

Algebraische Zahlentheorie II.

Übungsbücher: Vorlesungshomepage.

01. PROENGLICHE GRUPPEN

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

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

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

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

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

z.B.: (X, d) metrischer Raum $\Rightarrow \{B_\epsilon(x) \mid x \in X, \epsilon > 0\}$ 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 $\text{cl}(U) = \overline{U} \subseteq UU^{-1}$
- (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 $\Leftrightarrow \{e\} \subseteq G$ 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.

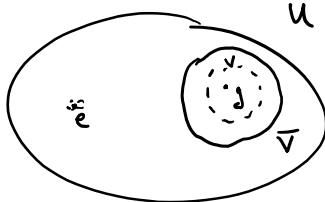
Beweis.

- (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) $G = \bigcup_{\substack{g \in G/H \\ g \neq 0}} \underbrace{gH}_{\text{offen}}$ $\quad G$ 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.

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

$\Rightarrow \varprojlim_{i \in I} G_i$ 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. $x \sim_{\text{zh}} y : \Leftrightarrow \exists Y \subseteq X$ zshgd.: $x, y \in Y$ 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 unzshgd. \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 $\left\{ \prod_{i \in I_0} \{e_{i_0}\} \times \overline{\prod_{I \setminus I_0} G_i} \mid I_0 \subseteq I \text{ endlich} \right\} =: U_e$ 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 unzshgd. 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. $\hat{\mathbb{Z}} \cong \prod_{p \text{ prim}} \mathbb{Z}_p$ pro endl.

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

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

$$=: U_n$$

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 $\mathbb{Z}_p \times G \rightarrow G$

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

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

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

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

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

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

(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
 $\Rightarrow G \cong \mathbb{Z}_p^r \times \prod_{i=1}^k \mathbb{Z}/p^{n_i}$ - - -

02. GALOISTHEORIE UND UNENDLICHE GALOISERWEITERUNGEN

Wdg. $L|K$ algebraische Erweiterung von Körpern

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

$L|K$ separabel $\Leftrightarrow \forall \alpha \in L : m_{\text{irr}, K}(\alpha)$ 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.

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

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

