Algebraische Zahlentheorie II
Sommersemester 2022

Dr. Katharina Hübner
basierend auf Alexander Schmidts AZT2-Skript von 2014

1 Unendliche Galoistheorie

1.1 Proendliche Gruppen

In dieser Vorlesung ist ein kompakter topologischer Raum per Definition quasikompakt (d.h. jede offene Überdeckung hat eine endliche Teilüberdeckung) und Hausdorffsch (d.h. verschiedene Punkte haben disjunkte offene Umgebungen).

Theorem 1.1 (Satz von Tychonov)**.** *Das Produkt kompakter topologischer Räume ist kompakt.* □

Man erinnere sich daran, dass der projektive Limes eines projektiven Systems topologischer Räume $(T_i)_{i\in I}$ mit Übergangsabbildungen $\phi_{ij} : T_i \to T_j$ als Teilraum des Produktes konstruiert werden kann:

$$\varprojlim_i T_i = \{(x_i) \in \prod_i T_i \mid \varphi_{ij}(x_i) = x_j\}.$$

Dabei ist die Topologie die Unterraumtopologie von $\prod_i T_i$ mit der Produkttopologie. Sind $\varphi_k : \varprojlim_i T_i \to T_k$ die natürlichen Projektionen, so ist eine Basis der Topologie von $\varprojlim_i T_i$ gegeben durch

$$\{\varphi^{-1}(U_i) \mid i \in I,\ U_i \subseteq T_i \text{ offen}\}.$$

Satz 1.2. *Sei T_i ein projektives System nichtleerer kompakter topologischer Räume. Dann ist $\varprojlim_i T_i$ kompakt und nichtleer.*

Beweis. Setze für $i \geq j$:

$$U_{ij} = \left\{(x_k) \in \prod_{k\in I} T_k \mid \varphi_{ij}(x_i) \neq x_j\right\}$$

1) die U_{ij} sind offene Teilmengen in $\prod T_k$
2) jede endliche Vereinigung von Mengen der Form U_{ij} ist echt kleiner als $\prod T_k$

Zu 1) ist einfach. Zu 2) wähle ein $n \in I$ größer gleich allen i, j die auftreten. Wähle $x_n \in T_n$ beliebig und setze

$$x_m = \begin{cases} \varphi_{nm}(x_n) & \text{falls} \quad m \leq n \\ \text{beliebiges Element in} & T_m \quad \text{sonst.} \end{cases}$$

Dann liegt $x = (x_m)$ nicht in der Vereinigung der U_{ij}.
3) Die Vereinigung aller U_{ij} ist das Komplement von $\varprojlim T_i$ in $\prod T_i \Longrightarrow \varprojlim T_i$ abgeschlossen.

Bleibt zu zeigen $\varprojlim T_i \neq \varnothing$. Ansonsten würden die U_{ij} ganz $\prod T_i$ überdecken. Da $\prod T_i$ kompakt ist, gäbe es eine endliche Teilüberdeckung, was nach 2) nicht möglich ist. □

Korollar 1.3. *Der projektive Limes eines Systems endlicher nichtleerer Mengen ist nichtleer.*

Definition. Eine Folge topologischer Gruppen und stetiger Homomorphismen

$$G' \xrightarrow{\varphi} G \xrightarrow{\psi} G''$$

heißt **exakt**, wenn $\psi \circ \varphi = 0$ und die natürliche Abbildung

$$\begin{array}{ccc} \mathrm{im}(\varphi) & \longrightarrow & \ker(\psi) \\ \nearrow & & \nwarrow \\ \text{Quot.top.} & & \text{Unterraumtopologie} \end{array}$$

ein Homöomorphismus ist.

Bemerkung. Ist G' kompakt und G Hausdorffsch so ist die Folge exakt, wenn sie als Folge abstrakter Gruppen exakt ist. Grund: $\mathrm{im}(\varphi) \to \ker(\psi)$ ist dann bijektiv, stetig und abgeschlossen.

Ist $(G_i)_{i \in I}$ ein projektives System topologischer Gruppen, so ist $\varprojlim G_i$ in natürlicher Weise eine topologische Gruppe.

