Lecture 1: Introduction/Overview

Idea: $G_K = \mathrm{Gal}(\overline{K}^{\mathrm{s}}|K)$, K a field, $\overline{K}^{\mathrm{s}}$ a separable closure of K, (resp. $\pi_1^{\text{ét}}(X) = \pi_1^{\text{ét}}(X, \overline{x})$, X algebraic variety over base S, geometric point $\overline{x} : \mathrm{Spec}(\overline{K}^{\mathrm{s}}) \to X$,) gives information on K (resp. X)

Good ('anabelian'): isomorphism type of K (resp. X) 'obtainable'

Even better: object isomorphic to K (resp. X) 'constructible' from G_K (resp. $\pi_1^{\text{ét}}(X)$)

example 0: G_K trivial $\Leftrightarrow$ K separably closed

example 1: X smooth projective curve over $\mathbb{C}$. Then, by [1, Corollaire XII.5.2] we have

$$\pi_1^{\text{ét}}(X) = \widehat{\pi_1^{\text{top}}(X(\mathbb{C}))}^{\text{prf.}} \approx \widehat{\left\langle \alpha_1, \ldots, \alpha_g, \beta_1, \beta_2, \ldots, \beta_g \mid \prod_{i=1}^{g} [\alpha_i, \beta_i] = 1 \right\rangle}^{\text{prf.}} .$$

Hence, $\pi_1^{\text{ét}}(X)$ encodes only the topological genus g.

More interesting cases: Let us look at $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and related objects. (One can replace $G_{\mathbb{Q}}$ with G_K, K a number field, in the following discussion.)

example 2:

Theorem 1 (Artin 1924 [2])**.** *$K \subset \overline{\mathbb{Q}}$ a subfield. Then, G_K is non-trivial finite $\Leftrightarrow$ $\exists \iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{R}}$ such that $K = \iota^{-1}(\mathbb{R})$ $\Leftrightarrow$ $\exists$ archimedean place v of $\overline{\mathbb{Q}}$ such that $K = \overline{\mathbb{Q}}^{D_v}$ ($D_v = \mathrm{Stab}_{G_{\mathbb{Q}}}(v)$ decomposition group).*

Proof. See Section 1.8. □

Corollary 1. *The decomposition groups of archimedean places are the finite non-trivial closed subgroups of $G_{\mathbb{Q}}$.*

Recall (for now): a place of K is an equivalence class of absolute values on K.

Write $\mathcal{P}(K)$ for the places of K. Note that $\mathcal{P}(\overline{\mathbb{Q}}) = \varprojlim_{K \subseteq \overline{\mathbb{Q}} \text{ number field}} \mathcal{P}(K)$.

$\mathcal{P}_f(K)$ = non-archimedean places, $\mathcal{P}_\infty(K)$ = archimedean places

Question: What about non-archimedean places?

Theorem 2 (Neukirch 1969 [25])**.** *$K \subset \overline{\mathbb{Q}}$. Then, ($G_K$ is solvable, has l-cohomological dimension 2 for any prime l and either there exists a prime $p \neq 2$ such that the maximal pro-p quotient $G_k(p)$ of G_K is a free pro-p group of rank 2 or $G_k(2)$ is a Demuskin group of rank 3) $\Leftrightarrow$ $G_K \approx \mathrm{Gal}(\overline{L}/L)$ ($L/\mathbb{Q}_p$ finite extension) $\Leftrightarrow$ $\exists \iota : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ such that $\iota^{-1}(\mathbb{Q}_p) \subseteq K$ $\Leftrightarrow$ $\exists!$ $v \in \mathcal{P}_f(\overline{\mathbb{Q}})$ such that K is finite extension of $\overline{\mathbb{Q}}^{D_v}$.*

Corollary 2. *$\exists$ group-theoretic characterization of decomposition subgroups of $G_{\mathbb{Q}}$.*

Tools for proof of Theorem 2:

uniqueness: $D_v \cap D_w = \{1\}$ for any $v \neq w \in \mathcal{P}(\overline{\mathbb{Q}})$. (Hence, $\overline{\mathbb{Q}}^{D_v} \cdot \overline{\mathbb{Q}}^{D_w} = \overline{\mathbb{Q}}$.)

existence: - class field theory, - Brauer groups $\mathrm{Br}(K) = H^2(G_K, \overline{K}^*)$, - Hasse principle ($K$ a number field):

$$1 \to \mathrm{Br}(K) \to \sum_{v \,\in\, \mathcal{P}(K)} \mathrm{Br}(K_v) \to^{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 1,$$

- structure of absolute Galois groups of local fields

1.1 The anabelian geometry of finitely generated fields

Theorem 3 (Neukirch 1969 [25], Uchida [47])**.** *K, L number fields. Then, $\Phi : G_K \to G_L$ is an isomorphism $\Rightarrow$ $\exists!$ $\phi : \overline{L}^{\mathrm{s}} \to \overline{K}^{\mathrm{s}}$ such that $\Phi(g) = \phi^{-1} g \phi$. In particular, $K \approx L$ and*

$$\mathrm{Isom}(L, K) \to \mathrm{Isom}(G_K, G_L)/\,\mathrm{Inn}(G_L),$$

where for $\sigma : L \to K$ we choose a lifting $\overline{\sigma} : \overline{L}^{\mathrm{s}} \to \overline{K}^{\mathrm{s}}$. This induces $\overline{\sigma}^* : G_K = \mathrm{Gal}(\overline{K}^{\mathrm{s}}|K) \to \mathrm{Gal}(\overline{L}^{\mathrm{s}}|L) = G_L$, $\varphi \mapsto \overline{\sigma}^{-1} \circ \varphi \circ \overline{\sigma}$, unique up to inner automorphisms of G_L.

Sketch of proof:

(1) Theorems 1 and 2 give a bijection between $\mathcal{P}(\overline{K}^{\mathrm{s}}) \approx \mathcal{P}(\overline{L}^{\mathrm{s}})$.

(2) From this, deduce a correspondence $\mathcal{P}(K) \approx \mathcal{P}(L)$.

(3) Show that the primes splitting completely in $L/\mathbb{Q}$ and $K/\mathbb{Q}$ agree.

(4) Assume L, K normal for simplicity: Use Cebotarev's Theorem.

Generalizations:

(1) (Neukirch 1969 [24]) In Theorem 12 we can replace the isomorphism $\Phi : G_K \to G_L$ by an isomorphism $G_K^{\text{max.solv.}} \to G_L^{\text{max.solv.}}$, where $G^{\text{max.solv.}}$ denotes the maximal solvable quotient of G.

(2) (Uchida 1977 [48]) function fields (transcendence degree 1 over finite field)

(3) (Pop 1995 [31, 32, 33, 44]) finitely generated fields (i.e. fields that are finitely generated over their prime fields)

1.2 Some anabelian yoga (after Grothendieck,...)

Want: precise notion of anabelian categories to talk about above results.

Caveat: The following is only correct for bases $S \to \mathrm{Spec}(\mathbb{Q})$. Otherwise inseparability issues.

A subcategory $\mathcal{A} \subset \mathrm{Sch}_{S,\text{conn.}}$ is S-anabelian if

(1) $\forall X, Y \in \mathrm{obj}(\mathcal{A}) : \mathrm{morph}_{\mathcal{A}}(X,Y) = \mathrm{Isom}_{\mathrm{Sch}_S}(X,Y)$

(2) $X \mapsto \pi_1^{\text{ét}}(X)$ induces fully faithful (covariant) functor $\mathcal{A} \to \mathcal{G}$, $\mathrm{obj}(\mathcal{G})$ = profinite groups with augmentations $G_2 \to \pi_1^{\text{ét}}(S)$, $\mathrm{morph}(G_1, G_2) = \mathrm{Isom}_{\pi_1^{\text{ét}}(S)}(G_1,G_2)/\,\mathrm{Inn}(\ker(G_2 \to \pi_1^{\text{ét}}(S)))$.

Above (Pop): Finitely generated fields (at least those of characteristic 0 with our notations) form an anabelian category over $\mathrm{Spec}(\mathbb{Z})$.

Conjecture 1 (Grothendieck 1983 [9])**.** *Let K be a number field. Then, hyperbolic curves over K form an anabelian category over* $\mathrm{Spec}(K)$.

hyperbolic = smooth, geometrically connected, negative Euler characteristic $\chi = 2-2g-n < 0$

Examples: $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, $E \setminus \{P\}$, hyperelliptic curves

Note: $\pi_1^{\text{ét}}(X)$ non-abelian iff $g(X) \geq 2$. This explains the term 'anabelian'.

Theorem 4 (Tamagawa 1997 [46])**.** *K number field. The affine hyperbolic curves over K form an anabelian category over* $\mathrm{Spec}(K)$.

Proof: hyperbolic curves over finite fields, Uchida's technique

Theorem 5 (Mochizuki 1996 [20])**.** *K number field. The hyperbolic curves over K form an anabelian category over* $\mathrm{Spec}(K)$.

Proof: builds upon Theorem 4.

Mochizuki was also able to prove the following unexpected result:

Theorem 6 (Mochizuki 1999 [22])**.** *$L/\mathbb{Q}_p$ local field. The proper hyperbolic curves over L form an anabelian category over* $\mathrm{Spec}(L)$.

Proof: uses p-adic Hodge theory

1.3 A model-theoretic analogue

Replace $G_K \approx G_L$ by $\mathrm{Th}(K) \approx \mathrm{Th}(L)$, where $\mathrm{Th}(K)$ is the first-order theory associated with K considered as a model of the standard theory of fields. (This means K and L have the same elementary type.)

Conjecture 2. *K, L finitely generated fields. Then,* $\mathrm{Th}(K) \approx \mathrm{Th}(L)$ *implies $K \approx L$.*

As of today, this conjecture is still open in general.[1] Many cases are proven in [34].

1.4 The 'anabelian' geometry of local fields

Given Theorem 6, is there a version of Theorem 12 for local fields $L/\mathbb{Q}_p$?
Hope: $G_K \approx G_L \Rightarrow K \approx L$. This is totally wrong.
In fact,

Theorem 7 (Jannsen-Wingberg [13], Diekert 1984 [5])**.** *Let $L/\mathbb{Q}_p$ a local field and assume $\sqrt{-1} \in L$ if $p = 2$. Then, $G_L \approx$ an explicit pro-finite (topologically) finitely generated group.*

For the precise description of G_L (if $p \neq 2$) see Theorem 7.5.14 in the web-version of [29].

Theorem 8 (Jarden-Ritter [14], Ritter 1978 [37], Jenkner [15])**.** *$L, K/\mathbb{Q}_p$ local fields and assume $\sqrt{-1} \in L$ if $p = 2$. Then, $G_L \approx G_K$ if and only if $L^0 = K^0$ (L^0, K^0 maximal abelian subfield of L, K) and $[L : \mathbb{Q}] = [K : \mathbb{Q}]$.*

Solution: Use more group-structure, namely the upper ramification filtration $\Gamma_K^{(r)}$ of G_K
Write $G_K^{\text{filt.}} = (G_K, (\Gamma^r_K)_{r\in\mathbb{Z}})$ and $\operatorname{Isom}_{\text{filt.}}$ for filtration-preserving isomorphism.

Theorem 9 (Mochizuki 1996 [21])**.** *K, L local fields. Then,*

$$\operatorname{Isom}(L, K) \to \operatorname{Isom}_{\text{filt.}}(G_K^{\text{filt.}}, G_L^{\text{filt.}})/\operatorname{Inn}(G_L)$$

is an isomorphism.

This result is the little brother of Theorem 6; its proof uses p-adic Hodge theory.

[1] The proof in [39] is incorrect, cf. [40].

Lecture 2: Introduction/Overview II

Recall (last time): S-anabelian categories $\mathcal{A} \subset \mathrm{Sch}_{S,\mathrm{conn.}}$, $\mathcal{A} \to \mathcal{G}$, $X \mapsto (\pi_1^{\text{ét}}(X) \to \pi_1^{\text{ét}}(S))$. The category $\mathcal{A}$ is anabelian iff

$$\mathrm{morph}_{\mathcal{A}}(X,Y) = \mathrm{Isom}_{\mathrm{Sch}_S}(X,Y) = \mathrm{Isom}_{\pi_1^{\text{ét}}(S)}(\pi_1^{\text{ét}}(X), \pi_1^{\text{ét}}(Y))/\,\mathrm{Inn}_{\pi_1^{\text{ét}}(Y)}(\ker(\pi_1^{\text{ét}}(Y) \to \pi_1^{\text{ét}}(S))).$$

No mention of base points. Well-defined by fact (3) below. (Here, a base point $\overline{s} \to S$ is chosen and all $\overline{x}, \overline{y}$ must map to $\overline{s}$.)

Question: What about homomorphisms/objects of different dimension?

1.5 The Section conjecture

Facts on $\pi_1^{\text{ét}}(X, \overline{x})$ (References: [1] or [45] (nice read))

Recall: étale = flat and unramified

(1) SGA I [1]: X connected algebraic variety, $\overline{x} \to X$ geometric point. Consider fiber functor $F_{(X,\overline{x})} : \mathbf{FEt}_{/X} \to \mathbf{Sets}$, $Y \mapsto \mathrm{Hom}_X(\overline{x}, Y) =$ 'point $y \in Y$ over x (= image of $\overline{x}$ in X) and $k(y) \to k(\overline{x})$'. Set $\pi_1^{\text{ét}}(X, \overline{x}) = \mathrm{Aut}(F)$. The group $\pi_1^{\text{ét}}(X, \overline{x})$ classifies the finite étale coverings of X in analogy to the topological fundamental group classifying topological coverings.

Fact: $\exists$ inverse system $(X_i, \overline{x_i}) \to (X, \overline{x})$, $i \in I$, of finite étale Galois coverings such that

$$\varinjlim \mathrm{Hom}_X(X_i, Y) = F_{(X,\overline{x})}(Y) \text{ (pro-representable).}$$

$\varprojlim (X_i, \overline{x_i}) =$ pro-étale universal covering $(\widetilde{X}, \widetilde{x})$ of $(X, \overline{x})$. $\pi_1^{\text{ét}}(X, \overline{x}) = \mathrm{Aut}_X(\widetilde{X}, \widetilde{x}) = \varprojlim \mathrm{Aut}_X(X_i)$. Hence, $\pi_1^{\text{ét}}(X, \overline{x})$ is pro-finite.

Example: $\mathbb{G}_{m,\mathbb{C}}$ has finite étale-coverings $\varphi_n : X_n = \mathbb{G}_m \to \mathbb{G}_m, t \mapsto t^n$, $n \geq 1$. $\widetilde{X}$ is the pro-scheme $\varprojlim_n X_n$ with morphisms $X_n \to X_m, t \mapsto t^{n/m}$, if $m|n$. From $\mathrm{Aut}_{\mathbb{G}_m}(\varphi_n : X_n \to \mathbb{G}_m) = \mu_n(\mathbb{C})$ we infer $\mathrm{Aut}_{\mathbb{G}_m}(\widetilde{X}) = \mu(\mathbb{C}) \approx \widehat{\mathbb{Z}}$. (Base-points 'do not matter' in this case by (2).)

(2) functoriality: Given $\overline{x} \to X$, $\overline{y} \to Y$, $f : X \to Y$, $f(\overline{x}) = \overline{y}$.

$X \to Y$ induces $\mathbf{FEt}_{/Y} \to \mathbf{FEt}_{/X}$, $Z \mapsto Z \times_Y X$. It is easy to see that

$$F_{(X,\overline{x})}(Z \times_Y X) = \mathrm{Hom}_X(\overline{x}, Z \times_Y X) = \mathrm{Hom}_Y(\overline{x}, Z) = Hom_Y(\overline{y}, Z) = F_{(Y,\overline{y})}(Z),$$

where in the second equation $f(\overline{x}) = \overline{y}$ is used. Get $\pi_1^{\text{ét}}(X, \overline{x}) \to \pi_1^{\text{ét}}(Y, \overline{y})$.

(3) different base points: If $\overline{x'}$ is another geometric point, then $\exists \gamma : F_{X,\overline{x}} \approx F_{X,\overline{x'}}$ (an étale path). This induces a map $\pi_1^{\text{ét}}(X, \overline{x}) \to \pi_1^{\text{ét}}(X, \overline{x'})$, $g \mapsto \gamma \circ g \circ \gamma^{-1}$. If $\gamma' : F_{X,\overline{x}} \approx F_{X,\overline{x'}}$ is another one, then $\gamma' \circ \gamma^{-1} \in \mathrm{Aut}(F_{X,\overline{x'}}) = \pi_1^{\text{ét}}(X, x')$. Conclusion: $\exists$ isomorphism $\pi_1^{\text{ét}}(X, \overline{x}) \to \pi_1^{\text{ét}}(X, \overline{x'})$, unique up to composing with an inner automorphism of $\pi_1^{\text{ét}}(X, \overline{x'})$.

Relative version: $(S, \overline{s})$ base, $\overline{x}, \overline{x'}$ over $\overline{s}$. $X \to S$. Can demand that $\gamma : F_{X,\overline{x}} \approx F_{X,\overline{x'}}$ induces the identity on pull-backs of $\mathbf{FEt}_{/S}$ (i.e., $F_{(X,\overline{x})}(Z \times_S X) = F_{(S,\overline{s})}(\overline{s}, Z) = F_{(X,\overline{x'})}(Z \times_S X)$ for all $Z \in \mathbf{FEt}_{/X}$). Uniqueness up to composing with $\mathrm{Inn}_{\pi_1^{\text{ét}}(X)}(\ker(\pi_1^{\text{ét}}(X) \to \pi_1^{\text{ét}}(S)))$ (instead of $\mathrm{Inn}(\pi_1^{\text{ét}}(X))$).

