01

Dienstag, 17. April 2018 22:21

Algebraische Zahlentheorie II.

Übungsblätter: Vorlesungshomepage.

01. Proendliche Gruppen

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

(0) $\emptyset, X \in \tau$ (1) $U, V \in \tau \Rightarrow U \cap V \in \tau$ (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 $x \in X$) $:\Leftrightarrow \exists V \in \tau : x \in V \subseteq W$.

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

z.B.: (X, d) metrischer Raum $\Rightarrow \{B_\varepsilon(x) \mid x \in X, \varepsilon > 0\}$ 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 $(G, e, \circ, \tau)$ besteht aus einer Gruppe $(G, e, \circ)$ und einem top. Raum (G, τ) so dass

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

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

$\leadsto$ Man erhält die Kategorie topologischer Gruppen $\underline{\text{Top Grp}}$.

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) $l_g : G \to G,\ h \mapsto g \circ h$, $\quad r_g : G \to G,\ h \mapsto h \circ g$ sind Automorphismen (insb. Homöomorphismen)

(ii) ϕ ist stetig $\iff \forall\, W' \in \mathcal{U}(e') : \exists\, W \in \mathcal{U}(e) : \phi(W) \subseteq W'$

(iii) Eine offene Untergruppe $H \underset{\text{offen}}{\leq} G$ ist abgeschlossen.

(iv) Eine abgeschlossene Untergruppe $H \underset{\text{abg.}}{\leq} G$ 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 $U \underset{\text{offen}}{\subseteq} G$, so ist $U^{-1} \underset{\text{offen}}{\subseteq} G$ und $cl(U) = \overline{U} \subseteq UU^{-1}$

(viii) G ist regulär, d.h. $\forall g \in G : \exists\, U, V \in \mathcal{U}(g)$ offen s.d. $V \subseteq \overline{V} \subseteq U$

(ix) G ist hausdorffsch $\iff \{e\} \underset{\text{abg.}}{\subseteq} G$

(x) Ist $N \trianglelefteq G$ Normalteiler, so ist $G/_N$ topologische Gruppe mit Quotiententopologie.
Dabei ist $G/_N$ hausdorffsch, falls $N \underset{\text{abg.}}{\subseteq} G$.

(xi) Sind $(G_i)_{i \in I}$ top. Grp., so ist $\prod_i G_i$ top. Grp.

Beweis.

(i) $l_g = G \to \{g\} \times G \xrightarrow{\text{inkl.}} G \times G \xrightarrow{\mu} G$ ist stetig, $\quad l_g \circ l_{g^{-1}} = id_G$

r_g analog.

(ii) "$\Rightarrow$": klar; "$\Leftarrow$": Sei $g \in G$, $g' := \phi(g)$, $W \in \mathcal{U}(g')$. 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) $$G = H \,\dot\cup\, \underbrace{\bigcup_{\substack{g \in G/H \\ g \neq 0}} gH}_{\text{offen, da } gH = l_g(H)}$$

(iv) wie (iii): $$G = H \,\dot\cup\, \underbrace{\bigcup_{\substack{g \in G/H \\ g \neq 0}} \underbrace{gH}_{\text{abg}}}_{\text{abg., da endliche Vereinigung wg. } [G:H] < \infty}$$

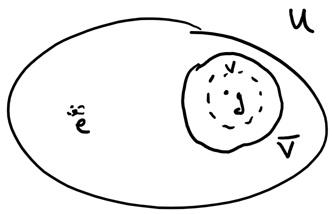
(v) $$G = \bigcup_{\substack{g \in G/H \\ g \neq 0}} \underbrace{gH}_{\text{offen}} \qquad G \text{ kompakt} \Rightarrow [G:H] < \infty$$

(vi), (vii): Übung.

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

<u>Beh.</u> (ii) $\exists$ offene Umgb. V von e mit $V \cdot V \subseteq U$, $V = V^{-1}$. Nun verwende (vii).

