Contents

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 $\mathbb{F}_q$.

Take **O the ring of holomorphic functions**

of an (affine) curve C_O defined over a finite field $\mathbb{F}_q$ with q elements.

1.1 Picard Groups

1.1.1 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.

Completion

There is a unique projective irreducible regular curve C with function field F containing $\widetilde{C_O}$ as affine part.

1.1.2 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 1.1 $T_\infty = \overline{C}(K_s)\backslash\overline{\widetilde{C_O}}(K_s)$ *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_∞ and S into themselves.
We assume that there is a K-rational point P_∞ in T_∞.

1.1.3 Conductor

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 ordinary double points.
Hence $\mathfrak{m}_{C_O} < \tilde{O}$ corresponds to $\prod_{P \in S} m_P$.

1.1.4 Ideal Classes

Definition 1.2 *Let $R \subset \overline{F}$ be an integrally closed subring,$f \in \overline{F}$.*
Then

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

For $H \subset \overline{F}$ we define

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

$(\overline{F}^*)_R$ form a group in a natural way which is the group of principal ideals of R denoted by $Princ_R$.
The group of invertible ideals in R is denoted by I_R. The Picard group Pic_R is defined by the exact sequence

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

Example 1.3 *Take for R the ring of holomorphic functions on $C(K_s) \backslash P_\infty$ which is equal to $\overline{O}_{P_\infty}$. For $P \in C(K_s)$ let v_P be the normalized valuation with valuation ideal $m_P < R$.*
Then

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

and $\mathrm{Pic}_{\overline{O}_{P_\infty}}$ *is isomorphic to the divisor class group of degree* 0, $\mathrm{Pic}^0_{\overline{C}}$ *of* $\overline{C}$.

Proposition 1.4 *We have the exact sequence of G_K-modules*

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

with

$$\mathcal{C}_{T_\infty} =< m_P;\ P \in T \setminus P_\infty > \subset I_{\overline{O_{P_\infty}}}$$

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

Next we want to describe $\mathrm{Pic}(\overline{O})$.
Let 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 $\overline{F^1_S}$ 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

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

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 $\sigma(\ldots, x_P, \ldots) = (\ldots, \sigma(x_P)_{\sigma(P)}, \ldots)$ and $\Delta(K_s^*)$ is the diagonal embedding.

A more geometric way to express this is

Proposition 1.5 *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*

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

Remark 1.6 *The isomorphism class of $\mathcal{T}_S$ is determined by its character group X, and this group is determined by the set S as G_K-set.*
So the Proposition 1.5 (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.

1.2 Pic and Jacobians

Using that $\mathrm{Pic}^0_{\overline{C}} \cong_{G_K} J_C(K_s)$ and putting all pieces together we get

Theorem 1.7 *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

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

Remark 1.8 *All the material of this section is to be found in*
J-P. Serre: Corps de classes et groupes algébriques.

2 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 Pic_O.
But in order to apply duality theorems as presented in the first lecture we should better switch to local fields as ground fields always taking care that this lifting is easy and that we do not loose fast operations.

Remark 2.1 *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.

2.1 Lifting the Galois Group

The maximal unramified extension of K is denoted by K_{nr}. There is a canonical lift (easily computable) of the Frobenius automorphism ϕ_q to K_{nr} also called the Frobenius automorphism and denoted by ϕ_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 π is an element in K with $w_p(\pi) = 1$. (Such elements are called *uniformizing elements* of K.) So L_n/K_{nr} is cyclic. We choose a primitive n-th root of unity ζ_n and denote by τ_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 ϕ_q and τ_n.

If we assume that $\zeta_n \in K$, or equivalently, that $n \mid (q-1)$ then $K(\pi^{1/n})$ is Galois over K and τ_n and ϕ_q commute and the maximal tamely ramified extension of K whose Galois group has exponent dividing n is the subfield of L_n fixed by ϕ_{q^n}.

Proposition 2.2 *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.

2.2 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 $\mathfrak{m}_O = \sum_{P \in S} P$ and the corresponding desingularized curve $\tilde{C}$ embedded in the projective nonsingular curve C. The set T_∞ was defined as $C(\overline{\mathbb{F}_q}) \setminus \tilde{C}(\overline{\mathbb{F}_q})$.

We denote by g_0 the genus of C.

We state the following (rather elementary) facts from the reduction theory of curves resp. abelian varieties.

