

Algebraische Zahlentheorie II.

Übungsbücher: Vorlesungshomepage.

01. PROENGLICHE GRUPPEN

Wkg.: X Menge, Topologie auf $X: \tau \subseteq \mathcal{P}(X)$ mit

$$(0) \emptyset, X \in \tau \quad (1) U, V \in \tau \Rightarrow U \cap V \in \tau \quad (2) (U_i)_{i \in I} \in \tau^I \Rightarrow \bigcup_i U_i \in \tau$$

$\mathcal{B} \subseteq \tau$ heißt **Basis**: $\Leftrightarrow \forall U \in \tau \exists (B_i)_{i \in I} \in \mathcal{B}^I: U = \bigcup_i B_i$

$W \subseteq X$ heißt **Umgebung (von $x \in X$)**: $\exists V \in \tau: x \in V \subseteq W$.

Für $x \in X$ sei $U(x)$ die Menge aller Umgebungen von x .

z.B.: (X, d) metrischer Raum $\Rightarrow \{\mathcal{B}_\epsilon(x) \mid x \in X, \epsilon > 0\}$ ist Basis für X .

$(X, \tau_X) \xrightarrow{f} (Y, \tau_Y)$ heißt **stetig**: $\Leftrightarrow f^{-1}(\tau_Y) \subseteq \tau_X$.

Produkttopologie: Seien $((X_i, \tau_i))_{i \in I}$ topologische Räume.

Basis der **Produkttopologie** auf $\prod_i X_i$: $\{\prod_i U_i \mid U_i \in \tau_i, U_i = X_i \text{ f.f.a. } i \in I\}$

Satz von Tychonoff: Sind alle X_i kompakt, so auch $\prod_i X_i$

Sei $X \xrightarrow{\pi} Y$ surjektiv, (X, τ) top. Raum.

$\{V \subseteq Y \mid \pi^{-1}(V) \in \tau\}$ heißt **Quotiententopologie**.

Def. 1.1.(a) Eine **topologische Gruppe** (G, e, \circ, τ) besteht aus einer Gruppe (G, e, \circ) und einem top. Raum (G, τ) so dass

$G \times G \xrightarrow{\mu} G, (g, h) \mapsto goh, G \xrightarrow{i} G, g \mapsto g^{-1}$ stetig sind, wobei $G \times G$ die Produkttopologie trägt.

(b) Ein **Morphismus topologischer Gruppen** ist ein stetiger Gruppenhomomorphismus.

⇒ Man erhält die Kategorie **topologischer Gruppen** Top Grp.

Bsp. (ü) K normierter Körper $\Rightarrow (K, +), (K^\times, \cdot)$ sind topologische Gruppen.

Facts 1.2. Seien G, G' top. Grp., $G \xrightarrow{\phi} G'$ ein Gruppenhomomorphismus.

- (i) $l_g : G \rightarrow G, h \mapsto gh$, $r_g : G \rightarrow G, h \mapsto hg^{-1}$ sind Automorphismen (insb. Homöomorphismen)
- (ii) ϕ ist stetig $\Leftrightarrow \forall W' \in \mathcal{U}(e') : \exists W \in \mathcal{U}(e) : \phi(W) \subseteq W'$
- (iii) Eine offene Untergruppe $H \leq G$ ist abgeschlossen.
- (iv) Eine abgeschlossene Untergruppe $H \leq G$ mit $[G : H] < \infty$ ist offen.
- (v) Ist G kompakt, $H \leq G$ offen, so gilt $[G : H] < \infty$.
- (vi) Ist $H \leq G$ Untergruppe, so ist $(H, \tau_{G|H})$ eine topologische Untergruppe (Unterraumtop.)
- (vii) Ist $U \subseteq G$, so ist $U^{-1} \subseteq G$ und $\text{cl}(U) = \bar{U} \subseteq UU^{-1}$
- (viii) G ist regulär, d.h. $\forall g \in G : \exists U, V \in \mathcal{U}(g)$ offen s.d. $V \subseteq \bar{V} \subseteq U$
- (ix) G ist hausdorffsch $\Leftrightarrow \{e\} \subseteq G$ abg.
- (x) Ist $N \trianglelefteq G$ Normalteiler, so ist G/N topologische Gruppe mit Quotiententopologie.
Dabei ist G/N hausdorffsch, falls $N \trianglelefteq G$ abg.
- (xi) Sind $(G_i)_{i \in I}$ top. Grp., so ist $\prod_i G_i$ top. Grp.

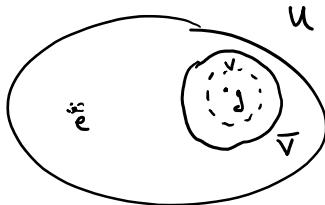
Beweis.

- (i) $l_g : G \rightarrow \{g\} \times G \xrightarrow{\text{inkl.}} G \times G \xrightarrow{N} G$ ist stetig, $l_g \circ l_{g^{-1}} = \text{id}_G$
 r_g analog.
- (ii) " \Rightarrow ": klar;
 " \Leftarrow ": Sei $g \in G$, $g' := \phi(g)$, $W \in \mathcal{U}(e)$. Wähle $V \in \mathcal{U}(e)$ mit $\phi(V) \subseteq \underbrace{(g')^{-1}W}_{= l_{g'^{-1}}(W)}$
 $\Rightarrow \phi(l_g(v)) \subseteq W$, also ist ϕ stetig.
- (iii) $G = H \cup \bigcup_{\substack{g \in G/H \\ g \neq 0}} gH$
 $\quad \quad \quad$ offen, da $gH = l_g(H)$
- (iv) wie (iii): $G = H \cup \bigcup_{\substack{g \in G/H \\ g \neq 0}} \underbrace{gH}_{\text{abg}}$
 $\quad \quad \quad$ abg., da endliche Vereinigung wg. $[G : H] < \infty$
- (v) $G = \bigcup_{\substack{g \in G/H \\ g \neq 0}} gH$ G kompakt $\Rightarrow [G : H] < \infty$
- (vi), (vii): Übung.

(viii) $\Leftrightarrow g = e$ wegen (i). Sei U offene Umgebung von e .

Bew. (ü) \exists offene Umgb. V von e mit $V \cdot V \subseteq U$, $V = V^{-1}$. Nun verwende (vii).

(ix) g.z.z.: können e und $g \neq e$ trennen (wg. (i))



$$G \setminus \bar{V} \cap V = \emptyset$$

(x), (xi) übung. ■

Why. I sei teilgeordnete, filtrierte Menge, d.h. $\forall i, j \in I : \exists k \in I : i, j \leq k$.

Ein **inverses System (von Gruppen)** besteht aus einer Familie von Gruppen $(G_i)_{i \in I}$ zusammen mit Gruppenhomomorphismen $\phi_{ji} : G_j \rightarrow G_i \quad \forall i, j \in I$ mit $i \leq j$.
so dass: (i) $\phi_{ii} = \text{id}_{G_i}$ (ii) $\phi_{ki} = \phi_{ji} \circ \phi_{kj} \quad \forall i \leq j \leq k$

Dann heißt $\varprojlim_{i \in I} G_i$ Limes des inversen Systems ... hat übliche universelle Eigenschaft.

• $\varprojlim_{i \in I} G_i$ existiert und ist gegeben durch $G := \{(g_i)_{i \in I} \in \prod_i G_i \mid \phi_{ji}(g_j) = g_i \quad \forall i \leq j\}$

Lemma 1.3. Sind alle G_i topologische Gruppen, so auch $\varprojlim_{i \in I} G_i$ mit der Unterräumtop. von $\prod_i G_i$.

Sind alle G_i hausdorffsch (kompakt + hausdorffsch),

so ist auch $\varprojlim_{i \in I} G_i$ hausdorffsch (kpt. + hd.).

Beweis.

① $\prod_i G_i$ ist selbst $\varprojlim_{i \in I} G_i$ für geeignet gewähltes inverses System I .

Alle G_i hausdorffsch $\rightarrow \prod_i G_i$ hausdorffsch (Produkte von Hausdorfräumen sind hausdorffsch)
Kompakt folgt mit dem Satz von Tychonoff.

② Allgemeiner Fall: Hausdorffsch überträgt sich auf Unterräume $\Rightarrow \varprojlim_{i \in I} G_i$ hd.

$$\varprojlim_{i \in I} G_i = \bigcap_{i \leq j} \underbrace{\{(g_k)_k \in \prod_k G_k \mid \phi_{ji}(g_j) = g_i\}}_{= \prod_{k \neq i,j} G_k \text{ abg.}} \subseteq \prod_k G_k$$

$\Rightarrow \varprojlim_{i \in I} G_i$ kpt. da abg. Teilraum eines kpt. Raumes. ■

Def. 1.4. Eine **proendliche Gruppe** ist ein inverser Limes $\lim_{\leftarrow} G_i$ endlicher, diskreter topologischer Grp. $(G_i)_{i \in I}$ mit der Topologie aus 1.3.
(insb.: alle G_i hausdorffsch und kompakt)

Def. 1.5. Ein topologischer Raum heißt **total unzusammenhängend**:
Jedes $x \in X$ besitzt eine Umgebungsbasis aus offen-abgeschlossenen Mengen
 \Leftrightarrow Die Zusammenhangskomponente von x ist $\{x\}$

Proposition 1.6. (ii) Eine kpt., hd. top. Grp. ist total unzusammenhängend \Leftrightarrow es besitzt eine Umgebungsbasis aus offen-abgeschlossenen Normalteilen von Gr.

□

05

Freitag, 20. April 2018 09:17

Korrektur: X top. Raum. X heißt **zusammenhängend** : $\Leftrightarrow \emptyset, X$ sind die einzigen offen + abg. Teilmengen. $x \sim_{\text{zh}} y : \Leftrightarrow \exists Y \subseteq X$ zushd.: $x, y \in Y$ ist ÄquivalenzrelationÄquivalenzklassen unter \sim_{zh} heißen **zusammenhangskomponenten**.

Lemma. (Ribes-Zaleski, Lemma 1.1.11)

 X kpt., hd. und $x \in X$. Dann ist die Zusammenhangskomp. die x enthält die Menge

$$[x]_{\text{zh}} = \bigcap \{U \subseteq X \mid x \in U, U \text{ offen abg.}\}$$

Def. 1.5. Ein topologischer Raum X heißt **total-zusammenhängend** \Leftrightarrow alle Zshgskomp. von X sind 1-elementig.Korollar. (aus Lemma) Sei X kompakt, hd. Dann gilt: X total unzshd \Leftrightarrow jedes $x \in X$ besitzt eine Umgebungsbasis aus offen-abg. Mengen.Satz 1.7. Sei G eine topologische Gruppe. Dann sind äquivalent:(i) G ist profinlich (ii) G ist kompakt, hausdorffsch und total unzusammenhängend.