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



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

(x), (xi) Übung. $\square$

Whg. 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 $\phi_{ji}: G_j \to G_i$ $\forall i,j \in I$ mit $i \leq j$.

so dass: (i) $\phi_{ii} = id_{G_i}$ (ii) $\phi_{ki} = \phi_{ji} \circ \phi_{kj}$ $\forall i \leq j \leq k$

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 $G := \{ (g_i)_{i \in I} \in \prod_i G_i \mid \phi_{ji}(g_j) = g_i \ \forall i \leq j \}$

Lemma 1.3. Sind alle G_i topologische Gruppen, so auch $\varprojlim G_i$ mit der Unterraumtop. von $\prod_i G_i$.

Sind alle G_i hausdorffsch (kompakt + hausdorffsch), so ist auch $\varprojlim G_i$ hausdorffsch (kpt. + hd.).

Beweis.

① $\prod_i G_i$ ist selbst $\varprojlim G_i$ für geeignet gewähltes inverses System I.

Alle G_i hausdorffsch $\rightarrow$ $\prod_i G_i$ hausdorffsch (Produkte von Hausdorffräumen sind hausdorffsch)

Kompakt folgt mit dem Satz von Tychonoff.

② Allgemeiner Fall: Hausdorffsch überträgt sich auf Unterräume $\Rightarrow$ $\varprojlim G_i$ hd.

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

($\Gamma_{\phi_{ji}} \underset{\text{abg.}}{\subseteq} G_i \times G_j$ da G_i hd.)

$\Rightarrow$ $\varprojlim G_i$ kpt. da abg. Teilraum eines kpt. Raumes. $\square$

04

Mittwoch, 18. April 2018 21:09

Def. 1.4. Eine proendliche Gruppe ist ein inverser Limes $\varprojlim G_i$ 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
$\underset{\text{ü}}{\Leftrightarrow}$ Die Zusammenhangskomponente von x ist $\{x\}$

Proposition 1.6. (ü) Eine kpt., hd. top. Grp. ist total unzusammenhängend <=>
e besitzt eine Umgebungsbasis aus offen-abgeschlossenen Normalteilern von G.

05

Freitag, 20. April 2018 09:17

Korrektur: X top. Raum.

X heißt zusammenhängend $:\iff \emptyset, X$ sind die einzigen offen + abg. Teilmengen.

$x \sim_{zh} y \;:\iff \exists\, Y \subseteq X$ zushgd.: $x, y \in Y$. ist Äquivalenzrelation

Äquivalenzklassen 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

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

Def. 1.5. Ein topologischer Raum X heißt total-unzusammenhängend $\iff$ alle Zshgskomp. von X sind 1-elementig.

Korollar. (aus Lemma) Sei X kompakt, hd. Dann gilt:
X total unzshgd $\iff$ 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 proendlich (ii) G ist kompakt, hausdorffsch und total unzusammenhängend.

Beweis.
(i) $\Rightarrow$ (ii): kompakt, hausdorffsch: letztes Mal.
g.z.z.: $e \in \prod G_i$ besitzt Umgebungsbasis aus offen abgeschlossenen Teilmengen.
Eine solche ist gegeben durch $\left\{ \prod_{i \in I_0} \{e_i\} \times \prod_{I \setminus I_0} G_i \;\middle|\; I_0 \subseteq I \text{ endlich} \right\} =: \mathcal{U}_e$ offen, abg. Normalteiler

letztes Mal: G kpt., hd., $H \leq G$ offene Untergrp. $\rightarrow H$ abg.

Allgemeiner Fall: Schneide $\mathcal{U}_e$ mit $\varprojlim G_i$.

(ii) $\Rightarrow$ (i): Konsequenz aus dem folgenden Lemma. ☒

Lemma 1.8. Sei G kompakt, hausdorffsch, total unzshgd. und $\mathcal{U}$ eine Umgebungsbasis der Eins bestehend aus offen-abg. Normalteilern.
Dann ist

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

ein Isomorphismus topologischer Gruppen. (G/N endl. diskret)

Beweis. φ stetig: "obvious".
betrachte $G \longrightarrow \prod_{N \in \mathcal{U}} G/N \leftarrow$ hat Umgebungsbasis $\mathcal{U}_e$ (s. 1.7).

