ENCODING ARITHMETIC IN GALOIS GROUPS

Jochen Koenigsmann

Oxford

Trinity Term 2022

Encoding Arithmetic in Galois groups

TT 2022

Lecture 1: Introduction

§1 Classical Results

<u>Galois</u>: $f \in K[X]$ irr. sep., L = splitting fld. of f/K

Then: f solvable by radicals $\Leftrightarrow$ $\mathrm{Gal}(L/K)$ soluble

<u>Kronecker-Weber</u> $F/\mathbb{Q}$ finite Galois

Then: F cyclotomic $\Leftrightarrow$ $\mathrm{Gal}(F/\mathbb{Q})$ abelian

§2 Absolute Galois groups

<u>Def.</u>: K field with fixed sep. closure K^{sep}

Then $G_K := \mathrm{Gal}(K^{sep}/K) = \varprojlim_{\substack{K \subseteq L \subseteq K^{sep} \\ \text{finite Galois}}} \mathrm{Gal}(L/K)$

is the <u>absol. Gal. gp.</u> of K (as profinite Gp.)

<u>Examples</u> • $K = K^{sep} \Leftrightarrow G_K = \{1\}$

• K real closed $\overset{\text{Tarski}}{\Leftrightarrow}$ $K \equiv \mathbb{R}$ $\overset{\text{Artin-Schreier}}{\Leftrightarrow}$ $G_K \cong \mathbb{Z}/2\mathbb{Z} \cong G_{\mathbb{R}}$

• K p-adically cl. $\underset{\text{Macintyre}}{\overset{\text{AKE/}}{\Leftrightarrow}}$ $K \equiv \mathbb{Q}_p$ $\overset{\text{K.}}{\Leftrightarrow}$ $G_K \cong G_{\mathbb{Q}_p}$

new elementary proof in this lecture

<u>Main Theme</u> of the Lecture:

What does G_K know about K?

<u>Def.</u>: K <u>elementarily characterized</u> by G_K

if for all fields F: $F \equiv K \Leftrightarrow G_F \cong G_K$

Thm. (K.'98) K el.^y char. by G_K iff $K \equiv$ one of

① $\mathbb{R}$

② $\mathbb{Q}_p$ or all finite almost abelian $L/\mathbb{Q}_p$

③ $L((\mathbb{Z}_{(q)}))$ where L as in ② and q prime $(= p$ or $\neq p)$

④ a weird henselian fld. which conjecturally doesn't exist

Variation · K el.^y determined by G_K if $G_F \cong G_K \Rightarrow F \equiv K$

· K el.^y characterised by $Th(G_K)$ if $G_F \equiv G_K \Leftrightarrow F \equiv K$

(always have $\Leftarrow$) — language of inv. system $S(G)$ for prof. grs. G

No examples known where variants differ.

Clear: char. by $Th(G_K) \Rightarrow$ char. by $G_K \Rightarrow$ det. by G_K

Counterexamples: $\mathbb{C}$, $\mathbb{F}_q$, $\mathbb{C}((t))$ and $\mathbb{Q}$: $G_{\mathbb{Q}} \cong G_{\mathbb{Q}((\mathbb{Q}))}$

[will also see later: $\mathbb{Q}^* \underset{\neq}{\succ} \mathbb{Q} \Rightarrow G_{\mathbb{Q}^*} \not\cong G_{\mathbb{Q}}$]

§3 Fields with the absolute Galois group of $\mathbb{Q}$

AGC: Absolute Galois Conjecture (K any field)

$G_K \cong G_{\mathbb{Q}} \Rightarrow \exists$ hens. val. on K with divisible value gr. and with res. fld. $\cong \mathbb{Q}$

[$\Leftarrow$ clear from general Galois theory of henselian flds]

Note that then $K \equiv \mathbb{Q}$ or $K \equiv \mathbb{Q}((\mathbb{Q}))$, so $\mathbb{Q}$ is $\frac{1}{2}$-det. by $G_{\mathbb{Q}}$.

Conjollary $K \cong \mathbb{Q} \Leftrightarrow G_K \cong G_{\mathbb{Q}}$ and $\forall x,y,z\, [x \cdot y \cdot z = 0 \vee x^3 + y^3 \neq z^3]$

Thm. (K.'15) K any field with $G_K \cong G_{\mathbb{Q}}$

$\Rightarrow$ · char $K = 0$

· K has unique ordering & $\forall p \in \mathbb{P}$ a unique p-adic v_p

· res: $G_K \to G_{\mathbb{Q}}$ is an isomorphism.

· K satisfies a lot of alg. number theory: Čebotarev Density Thm., LGP for quadr. forms, Kronecker-Weber, quadratic reciprocity, ...

Corollary (unconditional)

$K \cong \mathbb{Q} \iff G_K \cong G_{\mathbb{Q}}$ and $\mathcal{C}_a(K) = \mathcal{C}_a(\mathbb{Q})$ for all squ. free $a \in \mathbb{Z}\setminus\{0\}$

where $\mathcal{C}_a : Y^2 = a \cdot X(X^2-1)(X^2-4)$

BSC : Birational Section Conj. $/\mathbb{Q}$ (in Grothendieck's anabelian geometry)

$\mathcal{C}$ smooth proj. alg. curve over $\mathbb{Q}$.

Then any section s of $1 \to G_{\tilde{\mathbb{Q}}(\mathcal{C})} \to G_{\mathbb{Q}(\mathcal{C})} \underset{\underset{s}{\dashleftarrow}}{\xrightarrow{\pi}} G_{\mathbb{Q}} \to 1$

$$\begin{tikzcd}
 & & \widetilde{\mathbb{Q}(\mathcal{C})} \arrow[dl, dash, "G_{\mathbb{Q}}"'] \arrow[dd, dash] \arrow[dddd, dash, bend left=60, "G_{\mathbb{Q}(\mathcal{C})}"] \\
 & \mathrm{Fix}\, s(G_{\mathbb{Q}}) \arrow[dd, dash] & \\
 & & \tilde{\mathbb{Q}}(\mathcal{C}) \arrow[dd, dash, "G_{\mathbb{Q}}", "\pi"'] \\
\tilde{\mathbb{Q}} \arrow[urr, dash] \arrow[dd, dash, "G_{\mathbb{Q}}"'] & \mathrm{Fix}\, D_P \arrow[dr, dash] & \\
 & & \mathbb{Q}(\mathcal{C}) \\
\mathbb{Q} \arrow[urr, dash] & &
\end{tikzcd}$$

comes from a $\mathbb{Q}$-rat. $P \in \mathcal{C}(\mathbb{Q})$, i.e., $s(G_{\mathbb{Q}}) \leq D_P$, where D_P is a decomposition subgroup of $G_{\mathbb{Q}(\mathcal{C})}$ w.r.t. the discrete val. v_P on $\mathbb{Q}(\mathcal{C})$ associated to P.

Thm. AGS and BSC are equivalent.

In particular, it suffices to show AGS for t.d. $K/\mathbb{Q} = 1$.

Model-theoretic AGC (K any field)

$G_K \equiv G_{\mathbb{Q}} \Rightarrow K$ admits henselian val. with divisible value gp. & res. fld. $\equiv \mathbb{Q}$

[$\Leftarrow$ clear from Cherlin-vdDries-Macintyre '80]

N.B.: Model-theoretic AGC $\Rightarrow$ AGC :

From Corollary above: $G_K \cong G_{\mathbb{Q}}$ & $K \equiv \mathbb{Q} \Rightarrow K \cong \mathbb{Q}$

Model-theoretic AGC becomes easier when assuming $G_{\mathbb{Q}} \precsim G_K$ where the embedding comes from res: $G_K \to G_{\mathbb{Q}}$ [will still imply AGC]

§ 4 Plan for the lecture

week 2 : Val. theory : coarsenings, henselianity] classical
week 3 : Galois theory over henselian flds.]

week 4 : Henselianity encoded in G_K

week 5 : Galois code for p-adically cl. fields

week 6 : Fields with the absolute Gal. gp. of $\mathbb{Q}$

week 7 : Grothendieck's Anabelian Geometry

week 8 : Fields with $G_K \equiv G_{\mathbb{Q}}$, or
Fields el.^{y} characterized by G_K

Exercise

Give at least 3 reasons why $G_{\mathbb{Q}}$ is infinite

[other than that o/w we would know the Inverse Galois Problem to be unsolvable].

Lecture 2: Basics from valuation theory

Engler / Prestel: Valued Fields (Springer 2005)

$\boxed{\S 1 \text{ Valuations, valuation rings, places}}$

__Def.:__ K field, $\Gamma = \langle \Gamma; +, 0, \leq \rangle$ ordered abelian group

$v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ is a __valuation__ on K

if for any $x, y \in K$ (i) $v(x) = \infty \iff x = 0$

(ii) $v(x \cdot y) = v(x) + v(y)$

(iii) $v(x+y) \geq \min\{v(x), v(y)\}$

$[\infty > \gamma,\ \infty + \gamma = \gamma + \infty = \infty$ for any $\gamma \in \Gamma]$

Γ __value group__, often denoted by vK

$\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$ the __valuation ring__ of v

$(\mathcal{O} \subseteq K$ a subring of K s.t. $\forall x \in K: x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O})$

$\mathfrak{m}_v := \{x \in K \mid v(x) > 0\}$ the unique max. ideal of $\mathcal{O}_v$

$\mathcal{O}_v / \mathfrak{m}_v :=$ the __residue field__, often denoted by Kv

The residue map: $\mathcal{O}_v \to \mathcal{O}_v/\mathfrak{m}_v$, $a \mapsto \bar{a} := a + \mathfrak{m}_v$ gives rise

to the __place__ $\varphi_v : K \to Kv \cup \{\infty\}$

$$a \mapsto \begin{cases} \bar{a} & \text{if } a \in \mathcal{O}_v \\ \infty & \text{o/w} \end{cases}$$

$\varphi : K \to k \cup \{\infty\}$ s.t. $\varphi(x \overset{\cdot}{+} y) = \varphi(x) \overset{\cdot}{+} \varphi(y)$

$\varphi(1) = 1$

$[\infty + a = a + \infty = \infty,\ \infty \cdot a = a \cdot \infty = \infty \cdot \infty = \infty$ for any $a \in K$,

$\infty + \infty$, $0 \cdot \infty$ and $\infty \cdot 0$ are not defined$]$

$\Rightarrow \varphi^{-1}(k)$ is a valuation ring of K with max. ideal $\varphi^{-1}(\{0\})$

__Def.:__ v_1, v_2 val. on K: $v_1 \sim v_2 \iff \exists$

$$\begin{tikzcd} & \Gamma_1 \arrow[dd, leftrightarrow, "\cong"] \\ K^\times \arrow[ur, two heads, "v_1"] \arrow[dr, two heads, "v_2"'] & \\ & \Gamma_2 \end{tikzcd}$$

$$\begin{tikzcd} \{v \text{ val. on } K\}/_\sim \arrow[rr, leftrightarrow] \arrow[dr, leftrightarrow] & & \{\mathcal{O} \text{ val. ring on } K\} \arrow[dl, leftrightarrow] \\ & \{\varphi \text{ place on } K\} & \end{tikzcd}$$