Beweis.

(i) \Rightarrow (ii): kompakt, hausdorffsch: letztes Mal.z.B.z.: $e \in \prod G_i$ besitzt Umgebungsbasis aus offen abgeschlossenen Teilmengen.Eine solche ist gegeben durch $\left\{ \prod_{i \in I_0} \{e_{i_0}\} \times \prod_{i \in I \setminus I_0} G_i \mid I_0 \subseteq I \text{ endlich} \right\} =: U_e$ letztes Mal: G kpt., hd., $H \leq G$ offene Untergrp. $\Rightarrow H$ abg. NormalteilerAllgemeiner Fall: Schneide U_e mit $\lim_{\leftarrow} G_i$.(ii) \Rightarrow (i): Konsequenz aus dem folgenden Lemma.Lemma 1.8. Sei G kompakt, hausdorffsch, total unzshd. und U eine Umgebungsbasis der Eins beschreibend aus offen-abg. Normalteilern.

Dann ist

$$G \xrightarrow{\varphi} \lim_{N \in U} G/N, g \mapsto (gN)_{N \in U}$$

ein Isomorphismus topologischer Gruppen. (G/N endl. diskret)Beweis. φ stetig: "obvious".
beachte $G \xrightarrow{\varphi} \prod_{N \in U} G/N \leftarrow$ hat Umgebungsbasis U_e (s. 1.7).Für $I_0 \subseteq U_e$ endl. \rightsquigarrow Umgebung $\prod_{N \in I_0} G/N \times \prod_{N \in U_e \setminus I_0} G/N$ Urbild ist $\bigcap_{N \in I_0} N$ ist offen abg. Normalteiler in G \Rightarrow stetig bei $e \Rightarrow$ stetig. φ injektiv: $\varphi(g) = (gN)_{N \in U} \Rightarrow g \in N \quad \forall N \in U$.
Umgebungsbasis, G hausdorffsch.

$$\Rightarrow \bigcap_{N \in U_e} N = \{e\}, \text{ d.h. } g = e.$$

- φ surjektiv. sei $(g_N \cdot N)_{N \in \mathbb{N}} \in \varprojlim G/N$ ($N' \subseteq N \rightarrow g_{N'} \cdot N = g_N \cdot N$)

gesucht:

$$g \in \bigcap_{N \in \mathbb{N}} (g_N \cdot N)_{\text{abg.}} \subseteq G \text{ kompakt}$$

Ann.:

rechte Seite leer $\Rightarrow \exists I_0 \subseteq \mathbb{N}$ endlich: $\bigcap_{N \in I_0} g \cdot N = \emptyset$. \mathcal{U} Umgebungsbasis

$$\Rightarrow \exists N' \subseteq \bigcap_{N \in I_0} N$$

φ Homöomorphismus: φ bijektiv, stetig, G kompakt, $\varprojlim G/N$ hausdorffsch.

Bem. 1.9. (i) 1.8 ist anwendbar, wenn G proendlich

(ii) analog zu 1.8 lassen sich auch beweisen: G proendlich, \mathcal{U} wie 1.8

$$(a) \forall H \leq G \text{ abg. gilt: } H \xrightarrow{\sim} \varprojlim_{N \in \mathbb{N}} H/N \cdot H$$

$$(b) \forall H \cong G \text{ abg. gilt } G/H \xrightarrow{\sim} \varprojlim_{N \in \mathbb{N}} G/N \cdot H$$

Lemma 1.10. Sei G proendlich, $H \leq G$ Untergruppe. Dann sind äquivalent:

(i) H ist abgeschlossen

$$(ii) H = \bigcap \{ U \mid U \subseteq G \text{ offene Untergruppe mit } H \leq U \}$$

Bewis.

" \Leftarrow ": $U \subseteq G$ offen $\xrightarrow{G \text{ kpt.}}$ U abg. Untergruppe $\Rightarrow \bigcap \{ U - \}$ ist abgeschlossen.

" \Rightarrow ": Sei $V \in \mathcal{U}$ (\mathcal{U} wie oben) $\Rightarrow \underbrace{H \cdot V}_{= \bigcup_{h \in H} h \cdot V}$ ist offene Untergruppe von G .

$$\text{In ii: } H \leq G \text{ kompakt} \\ \text{Teilmenge} \quad \Rightarrow \quad \bigcap_{V \in \mathcal{U}} H \cdot V = H.$$

Def. 1.11. Eine **pro-p Gruppe** ist ein inverser Limes von endlichen p-Gruppen.

Def. 1.12. Sei G eine diskrete (i.a. unendliche) Gruppe.

Die **pro-p Komplettierung** von G ist **endliche proendliche**

$$\text{Bsp. } \hat{\mathbb{Z}}^p = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n \mathbb{Z} = \mathbb{Z}_p$$

$$\hat{G}^p := \varprojlim \{ G/N \mid N \trianglelefteq G \text{ und } G/N \text{ ist endliche p-Grp.} \}$$

(man kann auch Ringe pro-p oder pro-chdl. komplettieren)

Def. 1.13. Der **Prüferring** ist die proendliche Komplettierung von \mathbb{Z} , $\hat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/n \mathbb{Z}$

($\{ n\mathbb{Z} \mid n \in \mathbb{N} \}$ bzgl. Inklusion, d.h. Teilbarkeit geordnet)

Lemma. $\hat{\mathbb{Z}} \cong \prod_{p \text{ prim}} \mathbb{Z}_p$

Beweis.

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}_{n\infty} \stackrel{\text{crs}}{\cong} \varprojlim_n \left(\prod_{p \text{ prim}} \mathbb{Z}_{p^{v_p(n)}} \right); \prod_p \mathbb{Z}_p = \varprojlim_{n \in \mathbb{N}} \prod_p \mathbb{Z}_p / u_n$$

$$u_n = \left\{ \prod_p \mathbb{Z}_{p^{v_p(n)}} \mid n \in \mathbb{N} \right\}$$

$$=: u_n$$

Def. 1.14 Eine Teilmenge $S \subseteq G$ heißt **topologisches Erzeugendensystem** (ES) : \Leftrightarrow
 G ist der topologische Abschluss der von S erzeugten Untergruppe.

Bsp. $\{1\}$ ist topologisches ES von \mathbb{Z}_p und $\hat{\mathbb{Z}}$

Def. 1.15 Eine topologische Gruppe G heißt **topologisch endlich erzeugt** : $\Leftrightarrow \exists S \subseteq G$ endlich s.d.
 S ist top. ES von G

Bsp. Die proendl. bzw. pro-p Komplettierung der freien nicht-abelschen Gruppen mit endlich vielen Erzeugern

Satz 1.16. (**Burnside Basissatz**)

Sei G eine pro-p-Gruppe. Sei $\phi(G)$ der topologische Abschluss der von $[G, G]$ und
 $G^p = \{g^p \mid g \in G\}$ erzeugten Untergruppe. ($\phi(G)$ heißt **Frattini-Untergruppe** von G)

Dann:

G ist topologisch endl. erz. $\Leftrightarrow G/\phi(G)$ ist endlicher \mathbb{F}_p -VR.

Bilden $\bar{b}_1, \dots, \bar{b}_n$ eine Basis von $G/\phi(G)$, dann ist $\{b_1, \dots, b_n\}$ ein minimales ES.

Beweis. (ü).

Bem. 1) $G/\overline{[G, G]}$ ist abelsche, hausdorff. topol. Grp.

$\rightarrow G/\overline{[G, G]G^p}$ ist abelsche p -Torsionsgruppe (d.h. \mathbb{F}_p -VR)
 (-,-,- heißt **p-elementar abelsch**)

2) Sei G eine abelsche pro-p-Gruppe.

(a) Dann ist G ein \mathbb{Z}_p -Modul!, d.h. haben stetige \mathbb{Z}_p -Operation $\mathbb{Z}_p \times G \rightarrow G$

$$\underbrace{\alpha \cdot g}_{\in \mathbb{Z}_p} := (\alpha \bmod \#G_i \cdot j_i)_{i \in I} \in \varprojlim_I G_i = G,$$

$$\begin{aligned} &= \varprojlim_n \mathbb{Z}_{p^n} \\ &= (j_i)_i \in \varprojlim G_i \\ &\quad \text{endl. abelsche } p\text{-Grp.} \\ &= \alpha \bmod \text{ord}(j_i) \cdot j_i \end{aligned}$$

$$\left(\text{wohldef? } \pi_{j_i}: G_j \rightarrow G_i \quad \pi_{j_i}(\alpha \bmod \text{ord}(j_i) \cdot j_i) = (\alpha \bmod \text{ord}(j_i) \cdot j_i) \right)$$

$$\text{z.B. } (1+p\mathbb{Z}_p, \cdot) = \varprojlim_n \left(\frac{1+p\mathbb{Z}_p}{1+p^n\mathbb{Z}_p} \right) \quad \text{ord}(j_i) \mid \text{ord}(j_j)$$

$$\begin{aligned} \beta \in 1+p\mathbb{Z}_p, \alpha \in \mathbb{Z}_p \\ \sim p^\alpha \in 1+p\mathbb{Z}_p \end{aligned}$$

$$= \left\{ \beta \in (\mathbb{Z}/p^n\mathbb{Z})^\times \mid \beta \equiv 1 \pmod{n} \right\} = \langle 1+p \rangle \cong \mathbb{Z}/p^{n-1}$$

(b) G topol. endlich erzeugt $\Leftrightarrow G$ ist endl. erz. als \mathbb{Z}_p -Modul

In diesem Fall kann man den Struktursatz für endl. erz. Moduln über H.I.-Ringen anwenden
 $\Rightarrow G \cong \mathbb{Z}_p^r \times \prod_{i=1}^k \mathbb{Z}/p^{n_i} \mathbb{Z}$

02. GALOISTHEORIE UND UNENDLICHE GALOISERWEITERUNGEN

Wdg. $L|K$ algebraische Erweiterung von Körpern

$L|K$ normal $\Leftrightarrow \forall \alpha \in L : \text{minpol}_K(\alpha) \in K[X]$ zerfällt über L in Linearfaktoren

$L|K$ separabel $\Leftrightarrow \forall \alpha \in L : \text{minpol}_K(\alpha)$ besitzt nur einfache Nullstellen in K^{alg} .

