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

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

Beweis.
- Homomorphismus nach Konstruktion.
- Injektiv: $\rho(\sigma) = id \iff \sigma|_E = id_E \ \forall E \in \Sigma \implies \sigma = id_L$
- Surjektiv: Sei $(\sigma_E)_{E \in \Sigma} \in \varprojlim_{E \in \Sigma} Gal(E/K) \subseteq \prod_{E \in \Sigma} Gal(E/K)$

$$\underline{\text{d.h.:}} \quad E'/E \in \Sigma \implies \sigma_{E'}|_E = \sigma_E$$

Wegen $L = \bigcup_{E \in \Sigma} E$, definiere $\sigma : L \longrightarrow L$, $\alpha \longmapsto \sigma_E(\alpha)$ falls $\alpha \in E \in \Sigma$

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

$\implies \sigma \in Gal(L/K)$ mit $\rho(\sigma) = (\sigma_E)_E$

(Automorphismus da $\sigma|_E$ Automorphismus) $\square$

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

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

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

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

$\implies \overline{H} = \text{Bild von } H \text{ in } Gal(E/K) = \{ \sigma|_E \mid \sigma \in H \} \quad \left(= \frac{Gal(L|K)}{Gal(L/E)} \right)$

Sei $F = E^{\overline{H}}$ ... Prüfe: $H = Gal(L/F)$.

$$\text{endlich}\left[\begin{array}{c} L \\ | \\ E \\ | \\ F \\ | \\ K \end{array}\right] \quad \overline{H}$$

Umgekehrt: $F|K$ endl. Erweiterung in $L \rightsquigarrow$ Sei E der Galoisabschluss von $F|K$

$\implies [E:K] < \infty \implies \underbrace{Gal(L|E)}_{\text{offen}} \subseteq Gal(L|F)$.

$$\implies Gal(L|F) = \underbrace{\bigcup_{g \in Gal(L|F)/Gal(L|E)} g\, Gal(L|E)}_{\subseteq_{\text{offen}} Gal(L|K)}$$

$\square$

Korollar 2.4. Sei L wie in 2.3. Dann gilt:

$$\{H \leq Gal(L|K) \mid H \text{ abg.}\} = \{Gal(L|F) \mid L|F|K\}$$

Beweis.

"$\supseteq$": Schreibe $F = \bigcup_{i \in I} F_i$, I Menge, $F_i|K$ endl. Erw.

Dann: $$\underset{\sigma|_F = id_F}{Gal(L|F)} = \bigcap_{i \in I} \underbrace{\underset{\sigma|_{F_i} = id_{F_i}}{Gal(L|F_i)}}_{\text{offen-abgeschlossen}}$$

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

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

$$\underset{F = K[F_i | i \in I]}{\longrightarrow} \quad = \bigcap_{i \in I} Gal(L|F_i) = Gal(L|F)$$

$\square$

Satz 2.5. Sei $L|K$ galoisch. Dann sind die Abbildungen

$$\{H \leq Gal(L|K) \mid H \text{ abg.}\} \underset{Gal(L/F) \longleftarrow F}{\overset{H \longmapsto L^H}{\rightleftarrows}} \{F \subseteq L \mid F|K \text{ Körpererweiterung}\}$$

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

$$\{H \trianglelefteq Gal(L|K) \mid H \text{ abg. Normalteiler}\} \rightleftarrows \{E \subseteq L \mid E|K \text{ Galoiserweiterung}\}$$

Dabei gilt (topologisch): $$Gal(L/K)/N \xrightarrow{\sim} Gal(L^N/K)$$

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

$\square$

Bezeichnung: K ein beliebiger Körper.

K^{alg} bezeichne einen algebraischen Abschluss

$\underset{\text{ist galoisch über } K}{\underbrace{K^{sep}}} \subseteq K^{alg}$ bezeichne einen separablen Abschluss $\quad (K^{sep} = \{\alpha \in K^{alg} \mid K(\alpha)|K \text{ separabel}\})$

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

$$\left(\begin{matrix} Aut_K(K^{alg}) & \longrightarrow & G_K \\ \sigma & \longmapsto & \sigma|_{K^{sep}} \end{matrix} \quad \text{ist ein Isomorphismus} \right)$$