$\hookrightarrow v_{\mathcal{O}} : K^\times \twoheadrightarrow K^\times / \mathcal{O}^\times$

with $a\mathcal{O}^\times$ "$\leq$" $b\mathcal{O}^\times$

$\iff a^{-1}b \in \mathcal{O}$

§2 Coarsenings, refinements, dependence

<u>Def.</u>: v, w valuations on K. Then:

v is a <u>refinement</u> of w (w a <u>coarsening</u> of v) if $\mathcal{O}_v \subseteq \mathcal{O}_w$

TFAE (i) $\mathcal{O}_v \subseteq \mathcal{O}_w$

(ii) $\mathcal{O}_v^\times \subseteq \mathcal{O}_w^\times$

⚠ (iii) $\mathfrak{m}_w \subseteq \mathfrak{m}_v$

(iv) $\exists$ a convex subgp. $\Delta \leq \Gamma_v$ s.t. — namely $\Delta = v(\mathcal{O}_w^\times)$

$$\begin{tikzcd} K^\times \arrow[r, "v"] \arrow[rr, bend right, "w"'] & \Gamma_v \arrow[r] & \Gamma_v/\Delta \cong \Gamma_w \end{tikzcd}$$

and v induces a valuation $\bar{v}$ on Kw s.t. $\Gamma_{\bar{v}} = \Delta$

(v) $\exists$ a place $\varphi_{\bar{v}} : Kw \to Kv \cup \{\infty\}$ s.t.

$$\begin{tikzcd} K \arrow[r, "\varphi_w"] \arrow[rr, bend right, "\varphi_v"'] & Kw \cup \{\infty\} \arrow[r, "\varphi_{\bar{v}}"] & Kv \cup \{\infty\} \end{tikzcd}$$

<u>Example</u>

$\bar{v}$: $K(X) \to \mathbb{Z} \cup \{\infty\}$ the X-adic val. (res. fld. K)

w : $(K(X))(Y) \to \mathbb{Z} \cup \{\infty\}$ Y-adic (res. fld. $K(X)$)

v : $K(X,Y) \twoheadrightarrow \mathbb{Z} \oplus_{lex} \mathbb{Z} \cup \{\infty\}$ the refinement of w by $\bar{v}$:

on $K[X,Y]$: $v\left(\sum_{i=0}^m g_i(X) Y^i\right) = (i_0, \bar{v}(g_{i_0}(X)))$

where $i_0 = \min\{i \mid g_i(X) \neq 0\}$

<u>Note</u>. • $\{\text{convex } \Delta \leq \Gamma_v\} \Leftrightarrow \{\text{prime ideals of } \mathcal{O}_v\} \Leftrightarrow \{\text{coarsenings of } v\}$

(all three linearly ordered by inclusion)

• Any v, v' on K have a unique finest common coarsening w with $\mathcal{O}_w = \mathcal{O}_v + \mathcal{O}_{v'}$

Call v, v' <u>independent</u> iff $\mathcal{O}_w = K$ iff v, v' induce different topologies

basis of nbds. of 0: $\{a \cdot \mathfrak{m}_v \mid a \in K^\times\}$

[so, in particular, $\bar{v}$ and $\bar{v}'$ are independent on Kw]

Approximation Thm.

$$\left.\begin{array}{l} v_1, \dots, v_n \text{ pairwise indep. on } K \\ a_1, \dots, a_n \in K \\ \gamma_1 \in \Gamma_1, \dots, \gamma_n \in \Gamma_n \end{array}\right\} \Rightarrow \begin{array}{l} \exists\, x \in K \text{ s.t.} \\ v_i(x - a_i) > \gamma_i \\ \text{for all } i = 1, \dots, n \end{array}$$

Pf.: like Chinese Remainder Theorem applied to $R = \mathcal{O}_{v_1} \cap \dots \cap \mathcal{O}_{v_n}$:
$\mathfrak{p}_i := \mathfrak{m}_i \cap R$ is a prime ideal of R with $\mathcal{O}_{v_i} = R_{\mathfrak{p}_i}$ ∎

§3 Extensions and henselianity

Fact (Chevalley)

$$\left.\begin{array}{l} F/K \text{ field extension} \\ \mathcal{O}_v \text{ valuation ring on } K \end{array}\right\} \Rightarrow \begin{array}{l} \exists \text{ val. ring } \mathcal{O}_w \text{ on } F \\ \text{s.t. } \mathcal{O}_v = \mathcal{O}_w \cap K \end{array}$$

[hence $\mathcal{O}_v^\times = \mathcal{O}_w^\times \cap K$ & $\mathfrak{m}_v = \mathfrak{m}_w \cap K$ so $\Gamma_v \leq \Gamma_w$ & $Kv = \mathcal{O}_v/\mathfrak{m}_v \hookrightarrow \mathcal{O}_w/\mathfrak{m}_w = Kw$]

Call $w : F^\times \twoheadrightarrow \Gamma_w$ a prolongation of v

$$\begin{array}{ccc} F^\times & \twoheadrightarrow & \Gamma_w \\ \cup\!\mid & & \cup\!\mid \\ K^\times & \xrightarrow{v} & \Gamma_v \end{array}$$

$e(w/v) := [\Gamma_w : \Gamma_v]$ ramification index

$f(w/v) := [Kw : Kv]$ inertia degree

Fundamental Inequality

$[F:K] = n < \infty \Rightarrow v$ has only finitely many prolongations $w_1, \dots, w_r$ to F

and $\boxed{\sum_{i=1}^{r} e_i f_i \leq n}$ where $e_i = e(w_i/v)$, $f_i = f(w_i/v)$

Def.: (K, v) is henselian if v has a unique prolongation to any finite extension.

TFAE (1) (K,v) is henselian

(2) v has a unique prolongation to $\tilde{K}$ (equ.^{v} K^{sep})

(3) "Hensel's lemma": simple zeros lift:

originally proved by Hensel for $\mathbb{Q}_p$ →

$f(X) \in \mathcal{O}_v[X]$ monic, $a \in \mathcal{O}_v$ s.t. $\bar{f}(\bar{a}) = \bar{0} \neq \bar{f}'(\bar{a})$

$\Rightarrow \exists\, b \in \mathcal{O}_v$ with $f(b) = 0$ and $\bar{a} = \bar{b}$

(4) for each n and for any $a_0, a_1, \dots, a_{n-1} \in \mathfrak{m}_v$
$\exists\, x \in K$ s.t. $x^{n+1} + x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$

(5) "Krasner's lemma": $f, g \in \mathcal{O}_v[X]$ close with zeros $\alpha, \beta \in K^{sep}$ $\Rightarrow$ $K(\alpha) = K(\beta)$

Thm. (F. K. Schmidt)

If K has two independent hens. valuations then $K = K^{sep}$.

Pf.: Appr. Thm. + Krasner. ∎

Def.: Assume $K \neq K^{sep}$.

$H_1(K) := \{\mathcal{O} \mid \mathcal{O}$ henselian with $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}$ not sep.^{y} cl.$\}$

$H_2(K) := \{\mathcal{O} \mid \mathcal{O}$ hens. s.t. $\mathcal{O}/\mathfrak{m}_{\mathcal{O}}$ is sep.^{y} cl.$\}$

Then H_1 is ($\neq \emptyset$ and) linearly ordered by inclusion, any $\mathcal{O} \in H_1$ is coarser than any $\mathcal{O}' \in H_2$

If $H_2 = \emptyset$ then $\mathcal{O}_K := \bigcap_{\mathcal{O} \in H_1} \mathcal{O}$ is the unique finest henselian valuation on K.

If $H_2 \neq \emptyset$ then the composition $\mathcal{O}_K$ of all $\mathcal{O}' \in H_2$ is the unique coarsest $\mathcal{O}' \in H_2$

In either case, say $\mathcal{O}_K$ is the canonical hens. val. ring on K.

[Most of the time, $\mathcal{O}_K$ is 1st. order definable in $\mathcal{L}_{ring}$]

Examples (a) $K \equiv \mathbb{R} \Rightarrow \mathcal{O}_K = \mathrm{Con}_K \mathbb{Z} = \{x \in K \mid \exists\, n \in \mathbb{N}: -n < x < n\}$

and $\mathcal{O}_K = K$ iff K is archimedean.

In particular, $\mathcal{O}_K$ not definable for non-arch. K

(b) $K = \overbrace{(\mathbb{C}((X))}^{\mathcal{O}_K \in H_2}((Y))$ $\underset{\in H_1}{\uparrow}$ $\qquad \Gamma_{\mathcal{O}_K} = \underset{Y\text{-adic}}{\mathbb{Z}} \oplus_{lex} \underset{X\text{-adic}}{\mathbb{Z}}$

Lecture 3: Galois theory of valued fields

§1 The Conjugacy Theorem

Obs. 1 (K,v) valued, F/K finite

(a) F/K purely insep. $\Rightarrow$ v has unique prolong. to F

(b) w, w' inequiv. prol. to F $\Rightarrow$ $\mathcal{O}_w \not\subseteq \mathcal{O}_{w'}$

Pf.: (a) w.l.o.g. $F = K(\sqrt[p]{a})$ $\Rightarrow$ $w\left(\sum_{i=0}^{p-1} \lambda_i \sqrt[p]{a}^{\,i}\right) = \frac{1}{p} v\left(\sum \lambda_i^p a^i\right)$

(b) $\mathcal{O}_w \subsetneq \mathcal{O}_{w'}$, say $x \in \mathcal{O}_{w'} \setminus \mathcal{O}_w \Rightarrow x \in \mathcal{O}_{w'}^\times$ and $x^{-1} \in \mathfrak{m}_w$

let $e := e(w/v) < \infty$

$\Rightarrow \exists\, a \in K$ with $w(x^{-e}) = w(a) = w'(a) = v(a) > 0$

$\Rightarrow x^{-e} a^{-1} \in \mathcal{O}_w^\times \setminus \mathcal{O}_{w'}$ ↯ ∎

Obs. 2 $\mathcal{O} \subseteq K$ val. ring $\Rightarrow$ $\mathcal{O}$ integrally closed in K

Pf.: $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ for $x \in K$, $a_i \in \mathcal{O}$

$x \notin \mathcal{O} \Rightarrow x^{-1} \in \mathfrak{m}_{\mathcal{O}} \Rightarrow -1 = a_{n-1}x^{-1} + a_{n-2}x^{-2} + \ldots + a_0 x^{-n} \in \mathfrak{m}_{\mathcal{O}}$ ↯ ∎

Weak Approximation Thm.

$\mathcal{O}_1, \ldots, \mathcal{O}_n$ pairwise incomparable, $x_i \in \mathcal{O}_i \Rightarrow \exists\, x \in K$ s.t. $x - x_i \in \mathfrak{m}_{\mathcal{O}_i}$ for all i

Pf.: like Appr. Thm. $R = \bigcap \mathcal{O}_i$ + CRT. ∎

Conjugacy Thm

(K,v) valued
F/K normal finite
w, w' prolong. of v to F

$\Bigg\} \Rightarrow$ $\exists\, \sigma \in \mathrm{Aut}(F/K)$ s.t. $\mathcal{O}_{w'} = \sigma(\mathcal{O}_w)$ (hence $w' = w \circ \sigma$)

Pf.: By Obs. 1(a), w.l.o.g. F/K Galois, $G := \mathrm{Gal}(F/K)$

Let $\widetilde{\mathcal{O}}_v$ be the integral closure of $\mathcal{O}_v$ in F

$\Rightarrow \widetilde{\mathcal{O}}_v = \bigcap_{\sigma \in G} \sigma\mathcal{O}_w$: „$\subseteq$" by Obs. 2

„$\supseteq$": $x \in \bigcap \sigma\mathcal{O}_w \Rightarrow \sigma x \in \mathcal{O}_w$ for all $\sigma \in G$

$\Rightarrow \mathrm{Irr}(x/K) = \prod_{\sigma \in G}(X - \sigma x) \in \mathcal{O}_v[X]$.