$L|K$ galoissch: $\Leftrightarrow L|K$ normal + separabel

Definiere dann: $\text{Gal}(L|K) := G_{L|K} := \{ \sigma \in \text{Aut}(L) \mid \sigma|_K = \text{id}_K \}$

Fakt: Ist $L|F|K$ ein Zwischenkp., so ist $L|F$ galoissch.

Hauptsatz der endlichen Galoistheorie: $L|K$ endlich \Rightarrow Die Abbildungen

$$\{ H \in \text{Gal}(L|K) \mid H \text{G} \} \xrightleftharpoons[\text{Gal}(L|F) \hookleftarrow F]{} \{ L|F|K \text{ Zwischenkp.} \}$$

definiert eine Bijektion.

$$\{ H \trianglelefteq G \text{ NT} \} \xrightleftharpoons[1:1]{\quad} \{ F \text{ Zwkp.} \mid F|K \text{ galoissch} \}$$

Was geht schief, wenn $L|K$ unendlich?
 Man hat zu viele Untergruppen!

Proposition 2.1. Sei $L|K$ galoissch. Sei $\Sigma := \{E \mid L \text{ Unterkörper} \mid E|K \text{ endlich galoissch}\}$, geordnet mit \subseteq , $\rightsquigarrow (\Sigma, \subseteq) \rightarrow \text{Grp}, E \mapsto \text{Gal}(E|K)$ ist ein inverses System.

Dann ist $\text{Gal}(L|K) \xrightarrow{\delta} \varprojlim_{E \in \Sigma} \text{Gal}(E|K), \delta \mapsto (\delta|_E)_{E \in \Sigma}$
ein Gruppenisomorphismus.

Beweis.

- Homomorphismus nach Konstruktion.
- Injektiv: $\delta(\delta) = \text{id} \Leftrightarrow \delta|_E = \text{id}_E \forall E \in \Sigma \Rightarrow \delta = \text{id}_L$

- Surjektiv: Sei $(\delta_E)_{E \in \Sigma} \in \varprojlim_{E \in \Sigma} \text{Gal}(E|K) \subseteq \prod_{E \in \Sigma} \text{Gal}(E|K)$

$$\text{d.h.: } E' | E \in \Sigma \Rightarrow \delta_{E'}|_E = \delta_E$$

Wegen $L = \bigcup_{E \in \Sigma} E$, definiere $\delta: L \rightarrow L, x \mapsto \delta_E(x)$ falls $x \in E \in \Sigma$

(wohldefiniert, da $(\delta_E)_E$ kompatibel)

$$\Rightarrow \delta \in \text{Gal}(L|K) \text{ mit } \delta(\delta) = (\delta_E)_E$$

(Automorphismus da $\delta|_E$ Automorphismen)



Def. 2.2. Die Krulltopologie auf $\text{Gal}(L|K)$ ist die Topologie für welche δ ein Isomorphismus topologischer Gruppen wird. (mit der proendl. Topologie auf $\varprojlim_{\Sigma} \text{Gal}(E|K)$)

Konkret: Umgebungsbasis der Eins in $\text{Gal}(L|K)$ ist $\{\underbrace{\text{Gal}(L|E)}_{= \ker(\text{Gal}(L|K) \rightarrow \text{Gal}(E|K))} \mid E \in \Sigma\} \leftarrow$ Umgebungsbasis offen-abg.
Normalteiler von $\text{Gal}(L|K)$

Lemma 2.3. Sei $L|K$ galoissch. Dann sind die offenen Untergruppen von $\text{Gal}(L|K)$ gerade die Untergruppen $\text{Gal}(L|F)$ mit $F|K$ endlich.

Beweis. Sei $H \leq \text{Gal}(L|K)$ offene Untergruppe. Wähle $E \in \Sigma$ mit $\text{Gal}(L|E) \subseteq H$.

$$\Rightarrow \overline{H} = \text{Bild von } H \text{ in } \text{Gal}(E|K) = \{\delta|_E \mid \delta \in H\} \quad (= \frac{\text{Gal}(L|K)}{\text{Gal}(L|E)})$$

\vdash sei $F = E^{\overline{H}}$... Prüfe: $H = \text{Gal}(L|F)$.

$\begin{matrix} & E \\ \vdash & F \\ \text{endlich} & K \end{matrix} \vdash$ Umgekehrt: $F|K$ endl. Erweiterung in $L \rightsquigarrow$ Sei E der Galoisabschluss von $F|K$
 $\Rightarrow [E:K] < \infty \Rightarrow \underbrace{\text{Gal}(L|E)}_{\text{offen}} \subseteq \text{Gal}(L|F)$.

$$\Rightarrow \text{Gal}(L|F) = \bigcup_{\substack{j \in \text{Gal}(L|F) \\ \text{offen}}} j \text{Gal}(L|E) \subseteq \text{Gal}(L|K)$$



10 Korollar 2.4. Sei $L \mid K$ wie in 2.3. Dann gilt:
 $\{H \subseteq \text{Gal}(L \mid K) \mid H \text{ abg.}\} = \{\text{Gal}(L \mid F) \mid L \mid F \mid K\}$

Beweis.
 \hookrightarrow : Schreibe $F = \bigcup_{i \in I} F_i$, I Menge, $F_i \mid K$ endl. Erw.

Dann:
 $\text{Gal}(L \mid F) = \bigcap_{i \in I} \underbrace{\text{Gal}(L \mid F_i)}_{\text{offen abgeschlossen}}$
 $\sigma|_F = \text{id}_F \quad \sigma|_{F_i} = \text{id}_{F_i}$

" \subseteq ": Jede abg. Untergruppe einer proenzellischen Gruppe ist der Durchschnitt offener Untergruppen
(1.10)

$$H = \bigcap_{i \in I} u_i \quad u_i: \text{offene Untergruppe in } G, \quad u_i = \text{Gal}(L \mid F_i) \text{ nach 2.3}$$

$$\xrightarrow{F = K \cap F_i \mid i \in I} = \bigcap_{i \in I} \text{Gal}(L \mid F_i) = \text{Gal}(L \mid F)$$

Satz 2.5. Sei $L \mid K$ galoissch. Dann sind die Abbildungen

$$\{H \subseteq \text{Gal}(L \mid K) \mid H \text{ abg.}\} \xrightleftharpoons[\text{Gal}(L \mid F)]{H \mapsto L^+} \{F \subseteq L \mid F \mid K \text{ Körpererweiterung}\}$$

zueinander inverse Bijektionen (ordnungsmässig). Die Restriktionen der Abbildungen definieren Bijektion:

$$\{H \subseteq \text{Gal}(L \mid K) \mid H \text{ abg. Normalteiler}\} \xrightleftharpoons[\text{Gal}(L \mid F)]{} \{E \subseteq L \mid E \mid K \text{ Galoiserweiterung}\}$$

zubr. gilt (topologisch):

$$\text{Gal}(L \mid K) \xrightarrow[N]{\sim} \text{Gal}(L^N \mid K)$$

Beweis. Reduktion auf den endlichen Fall. - Sharifi 8.3.6.



Bezeichnung: K ein beliebiger Körper.

K^{alg} bezeichnet einen algebraischen Abschluss

$\underline{K^{sep}} \subseteq K^{alg}$ bezeichnet einen separablen Abschluss ($K^{sep} = \{x \in K^{alg} \mid K(x) \text{ separabel}\}$)
ist galoissch über K

$\rightsquigarrow G_K := \text{Gal}(K^{sep} \mid K)$ die absolute Galoisgruppe von K

$(\text{Aut}_K(K^{alg})) \longrightarrow G_K$ ist ein Isomorphismus
 $\delta \mapsto \delta|_{K^{sep}}$

$$11 \quad \text{Bsp. } \cdot \quad G_{\mathbb{F}_q} = \hat{\mathbb{Z}} \quad (\mathbb{F}_q \text{ perfekt} \Rightarrow \mathbb{F}_q^{\text{ab}} = \mathbb{F}_q^{\text{sep}})$$

$$\mathbb{F}_{q^n} = \{ \alpha \in \mathbb{F}_q^{\text{ab}} \mid \alpha^{q^n} = \alpha \} \quad | \quad \mathbb{F}_q \text{ galoissch mit } \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$$

$$(d_p: \alpha \mapsto \alpha^q) \quad \leftrightarrow 1$$

$$\text{und } \mathbb{F}_q^{\text{ab}} = \bigcup_n \mathbb{F}_{q^n} \quad \Rightarrow \quad G_{\mathbb{F}_q} = \varprojlim_{(n,1)} \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$$

$$\circ \quad \zeta_n := e^{\frac{2\pi i}{n}} \in \mathbb{C} \quad \Rightarrow \quad \mathbb{Q}_p(\zeta_{p^\infty}) := \bigcup_{n \in \mathbb{N}} \mathbb{Q}_p(\zeta_{p^n})$$

$$\Rightarrow \text{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) = \varprojlim \text{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) = \varprojlim (\mathbb{Z}_{p^n})^\times$$

$$= \mathbb{Z}_p^\times$$

$(\zeta_n \in K^{\text{alg}}$ primitive n -te EW sofern $\text{char } K \nmid n$ und falls n/n' ($\text{char } K \nmid n'$)
wählen $\zeta_n = (\zeta_{n'})$)

Bezeichnung: $G_{\mathbb{Q}_p} \xrightarrow{\text{kannische Projektion}} \text{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \xrightarrow{\text{obige isom.}} \mathbb{Z}_p^\times$
heißt p -adischer Kreistilingscharakter.

Analog: $\tilde{\mathbb{Q}} = \bigcup_n \mathbb{Q}(\zeta_n)$ (alle n) wissen $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \prod_{p \mid pZ} \text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$

$$\text{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}) \cong \varprojlim \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \prod_{p \mid pZ} \text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = \prod_p \mathbb{Z}_p^\times = (\hat{\mathbb{Z}})^\times$$

Satz (Kronecker-Weber)

$$\tilde{\mathbb{Q}} = \mathbb{Q}^{\text{ab}} \text{ wobei } K^{\text{ab}} = \bigcup \{ E \mid K \text{ galoissch} \mid \text{Gal}(E/K) \text{ abelsch} \}$$

$$\tilde{\mathcal{U}}: \text{Gal}(K^{\text{ab}}/K) \cong G_K^{\text{ab}} = \frac{G_K}{[\overline{G_K}, \overline{G_K}]}$$

Bemerkung: $G_{\mathbb{Q}_p}$ für $p > 2$ ist beschrieben durch Koch-Jansen-Wingberg. (~ 1985)
 $(\widehat{G}_K^p, K \text{ lokal: } \sim 1967)$

O3. WEITERE EIGENSCHAFTEN LOKALER KÖRPER

Sei K ein nicht-archimedischer lokaler Körper. Sei $\mathcal{O} = \mathcal{O}_K$ Bewertungsring, $\nu = \nu_K : K^\times \rightarrow \mathbb{Z}$ normalisierte Bewertung.

