abelian variety which has as special fiber the generalized Jacobian of $C_O \cup T_\infty$.*

[1] Recall that we have assumed that $C_0$ has only one singular point and the conductor is squarefree.

- *The set* ${T_\infty}^l$ *is* $G_K$*-invariant. It is mapped bijectively to* $T_\infty$*.*

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

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

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

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

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

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

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

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

   *Moreover there is an isogeny* $\varphi$ *from* $J_{C^1}$ *defined over* $K$ *with kernel isomorphic to* $\mathcal{C}_{T_\infty}$ *such that* $\mathrm{Pic}_O/[n]\mathrm{Pic}_O$ *is isomorphic to* $\varphi(J_C(K))/[n]\varphi(J_C(K))$*.*

Theorem 2.3.3 enables us to study all crypto systems based on ideal classes of curves over finite fields by using cohomology theory of local fields.

In most instances the situation will be rather simple. The curve $C$ will be either non-singular ( good reduction) or will have genus equal to zero (the toric case).
The set of missing points will consist (e.g. in the case of $C_{ab}$-curves ) of one point and so the group $\mathcal{C}_{T_\infty}$ is the trivial group.
The lift of curves in the toric case leads to the interesting theory of Mumford curves.

**Remark 2.3.4** *It is important that all interesting objects can be lifted over $K$.*
*This is so since $n$ is prime to $q$ and we are in the étale world. The next important observation is that the finite modules defined over $\mathbb{F}_q$ can be lifted to unramified Galois modules over $K$ which played a special role in the cohomology theory of local fields.*

**Connected components and ramification** In Theorem 2.3.3 we have assumed that $n$ is prime to the number of connected components of the special fiber of the Jacobian of the lifted curve. This is a very mild condition. On the one hand we have many choices for the construction of $C^l$ and we can do it such that this number is very small. On the other side the assumption is not really necessary; it only simplifies the formulation of Theorem 2.3.3 (which is long enough as it is). In certain cases it may be even desired to have an appropriate number of components which deliver torsion points on $J_{C^l}$ which are not coming from points on $\mathrm{Pic}_O$.
If, after the lifting, we extend $K$ by a ramified extension and if there was a singularity on $C_0$ then the group of connected components of the semi-abelian group scheme over $O_K$ will be multiplied by the ramification index, and so there is a ramified part of the torsion group of $J_{C^l}$ if there are singular points on $C_O$. This makes the cohomology theory of Galois modules attached to torsion points much richer.

**The Tate elliptic curve** Instead of proving the statements of Theorem 2.3.3 we give a simple but important example.

**Example 2.3.5** *We begin with the affine curve*

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

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

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

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

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

*There is one singular point* $(0,0)$ *on* $C$. *This point corresponds to 2 points (we have two different tangents at this point) on the desingularization. It follows that* $\mathrm{Pic}_O$ *is isomorphic to* $\mathbb{F}_q^*$.
*Let* $K$ *be a local field with residue field* $\mathbb{F}_q$ *and uniformizing element* $\pi$, $k \in \mathbb{N}$. *Then*

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

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

$$1 \to U_K \to E(K) \to \mathbb{Z}/k\mathbb{Z} \to 0,$$

*and all the assertions of the Theorem 2.3.3 can be checked immediately.*

## 2.4 The Tate-Lichtenbaum Pairing over Finite and Local Fields

Let $K$ be a local field and let $C_O$ be an affine curve defined over $K$ with corresponding projective curve $C$. Since we are interested in curves lifted from curves over finite fields we can simplify the situation by using the results of the previous section and assume that $C_O$ has no singularities.

**Theorem 2.4.1** *The Tate-Lichtenbaum pairing*

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

*is non-degenerate.*

**Corollary 2.4.2** *Assume that* $D_n$ *is a cyclic subgroup of* $J_C(K)/[n]J_C(K)$. *Then there is an element*

$$c \in H^1(G_K, J_C(K_s))[n]$$

*such that the restriction* $T_n \mid_{D_n \times \{c\}}$ *is a monomorphism. Hence the discrete logarithm in* $D_n$ *is transferred to the discrete logarithm in* $H^2(G_K, K_s^*)[n]$ *with costs arising from the complexity of computing* $T_n \mid_{D_n \times \{c\}}$.

So we can suspect that $\mathrm{Pic}_O/n\mathrm{Pic}_O$ has a bilinear structure. To decide this we have to describe how to compute $T_n$.