Now assume u is another prolong. $\neq \sigma w$ for any $\sigma \in G$

$$\Rightarrow \widetilde{\mathcal{O}}_v \underset{\substack{\uparrow \\ \text{Obs. 2}}}{\subseteq} \mathcal{O}_u \cap \bigcap_{\sigma \in G} \mathcal{O}_{\sigma w} \underset{\substack{\uparrow \\ \text{by weak appr. \& Obs. 1(b)}}}{\subsetneq} \bigcap_{\sigma \in G} \sigma\mathcal{O}_w = \widetilde{\mathcal{O}}_v \quad ↯ ∎$$

§2 Ramification Theory (Hilbert Theory)

Def.: $(L,w)/(K,v)$ Galois ext. of valued fields, $G = Gal(L/K)$

$D := D(w/v) := \{\sigma \in G \mid \sigma \mathcal{O}_w = \mathcal{O}_w\}$ decomposition subgp. of G

$= \{\sigma \in G \mid \forall x \in \mathcal{O}_w : \sigma x - x \in \mathcal{O}_w\}$

$I := \{\sigma \in G \mid \forall x \in \mathcal{O}_w : \sigma x - x \in \mathfrak{m}_w\}$ inertia group

$R := \{\sigma \in G \mid \forall x \in \mathcal{O}_w : \sigma x - x \in x\,\mathfrak{m}_w\}$ ramification group

with corresponding fixed fields $L_D = \mathrm{Fix}\, D$, L_I and L_R

Note • $R \trianglelefteq I \trianglelefteq D \leq G$

• these groups behave well in towers, i.e.
for $(L',w')/(L,w)/(K,v)$, $D' = D(w'/v)$ etc.
$\pi :\; Gal(L'/K) \twoheadrightarrow Gal(L/K)$ restriction map
$\Rightarrow \pi(D'/I'/R') = D/I/R$

• hence everything works also for infinite L/K Galois (where all subgps are closed)

Fact D $w_D := w \restriction L_D \Rightarrow$
(a) w is the unique prolongation of w_D to L
(b) v has $[G:D] = [L_D:K]$ prolongations of v to L
(c) The residue fields and value groups of all prolongations of v to L are isomorphic
(d) w_D/v is immediate, i.e. $L_D w_D = Kv$ & $\Gamma_{w_D} = \Gamma_v$

Fact I
$$\Phi : D = Gal(L/L_D) \to Aut(Lw/Kv)$$
$$\sigma \mapsto \bar{\sigma} : Lw \to Lw,\quad \bar{x} \mapsto \overline{\sigma x}$$
is a well-defined epimorphism with $\ker \Phi = I$ (so $I \trianglelefteq D$).
$L_I w_I = Lw \cap Kv^{sep}$ and L_I/L_D is purely inert,
i.e. "$n = f$": $[L_I : L_D] = [L_I w_I : Kv]$

Fact R

(a) The homomorphism $\psi_0 : I \to \mathrm{Hom}(L^\times, L_w^\times)$

$$\sigma \mapsto \left(\begin{array}{l} L^\times \to L_w^\times \\ x \mapsto \overline{\frac{\sigma x}{x}} \end{array} \right)$$

induces an epimorph.

$$\psi : I \to \mathrm{Hom}(\Gamma_w/\Gamma_v, \mu(L_w)) \; (\cong \chi(\Gamma_w/\Gamma_v))$$

with $\ker \psi = R$, where $\mu(L_w)$ = gp. of roots of 1 in L_w.

In particular, $R \triangleleft I$ and I/R is abelian.

(b) For $p = \mathrm{char}\, K_v$, R is the unique Sylow-p-subgp. of I ($=1$ if $p=0$), hence $R \triangleleft D$, and

L_R/L_I is purely ramified ("$e=n$") and <u>tame</u> ($p \nmid e$)

Galois group	field	value gp	res. fld. (char p)
1 —	L —	Γ_w —	L_w
$\vert$	$\vert$	$\vert$ p-div. hull	$\vert$ purely inseparable
$\mathrm{Syl}_p(I) \ni R$ —	L_R —	$\frac{1}{p^\infty}\Gamma_v \cap \Gamma_w$ —	$L_w \cap K_v^{sep}$
$\vert$ $\chi(\Gamma_w/\Gamma_v)$ (prime to p)	$\vert$ purely ram. & tame	$\vert$ p'-div. hull	$\Vert$
I —	L_I —	Γ_v —	$L_w \cap K_v^{sep}$
$\vert$ "Gal"(L_w/K_v)	$\vert$ purely inert	$\Vert$	$\vert$ max. sep.
D —	L_D —	Γ_v —	K_v
$\vert$	$\vert$ immediate	$\Vert$	$\Vert$
G —	K —	Γ_v —	K_v

If $L = K^{sep}$, L_D is the (up to conj.) unique <u>henselization K^h of (K,v)</u>.

§3 Henseling down

Theorem

Let L/K be an algebraic extension, $L \neq L^{sep}$, w a (not nec.^{y} proper) coarsening of v_L s.t. $Lw \not\models RCF$.
Then $v := w\restriction K$ is a coarsening of v_K in the following cases:

(i) L/K is normal

(ii) L/K is finite

(iii) $G_L \in Syl_p(G_K)$ for some prime p

Pf.: (i) w is the unique prolong. of v to L
(any other would be henselian & incomparable)

$w \in H_1(L) \Rightarrow v \in H_1(K)$

$w \in H_2(L) \Rightarrow w = v_L$ & any proper coarsenj $w' \in H_1(L)$

$\Rightarrow$ any proper coars. of v is $\in H_1(K)$

$\Rightarrow v$ coarsening of v_K.

(ii) pass to the normal hull of L/K and apply (i)
(use $Lw \not\models RCF$)

Recall: Artin-Schreier: $1 < |G_F| < \infty \iff F \models RCF$

(iii) Claim: For any finite Galois M/L, the unique prolongation u of w to M is the only henselian prolong. of w to M

Pf.: o/w let u' be another $\Rightarrow u, u' \in H_2(M)$ & $\mathcal{O}_u \subsetneq \mathcal{O}_{v_M} \in H_2(M)$

$\Rightarrow \mathcal{O}_w \subsetneq \mathcal{O}_{v_L} = \mathcal{O}_{v_M} \cap L \in H_2(L)$ ↯ ∎ claim

Suppose v not hens., F/K finite Galois with prolong. $v_1 \neq v_2$

$$\begin{tikzcd}[column sep=small]
 & (M = LF, u) \arrow[dl, dash] \arrow[d, dash] & (\sigma M, \tilde{v}_2) \arrow[dl, dash] \\
(L,w) \arrow[d, dash] & (F, v_1 \neq v_2) \arrow[dl, dash] & \\
L \cap F \arrow[d, dash] & & \\
(K,v) & &
\end{tikzcd}$$

$\Rightarrow M/L$ finite Gal. & $G_M \in Syl_p(G_F)$

$u\restriction F = v_1 \neq v_2$

$\tilde{u}, \tilde{v}_2$ prol. of u, v_2 to K^{sep}

$\Rightarrow \exists\, \sigma \in G_K : \mathcal{O}_{\tilde{v}_2} = \sigma \mathcal{O}_{\tilde{u}}$

$\Rightarrow F \subseteq \sigma M$ & $G_{\sigma M} \in Syl_p(G_F)$

$\Rightarrow \exists\, \tau \in G_F$ with $\tau(\sigma M) = M$

$\Rightarrow \tau(\mathcal{O}_{\tilde{v}_2} \cap \sigma M)$ is hens. on $M \neq u$ (restr. to F is $\mathcal{O}_{v_2}$)
and prolongs v ↯ to claim ∎

Lecture 4: A Galois code for henselianity

§1 Tamely branching valuations

$G_K := \mathrm{Gal}(K^{sep}/K)$

K real closed $\iff G_K \cong \mathbb{Z}/2\mathbb{Z} \iff 1 < |G_K| < \infty$

Goal: K henselian $\iff G_K \cdots$
(for some non-triv. v)

Obstacles: • Γ_v should not be divisible, e.g. for char $k = 0$:
$G_k \cong G_{k((\mathbb{Q}))}$ and k may or may not be henselian

• G_K should not be too simple: $G_{\mathbb{F}_p} \cong \hat{\mathbb{Z}} \cong G_{\mathbb{C}((t))}$

Def.: A valuation v on K is tamely branching at the prime p if $\Gamma_v \neq p\Gamma_v$, char $Kv \neq p$ and, if $[\Gamma_v : p\Gamma_v] = p$ then $p^2 \mid \# G_{Kv}$.

Theorem

K henselian w.r.t. some tamely branching v
$\iff \exists\ 1 \neq N \lhd P \in \mathrm{Syl}_p(G_K)$ with N abelian
and $P \not\cong \mathbb{Z}_p$, $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$.

Proof: „$\Rightarrow$" Suppose v henselian & tamely branching @ p
$\Rightarrow$ the unique prolong. w of v to $L := \mathrm{Fix}\, P$
for some/any $P \in \mathrm{Syl}_p(G)$ is tamely br. @ p
& $N :=$ inertia subgp. of P is $\neq 1$ and abelian $\lhd P$
(ram. subgp. of P trivial as char $Kv \neq p$, so $N = \chi(\Gamma_w) \cong \mathbb{Z}_p^{\dim_{\mathbb{F}_p} \Gamma_w/p\Gamma_w}$)
& , if $[\Gamma_v : p\Gamma_v] = p$, then $N \cong \mathbb{Z}_p$, but $p^2 \mid \# G_{Lw} \cong P/N$
hence $P \not\cong \mathbb{Z}_p$, $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$

note that $P \cong N \rtimes G_{Lw}$:
if $A \subseteq L^\times$ s.t. $v(A)$ induces an $\mathbb{F}_p$-basis on $\Gamma_w/p\Gamma_w$
then $L(\sqrt[p^\infty]{A})$ is a complement to $\mathrm{Fix}\, N$ in K^{sep}

"$\Leftarrow$" Claim: It suffices to prove the

Classical case $G_F \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p \Rightarrow F$ hens. w.r.t. some v t.^{y} br. @ p

("Classical", because for $F = \mathrm{Fix}\, P$, where $P \in \mathrm{Syl}_p(\mathbb{Q}_\ell)$ with $\ell \neq p$

$G_F = P = \mathbb{Z}_p \rtimes_{\chi(\mathbb{Z}_{(p)})} \mathbb{Z}_p \in \mathrm{Syl}_p(\mathbb{F}_\ell$)

Pf (Claim): Note that if v is t.^{y} br. @ p & henselian on F then so is the finest common coarsening of v and v_F

Case 1 $N \not\cong \mathbb{Z}_p \Rightarrow \exists N_0 \cong \mathbb{Z}_p \times \mathbb{Z}_p \trianglelefteq N$

$\Rightarrow$ (classical case) $\exists\,$hens. w t.^{y} br. @ p on $L := \mathrm{Fix}\, N_0$ & w.l.o.g. $\mathcal{O}_{v_L} \subseteq \mathcal{O}_w$

Henseling down normal $\Rightarrow w\restriction \mathrm{Fix}\, N$ and $w \restriction \mathrm{Fix}\, P$ are hens.