(4) homotopy exact sequence ([1, Théorème IX.6.1]: K a field, $X \to \mathrm{Spec}(K)$ an algebraic variety, $\overline{x} : \mathrm{Spec}(\overline{K}^{\mathrm{s}}) \to \overline{X} = X \otimes_K \overline{K}^{\mathrm{s}} \to X \to \mathrm{Spec}(K)$ a geometric point. Then,

$$\pi_1^{\text{ét}}(X/K) : 1 \to \pi_1^{\text{ét}}(\overline{X}, \overline{x}) \to \pi_1^{\text{ét}}(X, \overline{x}) \to \pi_1^{\text{ét}}(\mathrm{Spec}(K), \overline{x}) \approx G_K \to 1 \tag{1}$$

Back to above question: Recall

$$\mathrm{morph}_{\mathcal{G}}(G_1, G_2) = \mathrm{Isom}_{\pi_1^{\text{ét}}(S)}(G_1, G_2)/\,\mathrm{Inn}(\ker(G_2 \to \pi_1^{\text{ét}}(S))).$$

Try instead:

$$\mathrm{morph}_{\mathcal{G}}(G_1, G_2) = \mathrm{Hom}_{\pi_1^{\text{ét}}(S)}(G_1, G_2)/\,\mathrm{Inn}(\ker(G_2 \to \pi_1^{\text{ét}}(S))).$$

Given K be a number field (or a finitely generated field), X a hyperbolic curve over K, set $S = \mathrm{Spec}(K)$, $G_1 = \pi_1^{\text{ét}}(S) = G_K$, $G_2 = \pi_1^{\text{ét}}(X, \overline{x})$. Outcome:

$$X(K) = \mathrm{Hom}_{\mathrm{Spec}(K)}(\mathrm{Spec}(K), X) =^? \mathrm{Hom}_{G_K}(G_K, \pi_1^{\text{ét}}(X, \overline{x}))/\,\mathrm{Inn}(\ker(\pi_1^{\text{ét}}(X, \overline{x}) \to G_K)) =: \mathcal{S}_{\pi_1^{\text{ét}}(X/K)}.$$

Note that $\ker(\pi_1^{\text{ét}}(X, \overline{x}) \to G_K)) = \pi_1^{\text{ét}}(\overline{X}, \overline{x})$ by (1). Hence, $\mathcal{S}_{\pi_1^{\text{ét}}(X/K)}$ are $\pi_1^{\text{ét}}(\overline{X}, \overline{x})$-conjugacy classes of splittings of (1).

In analogy to Theorem 12, $\exists$ a canonical map $\kappa : X(K) \to \mathcal{S}_{\pi_1^{\text{ét}}(X/K)}$ (profinite Kummer map): Let $a : \mathrm{Spec}(K) \to X$. Choose $\overline{a} : \mathrm{Spec}(\overline{K}^{\mathrm{s}}) \to X$ over a. (3) above: $G_K = \pi_1^{\text{ét}}(\mathrm{Spec}(K), \overline{x}) \to \pi_1^{\text{ét}}(X, \overline{a})$. Relative version of (2): Get a homomorphism $G_K \to \pi_1^{\text{ét}}(X, \overline{x})$, unique up to inner conjugation with $\pi(\overline{X}, \overline{x})$ (not just $\pi(X, \overline{x})$).

Lemma 1. *κ is injective.*

Proof. Jacobian embedding, Mordell-Weil theorem, and factorization

$$\begin{tikzcd}
& A(K) \arrow[dl] \arrow[dr, hook, "\text{classical Kummer map } \delta"] & \\
\mathcal{S}_{\pi_1^{\text{ét}}(A/K)} \arrow[rr, "\sim"] & & H^1(K, \pi_1^{\text{ét}}(\overline{A}))
\end{tikzcd}$$

Recall (classical Kummer map):

$$1 \to A(\overline{K}^{\mathrm{s}})[n] \to A(\overline{K}^{\mathrm{s}}) \to^{[n]} A(\overline{K}^{\mathrm{s}}) \to 1$$

induces long exact sequence

$$1 \to A(K)[n] \to A(K) \to^{[n]} A(K) \to^{\delta_n} H^1(K, A(\overline{K}^{\mathrm{s}})[n]) \to \cdots$$

Take the inverse limit over n: as $\pi_1^{\text{ét}}(\overline{A}) = \varprojlim A(\overline{K}^{\mathrm{s}})[n]$ (as G_K-modules, [23, Section 18]) we get $\delta : A(K) \to H^1(K, \pi_1^{\text{ét}}(\overline{A}))$ with kernel $\bigcap_{n \geq 1} [n]A(K) = 0$ by Mordell-Weil (K-rational points finitely generated over $\mathbb{Z}$). □

$X(K) \approx \mathrm{im}(\kappa) \subset \mathcal{S}_{\pi_1^{\text{ét}}(X/K)} =$ diophantine sections

Conjecture 3 ((strong) Section Conjecture **sSC** [9])**.** *If X is projective, then all sections in $\mathcal{S}_{\pi_1^{\text{ét}}(X/K)}$ are diophantine.*

Problem: For non-projective hyperbolic curves, missing points (= cusps) give cuspidal sections - incorporate this!

Relation with Mordell Conjecture:

(1) Endow $\mathcal{S}_{\pi_1^{\text{ét}}(X/K)}$ with a topology; idea: finite étale covers $X' \to X$ induce maps $\mathcal{S}_{\pi_1^{\text{ét}}(X'/K)} \to \mathcal{S}_{\pi_1^{\text{ét}}(X/K)}$; their images form an open basis of the topology.

(2) Fact ([43, Proposition 97]): This topology is pro-finite, hence $\mathcal{S}_{\pi_1^{\text{ét}}(X/K)}$ is compact.

(3) Faltings' Theorem $\Rightarrow$ induced topology on $\mathrm{im}(\kappa) \subset \mathcal{S}_{\pi_1^{\text{ét}}(X/K)}$ is discrete. Idea: the sections associated with finitely many points can be easily separated. (Note, a closed subgroup of a profinite group is the intersection of all opens containing it.)

Open problems: Show this without Faltings' Theorem. Show that $\mathcal{S}_{\pi_1^{\text{ét}}(X/K)}$ is discrete.

Some variants:

(1) (Weak Section Conjecture **wSC**) X projective smooth curve of genus 2. Then, $\mathcal{S}_{\pi_1^{\text{ét}}(X/K)} \neq \emptyset \Rightarrow X(K) \neq \emptyset$.

(2) birational versions (i.e. splittings of

$$1 \to G_{K(X)\overline{K}^{\mathrm{s}}} \to G_{K(X)} \to G_K \to 1)$$

(3) Replace K by other fields (finitely generated, local fields)

(4) Describe diophantine sections for finite fields (Tamagawa [46])

(5) Push out by maximal pro-p quotient $\pi_1^{\text{ét}}(\overline{X}, \overline{x}) \to \pi_1^{\text{ét}^{pro-p}}(\overline{X}, \overline{x})$; the analogue of sSC is then wrong (Hoshi [12])

1.6 Evidence for the Section conjecture

(1) Stix [43], Harari-Szamuely [11]: There exist hyperbolic curves without sections. ⇒ **sSC** holds for them.

Problem: Prove for a single (!) curve that it has a finite but non-zero number of sections.

(2) Hain [10]: no universal sections; simplified:

Theorem 10. *Let k a number field (or a p-adic local field) $\mathcal{C} \to \mathcal{M}_g$ universal curve of genus $g \geq 5$ over k. $K = k(\mathcal{M}_g)$. $\overline{x} \to \mathcal{C} \otimes_k K$ a geometric point. Then,*

$$1 \to \pi_1^{\text{ét}}(\mathcal{C} \otimes_k \overline{K}^{\text{s}}, \overline{x}) \to \pi_1^{\text{ét}}(\mathcal{C} \otimes_k K, \overline{x}) \to G_K \to 1$$

does not split.

(3) Koenigsmann 2005 [17]: birational section conjecture over p-adic local fields.

Proof: model-theory

(4) Pop-Stix 2015+ [30]: valuative version of section conjecture over p-adic local fields. To wit, a reformulation of Conjecture (resp. its p-adic analogue) 3 is

Conjecture 4. *X projective, hyperbolic curve over a number field (resp. a p-adic local field) K. Then, for each section $s : G_K \to \pi_1^{\text{ét}}(X)$ there exists $v \in \mathcal{P}(K(\tilde{X}))$, $K(\tilde{X})$ the function field of the universal pro-étale cover $\tilde{X}$, such that*

- *$s(G_K) \subseteq D_v$ (D_v = decomposition group of v in $\pi_1^{\text{ét}}(X)$),*
- *$v|K$ is trivial, and*
- *$v|K(X)$ has residue field K.*

Indeed, the two last conditions give a rational point giving rise to D_v (and hence to s). As $D_v \approx G_K$ compatibly with the projection to G_K, the first condition actually implies $s(G_K) = D_v$.

The result of Pop and Stix is

Theorem 11. *X projective, hyperbolic curve over a p-adic local field K. Then, for each section $s : G_K \to \pi_1^{\text{ét}}(X)$ there exists $v \in \mathcal{P}(K(\tilde{X}))$, $K(\tilde{X})$ the function field of the universal pro-étale cover $\tilde{X}$, such that*

- *$s(G_K) \subseteq D_v$ (D_v = decomposition group of v in $\pi_1^{\text{ét}}(X)$).*

In summary, the image of every section is contained in the decomposition subgroup of a place $\mathcal{P}(K(\tilde{X}))$. However, this place does not need to come from a rational point as the other two conditions from Conjecture 4 are missing.

1.7 Not in this lecture

Bogomolov's birational anabelian program etc. ([4, 35])

Kim's anabelian geometry ([16])

Grothendieck-Teichmüller theory

1.8 Proof of Artin's Theorem

In this section, we provide Artin's original elementary proof for Theorem 1. A more modern proof using Galois cohomology can be found in [29, Theorem 12.1.7]. We do not need this theorem in the sequel so this section may be skipped.

Let K be a subfield of algebraic numbers such that $\overline{\mathbb{Q}}/K$ is a finite field extension.

Lemma 2. *Let $K \subset \overline{\mathbb{Q}}$ be a subfield of finite index. Then, $\overline{\mathbb{Q}} = K(\sqrt{-1})$.*

Proof. We assume first that $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is of prime order p; we claim that $p = 2$ and $\overline{\mathbb{Q}} = K(\sqrt{-1})$ in this case. Write ζ_{p^n} for an (arbitrarily fixed) primitive p^n-th root of unity in $\overline{\mathbb{Q}}$. As $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, we have $\zeta_p \in K$. By Kummer theory (e.g. [27, Theorem IV.3.2]), there exists $\alpha \in \overline{\mathbb{Q}}$ such that $\overline{\mathbb{Q}} = K(\alpha)$ and $\alpha^p \in K$.

In contrast, $\zeta_{p^2} \notin K$. To derive a contradiction, assume that $\zeta_{p^2} \in K$. The polynomial $f(X) = X^{p^2} - \alpha^p \in K[X]$ cannot be irreducible as it is of degree p^2. Writing $\beta \in \overline{\mathbb{Q}}$ for a p-th root of α, the roots of f are $\zeta_{p^2}^i \beta$ $(0 \leq i < p^2)$. None of these is in K, since otherwise $\beta \in K$ and $\alpha = \beta^p \in K$. Hence, f has an irreducible factor $g \in K[X]$ of degree p. This gives again a contradiction to $\alpha \notin K$ because $g(0) \in K$ is of the form $\zeta_{p^2}^i \beta^p = \zeta_{p^2}^i \alpha$ for some integer i.

We have $\overline{\mathbb{Q}} = K(\zeta_{p^3})$, which means that ζ_{p^3} must be a root of a polynomial $h \in K[X]$ with $\deg(h) = p$. In addition, $h \in \mathbb{Q}(\zeta_{p^3})[X]$ and hence the coefficients of h are contained in $F = K \cap \mathbb{Q}(\zeta_{p^3})$. Evidently, $[\mathbb{Q}(\zeta_{p^3}) : F] = p$ and thus $[F : \mathbb{Q}] = p(p-1)$. If p is odd, $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^3})/\mathbb{Q}) \approx (\mathbb{Z}/p^3\mathbb{Z})^\times$ is cyclic and $F = \mathbb{Q}(\zeta_{p^2})$ because both are subfields of index p in $\mathbb{Q}(\zeta_{p^3})$. This implies the contradiction $\zeta_{p^2} \in K$ and we infer that $p = 2$. Now, $\overline{\mathbb{Q}} = K(\zeta_{p^2}) = K(\sqrt{-1})$ as claimed.

Let now $\overline{\mathbb{Q}}/K$ be an arbitrary finite extension. We may assume that $\overline{\mathbb{Q}} \neq K(\sqrt{-1})$. Under this assumption, there exists a field $K(\sqrt{-1}) \subseteq F \subsetneq \overline{\mathbb{Q}}$ such that $[\overline{\mathbb{Q}} : F]$ is a prime number. By the above, this implies $\overline{\mathbb{Q}} = F(\sqrt{-1}) = F$ – a clear contradiction. □

It remains to establish that K is the decomposition field of a real place. For this, we have to prove an intermediate result first.

Lemma 3. *If α is a sum of squares $\sum_{i=1}^n \beta_i^2$, $\beta_i \in K$, then α is a square in K.*

Proof. We establish first that -1 is not a sum of two squares in K. For this, assume that $-1 = \gamma_1^2 + \gamma_2^2$ with $\gamma_i \in K$. As $\sqrt{-1} \notin K$, we have $\gamma_i \neq 0$. Consider now the polynomial

$$f(X) = (X^2 - \gamma_1)^2 + \gamma_2^2 \in K[X].$$

Its roots are $\pm\sqrt{\gamma_1 \pm \sqrt{-1}\gamma_2} \in \overline{\mathbb{Q}}$. Evidently, none of these roots can be contained in K as otherwise $\sqrt{-1} \in K$. In addition, $[\overline{\mathbb{Q}} : K] = 2$. Therefore, f has an irreducible factor g of degree 2 over K. The constant term $g(0) \in K$ is a product of two roots of f and thus equals $\pm(\gamma_1 \pm \sqrt{-1}\gamma_2)$ or $\pm\sqrt{\gamma_1^2 + \gamma_2^2} = \pm\sqrt{-1}$. However, none of these numbers can be contained in K; this contradiction yields that -1 is not a sum of two square in K.

We next show that each element $\beta \in K$ is either a square γ^2 or a negative square $-\gamma^2$ $(\gamma \in K)$. Indeed, β is a square in $\overline{\mathbb{Q}} = K(\sqrt{-1})$. This means $\beta = \gamma^2$ with $\gamma = \gamma_1 + \gamma_2\sqrt{-1}$, $\gamma_i \in K$. Squaring this equation, we obtain $\gamma_1\gamma_2 = 0$. If $\gamma_1 = 0$ then $\beta = -\gamma_2^2$ and if $\gamma_2 = 0$ then $\beta = \gamma_1^2$. This shows our claim.

For proving the lemma, it suffices to show that the sum of any two squares is a square itself. For this, let $\beta = \gamma_1^2 + \gamma_2^2$ with $\gamma_i \in K$. We may also assume that $\beta \neq 0$. It is shown above that there exists $\gamma \in K^\times$ such that β is either γ^2 or $-\gamma^2$. We infer

$$\left(\frac{\gamma_1}{\gamma}\right)^2 + \left(\frac{\gamma_2}{\gamma}\right)^2 = \pm 1.$$

As -1 is not a sum of two squares in K, it follows that $\beta = \gamma^2$ as claimed. □

We now conclude the proof of Artin's Theorem: If -1 is a sum of squares in K then -1 itself is a square in K by the above lemma. This would contradict $K(\sqrt{-1}) = \overline{\mathbb{Q}} \neq K$. We can hence apply Lemma 4 below to any number field $L \subset K$. It shows that $\mathcal{P}_\infty(L)$ contains a real place. Exhausting K by an ascending chain of number fields L_i, it follows that K itself has a real place and this finishes the proof of Artin's Theorem 1.