$k := k_K$ (endl.!) Restklassenkörper, $\pi \in \mathcal{O}$ Primelement (Uniformisator von K)

$p = \text{char } k$, $q = \#k$, $f = [k : \mathbb{F}_p]$, $e := \begin{cases} e(K/\mathbb{Q}_p), & K \nmid \mathbb{Q}_p \\ 0, & \text{sonst} \end{cases}$

A. Die multiplikative Gruppe von K

Def. 3.1. Für $i \in \mathbb{N}_0$ sei $U_i := U_i(K)$ definiert als $U_0 := \mathcal{O}^\times$, $U_i = 1 + \pi^i \mathcal{O}$ für $i \geq 1$.

Sei $P^{(p)}(K) = \{\gamma \in K^\times \mid \exists n \in \mathbb{N} : \gamma^n = 1 \text{ und } p \nmid n\} \subseteq \mathcal{O}^\times$ endliche Untergruppe

Lemma 3.2. $P^{(p)}(K) \rightarrow k^\times, \gamma \mapsto \gamma \bmod \pi$ ist Gruppeniso. (ii)

Proposition 3.3. Die kanonische Abbildung $\pi^\mathbb{Z} \times P^{(p)}(K) \times U_1 \rightarrow K^\times$ ist ein topologischer Isomorphismus
(ANT I, topologisch: ii)

Lemma 3.4. Viein $\frac{U_i}{U_{i+1}} \xrightarrow{\sim} (\mathbb{Z}, +)$, $1 + a\pi^i \mapsto a \bmod \pi$ ist Gruppenisomorphismus.

Beweis. $(1 + a\pi^i)(1 + b\pi^i) = 1 + (a + b(1 + \pi^{i-1}a))\pi^i \quad (i \geq 1)$
 $\in (1 + (ab)\pi^i)U_{i+1}$

$\Rightarrow U_i \xrightarrow{\sim} (\mathbb{Z}, +)$, $1 + a\pi^i \mapsto a \bmod \pi$ ist Gruppenhomomorphismus
mit Kern U_{i+1} . □

Korollar 3.5. Viein $\frac{U_i}{U_j} \xrightarrow{\sim} \varprojlim_{j \geq i} \frac{U_i}{U_j}$ ($\neg U_i$ ist pro-p Gruppe)

Beweis.

injektiv: ✓

surjektiv: Sei $\bar{x}_j \in \frac{U_i}{U_j}$ kompatible Familie. Wähle $x_j \in U_i$ mit Reduktion \bar{x}_j .

$\Rightarrow (x_j)_j$ bilden CF in $\mathcal{O}^\times \leq \mathcal{O}$ $\xrightarrow{\mathcal{O} \text{ kpt.}} x := \lim_{U_i \text{ kpt.}} x_j$ existiert in U_i .
(\mathcal{O} kpt. !)

$\Rightarrow x \mapsto (\bar{x}_j)_j$. □

13

Lemma 3.6. Sei K p -adisch, $i \geq 1$. Dann:

- (0) $(1 + \pi^i a)^p \equiv 1 + p\pi^i a + \pi^{pi} a^p \pmod{\pi^{e+2i}}$ (0) $e = e(K/\mathbb{Q}_p)$
 $= v_K(p)$
- (1) $(1 + \pi^i a)^p \equiv 1 + a^p \pi^{ip} \pmod{\pi^{ip+1}}$, falls $i < \frac{e}{p-1}$ ($p \leq \pi^e$)
- (2) $(1 + \pi^i a)^p \equiv 1 + p\pi^i a \pmod{\pi^{ite+1}}$, falls $i > \frac{e}{p-1}$
- (3) $(1 + \pi^i a)^p \equiv 1 \pmod{\pi^{ite}}$, falls $i = \frac{e}{p-1}$

Beweis. (0): Binomischer Lehrsatz und $p \mid \binom{p}{j}$ für $j=1-p-1$

$$\text{und } v(\pi^{2i} p) = 2i + e$$

$$(1) - (3): v(p\pi^i) > v(\pi^{pi}) \Leftrightarrow e+i > pi \Leftrightarrow \frac{e}{p-1} > i, \text{ etc.}$$

■

Korollar 3.7. Sei K p -adisch. $\mathcal{O}^\times \xrightarrow{\varphi} \mathcal{O}^\times$, $a \mapsto a^p$. Dann gilt:

$$(1) \forall i > \frac{e}{p-1}: \forall k \geq 1: \varphi \text{ induziert Isomorphismus } \frac{\mathcal{U}_i}{\mathcal{U}_{i+k}} \xrightarrow{\sim} \frac{\mathcal{U}_{ite}}{\mathcal{U}_{ite+k}}$$

$$(2) \forall i > \frac{e}{p-1}: \varphi \text{ induziert Isomorphismus } \mathcal{U}_i \xrightarrow{\sim} \mathcal{U}_{ite}$$

Beweis.

$$(1) \underline{k=1}: \frac{\mathcal{U}_i}{\mathcal{U}_{i+1}} \xrightarrow{\sim} \frac{\mathcal{U}_{ite}}{\mathcal{U}_{ite+1}}, \quad (1 + a\pi^i) \mathcal{U}_{i+1} \xrightarrow[\text{3.6.}]{} (1 + pa\pi^i) \mathcal{U}_{ite+1}$$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ (k,+)_1 & \xrightarrow{\sim} & (k,+)_2 \\ (k,+)_1 & & a \pmod{\pi} \\ & & a \cdot \frac{p}{\pi^e} \pmod{\pi} \\ & & \text{Einheit} \end{array}$$

(aus 3.6. Isomorphismus!)

Induktion:

$$\begin{array}{ccccccc} 1 & \xrightarrow{\sim} & \frac{\mathcal{U}_i}{\mathcal{U}_{i+k+1}} & \xrightarrow{\sim} & \frac{\mathcal{U}_i}{\mathcal{U}_{i+k+1}} & \xrightarrow{\sim} & \frac{\mathcal{U}_{ite}}{\mathcal{U}_{ite+k+1}} \xrightarrow{\sim} 1 \\ \text{IV} \downarrow \simeq & & \text{II} & & \text{II} & & \text{IV} \downarrow \simeq \\ 1 & \xrightarrow{\sim} & \frac{\mathcal{U}_{ite+1}}{\mathcal{U}_{ite+k+1}} & \xrightarrow{\sim} & \frac{\mathcal{U}_{ite}}{\mathcal{U}_{ite+k+1}} & \xrightarrow{\sim} & \frac{\mathcal{U}_{ite+k}}{\mathcal{U}_{ite+k+1}} \xrightarrow{\sim} 1 \end{array}$$

 \simeq : Schlangenlemma.

$$(2) \text{ verwendet } \frac{\mathcal{U}_i}{\mathcal{U}_e} \xrightarrow{\sim} \varprojlim_{j \geq i} \frac{\mathcal{U}_i}{\mathcal{U}_j}, \quad \frac{\mathcal{U}_e}{\mathcal{U}_{ite}} \xrightarrow{\sim} \varprojlim_{j \geq i} \frac{\mathcal{U}_e}{\mathcal{U}_j} \simeq \varphi \pmod{\dots} \text{ rechts Isomorphismus wegen (a).}$$

■

(2) alternativ:

$$\begin{array}{ccc} \underbrace{(1 + \pi^i U_i)}_{= U_i} & \xrightarrow[\text{exp}]{} & (\pi^i U, +) \\ \downarrow \gamma & \approx & \downarrow p - \text{ist Isomorphismus} \\ (U_{\text{inte}}, -) & \xleftarrow[\text{exp}]{} & (\pi^{i+\epsilon} U, +) \end{array}$$

□

Satz 3.8. K sei p -adischer Körper. Dann:

27.04.18

(1) $U_1(K) \cong \mu_{p^\infty}(K) \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ als topologische Gruppen.

(2) $K^\times \cong \pi^\mathbb{Z} \times \mu^{(p)}(K) \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ als topologische Gruppen.

Beweis:

$\cdot \mu_{p^\infty}(K) = \{\zeta \in K^\times \mid \exists n > 0: \zeta^{p^n} = 1\}$

$\cdot \#\mu_{p^\infty}(K) < \infty: [K:\mathbb{Q}_p] < \infty \text{ und } [\mathbb{Q}_p(\zeta_{p^n}) : \mathbb{Q}_p] = \phi(p^n)$
 $p^{n-1}(p-1) \xrightarrow{n \rightarrow \infty} 0$

Bemerkung: • $U_1(K)$ ist abelsche pro- p -Gruppe, d.h. \mathbb{Z}_p -Modul

• $U_1(K)_{\text{tors}} \cong \mu_{p^\infty}(K) \quad \text{und} \quad U_1(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_p^{[K:\mathbb{Q}_p]}$

Beweis. (2) folgt aus (1) und 3.3.

(1) $U_1(K)$ ist abelsche pro- p -Gruppe.