Für $I_0 \subseteq \mathcal{U}_e$ endl. $\rightsquigarrow$ Umgebung $\prod_{N \in I_0} N/N \times \prod_{N \in \mathcal{U}_e \setminus I_0} G/N$

Urbild ist $\bigcap_{N \in I_0} N$ ist offen abg. Normalteiler in G $\Rightarrow$ stetig bei e $\Rightarrow$ stetig.

φ injektiv: $\varphi(g) = (e_N)_{N \in \mathcal{U}} \Rightarrow g \in N \;\forall N \in \mathcal{U}$.
Umgebungsbasis, G hausdorffsch.

$\rightarrow \bigcap_{\mathcal{U}_0} N = \{e\}$, d.h. $g = e$.

· φ surjektiv. Sei $(g_N \cdot N)_{N \in \mathfrak{U}} \in \varprojlim G/N$ $\quad (N' \subseteq N \Rightarrow g_{N'} N = g_N N)$

gesucht:
$$g \in \bigcap_{N \in \mathfrak{U}} \underbrace{(g_N N)}_{\text{abg.}} \subseteq G \text{ kompakt}$$

Anm.:
rechte Seite leer $\Rightarrow \exists I_0 \subseteq \mathfrak{U}$ endlich: $\bigcap_{N \in I_0} g N = \emptyset$. $\mathfrak{U}$ 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, $\mathfrak{U}$ wie 1.8

(a) $\forall\ H \leq G$ abg. gilt: $H \xrightarrow{\sim} \varprojlim_{N \in \mathfrak{U}} H/N \cap H$

(b) $\forall\ H \trianglelefteq G$ abg. gilt $G/H \xrightarrow{\sim} \varprojlim_{N \in \mathfrak{U}} G/N \cdot H$

Lemma 1.10. Sei G proendlich, $H \leq G$ Untergruppe. Dann sind äquivalent:
(i) H ist abgeschlossen
(ii) $H = \bigcap \{ U \mid U \leq G$ offene Untergruppe mit $H \leq U \}$

Beweis.
"$\Leftarrow$": $U \leq G$ offen $\underset{G \text{ kpt.}}{\Rightarrow}$ U abg. Untergruppe $\Rightarrow \bigcap \{U \ldots\}$ ist abgeschlossen.

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

In Ü: $\underset{\text{Teilmenge}}{H \subseteq G}$ kompakt $\Rightarrow \bigcap_{V \in \mathfrak{U}} H \cdot V = H$. ▨

Def. 1.11. Eine pro-p Gruppe ist ein inverser Limes von endlichen p-Gruppen.
(Insb. proendlich)

Def. 1.12. Sei G eine diskrete (i.a. unendliche) Gruppe.
Die pro-p Komplettierung von G ist
proendliche

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

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

(man kann auch Ringe pro-p oder pro-endl. 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. $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \overset{\cong}{\underset{CRS}{}} \varprojlim_n \left(\prod_{p \text{ prim}} \mathbb{Z}/p^{v_p(n)}\mathbb{Z} \right)$; $\prod_p \mathbb{Z}_p = \varprojlim_{U \in \mathcal{U}} \overset{\text{pro endl.}}{\prod \mathbb{Z}_p / U}$

$\mathcal{U} = \{ \underbrace{\prod_p (p^{v_p(n)} \mathbb{Z}_p)}_{=: U_n} \mid n \in \mathbb{N} \}$ $\qquad = \varprojlim_n \prod \mathbb{Z}_p / U_n$ ☒

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

Bsp. $\{1\}$ ist topologisches EZS 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. EZS 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 $\bar{b}_1, .., \bar{b}_n$ eine Basis von $G/\phi(G)$, dann ist $\{b_1, .., b_n\}$ ein <u>minimales</u> EZS.