Lemma 4. *Let L be a totally imaginary number field (i.e., L has no real places). Then, -1 is a sum of squares in L.*

Proof. Let α be such that $L = \mathbb{Q}(\alpha)$ and let $f \in \mathbb{Q}[X]$ be the monic minimal polynomial of α. As f has no real zeros, $f(x) > 0$ for all $x \in \mathbb{R}$. The leading term dominates for large $|x|$ and a compactness arguments shows that $f(x) > c$ for some positive constant c. Hence, there exists some positive integer n such that $(1 - n^{-2})f(X) - n^{-2} \in \mathbb{Q}[X]$ is also positive on $\mathbb{R}$. From Lemma 5 below, we know that there exist polynomials $g_i \in \mathbb{Q}[X]$ such that

$$(1 - n^{-2})f(X) - n^{-2} = \sum_i g_i(X)^2$$

Evaluation at $X = \alpha$ gives a presentation of $-n^{-2}$ as a sum of squares in L. This finishes the proof. □

Lemma 5 (Landau [18])**.** *Let $P \in \mathbb{Q}[X]$ be a polynomial that takes non-negative values on the reals. Then, P can be written as a sum of squares $\sum P_i(X)^2$ with $P_i \in \mathbb{Q}[X]$.*

Proof. Evidently, P must be of even degree $\deg(P)$. We proceed by induction on $\deg(P)$. Every positive rational number is evidently a sum of squares as

$$\frac{a}{b} = \frac{ab}{b^2} = \underbrace{\frac{1}{b^2} + \frac{1}{b^2} + \cdots + \frac{1}{b^2}}_{ab \text{ summands}}.$$

This settles the case $\deg(P) = 0$. Assume now $\deg(P) = 2k$, $k \geq 1$, and that the lemma is already established for all $2k' < 2k$. We may assume that P is monic and write

$$P(X) = X^{2k} + a_{2k-1}X^{2k-1} + \cdots + a_0.$$

Replacing $P(X)$ with $Q(X) = P(X - a_{2k-1}/2k)$, we may and do assume $a_{2k-1} = 0$. In addition, we can assume that P has no real zero ξ. Otherwise, expanding P locally near $X = \xi$ yields that the zero order $\mathrm{ord}_{X=\xi}(P)$ is even. Decomposing f into its distinct linear factors $f = \prod(X - \alpha_i)^{n_i}$, we set $f_1 = \prod_{n_i \text{ even}}(X - \alpha_i)^{n_i/2}$ and $f_2 = \prod_{n_i \text{ odd}}(X - \alpha_i)^{n_i}$. Note that both f_i are products of $\mathbb{Q}$-irreducible factors in f and hence have rational coefficients. In conclusion, $f = f_1^2 f_2$ with $\deg(f_1) \neq 0$ and $\deg(f_2) = 2k'$. As $2k' = \deg(f_2) < \deg(f) = 2k$, f_2 is a sum of squares in $\mathbb{Q}[X]$ by the induction hypothesis. In the sequel, we assume that P has only complex conjugate zeros. Write

$$P(X) = \prod_{i=1}^{k}(X - x_i - iy_i)(X - x_i + iy_i) = \prod_{i=1}^{k}((X - x_i)^2 + y_i^2), \; x_i \in \mathbb{R}, y_i \in \mathbb{R}^\times.$$

By assumption, $\sum_{i=1}^k x_i = -a_{2k-1}/2 = 0$. In addition, $Q(X) = P(X) - \prod_{i=1}^k (X - x_i)^2 \in \mathbb{R}[X]$ attains only values larger than $\prod_{i=1}^k y_i^2 > 0$ on $\mathbb{R}$. Furthermore, $\deg(Q) \leq 2k - 1$ and hence $\deg(Q) \leq 2k - 2$ by positive definiteness. The X^{2k-2}-coefficient of Q is $\sum_{i=1}^k y_i^2 > 0$ and hence $\deg(Q) = 2k - 2$ and there exists a positive constant c such that $Q(x) > \left(\frac{1}{2}\sum_{i=1}^k y_i^2\right) x^{2k-2}$ for all $|x| > c$. It is easy to see that we can approximate the reals $x_i \in \mathbb{R}$ by rationals $x_i' \in \mathbb{Q}$ such that $\sum_{i=1}^k x_i' = 0$ and

$$\left|\prod_{i=1}^{2k}(x - x_i)^2 - \prod_{i=1}^{2k}(x - x_i')^2\right| \leq \frac{1}{2} \cdot \begin{cases} \prod_{i=1}^k y_i^2 & \text{if } |x| \leq c \\ \left(\sum_{i=1}^k y_i^2\right) x^{2k-2} & \text{if } |x| > c \end{cases}.$$

In conclusion,

$$Q'(X) = P(X) - \prod_{i=1}^{2k} (x - x_i')^2 \in \mathbb{Q}[X]$$

satisfies

$$Q'(x) = \underbrace{P(x) - \prod_{i=1}^{2k} (x - x_i)^2}_{Q(x)} + \left(\prod_{i=1}^{2k} (x - x_i)^2 - \prod_{i=1}^{2k} (x - x_i')^2 \right) > 0$$

for all real x. By our inductive hypothesis, $Q'(X)$ is a sum of squares and the same is true for $P(X)$. □

Lecture 3: The Theorem of Neukirch-Uchida

2 The Theorem of Neukirch-Uchida

Global field: either a) a number field (i.e., a finite extension of $\mathbb{Q}$) or b) a finitely generated field of transcendence degree 1 over a finite field $\mathbb{F}_q$ (i.e., a function field of a positive characteristic curve).

Global fields = fields of Kronecker dimension 1

Recall from the Introduction:

Theorem 12 (Neukirch 1969 [25], Uchida 1976 [47], Uchida 1977 [48])**.** *K, L be global fields. Then, $\Phi : G_K \to G_L$ is an isomorphism $\Rightarrow \exists!\ \phi : \overline{L}^{\mathrm{s}} \to \overline{K}^{\mathrm{s}}$ such that $\phi(L) = K$ and $\Phi(g) = \phi^{-1}g\phi$. In particular, $K \approx L$ and*

$$\mathrm{Isom}(L, K) \to \mathrm{Isom}(G_K, G_L)/\,\mathrm{Inn}(G_L),$$

where for $\sigma : L \to K$ we choose a lifting $\overline{\sigma} : \overline{L}^{\mathrm{s}} \to \overline{K}^{\mathrm{s}}$. This induces $\overline{\sigma}^* : G_K = \mathrm{Gal}(\overline{K}^{\mathrm{s}}|K) \to \mathrm{Gal}(\overline{L}^{\mathrm{s}}|L) = G_L$, $\varphi \mapsto \overline{\sigma}^{-1} \circ \varphi \circ \overline{\sigma}$, unique up to inner automorphisms of G_L.

Additional reference (for my own record): [26]

2.1 Local Correspondence

In this section, we want to establish

Lemma 6. *The isomorphism $\Phi : G_K \to G_L$ induces a bijection $\mathcal{P}_f(\overline{K}^{\mathrm{s}}) \to \mathcal{P}_f(\overline{L}^{\mathrm{s}})$ of non-archimedean places. This bijection is characterized uniquely by the fact that $\Phi(D_v) = D_w$ if $v \in \mathcal{P}_f(\overline{K}^{\mathrm{s}})$ is sent to $w \in \mathcal{P}_f(\overline{L}^{\mathrm{s}})$.*

It should be noted that this induces not only a correspondence $\mathcal{P}_f(\overline{K}) \approx \mathcal{P}_f(\overline{L})$ but also correspondences $\mathcal{P}_f(\overline{K}^H) \approx \mathcal{P}_f(\overline{L}^{\Phi(H)})$ for any closed subgroup H; for two places $v, w \in \mathcal{P}_f(\overline{K})$ restrict to the same place of $\overline{K}^H$ if and only if their decomposition groups $D_v, D_w \subset G_K$ are conjugate by an element of H. To be precise, we define a bijection $\mathcal{P}_f(K) \to \mathcal{P}_f(L)$ in the following way: For any $v \in \mathcal{P}_f(K)$ there exists a place $\widetilde{v} \in \mathcal{P}_f(\overline{K})$ such that $\widetilde{v}|_K = v$. By the above lemma, there is a unique place $w \in \mathcal{P}_f(\overline{L})$ such that $D_{\widetilde{v}} = \Phi(D_{\widetilde{w}})$. Evidently, choosing a different $\widetilde{v}$ changes $D_{\widetilde{v}}$ into a one of its $\mathrm{Gal}(\overline{K}/K)$-conjugates, hence $D_{\widetilde{w}}$ into one of its $\mathrm{Gal}(\overline{L}/L)$-conjugates. The restriction $w|_L \in \mathcal{P}_f(L)$ is hence unique.

Strategy of proof:

(1) Decomposition groups D_v, $v \in \mathcal{P}_f(\overline{K}^{\mathrm{s}})$, correspond biuniquely to places. *For any place $v \in \mathcal{P}_f(\overline{K}^{\mathrm{s}})$ there is a unique decomposition group D_v but we may have $D_v = D_w$ for $v \neq w \in \mathcal{P}_f(\overline{K}^{\mathrm{s}})$.*

(2) Φ sends decomposition groups of G_K to decomposition groups of G_L.

We start with (1):

Lemma 7. *Let $v, w \in \mathcal{P}(\overline{K}^{\mathrm{s}})$ two distinct places of $\overline{K}^{\mathrm{s}}$. Then, $D_v \cap D_w = \{1\}$.*

Some spectacular consequences:

1. Every decomposition group $D_v \subseteq G_K$ is its own normalizer.

Proof: Suppose $\sigma \in G_K$ is such that $\sigma D_v \sigma^{-1} = D_v$. This implies $D_{\sigma v} = D_v$ and hence $\sigma v = v$. By the definition of D_v, this means $\sigma \in D_v$.

2. L/K finite Galois extension of global fields. $G_K \to \mathrm{Aut}(G_L)$ is injective.

Proof: Let $\sigma \in G_K$ such that $\sigma \circ \tau \circ \sigma^{-1} = \tau$ for all $\tau \in G_L$. Let $D_v \subset G_K$ be any non-archimedean decomposition group. Then, $D_v \cap G_L = \sigma D_v \sigma^{-1} \cap G_L = D_{\sigma v} \cap G_L$. As both $D_v \cap G_L$ and $D_{\sigma v} \cap G_L$ have infinite cardinality, it follows that $v = \sigma v$.

3. In particular, G_K has trivial center.

Proof: This is just the case $L = K$ above.

In fact, we will even show

Theorem 13 (F.K. Schmidt [41]). *Let F be a non-separably closed field. Then, F is Henselian for at most one non-archimedean place v (= equivalence class of absolute values $|\cdot|_v$ on F).*

A field F with absolute value $|\cdot|_v$ is Henselian if $|\cdot|_v$ extends uniquely to every algebraic extension. If $(F, |\cdot|_v)$ is a Henselian field, we will denote the unique extension of $|\cdot|$ to $\overline{F}^{\mathrm{s}}$ again by $|\cdot|$. One can prove that a field F with non-archimedean absolute value $|\cdot|$ is Henselian iff $\mathcal{O}_F/\mathfrak{m}_F$ is a Henselian local ring.

Note: We work here with absolute values and hence our results are restricted to rank 1 valuations. Recall that we call two absolute values equivalent if they induce the same topology on F. All here can be done for general valuations as well, appropriately (!) modified. See [6, Chapter 4]. Examples: p-adic local fields $L/\mathbb{Q}_p$, fixed fields $(\overline{K}^{\mathrm{s}})^{D_v}$, $v \in \mathcal{P}(\overline{K}^{\mathrm{s}})$.

A converse to Schmidt's Theorem is also true: If F is separably closed then F is Henselian with respect to all its valuations; this is rather obvious as valuations do not split in purely inseparable extensions (cf. [6, Corollary 3.2.10]).

Proof of Lemma 7. $(\overline{K}^{\mathrm{s}})^{D_v} \cdot (\overline{K}^{\mathrm{s}})^{D_w}$ is Henselian both for v and w. By Theorem 13 it is separably closed. Hence, $(\overline{K}^{\mathrm{s}})^{D_v} \cdot (\overline{K}^{\mathrm{s}})^{D_w} = \overline{K}^{\mathrm{s}}$ and $D_v \cap D_w = 1$. □

Before we start with the proof of Theorem 13, we recall an important lemma:

Lemma 8 (Krasner's Lemma). *Let $(F, |\cdot|)$ be non-archimedean Henselian with separable closure $(\overline{F}^{\mathrm{s}})$. Let $\alpha \in \overline{F}^{\mathrm{s}}$ with F-conjugates $\alpha = \alpha_1, \ldots, \alpha_n$. For each $\beta \in \overline{F}^{\mathrm{s}}$,*

$$|\alpha - \beta| < \min_{2 \leq i \leq n} |\alpha - \alpha_i|$$

implies $F(\alpha) \subseteq F(\beta)$.

Proof. Start with $\sigma \in \mathrm{Gal}(\overline{F}^{\mathrm{s}}/F(\beta))$. As we have to prove $\sigma\alpha = \alpha$ we may assume that $\sigma\alpha = \alpha_i$ for some $1 < i \leq n$. Since both $|\cdot|$ and $|\sigma(\cdot)|$ extend the value $|\cdot|$ on F, we must have $|\sigma x| = |x|$ for all $x \in \overline{F}^{\mathrm{s}}$. Hence, we have $|\beta - \alpha_i| = |\sigma^{-1}(\beta - \alpha)| = |\beta - \alpha|$ and

$$|\alpha - \alpha_i| \leq \min\{|\alpha - \beta|, |\beta - \alpha_i|\} < \min_{2 \leq i \leq n} |\alpha - \alpha_i|$$

by assumption. This is a clear contradiction. □

Actually, Krasner's Lemma is equivalent to being Henselian [6, Exercise 4.5.2]. We apply Lemma 8 to obtain:

Lemma 9. *Let F be a complete local field with separable closure $\overline{F}^{\mathrm{s}}$. $f_1 \in F[X]$ a separable polynomial of degree d. There exists a constant $c(f_1) > 0$ such that each $f_2 \in F[X]$, $\deg(f_2) = d$, with $|f_1 - f_2| < c(f_1)$ has the same splitting field as f_1 in $\overline{F}^{\mathrm{s}}$.*

Here, if $|\cdot|$ is an absolute value on F, set $|\sum_{i=0}^{d} a_i X^i| = \max_{0 \leq i \leq d} \{|a_i|\}$.

Proof. The case $F = \mathbb{C}$ is trivial. The case $F = \mathbb{R}$ is likewise easy by continuity of roots; for if f_1 has a non-real root then any sufficiently near polynomial f_2 has also a non-real root and hence both splitting fields are $\mathbb{C}$. In the sequel, we may and do assume that F is non-archimedean. Write $f_1 = c_1 \prod_{i=1}^{d}(X - \alpha_i)$ and $f_2 = c_2 \prod_{j=1}^{d}(X - \beta_j)$. We have

$$\min_{1 \leq j \leq d} |\alpha_i - \beta_j|^d \leq |c_2|^{-1}|f_2(\alpha_i)| = |c_2|^{-1}|f_2(\alpha_i) - f_1(\alpha_i)| \leq |f_2 - f_1| \max\{|c_2|^{-1}, |c_2|^{-1}|\alpha_i|^d\}.$$

Hence, we may arrange that $|\alpha_i - \beta_j| < \min_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|$ by making $c(f_1)$ sufficiently small. In other words, there exists $j(i)$ so that $|\alpha_i - \beta_{j(i)}| < \min_{1 \leq i < j \leq n} |\alpha_i - \alpha_j|$. This $j(i)$ can be easily seen to be unique by the triangle inequality. Furthermore, for each $i_1 \neq i_2$ we have $\max\{|\beta_{j(i_1)} - \alpha_{i_1}|, |\alpha_{i_2} - \beta_{j(i_2)}|\} < |\alpha_{i_1} - \alpha_{i_2}|$ and hence

$$|\beta_{j(i_1)} - \beta_{j(i_2)}| = \max\{|\beta_{j(i_1)} - \alpha_{i_1}|, |\alpha_{i_1} - \alpha_{i_2}|, |\alpha_{i_2} - \beta_{j(i_2)}|\} = |\alpha_{i_1} - \alpha_{i_2}|.$$

From $|\alpha_i - \beta_{j(i)}| < \min_{1\leq i<j\leq n} |\alpha_i - \alpha_j|$ it follows by Krasner's Lemma that $F(\alpha_i) \subseteq F(\beta_{j(i)})$. Finally, from $|\alpha_i - \beta_{j(i)}| < \min_{1\leq i<j\leq n} |\beta_i - \beta_j|$ it follows that $F(\beta_{i(j)}) \subseteq F(\alpha_i)$. □

Proof of Theorem 13. Let $|\cdot|_v$ and $|\cdot|_w$ be two non-equivalent values. We show that each $\alpha \in \overline{F}^{\mathrm{s}}$ is contained in F. Let $f_1 \in F[X]$ be the minimal polynomial of α. Choose any $f_2 = \prod_{i=1}^{d}(X - \alpha_i) \in F[X]$ with $\alpha_i \in F$ (i.e. such that f_2 decomposes into linear factors over F). By the approximation theorem ([6, Theorem 2.4.1]) (a corollary of Chinese Remainder Theorem), there exists $f \in F[X]$ such that $|f - f_1| < c(f_1)$ and $|f - f_2| < c(f_2)$. With 9, we conclude that $F(\alpha) = F(f_1) = F(f) = F(f_2) = F$. As $\alpha \in \overline{F}^{\mathrm{s}}$ arbitrary, $\overline{F}^{\mathrm{s}} = F$. Contradiction! □

For the second part of the proof of Lemma 6, we need some group cohomology and class field theory. We briefly summarize the basics in the next two sections.

Lecture 4: The Theorem of Neukirch-Uchida II

2.2 Interlude: Group Cohomology

Reference: [28, Chapter 1]

Group cohomology: Now: G a finite group, A a G-module. Later: G a pro-finite group, A a discrete G-module.

Standard resolution: exact complex of free $\mathbb{Z}[G]$-modules

$$0 \leftarrow \mathbb{Z} \leftarrow^{\epsilon} X_0 \leftarrow^{\delta_1} X_1 \leftarrow^{\delta_2} \cdots,$$

with $X_0 = \mathbb{Z}[G]$ and $X_q = \oplus_{(\sigma_1,\cdots,\sigma_q)\in G^q}\mathbb{Z}[G](\sigma_1,\ldots,\sigma_q)$, $q \geq 1$ (q-cells). The map $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ is the augmentation map $\sum_{\sigma\in G} n_\sigma(\sigma) \mapsto \sum_{\sigma\in G} n_\sigma$, $d_1((\sigma)) = \sigma - 1$, and

$$d_q((\sigma_1,\ldots,\sigma_q)) = \sigma_1(\sigma_2,\ldots,\sigma_q)+\sum_{i=1}^{q-1}(-1)^i(\sigma_1,\ldots,\sigma_{i-1},\sigma_i\sigma_{i+1},\sigma_{i+2},\cdots,\sigma_q)+(-1)^q(\sigma_1,\ldots,\sigma_{q-1}).$$

$D(G-mod)$ = discrete G-modules

group cohomology: $H^n(G,A) = Ext^n_{D(G-mod)}(\mathbb{Z},A) = H^n(\mathrm{Hom}_G(X.,A))$.

$H^n(G,A)$ has interpretation as maps $G^n \to A$ (modulo sth.): $(\sigma_1,\ldots,\sigma_n) \mapsto \varphi((\sigma_1,\ldots,\sigma_n))$.

$$0 \to \mathrm{Hom}_G(X_0,A) \to \mathrm{Hom}_G(X_1,A) \to \cdots,$$

long exact sequence: $0 \to A \to B \to C \to 0$, then $0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \to H^1(G,A) \to \cdots$.

Examples:

(1) $H^0(G,A) = A^G = \{a \in A \mid \forall\sigma \in G : a^\sigma = a\}$.

(2) $H^1(G,A) = \{c : G \to A \mid c(\sigma\tau) = c(\sigma)c(\tau)^\sigma\}/\sim$, where $c_1 \sim c_2$ if there exists $a \in A$ such that $c_1(\sigma)c_2(\sigma)^{-1} = \sigma a/a$.

(3) A discrete topological group with trivial G-action, $H^1(G,A) = \mathrm{Hom}(G,A)$.

group homology: $H_n(G,A) = Tor_n^{D(G-mod)}(A,\mathbb{Z})$.