### 2.4.1 Explicit Description over Local Fields

We assume that $K$ is a local field with residue field $\mathbb{F}_q$.
Though the general case is interesting we restrict ourselves to the case that the curve $C$ has good reduction (hence is the lift of a nonsingular curve $C_0$ over $\mathbb{F}_q$) and that we look for Picard groups with only one point at infinity.
So we have a non-degenerate pairing

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

Since we have assumed good reduction and $n$ prime to $q$ we get

$$H^1_{nr}(K, J_C(K_s))[n] = 0.$$

Hence we need ramified extensions and so we have to adjoin $\zeta_n$ to $K$ (or, equivalently, to $\mathbb{F}_q$).
Let $k$ be the smallest number with

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

$k$ is called the "embedding degree".
Define $K(\zeta_n) := K_n$ and let $L$ be "the" ramified extension of degree $n$ of $K_n$,eg. take $L = K_n(\pi_K^{1/n})$, and take $\tau$ as generator of $G(L/K_n)$.
We note that $\phi_q$ acts on $\tau$ by conjugation which is equal to the exponentiation with the cyclotomic character, ie. powering by $q$. We are now ready to determine $H^1(G_K, J(K_s))[n]$. Every element of this group is split by $L$ and hence (using the inflation map) it can be identified with an element in $H^1(G(L/K), J(L))$ which is invariant under the action of $\phi_q$. Here we use that elements of order $n$ in $H^1(G_K, J(K_s))$ are split by field extensions of degree $n$ (which necessarily have to be ramified) and the inflation-restriction-sequence.
As seen in Example 2.2.2 we get for a $\zeta \in c \in H^1(G_K, J_C(K_s))[n]$ that $\zeta(\tau)$ modulo $w_{\mathfrak{p}_L}$ is a point of order $n$. Hence we can assume that $P = \zeta(\tau)$ has order $n$ and that it is contained in $J_C(K_n)$.
But this means that $\zeta \in \mathrm{Hom}(< \tau >, J_C(K_n)[n])$. The invariance condition yields that

$$\phi_q((\zeta(\tau)) = q \circ \zeta(\tau).$$

Hence we can identify (depending on the choice of $\tau$) $H^1(G_K, J_C(K_n))[n])$ with the eigenspace of $\phi_q$ with eigenvalue $q \mod n$ in $J_C(K_s)[n]$ which we

denote by $J_C(K_s)[\chi_q]$.
Now take $\varphi \in \mathrm{Hom}(G_K, J_C(K_n)[n])$ with $\varphi(\tau) = P$ and $\phi_q(P) = q \circ P$.
Let $nP = (f_P)$ and assume that a representative of $Q$ of $\overline{Q} \in J_C(K)$ is chosen such that $f_P(Q)$ is defined.
Then

$$T_n(P, \overline{Q})$$

is the class of cyclic algebra corresponding (wrt. $\tau$) given by $f_P(Q)$.

Moreover, we can change $f_P(Q)$ by a factor in $N_{L/K_n}$ without changing the class of the algebra, and so we can interpret $T_n$ as pairing with values in

$$K_n^*/N_{L/K_n} \cong \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^n.$$

Hence we get a pairing

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

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

### 2.4.2 The Tate-Lichtenbaum Pairing over Finite Fields

We can look at the result above modulo $m_v$ (cf. Theorem 2.3.3) and get an explicit description of the Tate-Lichtenbaum pairing in the case of good reduction which only uses objects attached to the curve modulo $m_v$.

**Theorem 2.4.3** *Assume that $C$ is a projective irreducible non-singular curve define over $\mathbb{F}_q$. Then we get a pairing*

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

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

So the lifting is not necessary for the definition of $T_n$ but the relation with Brauer groups is remarkable and to see the whole background may be advisable even if one wants to use the extremely simple pairing only.