$U_1(K)_{\text{tors}} = \{x \in U_1(K) \mid \exists n \in \mathbb{N}: x^{p^n} = 1\} = \mu_{p^\infty}(K) (< \infty)$

Beh. $U_1(K)$ topol. endl. erz. $\begin{cases} \Rightarrow U_1(K) \text{ endl. erz. } \mathbb{Z}_p\text{-Modul} \\ \Rightarrow U_1(K) \cong U_1(K)_{\text{tors}} \times \mathbb{Z}_p^n \text{ für ein } n \in \mathbb{N}_0 \end{cases}$ Dazu: (Burnside Basisatz) z.B. $U_1(K)/U_1(K)^p$ endlich

dazu: $U_1(K)^p \cong U_{i_0}(K)^p \stackrel{\exists i_0}{=} U_{i_0+\epsilon}(K) \quad \text{für } i_0 = \lceil \frac{e}{p-1} \rceil$

 $\Rightarrow U_1(K)/U_1(K)^p$ ist Quotient von $U_1(K)/U_{i_0+\epsilon}(K)$ ← endliche p -Gruppe
 \Rightarrow Behauptung gezeigt. $(U_i/U_{i+1} \cong (k, +) \text{ endl.})$ Behauptung: $r = [K:\mathbb{Q}_p] \quad U_1/U_i \text{ endl. } \forall i \geq 1$

$\Rightarrow \text{rang}_{\mathbb{Z}_p} U_1 = \text{rang}_{\mathbb{Z}_p} U_{i_0}$

wegen $\log, \exp: U_{i_0} \xrightarrow{\sim} \pi^{i_0} \mathcal{O}_K$ als \mathbb{Z}_p -Modul (als pro- p -Gruppe)

$$\text{rang}_{\mathbb{Z}_p} \mathcal{O}_K = \text{rang}_{\mathbb{Q}_p} \mathcal{O}_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \dim_{\mathbb{Q}_p} K = [K : \mathbb{Q}_p]$$

Alternativ: U_{i_0} ist p -torsionsfrei, denn $x \mapsto x^p$ ist Isomorphismus $U_{i_0} \rightarrow U_{i_0+e}$
 $\Rightarrow U_{i_0}$ ist freier \mathbb{Z}_p -Modul (von endl. Rang)

$$\begin{aligned} \xrightarrow{\text{Nakayama}} \text{rang}_{\mathbb{Z}_p} U_{i_0} &= \text{rang}_{\mathbb{F}_p} \frac{U_{i_0}}{U_{i_0}^p} = \text{rang}_{\mathbb{F}_p} \frac{U_{i_0}}{U_{i_0+e}} = \log_p (\# \frac{U_{i_0}}{U_{i_0+e}}) \\ &= \log_p (\underbrace{(\# k)}_{= p^e}) = ef = [K : \mathbb{Q}_p] \end{aligned}$$

□

Satz 3.9. (ohne Beweis, s.ü.)

Für $K \cong \mathbb{F}_q((\pi))$ gilt $U_1(K) \cong \mathbb{Z}_p^{\mathbb{N}}$

Abb: $\mathbb{Z}_p^{\mathbb{N}} \rightarrow U_1$: Sei b_1, \dots, b_f Basis von k über \mathbb{F}_p .

Behauptung: $\prod_{\substack{n \in \mathbb{N} \\ p \nmid n}} \prod_{j=1}^f \mathbb{Z}_p \rightarrow U_1(K), (a_{n,j})_{n,j} \mapsto \prod_{n,j} (1 + b_j \pi^n)^{a_{n,j}}$

□

B. Zähm verzweigte Erweiterungen (ζ_n primitive n -te EW)

Proposition 3.10. $L|K$ lokale Körper, $n \in \mathbb{N}$ mit $p \nmid n$.

(a) $K(\zeta_n)$ ist unverzweigt über K

(b) Für $m := \# k_L^\times$ gilt $K(\zeta_m) \subseteq L$ und $K(\zeta_m)$ ist größte unverzweigte Erweiterung von K in L . ($\Rightarrow L|K(\zeta_m)$ ist total verzweigt)

(c) Zu $e \in \mathbb{N}$ $\exists!$ unverzweigte Erweiterung K_e von K mit $[K_e : K] = e$, nämlich $K = K(\zeta_{q^{e-1}})$, $K_e|K$ ist galoissch und

$$\text{Gal}(K_e|K) \xrightarrow{\sim} \text{Gal}(k(\zeta_{q^{e-1}})/k) \cong \mathbb{Z}/e\mathbb{Z}$$

Beweis. (vgl. ANT I)

(a) Man betrachtet $X^m - 1$ ($p \nmid m$ und wandelt Hensels Lemma an. $\Rightarrow [K(\zeta_n) : K] = [k(\zeta_n) : k]$)
 $\Rightarrow f(K(\zeta_n)|K) = [K(\zeta_n) : K]$

(Hensel: $\text{d}_{\text{H}} \text{mipo}_K \zeta_m = \text{d}_{\text{H}} \text{mipo}_k \zeta_m$). Hensel zeigt auch $K(\zeta_m) \subseteq L$ und $k_L = k_K(\zeta_m)$
 $(\Rightarrow L|K(\zeta_m) \text{ voll verzweigt}) \Rightarrow (a), (b), (c)$.

Hatten in ANT I gezeigt. \exists kanonische Surjektion $\rho_{L|K}: \text{Gal}(L|K) \rightarrow \text{Gal}(k_L|k)$ falls $L|K$ galoissch.

□

Für $L|K$ algebraisch ($L \subseteq K^{\text{alg}}$, $K \subseteq L$) sei

$$\mathcal{F}_{L|K} := \{F \subseteq L \mid F|K \text{ endl. Körpererweiterung}\}$$

Def. 3.11.

- (1) $L|K$ heißt unverzweigt: \Leftrightarrow alle $F \in \mathcal{F}_{L|K}$ sind unverzweigt über K .
- (2) $L|K$ heißt total verzweigt: \Leftrightarrow alle $F \in \mathcal{F}_{L|K}$ sind total verzweigt über K .
- (3) $K^{\text{ur}} := \bigcup \{F \in \mathcal{F}_{K^{\text{sep}}|K} \mid F|K \text{ unverzweigt}\}$ ($= \varprojlim \dots$)

(die max. unverzweigte Erweiterung von K (in K^{alg}))

- (4) Für $F \subseteq F'$ in $\mathcal{F}_{L|K}$ haben kanonische Inklusionen $k_F \hookrightarrow k_{F'}$

Sei $k_L = \bigcup \{k_F \mid F \in \mathcal{F}_{L|K}\}$ ($= \varprojlim \dots$)

(Bem.: $k_L \xleftarrow{\sim} \mathcal{O}_L/\mathfrak{m}_L$; Bewertung auf K setzt sich endl. auf L fort)

Bem. (a) $K^{\text{ur}} = \bigcup_m K(\zeta_{q^{m-1}})$ ($= \varinjlim \dots$)

(b) $K^{\text{ur}} \cap L$ für tel. L ist die maximale unverzweigte Erweiterung von K in L .

Def. 3.12. $L|K$ galoissch.

(i) Erhalten kanonischen Homomorphismus $\rho_{L|K}: \text{Gal}(L|K) \rightarrow \text{Gal}(k_L|k)$

(als $\varprojlim \rho_{E|K}: \varprojlim_{\substack{E \in \mathcal{F}_{L|K} \\ E|K \text{ galoissch}}} (\text{Gal}(E|K) \rightarrow \text{Gal}(k_E|k))$)

(ii) $I_{L|K} := \ker(\rho_{L|K})$, $I_K := I_{K^{\text{sep}}|K}$

(iii) Haben $\sigma: k_L \rightarrow k_L$, $x \mapsto x^q$ in $\text{Gal}(k_L|k)$ (topol. Erz.) $q = \# k$
Neue $F_r \in \text{Gal}(L|K)$ ein Frobeniusautomorphismus: $\Leftrightarrow \rho_{L|K}(F_r) = \sigma$

Bem. (1) Haben "wieder" kurze exakte Sequenzen $1 \rightarrow I_{K|L} \rightarrow \text{Gal}(L|K) \xrightarrow{\rho_{L|K}} \text{Gal}(k_L|k) \rightarrow 1$
als inverser Limes analoger Sequenzen für $E \in \mathcal{F}_{L|K}$ mit $E|K$ galoissch.

(2) F_r ist eindimensional $\Leftrightarrow \rho_{L|K}$ ist Isomorphismus $\Leftrightarrow L|K$ ist unverzweigt (d.h. $I_{L|K} = \{1\}$)

Für $L = K^{\text{ur}}$: $\text{Gal}(K^{\text{ur}}|K) \xrightarrow{\sim} \text{Gal}(k^{\text{alg}}|k) \cong \hat{\mathbb{Z}}$.

17

- Def. 3.13. (a) Gilt $[L:K] < \infty$, so heißt $L|K$ zähm verzweigt $\Leftrightarrow p \nmid e(L|K)$
- (b) $L|K$ heißt zähm verzweigt \Leftrightarrow alle $F \in \mathcal{F}_{L|K}$ sind zähm verzweigt über K
- (c) $L|K$ heißt wild verzweigt $\Leftrightarrow L|K$ ist nicht zähm verzweigt.
($p \mid e(F|K)$ für ein $F \in \mathcal{F}_{L|K}$)

- Bsp. (a) $e \in \mathbb{Z}_{\geq 2}$ mit $p \nmid e \Rightarrow L = K(\sqrt[p]{\pi})$ zähm verzweigt (und total unverzweigt)
- (b) $p = \text{char } k$, $L|K$ inseparabel $\rightarrow L|K$ wild verzweigt
- (c) $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$ zähm, total verzweigt. ($e = \phi(p) = p-1$)
 $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ wild verzweigt für $n \geq 2$ ($e = \phi(p^n)$)

Proposition 3.14. Sei $L|K$ zähm verzweigt, $[L:K] < \infty$, $E = L \cap K^{\text{ur}}$, $e = e(L|K)$. Dann:

- (a) $L = E(\sqrt[p]{\pi_E})$ für π_E geeignetes Primideal von E .
- (b) $E' := E(\zeta_{e \cdot \# k_E^\times})$, $L' := LE' \Rightarrow L' = E'(\sqrt[p]{\frac{\pi}{\pi_K}})$
und $E'|K$ unverzweigt, $L'|L$ unverzweigt $\rightarrow (L'|K)$ galoissch

Beweis.

$$(a) \text{ Sei } \pi_L \text{ Primideal von } \mathcal{O}_L \Rightarrow \pi \mathcal{O}_L = \pi_L^e \mathcal{O}_L, \text{ d.h. } \alpha \in \mathcal{O}_L^\times : \pi = \pi_L^e \alpha$$

wissen $\mathcal{O}_L^\times = \mu^{(p)}(L) \times U_1(L)$ { $U_1(L)$ ist (endl. ord.) \mathbb{Z}_p -Modul, $e \in \mathbb{Z}_p^\times$
 $\Rightarrow \alpha = \zeta \cdot u \quad \} \Rightarrow \exists u' \in U_1(L) : (u')^e = u$.

$$\Rightarrow \zeta^{-\pi} = (\pi_L \cdot u')^e$$

beachte: $\mu^{(p)}(L) = \mu^{(p)}(E)$ da $k_L = k_E$ } $\Rightarrow \pi_E := \zeta^{-\pi} \text{ Primideal von } \mathcal{O}_E \text{ und}$
 $L = E(\sqrt[p]{\pi_E})$

(denn: $L = E(\pi_L)$, da $[L:E] = e(L|E) = e(L|K) = e$)

- (b) wähle $\zeta \in \mu^{(p)}(E)$ mit $\zeta^e = \zeta$ ($\zeta^{\# k_E^\times} = 1$)
Dann: $\pi = (\pi_L \cdot u' \zeta)^e \Rightarrow L' = E'(\sqrt[p]{\pi})$.