All of this works in the slightly more general setting where G is a profinite group and A is a discrete G-module. However, $\mathbb{Z}[G]$ has to be replaced by the complete group algebra $\mathbb{Z}[[G]]$ and all maps have to be continuous. In the description of $H^n(G,A)$ by explicit maps $G^n \to A$ nothing changes except for the fact that continuity has to be supposed everywhere. For details, see [36].

Inflation: $H \subseteq G$ normal subgroup, $q \geq 0$. For $x : G/H \times \cdots \times G/H \to A^H$ define $\inf(x) : G \times \cdots \times G \to A$ by

$$\inf(x)(g_1,\ldots,g_q) = x(g_1 \bmod H,\ldots,g_q \bmod H).$$

Get $\inf : H^q(G/H,A^H) \to H^q(G,A)$.

Restriction: H a subgroup of G, $q \geq 0$. For $x : G\times\cdots\times G \to A^q$ define $\mathrm{res}(x) : H\times\cdots\times H \to A$ by 'restriction'. Get $\mathrm{res} : H^q(G,A) \to H^q(H,A)$.

Hochschild-Serre spectral sequence: G profinite, H closed normal subgroup, A a G-module.

$$E_2^{pq} = H^p(G/H,H^q(H,A)) \Rightarrow H^{p+q}(G,A)$$

Inflation-Restriction Sequence:

$$0 \to H^1(G/H,A^H) \to^{inf} H^1(G,A) \to^{res} H^1(H,A)$$

is exact. Some extension: If $H^i(H,A) = 0$ for $i = 1,\ldots,q-1$, $q \geq 1$, then

$$0 \to H^q(G/H,A^H) \to^{inf} H^q(G,A) \to^{res} H^q(H,A)$$

is exact.

Induced modules: H a subgroup of G. A is G/H-induced, if there exists a H-submodule $D \subseteq A$ such that $A = \bigoplus_{\sigma \in G/H} \sigma D$.

Shapiro's Lemma: Let $A = \bigoplus_{\sigma \in G/H} \sigma D$ be G/H-induced. Then, $H^q(G, A) = H^q(H, D)$ (canonical isomorphism).

Dimension shift: $0 \to A \to \sum_{\sigma \in G} \sigma A_0 = Maps(G, A_0) \to A_1 \to 0$. $A_0 = A$ with trivial G-action.

Torsion: If the order of G is coprime to p, then $H^i(G, A)(p) = 0$, $i > 0$. (by [29][1.6.10] $H^i(G, A)$ injects into $H^i(G^{(p)}, A)$, $G^{(p)}$ a p-Sylow subgroup)

Limits: $H^n(\varprojlim_i G_i, \varinjlim_i A_i) = \varinjlim_i H^n(G_i, A_i)$. (maps canonical)

Two applications:

1. G profinite, A discrete G-module. Then, $G = \varprojlim_{U \text{ open}} G/U$ and $A = \varinjlim A^U$. Hence, $H^n(G, A) = \varinjlim_i H^n(G/U, A^U)$. Thus, profinite group cohomology is just an inverse limits of ordinary group cohomology.

2. G profinite, H a closed subgroup. Then, $H = \bigcap_{U \text{ open, } H \subset U} U = \varprojlim_{U \text{ open, } H \subset U} U$ (with inclusions as morphisms). Thus, $H^n(H, A) = \varinjlim_{U \text{ open, } H \subset U} H^n(U, A)$. (Each co-cycle lifts to an open supergroup.)

Tate cohomology modules $\widehat{H}^i$: I hope I will not use them.

cohomological p-dimension: $cd_p(G)$ = minimal n such that $H^q(G, A)(p) = 0$ for all $q > n$ and all discrete torsion G-modules A. (Equivalently: $H^q(G, A) = 0$ for all $q > n$ and all discrete p-torsion G-modules)

Facts: (1) H closed subgroup of G, then $cd_p(H) \leq cd_p(G)$ (Shapiro's Lemma); in fact, equality holds if $p \nmid [G : H]$

(2) $cd_p(G) = cd_p(G^{(p)})$, $G^{(p)}$ p-Sylow subgroup of G. (a corollary of (1))

(3) If G is a pro-p group, then $cd_p(G) \leq n \Leftrightarrow H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$. (This uses that every discrete simple p-primary G-module is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ if G is pro-p; this is not completely trivial: see [36, Lemma 7.1.5])

Remark: (3) is very useful in combination with (2).

2.3 Interlude: Class Field Theory I

Notation: Write $H^i(L|K, A)$ (resp. $H^i(K, A)$) instead of $H^i(\mathrm{Gal}(L/K), A)$ (resp. $H^i(G_K, A)$). Also $cd_p(K) = cd_p(G_K)$.

General remark: inner automorphisms induces the identity maps on cohomology (nothing happens for $A^G = H^0(G, A)$ + dimension shift)

Hilbert's Satz 90: $L|K$ Galois field extension, then $H^1(L|K, L^\times) = 0$.

Brauer groups: k a field, $Br(k)$ = central simple algebras over k (central: center = k, simple = no two-sided ideals) modulo similarity ($\sim$). $A \sim B$ iff $A \otimes_k M_r(k) \cong B \otimes_k M_s(k)$.

a central simple algebra (c.s.a.) splits in l/k if $A \otimes_k l$ is a matrix algebra.

subgroup $Br(l|k)$ generated by those c.s.a. that split in l

Facts:

(1) $H^2(k, \overline{k}^\times) = Br(k)$ such that $H^2(l|k, l^\times) = Br(l|k)$ (w.r.t. inflation).

(2) the restriction map $Br(k) \to Br(l)$ is given by $[A] \mapsto [A \otimes_k l]$.

(3) suppose $l = \bigcup l_i$, then $Br(l) = \varinjlim_i Br(l_i)$ (maps = restrictions).

(4) k a finite field, then $Br(k) = 0$. (Let l/k be a finite extension. Then $\mathrm{Gal}(l/k)$ is a finite cyclic group and the group cohomology is hence of periodicity = 2. Furthermore, $l^\times$ is a finite $\mathrm{Gal}(l/k)$-module, hence the Herbrand coefficient = 1. By Hilberts Satz 90 all = 1 for $q \geq 1$).

Relation with cohomological dimension:

Lemma 10. *K field, $char(K) \neq p$. We have $Br(L)(p) = 0$ for every finite separable extension $L|K$ if and only if $cd_p(K) \leq 1$.*

Proof. Let $F \subset \overline{K}^{\mathrm{s}}$ be the fixed field of a p-Sylow group of G_K. Then, $cd_p(K) = cd_p(F)$ and $\mu_p \subset F$ ($[K(\mu_p) : K] | p-1$). Now, we have to prove $0 = H^2(F, \mathbb{Z}/p\mathbb{Z}) = H^2(F, \mu_p)$. Let $F = \bigcup F_i$ with $[F_i : K] < \infty$ and $\mu_p \subset F_i$. Use Kummer sequence

$$1 \to \mu_p \to (\overline{K}^{\mathrm{s}})^\times \to^{\cdot p} (\overline{K}^{\mathrm{s}})^\times \to 1$$

and Hilbert 90: $H^2(F_i, \mu_p) = \ker(\mathrm{Br}(F_i) \to^{\cdot p} \mathrm{Br}(F_i)) = \mathrm{Br}(F_i)[p] = 0$. A limit gives $H^2(F, \mu_p) = \mathrm{Br}(F)[p] = \varinjlim \mathrm{Br}(F_i)[p] = 0$.

Conversely, if $cd_p(K) \le 1$ then $\mathrm{Br}(L)[p] = 0$ for all finite extensions L/K. Indeed, $cd_p(K) \le 1$ implies $cd_p(L) \le 1$ and the Kummer exact sequence (plus Hilbert's Theorem 90)

$$1 \to \mu_p \to (\overline{K}^{\mathrm{s}})^\times \to^{\cdot p} (\overline{K}^{\mathrm{s}})^\times \to 1$$

yields $0 = H^2(L, \mu_p) = \mathrm{Br}(L)[p]$. □

Local class field theory:

K, L local non-archimedean fields. $\exists$ canonical isomorphism

$$inv : Br(K) = H^2(K, \overline{K}^\times) \to \mathbb{Q}/\mathbb{Z}$$

s.t.

$$H^2(L|K, L^\times) \to [L:K]^{-1}\mathbb{Z}/\mathbb{Z} \text{ (inflation).}$$

Furthermore,

$$\begin{tikzcd} H^2(K, \overline{K}^\times) \arrow[r] \arrow[d, "\mathrm{res}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\cdot [L:K]"] \\ H^2(L, \overline{L}^\times) \arrow[r] & \mathbb{Q}/\mathbb{Z} \end{tikzcd}$$

Fact: $H^2(K, \overline{K}^\times) = \bigcup_{L|K \text{ unramified}} H^2(L|K, K^\times)$.

Corollary: Brauer group $Br(K) \approx \mathbb{Q}/\mathbb{Z}$.

There is also an archimedean analogue of this, which is rather simple: In fact, $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Br}(\mathbb{C}) = \{1\}$.

We note an important consequence for later use:

Lemma 11. *l a prime. K a local non-archimedean field. $K \subseteq F \subseteq \overline{K}^{\mathrm{s}}$. Then,* $\mathrm{Br}(F)(l) = 0$ *iff* $l^\infty | [F:K]$ *and* $\mathrm{Br}(F)(l) = \mathbb{Q}_l/\mathbb{Z}_l$ *iff* $l^\infty \nmid [F:K]$.

Proof. We know that

$$\mathrm{Br}(F)(l) = \varinjlim_{\mathbb{Q}_p \subset K \subset F, [K:\mathbb{Q}_p] < \infty} \mathrm{Br}(K)(l) = \varinjlim_{\mathbb{Q}_p \subset K \subset F, [K:\mathbb{Q}_p] < \infty} \mathbb{Q}_l/\mathbb{Z}_l,$$

and the morphisms in the limit are the restrictions, namely $\mathbb{Q}_l/\mathbb{Z}_l \approx \mathrm{Br}(K)(l) \to \mathrm{Br}(L)(l) \approx \mathbb{Q}_l/\mathbb{Z}_l$ is multiplication by $[L:K]$ for each extension L/K of local fields. □

Lemma 12. *A field K of characteristic p has p-dimension $cd_p(K) \le 1$.*

Proof. Let F be the fixed field of a p-Sylow group of G_K. Then, $cd_p(K) = cd_p(F)$ and we have to prove $H^2(F, \mathbb{Z}/p\mathbb{Z}) = 0$. For this we use the long exact sequence associated to the Artin-Schreier exact sequence ($\wp(X) = X^p - X$):

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \overline{K}^{\mathrm{s}} \to^{\wp} \overline{K}^{\mathrm{s}} \to 0.$$

As $H^i(F, \overline{K}^{\mathrm{s}}) = 0$, $i > 0$ (by normal basis theorem, the additive module of each finite extension $F \subset F_0 \subset \overline{K}^{\mathrm{s}}$ is induced), we have $H^2(F, \mathbb{Z}/p\mathbb{Z}) = 0$. □

Lemma 13. *K a p-adic field local or a field of Laurent power series. $l \neq \mathrm{char}(K)$ an arbitrary prime. Then, $cd_l(K) = 2$.*

(To be precise, one can show that $cd_p(K) = 2$ if $\mathrm{char}(K) \neq p$ and $cd_p(K) = 1$ if $\mathrm{char}(K) = p$.)

Proof of Theorem 13. $cd_l(K) \geq 2$: This follows from $\mathrm{Br}(K) \approx \mathbb{Q}/\mathbb{Z}$ and Lemma 10 above.

$cd_l(K) \leq 2$: Let K^{nr} be the maximal unramified extension of K. By Hochschild-Serre,

$$H^p(K^{nr}|K, H^q(K^{nr}, A)) \Longrightarrow H^{p+q}(K, A).$$

Hence, it suffices to show that $\mathrm{Gal}(K^{nr}/K)$ and K^{nr} have cohomological l-dimension ≤ 1.

$\mathrm{Gal}(K^{nr}/K)$: isomorphic to the absolute Galois group of a finite field (Brauer group $= 0$, Lemma 12).

K^{nr}: Let F be a finite extension of K^{nr}. Then $H^2(F, \overline{K}^\times)(l) = Br(F)(l) = 0$ by restrictions from the fact that $l^\infty | [F : K]$. Hence, $cd_l(K^{nr}) = 1$ by Lemma 10 above. □

Global class field theory: K, L global fields

Ideles: $I_K = \prod'_{v \in \mathcal{P}(K)} K_v^\times$ (restricted product with respect to $\mathcal{O}_v \subseteq K_v$)

Decomposition of cohomology: L/K Galois, $H^i(L|K, I_L) = \oplus_v H^i(L_w|K_v, L_w^\times)$. (For any v one just chooses just one $w \in \mathcal{P}(L)$ above $v \in \mathcal{P}(K)$.)

Idele group: $I = \varinjlim_{[L:K]<\infty} I_L$

By limit: $H^i(K, I) = \oplus_v H^i(K_v, \overline{K_v}^\times)$ (note $\overline{K_v} = \overline{K}_w$, $w|v$, by Krasner).

Facts:

(1) $H^1(K, I) = 0$. Hence, $H^2(L|K, I) \hookrightarrow H^2(K, I)$ by inflation-restriction sequence.

(2) $H^2(K, \overline{K}^\times) = \bigcup_{L|K \text{ cyclic}} H^2(L|K, K^\times)$.

Invariant map: $H^2(K, I) \to \mathbb{Q}/\mathbb{Z}$ given by $\sum_v \mathrm{inv}_v$ in above decomposition.

$\ker(\mathrm{inv}) = H^2(K, K^\times) \subset H^2(K, I)$ (diagonal map).

Theorem 14 (Hasse principle for Brauer groups, Theorem 8.1.17 in [29])**.** *Let K be a global field. Then, there is an exact sequence*

$$1 \to \mathrm{Br}(K) \to \bigoplus_{v \in \mathcal{P}(K)} \mathrm{Br}(K_v) \to^{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 1.$$

As $H^2(K, I) = H^2(G_K, I) = \oplus_{v \in \mathcal{P}(K)} H^2(D_v, \overline{K_v}^\times)$, this Hasse principle follows from

$$1 \to H^2(K, (\overline{K}^{\mathrm{s}})^\times) \to H^2(K, I) \to^{\sum \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 1.$$

We derive the important consequence:

Corollary 3. *Let K be a global field and $K \subseteq F \subseteq \overline{K}^{\mathrm{s}}$. Then, the canonical map $\mathrm{Br}(F) \to \prod_{v \in \mathcal{P}(F)} Br(F_v)$ is injective and surjects onto each finite number of factors.*

Proof. Restrictions induce a commuting diagram:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Br}(K) \arrow[r] \arrow[d, "res"] & \oplus_{v \in \mathcal{P}(K)} \mathrm{Br}(K_v) \arrow[r, "\sum inv_v"] \arrow[d] & \mathbb{Q}/\mathbb{Z} \arrow[r] \arrow[d, "\cdot [L:K]"] & 1 \\
1 \arrow[r] & \mathrm{Br}(L) \arrow[r] & \oplus_{w \in \mathcal{P}(L)} \mathrm{Br}(L_w) \arrow[r, "\sum inv_w"] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 1
\end{tikzcd}$$

In the middle vertical map, $\eta \in \mathrm{Br}(K_v)$ is send to $\sum_{w|v} res_{L_w|K_v} \eta$. Taking direct limits, which preserve exactness, we obtain the exact sequence

$$1 \longrightarrow \varinjlim_{K \subset L \subset F, [L:K] \leq \infty} \mathrm{Br}(L) \longrightarrow \varinjlim_{K \subset L \subset F, [L:K] \leq \infty} \prod_{w \in \mathcal{P}(F)} \mathrm{Br}(L_w)$$

Note that $\varinjlim_{K \subset L \subset F, [L:K] \leq \infty} \mathrm{Br}(L) = \mathrm{Br}(F)$. The assertion follows. □

Lecture 5: The Theorem of Neukirch-Uchida III

2.1 Local Correspondence (cont.)

Recall K, L global fields, $\Phi : G_K \to G_L$ isomorphism. Let $\overline{K}$ and $\overline{L}$ be the separable closures of K and L. We will have no use for the algebraic closure in this lecture and I should have never introduced $\overline{K}^s$ instead of $\overline{K}$ for the separable closure.

Lemma 14. *Let $v \in \mathcal{P}_f(\overline{K})$. Then,* $\mathrm{Br}(\overline{K}^{D_v}) \approx \mathbb{Q}/\mathbb{Z}$.

Proof. We show that for any $w \neq v$ in $\mathcal{P}_f(\overline{K}^{D_v})$ we have $(\overline{K}^{D_v})_w = \overline{K}_w$ and hence $\mathrm{Br}((\overline{K}^{D_v})_w) = 0$. The lemma follows directly from Corollary 3. The proof is similar to that of Theorem 13, which means that we use Lemma 9 and the approximation theorem. In fact, let $\alpha \in \overline{K}_w$ with minimal polynomial $f_1(X) \in (\overline{K}^{D_v})_w[X]$. In addition, choose a random separable polynomial $f_2(X) \in \overline{K}^{D_v}[X]$ that splits completely in linear factors over $\overline{K}^{D_v}$. By the approximation theorem, there exists some $f(X) \in \overline{K}^{D_v}[X]$ such that $|f - f_1|_w < c(f_1)$ and $|f - f_2|_v < c(f_2)$ with $c(f_i)$ the constant from Lemma 9. By this lemma, $\overline{K}^{D_v} = \overline{K}^{D_v}(f_2) = \overline{K}^{D_v}(f)$ and $(\overline{K}^{D_v})_w(f_1) = (\overline{K}^{D_v})_w(f) = (\overline{K}^{D_v})_w$. This shows that $\alpha \in (\overline{K}^{D_v})_w$. As α is arbitrary we infer $(\overline{K}^{D_v})_w = \overline{K}_w$ as claimed. □

Lemma 15. *$l \neq 2$ a prime. $K \subseteq F \subseteq \overline{K}^{\mathrm{s}}$ a subfield. Then, F is Henselian if for all finite extensions $F \subset F_0 \subset \overline{K}^{\mathrm{s}}$ we have* $\mathrm{Br}(F_0)[l] \approx \mathbb{Z}/l\mathbb{Z}$.