Certainly this is necessary for the general case. We use the results stated in Theorem 2.3.3 and get

**Theorem 2.4.4** *The discrete logarithm in ideal classes of rings of holomorphic functions of affine curves $C$ over finite fields $\mathbb{F}_q$ is transferred to $H^2(G_K, K_s^*)$ by the Tate-Lichtenbaum pairings $T_n$.*

**Remarks 2.4.5**

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

2. *Of course the practical value of Theorem 2.4.4 depends on the assumption that the pairing $T_n$ has low computational complexity. At present, this means that the embedding degree $k$ has to be small.*

### 2.4.3 Evaluation

To compute $T_n$ one has to evaluate a divisor $D$ at $f_P$.
A naive approach is, because of the high degrees needed in practice, not possible.
The way out was found by **V. Miller** for elliptic curves (applied to the Weil pairing). The background is the theory of Mumford's Theta groups which describes 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

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

One has to repeat such an step $O(\log(n))$ times.
**CONSEQUENCE:**
We can reduce the discrete logarithm in ideal class groups of rings of holomorphic functions of curves over $\mathbb{F}_q$ to the discrete logarithm in $H^2(G_K, K_s^*)[n]$ with the costs $O(log(\mid \mathbb{F}_{q^k}) \mid)$.

It is easy to implement the algorithm at least in the case that the ideal class group is equal to the divisor class group of degree 0 of a function field, 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 $g > 1$ nothing is known if $J_C$ is not supersingular.
A successful approach to this problem could be interesting since one can speed up the computation of $T_n$ by a factor $g$ in interesting protocols.

# Chapter 3

# Brauer Groups of Local and Global Fields

## 3.1 The Brauer Group

In the second chapter we motivated the importance of the second cohomology group of the multiplicative group of local fields.

### 3.1.1 Definition and First Properties of Brauer Groups

Let $K$ be a field.

**Definition 3.1.1** *The Brauer group of $K$ is the cohomology group*

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

*It is denoted by*

$$\mathrm{Br(K)}.$$

Br(K) is a torsion group.
One can interpret its elements as classes of simple $K$-algebras with center $K$.

The addition in the cohomology group corresponds to the tensor product. The unit element in Br(K) corresponds to the class of full matrix algebras.
Let $L$ be an extension field of $K$, $A$ an algebra representing $c \in \mathrm{Br(K)}$.
Then $A \otimes_K L$ represents $c_L = \mathrm{res}_{K/L}(c)$. Recall that for Galois extensions $L/K$ the inflation map from $H^2(G(L/K), L^*)$ to $H^2(G_K, K_s^*)$ is injective and that the kernel of the restriction map $\mathrm{res}_{K/L}$ is equal to $H^2(G(L/K), L^*) := \mathrm{Br(L/K)}$, the relative Brauer group.
Assume that $L/K$ is a cyclic extension of degree $n$ with $G(L/K) =< \tau >$.
Algebras corresponding to elements in $H^2(G(L/K), L^*)$ are called *cyclic* algebras. *Recall:* We get all cyclic algebras split be $L$ as cohomology classes of cocycles in the following way:
For $a \in K^*$ define $f_{\tau,a} : G \times G \to L^*$ by

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

For two elements $a, a'$ the cocycles $f_{\tau,a}$ and $f_{\tau,a'}$ 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

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

We get $\mathrm{Br(L/K)} \cong \mathrm{K^*/N_{L/K}(L^*)}$.
Note that this isomorphism depends on the choice of $\tau$!

### 3.1.2 Brauer Groups of Local Fields

#### Invariants

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

$$G(L_u/K) =< \phi_q >$$

where $\phi_q$ is the lift of the Frobenius automorphism of $\mathbb{F}_q$.
Let $c \in \mathrm{Br(K)}$ be split by $L_u$.
Since both $L_u$ and $\phi_q$ are canonically given we can characterize $c$ in a canonical way by

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

Since

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

with $\pi$ an uniformizing element of $K$ the class of $c$ is uniquely determined by $w_{\mathfrak{p}}(a) \bmod n$.

**Definition 3.1.2** *Let $c \in H^2(G(L_u/K), L_u^*)$ be given by the triple $(L_u, \phi_q, a)$. Then $w_{\mathfrak{p}}(a) \in \mathbb{Z}/n\mathbb{Z}$ is the* invariant $\mathrm{inv}_K(c)$ *of $c$.*

It is obvious that the discrete logarithm in $H^2(G(L_u/K), L_u^*)$ is computable in polynomial time if the elements in this group are given in the "canonical" way, i.e. as cyclic algebras with automorphism $\phi_q$.

**Lemma 3.1.3** *Assume that $\tau$ is another generator of $G(L_u/K)$ and $c$ is given by the triple $(L_u, \tau, a)$. Let $f \in \mathbb{Z}$ be such that $\tau^f = \phi_q$ .*
*Then* $\mathrm{inv}(c) = f \cdot w_{\mathfrak{p}}(a) \bmod n$.