Bsp. • $G_{\mathbb{F}_q} \simeq \hat{\mathbb{Z}}$ $\quad$ ($\mathbb{F}_q$ perfekt $\Rightarrow$ $\mathbb{F}_q^{alg} = \mathbb{F}_q^{sep}$)

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

$$(\sigma_q : \alpha \mapsto \alpha^q) \longmapsto 1$$

und $\mathbb{F}_q^{alg} = \bigcup_n \mathbb{F}_{q^n}$ $\Rightarrow$ $G_{\mathbb{F}_q} \cong \varprojlim_{(\mathbb{N}, |)} Gal(\mathbb{F}_{q^n} \mid \mathbb{F}_q) \cong \hat{\mathbb{Z}}$

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

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

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

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

Bezeichnung: $G_{\mathbb{Q}_p} \xrightarrow[\text{Projektion}]{\text{kanonische}} Gal(\mathbb{Q}_p(\zeta_{p^\infty}) / \mathbb{Q}_p) \xrightarrow[\text{isom.}]{\text{obiger}} \mathbb{Z}_p^\times$

heißt p-adischer Kreisteilungscharakter.

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

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

Satz (Kronecker-Weber)

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

$$\text{ü}: \quad Gal(K^{ab} / K) \simeq G_K^{ab} = G_K / \overline{[G_K, G_K]}$$

∎

Bemerkung. $G_{\mathbb{Q}_p}$ für $p > 2$ ist beschrieben durch Koch-Jansen-Wingberg. (~1985)

($\hat{G}_K^p$, K lokal: ~1967)

03. Weitere Eigenschaften lokaler Körper

Sei K ein nicht-archimedischer lokaler Körper. Sei $\mathcal{O} = \mathcal{O}_K$ Bewertungsring,

$v = v_K : K^\times \to \mathbb{Z}$ normalisierte Bewertung.

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

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

A. Die multiplikative Gruppe von K

Def. 3.1. Für $i \in \mathbb{N}_0$ sei $\mathcal{U}_i := \mathcal{U}_i(K)$ definiert als $\mathcal{U}_0 := \mathcal{O}^\times$, $\mathcal{U}_i = 1 + \pi^i \mathcal{O}$ für $i \geq 1$.
Sei $\mu^{(p)}(K) = \{ \zeta \in K^\times \mid \exists\, n \in \mathbb{N} : \zeta^n = 1 \text{ und } p \nmid n \} \subseteq \mathcal{O}^\times$ endliche Untergruppe

Lemma 3.2. $\mu^{(p)}(K) \to k^\times$, $\zeta \mapsto \zeta \bmod \pi$ ist Gruppeniso. (Ü)

Proposition 3.3. Die kanonische Abbildung $\pi^{\mathbb{Z}} \times \mu^{(p)}(K) \times \mathcal{U}_1 \longrightarrow K^\times$ ist ein topologischer Isomorphismus
(ANT I, topologisch: Ü)

Lemma 3.4. $\forall i \in \mathbb{N}_0$: $\mathcal{U}_i / \mathcal{U}_{i+1} \xrightarrow{\sim} (k, +)$, $1 + a\pi^i \longmapsto a \bmod \pi$ ist Gruppenisomorphismus.

Beweis. $(1 + a\pi^i)(1 + b\pi^i) = 1 + (a + b(1 + \pi^i a))\pi^i$ $\quad (i \geq 1)$

$$\in (1 + (a+b)\pi^i)\, \mathcal{U}_{i+1}$$

$\Longrightarrow$ $\mathcal{U}_i \to (k, +)$, $1 + a\pi^i \mapsto a \bmod \pi$ ist Gruppenhomomorphismus

mit Kern $\mathcal{U}_{i+1}$.

$\boxtimes$

Korollar 3.5. $\forall i \in \mathbb{N}_{\geq 1}$: $\mathcal{U}_i \xrightarrow{\sim} \varprojlim_{j \geq i} \mathcal{U}_i / \mathcal{U}_j$ ($\rightsquigarrow \mathcal{U}_i$ ist pro-p Gruppe)

Beweis.
<u>injektiv</u>: ✓
<u>surjektiv</u>: Sei $\overline{\alpha}_j \in \mathcal{U}_i / \mathcal{U}_j$ kompatible Familie. Wähle $\alpha_j \in \mathcal{U}_i$ mit Reduktion $\overline{\alpha}_j$.