■

Bsp. (ii) $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p]{\pi})$ für geeigneten Uniformisator in \mathbb{Q}_p .
Bch.: $\pi = -p$ tut's!

Def. G pro-endlich abelsch. $\Rightarrow G$ ist $\hat{\mathbb{Z}}$ -Modul.

Modulstruktur: $\hat{\mathbb{Z}} \times G \longrightarrow G, (\alpha, g) \mapsto \underbrace{\alpha \cdot g}_{\mathbb{Z}}$

$$n \in \mathbb{Z} \Rightarrow n \cdot g := g^n$$

Für $\hat{\alpha} \in \hat{\mathbb{Z}}$ beliebig: schreibe $\hat{\alpha} = (\alpha_n)_n \in \varprojlim_n (\mathbb{Z}/n\mathbb{Z})$ ($\alpha_n \in \mathbb{Z}$)

prüfe: (g^{α_n}) "konvergieren" ((g^{α_n}) hat endl. Häufungspunkt!)

Proposition 3.15:

- (a) Sind L, L' zahm verzweigt über K , so auch LL' ($\Rightarrow 3$ größte zahm verzwe. Erw. K^{tr} von L)
- (b) Die maximal zahm verzweigte Erweiterung von K in K^{alg} ist in K^{sep}

$$K^{tr} = \bigcup_{p \nmid n} K^{ur}(\sqrt[n]{\pi})$$

(c) K^{tr}/K^{ur} ist galoissch und $\text{Gal}(K^{tr}/K^{ur}) \cong \overline{\prod_{\substack{\ell \mid p \\ \ell \text{ prim}}} \mathbb{Z}_\ell} =: \hat{\mathbb{Z}}^{(p)}$

(d) K^{tr}/K ist galoissch mit $\text{Gal}(K^{tr}/K) \cong \hat{\mathbb{Z}}^{(p)} \rtimes \hat{\mathbb{Z}}$ so dass für geeignete topologische Erzeuger $t \in \hat{\mathbb{Z}}^{(p)}$ und $s \in \hat{\mathbb{Z}}$ gilt:

$$sts^{-1} = t^q \quad (q = \# h)$$

Beweis.

- (a) Für $L, L' | K$ endl: $e(LL'/K) \mid e(L|K) e(L'|K)$ (aus ANT 1) oder 3.14
- (b) Folgt aus 3.14 (b)
- (c) $\text{Gal}(K^{ur}(\sqrt[n]{\pi}) | K^{ur}) \cong \mathbb{Z}/n\mathbb{Z}$ (nach Kummertheorie)

$(p+n)$ Galoiskonjugatiken von $\sqrt[n]{\pi}$ seien $(\zeta_{q^{n-1}}^i \sqrt[n]{\pi})_{i=1}^n$ (Algebra I)

$$\varprojlim (\quad) = \varprojlim_{\substack{\ell \mid p \\ \ell \text{ prim}}} (\quad) \cong \hat{\mathbb{Z}}^{(p)}$$

(d) (ii) Sei $K(n) := K(\zeta_{q^{n-1}}, \sqrt[n]{\pi})$; Beh.: $K(n)|K$ galoissch mit $\text{Gal}(K(n)|K) \cong \frac{\mathbb{Z}/q^{n-1}\mathbb{Z}}{\mathbb{Z}/n\mathbb{Z}} \cong \hat{\mathbb{Z}}^{(p)}$
 und: $sts^{-1} = t^q$

$\begin{array}{ccc} \text{zähm total} & & \text{unverzweigt} \\ \text{verzweigt} & & \text{Gal}(K(n)|K) \end{array}$

04. HÖHERE VERZWEIGUNGSGRUPPEN.

Sei K ein lokaler Körper. Seien $\mathcal{O}, \pi, k = k_K, v = v_K, q$ wie in 03.

Sei $L|K$ endlich galoissch mit $G = \text{Gal}(L|K)$. Seien $\mathcal{O}_L, \pi_L, k_L, v_L$ wie für K .

(v_L normalisiert, keine Fortsetzung von v_K)

Wtg. ANT1: $\exists x \in \mathcal{O}_L$ mit $\mathcal{O}_K[x] = \mathcal{O}_L$ ($L|K$ total verzweigt $\Rightarrow \mathcal{O}_L = \mathcal{O}_K[\pi_L]$)

Lemma 4.1. Für $\sigma \in G$ und $i \in \mathbb{Z}_{\geq -1}$ sind äquivalent:

- a) σ operiert trivial auf $\mathcal{O}_L/\pi_L^{i+1}\mathcal{O}_L$
- b) $v_L(\sigma(a) - a) \geq i+1 \quad \forall a \in \mathcal{O}_L$
- c) $v_L(\sigma(x) - x) \geq 1$ für x wie oben.

Beweis.

a) \Leftrightarrow b) \Rightarrow c): klar.

$$c) \Rightarrow b): \sigma\left(\sum_{\substack{i \\ a_i \in \mathcal{O}_K}} a_i x^i\right) - \sum_i a_i x^i = (\sigma x - x) \sum_i a_i \underbrace{\frac{(\sigma x)^i - x^i}{\sigma x - x}}_{\in \mathcal{O}_L} \geq i+1$$

$$v_L(\dots) = v_L(\sigma x - x) + \underbrace{\dots}_{\geq 0} \geq i+1$$

□

Def. 4.2.

$$(i) i_{L|K}(\sigma) := v_L(\sigma x - x) \quad \forall \sigma \in G$$

(ii) Für $i \geq -1$ sei $G_i := \{\sigma \in G \mid i_{L|K}(\sigma) \geq i+1\}$ die i -te höhere Verzweigungsgruppe.

Bemerkung 4.3.

$$(0) G_i = \bigcap_{\bar{x} \in \mathcal{O}_L/\pi_L^{i+1}\mathcal{O}_L} \text{Stab}_G(\bar{x}) \Rightarrow G_i \text{ Untergruppe.}$$

$$(1) G_1 = G, \quad G_i = \{\text{id}\} \text{ für } i > 1 \quad (\sigma \neq \text{id} \Rightarrow \sigma x - x \neq 0 \dots)$$

$$G_0 = \{ \sigma \in G \mid \sigma x \equiv x \pmod{\pi} \} = I_{L|K} = \ker(G \rightarrow \text{Gal}(k_L|k_K))$$

$$(2) H \leq G \text{ Untergruppe zum Zwischenkörper } E = L^H \text{ (beachte } \mathcal{O}_L = \mathcal{O}_E[x])$$

$$\text{Dann: } H_i = H \cap G_i \quad (i_{L|E}(\sigma) = i_{L|K}(\sigma) \text{ für } \sigma \in H)$$

$$\text{z.B. } H = G_0 \Rightarrow L^H = L \cap K^{\text{ur}} \text{ und } G_i = (G_0)_i = H_i \quad \forall i \geq 0$$

(3) $i_{L/K}$ ist unabhängig von der Wahl von x (wegen 4.1)

(4) $i_{L/K} : G \rightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\}$

Lemma 4.4. Es gilt $G_i \leq G \quad \forall i \geq -1$

Beweis.

$$G_i = \ker(G \rightarrow \text{Aut}(\mathcal{O}_L/\pi^{i+1}\mathcal{O}_L)) .$$

□

Korollar 4.5. Seien $d, \tau \in G_0$. Dann gelten:

$$(i) \quad i_{L/K}(d\tau\tau^{-1}) = i_{L/K}(\tau)$$

$$(ii) \quad i_{L/K}(d\tau) \geq \min(i_{L/K}(d), i_{L/K}(\tau)) \text{ mit Gleichheit falls } i_{L/K}(d) \neq i_{L/K}(\tau).$$

Beweis. (i) wegen 4.4.

$$\begin{aligned} (ii) \quad \underbrace{v_{L/K}(d\tau x - x)}_{v_{L/K}(d\tau)} &\geq \min(\underbrace{v_{L/K}(d(\tau x) - \tau x)}_{= i_{L/K}(d)}, \underbrace{v_{L/K}(\tau x - x)}_{= i_{L/K}(\tau)}) \\ &\text{auch } \mathcal{O}_L = \mathcal{O}_K[\tau x] \\ &\text{nun 4.3 (3)} \end{aligned}$$

Gleichheitsaussage wegen "analoger" Eigenschaft von v_L .

□

Lemma 4.6. Für $d \in G_0$ und $i \geq 0$ gelten:

$$d \in G_i \iff \begin{cases} v_L(d\pi_L - \pi_L) \geq i+1 \\ (ii) \quad \frac{d\pi_L}{\pi_L} \in \mathcal{U}_i(L) \end{cases}$$

Beweis. (i) o.E.: $L|K$ voll verzweigt (ersetze K durch $K^{ur,n}L$)

dann: klar wegen Wiederholung ANT 1 + 4.3. (3).

$$\begin{aligned} (ii) \quad v_L(\pi_L) = 1 \Rightarrow \left(v_L(d\pi_L - \pi_L) \geq i+1 \iff v_L\left(\frac{d\pi_L}{\pi_L} - 1\right) \geq i \right. \\ \left. \iff \frac{d\pi_L}{\pi_L} \in \mathcal{U}_i(L) \right). \end{aligned}$$

□

1. Anwendung: $v_L(\mathcal{D}_{L/K})$?

$$\mathcal{D}_{L/K}^{-1} = \{ \alpha \in L \mid \text{Tr}_{L/K}(\alpha\beta) \in \mathcal{O}_K \quad \forall \beta \in \mathcal{O}_L \}$$

und ($\mathcal{O}_L = \mathcal{O}_K[x]$) ist $p_x \in \mathcal{O}_K[X]$ das Mipo von x , so gilt $\mathcal{D}_{L/K} = p_x^1(x) \mathcal{O}_L$.