Beweis. (ü).

☒

<u>Bem.</u> 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 $\mathbb{Z}_p \times G \to G$

$$\underbrace{\alpha}_{\in \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}} \cdot \underbrace{g}_{=(g_i)_i \in \varprojlim \underset{\text{endl. abelsche p-Grp.}}{G_i}} := (\alpha \bmod \underbrace{\# G_i}_{p\text{-Potenz}} \cdot g_i)_{i \in I} \in \varprojlim_I G_i = G.$$

$$= \alpha \bmod \operatorname{ord}(g_i) \cdot g_i$$

(<u>wohldef</u>? $\pi_{ji}: \begin{cases} G_j \to G_i \\ g_j \mapsto g_i \end{cases}$ $\quad \pi_{ji}(\alpha \bmod \operatorname{ord}(g_j) \cdot g_j) = (\alpha \bmod \operatorname{ord}(g_i) \cdot g_i)$)

$\operatorname{ord}(g_i) \mid \operatorname{ord}(g_j)$

z.B. $(1 + p\mathbb{Z}_p, \cdot) = \varprojlim_n \underbrace{\left({}^{1+p\mathbb{Z}_p} / {}_{1+p^n\mathbb{Z}_p} \right)}_{= \{\beta \in (\mathbb{Z}/p^n\mathbb{Z})^\times \mid \beta \equiv 1 \ (n)\} = \langle 1+p \rangle \cong \mathbb{Z}/p^{n-1}}$ ☒

$\beta \in 1+p\mathbb{Z}_p$, $\alpha \in \mathbb{Z}_p$
$\leadsto \beta^\alpha \in 1 + p\mathbb{Z}_p$

(b) G topol. endlich erzeugt $\overset{}{\underset{\text{ü}}{\Longleftrightarrow}}$ G ist endl. erz. als $\mathbb{Z}_p$-Modul

In diesem Fall kann man den Struktursatz für endl. erz. Moduln über HI-Ringen anwenden

$$\Rightarrow G \simeq \mathbb{Z}_p^r \times \prod_{i=1}^{t} \mathbb{Z}/p^{n_i} \quad \ldots$$

02. Galoistheorie und unendliche Galoiserweiterungen

Whg. $L|K$ algebraische Erweiterung von Körpern

$L|K$ normal $\Leftrightarrow \forall \alpha \in L$: $\mathrm{mipo}_K(\alpha) \in K[X]$ zerfällt über L in Linearfaktoren
$L|K$ separabel $\Leftrightarrow \forall \alpha \in L$: $\mathrm{mipo}_K(\alpha)$ besitzt nur einfache Nullstellen in K^{alg}.
$L|K$ galoissch $:\Leftrightarrow$ $L|K$ normal + separabel

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

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

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

$$\{ H \leq \mathrm{Gal}(L|K) \text{ UG} \} \underset{\mathrm{Gal}(L|F) \leftarrow\!\shortmid F}{\overset{H \mapsto L^H}{\longleftrightarrow}} \{ L|F|K \text{ Zwischenkp.} \}$$

definiert eine Bijektion.

$$\{ H \trianglelefteq G \text{ NT} \} \overset{1:1}{\longleftrightarrow} \{ F \text{ Zwkp.} \mid F|K \text{ galoissch} \}$$

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 $\subseteq$, $\rightsquigarrow (\Sigma, \subseteq) \longrightarrow \mathrm{Grp}$, $E \longmapsto \mathrm{Gal}(E|K)$ ist ein inverses System.

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

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

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

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)

$\implies \sigma \in \mathrm{Gal}(L/K)$ mit $\varrho(\sigma) = (\sigma_E)_E$

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

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

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

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

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

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

$L - E - F - K$, $[E:F] = \overline{H}$, endlich

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

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

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

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

▨

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

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

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

Dann:
$$\mathrm{Gal}(L|F) = \bigcap_{i\in I} \underbrace{\mathrm{Gal}(L|F_i)}_{\text{offen} \Rightarrow \text{abgeschlossen}}$$

$$\sigma|_F = id_F \qquad \sigma|_{F_i} = id_{F_i}$$

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

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

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

$\square$

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

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

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

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

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

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

$\square$

Bezeichnung: K ein beliebiger Körper.