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

**Example 3.1.4** *Assume that $L_u = K(\alpha)$ with $\alpha \in U(K)$ such that $\tau(\alpha) = \beta \cdot \alpha$ with $\beta \in K$.*
*Then $\tau^f = \phi_q$ if and only if $\beta^f \equiv \alpha^{q-1}$ modulo the maximal ideal of $K$. So we have to solve a discrete logarithm problem in $\mathbb{F}_q$.*

Because of the duality theorem we know that Br(K)[n] is cyclic. Hence every element of $c$ in Br(K)[n] (resp. every central simple algebra $A$ over $K$) is equivalent to a cyclic algebra split by $L_u$. So we can associate to $c$ (resp. $A$) its invariant and we get an isomorphism

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

The discrete logarithm in Br(K)[n] would be trivial if we could compute invariants.
The application of the Tate-Lichtenbaum pairing leads to cyclic algebras split by ramified extensions.

Assume that $n \mid q-1$.
Take $L_n = K(\pi^{1/n})$ and $\tau \in G(L_n/K)$ with

$$\tau(\pi^{1/n}) = \zeta_n \pi^{1/n}.$$

Since $\pi$ is a norm element and $\tau$ acts trivially on the residue field of $K$ the class $c$ is determined by a triple

$$(L_n, \tau, \zeta_n^k).$$

Let $M_n$ be the composite of $L_n$ and $L_u$. It is a Galois extension with Galois group $< \tau, \phi_q >$.
To compute the invariant of $c$ we have to find a number $\ell$ such that

$$\inf_{M/L_n}(c) = inf_{M/L_u}((L_u, \phi_q^\ell, \pi_q)).$$

This can be worked out in an explicit way, and as result we see that again we have to compute a discrete logarithm in $\mathbb{F}_q^*$.

### 3.1.3 The Local-Global Relation

We go one step further and lift local fields to global fields.
Let $K$ be a global field, i.e. $K$ is either a finite algebraic extension of $\mathbb{Q}$ or a function field of one variable over a finite field $\mathbb{F}_q$.

#### Localization

Let $\mathfrak{p}$ be a non-archimedean place on $K$. Let $\tilde{\mathfrak{p}}$ be an extension of $\mathfrak{p}$ to $K_s$. Its decomposition group depends up to conjugation only on $\mathfrak{p}$ and is denoted by $G_\mathfrak{p}$. It will be identified with $G_{K_\mathfrak{p}}$, the Galois group of the completion of $K$ at $\mathfrak{p}$.
The set of all places of $K$ is denoted by $\Sigma_K$.
A $G_K$-module $M$ has (by restriction) a natural structure as $G_\mathfrak{p}$-module and so we have restriction maps

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

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

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

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

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

**Theorem 3.1.5** *Let $K$ be a global field and $n \in \mathbb{N}$ odd and prime to char$(K)$. Then the sequence*

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

*is exact.*

Trivial but useful is

**Corollary 3.1.6** *Let $T$ be a finite set of places of $K$. For each $\mathfrak{p} \in T$ let $A_{\mathfrak{p}}$ be a given simple algebra with center $K_{\mathfrak{p}}$ in* $\mathrm{Br(K_{\mathfrak{p}})[n]}$.
*Let $L/K$ be a cyclic extension of order $n$ with Galois group generated by $\tau$. Let $A = (L, \tau, c)$ be a cyclic algebra over $K$ such that*

$$A \bigotimes K_{\mathfrak{p}} \cong A_{\mathfrak{p}}$$

*for $\mathfrak{p} \in T$.*
*Then*

$$-\sum_{\mathfrak{p}\in T} \mathrm{inv}_{\mathfrak{p}}(\rho_{\mathfrak{p}}(A)) = \sum_{\mathfrak{p}\in\Sigma_K\setminus T} \mathrm{inv}_{\mathfrak{p}}((L_{\mathfrak{p}}, \tau^{h_{\mathfrak{p}}}, c^{h_{\mathfrak{p}}})$$

*with $G(L_{\mathfrak{p}}/K_{\mathfrak{p}}) =< \tau^{h_{\mathfrak{p}}} >$.*

**Remark 3.1.7** *For the existence of lifts $A$ of $A_{\mathfrak{p}}$ we need* existence theorems *for cyclic extensions of $K$ with* restricted *ramification, and such results are delivered by* global class field theory *(in an explicit way e.g. by CM theory).*