Henseling down Sylow $\Rightarrow w\restriction K$ is hens.

Case 2 $N \cong \mathbb{Z}_p$, w.l.o.g. $\sqrt{-1} \in K$ (hensel down finite)

Pick $\sigma \in P \setminus N \Rightarrow \langle N, \sigma \rangle \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$

$\Rightarrow$ (classical case) $\exists$ hens. w t.^{y} br. @ p on $L := \mathrm{Fix}\,\langle N,\sigma\rangle$ & $\mathcal{O}_{v_L} \subseteq \mathcal{O}_w$.

$u :=$ unique prol. of w to $\mathrm{Fix}\, N = F$

$F = \mathrm{Fix}\, N \quad \mathcal{O}_u$

$L = \mathrm{Fix}\,\langle N, \sigma\rangle \quad \mathcal{O}_w$

$\mathrm{Fix}\, P$

$\mathcal{O}_{v_F} \subseteq \mathcal{O}_u \Rightarrow$ hensel down $\rightsquigarrow v = u\restriction K = w \restriction K$ will do

$\mathcal{O}_u \subsetneq \mathcal{O}_{v_F} \Rightarrow F v_F = F_{v_F}^{sep}$ & $\Gamma_{v_F} \neq p\Gamma_{v_F}$ & char $Fv_F \neq p$

$\Rightarrow v_F \restriction L$ is proper coarsening of v_L, hence $\in H_1(L)$ and so t.^{y} br. @ p

$\Rightarrow v_F \restriction K$ hens. & t.^{y} br. @ p ■ Claim

for the classical case we need

$\boxed{\text{§ 2 Rigid elements}}$

Def.: $T \leq K^\times$, $x \in K^\times \setminus T$ is T-rigid if $T + xT \subseteq T \cup xT$

Example v val. on K, $\Gamma_v \neq p\Gamma_v$, $T := v^{-1}(p\Gamma_v)$

$\Rightarrow$ any $x \in K^\times \setminus T$ is T-rigid

Proposition

Let $p>2$ be prime, $(K^\times)^p \leq T \lneqq K^\times$ such that every $x \in K^\times \setminus T$ is T-rigid. Then

$$\mathcal{O}(T) := \mathcal{O}_1(T) \cup \mathcal{O}_2(T) \quad \text{with}$$
$$\mathcal{O}_1(T) := \{x \in K \setminus T \mid 1+x \in T\}$$
$$\mathcal{O}_2(T) := \{x \in K \mid x\,\mathcal{O}_1(T) \subseteq \mathcal{O}_1(T)\}$$

is a valuation ring of K with $\mathcal{O}(T)^\times \leq T$

Pf.: Claim 1: $-\mathcal{O}_1 = \mathcal{O}_1$

$$x \in \mathcal{O}_1 \overset{p>2}{\Longrightarrow} -x \notin T = -T \text{ and } \pm x^2 \notin T$$
$$\Rightarrow 1-x^2 = (1+x)(1-x) \in (T \cup x^2T) \cap (T \cup xT) = T$$
$$\Rightarrow 1-x \in T$$
$$\Rightarrow -x \in \mathcal{O}_1$$

similar elementary proofs:

Claim 2 $\quad \mathcal{O}\cdot\mathcal{O} \subseteq \mathcal{O}$ ($\mathcal{O}_2\cdot\mathcal{O} \subseteq \mathcal{O}$ clear, so to show: $\underset{\substack{\Uparrow \\ x}}{\mathcal{O}_1}\cdot\underset{\substack{\Uparrow \\ y}}{\mathcal{O}_1} \subseteq \mathcal{O}$ $\left\langle \begin{array}{l} xy \notin T \\ xy \in T \end{array}\right.$)

Claim 3 $\quad \forall x \in K: x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$ (and if both, $x \in \mathcal{O}_2$)

Claim 4 $\quad 1+\mathcal{O}_1 \subseteq \mathcal{O}_2$

Claim 5 $\quad 1+\mathcal{O}_2 \subseteq \mathcal{O}$

Claim 6 $\quad \mathcal{O}+\mathcal{O} \subseteq \mathcal{O}$

(Code 117/118)

$\Rightarrow \mathcal{O}$ val. ring of K with $\mathcal{O}^\times \subseteq \mathcal{O}_2 \subseteq T$ $\blacksquare$

Lemma (The wonderful creation of rigid elements)

Let $p>2$, $(K^\times)^p \leq S \lneqq K^\times$ and assume that $[K^\times : S] \geq p^2$ and for every $x \in K^\times \setminus S$: $\quad S + xS \subseteq \bigcup_{i=0}^{p-1} x^i S$.

Then $\exists$ $S \leq T \leq K^\times$ with $[T:S] \leq p$ s.t. every $x \in K^\times \setminus T$ is T-rigid.

Pf.: Code 119/120.

$\boxed{\S 3 \text{ Proof of the classical case } G_K \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p \text{ (for } p>2)}$

Step 1 L/K finite $\Rightarrow G_L \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$:

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{Z}_p \arrow[r] & G_K \arrow[r, "\pi"] & \mathbb{Z}_p \arrow[r] & 1 \\ 1 \arrow[r] & G_L \cap \mathbb{Z}_p \arrow[r] \arrow[u, hook] & G_L \arrow[r] \arrow[u, hook] & \pi(H) \arrow[r] \arrow[u, hook] & 1 \\ & \cong \mathbb{Z}_p & & \cong \mathbb{Z}_p & \end{tikzcd}$$

Step 2 $\operatorname{char} K \neq p$ and hence $\zeta_p \in K$

assume $\operatorname{char} K = p$ & let $\wp(K) := \{x^p - x \mid x \in K\} \leq (K,+)$

$\Rightarrow \dim_{\mathbb{F}_p} K/\wp(K) = 2$ (by "additive Kummer" = Artin-Schreier)

let $a, b \in K$ be $\wp(K)$-independent

$L := K(x)$ where $x^p - x - a = 0 \Rightarrow L/K$ Gal. degree p

$\Rightarrow (x^{-1})^p + a^{-1}(x^{-1})^{p-1} - a^{-1} = 0 \Rightarrow \operatorname{Tr}_{L/K} x^{-1} = -a^{-1}$

$\Rightarrow$ for $\alpha = -x^{p-1} = -1 - a x^{-1}$, $\operatorname{Tr}(\alpha) = 1$ and $K(x) = K(\alpha)$

$\Rightarrow b, b\alpha$ and $a\alpha$ are $\mathbb{F}_p$-ind. mod $\wp(L)$:

$ib + jb\alpha + ka\alpha = u^p - u \overset{\operatorname{Tr}}{\Rightarrow} jb + ka = \operatorname{Tr}(u)^p - \operatorname{Tr}(u) \Rightarrow j = k = 0$

$\Rightarrow i = 0$ ($b \notin \wp(L)$)

$\Rightarrow \operatorname{rk} G_L > 2$ ↯ to Step 1

Step 3 $\forall x \in K \setminus K^p$: $N(K(\sqrt[p]{x})) = \langle x \rangle \cdot (K^\times)^p$

$\left.\begin{array}{l} L = K(\sqrt[p]{x}) \Rightarrow N_{L/K}(\sqrt[p]{x}) = x \Rightarrow \sqrt[p]{x} \notin L^\times \\ \text{choose } b \in K^\times \setminus \langle x \rangle (K^\times)^p \end{array}\right\} \Rightarrow b, \sqrt[p]{x}$ basis of $L^\times/(L^\times)^p$

Step 4 (Lemma) $\exists\, (K^\times)^p \leq T \lneq K^\times$ s.t. all $x \in K^\times \setminus T$ are T-rigid

(Prop.) $\mathcal{O}(T)^\times \leq T$ and so for v with $\mathcal{O}_v = \mathcal{O}(T)$, $\Gamma_v \neq p\Gamma_v$

Step 5 w.l.o.g. Γ_v has no p-div. convex subgp. and $\operatorname{char} K_v \neq p$

o/w $\exists \pi \in K$ with $v(\pi) \notin p\Gamma_v$ and $0 < v(\pi) < v(p)$

$L := K(\sqrt[p]{\pi}) \Rightarrow \pi, 1+\pi \in N_{L/K}$, so $1 + \pi = \pi^k y^p$ $(0 \leq k < p)$

$\Rightarrow k = 0$ & $1 + \pi = (1+z)^p$ for some $z \in \mathfrak{m}_v$

$= 1 + \underbrace{\sum_{j=1}^{p-1} \binom{p}{j} z^j}_{\in p\,\mathfrak{m}_v} + z^p \Rightarrow v(\pi) = v(z^p)$ ↯

Step 6 v henselian

o/w L/K Gal. of degree p with prol. $v_1, \ldots, v_p$ & $\exists\, x_i \in \mathfrak{m}_{v_i} \cap \bigcap_{j \neq i} \mathcal{O}_{v_j}^\times$

w.l.o.g. $v_i(x_i) \notin p\Gamma_{v_{(i)}}$ (o/w take $a + x_i$ where $a \in K$ with $0 < v(a) < v(x_i)$ and $v(a) \notin p\Gamma_v$)

$\Rightarrow L(\sqrt[p]{x_i})$ $(i = 1, \ldots, p)$ are p indep. ext. of L

but $[L^\times : (L^\times)^p] = p^2 < p^p$ ↯ ∎

Lemma 2.14 *Let p be a prime > 2, let F be a field and let H and G be subgroups of $F^\times$ with $(F^\times)^p \leq H \leq G$, $[G : H] \geq p^2$ satisfying the condition*

$$(\star) \quad \forall c \in G \setminus H : \ H + cH \subseteq \bigcup_{i=0}^{p-1} c^i H.$$

Then there is a subgroup T of G containing H with $[T : H] \leq p$ such that

$$\forall c \in G \setminus T : \ H + cH \subseteq H \cup cH,$$

and hence also

$$\forall c \in G \setminus T : \ T + cT \subseteq T \cup cT.$$

Proof Let us assume that the conclusion of the lemma is false. Then we find elements $a, b \in G$ with $[\langle a, b\rangle H : H] = p^2$, and elements $x, y \in H$ such that for some $k, l \in \{2, 3, \dots, p-1\}$:

$$x + a \in a^k H,$$
$$y + b \in b^l H.$$

Claim: $y - b \in b^{\frac{l}{2l-1}} H$ and $2l - 1 \neq 0 \in \mathbb{F}_p$.

As $(F^\times)^p \leq H$, we only have to consider exponents modulo p, i.e., we understand them as elements of $\mathbb{F}_p$.