K^{alg} bezeichne einen algebraischen Abschluss

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

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

$$\left(\begin{array}{ccc} \mathrm{Aut}_K(K^{alg}) & \longrightarrow & G_K \\ \sigma & \longmapsto & \sigma|_{K^{sep}} \end{array} \text{ ist ein Isomorphismus} \right)$$

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

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

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

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)

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

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

∎

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

($\widehat{G_K}^p$, 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. $\mu^{(p)}(K) \longrightarrow k^\times$, $\zeta \longmapsto \zeta \bmod \pi$ 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. $$(1 + a\pi^i)(1 + b\pi^i) = 1 + (a + b(1 + \pi^i a))\pi^i \qquad (i \geq 1)$$
$$\in (1 + (a+b)\pi^i)\,\mathcal{U}_{i+1}$$

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

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

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 $\overline{\alpha}_j$.
$\Rightarrow$ $(\alpha_j)_j$ 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 $\mathcal{U}_i$.

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

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

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

(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 $\mathcal{U}_i / \mathcal{U}_{i+k} \xrightarrow{\sim} \mathcal{U}_{i+e} / \mathcal{U}_{i+e+k}$

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

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

$$\begin{array}{ccc} \mathcal{U}_i/\mathcal{U}_{i+1} & \longrightarrow & \mathcal{U}_{i+e}/\mathcal{U}_{i+e+1} \\ \wr\wr & & \wr\wr \\ (k,+) & & (k,+) \end{array}, \quad \begin{array}{ccc} (1+a\pi^i)\,\mathcal{U}_{i+1} & \overset{}{\underset{3.6}{\longmapsto}} & (1+pa\pi^i)\,\mathcal{U}_{i+e+1} \\ \downarrow & & \downarrow \\ a \mod \pi & & a \cdot \underbrace{\frac{p}{\pi^e}}_{\text{Einheit}} \mod \pi \end{array}$$

(aus 3.6. Isomorphismus!)

Induktion:

$$\begin{array}{ccccccccc} 1 & \to & \mathcal{U}_{i+1}/\mathcal{U}_{i+k+1} & \to & \mathcal{U}_i/\mathcal{U}_{i+k+1} & \to & \mathcal{U}_{i+k}/\mathcal{U}_{i+k+1} & \to & 1 \\ & & \text{IV}\ \downarrow\wr & & \downarrow\wr & & \downarrow\wr\ \text{IV} & & \\ 1 & \to & \mathcal{U}_{i+e+1}/\mathcal{U}_{i+e+k+1} & \to & \mathcal{U}_{i+e}/\mathcal{U}_{i+e+k+1} & \to & \mathcal{U}_{i+e+k}/\mathcal{U}_{i+e+k+1} & \to & 1 \end{array}$$

$\simeq$: Schlangenlemma.

(2) verwendet

$$\begin{array}{ccc} \mathcal{U}_i & \xrightarrow{\sim} & \varprojlim_{j \geq i} \mathcal{U}_i/\mathcal{U}_j \\ \downarrow\wr & & \downarrow\wr\ \varphi \text{ mod} \dots \\ \mathcal{U}_{i+e} & \longrightarrow & \varprojlim_{j \geq i} \mathcal{U}_{i+e}/\mathcal{U}_{j+e} \end{array}$$

rechts Isomorphismus wegen (1). ▨

(2) alternativ:

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

$p\cdot -$ ist Isomorphismus

$\boxtimes$

Satz 3.8. K sei p-adischer Körper. Dann: 27.04.18

(1) $\mathcal{U}_1(K) \cong \mu_{p^\infty}(K) \times \mathbb{Z}_p^{[K:\mathbb{Q}_p]}$ 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.