Proof. As $\mathrm{Br}(F)[l] \approx \mathbb{Z}/l\mathbb{Z}$, there must exist a unique (!) non-archimedean place v of F such that $\mathrm{Br}(F_v)[l] \approx \mathbb{Z}/l\mathbb{Z}$ by Corollary 3. Let p be the rational prime dividing v. By Lemma 11, we have even $\mathrm{Br}(F_v)(l) \approx \mathbb{Q}_l/\mathbb{Z}_l$ and $l^\infty \nmid [F_v : \mathbb{Q}_p]$. We claim that F is Henselian for v. Assume that v extends to two different places v_1 and v_2 in a finite extension F_0 of F. Then, again by Corollary 3 we deduce

$$\mathrm{Br}(F_0) \twoheadrightarrow \mathrm{Br}(F_{0,v_1}) \times \mathrm{Br}(F_{0,v_2}).$$

This is not possible as $\mathrm{Br}(F_0)[l] \approx \mathbb{Z}/l\mathbb{Z}$ and $\mathrm{Br}(F_{0,v_1})[l] \approx \mathrm{Br}(F_{0,v_2})[l] \approx \mathbb{Z}/l\mathbb{Z}$. Indeed, the prime l divides $[F_{0,v_i} : \mathbb{Q}_p]$, $i \in \{1,2\}$, only finitely many times and hence $\mathrm{Br}(F_{0,v_i}) \approx \mathbb{Q}_l/\mathbb{Z}_l$, $i \in \{1,2\}$. In conclusion, F is Henselian for v. □

We need another lemma that shows that the characteristic of K is an invariant of the absolute Galois group G_K. It is common usage to refer to such pieces of information that can be determined solely from knowing an absolute Galois group as group-theoretic. It should not be forgotten that there is usually an additional assumption on the objects considered, e.g. one restricts to Galois groups of global fields in Lemma 16.

Lemma 16. *Let K be a global or local field. Then,* $\mathrm{char}(K) = p$ *if* $cd_p(K) \leq 1$ *and* $\mathrm{char}(K) = 0$ *if there is no such prime p.*

Proof. K global field: Assume $\mathrm{char}(K) = l > 0$. Then, $cd_l(K) \leq 1$ by Lemma 12. Assume now $\mathrm{char}(K) \neq l$ and choose an arbitrary non-archimedean place v of K. By Lemma 13, $cd_l(D_v) = 2$ and hence $cd_l(K) \geq 2$ as $D_v \subset G_K$.

K local field: same (easier) proof. □

As a corollary, note that $G_K \approx G_L$ implies that either K and L are both number fields or both function fields (of the same characteristic). As a late addendum to Krasner's Lemma 8, I would like to indicate the following consequence:

Lemma 17. *Let K be a local field. For each positive integer n, $(n, \mathrm{char}(K)) = 1$, there are only finitely many extensions L/K of degree n.*

Not that the assertion is trivial for archimedean local fields. The assumption $(n, \mathrm{char}(K)) = 1$ is necessary because the maximal pro-p quotient $G_K(p)$ of a local field K with characteristic p is free of infinite rank (cf. [29, Proposition 6.1.7]). In this situation, there are hence infinitely many distinct extensions of degree p.

Proof. It suffices to show that a local field has only finitely many totally ramified and finitely many unramified extensions of given degree n.

By (the well-known) [7, Theorem II.3.6], any totally ramified extension L/K is generated by the root of an Eisenstein polynomial

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0,$$

where $a_i \in \mathfrak{m}_K$, $0 \leq i \leq n-1$, and $a_0 \notin \mathfrak{m}_K^2$. The space of all such polynomials, considered as a subset of K^n, is compact as K is locally compact. Now, any Eisenstein polynomial is irreducible [7, Theorem II.3.6] and in particular separable (by our assumption on n) so that we may apply our Lemma 9 to each of them. We infer that nearby Eisenstein polynomials span the same local field L so that by compactness there are only finitely many distinct totally ramified extensions L of K having degree n.

The unramfied extensions of K are generated by roots of unity ([38, Theorem 2.4.3]). There are only finitely many subfields of the maximal cyclotomic extension of K of any given degree n and this concludes the proof. □

Eventually, we can now prove

Lemma 18. *$v \in \mathcal{P}_f(\overline{K}^{\mathrm{s}})$. Then $\Phi(D_v) = D_w$ for a place $w \in \mathcal{P}_f(\overline{L}^{\mathrm{s}})$.*

The place w is unique by Lemma 7.

Proof. We show that $\Phi(D_v)$ is contained in a decomposition group D_w. By symmetry, $\Phi^{-1}(D_w)$ is then also contained in a decomposition group D_w. By Lemma 7, $D_v = D_w$ and hence $D_w = \Phi(D_v)$.

Let l be an odd prime such that $l \nmid \mathrm{char}(K), \mathrm{char}(L)$. Let H be any open subgroup of D_v such that $\mu_l \subset (\overline{K}^{\mathrm{s}})^H =: F_0^{(1)}$ and $\mu_l \subset (\overline{L}^{\mathrm{s}})^{\Phi(H)} =: F_0^{(2)}$. (One can find even a group-theoretic version of this condition although this is not strictly needed here: In the number field case, the condition on H may be that it contains the intersection of all open subgroups of D_v having degree dividing $l-1$. By Lemma 17 this is a finite intersection so that there exist such subgroups H. In the function field case, we need a constant field extension and also this could be described in group-theoretic terms as will follow from some results of next lecture.)

$$\begin{tikzcd}
\overline{K} \arrow[d, dash] & \overline{L} \arrow[d, dash] \\
F_0^{(1)} = \overline{K}^H \arrow[d, dash] & \overline{L}^{\Phi(H)} = F_0^{(2)} \arrow[d, dash] \\
F^{(1)} = \overline{K}^{D_v} \arrow[d, dash] & \overline{L}^{\Phi(D_v)} = F^{(2)} \arrow[d, dash] \\
K & L
\end{tikzcd}$$

Kummer

$$1 \to \mu_p \to \overline{K}^\times \to^{\cdot p} \overline{K}^\times \to 1$$

implies

$$\cdots \to H^1(F_0^{(1)}, \overline{K}^\times) \to H^2(F_0^{(1)}, \mu_l) \to H^2(F_0^{(1)}, \overline{K}^\times) \to H^2(F_0^{(1)}, \overline{K}^\times) \to H^3(F_0^{(1)}, \mu_l) \to \cdots$$

Now, by Hilbert 90 $H^1(F_0^{(1)}, \overline{K}^\times) = 0$. It follows that

$$H^2(F_0^{(1)}, \mu_l) = \ker(H^2(F_0^{(1)}, \overline{K}^\times) \to^{\cdot l} H^2(F_0^{(1)}, \overline{K}^\times)) = \mathrm{Br}(F_0^{(1)})[l]$$

Similarly, $H^2(F_0^{(2)}, \mu_l) = \mathrm{Br}(F_0^{(2)})[l]$. By assumption on H, we have $\mu_l \approx \mathbb{Z}/l\mathbb{Z}$ as $G_{F_0^{(i)}}$-modules ($i = 1, 2$). By Lemma 14, we have $\mathrm{Br}(F_0^{(1)}) \approx \mathbb{Q}/\mathbb{Z}$. Hence,

$$\mathbb{Z}/l\mathbb{Z} \approx \mathrm{Br}(F_0^{(1)})[l] = H^2(F_0^{(1)}, \mu_l) = H^2(F_0^{(1)}, \mathbb{Z}/l\mathbb{Z}) = H^2(F_0^{(2)}, \mathbb{Z}/l\mathbb{Z}) = H^2(F_0^{(2)}, \mu_l) = \mathrm{Br}(F_0^{(2)})[l].$$

Since H was arbitrary, it follows by Lemma 15 that $F_0^{(2)}$ is Henselian. This means that there exists a unique $w \in \mathcal{P}_f(\overline{L})$ such that $\Phi(H) \subseteq D_w$. (w is non-archimedean because of $l \neq 2$.)

It remains to show that even $\Phi(D_v) \subseteq D_w$; for this, we show that $F^{(2)}$ is Henselian for $w|_{F^{(2)}}$. Let $w_1 = w|_{F_0^{(2)}}, w_2, \ldots, w_n$ be the extensions of $w|_{F^{(2)}}$ to $F_0^{(2)}$. By Corollary 3, we have a surjection

$$\mathrm{Br}(F_0^{(2)})(l) \twoheadrightarrow \prod_{i=1}^{n} \mathrm{Br}((F_0^{(2)})_{w_i})(l)$$

As $\mathrm{Br}(F_0^{(2)})[l] \approx \mathbb{Z}/l\mathbb{Z}$ and $\mathrm{Br}((F_0^{(2)})_{w_i})(l) \approx \mathbb{Q}_l/\mathbb{Z}_l$ by Lemma 11, we have $n = 1$. Hence, $F^{(2)} = \overline{L}^{\Phi(D_v)}$ is Henselian for w. We conclude that $\Phi(D_v) \subseteq D_w$. □

Note that nor Lemma 15 nor the above proof shows that the decomposition groups of a global fields are group-theoretic (i.e., that they may be determined solely from the absolute Galois group). The problem is that the Brauer group $\mathrm{Br}(F)$ (resp. $\mathrm{Br}(F)[l]$) does also depend on $F^\times$ (resp. μ_l), which is not obtainable from the subgroup G_F of G_K. However, it can be shown that this is the case by more refined tools. The criterion from [25, Satz 8] is given in Theorem 2 above.

2.4 The Theorem of Neukirch-Uchida: Normal number fields

We recall the definition of Dirichlet density and various well-known corollaries of the Cebotarev density theorem. Our reference is [27, Section VII.13].

Let $\mathcal{S}$ be a set of rational primes. Provided that it exists, the limit

$$d(\mathcal{S}) = \lim_{\substack{s \to 1 \\ \mathrm{Re}(s) > 1}} \frac{\sum_{p \in \mathcal{S}} p^{-s}}{\sum_{p \text{ prime}} p^{-s}}$$

is called the Dirichlet density of $\mathcal{S}$. We just need this density for a special type of sets $\mathcal{S}$. For any number field K, we set

$$\mathcal{S}(K) = \{p \in \mathbb{Q} \text{ prime} \mid \mathcal{O}_K \text{ has } [K : \mathbb{Q}] \text{ distinct prime ideals over } p\}.$$

In other words, $\mathcal{S}(K)$ consists of the rational primes that split completely in $K/\mathbb{Q}$. The following facts are straightforward consequences of the Cebotarev density theorem ([27, Corollary VII.13.6]):

1. The Dirichlet density of $\mathcal{S}(K)$ exists and $d(\mathcal{S}(K)) \geq [K : \mathbb{Q}]^{-1}$.
2. Additionally, $K/\mathbb{Q}$ is normal if and only if $d(\mathcal{S}(K)) = [K : \mathbb{Q}]^{-1}$.

We now want to establish a first result in the direction of the Neukirch-Uchida Theorem 12.

Lemma 19. *Let K and L be number fields in $\overline{\mathbb{Q}}$ and assume that K is normal. Then, $G_K \approx G_L$ implies $K = L$ (as subfields of $\overline{\mathbb{Q}}$).*

It is not necessary to fix here a common algebraic closure $\overline{\mathbb{Q}}$; this is just done to be in line with [27, Section VII.13]. It should also be mentioned that Lemma 19 is not trivially equivalent to Theorem 12 for normal number fields because there is no functoriality in Lemma 19. However, Lemma 19 is the main tool to prove Theorem 12 as we shall see.

Proof. Recall that Lemma 6 establishes a bijection $\mathcal{P}_f(K) \approx \mathcal{P}_f(L)$, $v \mapsto w$, such that the corresponding decomposition groups D_v and D_w are isomorphic. As $D_v \approx \mathrm{Gal}(\overline{K_v}/K_v)$, we will see in the next lecture (Lemma 20) that the local fields K_v and L_w have the same residue characteristic, and the same absolute ramification and inertia degrees. Additionally, for any rational prime p there is the well-known identity $\sum_{p|v}[K_v : \mathbb{Q}_p] = [K : \mathbb{Q}]$ (see e.g. [27, Corollary II.8.4]) and we derive $[K : \mathbb{Q}] = [L : \mathbb{Q}]$. From these facts, we infer that $G_K \approx G_L$ implies $\mathcal{S}(K) = \mathcal{S}(L)$. As $K/\mathbb{Q}$ is normal, $d(\mathcal{S}(K)) = [K : \mathbb{Q}]^{-1}$. It follows that $d(\mathcal{S}(L)) = [L : \mathbb{Q}]^{-1}$ and hence $L/\mathbb{Q}$ is also normal. Consequently, the composite KL is also normal over $\mathbb{Q}$. Furthermore, $\mathcal{S}(KL) = \mathcal{S}(K) \cap \mathcal{S}(L) = \mathcal{S}(K)$ implies

$$[KL : \mathbb{Q}]^{-1} = d(\mathcal{S}(KL)) = \mathcal{S}(K) = [K : \mathbb{Q}]^{-1}$$

and hence $L \subseteq KL = K$. Similarly, we have $K \subseteq L$ and the assertion is proven. □

Lecture 6: The Theorem of Neukirch-Uchida IV

2.5 Absolute Galois groups of local fields I: Group-theoretic data

Easy: A local field is archimedean if $|G_K| \in \{1, 2\}$.

From now on, let K be a non-archimedean local field.

Recall group-theoretic means all information on K that is encoded somehow in the abstract topological group G_K.

Lemma 20. *Let K be a non-archimedean local field. The following are group-theoretic (i.e., encoded in G_K):*

1. *the characteristic* $\mathrm{char}(K)$*,*
2. *the G_K-module $\mu(\overline{K}^\times)$;*
3. *the residue field $\mathcal{O}_K/\mathfrak{m}_K$ (resp. the absolute inertia degree $f_K = |\mathcal{O}_K/\mathfrak{m}_K|$);*
4. *the inertia subgroup $I_K \subset \mathrm{Gal}(\overline{K}/K)$;*
5. *the Frobenius class* Frob *in G_K/I_K;*
6. *the unit group U_K and the group of principal units $U_K^{(1)} = 1 + \mathfrak{m}_K$;*
7. *the multiplicative group $K^\times$;*
8. *the valuation* $\mathrm{ord} : K^\times \twoheadrightarrow \mathbb{Z}$*;*
9. *the universal norm residue symbol $(\cdot, K) : K^\times \to G_K^{ab}$.*

In addition, if K is a p-adic local field, the following are also group-theoretic data:

a. *the residue characteristic p;*

b. *the degree $[K : \mathbb{Q}_p]$;*

c. *the absolute ramification degree e_K.*

Admittedly, the formulation of our above lemma is rather vague. To understand its actual meaning do note the following when reading the proof: Given G_K as an abstract topological group, we give a – rather lengthy but purely group-theoretic – description of a subgroup $U_K(G)$ (resp. $K^\times(G)$) in G_K^{ab} such that $U_K \approx U_K(G)$ (resp. $K^\times \approx K^\times(G)$). In fact, $K^\times(G)$ is nothing but the image of $K^\times$ under the universal norm residue symbol; this is not its group-theoretic description, of course. Moreover, with the second assertion we mean to give a G_K-module $\mu(G)$ that is isomorphic to the G_K-module $\mu(\overline{K}^\times)$. One could and sometimes should be more precise at these places but statements as above are common in anabelian geometry. In any case, a clear consequence is that any isomorphism $G_K \approx G_L$ for local fields K and L induces unique isomorphisms $K^\times \approx L^\times$ and the various data (e.g., characteristic, residue characteristic, degrees) coincide.

To prove Lemma 20, we need some more local class field theory.

2.6 Interlude: Class Field Theory II

Here: Tate cohomology $\widehat{H}^i$ instead of ordinary group cohomology H^i. For this, one starts from a more complicated complex

$$\begin{tikzcd}
\cdots & X_{-2} \arrow[l, "d_{-2}"'] & X_{-1} \arrow[l, "d_{-1}"'] & & X_0 \arrow[ll, "d_0"'] \arrow[dl, "\epsilon"] & X_1 \arrow[l, "d_1"'] & X_2 \arrow[l, "d_2"'] & \cdots \arrow[l, "d_3"'] \\
& & & \mathbb{Z} \arrow[ul, "\mu"] \arrow[dl] & & & & \\
& & 0 & & 0 \arrow[ul] & & &
\end{tikzcd}$$

From this, $\widehat{H}^i = H^i$ if $i \geq 1$ but $\widehat{H}^0 \neq H^0$ and the $\widehat{H}^i$, $i < 0$, are all new. For any details, I refer to [28, Section I.2].[2]

Most importantly, the restriction of ordinary group homology extends to Tate cohomology naturally ([28, Definition I.4.9]). However, its extension to negative degrees is defined by compatibility conditions and not as simple and explicit as for positive degrees. In contrast, inflation maps are not even defined for $\widehat{H}^i$, $i \leq 0$. Be warned!

Class Formations:

A very convenient way to formulate class field theory both in the local and the global case employs the axiomatic notion of a class formation as in [3, Chapter XIV] or [28].

A formation is a pair (G, A) consisting of a profinite group G and a discrete G-module A. With applications in mind, we denote the open subgroups of G by G_K and the index K is called a 'field'. The field K_0 such that $G_{K_0} = G$ is the 'base field'. For any inclusion $G_L \subseteq G_K$, we write $K \subseteq L$ (or $L|K$) and $[L : K] = [G_K : G_L]$ is called the degree of this 'extension' $L|K$. An extension $L|K$ is called normal if G_L is a normal subgroup of G_K. It is called finite if $[L : K]$ is finite. In addition, we write A_K for A^{G_K}. Concerning cohomology groups, we adopt a notation that is compatible with our previous one: We write $H^q(L|K, A_L)$ (or even $H^q(L|K)$) for $H^q(G_K/G_L, A_L)$. For any tower $N \supseteq L \supseteq K$ with $N|K$ normal, we let

$$\mathrm{res}_L : H^q(N|K, A_N) \to H^q(N|L, A_N)$$

be the standard restriction of group cohomology.