We use Corollary 3.1.6 in the following situation.
Let $\mathfrak{m}$ be an ideal in $O_K$, the ring of integers of $K$. We *assume* that there is a cyclic extension $L$ of odd degree $n$ of $K$ unramified outside of $T_{\mathfrak{m}}$, the set of places dividing $\mathfrak{m}$.
Let $\tau$ 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 $G(L/K)$, and $f_{\mathfrak{p}}$ so that

$$\tau^{f_{\mathfrak{p}}} = \phi_{\mathfrak{p}}.$$

For $a \in K^*$ define the cyclic algebra $A$ by $(L, \tau, a)$.Then

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

where $w_{\mathfrak{p}}$ is the normed valuation in $\mathfrak{p}$.
We use this as a test for the existence of cyclic extensions unramified outside of $\mathfrak{m}$.

**Proposition 3.1.8** *If there is a cyclic extension of $K$ of degree $n$ unramified outside of $\mathfrak{m}$ then the following holds:*
*For all $\mathfrak{p} \in \Sigma_K$ not dividing $\mathfrak{m}$ there are numbers $f_{\mathfrak{p}}$ such that for all elements $a_1, a_2 \in K^*$ prime to $\mathfrak{m}$ with $a_1^s \equiv a_2 \mod \mathfrak{m}$ we have*

$$\left( \sum_{\mathfrak{p} \notin T_{\mathfrak{m}}} (s \cdot w_{\mathfrak{p}}(a_2) - w_{\mathfrak{p}}(a_1)) f_{\mathfrak{p}} \right) \equiv 0 \bmod n$$

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

### 3.1.4 Application to Ring Class Numbers

Apply Proposition 3.1.8 to the following problem:
For $\mathfrak{m} < O_K$ compute the order $\varphi(\mathfrak{m})$ of the ring class group of $O_K$ with

module $\mathfrak{m}$, i.e. the order of the ideal class group of the order in $K$ with conductor $\mathfrak{m}$.
Define

$$K_{\mathfrak{m}} = \{a \in K^* \text{ with } \sum_{\mathfrak{p} \in T_{\mathfrak{m}}} \text{inv}_{\mathfrak{p}}((L, \tau, a)) = 0\}$$

for all cyclic extensions of $K$ with conductor $\leq \mathfrak{m}$.
A subset of $K_{\mathfrak{m}}$ are the elements $a$ in $K$ for which

$$w_{\mathfrak{p}}(a-1) \geq 1;\ \mathfrak{p} \in T_{\mathfrak{m}}.$$

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

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

has a non-trivial solution modulo $l$.

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

**Example 3.1.9** *Take $K = \mathbb{Q}$.*
*For $m \in \mathbb{N}$ the function $\varphi(m)$ is the classical Euler totient function. The global class field theory of $\mathbb{Q}$ is completely determined by the theorem of Kronecker and Weber.*
*We now assume that the prime number $\ell$ divides $\varphi(m)$ and consider a global algebra $A$ of the form $A = (L/K, \sigma, a)$ corresponding to this extension with $a$ prime to $m$. To be explicit we choose a random number $1 < k < m$ and assume that the exponentiation of $m$-th roots of unity by $k$ induces $\sigma$ on $L$. For $a = \prod p^{n_p}$ the theorem by Hasse–Brauer–Noether leads to a relation of the form*

$$\sum_{p \mid m} \text{inv}_p A + \sum_{\gcd(p,m)=1} n_p f_p \equiv 0 \bmod \ell \tag{3.1}$$

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

$$\sum_{\gcd(p,m)=1} n_p f_p \equiv 0 \bmod \ell. \tag{3.2}$$

### 3.1.5 Computation of the Classical DL

Let $\mathfrak{m} = \mathfrak{p}_0$ be a prime ideal of the ring of integers $O_K$ of $K$ with residue field $\mathbb{F}_q$. We assume that $\ell$ is a prime number dividing $q-1$ and that there is a cyclic extension of $K$ of degree $\ell$ totally ramified at $\mathfrak{p}_0$. For instance this is the case if the class number of $K$ is prime to $\ell$.
Let $\zeta$ and $\zeta_1$ be two $\ell$-th roots of unity which are the reduction modulo $\mathfrak{p}_0$ of two integers $a$ and $a_1$ in $O_K$.