Using the hypothesis $(\star)$, we see that for some $j, r, s, t \in \mathbb{F}_p$,

$$xy + bx + ay = \begin{cases} xy + a(y + a^{-1}bx) & \in & (a^{1-j}b^j)^r H \\ b(x + b^{-1}(x+a)y) & \in & b(a^k b^{-1})^s H \\ a(y + a^{-1}(y+b)x) & \in & a(a^{-1}b^l)^t H \end{cases}$$

So comparing the exponents of a and b yields

$$(1) \quad r(1-j) = ks = 1 - t$$
$$(2) \quad rj = 1 - s = lt$$

As $l \neq 0$, this implies $r \neq 0$.

$$(1) + (2) \quad \Rightarrow \quad r = (l-1)t + 1$$
$$(1) + k(2) \quad \Rightarrow \quad k = (kl-1)t + 1$$

Therefore, as $k \neq 1$, we have $kl - 1 \neq 0$. Thus

$$t = \frac{k-1}{kl-1} \text{ and } r = \frac{2kl - k - l}{kl - 1},$$

and so $2kl - k - l \neq 0$. ¿From (2) we then obtain

$$j = \frac{lt}{r} = \frac{l(k-1)}{2kl - k - l} \neq 0.$$

Now let $y - b = b^i H$. We have to compute i. We recall that $bx + ay \in a^{1-j}b^j H$. On the other hand

$$bx + ay = (b - y)x + (a + x)y \in a^k (a^{-k} b^i)^q H$$

for some q. So $1 - j = k(1 - q)$ and $j = iq = \frac{i(j+k-1)}{k} \neq 0$. As

$$j + k - 1 = \frac{(k-1)(l + 2kl - k - l)}{2kl - k - l} = \frac{(k-1)k(2l-1)}{2kl - k - l},$$

this implies $2l - 1 \neq 0$ and

$$i = \frac{jk}{j+k-1} = \frac{kl(k-1)}{k(k-1)(2l-1)} = \frac{l}{2l-1}$$

which proves the claim.

Note that it also follows that $i \neq 0, 1$ as otherwise $l = 0$ or $l = 1$. Therefore, the set

$$I := \{i \in \mathbb{F}_p \setminus \{0,1\} \mid \exists b' \in \langle b \rangle H \setminus H \ \ \exists y \in H : \ y + b' \in b'^i H\}$$

is non-empty. Also, I is closed under $i \mapsto \frac{1}{i}$: if $y + b' = b'^i z$ for some $z \in H$, then $b'' := -b'^i z$ satisfies $y + b'' \in (b'')^{\frac{1}{i}} H$. And, by the proof of the claim, I is closed under $i \mapsto \frac{i}{2i-1}$ and $\frac{1}{2} \notin I$.

Such a set, however, does not exist. For, inductively, I contains no element of the form $\frac{m}{m+1}$ for $1 \leq m \leq p-2$: $\frac{1}{1+1} \notin I$ and if $\frac{m}{m+1} \in I$ and $m > 1$, then also

$$\frac{m-1}{m} = (\frac{m}{m-1})^{-1} = (\frac{\frac{m}{m+1}}{2\frac{m}{m+1} - 1})^{-1} \in I.$$

On the other hand, each $i \in \mathbb{F}_p$ *can* be written in this form:

$$i = \frac{\frac{i}{1-i}}{\frac{i}{1-i} + 1}$$

contradicting $I \neq \emptyset$.

It follows that $T + cT \subseteq T \cup cT$ for any $c \in G \setminus T$, because $T = \bigcup_{i=0}^{p-1} d^i H$ for some $d \in T$, so given $c \in G \setminus T$, $x, y \in H$ and $i, j < p$, one has $cd^{i-j} \in G \setminus T$ and

$$(d^i x) + c(d^j y) = d^i(x + (cd^{j-i})y) \in d^i(H \cup cd^{j-i}H) \subseteq T \cup cT.$$

□

2.6 Galois characterization of p-henselian fields. By now we are prepared for the theorem which is one of the two main inputs for the Galois characterization of henselian fields: For $p = 2$ the theorem appears in section 4 of [15]. For $p > 2$ it is the Main Theorem of [13]:

Theorem 2.15 *Let p be a prime, let F be a field containing a primitive p-th root ζ_p of unity (so* $\operatorname{char} F \neq p$*) and assume $G_F(p) \not\cong \mathbb{Z}_p$ and, if $p = 2$, also $G_F(p) \not\cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$.*

Then F admits a p-henselian valuation tamely branching at p iff $G_F(p)$ has a non-trivial abelian normal subgroup.

As in Theorem 1, one direction is trivial: if F admits a p-henselian valuation v with $\Gamma_v \neq p\Gamma_v$ and $\operatorname{char} Fv \neq p$ then the inertia subgroup of $G_F(p)$ is non-trivial ($\Gamma_v \neq p\Gamma_v$), abelian ($\operatorname{char} Fv \neq p$) and normal ($v$ p-henselian, i.e., $G_F(p)$ is its own decomposition subgroup w.r.t. v).

It is also clear that one has to exclude the exceptional cases $G_F(p) \cong \mathbb{Z}_p$, $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbf{Z}$: each of them occurs among fields with and without any non-trivial p-henselian valuation:

$$\begin{array}{rcccl} G_{\mathbb{C}((t))}(p) & \cong & \mathbb{Z}_p & \cong & G_{\mathbb{F}_q}(p) \\ G_{\mathbb{R}((\mathbb{Q}))}(2) & \cong & \mathbb{Z}/2\mathbb{Z} & \cong & G_{\mathbb{R}}(2) \\ G_{\mathbb{R}((t))}(2) & \cong & \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z} & \cong & G_F(2), \end{array}$$

Lecture 5/6: A Galois characterization of p-adically closed fields

§1 p-adically closed fields

Def.: • A val. v on K is a <u>p-valuation</u> (p prime) if $Kv = \mathbb{F}_p$ & $v(p)$ is min. positive ($\Rightarrow$ char $K = 0$ & v non-trivial)

• (K, v) is <u>p-adically closed</u> if v is a p-valuation on K not extending to a p-val. on any proper algebraic L/K

Prop. For p-valued (K, v) TFAE:

(i) (K, v) is p-adically closed

(ii) v is henselian and $\Gamma_v \equiv \mathbb{Z}$ ("Γ_v is a $\mathbb{Z}$-gp.")

Lemma For an o.a. gp. TFAE:

(i) Γ is a $\mathbb{Z}$-gp

(ii) Γ has a convex subg $Z \cong \mathbb{Z}$ s.t. Γ/Z is divisible

(iii) Γ has a min. pos. elt. and $\forall n \in \mathbb{N}$: $[\Gamma : n\Gamma] = n$

Pf.: (Lemma) (i) $\Rightarrow$ (iii) $\Leftrightarrow$ (ii) ✓

(iii) Let $T = Th(\text{iii})$ in $\mathcal{L}^+_{oag} := \{+; <; ,0; 1; (D_n)_{n \in \mathbb{N}}\}$ where 1 min. pos. & $D_n \sim n\Gamma$

$\left.\begin{array}{l}\Rightarrow T \text{ has QE in } \mathcal{L}^+_{oag} \text{ (Exercise)} \\ \quad \& \text{ a prime model } \mathbb{Z}\end{array}\right\} \Rightarrow T$ complete ∎

Proof: (Prop.) (i) $\Rightarrow$ (ii) ✓

(ii) $\Rightarrow$ (i) Assume (ii) and $K(\alpha)/K$ proper immediate alg.

w.l.o.g. $\Gamma_v = \mathbb{Z}$ ($\mathcal{O}_w$ with $\mathcal{O}_w = \mathcal{O}_v[\frac{1}{p}]$ has $\Gamma_w = \Gamma_v / Z$ div. and char $Kw = 0$ & hens. $\Rightarrow$ no imm. alg. ext.)

approximate α by $a \in K$ until $v(\alpha - a) > v(\alpha - \alpha')$ for any conj. α' of α

$\Rightarrow$ (Krasner) $\alpha \in K(a) = K$ ↯ ∎

Examples: $\mathbb{Q}_p$, $\mathbb{Q}_p^{alg} := \mathbb{Q}_p \cap \tilde{\mathbb{Q}}$, $\mathbb{Q}_p((\mathbb{Q}))$

Non-examples $(\mathbb{Q}, v_p)$, $\mathbb{Q}_p((t))$

$$\begin{array}{c} K \subseteq F \equiv \mathbb{Q}_p \\ \Rightarrow \tilde{K} \cap F \equiv \mathbb{Q}_p \\ | \\ K \end{array}$$

$\left.\begin{array}{l}\text{Ax-Kochen / Ershov} \\ \text{\& Macintyre}\end{array}\right\}$ K p-adically cl. $\Leftrightarrow$ $K \equiv \mathbb{Q}_p$

§ 2 Three general lemmas

Lemma 1

(F,v) of characteristic $(0,p)$, $\zeta_p \in F$, $a \in \mathcal{O}_v$:

$$1+(1-\zeta_p)^p \cdot a \in F^p \Rightarrow \exists x \in F_v : x^p - x - \bar{a} = 0$$

$$\Leftarrow \quad \text{when } v \text{ hens.}$$

& Then, in particular, $1+(1-\zeta_p)^p \mathfrak{m}_v \subseteq (F^\times)^p$.

Pf.: $1+(1-\zeta_p)^p \cdot a \in F^p \Leftrightarrow f(X) := \left(X + \frac{1}{1-\zeta_p}\right)^p - \left(\left(\frac{1}{1-\zeta_p}\right)^p + a\right)$ has a zero in F

But $f(X) \in \mathcal{O}_v[X]$ with $\bar{f}(X) = X^p - X - \bar{a} \in F_v[X]$

because $v(1-\zeta_p) = \frac{1}{p-1} v(p)$ and $\frac{p}{(1-\zeta_p)^{p-1}} \in -1 + \mathfrak{m}_v$:

If $g(X) = X^{p-1} + \ldots + 1 = \mathrm{Irr}(\zeta_p/\mathbb{Q})$ then

$$p = g(1) = (1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1})$$
$$= (1-\zeta_p)^{p-1} \cdot \underbrace{1\cdot(1+\zeta_p)\cdots(1+\zeta_p+\ldots+\zeta_p^{p-2})}_{\equiv 1\cdot 2 \cdots (p-1) \equiv -1 \bmod \mathfrak{m}_v \text{ (Wilson)}} \blacksquare$$

Lemma 2

$\mathrm{char}\, K = p \Rightarrow$ any C_p-ext. L/K embeds into a C_{p^2}-ext.