21

$$\text{Satz 4.7. } \underline{\nu_L(\mathcal{D}_{L/K})} = \sum_{\sigma \in G \setminus \text{id}_L} i_{L/K}(\sigma) = \sum_{i=0}^{\infty} (\# G_i - 1)$$

$$= \nu_L(\mu_n^{(x)})$$

(Bem.: weiter unten: L/K zahm verzweigt $\leftrightarrow G_1 = \{1\}$

$$\Downarrow \nu_L(\mathcal{D}_{L/K}) = \# G_0 - 1 = e(L/K) - 1$$

Beweis.

$$\mu_x(X) = \prod_{\sigma \in G} (X - \sigma x) \Rightarrow \mu_x'(X) = \prod_{\sigma \in G \setminus \{1\}} (X - \sigma x)$$

$$\Rightarrow \nu_L(\mathcal{D}_{L/K}) = \sum_{\sigma \in G \setminus \{1\}} \nu_L(x - \sigma x) = \sum_{\sigma \in G \setminus \{1\}} \underbrace{i_{L/K}(\sigma)}_{\in \mathbb{Z}_{\geq 0}}.$$

$$= \sum_{i=0}^{\infty} i \left(\sum_{\substack{\sigma \in G \setminus \{1\} \\ i_{L/K}(\sigma) = i}} 1 \right) = \sum_{i=1}^{\infty} i \left(\# G_{i-1} - \underbrace{\# G_i}_{=: j_i} \right)$$

$$= \sum_{i=0}^{\infty} (\# G_i - 1)$$

Abel-
summation

$$0 \cdot (j_{-1} - j_0) + 1(j_0 - j_1) + 2(j_1 - j_2) + 3(j_2 - j_3) + \dots + n(j_{n-1} - \underbrace{j_n}_{=1}) + 0$$

$$= j_0 + j_1 + j_2 + \dots + j_{n-1} - n$$

$$= \sum_{k=0}^{n-1} (j_k - 1)$$

■

Korollar 4.8. (ii) Sei E/K endl. separable Erweiterung mit Galoisgruppe L und

$$H = \text{Gal}(L/E). \text{ Dann: } \nu_{E/K}(\mathcal{D}_{E/K}) = \frac{1}{e(L/E)} \sum_{\sigma \in G \setminus H} i_{L/K}(\sigma)$$

Die Gruppen $\frac{G_i}{G_{i+n}}$:

Lemma 4.9. $\forall i \geq 0$ ist die Abbildung $\theta_i : \frac{G_i}{G_{i+n}} \rightarrow \frac{U_i(L)}{U_{i+n}(L)}$, $\sigma G_{i+n} \mapsto \frac{\sigma(\bar{\pi}_L)}{\pi_L^{i+n}} U_{i+n}(L)$ wohldefiniert, unabhängig von $\bar{\pi}_L$ und ein injektiver Gruppenhomomorphismus.

$$\text{(Erinnerung: } \frac{U_0(L)}{U_1(L)} \cong (k_L^\times, \cdot), \quad \frac{U_i(L)}{U_{i+1}(L)} \cong (k_L, +) \cong \mathbb{F}_p^{[k_L : \mathbb{F}_p]} \\ \cong \mathbb{Z}_{(q_L - 1)})$$

Beweis: unabhängig von $\bar{\pi}_L$. Gelte $\bar{\pi}^i = u \bar{\pi}_L$ für ein $u \in \mathcal{O}_L^\times$.

$$\begin{aligned} 4.1 \Rightarrow \forall u \in U_i & \quad \bar{c}u \equiv u \pmod{\bar{\pi}_L^{i+1}}, \text{ d.h. } \frac{\bar{c}u}{u} \equiv 1 \pmod{\bar{\pi}_L^{i+1}} \\ \Rightarrow \frac{\bar{c}\bar{\pi}^i}{\bar{\pi}^i} &= \frac{\bar{c}u}{u} \quad \frac{\bar{c}\bar{\pi}_L}{\bar{\pi}_L} \equiv \frac{\bar{c}\bar{\pi}_L}{\bar{\pi}_L} \pmod{U_{i+1}(L)} \end{aligned}$$

$\tilde{\theta}_i: G_i \rightarrow \frac{U_i(L)}{U_{i+1}(L)}, c \mapsto \frac{c(\bar{\pi}_L)}{\bar{\pi}_L} \pmod{U_{i+1}(L)}$ ist wohldef. Gruppenhomomorphismus.

$$\frac{c\bar{\pi}_L}{\bar{\pi}_L} \underset{4.6}{\in} U_i(L) \Rightarrow \text{wohldefiniert.} \quad \text{unabh. von } \bar{\pi}_L$$

$$\text{Homomorphismus: } \tilde{\theta}_i(c\tau) = \frac{c\tau(\bar{\pi}_L)}{\bar{\pi}_L} = \frac{c(\tau\bar{\pi}_L)}{\tau\bar{\pi}_L} \cdot \frac{\tau(\bar{\pi}_L)}{\bar{\pi}_L} \stackrel{!}{=} \frac{c\bar{\pi}_L}{\bar{\pi}_L} \cdot \frac{\tau\bar{\pi}_L}{\bar{\pi}_L}$$

$$U_L(\tau\bar{\pi}_L) = 1$$

inj., wohldefiniert:

$$\ker \tilde{\theta}_i = G_{i+1} \text{ nach Lemma 4.6.} \quad \square$$

Korollar 4.10. (i) $\frac{G_0}{G_1}$ ist endl. zykl. Grp. von Ordnung teilerfremd zu p.

(ii) G_1 ist eine p-Gruppe

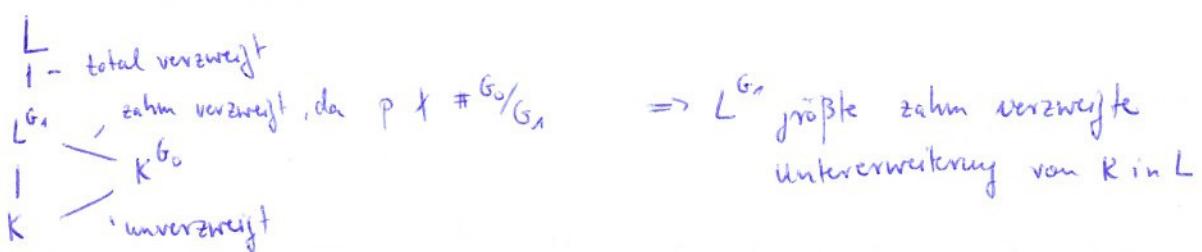
(iii) L^{G_1} ist der max. zahm verzweigte Unterkörper von L über K

(iv) G ist auflösbar. (sogen "überauflösbar")

Beweis. (i), (ii): klar nach 4.9.

(iv): benötigt zusätzlich: $\text{Gal}(k_L/k)$ auflösbar ist.

(iii)



$\Rightarrow L^{G_1}$ größte zahm verzweigte

Untererweiterung von K in L

$$\text{Ü: } G_0 \cong G_n \rtimes \frac{G_0}{G_n} \quad (\text{Schur-Zassenhaus, ... licher elementar})$$

Def. 4.11. $G_n \trianglelefteq G$ heißt wilde Verzweigungsgruppe von G .

Bsp 4.12. (ü) Sei $L_i = \mathbb{Q}_p(\zeta_{p^i})$ $i \geq 0$

$$\text{Gal}(L_n/\mathbb{Q}_p)_i = \begin{cases} G, & -1 \leq i \leq 0 \\ \text{Gal}(L_n/L_k), & p^{k-1} \leq i \leq p^k - 1 \quad k \in \{1, \dots, n-1\} \\ \{1\}, & i \geq p^{n-1} \end{cases}$$

Bemerkung 4.13 (siche Serre) $\sigma \in G_i, \tau \in G_j, i, j \geq 1$
 $\Rightarrow \sigma \tau \sigma^{-1} \tau^{-1} \in G_{i+j+1}$

Der Satz von Herbrand.

Für $u \in \mathbb{R}_{\geq -1}$ setze $G_u := G_{\lceil u \rceil}$

$(G \in G_u \iff i_{\text{LIK}}(G) \geq u+1)$

Def. 4.14. (Herbrand Funktion)

$$\phi = \phi_{\text{LIK}}: [-1, \infty) \rightarrow [-1, \infty), \quad t \mapsto \int_{s=0}^t \frac{1}{[G_0 : G_s]} ds$$

beachte: $s \mapsto [G_0 : G_s]^{-1}$ ist monoton wachsend in s und $\frac{1}{[G_0 : G_s]} \geq \frac{1}{\# G_0}$

Prop. 4.15. (ü)

- (i) ϕ ist stetig, stückweise linear (auf $(i, i+1)$) streng monoton wachsend und konkav.
- (ii) $\phi(0) = 0$, Steigung 1 auf $-1 \leq t \leq 0$
- (iii) Für $u \in \mathbb{R}_{\geq 1} \setminus \mathbb{Z}$: $\phi'(u) = \frac{1}{[G_0 : G_u]} \geq \frac{1}{\# G_0}$
- (iv) $\phi: [-1, \infty) \rightarrow [-1, \infty)$ ist bijektiv.

Sei $\psi = \psi_{\text{LIK}} = \phi^{-1}: [-1, \infty) \rightarrow [-1, \infty)$

Korollar 4.16. (ü) (i) ψ ist stetig, stückweise linear, streng monoton wachsend, konkav

(ii), (iv) wie für ϕ

(iii) Sei $v = \phi(u), u \notin \mathbb{Z} \Rightarrow \psi'(v) = [G_0 : G_u] (\in \mathbb{N})$ | (v) $u \in \mathbb{Z}_{\geq 1} \Rightarrow u = \psi(v) \in \mathbb{Z}_{\geq 1}$.

Beweis.

(v) OE $v \geq 1$. ($v=0, v=-1$ klar wegen \hat{u}) $\exists i: i \leq v \leq i+1$

$$\Rightarrow \underbrace{\#G_v}_{{N=\phi(v)}} v = \underbrace{\#G_1}_{[0,1]} + \underbrace{\#G_2}_{[1,2]} + \dots + \underbrace{\#G_i}_{[i-1,i]}$$

teile durch
 $\#G_{i+1}$

$$[G_v : G_u] = \frac{\#G_v}{\#G_u}$$

$$\Rightarrow u - i \in \mathbb{Z} \Rightarrow u = i.$$

□

Def. 4.17. $G^v := G_{\psi(v)}$ (Verzweigungsgruppen in ehrer Nummerierung!)Satz 4.18. (Herbrand) Für $N \trianglelefteq G$ Normalteiler gilt:

$$\left(\frac{G}{N}\right)^v = G^v N / N. \quad \forall v \in \mathbb{R}_{\geq -1}$$

08.05.18

Bem. zu 4.17.