Theorem 2.3 *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 is a semi-abelian group scheme over spec(O_K), the ring of integers of K, whose connected component has as special fiber the generalized Jacobian of $C_O \cup T_\infty$.*
- *The set ${T_\infty}^l$ is G_K-invariant. It is mapped bijectively to T_∞.*

2. *Denote by O^l the ring of holomorphic functions on $C^l \backslash {T_\infty}^l$. For all numbers n prime to q we get*

   - $\mathrm{Pic}_{O^l}/[n]\mathrm{Pic}_{O^l}$ *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*

     $$1 \rightarrow \mathcal{T}_S^l(U_K)/(\mathcal{T}_S^l(U_K))^n \rightarrow$$

     $$\mathrm{Pic}_{O^l}/[n]\mathrm{Pic}_{O^l} \rightarrow \mathrm{Pic}_{\tilde{O}}/[n]\mathrm{Pic}_{\tilde{O}} \rightarrow 0$$

     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*

   $$0 \rightarrow (\mathcal{C}_{T_\infty}/[n]\mathcal{C}_{T_\infty})^{G_K} \rightarrow$$

   $$J_{C^l}(K)/[n]J_{C^l}(K) \rightarrow \mathrm{Pic}_O/[n]\mathrm{Pic}_O \rightarrow 0.$$

   Moreover there is an isogeny φ 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 $\varphi(J_C(K))/[n]\varphi(J_C(K))$.*

Remark 2.4 *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.

Theorem 2.3 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 nonsingular (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. Instead of proving the statements of Theorem 2.3 we give the simplest example for these curves.

Example 2.5 *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_∞ *corresponds to the point* $(0, 1, 0)$ *on the projective curve*

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

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* Pic_O *is isomorphic to* $\mathbb{F}_q^*$*.*

Let K be a local field with residue field $\mathbb{F}_q$ and uniformizing element π. Then

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

is the affine part of an elliptic curve with reduction equal to C. It is a Tate curve with period Q with $w_{\mathfrak{p}}(Q) = 1$. The group of rational points $E(K)$ is isomorphic to $K^*/ < Q > \cong U_K$, and all the assertions of the Theorem 2.3 can be checked immediately.

3 The Lichtenbaum Pairing

We return to a general field K.
As promised in the first lecture I begin with explicit definitions of relevant cohomology groups.

3.1 Low Cohomology groups

Let G be a profinite group, i.e. G is the projective limit of its finite quotient groups.
Being a projective limit of finite groups G carries in a natural way the Krull topology and is compact in this topology. As always we tacitly assume that all maps are continuous.
Let M be a G-module.

Definition 3.1 *1.*

$$H^0(G, M) = M^G$$

2. $C^1(G, M)$ *consists of* 1*-cocycles*

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

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

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

$B^1(G, M)$ *consists of* 1*-coboundaries*

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

for which there exists an element $m \in M$ *with*

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

for all $\sigma \in G$.

The first cohomology group of M *is*

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

3. 2*-cocycles are maps*

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

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

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

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

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

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

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

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

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

Let U be a closed subgroup of G.
By restricting cocycles one gets restriction homomorphisms

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

Assume that U is a normal subgroup of G and that M_U is a G/U-module contained in a G-module M. By composition with the quotient map

$$\pi_U : G \to G/U$$

one gets the *inflation maps*

$$\mathrm{inf}_{U/G} : H^n(G/U, M_U) \to H^n(G, M).$$

is called the *inflation map*.

The inflation and the restriction maps are related. Very useful is the sequence

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

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

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

is injective.

Example 3.3 *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

$$Br(K) = H^2(G_K, K_s^*) =$$

$$\bigcup_L \inf_{G_L/G_K} H^2(G(L/K, L*)$$

where L runs over all finite Galois extensions of K.

3.1.1 The Boundary Maps

We assume that

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

is an exact sequence of G-modules. For $n \geq 0$ the maps α resp. β induce (by composition with cocycles) in a natural way homomorphisms
$\alpha^n : H^n(G, A) \to H^n(G, B)$ resp.
$\beta^n : H^n(G, B) \to H^n(G, C)$.
There are homomorphisms

$$\delta^n : H^n(G, C) \to H^{n+1}(G, A)$$

such that the infinite sequence

$$\ldots H^n(G, A) \overset{\alpha^n}{\to} H^n(G, B) \overset{\beta^n}{\to} H^n(G, C)$$

$$\overset{\delta^n}{\to} H^{n+1}(G, A) \overset{\alpha^{n+1}}{\to} H^{n+1}(G, B) \to \ldots$$

is exact.

We shall need the connecting homomorphisms δ^n only for $n = 0, 1$.

Definition of δ^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 δ^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 ζ is a cocycle, in A.

Take $\delta^1(c)$ as class of $\delta(\sigma, \tau)$ in $H^2(G, A)$.

3.2 Definition of the Pairing

We continue to work with rings O resp. $\overline{O}$ as above. In view of Theorem 2.3 we take $S = \emptyset$ and hence

$$\mathrm{Pic}_{\overline{O}} \cong_{G_K} J_C(K_s).$$

3.2.1 The complete Case

We assume that $T_\infty = \{P_\infty\}$ and so $\overline{O} = O_{P_\infty}$. We use the exact sequence

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

and get as part of the long exact cohomology sequence

$$H^1(G_K, I_{\overline{O}}) \rightarrow H^1(G_K, \mathrm{Pic}_{\overline{O}}) \xrightarrow{\delta^1}$$

$$H^2(G_K, (\overline{F})).$$

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 $H^1(G_K, I_{\overline{O}}) = 0$.
So the map δ^1 is injective. As described above 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 with a (chosen) representative $D(\sigma) \in I_{\overline{O}}$.
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 $(f(\sigma, \tau))$ and $\delta^1(c)$ is the cohomology class of the $2-cocycle$

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

We have some choices. For instance we can change $D(\sigma)$ by a principal ideal. So for a given ideal $A \in I_O$ we can and will choose $D(\sigma)$ 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

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

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 lecture (*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

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

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

Definition 3.4 *To define the* ***Lichtenbaum pairing***

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

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 $\zeta(\sigma,\tau) := Q(\sum z_P \cdot P, f(\sigma,\tau))$.