Pf.: Pick $b \in L$ with $\mathrm{Tr}_{L/K}(b) = 1$ (cf. page 16, Step 2), $\mathrm{Gal}(L/K) = \langle \sigma \rangle$

$\Rightarrow \mathrm{Tr}_{L/K}(b^p - b) = 0 \Rightarrow$ (add. Hilb. 90) $\exists a \in L$ s.t. $b^p - b = \sigma a - a$

$\Rightarrow L(\alpha)/K$ with $\alpha^p - \alpha - a = 0$ is the required C_{p^2}-ext. ... $\blacksquare$

Lemma 3

$\zeta_p \in K$, $\mathrm{Gal}(L/K) \cong C_p$. Then:

L/K embeds into a C_{p^2}-ext. $\Leftrightarrow \zeta_p \in \mathrm{Im}\, N_{L/K}$

Pf.: „$\Rightarrow$" $K \subseteq L \subseteq M = L(\sqrt[p]{d})$ with $\mathrm{Gal}(M/K) \cong C_{p^2} \Rightarrow \sigma d \in d^i \cdot (L^\times)^p$ $(i=1,\ldots,p-1)$

pick $j \le p-1$ with $i\cdot j \equiv 1 \bmod p$ & replace σ by σ^j to assume $i=1$, say $\frac{\sigma d}{d} = e^p$

$\Rightarrow N_{L/K}(e) \in \langle \zeta_p \rangle$ & by H90 $N_{L/K}(e) \neq 1$ (o/w M/K $C_p \times C_p$)

„$\Leftarrow$" $N_{L/K}(e) = \zeta_p \Rightarrow N_{L/K}(e^p) = 1 \Rightarrow$ H90 $e^p = \frac{\sigma d}{d}$ & $d \notin (L^\times)^p$

$\Rightarrow M := L(\sqrt[p]{d})$ is the required C_{p^2}-ext. ... $\blacksquare$

§3 Properties of $G_{\mathbb{Q}_p}$

$G_{\mathbb{Q}_p}$ ① $\quad 1 \triangleleft \underset{\text{pro-}p}{R} \triangleleft I \triangleleft G_{\mathbb{Q}_p}$, $\quad I/R = \prod_{q\neq p} \mathbb{Z}_q = \mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, \mu(\overline{\mathbb{F}}_p))$, $\quad G_{\mathbb{Q}_p}/I = \hat{\mathbb{Z}} = G_{\mathbb{F}_p}$

$\boxed{\text{In part., for } q \neq p \text{ prime, } \mathbb{Z}_q \rtimes \underbrace{\mathbb{Z}_q}_{\text{not }\times} \in \mathrm{Syl}_q(G_{\mathbb{Q}_p})}$

$G_{\mathbb{Q}_p}$ ② $\boxed{K = \mathbb{Q}_p(\zeta_p, \zeta_{p-1}) \text{ has } C_p\text{-ext. not embeddable in } C_{p^2}\text{-ext.}}$

Pf.: Let $\pi = \zeta_p - 1$, $L = K(\sqrt[p]{1+\pi^2}) \Rightarrow \zeta_p = 1+\pi \notin N_{L/K} \overset{L3}{\Rightarrow} L \not\hookrightarrow C_{p^2}$

Note that K is the unique $C_{p-1}\times C_{p-1}$-ext. of $\mathbb{Q}_p$.

$G_{\mathbb{Q}_p}$ ③ $\quad q \neq p$ prime, $r \geq 1 \Rightarrow$

$\boxed{\mathbb{Q}_p \text{ has } C_{q^r}\times C_{q^r}\text{-ext.} \Leftrightarrow \mu_{q^r} \subseteq \mathbb{Q}_p \Leftrightarrow q^r \mid p-1}$

$G_{\mathbb{Q}_p}$ ④ $\boxed{\left.\begin{array}{l} F/\mathbb{Q}_p \text{ finite} \\ \ell \text{ prime } \& \ \zeta_\ell \in F \end{array}\right\} \Rightarrow \dim_{\mathbb{F}_\ell} F^\times/(F^\times)^\ell = \begin{cases} 2 & \text{for } \ell \neq p \\ [F:\mathbb{Q}_p]+2 & \text{for } \ell = p \end{cases}}$

Pf.: $(F,w)/(\mathbb{Q}_p, v_p)$ with $e = e(w/v_p)$ and $f = f(w/v_p)$, $\pi \in F$ uniformizer

$\Rightarrow F^\times = \langle \pi \rangle \times \mathcal{O}_w^\times = \langle \pi \rangle \times \mu_{p^f-1} \times (1+\mathfrak{m}_w)$
$\cong \mathbb{Z} \times \mathbb{F}_w^\times \times (1+\mathfrak{m}_w) \qquad (*)$

$\ell \neq p \Rightarrow \pi, \zeta_{p^f-1}$ induce $\mathbb{F}_\ell$-basis of $F^\times/(F^\times)^\ell$: $\ell \mid p^f-1$ (as $\zeta_\ell \in F$)
and $1+\mathfrak{m}_w \subseteq (F^\times)^\ell$

$\ell = p \Rightarrow \varphi_i : 1+\pi^i\mathcal{O}_w \twoheadrightarrow \mathbb{F}_w$, $1+\pi^i a \mapsto \bar{a}$ is epim. with kernel $\varphi_i = 1+\pi^{i+1}\mathcal{O}_w$

$\Rightarrow 1+\mathfrak{m}_w = 1+\pi\mathcal{O}_w \geq 1+\pi^2\mathcal{O}_w \geq \ldots \geq 1+\pi^{\frac{e\cdot p}{p-1}+1}\mathcal{O}_w = 1+(1-\zeta_p)^p\mathfrak{m}_w \overset{L1}{\leq} (F^\times)^p$
with all quotients $\cong (\mathbb{F}_w, +)$

$\Rightarrow |(1+\mathfrak{m}_w)/(1+\mathfrak{m}_w)^p| \leq (p^f)^{\frac{e\cdot p}{p-1}} = p^{n+\frac{n}{p-1}} \qquad (n = [F:\mathbb{Q}_p] = e\cdot f)$

elt. in $(1+\mathfrak{m}_w)^p$ represented by $(1+a_1\pi + a_2\pi^2 + \ldots + a_{\frac{e}{p-1}}\pi^{\frac{e}{p-1}})^p$ with $a_i \in \mu_{p^f-1} \cup \{0\}$

$\Rightarrow$ there are $p^{f\cdot\frac{e}{p-1}-1}$ many ("-1" comes from $\langle \zeta_p \rangle = \mathrm{kernel}\begin{pmatrix} (1+\mathfrak{m}_w) \to (1+\mathfrak{m}_w) \\ x \mapsto x^p \end{pmatrix}$)

$\Rightarrow \dim_{\mathbb{F}_p} (1+\mathfrak{m}_w)/(1+\mathfrak{m}_w)^p = n + \frac{n}{p-1} - (f\cdot\frac{e}{p-1} - 1) = n+1$

$(*) \Rightarrow$ (as $\mathbb{F}_w^\times = (\mathbb{F}_w^\times)^p$) $\dim_{\mathbb{F}_p} F^\times/(F^\times)^p = n+2$ ∎

Cor ④' $\forall n \in \mathbb{N}$: $\mathbb{Q}_p$ has only finitely many $F/\mathbb{Q}_p$ with $[F:\mathbb{Q}_p] \leq n$.

$G_{\mathbb{Q}_p}$ (5) $\boxed{1 \neq N \lhd G_{\mathbb{Q}_p} \Rightarrow N \text{ has non-procyclic Sylow-}p\text{ subgroups}}$

<u>Pf.:</u> Let $L = \operatorname{Fix} N$.

Choose $F/\mathbb{Q}_p$ finite Galois s.t. $[LF : L] = n \geq 3$

w.l.o.g. $\zeta_p \in L \cap F$

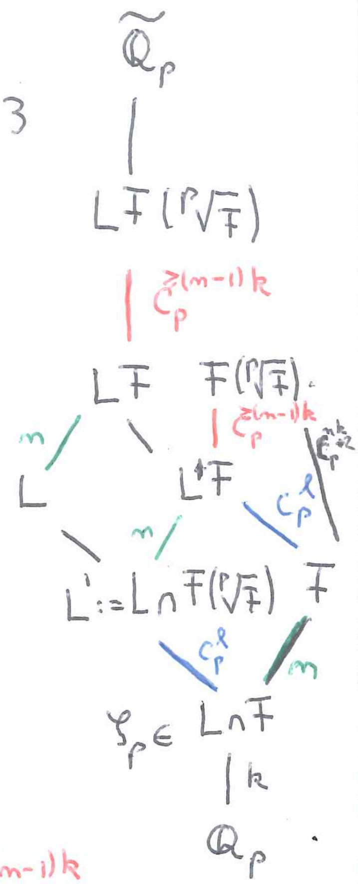
Let $k := [L \cap F : \mathbb{Q}_p]$.

$\Rightarrow [F : L \cap F] = [LF : L] = n$

and $[F : \mathbb{Q}_p] = nk$

Let $F(\sqrt[p]{F}) := F(\{\sqrt[p]{x} \mid x \in F\})$

and let $L' := L \cap F(\sqrt[p]{F})$



$\Rightarrow$ By $G_{\mathbb{Q}_p}$ (4), $\operatorname{Gal}(F(\sqrt[p]{F})/F) \cong C_p^{nk+2}$

$\Rightarrow \operatorname{Gal}(L'F/F) \cong \operatorname{Gal}(L'/L \cap F) \cong C_p^{\ell}$ where $\ell \leq k+2$

$\Rightarrow \operatorname{Gal}(LF(\sqrt[p]{F})/LF) \cong \operatorname{Gal}(F(\sqrt[p]{F})/L'F) \cong C_p^{\geq (n-1)k}$

$(n-1)k \geq 2 \Rightarrow$ Syl-p subgp. of $N = G_L$ non-procyclic. ∎

$\boxed{\S 3 \text{ The Galois code for } \operatorname{Th}(\mathbb{Q}_p)}$

<u>Theorem</u> (K.'95) $\quad G_K \cong G_{\mathbb{Q}_p} \iff K \equiv \mathbb{Q}_p$

<u>Pf.:</u> "$\Leftarrow$" Assume $K \equiv \mathbb{Q}_p$

Let F_m be the compositum of the finitely many extensions of $\mathbb{Q}_p$ of degree $\leq m$ (Cor (4'))

and let $G_m = \operatorname{Gal}(F_m/\mathbb{Q}_p)$

$\Rightarrow K \equiv \mathbb{Q}_p \models \varphi_m$: "the Gal. gp. of the comp. of all degree $\leq m$ extensions is $\cong G_m$"

$\Rightarrow \quad G_K \cong \varprojlim G_m \cong G_{\mathbb{Q}_p}$.

"$\Rightarrow$" Assume $G_K \cong G_{\mathbb{Q}_p}$

<u>Step 1</u> $G_{\mathbb{Q}_p}$ 1 + Galois code for henselianity

$\Rightarrow$ $\forall q \neq p$ prime $\exists$ hens. w_q on K + br. @q s.t. $[\Gamma_w : q\Gamma_w] = q$
char $Kw \neq q$ & $\mu_{q^\infty} \not\subseteq \mathrm{Fix}\, \mathrm{Syl}_q(G_K)$ and $\mathcal{O}_{v_K} \subseteq \mathcal{O}_{w_q}$

$\Rightarrow$ char $K \neq q$, $Kv_K \neq Kv_K^{sep}$ and $\Gamma_{v_K} \neq q\Gamma_{v_K}$

<u>Step 2</u> <u>char $K = 0$</u>

by $G_{\mathbb{Q}_p}$ 2 the unique $C_{p-1} \times C_{p-1}$-ext. F/K has C_p-ext. $\not\Rightarrow C_{p^2}$

$\Rightarrow$ char $K \neq p$

<u>Step 3</u> <u>$\mu'(K) :=$ prime-to-p part of $\mu(K) = \mu_{p-1}$</u>

by $G_{\mathbb{Q}_p}$ 3, $q \neq p, r \geq 1$: $q^r \mid p-1 \Leftrightarrow K$ has $C_{q^r} \times C_{q^r}$-ext. $\Leftrightarrow \zeta_{q^r} \in K$

<u>Step 4</u> <u>char $Kv_K = p$, and so $Kv_K \cap \widetilde{\mathbb{F}}_p = \mathbb{F}_p$</u>

by $G_{\mathbb{Q}_p}$ 5, char $Kv_K \neq 0$ (o/w $\mathbb{Z}_q \trianglelefteq G_K$ for $q \neq p$)
and char $Kv_K \neq q\ (\neq p)$ (o/w ram. subgp. $R \trianglelefteq G$ is pro-q, $\neq 1$)

<u>Step 5</u> <u>For w with $\mathcal{O}_w = \mathcal{O}_{v_K}[\frac{1}{p}]$, Γ_w is divisible, so w.l.o.g. $\mathcal{O}_{v_K}[\frac{1}{p}] = K$.</u>

char $Kw = 0$ ~ 5.