**Proposition 3.1.10** *Let* $k \in \mathbb{Z}$. *Then* $\zeta^k = \zeta_1$ *if and only if*

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

Recall that we have seen already that the discrete logarithm in Brauer groups of local fields is (at least if we deal only with cyclic algebras) transferred to the discrete logarithm in their residue fields. Proposition 3.1.10 shows that we can compute the discrete logarithm in finite fields if we can compute the numbers $f_{\mathfrak{p}}$ at least for divisors of lifts of $\zeta$ and $\zeta_1$.

### 3.1.6 Description of cyclic extensions

How can one describe extension fields $L$ of global fields $K$ by objects defined over $K$?
A first answer is to use polynomials (maybe monic over the ring of integers $O_K$) which define $L$ and then the decomposition of these polynomials modulo the places of $K$ give all the information necessary for studying the arithmetic of $L$.

In practice this method is working only for small degrees of $L/K$ and definitely not for degrees of the size which occur in cryptography (e.g. $\ell \sim 10^{60}$)).
Alternatively we could try to compute for a given extension $L$ and a given prime $\mathfrak{p}$ of $O_K$ the number $f_{\mathfrak{p}}$.
If we would succeed we would have a very satisfying description of the arithmetic of $L$. It would be much finer than a description of the splitting behavior of primes in $L$ which alone characterizes $L$.

## 3.2 Index-Calculus in Global Brauer Groups

The results of the previous sections motivate the search for algorithms to determine the numbers $f_{\mathfrak{p}}$ which characterize the Frobenius automorphisms at places $\mathfrak{p}$ of $K$ related to cyclic extensions with conductor dividing an ideal $\mathfrak{m}$.
The method to do this is an index-calculus algorithm of the type one is used to see in algorithms for factoring numbers. To demonstrate the principle we take $K = \mathbb{Q}$ and so $\mathbb{F}_q = \mathbb{F}_p$.
The congruences (3.1) can be seen as system of linear equations relating the indeterminates $f_p$ for $p$ prime to $m$ and $\mathrm{inv}_p(A)$ for $p \mid m$. 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 big enough such that many elements $a$ can be found, and small enough to make linear algebra feasible.
The key concept is the notion of smooth numbers.
Let $B$ be a natural number.

**Definition 3.2.1** *A number $n \in \mathbb{N}$ is $B$-smooth if all prime numbers dividing $n$ are bounded by $B$.*

There are results from analytic number theory, eg. the Theorem of *Canfield-Erdös-Pomerance* which predict the probability to find smooth numbers.

**Example 3.2.2** *We define the subexponential function*
$L_x(\alpha, c) := exp(c \log(x)^{\alpha} \cdot \log\log(x)^{1-\alpha})$.
*The heuristic probability to find a smooth number with smoothness bound $B = L_x(1/2, c)$ in $[1, x]$ is $L_x(1/2, -1/2c)$.*

*If we want to find $B$ such numbers we have (again heuristically) to make $\sim L_x(1/2, \frac{2c-1}{2c})$ trials.*

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

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

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

*Assume* that for $\delta \in L$ both

$$a_1(\delta) \text{ and } a_2(\delta)$$

are $B$-smooth. Then we get a relation in which the coefficient of $f_p$ is $\neq 0$ only if $p$ is in the factor base. To find such $\delta \in L$ we can use sieves.

**Relations Arising from Quadratic Fields** We are interested in cyclic extensions $L$ of odd degree $\ell$ with conductor $m$ over $\mathbb{Q}$ and generator $\tau$ of $G(L/\mathbb{Q})$. The composite of such an extension with a quadratic extension field $K$ of $\mathbb{Q}$ has the same properties. So we can use cyclic algebras over $K$ given by a triple $A = (L/K, \tau, c)$ with $c \in K^*$.
For places $\mathfrak{p} \in \Sigma_K$ we have numbers $f_\mathfrak{p}$ 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 $\mathfrak{p} \mid p$. 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 $\ell$ we get that there is an cyclic extension cyclic of degree $\ell$ 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.

Take odd $\epsilon \in \mathbb{N}$ and $d \in \mathbb{Z} \setminus \mathbb{Z}^2$, $\gcd(d, \epsilon) = 1$ and $d \equiv \epsilon^2 \bmod m$. 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

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

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

Straightforward calculations yield

$$\sum_{p \text{ split in } K_d} w_p(\epsilon^2(1+u^2)^2 - (1-u^2)^2 d)$$

$$\equiv w_p(2\epsilon u)) f_p \mod \ell.$$

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

## 3.3 Construction of Elements in the Brauer Group

We are looking for more methods to construct elements in the Brauer group of number fields. The theoretical background for the success (or failure) is the duality theorem of Tate-Poitou.