$\Longrightarrow$ $(\alpha_j)_j$ bilden CF in $\mathcal{O}^\times \subseteq \mathcal{O}$ $\underset{\substack{\mathcal{U}_i \text{ kpt.} \\ (\mathcal{O} \text{ kpt.!})}}{\Longrightarrow}$ $\alpha := \lim_j \alpha_j$ existiert in $\mathcal{U}_i$.

$\rightsquigarrow$ $\alpha \longmapsto (\overline{\alpha}_j)_j$.

$\boxtimes$

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

(0) $(1+\pi^i a)^p \equiv 1 + p\pi^i a + \pi^{pi} a^p \mod \pi^{e+2i}\mathcal{O}$ $\qquad e = e(K/\mathbb{Q}_p) = v_K(p)$ $\quad (p \mathrel{\hat{=}} \pi^e)$

(1) $(1+\pi^i a)^p \equiv 1 + a^p \pi^{ip} \mod \pi^{ip+1}$, falls $i < \frac{e}{p-1}$

(2) $(1+\pi^i a)^p \equiv 1 + p\pi^i a \mod \pi^{i+e+1}$, falls $i > \frac{e}{p-1}$

(3) $(1+\pi^i a)^p \equiv 1 \mod \pi^{i+e}$, falls $i = \frac{e}{p-1}$

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

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

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

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

(1) $\forall i > \frac{e}{p-1} : \forall k \geq 1$: φ induziert Isomorphismus $U_i/U_{i+k} \xrightarrow{\sim} U_{i+e}/U_{i+e+k}$

(2) $\forall i > \frac{e}{p-1}$: φ induziert Isomorphismus $U_i \xrightarrow{\sim} U_{i+e}$

Beweis.

(1) $\underline{k=1}$:

$$\begin{tikzcd} U_i/U_{i+1} \arrow[r] \arrow[d, phantom, "\cong"] & U_{i+e}/U_{i+e+1} \arrow[d, phantom, "\cong"] \\ (k,+) & (k,+) \end{tikzcd} , \quad \begin{tikzcd} (1+a\pi^i)\,U_{i+1} \arrow[r, mapsto, "3.6"'] \arrow[d, mapsto] & (1+pa\pi^i)\,U_{i+e+1} \arrow[d, mapsto] \\ a \bmod \pi & a \cdot \underbrace{\frac{p}{\pi^e}}_{\text{Einheit}} \bmod \pi \end{tikzcd}$$

(aus 3.6. Isomorphismus!)

Induktion:

$$\begin{tikzcd} 1 \arrow[r] & U_{i+1}/U_{i+k+1} \arrow[r] \arrow[d, "\cong", "\text{IV}"'] & U_i/U_{i+k+1} \arrow[r] \arrow[d, "\cong"] & U_{i+k}/U_{i+k+1} \arrow[r] \arrow[d, "\cong", "\text{IV}"'] & 1 \\ 1 \arrow[r] & U_{i+e+1}/U_{i+e+k+1} \arrow[r] & U_{i+e}/U_{i+e+k+1} \arrow[r] & U_{i+e+k}/U_{i+e+k+1} \arrow[r] & 1 \end{tikzcd}$$

$\cong$: Schlangenlemma.

(2) verwendet

$$\begin{tikzcd} U_i \arrow[r, "\sim"] \arrow[d, "\cong"] & \varprojlim_{j \geq i} U_i/U_j \arrow[d, "\cong\ \varphi \bmod \ldots"] \\ U_{i+e} \arrow[r] & \varprojlim_{j \geq i} U_{i+e}/U_{j+e} \end{tikzcd}$$

rechts Isomorphismus wegen (1). ▨

(2) alternativ:

$$\begin{tikzcd}
(\underbrace{1+\pi^i \mathcal{O}}_{=\mathcal{U}_i}, \cdot) \arrow[r, shift left, "\log"] \arrow[d, "\varphi"'] \arrow[dr, phantom, "="] & (\pi^i \mathcal{O}, +) \arrow[l, shift left, "\exp", "\sim"'] \arrow[d, "p \cdot -"] \\
(\mathcal{U}_{i+e}, \cdot) \arrow[r, shift left, "\log"] & (\pi^{i+e} \mathcal{O}, +) \arrow[l, shift left, "\exp", "\sim"']
\end{tikzcd}$$

ist Isomorphismus