<u>Step 6</u> <u>Kv_K is perfect</u>

$|K^\times/(K^\times)^p| < \infty \Rightarrow |Kv_K^\times/(Kv_K^\times)^p| < \infty$

Kv_K <u>not</u> perfect $\Rightarrow |Kv_K| = \infty \Rightarrow \forall a \in Kv_K\ \exists x \neq y,\ z \neq 0,1$ s.t. $(a - x^p) = (a - y^p)z^p$

$\Rightarrow a = \dfrac{x^p - y^p z^p}{1 - z^p} \in Kv_K^p$ ↯

<u>Step 7</u> <u>$\Gamma_{v_K} \neq p\Gamma_{v_K}$</u> (see below Proposition)

<u>Step 8</u> <u>$\Gamma_{v_K} \cong \mathbb{Z}$</u>

$v_p :=$ coarsest coarsening of v_K with res. char. p ($\Rightarrow v_p$ rank-1)

$\Rightarrow Kv_p$ perfect, so $\bar{v}_K$ induced by v_K on Kv_p has p-div. $\Gamma_{\bar{v}_K} \Rightarrow \Gamma_{v_p} \neq p\Gamma_{v_p}$

Let $1 + a_j \in 1 + \mathfrak{m}_{v_p}$ $(j = 1, \dots, m)$ induce $\mathbb{F}_p$-basis of $(1+\mathfrak{m}_v)/(1+\mathfrak{m}_v)^p$

$\Rightarrow \forall a \in \mathfrak{m}_v$: $1 + a = (1+b)^p \prod_{j=1}^{m} (1+a_j)^{r_j}$ for some $b \in \mathfrak{m}_v$, $0 \leq r_j < p$

$\Rightarrow$ for $v_p(a) < \delta := \min\{v_p(p), v_p(a_1), \dots, v_p(a_m)\}$: $v_p(a) = v_p(b^p)$

$\Rightarrow$ each $\gamma \in]0, \delta[$ is p-div. $\Rightarrow \Gamma_{v_p} = \bigcup_{n \in \mathbb{Z}} n \cdot [0, \delta[$ is p-div. ↯

$\Rightarrow \Gamma_{v_p} = \delta \cdot \mathbb{Z}$ (we see $v_p = v_K$ in Step 9.)

Step 9 $\quad Kv_K = \mathbb{F}_p$

By Step 8, v_p is discrete, so $(1+\mathfrak{m}_{v_p})^p \subseteq 1+\mathfrak{m}_{v_p}^2$

and we have epimorph. $\underbrace{1+\mathfrak{m}_{v_p}/(1+\mathfrak{m}_{v_p})^p}_{\text{finite}} \twoheadrightarrow 1+\mathfrak{m}_{v_p}/1+\mathfrak{m}_{v_p}^2 \twoheadrightarrow Kv_p$

$\Rightarrow Kv_p$ finite $\Rightarrow v_K = v_p$ and, by Step 4, $Kv_K = \mathbb{F}_p$

Step 10 $\quad v_K(p)$ is minimal positive

o/w the uniformizer π in the unique $C_{p-1}\times C_{p-1}$ - extension F/K has $v_K(\pi) < \frac{1}{p-1} v_K(p)$

$\Rightarrow \dim_{\mathbb{F}_p} F^\times/(F^\times)^p > (p-1)^2 + 2$ (by the proof of $G_{\mathbb{Q}_p}$ 4)

contradiction ■

Proposition

(K,v) henselian of char. $(0,p)$, $\mathcal{O}_v[\frac{1}{p}] = K$, G_K small

Then TFAE (i) $\Gamma_v = p\Gamma_v$

(ii) $G_K \cong G_F$ for some F with char $F = p$

[This implies Step 7 using that $G_K \cong G_{\mathbb{Q}_p}$ forces char $K = 0$ by Step 2]

Pf.: $\boxed{(i) \Rightarrow (ii)}$:

Assume $\Gamma_v = p\Gamma_v$.

Let $(K^*, v^*) \succeq (K,v)$ be an elementary $\aleph_1$-saturated extension.

Let $v_p^* :=$ the coarsest coarsening of v^* of res. char. p

$v_0^* :=$ " finest " " " 0

Let $E := K^* v_0^*$

$\Rightarrow v_p^*$ induces (hens.) rk-1 val. $w = v_p^*/v_0^*$ on E with $Ew \cong K^* v_p^*$

$\Rightarrow$ (a) $\underline{\Gamma_w \cong \mathbb{R}}$: as $\Gamma_{v^*} = p\Gamma_{v^*}$ also $\Gamma_w = p\Gamma_w$, so Γ_w is dense in $\mathbb{R}$, and all Dedekind cuts are realized, by (K^*, v^*) being $\aleph_1$-saturated:

Given $\gamma \in \mathbb{R}^{>0}$ there is $x \in K^*$ realizing the type

$$\Phi(x) = \{ r v^*(p) < v^*(x) < s v^*(x) \mid r, s \in \mathbb{Q} \text{ with } r w(p) < \gamma < s w(p) \}$$

then $w(\bar{x}) = \gamma$, where $\bar{x} = x + \mathfrak{m}_{v_0^*} \in E$.

(b) <u>Ew is perfect</u> (as in Step 6)

(c) <u>(E, w) is defectless</u>, i.e. $n = e \cdot f$ for any finite ext. of E

First show: (E, w) has no proper immediate finite ext.:

o/w let $E(\alpha)/E$ be such, $f := \mathrm{Irr}(\alpha/E)$

$\Rightarrow w(f(E))$ bounded, by Krasner

let $\gamma := \sup(w(f(E))) \in \Gamma_w = \mathbb{R}$

and find, by saturation, $x \in E$ with $w(x) = \gamma$

$E(\alpha)/E$ immediate $\Rightarrow \forall \beta \in E(\alpha)\ \exists y \in E$ with $w(y - \beta) > w(\beta)$

$\Rightarrow \exists y \in E$ s.t. $w(y - (x - \alpha)) > w(x - \alpha)$

Let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ be the conjugates of α over E

$\Rightarrow w(z - \alpha_i) = w(z - \alpha_j)$ for all $z \in E$

$\Rightarrow w(f(x-y)) = w\left(\prod_{i=1}^{n} (x - y - \alpha_i)\right) > w\left(\prod_{i=1}^{n} (x - \alpha_i)\right) = w(f(x))$

contradicting $w(x) = \sup(w(f(E)))$.

Same argument for any finite ext. E_1/E

(E_1 has no proper immediate extension)

Hence, the ramification subgroup of G_E w.r.t. w is trivial

$\Rightarrow G_E \cong G_{Ew}$

Note: $\Gamma_{v_0^*}$ is divisible: $\forall$ primes $q\ \exists x_1, \dots, x_r$ s.t. $v(x_i) < v(p)$ and $v(x_1), \dots, v(x_r)$ induce $\mathbb{F}_q$-basis of $\Gamma_v / q\Gamma_v$

(as G_K is small)

$\Rightarrow G_K \cong G_{K^*} \cong G_E \cong G_{Ew}$, so $F = Ew$ does it.

$\boxed{(ii) \Rightarrow (i)}$ [not needed for pf. of Thm]

Assume $\Gamma_v \neq p\Gamma_v \Rightarrow Kv$ perfect, $\Gamma_v \cong \mathbb{Z}$ & Kv finite (as in Steps 6, 8, 9)

$\Rightarrow \exists$ max. r with $\zeta_{p^r} \in K$ (w.l.o.g. $r \geq 1$)

$\Rightarrow K$ admits C_{p^r}-ext. $\not\Rightarrow C_{p^{r+1}}$ (similar to $G_{\mathbb{Q}_p}$ ②)

$\Rightarrow G_K \cong G_F$ for char $F = p$ impossible (similar to Lemma 2) ∎

Lecture 7: Fields with the absolute Galois group of $\mathbb{Q}$

§1 Two Conjectures

Conjecture 1 (K any field)

$G_K \cong G_{\mathbb{Q}} \Rightarrow$ K has henselian valuation v with divisible value gp. and with res. fld. $\mathbb{Q}$

($\Leftarrow$ is clear from Galois theory of henselian fields)

Consequence

$$K = \mathbb{Q} \iff G_K \cong G_{\mathbb{Q}} \ \& \ \forall x, y, z \ (x \cdot y \cdot z = 0 \vee x^3 + y^3 \neq z^3)$$

Theorem (unconditional)

$$K = \mathbb{Q} \iff G_K \cong G_{\mathbb{Q}} \ \& \text{ for all } a \in \mathbb{Z} \setminus \{0\} \ \mathcal{C}_a(K) = \mathcal{C}_a(\mathbb{Q})$$

where $\mathcal{C}_a : \ Y^2 = a \cdot X \cdot (X^2 - 1)(X^2 - 4)$

Conjecture 2 (Birational Section Conjecture in Grothendieck's Anabelian Geometry over $\mathbb{Q}$)

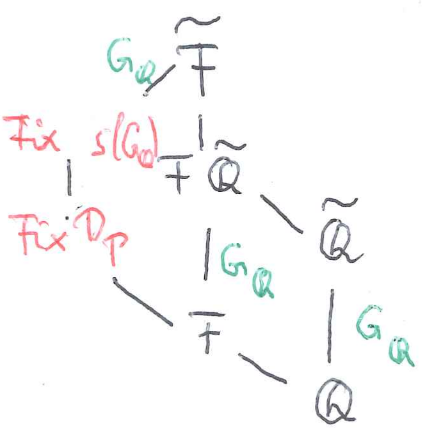
$\mathcal{C}$ smooth projective curve $/\mathbb{Q}$, $F = \mathbb{Q}(\mathcal{C})$

$\Rightarrow$ any section $s : G_{\mathbb{Q}} \to G_F$ of the exact sequ.

$$\begin{tikzcd} 1 \arrow[r] & G_{F\tilde{\mathbb{Q}}} \arrow[r] & G_F \arrow[r, "res"] & G_{\mathbb{Q}} \arrow[r] \arrow[l, bend left, dashed, "s"] & 1 \end{tikzcd}$$

comes from a $\mathbb{Q}$-rational point $P \in \mathcal{C}(\mathbb{Q})$, i.e., $s(G_{\mathbb{Q}}) \subseteq D_P :=$ a decomposition subgp. of G_F w.r.t. v_P on $\tilde{F}$

Note Conj. 2 "=" Conj. 1 for t.d. $K/\mathbb{Q} = 1$



We will, in fact, see that the two Conjectures are equivalent (§3)

§ 2 Exploiting the local structure

$$\varphi : G_K \xrightarrow{\cong} G_{\mathbb{Q}}$$

p prime : let $K_p := \mathrm{Fix}\, \varphi^{-1}(G_{\mathbb{Q}_p^{alg}})$

$\Rightarrow K_p \equiv \mathbb{Q}_p \equiv \mathbb{Q}_p^{alg}$ (Lecture 5/6)

$$\begin{array}{ccccc} \langle G_{K_p} \mid p \in \mathbb{P} \rangle = & G_K & \xrightarrow[\varphi]{\cong} & G_{\mathbb{Q}} & = \langle G_{\mathbb{Q}_p^{alg}} \mid p \in \mathbb{P} \rangle \\ & \rotatebox{90}{$\leq$} & & \rotatebox{90}{$\leq$} & \\ & G_{K_p} & \xrightarrow[\varphi]{\cong} & G_{\mathbb{Q}_p^{alg}} & \end{array}$$

$\Rightarrow$
- K has a unique ordering (all involutions are conjugate)
- for each $p \in \mathbb{P}$, K has a unique p-adic valuation with henselisation K_p
- Let L/K be finite Galois, w_p proleng. of v_p to L

  I_p resp. R_p inertia resp. ramification subgp. of G_{K_p}

  $\Rightarrow$ characteristic subgps (as for $G_{\mathbb{Q}_p}$), so respected by φ.