### 3.3.1 Pairings with Dirichlet Characters

This method is due to **Huang-Raskind**.
It uses the duality between $\mathbb{Z}/n$ and $\mu_n$ and leads to well known "symbols"

in class field theory.
$H^1(G_K, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_K, \mathbb{Q}/\mathbb{Z})$ consists of Dirichlet characters of $K$.
We use the Kummer sequence for the multiplicative group and map $K^*$ to $H^1(G_K, \mu_n)$ (in fact, this is the original "Kummer theory"). The cup product yields a pairing

$$K^* \times \mathrm{Hom}(G_K, \mathbb{Z}/n) \to \mathrm{Br(K)}$$

sending $(a, \chi)$ to $< a, \chi >$.
By restriction we get local pairings (local symbols) and of course there is a reciprocity law for the invariant. We look at the Dirichlet characters as test functions to get information about discrete logarithms at various places.
Hence we are interested in finding Dirichlet characters with prescribed ramification (see discussion above). The answer to this is given by the Tate-Poitou duality theorem.
One nice application is: Let $K$ be a real quadratic field.
Under suitable conditions one proves the existence of a Dirichlet character ramified at two given places. Applying $<,>$ to a unit of $K$ one gets relations between the discrete logarithm at the two places. For details I refer to: Ming-Deh Huang and Wayne Raskind: Signature Calculus and Discrete Logarithm Problem, ANTS 2006.

### 3.3.2 Pairings with Principal Homogenous Spaces

Of course, one can try to do analogue things with abelian varieties instead of using the multiplicative group.
Hence one uses elements in $H^1(G_K, A(K_s)$ as test functions, and of course, the pairing is the Tate-Lichtenbaum pairing.
The situation is much more rigid. The duality theorem of Tate-Poitou predicts that there are not many suitable elements and our local description tells us that we get "very sparse" relations.
Assume that we have a Jacobian variety $A$ (e.g. an elliptic curve) over a global field $K$ with a point $P \in A(K)$ and that we have an element

$$\varphi \in H^1(G_K, A(K_s))[n].$$

Then $T_n(P, \varphi)$ is an element in $Br(K)[n]$ which is very sparse.
At all $\mathfrak{p}$ prime to $n \cdot cond(A)$ at which $\varphi$ is unramified or at which the reduction

of $P$ lies in $nA(K_\mathfrak{p})$ the value of the local pairing is 0. Hence

$$\sum_{\mathfrak{p}\in S} inv_\mathfrak{p}(T_n(P,\varphi)) = 0$$

with

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

### 3.3.3 Cassel's Pairing

One of the complications occurring when we use $\varphi \in H^1(G_K, A(K_s))[n]$ for testing is that $\varphi$ becomes trivial at many places.
This has a geometric interpretation. In a canonical way $\varphi$ corresponds to a principal homogeneous space $V_\varphi$ attached to $A$ which becomes isomorphic to $A$ over any field $L$ with $V_\varphi(L) \neq \emptyset$.
So its restriction at $\mathfrak{p}$ becomes trivial iff $V_\varphi$ has a $K_\mathfrak{p}$-rational point.
In the extreme case this happens at all places. Then $\varphi$ is an element of the Tate-Shafarevich group $TS(A)$.
Hopefully this group is finite. But certainly its order cannot be bounded if we vary $A$.
For elliptic curves Heegner points and the corresponding Kolyvagin-Euler-systems are good candidate for yielding elements in $TS(A)$.
***Cassels*** has used the Tate-Shafarevich group to define a very interesting skew symmetric pairing which is non-degenerate iff $TS(A)$ is finite. And then the order is a square! Cassels' pairing is really a global object. To define it one has to leave the world of Brauer groups (which are good for local duality) and go to the second cohomology of idele classes, which is isomorphic to $\mathbb{Q}/\mathbb{Z}$ again.
Ideles (and so cocycles) have entries at all places of $K$ coming from local fields, and so as result of the pairing we find again a collection of elements in local Brauer groups. But now the sum of invariants will not be 0 in general, but we are not far away!
So, besides of the great importance of Cassels' pairing for theory it could be an interesting object for cryptography, and I refer to ongoing work done by *K. Eisenträger, D. Jetchev and K.Lauter.*