A formation (G, A) is a field formation if for any finite normal extension $L|K$ we have

$$H^1(L|K, A_L) = 1$$

(Hilbert 90, formally). For a field formation (G, A) the inflation-restriction sequence

$$0 \to H^2(L_1|K, A_{L_1}) \to^{inf} H^2(L_2|K, A_{L_2}) \to^{res} H^2(L_2|L_1, A_{L_2})$$

is exact whenever $L_2|L_1|K$ is a chain of normal extensions. Consequently, we have injections

$$H^2(L_1|K, A_{L_1}) \hookrightarrow \varinjlim_{L_2|K} H^2(L_2|K, A_{L_2}) = H^2(G_K, A)$$

This allows us to consider each $H^2(L|K, A_L)$, $L|K$ a normal extension, as a subgroup of $H^2(G_K, A)$. In the sequel, this is tacitly assumed.

A field formation (G, A) is called a class formation if for any finite normal extension there exists an isomorphism

$$\mathrm{inv}_{L|K} : H^2(L|K, A_L) \longrightarrow [L : K]^{-1}\mathbb{Z}/\mathbb{Z}$$

such that

1. If $L_2 \supseteq L_1 \supseteq K$ are normal finite extensions, then $\mathrm{inv}_{L_1|K} = \mathrm{inv}_{L_2|K}|_{H^2(L_1|K, A_{L_1})}$.

[2] The standard cohomology H^i in *loc.cit.* is the Tate cohomology denoted by $\widehat{H}^i$ here.

2. If $N \supseteq L \supseteq K$ are open subgroups with $N|K$ normal, then

$$\mathrm{inv}_{N|L} \circ \mathrm{res}_L = [L : K] \cdot \mathrm{inv}_{N|K}.$$

Local Class Field Theory:

Main reference is [28]. Let K be a local non-archimedean field. (This will serve as the base field of our class formation denoted K_0 above.) $G_K = \mathrm{Gal}(\overline{K}/K)$ its absolute Galois group. K_H the fixed field of H in $\overline{K}$.

By definition, $\widehat{H}^0(L|K, K^\times) = K^\times/N_{L/K}L^\times$ and $\widehat{H}^{-2}(L|K, \mathbb{Z}) \approx \mathrm{Gal}(L/K)^{ab}$ by an elementary argument [28, Proposition I.3.19].

$(G_K, \overline{K}^\times)$ is a class formation ([28, Theorem II.5.6]) in the sense of Artin and Tate [3]:

$\exists!$ fundamental class $u_{L/K} \in \widehat{H}^2(L|K, L^\times)$ of L/K

cup product with $u_{L/K}$ yields the Nakayama map

$$\mathrm{Gal}(L/K)^{ab} = \widehat{H}^{-2}(L|K, \mathbb{Z}) \longrightarrow \widehat{H}^0(L|K, L^\times) = K^\times/N_{L/K}L^\times$$

of local class field theory ([28, Theorem II.1.9]), which is an isomorphism.

Its inverse is the (Artin) reciprocity map $\mathrm{rec}_{L/K} : K^\times/N_{L/K}L^\times \to \mathrm{Gal}(L/K)^{ab}$.

(Classical) norm residue symbol

$$(\cdot, L/K) : K^\times \to \mathrm{Gal}(L/K)^{ab}, \alpha \mapsto \mathrm{rec}_{L/K}(\alpha).$$

Facts: (1) Norm subgroups $N_{L|K}L^\times$, L a finite extension = finite index subgroups of $K^\times$ [28, Theorem II.6.3]

(2) $\bigcap_{[L:K]<\infty} N_{L|K}L^\times = 1$ (see [28, Corollary II.3.6])

Projective limit: universal residue symbol $(\cdot, K) : K^\times \hookrightarrow G_K^{ab}$; gives identification of G_K^{ab} with the profinite completion $\widehat{K^\times}$ (see [28, Theorem II.5.13]).

Split exact sequence

$$1 \longrightarrow U_K \longrightarrow K^\times \xrightarrow{\mathrm{val}} \mathbb{Z} \longrightarrow 0,$$

where U_K is the group of units and $\mathrm{val} : K^\times \to \mathbb{Z}$ is the (normalized) p-adic valuation on K.

For both the p-adic and the profinite topology on U_K translates of $U_K^{(n)} = 1 + \mathfrak{m}_K^n$ form a basis. Therefore, the profinite and the p-adic topology on U_K coincide. Particularly, U_K equals its profinite completion. In conclusion, the above exact sequence induces an exact sequence

$$1 \longrightarrow U_K \longrightarrow G^{ab} = \widehat{K^\times} \xrightarrow{\widehat{\mathrm{val}}} \widehat{\mathbb{Z}} \longrightarrow 0. \tag{2}$$

Denote by K_H the subfield of $\overline{K}$ that is fixed by H. From (2), we get for each open normal subgroup $H \subseteq G$ the multiplicative module $\widehat{K_H^\times}$. If H is normal we get also its G_K-module structure. Indeed, by [28, Theorem 1.11.d] $(\sigma a, K_H) = \sigma(a, K_H)\sigma^{-1}$ for any $a \in K_H$ and any $\sigma \in G_K$; this makes sense as $(a, K_H) \in H^{ab}$ and $\sigma H \sigma^{-1} = H$ by assumption. This means precisely that the G_K-action on $K_H^\times \subset \widehat{K_H^\times} = H^{ab}$ is extended by the action of G_K on H^{ab} through conjugation. The embedding $K \hookrightarrow K_H$ corresponds to the (classical) Verlagerung (transfer) Ver : $G^{ab} \to H^{ab}$ [28, Theorem 1.11.b]. This means that the following diagram is commutative:

$$\begin{tikzcd}
K \arrow[r, hook] \arrow[d, "{(\cdot,K)}"] & K_H \arrow[d, "{(\cdot,K_H)}"] \\
G^{ab} \arrow[r, "\mathrm{Ver}"] & H^{ab}
\end{tikzcd} \tag{3}$$

Note that the Verlagerung (transfer) $G^{ab} \to H^{ab}$ is nothing but the (cohomological) restriction $\mathrm{res} : \widehat{H}^{-2}(G, \mathbb{Z}) \to \widehat{H}^{-2}(H, \mathbb{Z})$ associated with $H \subseteq G$ (cf. [28, Definition I.4.10]).

Global Class Field Theory:

Let K be a global field. (This serves as the base field K_0 of our class formation.) For each finite extension L of K, we denote by I_L its idèle group and by $C_L = I_L/L^\times$ its idèle class group. For an extension L_2/L_1 of global fields containing K one has a standard inclusion $I_{L_1} \hookrightarrow I_{L_2}$, inducing an inclusion $C_{L_1} \hookrightarrow C_{L_2}$ ([28, Proposition III.2.6]). In addition, the profinite Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ induces (continuous) homomorphisms $I_K \to I_{\sigma K}$ and $C_K \to C_{\sigma K}$. If L_2/L_1 is normal with Galois group $G = \mathrm{Gal}(L_2/L_1)$ then $I_{L_1} = I_{L_2}^G$ ([28, Proposition III.2.5]) and $C_{L_1} = C_{L_2}^G$ by Hilbert's Satz 90 ([28, Theorem III.2.7]). We set $C = \varinjlim_L C_L$ with L ranging over all finite extensions of K in $\overline{K}$ and with respect to the above inclusions. It is easy to see that the maps $C_L \to C_{\sigma L}$ mentioned above give arise to a continuous automorphism σ of C. This makes C a discrete G_K-module and $C^{G_L} = C_L$ for all fields $K \subseteq L \subseteq \overline{K}$.

Now, (G_K, C) is a class formation ([28, Theorem III.6.9]).

Hence, as above: $\exists!$ fundamental class $u_{L/K} \in \widehat{H}^2(L|K, C_L)$ of L/K

Nakayama map (isomorphism!) of global class field theory:

$$\mathrm{Gal}(L/K)^{ab} = \widehat{H}^{-2}(L|K, \mathbb{Z}) \longrightarrow \widehat{H}^0(L|K, C_L) = C_K/N_{L/K}C_L$$

As in the local theory, we get a global universal norm residue symbol

$$I_K/K^\times = C_K \to G_K^{ab}$$

We write $I_K \to G_K^{ab}$, $a \mapsto (a, K)$, for the composition of this map with the quotient $I_K \to I_K/K^\times$. We call this the Artin symbol (or map). The image of C_K in G_K^{ab} is still dense in the pro-finite topology but the kernel D_K is non-trivial if K is a number field. In fact, D_K is the connected component of C_K that contains the identity. For more details, including the structure of D_K, see [3, Theorem IX.3]. If K is a function field, then $I_K/K^\times = C_K \to G_K^{ab}$ is still injective (see [3, Section VIII.3]). This means that the kernel of the Artin symbol is precisely $K^\times$.

There is a close relation between global and local reciprocity: For each place $v \in \mathcal{P}(K)$, we choose a lifting $\tilde{v} \in \mathcal{P}(\overline{K})$ and an embedding $\iota_v : G_{K_v} = D_{\tilde{v}} \hookrightarrow G_K$. Note that the induced map $G_{K_v} \to G_K^{ab}$ does not depend on the lifting $\tilde{v}$ as all such liftings are G_K-conjugates. Via this map, we consider (a_p, K_v) as an element of G_K^{ab} in the sequel.

Lemma 21. *([28, Theorem 6.15] or [3, Corollary VII.3.2]) Let K be a global field. For each $a = (a_v) \in I_K$, we have*

$$(a, K) = \prod_{v \in \mathcal{P}(K)} (a_v, K_v).$$

2.5 Absolute Galois groups of local fields I: Group-theoretic data (cont.)

Proof of Lemma 20. (1) is already done in Lemma 16 above

(2) For each finite Galois extension $L \supseteq K$ we have $\mu(\widehat{L^\times}) = \mu(L^\times)$ by the above exact sequence (2) and we obtained $\widehat{L^\times}$ as a G_K-module above.

(3) As the residue field is finite, it suffices to show that its cardinality is prescribed by G_K. If K is a function field (resp. a p-adic field) then the multiplicative group of the residue field is isomorphic to the roots of unity $\mu(K^\times)$ (resp. the roots of unity in $\mu(K^\times)$ with order coprime to the residue characteristic p). Note that the residue characteristic p in the p-adic case is obtained by (a) below.

(4) By using (3) for an arbitrary open subgroup $H \subset G$ we can determine whether K_H/K is unramified (i.e., whether $f_{K_H}/f_K = [G : H]$). The intersection of all such subgroups H is precisely the inertia subgroup I_K.

(5) As the maximal unramified extension is contained in the maximal cyclotomic extension, the Frobenius Frob $\in G_K/I_K$ can be characterized completely by its action on $\mu(\overline{K}^{\times})$.

(6) By [28, Theorem II.4.10], the unit group U_K is isomorphic to the image of I_K in G_K^{ab}. In addition, $U_K^{(1)}$ is the (unique) p-Sylow subgroup of U_K.

(7) Again by [28, Theorem II.4.10], the image of $K^{\times}$ in $\widehat{K^{\times}} \subset G_K^{ab}$ is generated by a lifting of Frob $\in G_K/I_K$ and the image I_K in G_K^{ab}.

(8) We have constructed $K^{\times}$ and U_K as subgroups of $K^{\times}$. Now, $K^{\times}/U_K \approx \mathbb{Z}$ and we can single out the right orientation because uniformizers of $K^{\times}$ are sent to liftings of the Frobenius Frob via the universal norm residue map (cf. [28, Theorem II.4.10]).

(9) This is rather tautological as we have described the image of $K^{\times}$ in G_K^{ab} under the universal norm residue map in group-theoretic terms above.

(a), (b) As a profinite group, G^{ab} has a natural structure of $\widehat{\mathbb{Z}}$-module.[3] In particular, it is a $\mathbb{Z}_l$-module for any prime l. Using the p-adic logarithm we deduce that an open (i.e., finite index) subgroup of U_K is isomorphic to $\mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ (see [27, Theorem II.5.7]). Consequently, the exact sequence (2) shows that $\dim_{\mathbb{Q}_p}(G^{ab} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_p) = [K : \mathbb{Q}_p] + 1$ for the residue characteristic p and $\dim_{\mathbb{Q}_l}(G^{ab} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l) = 1$ for any other prime l. This yields p and $[K : \mathbb{Q}_p]$. (In less fancy terms, $G^{ab} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Z}_l$ is the pro-l completion of G^{ab} and $G^{ab} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_l = G^{ab} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ the quotient by its torsion.)

(c) Use $[K : \mathbb{Q}_p] = e_K f_K$.

□

[3] In fact, let G be a profinite group and $x \in G$. Let $\lambda \in \widehat{\mathbb{Z}}$ and $n_i \in \mathbb{Z}^{\mathbb{N}}$ be a sequence converging to λ. It is easy to see that x^{n_i} converges with respect to the profinite topology of G. In addition, the limit x^{λ} does only depend on λ and not on the sequence n_i. In this way, G is endowed with a natural structure of $\widehat{\mathbb{Z}}$-module. See also [36, Lemma 4.1.1].

Lecture 7: The Theorem of Neukirch-Uchida V

2.7 The Theorem of Neukirch-Uchida: Function fields

In this section, we establish Theorem 12 in the case of function fields. For this, let K be a function field of characteristic p and L an arbitrary global field. By Lemma 16, $G_K \approx G_L$ implies that L is also a function field of characteristic p. This already implies that $\mathrm{Isom}(\overline{L}, \overline{K}) \neq \emptyset$ (i.e., the algebraic closures are non-canonically isomorphic). Let $\Phi : G_K \to G_L$ be an isomorphism. We have to show that there exists a unique $\phi : \overline{K} \to \overline{L}$ such that $\phi(K) = L$ and $\Phi(g) = \phi g \phi^{-1}$.

Uniqueness of ϕ: Suppose $\phi_1, \phi_2 : \overline{K} \to \overline{L}$ are such that $\phi_1 g \phi_1^{-1} = \Phi(g) = \phi_2 g \phi_2^{-1}$ for all $g \in G_K$. In other words, $(\phi_1^{-1}\phi_2) g (\phi_1^{-1}\phi_2)^{-1} = g$ for all $g \in G_K$. This means that g is contained in the center of G_K. However, we observed that G_K has trivial center as a consequence of Lemma 7. Hence, $\phi_1 = \phi_2$.

Existence of ϕ:[4] Let $v \in \mathcal{P}(K)$ and $\widetilde{v} \in \mathcal{P}(\overline{K})$ a place above v. Then, the decomposition group

$$D_{\widetilde{v}} = \{g \in G_K \mid g\widetilde{v} = \widetilde{v}\}$$

is isomorphic to $\mathrm{Gal}(\overline{K_v}/K_v)$ and by Lemma 20 (7) we can 'reconstruct' the multiplicative monoid $K_v^\times \subseteq D_{\widetilde{v}}^{ab}$ from this Galois group. If $w \in \mathcal{P}(L)$ corresponds[5] to v, then $D_{\widetilde{v}}^{ab} \approx D_{\widetilde{w}}^{ab}$ induces a canonical isomorphism $K_v^\times \approx L_w^\times$. Using also assertion (6) from Lemma 20, we get an isomorphism $\phi_I : I_K \to I_L$ by taking restricted products over the various local fields and their unit groups. In addition, from Lemma 20 (9) and Lemma 21 we get the Artin symbol $(\cdot, K) : I_K \to G_K^{ab}$ (resp. $(\cdot, L) : I_L \to G_L^{ab}$) such that we have a commutative diagram

$$\begin{tikzcd}
I_K \arrow[r, "{(\cdot,K)}"] \arrow[d, "\phi_I"'] & G_K^{ab} \arrow[d, "\Phi^{ab}"] \\
I_L \arrow[r, "{(\cdot,L)}"] & G_L^{ab}.
\end{tikzcd}$$

The kernel of the global Artin map $(\cdot, K)$ (resp. $(\cdot, L)$) is $K^\times$ (resp. $L^\times$). In this way, we obtain an isomorphism $\phi : K^\times \to L^\times$ from the above diagram. We also obtain the embeddings $\iota_v : K^\times \hookrightarrow K_v^\times$ for free and the local valuations $\mathrm{ord}_v : K^\times \to \mathbb{Z}$ from Lemma 20 (8). We write $\mathrm{div}(x)$ for the divisor $\sum_{v \in \mathcal{P}(K)} \mathrm{ord}_v(x)[v] \in \bigoplus_{v \in \mathcal{P}(K)} \mathbb{Z}[v]$ as well as $\mathrm{div}_0(x) = \sum_{v \in \mathcal{P}(K), \mathrm{ord}_v(x) > 0} \mathrm{ord}_v(x)[v]$ (resp. $\mathrm{div}_\infty(x) = -\sum_{v \in \mathcal{P}(K), \mathrm{ord}_v(x) < 0} \mathrm{ord}_v(x)[v]$). All of these definitions are compatible – in the obvious sense, which we leave to the reader to make precise – with the isomorphism ϕ as can be easily seen. For $D_1 = \sum_{v \in \mathcal{P}(K)} m_v[v]$ and $D_2 = \sum_{v \in \mathcal{P}(K)} n_v[v]$, we write $D_1 \preccurlyeq D_2$ if and only if $m_v \leq n_v$ for all $v \in \mathcal{P}(K)$. This gives a partial ordering on $\bigoplus_{v \in \mathcal{P}(K)} \mathbb{Z}[v]$. In addition, for each $D = \sum_{v \in \mathcal{P}(K)} m_v[v]$ we call $\mathrm{supp}(D) = \{v \in \mathcal{P}(K) \mid m_v \neq 0\}$ its support.