$\Rightarrow$ For $\pi : G_K \twoheadrightarrow \mathrm{Gal}(L/K)$ canonical restriction,

$D_p(L/K) = \pi(G_{K_p})$ decomp. subgp. w.r.t. w_p

$I_p(L/K) = \pi(I_p)$ $\quad\Rightarrow e(w_p/v_p) = \#\pi(I_p)$

$R_p(L/K) = \pi(R_p)$ $\quad f(w_p/v_p) = [\pi(G_{K_p}) : \pi(I_p)]$

$\Rightarrow$ only finitely many v_p ramify in L/K

& <u>Čebotarev Density Theorem</u>

for $\sigma \in \mathrm{Gal}(L/K)$:

$$\delta(\{p \in \mathbb{P} \mid e(w_p/v_p) = 1 \text{ \& } \sigma \text{ induces Frob. on } \bar{L}/\bar{K}\}) = \frac{\#[\sigma]}{\#\mathrm{Gal}(L/K)}$$

<u>Minkowski-Hensel</u>

For any finite $S \subseteq \mathbb{P}$ and any $n \in \mathbb{N}$ there are only finitely many extensions L/K of degree $\leq n$ unramified outside S.

<u>Prop.</u>: $G_K \cong G_{\mathbb{Q}} \Rightarrow \mathrm{res}: G_K \to G_{\mathbb{Q}}$ is an isomorphism

<u>Pf.</u>: • $K \cap \tilde{\mathbb{Q}} = \mathbb{Q}$, as $K_p \cap \tilde{\mathbb{Q}} = \mathbb{Q}_p^{alg}$

and $\bigcap_p K_p \cap \tilde{\mathbb{Q}} = K \cap \tilde{\mathbb{Q}} = \bigcap_p \mathbb{Q}_p^{alg} = \mathbb{Q}$

$\Rightarrow \mathrm{res}: G_K \to G_{\mathbb{Q}}$ is onto.

• Let $K^{(n)} :=$ compositum of all Galois extensions L/K of degree $\leq n$ ramifying only at primes $\leq n$

$\Rightarrow K^{(n)}/K$ is finite Galois with

$$\left.\begin{array}{l} \mathrm{Gal}(K^{(n)}/K) \cong \mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q}) \\ K\mathbb{Q}^{(n)} \subseteq K^{(n)} \ \& \ K \cap \tilde{\mathbb{Q}} = \mathbb{Q} \end{array}\right\} \Rightarrow K\mathbb{Q}^{(n)} = K^{(n)}$$

$\Rightarrow \tilde{K} = \bigcup_n K^{(n)} = \bigcup_n K\mathbb{Q}^{(n)} = K(\bigcup_n \mathbb{Q}^{(n)}) = K\tilde{\mathbb{Q}}$

$\Rightarrow \mathrm{res}: G_K \to G_{\mathbb{Q}}$ is 1-1 ∎

<u>Corollary</u> K satisfies <u>Kronecker-Weber</u>

Also get <u>Local-Global Principles</u> for quadratic forms (<u>Hasse-Minkowski</u>), for Brauer groups (<u>Hasse-Brauer-Noether</u>), the <u>Quadratic Reciprocity Law</u>, the <u>Four Squares Theorem</u> etc.

<u>Proof of Thm (p. 24)</u> „$\Leftarrow$" („$\Rightarrow$" is trivial)

Assume $G_K \cong G_{\mathbb{Q}}$, but $K \neq \mathbb{Q}$

pick $x \in K \setminus \mathbb{Q} \Rightarrow x$ transcendental $/\mathbb{Q}$

and, as $\mathrm{res}: G_K \to G_{\mathbb{Q}}$ is an iso.,

the square class of $x \cdot (x^2-1) \cdot (x^2-4)$

is represented by some (squarefree) $a \in \mathbb{Z} \setminus \{0\}$

$\Rightarrow K \models \exists y \ \ y^2 = a \cdot x \cdot (x^2-1)(x^2-4)$

$\Rightarrow \mathcal{C}_a(K) \supsetneq \mathcal{C}_a(\mathbb{Q}) \leftarrow$ finite by Faltings ∎

§3 Reduction to t.d. $K/\mathbb{Q} = 1$

Assume $G_K \cong G_{\mathbb{Q}}$, but $K \neq \mathbb{Q}$

and assume Conj. 1 for all $L/\mathbb{Q}$ of t.d. 1 with $G_L \cong G_{\mathbb{Q}}$.

$\Rightarrow$ for $L/\mathbb{Q}$ of t.d. 1 with $L \subseteq K$ rel.y alg.y cl. we have

$$\begin{tikzcd} G_K \arrow[r, "res", "\cong"'] \arrow[rr, bend right, "res"', "\cong"] & G_L \arrow[r, "res", "\cong"'] & G_{\mathbb{Q}} \end{tikzcd}$$

$\cong$ ← from Prop.

Let v_p on K be as in §2

and let $\tilde{v}_p$ be the coarsening of v_p with $\mathcal{O}_{\tilde{v}_p} = \mathcal{O}_{v_p}[\frac{1}{p}]$.

Let w be the henss. val. on L with Γ_w div. & $Lw = \mathbb{Q}$

$\Rightarrow$ for all primes p, q: $\mathcal{O}_w = \mathcal{O}_{\tilde{v}_p^L} = \mathcal{O}_{\tilde{v}_q^L}$

where $v_p^L = v_p \upharpoonright L$

$\Rightarrow \{0\} \neq \mathfrak{m}_{\tilde{v}_p^L} = \mathfrak{m}_{\tilde{v}_q^L}$

$\Rightarrow \{0\} \neq \mathfrak{m}_{\tilde{v}_p} = \mathfrak{m}_{\tilde{v}_q}$ on K:

if $x \in \mathfrak{m}_{\tilde{v}_p} \setminus \mathfrak{m}_{\tilde{v}_q}$ consider $L' := \widetilde{\mathbb{Q}(x)} \cap K$

$\Rightarrow \exists$ non-trivial valuation v on K

with $\mathfrak{m}_v = \mathfrak{m}_{\tilde{v}_p}$ for all primes p

$\Rightarrow$ Γ_v is divisible

& Kv is the compositum of all Lw's $= \mathbb{Q}$

& v is henselian:

o/w the henselisation K^h w.r.t. v is a proper ext. of K

$\Rightarrow G_{\mathbb{Q}} \cong G_{K^h} \lneq G_K \cong G_{\mathbb{Q}}$

Contradicting a Theorem of Neukirch ∎

§ 4 Global integers

Lemma $G_K \cong G_{\mathbb{Q}}$, $\mathcal{O}_K := \bigcap_{p \in \mathbb{P}} \mathcal{O}_{v_p}$, $\mathfrak{m}_K := \bigcap_{p \in \mathbb{P}} \mathfrak{m}_{v_p}$

$\Rightarrow$ (a) $\mathcal{O}_v^\times = \bigcap_p \mathcal{O}_{v_p}^\times = \pm 1 + \mathfrak{m}_K$

(b) for $x \in K$, $\Sigma^+(x) := \{ p \in \mathbb{P} \mid v_p(x) \geq 0 \}$

is either $= \mathbb{P}$ or $\delta(\Sigma^+(x)) = 0$

(c) $\mathfrak{m}_K$ is a prime ideal of $\mathcal{O}_K$.

Note • If K satisfies Conj. 1 with henselian v..

then $\mathcal{O}_K = \mathbb{Z} + \mathfrak{m}_v$ and $\mathfrak{m}_K = \mathfrak{m}_v$.

• without Conj. 1, we don't know whether $K = \mathrm{Frac}(\mathcal{O}_K)$

or whether $\mathcal{O}_K \neq \mathbb{Z}$ (for $K \neq \mathbb{Q}$)

Pf. (b) pick $q \in \mathbb{P} \setminus \Sigma^+(x)$

$\Rightarrow 1 + x^2 q^{-1} \notin K_q^2$, but $1 + x^2 q^{-1} \in K_p^2$ for all $p \in \Sigma^+(x) \setminus \{2\}$

$\Rightarrow$ by Čebotarev applied to $\sigma = 1 \in \mathrm{Gal}(K(\sqrt{1+x^2q^{-1}})/K)$,

$\delta(\Sigma^+(x)) \leq \frac{1}{2}$

Let $1 + x^2 q^{-1} \in q_1 \cdots q_r \cdot (K^\times)^2$ for some primes $q_1, \ldots, q_r$

$\Rightarrow$ for $\ell \in \mathbb{P} \setminus (\Sigma^+(x) \cup \{2, q_1, \ldots, q_r\})$, $1 + x^2 \ell^{-1} \notin K_\ell^2$

$\Rightarrow$ Čeb. applied to $\sigma = 1 \in \mathrm{Gal}(K(\sqrt{1+x^2q^{-1}}, \sqrt{1+x^2\ell^{-1}})/K)$

$\cong C_2 \times C_2$

get $\delta(\Sigma^+(x)) \leq \frac{1}{4}$ etc...

(c) If $x, y \in \mathcal{O}_K$ with $x \cdot y \in \mathfrak{m}_K$

then $\mathbb{P} = \Sigma^+(x \cdot y) \subseteq \Sigma^+(x) \cup \Sigma^+(y)$

$\Rightarrow$ by (b), $\mathbb{P} \subseteq \Sigma^+(x)$ or $\mathbb{P} \subseteq \Sigma^+(y)$

so $x \in \mathfrak{m}_K$ or $y \in \mathfrak{m}_K$ ∎

<u>Corollary</u> (the semilocal case)

$G_K \equiv G_{\mathbb{Q}}$, t.d. $K/\mathbb{Q} = 1$,
assume there is $P \subseteq \mathbb{P}$ with $\delta(P) > 0$ s.t.
all v_p $(p \in P)$ induce the same topology
[e.g. if the v_p's $(p \in \mathbb{P})$ induce only finitely many topologies on K]
$\Rightarrow$ $\exists$ hens. v on K with divisible Γ_v and $Kv = \mathbb{Q}$.

§5 The model-theoretic variant

<u>Super-strong Conjecture!</u>

$$\left.\begin{array}{l} G_K \equiv G_{\mathbb{Q}} \\ G_K \succeq G_{\mathbb{Q}} \end{array}\right\} \Rightarrow$$ K has hens. val. v with divisible Γ_v and $Kv \equiv \mathbb{Q}$

<u>Note</u> Super $\Rightarrow$ Strong $\Rightarrow$ Conjecture

For any $\mathbb{Q}^* \underset{\neq}{\succeq} \mathbb{Q}$: res: $G_{\mathbb{Q}^*} \to G_{\mathbb{Q}}$ is onto,
but <u>not</u> 1-1

The model-theoretic analogue for Prop. (on page 26):

$$G_K \equiv G_{\mathbb{Q}} \Rightarrow G_K \succeq G_{\mathbb{Q}}$$

is probably extremely hard to show (if true).