Dabei:

- $\mu_{p^\infty}(K) = \{\zeta \in K^\times \mid \exists n>0: \zeta^{p^n} = 1\}$
- $\#\mu_{p^\infty}(K) < \infty$: $[K:\mathbb{Q}_p] < \infty$ und $[\mathbb{Q}_p(\zeta_{p^n}) : \mathbb{Q}_p] = \phi(p^n)$

$$p^{n-1}(p-1) \xrightarrow[n\to\infty]{} \infty$$

Bemerkung: · $\mathcal{U}_1(K)$ ist abelsche pro-p-Gruppe (letztes mal), d.h. $\mathbb{Z}_p$-Modul.

· $\mathcal{U}_1(K)_{tors} \cong \mu_{p^\infty}(K)$ und $\mathcal{U}_1(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_p^{[K:\mathbb{Q}_p]}$

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

(1) $\mathcal{U}_1(K)$ ist abelsche pro-p-Gruppe.

$$\mathcal{U}_1(K)_{tors} = \{x \in \mathcal{U}_1(K) \mid \exists n \in \mathbb{N}: x^{p^n} = 1\} = \mu_{p^\infty}(K) \quad (<\infty)$$

Beh. $\mathcal{U}_1(K)$ topol. endl. erz. $\Rightarrow \mathcal{U}_1(K)$ endl. erz. $\mathbb{Z}_p$-Modul

$\Rightarrow \mathcal{U}_1(K) \cong \mathcal{U}_1(K)_{tors} \times \mathbb{Z}_p^r$ für ein $r \in \mathbb{N}_0$

Dazu: (Burnside Basissatz) z.z. $\mathcal{U}_1(K)/\mathcal{U}_1(K)^p$ endlich

dazu: $\mathcal{U}_1(K)^p \supseteq \mathcal{U}_{i_0}(K)^p \overset{3.7.}{=} \mathcal{U}_{i_0+e}(K)$ für $i_0 = \left\lceil \frac{e}{p-1} \right\rceil$

$\Rightarrow \mathcal{U}_1(K)/\mathcal{U}_1(K)^p$ ist Quotient von $\mathcal{U}_1(K)/\mathcal{U}_{i_0+e}(K)$ ← endliche p-Gruppe

($\mathcal{U}_i/\mathcal{U}_{i+1} \cong (k,+)$ endl.)

$\Rightarrow$ Behauptung gezeigt.

Behauptung: $r = [K:\mathbb{Q}_p]$ $\quad \mathcal{U}_1/\mathcal{U}_i$ endl. $\forall i \geq 1$

$\Rightarrow \operatorname{rang}_{\mathbb{Z}_p} \mathcal{U}_1 = \operatorname{rang}_{\mathbb{Z}_p} \mathcal{U}_{i_0}$

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

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

Alternativ: U_{i_0} ist p-torsionsfrei, denn $x \mapsto x^p$ ist Isomorphismus $U_{i_0} \to U_{i_0+e}$

$\Rightarrow U_{i_0}$ ist freier $\mathbb{Z}_p$-Modul (von endl. Rang)

$$\underset{\text{Nakayama}}{\Longrightarrow} \operatorname{rang}_{\mathbb{Z}_p} U_{i_0} = \operatorname{rang}_{\mathbb{F}_p} U_{i_0}/U_{i_0}^p = \operatorname{rang}_{\mathbb{F}_p} U_{i_0}/U_{i_0+e} = \log_p(\# U_{i_0}/U_{i_0+e})$$

$$= \log_p((\underbrace{\# k}_{=p^f})^e) = ef = [K:\mathbb{Q}_p]$$

$\blacksquare$

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

__Behauptung:__ $$\prod_{\substack{n\in\mathbb{N}\\ p\nmid n}} \prod_{j=1}^{f} \mathbb{Z}_p \longrightarrow U_1(K), \quad (a_{nj})_{n,j} \longmapsto \prod_{n,j} (1+b_j\pi^n)^{a_{nj}}$$

$\blacksquare$

B. Zahm 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 $\ \in\mathbb{N}$ $\exists!$ unverzweigte Erweiterung K_ℓ von K mit $[K_\ell:K] =\ $, nämlich $K = K(\zeta_{q^\ell-1})$, $K_\ell|K$ ist galoissch und

$$\operatorname{Gal}(K_\ell|K) \xrightarrow{\sim} \operatorname{Gal}(k(\zeta_{q^\ell-1})/k) \cong \mathbb{Z}/\ell\mathbb{Z}$$

Beweis. (vgl. ANT I)

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

$\Rightarrow f(K(\zeta_n)|K) = [K(\zeta_n):K]$

(__Hensel:__ $\deg \operatorname{mipo}_K \zeta_m = \deg \operatorname{mipo}_k \zeta_m$). Hensel zeigt auch $K(\zeta_m) \subseteq L$ und $k_L = k_K(\zeta_m)$

($\Rightarrow L|K(\zeta_m)$ voll verzweigt) $\Rightarrow$ (a), (b), (c).

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

$\blacksquare$

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

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

Def. 3.11.

(1) $L|K$ heißt unverzweigt $:\Longleftrightarrow$ alle $F \in \mathcal{F}_{L|K}$ sind unverzweigt über K.

(2) $L|K$ heißt total verzweigt $:\Longleftrightarrow$ alle $F \in \mathcal{F}_{L|K}$ sind total verzweigt über K.

(3) $K^{ur} := \bigcup \{ F \in \mathcal{F}_{K^{sep}|K} \mid F/K \text{ unverzweigt} \}$ $\left(= \varinjlim \ldots \right)$

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

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

Sei $k_L = \bigcup \{ k_F \mid F \in \mathcal{F}_{L|K} \}$ $\left(= \varinjlim \ldots \right)$

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

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

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

Def. 3.12. $L|K$ galoissch.

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

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

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

(iii) Haben $\sigma : k_L \to k_L$, $\alpha \mapsto \alpha^q$ in $Gal(k_L/k)$ (topol. Erz.) $q = \# k$

Nenne $Fr \in Gal(L|K)$ einen Frobeniusautomorphismus $:\Longleftrightarrow \rho_{L|K}(Fr) = \sigma$

Bem. (1) Haben "wieder" kurze exakte Sequenzen $1 \to I_{K/L} \to Gal(L|K) \xrightarrow{\rho_{L|K}} Gal(k_L/k) \to 1$

als inverser Limes analoger Sequenzen für $E \in \mathcal{F}_{L|K}$ mit $E|K$ galoissch.

(2) Fr ist eindeutig $\Longleftrightarrow$ $\rho_{L|K}$ ist Isomorphismus $\Longleftrightarrow$ $L|K$ ist unverzweigt (d.h. $I_{L|K} = \{1\}$)

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

Def. 3.13. (a) Gilt $[L:K] < \infty$, so heißt $L|K$ zahm verzweigt $:\Leftrightarrow p \nmid e(L|K)$ (p = char k)

(b) $L|K$ heißt zahm verzweigt $:\Leftrightarrow$ alle $F \in \mathcal{F}_{L|K}$ sind zahm verzweigt über K

(c) $L|K$ heißt wild verzweigt $:\Leftrightarrow$ $L|K$ ist nicht zahm verzweigt.

($p \mid e(F|K)$ für ein $F \in \mathcal{F}_{L|K}$)

Bsp. (a) $e \in \mathbb{Z}_{\geq 2}$ mit $p \nmid e \Rightarrow L = K(\sqrt[e]{\pi})$ zahm verzweigt (und total unverzweigt)

(b) $p = \operatorname{char} k$, $L|K$ inseparabel $\rightarrow$ $L|K$ wild verzweigt

(c) $\mathbb{Q}_p(\zeta_p) / \mathbb{Q}_p$ zahm, 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 $L|K$ zahm verzweigt, $[L:K] < \infty$, $E = L \cap K^{ur}$, $e = e(L|K)$. Dann:

(a) $L = E(\sqrt[e]{\pi_E})$ für π_E geeignetes Primelement von E.

(b) $E' := E(\zeta_{e \cdot \# k_E^\times})$, $L' := LE'$ $\Rightarrow L' = E'(\sqrt[e]{\underbrace{\pi}_{=\pi_K}})$

und $E'|K$ unverzweigt, $L'|L$ unverzweigt --- ($L'|K$ galoissch)

Beweis.

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

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

$\Rightarrow \zeta^{-1}\pi = (\pi_L \cdot u')^e$

beachte: $\mu^{(p')}(L) = \mu^{(p')}(E)$ da $k_L = k_E$ $\Big\}$ $\Rightarrow \pi_E := \zeta^{-1}\pi$ Primelement von $\mathcal{O}_E$ und $L = E(\sqrt[e]{\pi_E})$

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

(b) wähle $\xi \in \mu^{(p')}(E)$ mit $\xi^e = \zeta$ $\quad (\zeta^{\# k_E^\times} = 1)$

Dann: $\pi = (\pi_L \cdot u' \xi)^e \Rightarrow L' = E'(\sqrt[e]{\pi})$.

$\blacksquare$

Bsp. (ii) $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{\pi'})$ für geeigneten Uniformisierer in $\mathbb{Q}_p$.

Bch.: $\pi = -p$ tut's!

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

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

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

Für $\hat{a} \in \hat{\mathbb{Z}}$ beliebig: schreibe $\hat{a} = (a_n)_n \in \varprojlim_n (\mathbb{Z}/n\mathbb{Z})$ $\quad (a_n \in \mathbb{Z})$

prüfe: (g^{a_n}) "konvergieren" $\quad ((g^{a_n})$ hat end. Häufungspunkt!)

Proposition 3.15.

(a) Sind L, L' zahm verzweigt über K, so auch LL' $\quad (\Rightarrow \exists$ größte zahm verzw. Erw. K^{tr} von L in K^{sep})

(b) Die maximal zahm verzweigte Erweiterung von K in K^{alg} ist

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

(c) K^{tr}/K^{ur} ist galoissch und $\underbrace{Gal(K^{tr}/K^{ur}) \underset{\text{kan.}}{\cong} \prod_{\substack{\ell \neq p \\ \ell \text{ prim}}} \mathbb{Z}_\ell}_{=\hat{\mathbb{Z}}/\mathbb{Z}_p} =: \hat{\mathbb{Z}}^{(p)}$

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

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

Beweis.

(a) Für $L, L' | K$ endl: $e(LL'/K) \mid e(L|K)\,e(L'|K)$ $\quad$ (aus ANT 1) oder 3.14

(b) Folgt aus 3.14 (b)

(c) $Gal(K^{ur}(\sqrt[n]{\pi}) \mid K^{ur}) \cong \mathbb{Z}/n\mathbb{Z}$ $\quad$ (nach Kummertheorie)

$(p \nmid n)$ Galoiskonjugierten von $\sqrt[n]{\pi}$ sind $(\zeta_n^i \sqrt[n]{\pi})_{i=1}^n$ $\quad$ (Algebra I)

$\varprojlim(\ldots) = \varprojlim_{p \nmid n}(\ \ ) \cong \hat{\mathbb{Z}}^{(p)}$

(d) (ii) Sei $K(n) := K(\zeta_{q^n-1}, \sqrt[q^n-1]{\pi})$; Beh.: $K(n)|K$ galoissch mit $Gal(K(n)|K) \cong \underbrace{\mathbb{Z}/_{q^n-1}\mathbb{Z}}_{t=1} \rtimes \underbrace{\mathbb{Z}/n\mathbb{Z}}_{s=1}$

zahm total verzweigt $\quad$ unverzweigt $Gal(K(\zeta_{q^n-1})|K)$

$\underline{\underline{\text{und}}}$: $sts^{-1} = t^q$