We want to show that ϕ extends to an additive map $K = K^\times \cup \{0\} \to L = L^\times \cup \{0\}$. By abuse of notation, we denote this map again by ϕ. This slight abuse of notation should not be confusing. Let $K_0 = \bigcap_{v \in \mathcal{P}(K)} \ker(\mathrm{ord}_v)$ (resp. $L_0 = \bigcap_{v \in \mathcal{P}(L)} \ker(\mathrm{ord}_v)$) be the constant functions in K (resp. L). Note that ϕ sends K_0 isomorphically onto L_0 by the group-theoreticity of valuations stated in Lemma 20 (8). We start with establishing additivity on this restriction.

Lemma 22. *$\phi|_{K_0} : K_0 \to L_0$ is additive. Consequently, $\phi|_{K_0}$ is an isomorphism of fields.*

[4] We follow the original proof of Uchida [48] here. In order to prove Theorem 4, Tamagawa gives a stronger result in [46, Lemma 4.7], which (among other refinements) actually claims that the field K can be given explicitly by a group-theoretic construction from G_K (i.e., the field K is group-theoretic in our terminology). Then, $G_K \approx G_L$ immediately implies $K \approx L$.

[5] See the comment below Lemma 6 on how to obtain a bijection $\mathcal{P}(K) \approx \mathcal{P}(L)$ from the bijection $\mathcal{P}(\overline{K}) \approx \mathcal{P}(\overline{L})$ of Lemma 6.

Before we start with the proof of this lemma, let us make some general observations: Let $x, y \in K^\times$ be two non-zero functions and let $v \in \mathcal{P}(K) \setminus \mathrm{supp}(\mathrm{div}(x)) \cup \mathrm{supp}(\mathrm{div}(y))$ be a place such that neither x nor y has a zero or pole at v. Then,

$$x - y \in \mathfrak{m}_v \iff x/y \in U_{K_v}^{(1)} \iff \phi(x)/\phi(y) \in U_{L_w}^{(1)} \iff \phi(x) - \phi(y) \in \mathfrak{m}_w. \tag{4}$$

The first (resp. third) equivalence can be proved easily by considering the expansions of x and y (resp. $\phi(x)$ and $\phi(y)$) in a uniformizer at v (resp. w). The middle equivalence follows from the description of the principal units as in Lemma 20 (6).

In addition, it should not be overlooked that $\phi(-1) = -1$ as we use it in the proof below demands a proof. For $p = 2$, this reduces to $\phi(1) = 1$ and there is nothing to proof. For odd characteristic p, -1 is characterized as the unique element x of $K^\times$ (resp. $L^\times$) such that $x \neq 1$ and $x^2 = 1$. This description in 'multiplicative terms' yields what we want.

Proof of Lemma 22. For the proof, we choose a non-constant $x \in K^\times$ with minimal denominator $\mathrm{div}_\infty(x)$. This means that $\mathrm{div}_\infty(x_0) \preccurlyeq \mathrm{div}_\infty(x)$ implies $\mathrm{div}_\infty(x_0) = 0$ (i.e., $x_0 \in K_0^\times$). Note that also $\phi(x) \in L^\times$ has minimal denominator. Let now $\lambda \in K_0^\times$. Our first goal is to show that

$$\phi(x + \lambda) - \phi(x) = \phi(\lambda). \tag{5}$$

We do this in two steps. First, we show that the left hand side is a constant (i.e., is contained in $L_0^\times$). We can then prove the equality by evaluation at a point. Note that

$$\mathrm{div}_\infty(x + \lambda) = \mathrm{div}_\infty(x)$$

and hence

$$\mathrm{div}_\infty(\phi(x + \lambda)) = \mathrm{div}_\infty(\phi(x)).$$

Consequently,

$$\mathrm{div}_\infty(\phi(x + \lambda) - \phi(x)) \preccurlyeq \mathrm{div}_\infty(\phi(x)).$$

If this inequality is strict then $\phi(x+\lambda) - \phi(x)) \in L_0^\times$ by minimality of $\phi(x)$. Thus, assume that

$$\mathrm{div}_\infty(\phi(x + \lambda) - \phi(x)) = \mathrm{div}_\infty(\phi(x)). \tag{6}$$

We establish that also

$$\mathrm{supp}(\mathrm{div}_0(\phi(x + \lambda) - \phi(x))) \subseteq \mathrm{supp}(\mathrm{div}_\infty(\phi(x)). \tag{7}$$

Let $w \notin \mathrm{supp}(\mathrm{div}_\infty(\phi(x))$ (i.e., $\phi(x)$ has no pole at w) be a place of L and let $v \in \mathcal{P}(K)$ be the place corresponding to w. By compatibility, $\mathrm{ord}_w(\phi(x)) \geq 0$ implies $\mathrm{ord}_v(x) \geq 0$, $\mathrm{ord}_v(x + \lambda) \geq 0$, and thus $\mathrm{ord}_w(\phi(x + \lambda)) \geq 0$. By (4), $\lambda = (x + \lambda) - x \notin \mathfrak{m}_v$ implies $\phi(x + \lambda) - \phi(x) \notin \mathfrak{m}_w$. In other words, $w \notin \mathrm{supp}(\mathrm{div}_0(\phi(x + \lambda) - \phi(x)))$ and we deduce (7). However, (6) and (7) are only simultaneously satisfiable if $\mathrm{div}_0(\phi(x+\lambda) - \phi(x)) = 0$ and hence $\phi(x + \lambda) - \phi(x)) \in L_0^\times$ in any case. Now, we use again (4) in evaluating $\phi(x + \lambda) - \phi(x)$ at an arbitrary $w \in \mathrm{supp}(\mathrm{div}_0(\phi(x + \lambda)))$. Again, let $v \in \mathcal{P}(K)$ correspond to w. By our assumption on w, $\mathrm{ord}_v(x + \lambda) > 0$ and hence $\mathrm{ord}_v(x) = 0$ as λ is a non-zero constant. By (4), it follows that $\phi(x) + \phi(\lambda) = \phi(x) - \phi(-\lambda) \in \mathfrak{m}_v$ and therefore

$$\phi(x + \lambda) - \phi(x) \equiv \phi(\lambda) \mod \mathfrak{m}_v.$$

This immediately implies (5). Let now $\lambda_1, \lambda_2 \in K_0$. We want to show that

$$\phi(\lambda_1 + \lambda_2) = \phi(\lambda_1) + \phi(\lambda_2). \tag{8}$$

The case $\lambda_1 = 0$ or $\lambda_2 = 0$ is trivial so that we may assume that both are non-zero constants. In addition, for $\lambda_2 = -\lambda_1$ the above equality reduces to $\phi(0) = \phi(\lambda_1) + \phi(-\lambda_1)$ and this is easily seen to be true. Therefore, we may and do assume that $\lambda_2 \neq -\lambda_1$ (i.e., $\lambda_1 + \lambda_2 \in K_0^\times$).

Let $y \in K^\times$ have minimal denominator. Note that if y has a minimal denominator then so has $y + \lambda$ for any $\lambda \in K_0$. Applying (5) with $x = y + \lambda_1$ and $\lambda = \lambda_2 \in K_0^\times$ yields

$$\phi((y + \lambda_1) + \lambda_2) - \phi(y + \lambda_1) = \phi(\lambda_2);$$

applying it with $x = y$ and $\lambda = \lambda_1 \in K_0^\times$ yields

$$\phi(y + \lambda_1) - \phi(y) = \phi(\lambda_1);$$

finally applying it with $x = y$ and $\lambda = \lambda_1 + \lambda_2 \in K_0^\times$ yields

$$\phi(y + (\lambda_1 + \lambda_2)) - \phi(y) = \phi(\lambda_1 + \lambda_2),$$

Subtracting the third of the above three equations of the sum of the other two yields (8). □

Lecture 8: The Theorem of Neukirch-Uchida VI

For any two corresponding places $v \in \mathcal{P}(K)$ and $w \in \mathcal{P}(L)$, $\phi : K^\times \to L^\times$ induces an isomorphism $U_{K_v}/U_{K_v}^{(1)} \to U_{L_w}/U_{L_w}^{(1)}$ of multiplicative monoids by Lemma 20 (6). For each local field F of positive characteristic, $U_F/U_F^{(1)}$ can be identified canonically with the multiplicative group of the residue field $\mathcal{O}_F/\mathfrak{m}_F$ by (4). Hence, ϕ induces canonically isomorphisms $\overline{\phi}_v : k_v^\times \to l_w^\times$ where $k_v^\times$ (resp. $l_w^\times$) is the residue field of K_v (resp. L_w). Abusing notation, we write $\overline{\phi}_v : k_v \to l_w$ for the extension of $\overline{\phi}_v$ satisfying $\overline{\phi}_v(0) = 0$.

Lemma 23. *$\overline{\phi}_v : k_v \to l_w$ is additive (i.e., an isomorphism of fields).*

Proof. This is an obvious consequence of Lemma 22 if the constants K_0 surject onto k_v. In the general case, there is a finite extension K_0 of K and a lifting $\widetilde{v} \in \mathcal{P}(K_0)$ so that its constants K_0 surject onto $k_{0,\widetilde{v}}$. Let L_0 be the field corresponding to K_0 via Φ and $\widetilde{w} \in \mathcal{P}(L_0)$ the place corresponding to $\widetilde{v}$. Checking various compatibilities, one can deduce the additivity of $\overline{\phi}_v : k_v \to l_w$ from the additivity of $\overline{\phi}_{0,\widetilde{v}} : k_{0,\widetilde{v}} \to l_{0,\widetilde{w}}$. □

With these ample preparations, we can finally prove that $\phi : K \to L$ is additive. As ϕ is already multiplicative, it suffices to show that $\phi(x+1) = \phi(x)+1$ for all $x \in K$; for this implies

$$\phi(x+y) = \phi(y)\phi(x/y+1) = \phi(y)(\phi(x/y)+1) = \phi(y)(\phi(x)/\phi(y)+1) = \phi(x)+\phi(y)$$

for all $x, y \in K$. Let $v \notin \operatorname{supp}(\operatorname{div}_\infty(x))$ be a place of K and w the corresponding place of L. By Lemma 23, we have

$$\phi(x+1) \equiv \overline{\phi}_v(x+1) \equiv \overline{\phi}_v(x) + \overline{\phi}_v(1) \equiv \phi(x) + \phi(1) \equiv \phi(x) + 1 \mod \mathfrak{m}_w.$$

As this congruence is true for all but finitely many places $w \in \mathcal{P}(L)$, we have $\phi(x+1) = \phi(x)+1$. Hence, $\phi : K \to L$ is an isomorphism of fields. Furthermore, for any open subgroup H of G_K we obtain an isomorphism $\phi_H : \overline{K}^H \to \overline{L}^{\Phi(H)}$ by the above procedure. From their very construction, these must be compatible with each other. Thus we obtain an isomorphism $\phi : \overline{K} \to \overline{L}$ prolonging $\phi : K \to L$, abusing notation.

For Theorem 12, it remains to demonstrate that $\Phi(g) = \phi g \phi^{-1}$ for any $g \in G_K$. This follows from the commutativity of the following diagram:

$$\begin{tikzcd}
& L_0 \arrow[rr] \arrow[dd, "\Phi(g)"] & & I_{L_0} \arrow[rr] \arrow[dd, "\Phi(g)"] & & G_{L_0}^{ab} \arrow[dd, "\Phi(g)(\cdot)\Phi(g)^{-1}"] \\
K_0 \arrow[ur, "\phi"] \arrow[rr] \arrow[dd, "g"'] & & I_{K_0} \arrow[ur, "\phi_I"] \arrow[rr] \arrow[dd, "g"'] & & G_{K_0}^{ab} \arrow[ur, "\Phi^{ab}"] \arrow[dd, "g(\cdot)g^{-1}"] & \\
& L_0 \arrow[rr] & & I_{L_0} \arrow[rr] & & G_{L_0}^{ab} \\
K_0 \arrow[ur, "\phi"] \arrow[rr] & & I_{K_0} \arrow[ur, "\phi_I"'] \arrow[rr] & & G_{K_0}^{ab}. \arrow[ur, "\Phi^{ab}"'] &
\end{tikzcd}$$

Here, most commutation relations come directly from the construction. The only external ingredient is the commutativity of the right front and right back square, which is mainly [28, Theorem 1.11.d] (cf. the section on local class field theory above).

2.8 The Theorem of Neukirch-Uchida: General number fields

Let K and L be number fields. In this section, we finally establish Theorem 12 for them. For this, let $\Phi : G_K \to G_L$ be an isomorphism. We want to show that there exists a unique $\phi : \overline{L} \to \overline{K}$ such that $\phi(L) = K$ and $\Phi(g) = \phi^{-1} g \phi$.

Uniqueness of ϕ: This is proven in the same way as for function fields.

Existence of ϕ: For each normal open subgroup H of G_K, Φ induces an isomorphism $\Phi_H : G_K/H \to G_L/\Phi(H)$. By using compactness, it suffices to establish Lemma 24 below. For this, we introduce the set

$$\mathrm{Isom}_{L,K}(\overline{L},\overline{K}) = \{\phi \in \mathrm{Isom}(\overline{L},\overline{K}) \mid \phi(L) = K \text{ and } \phi|_L : L \to K \text{ is an isomorphism}\},$$

which has a natural topology as a pro-set; we describe a basis for this topology: With each finite normal extension $L \subset N_1 \subset \overline{L}$, we can associate a unique finite normal extension $K \subset N_2 \subseteq \overline{K}$. Indeed, if $\phi \in \mathrm{Isom}_{L,K}(\overline{L},\overline{K})$ then we set $N_2 = \phi(N_1)$. For any other $\phi' \in \mathrm{Isom}_{L,K}(\overline{L},\overline{K})$, there exists some $\psi \in G_K$ such that $\phi' = \psi \circ \phi$. As N_1 and hence N_2 are normal, it follows that $\phi'(N_1) = \psi(\phi(N_1)) = \psi(N_2) = N_2$. Hence, N_2 does not depend on the choice of ϕ and may be associated with N_1. For any N_1 with associated N_2, there is a restriction map

$$\mathrm{res}_{N_1} : \mathrm{Isom}_{L,K}(\overline{L},\overline{K}) \to \mathrm{Isom}_{L,K}(N_1,N_2)$$

and $\mathrm{Isom}_{L,K}(\overline{L},\overline{K}) = \varprojlim_{N_1,N_2} \mathrm{Isom}_{L,K}(N_1,N_2)$ as sets. The profinite topology on $\mathrm{Isom}(\overline{L},\overline{K})$ is the inverse limit of the discrete topologies on the finite sets $\mathrm{Isom}(N_1,N_2)$. This topology coincides with the topology induced from the bijection $\mathrm{Isom}_{L,K}(\overline{L},\overline{K}) \approx G_L$ (resp. $\mathrm{Isom}_{L,K}(\overline{L},\overline{K}) \approx G_K$) induced by post-composition (resp. pre-composition) with any element of $\mathrm{Isom}_{K,L}(\overline{K},\overline{L})$.

Lemma 24. *Let H be a normal open subgroup of G_K such that its fixed field $K_0 = \overline{K}^H$ is normal over $\mathbb{Q}$ (!). Then, there exists an isomorphism ϕ_H in $\mathrm{Isom}_{L,K}(\overline{L},\overline{K})$ such that*

$$(\phi_H)^* : G_K \to G_L,\ g \mapsto \phi_H^{-1} \circ g \circ \phi_H,$$

induces $\Phi_H : G_K/H \to G_L/\Phi(H)$.

We can indicate now how Lemma 24 implies Theorem 12. For each H as in Lemma 24, the set

$$K_H = \{\phi \in \mathrm{Isom}_{L,K}(\overline{L},\overline{K}) \mid \mathrm{res}_{\overline{K}^H}(\phi)^{-1} \circ \sigma \circ \mathrm{res}_{\overline{K}^H}(\phi) = \Phi_H(\sigma) \text{ for all } \sigma \in \mathrm{Gal}(\overline{K}^H/K)\}$$

is compact and ϕ induces Φ if and only if $\phi \in \bigcap_H K_H$. By Lemma 24, each K_H is non-empty. We infer that $\bigcap_H K_H$ is non-empty, settling the existence part of the Neukirch-Uchida Theorem.[6]

Let L/K be a Galois extension of number fields and $\mathfrak{p}$ (resp. $\mathfrak{P}$) a prime ideal of K (resp. L) such that $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is unramified. Then, we have inertia group $I(\mathfrak{P}|\mathfrak{p}) = 1$ and decomposition group $D(\mathfrak{P}|\mathfrak{p}) = \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$ with $l_{\mathfrak{P}}$ (resp. $k_{\mathfrak{p}}$) the residue field of $L_{\mathfrak{P}}$ (resp. $K_{\mathfrak{p}}$). In this situation, we write $\left(\frac{L/K}{\mathfrak{P}}\right)$ for the unique (!) element in $D(\mathfrak{P}|\mathfrak{p}) \subset \mathrm{Gal}(L/K)$ corresponding to the Frobenius of $\mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$. In other words, $\left(\frac{L/K}{\mathfrak{P}}\right)$ is the unique element $\sigma \in D(\mathfrak{P}|\mathfrak{p})$ such that

$$\sigma x \equiv x^p \mod \mathfrak{P}$$

for all $x \in \mathcal{O}_L$. From this description, it is obvious that for any homomorphism $\phi : L \to L'$ we have

$$\left(\frac{\phi(L)/\phi(K)}{\phi(\mathfrak{P})}\right) = \phi \circ \left(\frac{L/K}{\mathfrak{P}}\right) \circ \phi^{-1}.$$

[6] This is a standard argument: Let K_n, $n \in \mathbb{N}$, be a descending chain of non-empty compact (= quasi-compact and Hausdorff) sets. $U_n = K_0 \setminus K_n$, $n \in \mathbb{N}$, is an ascending chain of open subsets of K_0. Furthermore, $\bigcup_n U_n = K_0$ if $\bigcap_n K_n = \emptyset$. In this case, there is some n_0 such that $K_0 = \bigcup_n U_n = U_{n_0} = K_0 \setminus K_{n_0}$ and hence $K_{n_0} = \emptyset$ – a contradiction.