- i) $G^v = \{1\}$ für $v > 0$
- ii) $G^v = G_v$ ($\psi(0)=0$); $G^{-1}=G$
- iii) $\hat{u}: \psi(v) = \int_{w=0}^v [G^w, G^w] dw$

Übung: Die Abbildung $\phi = \phi_{\mathbb{Q}_p(\mathbb{F}_{p^n})/\mathbb{Q}_p}$ (mit Inverser ψ) erfüllt:

$$\phi'(t) = \begin{cases} 1, & -1 < t < 0 \\ \frac{1}{p^k - p^{k-1}}, & p^{k-1} - 1 < t < p^k - 1 \quad 1 \leq k \leq n-1 \\ \frac{1}{p^n - p^{n-1}}, & p^{n-1} - 1 < t \end{cases}$$

$$\psi'(t) = \begin{cases} 1, & -1 < t < 0 \\ p^k - p^{k-1}, & k-1 < t < k \quad 1 \leq k \leq n-1 \\ p^n - p^{n-1}, & n-1 < t \end{cases}$$

(Sprünge der Steigung von ψ an $\{0, \dots, n-1\}$)

Proposition 4.19. Gelede $N \leq G$ und sei $E = L^N$. Dann ist

$$\Psi_{EK} = \Psi_{EIK} \circ \Psi_{LIE} \quad \text{und} \quad \Psi_{LK} = \Psi_{EIK} \circ \Psi_{LIE}$$

Lemma 4.20. Für $N \leq G$ und $E = L^N$ gilt:

$$\forall \delta \in \text{Gal}(E/K) : i_{EIK}(\delta) = \frac{1}{e(LIE)} \sum_{\substack{g \in G \\ g|_E = \delta}} i_{LIE}(g)$$

$$G \begin{pmatrix} L \\ | \\ N \\ E \\ | \\ G/N \\ K \end{pmatrix}$$

Beweis. (Teile)

- Falls $\delta = \text{id}$: $\infty = \infty$.

- Falls $\delta \neq \text{id}$: Wähle $x \in \mathcal{O}_L$, $y \in \mathcal{O}_E$ mit $\mathcal{O}_K[x] = \mathcal{O}_L$, $\mathcal{O}_K[y] = \mathcal{O}_E$. Wähle $\tau \in G$ mit $\tau|_E = \delta \Rightarrow \{g \in G \mid g|_E = \delta\} = \tau \cdot N = N \cdot \tau$.

Beachte:

$$e(LIE) \cdot i_{EIK}(\delta) = v_L(\tau y - y)$$

$$i_{LIE}(g) = v_L(gx - x)$$

Behauptung: $a = \tau y - y$ und $b = \prod_{g \in N} (\tau g x - x)$ sind assoziiert in \mathcal{O}_L .

$a \mid b$: Sei $f \in E[X]$ das Minimalpolynom von x über E .

$$f(X) = \prod_{g \in N} (X - g x) = X^{\#N} + \sum_{i=0}^{\#N-1} b_i X^i \quad \text{mit } b_i \in \mathcal{O}_E \text{ da } x \text{ ganz über } \mathcal{O}_E.$$

$$\tau f - f = \sum_{i=0}^{\#N-1} \underbrace{(\tau b_i - b_i)}_{\tau b_i = \delta b_i} X^i$$

$$v_E(\tau f - f) \geq i_{EIK}(\delta) \quad (\tau b_i = \delta b_i)$$

$a \text{ teilt}$
 \Rightarrow
Koeffizienten von f

$$a \mid (\tau f - f)(x) = (\tau f)(x) = \prod_{g \in N} (x - \tau g x) = \pm b$$

$b \mid a$: Schreibe $y = g(x)$ für ein $g \in \mathcal{O}_K[X]$.

$\Rightarrow g(x) - y \in \mathcal{O}_E(X)$ und das Polynom hat x als Nullstelle.

$\Rightarrow g(x) - y = \underbrace{f(x) \cdot h(x)}_{\text{normiert}}$ für ein $h \in \mathcal{O}_E[X]$.

Wende τ_g an; anschließend x einsetzen. (beachte $\tau_g = g$)

$$\begin{aligned} \Rightarrow a &= y - \tau_g y = (\tau_f)(x) - (\tau_h)(x) \\ &= \pm b \cdot (\tau_h)(x) \end{aligned}$$

also gilt $b \mid a$.

■

Korollar 4.21. (s. Sure, Local Fields) Sei $N = G_j$ für ein $j \geq 0$. Dann:

$$(a) \quad (\mathbb{G}/N)_i = \frac{G_i}{N} \quad \text{für } i < j \quad (b) \quad (\mathbb{G}/N)_i = \{1\} \quad \text{für } i \geq j$$

Beweis. Übung.

■

Lemma 4.22. Für $t \geq -1$ gilt:

$$\phi_{L/K}(t) + 1 = \frac{1}{\# G_0} \sum_{g \in G} \min(i_{L/K}(g), t+1)$$

Beweis. Beide Seiten sind 1 an $t=0$, $(i_{L/K}(g)=0 \text{ für } g \in G \setminus G_0, \geq 1 \text{ für } g \in G_0)$
stückweise linear für $t \in [i, i+1]$ und stetig. Sei $t \in \mathbb{R}_{\geq -1} \setminus \mathbb{Z}$:

$$\phi_{L/K}^i(t) = \frac{1}{[G_0 : G_{i+1}]} = \frac{\# G_{i+1}}{\# G_0}$$

$$\begin{aligned} (\text{Rechte Seite})' (t) &= \frac{1}{\# G_0} \sum_{g \in G} \frac{d}{dt} \underbrace{\min\{i_{L/K}(g), t+1\}}_{\text{Flkt. konstant nahe } t \Leftrightarrow i_{L/K}(g) < t+1} \\ &\Leftrightarrow i_{L/K}(g) \leq t+1 \end{aligned}$$

$$= \frac{1}{\# G_0} \left(\sum_{g \in G \setminus G_{i+1}} 0 + \sum_{g \in G_{i+1}} 1 \right)$$

■

Lemma 4.23. Für $N \trianglelefteq G$, $E=L^N$, $\delta \in \text{Gal}(E/K)$ und $t \in \mathbb{R}_{\geq -1}$ gilt:

$$i_{E/K}(\delta) - 1 = \max \{ \phi_{L/E}(i_{L/K}(g) - 1) \mid g \in G, g|_E = \delta \}$$

Beweis. Wähle $\delta \in \{g' \in G \mid g'|_E = \delta\}$ für welches $i_{LIK}(\delta)$ maximal ist. Sei

$$m = i_{LIK}(\delta) - 1. \quad \underline{\text{Behauptung:}} \quad \forall \tau \in N: i_{LIK}(\delta\tau) = \min\{i_{LIK}(\tau), m+1\}$$

Fall $\tau \in N_m$: d.h. $i_{LIK}(\tau) - 1 \geq m \Rightarrow i_{LIK}(\delta\tau) \geq \min\{i_{LIK}(\delta), i_{LIK}(\tau)\}$
 $= m+1$ und = nach Wahl von δ .
 $= i_{LIK}(\delta)$

Fall $\tau \in N \setminus N_m$: $i_{LIK}(\tau) \leq m \xrightarrow{4.5(ii)} i_{LIK}(\delta\tau) = \begin{cases} i_{LIK}(\tau) \\ \text{wie oben} \end{cases} \Rightarrow \square \text{ Behauptung.}$

$$4.20 \Rightarrow i_{EIK}(\delta) = \frac{1}{e(E/K)} \sum_{\tau \in N} \min\{i_{LIK}(\tau), m+1\}$$

$$\Leftrightarrow \{g' \in G \mid g'|_E = \delta\} = G \cdot N$$

$$= \frac{1}{\#N_\delta} \sum_{\tau \in N} \min\{i_{LIE}(\tau), m+1\} \stackrel{4.22 \text{ f\"ur } N}{=} \phi_{LIE}(m) + 1$$

$$(O_K[x] = O_L \Rightarrow O_E[x] = O_L)$$

$$= \max \{ \phi_{LIE}(i_{LIK}(\delta) - 1) \mid \delta \in G, \delta|_E = \delta \} + 1$$

ϕ konvex
 $\Rightarrow \max(\phi) = \phi(\max)$

Korollar 4.24: (Herbrand's Theorem)

$$\text{Sei } u = \phi_{LIE}(u). \text{ Dann: } G_u \frac{N}{N} = \underbrace{(G/N)}_{\in \text{Gal}(E/K)}_u$$

Beweis. (Notation wie in 4.23)

$$\delta \in G_u \frac{N}{N} \Leftrightarrow \max \{ i_{LIK}(\delta) - 1 \mid \delta \in G, \delta|_E = \delta \} \geq u$$

$$\stackrel{4.23, \phi_{LIE} \text{ mon. wach.}}{\Leftrightarrow} i_{EIK}(\delta) - 1 \geq \phi_{LIE}(u) = u$$

$$\Leftrightarrow \delta \in (G/N)_u$$

Beweis von 4.19. (Transitivität)

(nur für ϕ , da $\psi = \phi^{-1}$) Sei $v \in \mathbb{R}_{\geq -1} \setminus \mathbb{Z}$.

$$\begin{aligned} \frac{d}{dt} (\phi_{E/K} \circ \phi_{L/E})(u) &= \phi'_{E/K}(v) \cdot \phi'_{L/E}(u) & N := \phi_{L/E}(u) \\ &= \frac{\#(\text{Gal}(E/K)_N)}{e(E/K)} \cdot \frac{\#(\text{Gal}(L/E)_u)}{e(L/E)} \stackrel{4.24}{=} \frac{\# \frac{G_u N}{N} \cdot \# \text{Gal}(L/E)_u}{e(L/K)} \\ &\left(\frac{G_u N}{N} \approx \frac{G_u}{N \cap G_u} = \frac{G_u}{N_u} \right) \Rightarrow = \frac{\# \frac{G_u}{\# N_u} \cdot \# N_u}{e(L/K)} \\ &= \phi'_{L/K}(u) \end{aligned}$$

□

Beweis von 4.18. Sei $v \in \mathbb{R}_{\geq -1}$, $x = \psi_{E/K}(v)$, $w = \psi_{L/E}(x) = \psi_{L/K}(v)$

$$(G/N)^v \underset{\text{Def.}}{=} \left(\frac{G}{N}\right)_{\psi_{E/K}(v)} = \left(\frac{G}{N}\right)_x \stackrel{4.24}{=} \frac{G_w N}{N} = \frac{G_{\psi_{L/K}(v)}}{N}$$

$$\underset{\text{Def.}}{=} \frac{G^v N}{N}.$$

□

Satz. (Hasse-Arf, o. Beweis, s. Serre)

Ist $\frac{G}{\text{Gal}(L/K)}$ abelsch, $v \in \mathbb{Q}$ ein Sprung der oberen verzweigungs. Filtrierung, so gilt: $v \in \mathbb{Z}$: