Algebraische Zahlentheorie II.

Übungsblätter: Vorlesungshomepage.

01. Proendliche Gruppen

Wdh. · X Menge, Topologie auf X: $\mathcal{T} \subseteq \mathcal{P}(X)$ mit
(0) $\emptyset, X \in \mathcal{T}$ (1) $U, V \in \mathcal{T} \Rightarrow U \cap V \in \mathcal{T}$ (2) $(U_i)_{i \in I} \in \mathcal{T}^I \Rightarrow \bigcup_i U_i \in \mathcal{T}$

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

· $W \subseteq X$ heißt Umgebung (von $x \in X$) $:\Leftrightarrow \exists V \in \mathcal{T}: x \in V \subseteq W$.

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.

· $(X, \mathcal{T}_X) \xrightarrow{f} (Y, \mathcal{T}_Y)$ heißt stetig $:\Leftrightarrow f^{-1}(\mathcal{T}_Y) \subseteq \mathcal{T}_X$.

· Produkttopologie: Seien $((X_i, \mathcal{T}_i))_{i\in I}$ topologische Räume.

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

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

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

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

Def. 1.1. (a) Eine topologische Gruppe $(G, e, \circ, \mathcal{T})$ besteht aus einer Gruppe $(G, e, \circ)$ und einem top. Raum $(G, \mathcal{T})$ 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.

$\rightsquigarrow$ 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) $l_g : G \to G,\ h \mapsto g \circ h$, $r_g : G \to G,\ h \mapsto h \circ g$ 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, $l_g \circ l_{g^{-1}} = id_G$

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

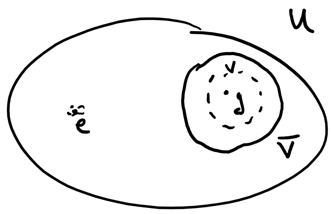
(v) $$G = \bigcup_{\substack{g \in G/H \\ g \neq 0}} \underbrace{gH}_{\text{offen}}$$ G kompakt $\Rightarrow [G:H] < \infty$

(vi), (vii): Übung.

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

Beh. (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. ∎

Def. 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) $\phi_{ii} = \mathrm{id}_{G_i}$ (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 $\to$ $\prod_i G_i$ 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.

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

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

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

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 $:\Longleftrightarrow$ $\emptyset, X$ sind die einzigen offen + abg. Teilmengen.

$x \sim_{zh} y \;:\Longleftrightarrow\; \exists\, Y \subseteq X$ 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 $\Longleftrightarrow$ alle Zshgskomp. von X sind 1-elementig.

Korollar. (aus Lemma) Sei X kompakt, hd. Dann gilt:
X total unzshgd $\Longleftrightarrow$ 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 $\left\{ \prod_{i \in I_0} \{e_{i_0}\} \times \prod_{I \setminus I_0} G_i \;\middle|\; I_0 \subseteq I \text{ endlich} \right\} =: \mathcal{U}_e$ ← 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

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

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

Beweis. φ stetig: "obvious".
betrachte $G \longrightarrow \prod_{N \in \mathcal{U}} G/N$ ← 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: $\varphi(g) = (e_N)_{N \in \mathcal{U}}$ $\Rightarrow$ $g \in N \quad \forall N \in \mathcal{U}$.
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. $\square$

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

Beweis.
"$\Leftarrow$": $U \leq G$ offen $\overset{G \text{ kpt.}}{\Rightarrow}$ 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 $\Rightarrow \bigcap_{V \in \mathfrak{U}} H \cdot V = H$. $\square$

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

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

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

☐

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 $\bar{b}_1, \dots, \bar{b}_n$ eine Basis von $G/\Phi(G)$, dann ist $\{b_1, \dots, b_n\}$ 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 $\mathbb{Z}_p \times G \to G$

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

(G_i endl. abelsche p-Grp.)

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

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

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

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

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

☐

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

In diesem Fall kann man den Strukturs atz für endl. erz. Moduln über HI-Ringen anwenden
$\Rightarrow G \simeq \mathbb{Z}_p^r \times \prod_{i=1}^{\ell} \mathbb{Z}/p^{n_i}$ ...

02. Galoistheorie und unendliche Galoiserweiterungen

Whg. $L|K$ algebraische Erweiterung von Körpern

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

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

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 $\Sigma := \{ E | L \text{ Unterkörper} \mid E|K \text{ endlich galoissch} \}$, 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) ▨

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: $H = Gal(L/F)$.

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

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

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

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

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 $L|K$ galoissch. Dann sind die Abbildungen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

heißt p-adischer Kreisteilungscharakter.

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

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

Satz (Kronecker-Weber)

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

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

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

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

O3. 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 Isomorphism
(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. $(1 + a\pi^i)(1 + b\pi^i) = 1 + (a + b(1 + \pi^i a))\pi^i \qquad (i \geq 1)$

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

$\Longrightarrow$ $\mathcal{U}_i \to (k, +)$, $1 + a\pi^i \mapsto a \bmod \pi$ 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) $(1+\pi^i a)^p \equiv 1 + p\pi^i a + \pi^{pi} a^p \mod \pi^{e+2i}\mathcal{O}$ $\qquad e = e(K/\mathbb{Q}_p) = v_K(p)$ $\quad (p \,\hat{=}\, \pi^e)$

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

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

(aus 3.6. Isomorphismus!)

Induktion:

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

$\simeq$: Schlangenlemma.

(2) verwendet

$$\begin{tikzcd} U_i \arrow[r, "\sim"] \arrow[d, "\simeq"] & \varprojlim\limits_{j \geq i} U_i/U_j \arrow[d, "\simeq\ \varphi \bmod \dots"] \\ U_{i+e} \arrow[r] & \varprojlim\limits_{j \geq i} U_{i+e}/U_{j+e} \end{tikzcd}$$

rechts Isomorphismus wegen (1). ▨

(2) alternativ:

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

ist Isomorphismus