Lecture 9: The Theorem of Neukirch-Uchida VII

Proof of Lemma 24. **We prove the lemma first in the case that $G_K/H \approx \mathrm{Gal}(K_0/K)$ is cyclic with generator σ.** Write $L_0 = \overline{L}^{\Phi(H)}$. By the Cebotarev density theorem (cf. [27, Theorem VII.13.4]), there exists a rational prime p that is unramified in K_0 and a prime $\mathfrak{p}$ above p such that $\sigma = \left(\frac{K_0/\mathbb{Q}}{\mathfrak{p}}\right)$. There is a lifting $\widetilde{\sigma} \in G_K$ and a place $v|\mathfrak{p}$ such that $\widetilde{\sigma} \in D_v$ is sent to the Frobenius $x \mapsto x^p$ of $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ by the canonical map $D_v \twoheadrightarrow D_v/I_v = \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. By the local correspondence established in Lemma 6, Φ associates with $v \in \mathcal{P}_f(\overline{K})$ a place $w \in \mathcal{P}_f(\overline{L})$ such that $D_v \approx D_w$. As local Galois groups determine the residue characteristics of the underlying p-adic fields (Lemma 20 (a)) w lies also over p. By restriction, w gives rise to a prime $\mathfrak{p}'$ of L_0 over p. By Lemma 20 (c), p is unramified in $L_0/\mathbb{Q}$. There exists an isomorphism $\phi_H \in \mathrm{Isom}(\overline{L}, \overline{K})$ (not $\mathrm{Isom}_{L,K}(\overline{L}, \overline{K})$!) such that $\phi_H(\mathfrak{p}') = \mathfrak{p}$ by Hilbert's ramification theory (see e.g. [27, Theorem I.9.1]). In addition, $\phi_H(L_0) = K_0$ – in other words, $\phi_H^{-1}\Phi(H)\phi_H = H$ – follows directly from our version of the Neukirch-Uchida theorem for normal number fields. Indeed, $G_{\phi_H(L_0)} \approx G_{L_0}$ and Φ induces an isomorphism $G_{L_0} \approx G_{K_0}$ so that we may apply Lemma 19 to $K_0, \phi_H(L_0) \subset \overline{K}$.

With any $g \in G_K$ we can associate now two (in general different) elements of $\mathrm{Gal}(\overline{L}/\mathbb{Q})$, both $\Phi(g)$ and $(\phi_H)^*(g) = \phi_H^{-1} g \phi_H$. The assertion of the lemma boils down to the statement that their restrictions to $\mathrm{Gal}(L_0/\mathbb{Q})$ are equal. As σ generates $\mathrm{Gal}(K_0/K)$, it suffices to prove this with $g = \widetilde{\sigma}$. On the one hand, $\Phi(\widetilde{\sigma})$ is a Frobenius of $D_w = \Phi(D_v)$ by Lemma 20 (5) and hence

$$\Phi(\widetilde{\sigma})|_{L_0} = \left(\frac{L_0/\mathbb{Q}}{\mathfrak{p}'}\right).$$

On the other hand, $\phi_H(\mathfrak{p}') = \mathfrak{p}$ implies that

$$\phi_H^{-1}|_{L_0} \left(\frac{K_0/\mathbb{Q}}{\mathfrak{p}}\right) \phi_H|_{L_0} = \left(\frac{\phi_H^{-1}(K_0)/\phi_H^{-1}(\mathbb{Q})}{\phi_H^{-1}(\mathfrak{p})}\right) = \left(\frac{L_0/\mathbb{Q}}{\mathfrak{p}'}\right).$$

This shows that $(\phi_H)^*$ induces Φ_H. In addition, we infer

$$\phi_H(L) = \phi_H(\overline{L}^{\langle \Phi(H), \Phi(\widetilde{\sigma})\rangle}) = \phi_H(\overline{L}^{\langle \phi_H H \phi_H^{-1}, \phi_H \widetilde{\sigma} \phi_H^{-1}\rangle}) = \overline{K}^{\langle H, \widetilde{\sigma}\rangle} = K_0^{\langle \sigma \rangle} = K.$$

In other words, $\phi_H \in \mathrm{Isom}_{L,K}(\overline{L}, \overline{K})$. This completes the proof in the cyclic case.

From now on, we consider general $G_K/H = \mathrm{Gal}(K_0/K)$. In the sequel, we identify both $\overline{K}$ and $\overline{L}$ with $\overline{\mathbb{Q}}$. In particular, we consider both K and L as subfields of $\overline{\mathbb{Q}}$. Evidently, this does not lead to any loss of generality. Write $N = \overline{K}^H = \overline{L}^{\Phi(H)}$ and $G = \mathrm{Gal}(N/\mathbb{Q})$. Let p be a prime such that $p > \#G = n$ and let $\widetilde{G} = \mathbb{F}_p[G] \rtimes_\rho G$ be the semidirect product such that $\rho(g) \in \mathrm{Aut}(\mathbb{F}_p[G])$ is multiplication with g considered as element of the group ring $\mathbb{F}_p[G]$. By Lemma 25, the embedding problem

$$\begin{tikzcd}
 & & & G_{\mathbb{Q}} \arrow[dl, dashed, "?"'] \arrow[d] & \\
1 \arrow[r] & \mathbb{F}_p[G] \arrow[r, "\iota"'] & \widetilde{G} \arrow[r, "\kappa"'] & G \arrow[r] & 1
\end{tikzcd} \tag{9}$$

has a proper solution. This means that there exists a normal extension M/N such that $\mathbb{F}_p[G] = \mathrm{Gal}(M/N)$; we use this identification without explicit mention in the sequel. With this, we have $g \circ \lambda \circ g^{-1} = \rho(g)(\lambda) = g \cdot \lambda$ for all $\lambda \in \mathrm{Gal}(M/N)$ and all $g \in G$. Additionally, $\Phi : G_K \to G_L$ induces a homomorphism

$$\Phi_0 : \mathbb{F}_p[G] = \mathrm{Gal}(M/N) \longrightarrow \mathrm{Gal}(M/N) = \mathbb{F}_p[G].$$

We claim that Φ_0 is of a rather simple shape. Namely, we assert that there exists some $h \in G$ such that $\Phi_0(\lambda) = h \cdot \lambda$ for all $\lambda \in \mathbb{F}_p[G]$. As a first approximation, we prove for each $\lambda \in \mathbb{F}_p[G]$ the existence of some $h_\lambda \in G$ with $\Phi_0(\lambda) = h_\lambda \cdot \lambda$. This is clear if $\lambda = 0$ so that we work with a non-zero $\lambda \in \mathbb{F}_p[G]$ from now on. Let K_1 (resp. L_1) be the fixed field of $\langle \lambda \rangle \subseteq \mathrm{Gal}(M/N)$ (resp. $\langle \Phi_0(\lambda) \rangle \subseteq \mathrm{Gal}(M/N)$). As $\mathrm{Gal}(M/K_1) = \langle \lambda \rangle$ is cyclic and M is normal, the cyclic case of Lemma 24 shows that there exists some $\phi \in \mathrm{Isom}_{L_1,K_1}(\overline{\mathbb{Q}}, \overline{\mathbb{Q}})$ such that

$$\phi^* : G_{K_1} \to G_{L_1},\ g \mapsto \phi^{-1} \circ g \circ \phi,$$

induces $\Phi_0|_{\mathrm{Gal}(M/K_1)} : \mathrm{Gal}(M/K_1) \to \mathrm{Gal}(M/L_1)$ by restriction. In other words,

$$\Phi_0(\lambda) = (\phi|_M)^{-1} \circ \lambda \circ \phi|_M = h_\lambda \cdot \lambda, \text{ where } h_\lambda = (\phi|_N)^{-1} \in G.$$

It follows that $\mathbb{F}_p[G] = \bigcup_{h \in G} U_h$ with $U_h = \{\lambda \in \mathbb{F}_p \mid \Phi_0(\lambda) = h \cdot \lambda\}$. If no U_h is equal to $\mathbb{F}_p[G]$ then $\#U_h \leq p^{n-1}$ for all $h \in G$. This implies

$$p^n = \#\mathbb{F}_p[g] \leq \sum_{h \in G} \#U_h \leq np^{n-1} < p^n$$

by assumption on p. As this is a clear contradiction, there exists some $h \in G$ such that $\Phi_0(\lambda) = h \cdot \lambda$ for all $\lambda \in \mathbb{F}_p[G]$. In addition, $h = h_\lambda = (\phi|_N)^{-1}$. For given $g \in \mathrm{Gal}(N/K)$, we have to prove that

$$\Phi_H(g) = (\phi|_N)^{-1} \circ g \circ \phi|_N = hgh^{-1}.$$

We have $\Phi_0(g) = hg$ by the above and $\Phi_0(g) = \Phi_0(g \cdot 1) = \Phi_H(g) \cdot \Phi_0(1)$ follows from a direct consideration. Combining these gives $h \cdot g = \Phi_H(g)\Phi_0(1) = \Phi_H(g)h$ and hence $hgh^{-1} = \Phi_H(g)$ as claimed. □

The following lemma and its proof are beyond the scope of this lecture. In order to formulate it, we introduce some terminology first. Let K be an arbitrary field. A Hilbert set of K is a subset of K^r, r an arbitrary positive integer, of the form

$$\{(a_1, \ldots, a_r) \in K^r \mid f(a_1, \ldots, a_r, X) \in K[X] \text{ defined and irreducible}\},$$

where $f_i(T_1, \ldots, T_r, X) \in K(T_1, \ldots, T_r)[X]$, $i = 1, \ldots, m$, are irreducible separable polynomials over $K(T_1, \ldots, T_r)$. A field is called Hilbertian if every Hilbert set is nonempty. An important class of Hilbertian fields are number fields (see [8, Section 13.3] for a proof). In contrast, p-adic local fields are not Hilbertian. In fact, the absolute Galois groups of Hilbertian fields can never be small (i.e., have only finitely many subgroups of index n for each positive integer n) by [8, Lemma 16.11.5] whereas the absolute Galois group of a p-adic local field is always small by Lemma 17.

Next we introduce embedding problems. Let K be some base field with absolute Galois group $\Gamma = \mathrm{Gal}(\overline{K}/K)$. In addition, let $N|K$ a finite normal extension with Galois group $G = \mathrm{Gal}(N/K)$. Let $\widetilde{G}$ be a group extension of G by some group H. We search for homomorphisms $\widetilde{\varphi} : G \to \widetilde{G}$ such that the following diagram commutes:

$$\begin{tikzcd}
 & & & \Gamma \arrow[dl, dashed, "\widetilde{\varphi}"'] \arrow[d, "\varphi"] & \\
1 \arrow[r] & H \arrow[r, "\iota"'] & \widetilde{G} \arrow[r, "\kappa"'] & G \arrow[r] & 1
\end{tikzcd} \tag{10}$$

These homomorphisms $\widetilde{\varphi}$ are called the solutions of the embedding problem (10). A solution is called proper if it is an epimorphism. Proper solutions are directly related to inverse Galois theory. Indeed, associating with a proper solution the fixed field $\widetilde{N} = N^{\ker(\widetilde{\varphi})}$, proper solutions correspond uniquely to normal extensions $N \subseteq \widetilde{N} \subseteq \overline{K}$ such that $\mathrm{Gal}(\widetilde{N}/N) = H$. Finally, the embedding problem is called split if the horizontal exact sequence in (10) splits and abelian if H is an abelian group.

Lemma 25. *[19, Theorem IV.2.4] Let K be a Hilbertian field. Any split embedding problem with abelian kernel has a proper solution.*

For historical completeness, it should be mentioned that we only need the case where K is a number field. In this special case, Lemma 25 appeared first in [42] and was proven by mainly class field theoretic tools. In addition, a more Galois cohomological proof of the above lemma is given in [28].

Bibliography

[1] *Revêtements étales et groupe fondamental (SGA 1).* Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].

[2] Emil Artin. Kennzeichnung des Körpers der reellen algebraischen Zahlen. *Abh. Math. Sem. Univ. Hamburg*, 3(1):319–323, 1924.

[3] Emil Artin and John Tate. *Class field theory.* AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[4] Fedor A. Bogomolov. On two conjectures in birational algebraic geometry. In *Algebraic geometry and analytic geometry (Tokyo, 1990)*, ICM-90 Satell. Conf. Proc., pages 26–52. Springer, Tokyo, 1991.

[5] Volker Diekert. Über die absolute Galoisgruppe dyadischer Zahlkörper. *J. Reine Angew. Math.*, 350:152–172, 1984.

[6] Antonio J. Engler and Alexander Prestel. *Valued fields.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.

[7] I. B. Fesenko and S. V. Vostokov. *Local fields and their extensions*, volume 121 of *Translations of Mathematical Monographs.* American Mathematical Society, Providence, RI, second edition, 2002. With a foreword by I. R. Shafarevich.

[8] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics].* Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[9] Alexander Grothendieck. Brief an G. Faltings. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 49–58. Cambridge Univ. Press, Cambridge, 1997. With an English translation on pp. 285–293.

[10] Richard Hain. Rational points of universal curves. *J. Amer. Math. Soc.*, 24(3):709–769, 2011.

[11] David Harari and Tamás Szamuely. Galois sections for abelianized fundamental groups. *Math. Ann.*, 344(4):779–800, 2009. With an appendix by E. V. Flynn.

[12] Yuichiro Hoshi. Existence of nongeometric pro-p Galois sections of hyperbolic curves. *Publ. Res. Inst. Math. Sci.*, 46(4):829–848, 2010.

[13] Uwe Jannsen and Kay Wingberg. Die Struktur der absoluten Galoisgruppe $\mathfrak{p}$-adischer Zahlkörper. *Invent. Math.*, 70(1):71–98, 1982/83.

[14] Moshe Jarden and Jürgen Ritter. On the characterization of local fields by their absolute Galois groups. *J. Number Theory*, 11(1):1–13, 1979.

[15] Wolfgang Jenkner. Les corps p-adiques dont les groupes de Galois absolus sont isomorphes. *Astérisque*, (209):14, 221–226, 1992. Journées Arithmétiques, 1991 (Geneva).

[16] Minhyong Kim. The motivic fundamental group of $\mathbb{P}^1\backslash\{0,1,\infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[17] Jochen Koenigsmann. On the 'section conjecture' in anabelian geometry. *J. Reine Angew. Math.*, 588:221–235, 2005.

[18] Edmund Landau. Über die Darstellung definiter binärer Formen durch Quadrate. *Math. Ann.*, 57(1):53–64, 1903.

[19] Gunter Malle and B. Heinrich Matzat. *Inverse Galois theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[20] Shinichi Mochizuki. The profinite Grothendieck conjecture for closed hyperbolic curves over number fields. *J. Math. Sci. Univ. Tokyo*, 3(3):571–627, 1996.

[21] Shinichi Mochizuki. A version of the Grothendieck conjecture for p-adic local fields. *Internat. J. Math.*, 8(4):499–506, 1997.

[22] Shinichi Mochizuki. The local pro-p anabelian geometry of curves. *Invent. Math.*, 138(2):319–423, 1999.

[23] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[24] Jürgen Neukirch. Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen. *J. Reine Angew. Math.*, 238:135–147, 1969.

[25] Jürgen Neukirch. Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper. *Invent. Math.*, 6:296–314, 1969.

[26] Jürgen Neukirch. Über die absoluten Galoisgruppen algebraischer Zahlkörper. In *Journées Arithmétiques de Caen (Univ. Caen, Caen, 1976)*, pages 67–79. Astérisque, No. 41–42. Soc. Math. France, Paris, 1977.

[27] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[28] Jürgen Neukirch. *Class Field Theory*. Springer, 2013.

[29] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[30] F. Pop and J. Stix. Arithmetic in the fundamental group of a p-adic curve: On the p-adic section conjecture for curves. *ArXiv e-prints*, November 2011.

[31] Florian Pop. On Grothendieck's conjecture of birational anabelian geometry. *Ann. of Math. (2)*, 139(1):145–182, 1994.

[32] Florian Pop. On Grothendieck's conjecture of birational anabelian geometry II. Heidelberg-Mannheim Preprint Series Arithmetik II (No 16), April 1995.

[33] Florian Pop. Alterations and birational anabelian geometry. In *Resolution of singularities (Obergurgl, 1997)*, volume 181 of *Progr. Math.*, pages 519–532. Birkhäuser, Basel, 2000.

[34] Florian Pop. Elementary equivalence versus isomorphism. *Invent. Math.*, 150(2):385–408, 2002.

[35] Florian Pop. On the birational anabelian program initiated by Bogomolov I. *Invent. Math.*, 187(3):511–533, 2012.

[36] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics].* Springer-Verlag, Berlin, second edition, 2010.

[37] Jürgen Ritter. $\mathfrak{p}$-adic fields having the same type of algebraic extensions. *Math. Ann.*, 238(3):281–288, 1978.

[38] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2000.

[39] Thomas Scanlon. Infinite finitely generated fields are biinterpretable with $\mathbb{N}$. *J. Amer. Math. Soc.*, 21(3):893–908, 2008.

[40] Thomas Scanlon. Erratum to "Infinite finitely generated fields are biinterpretable with $\mathbb{N}$" [mr2393432]. *J. Amer. Math. Soc.*, 24(3):917, 2011.

[41] Friedrich Karl Schmidt. Mehrfach perfekte Körper. *Math. Ann.*, 108(1):1–25, 1933.

[42] Arnold Scholz. Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoisscher Gruppe. *Math. Z.*, 30(1):332–356, 1929.

[43] Jakob Stix. On the period-index problem in light of the section conjecture. *Amer. J. Math.*, 132(1):157–180, 2010.

[44] Tamás Szamuely. Groupes de Galois de corps de type fini (d'après Pop). *Astérisque*, (294):ix, 403–431, 2004.

[45] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 2009.

[46] Akio Tamagawa. The Grothendieck conjecture for affine curves. *Compositio Math.*, 109(2):135–194, 1997.

[47] Kôji Uchida. Isomorphisms of Galois groups. *J. Math. Soc. Japan*, 28(4):617–620, 1976.

[48] Kôji Uchida. Isomorphisms of Galois groups of algebraic function fields. *Ann. of Math. (2)*, 106(3):589–598, 1977.