Example 3.5 *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 $\zeta(\tau^i)$.*
It follows 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 $D(\tau^j) = \sum_{k=0\ldots j-1} \tau(D)$.
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.
Then $\delta^1(c)$ is presented by the cocycle

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

and

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

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

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

and

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

This is an element in $H^2(G_K, K_s^*)$ *corresponding to a cyclic algebra(see third lecture).*

3.3 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 3.6 *(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.

3.3.1 The General Case

A first application is the definition of the Lichtenbaum pairing when T_∞ 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 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 $\mathrm{Pic}_O = \varphi(\mathrm{Pic}_{O_{P_\infty}})$.

Secondly the map from $\bar{F}$ to $Princ_{\overline{O}}$ has as kernel the group of functions U_T.

Hence we cannot evaluate the image of $\delta^1 : H^1(G_K, \mathrm{Pic}_{\overline{O}}) \to H^2(G_K, Princ_{\overline{O}})$ at points on $C \setminus T_\infty$.

To overcome these difficulties we have to apply an isogeny ψ 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 3.7 *The Lichtenbaum pairing induces a pairing, also denoted by* T_L *from* $\mathrm{Pic}(O) \times \psi^1(H^1(G_K, \overline{O}))$ *to* $H^2(G_K, K_s^*)$.

4 The Tate-Lichtenbaum Pairing over Finite and Local Fields

Theorem 4.1 *Let K be a local field. Then the Tate-Lichtenbaum pairing T_n is nondegenerate.*

Corollary 4.2 *Assume that D_n is a cyclic subgroup of $J_{C^l}(K)/[n]J_{C^l}(K)$. 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 $T_n \mid_{D_n \times \{c\}}$.

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 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

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

We need ramified extensions and so we have to adjoin ζ_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".

We extend $\mathbb{F}_q$ to $\mathbb{F}_{q^d}$ and K to $K(\zeta_n) := K_n$.
Let L be "the" ramified extension of degree n of K_n,eg. take $L = K_n(\pi_K^{1/n})$, and take τ as generator of $G(L/K_n)$. We can use Example 3.5. In particular we get for a $\zeta \in c \in H^1(G_K, J_C(K_s))[n]$ that $\zeta(\tau)$ modulo v_{K_n} is a point of order n. Hence we can assume that $P = \zeta(\tau)$ has order n and that it is contained in $J_C(K_n)$.

Identify (depending on the choice of τ)
$H^1(G_K, J_C(K_s)[n])$
with
$Hom(G_K, J_C(K_s)[n])$.
Take $\varphi \in Hom(G_K, J_C(K_s)[n])$ with $\varphi(\tau) = P$; $P \in J_C(K_n)[n]$ and
$\pi_q(P) = \chi_n P$
where χ_n is the cyclotomic character applied to π_q.
Let $nP = (f_P)$ and assume a representative of $Q \in J_C(K)$ is chosen such that $f_P(Q)$ is defined.
Then

$$T_n(P, Q)$$

is the class of cyclic algebra corresponding (wrt. τ) 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.

4.2 The Tate-Lichtenbaum Pairing over Finite Fields

In the general case we use the results stated in Theorem 2.3 we get

Corollary 4.3 *The discrete logarithm in ideal classes of rings of holomorphic functions of affine curves C over finite fields $\mathbb{F}_q$ is transferred to the Brauer group of local fields K with residue field $\mathbb{F}_q$ by the Tate-Lichtenbaum pairings T_n.*

Remarks 4.4 *1. By lifting curves from finite fields to local fields we get the nontriviality of cohomology groups involved in the pairings as well as a smoothing of the curve. We do not loose information about the torus part of the ideal class groups. The reason is that we have ramified extensions at hand.*

2. Of course the practical value of Corollary 4.3 depends on two assumptions: the pairing T_n has to have low computational complexity.
The reason is that only in this case we have ramified extensions cyclic of degree n defined over K. The second assumption will be discussed in the following sections.

In the case that C has no singularities we can reduce the T_n-pairing given in Subsection 4.1 and get

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

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.

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

$$J_C(K)/nJ_C(K)$$

to the discrete logarithm in

$$Br(K)_n$$

with the costs

$$O(log(\mid \mathbb{F}_{q^k}) \mid).$$

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 $g > 1$ 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 ($T.Lange$).