Satz 1.4. *Sei* $1 \to (G_i') \to (G_i) \to (G_i'') \to 1$ *eine exakte Folge projektiver Systeme kompakter topologischer Gruppen. Dann ist die Folge*

$$1 \longrightarrow \varprojlim G_i' \longrightarrow \varprojlim G_i \longrightarrow \varprojlim G_i'' \longrightarrow 1$$

exakt.

Beweis. Da die projektiven Limiten kompakt sind, genügt es zu zeigen, daß die Folge exakt ist als Folge abstrakter Gruppen. Die Exaktheit von

$$1 \longrightarrow \varprojlim G_i' \longrightarrow \varprojlim G_i \xrightarrow{f} \varprojlim G_i''$$

zeigt man vollkommen analog wie bei R-Moduln. Für

$$(x_i) \in \varprojlim G_i'' \text{ gilt } f^{-1}((x_i)) = \varprojlim_{i \in I} f_i^{-1}(x_i) \neq \varnothing,$$

da die topologischen Räume $f_i^{-1}(x_i)$ kompakt sind. Daher ist f surjektiv. □

Definition. Eine topologische Gruppe heißt proendlich, wenn sie isomorph zum projektiven Limes eines Systems endlicher diskreter Gruppen ist.

Beispiel. Sei K ein lokaler Körper. Dann sind

$$\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\pi^n \quad \text{und} \quad \mathcal{O}_K^\times \cong \varprojlim_n (\mathcal{O}_K/\pi^n)^\times$$

(abelsche) proendliche Gruppen.

Nach 1.2 sind proendliche Gruppen kompakt. Man nennt einen (nichtleeren) topologischen Raum X zusammenhängend, wenn $\varnothing$ und X die einzigen Teilmengen sind, die sowohl offen als auch abgeschlossen sind. Ein Raum X heißt total unzusammenhängend, wenn die einzigen zusammenhängenden Teilmengen von X einelementig sind. Es gilt der

Satz 1.5. *Für eine topologische Gruppe G sind äquivalent*

(i) *G ist proendlich.*
(ii) *G ist kompakt und es gibt eine aus offenen Normalteilern bestehende Umgebungsbasis der $1 \in G$.*
(iii) *G ist kompakt und total unzusammenhängend.*

Für einen Beweis siehe z.B. Neukirch/Schmidt/Wingberg: Cohomology of Number Fields, Proposition (1.1.3).

1.2 Unendliche Galoistheorie

Sei G eine Gruppe und $(U_i)_{i\in I}$ ein durch Inklusion gerichtetes System von Normalteilern (d.h. zu i, j existiert k mit $U_k \subset U_i \cap U_j$). Wir geben G die Topologie mit Basis $\{gU_i \mid g \in G,\ i \in I\}$.

Lemma 1.6. *Wir erhalten eine topologische Gruppe.*

G ist Hausdorffsch $\iff \bigcap_{i\in I} U_i = \{1\}$. □

Sei $L|K$ eine (evtl. unendliche) Galoiserweiterung, d.h. $L|K$ ist algebraisch, separabel und normal, und sei

$$G = \mathrm{Gal}(L|K) := \mathrm{Aut}_K(L)$$

Wir betrachten die Abbildungen

$$\left\{ \begin{array}{c} \text{Untergruppen} \\ H \subset G \end{array} \right\} \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \left\{ \begin{array}{c} \text{Zwischenkörper } M \\ K \subset M \subset L \end{array} \right\}$$

die durch

$$\varphi(H) = L^H = \{x \in L \mid h(x) = x \quad \forall\, h \in H\}$$

und

$$\psi(M) = \mathrm{Gal}(L|M) \subset \mathrm{Gal}(L|K)$$

gegeben sind. In der Algebra-Vorlesung wurde bewiesen:

- $\varphi \circ \psi = \mathrm{id}$, insbesondere ist ψ injektiv.
- $H \subset \varphi(\psi(H))$.
- $\psi(\sigma M) = \sigma\psi(M)\sigma^{-1}$, $\forall\, \sigma \in G$.
- Ist $L|K$ endlich, so ist auch $\varphi \circ \psi = \mathrm{id}$, d.h. wir erhalten eine 1-1 Korrespondenz.

Wir betrachten die gerichtete Menge L_i, $K \subset L_i \subset L$ aller endlichen Galoiszwischenerweiterungen. Da jedes $x \in L$ in einer endlichen Galoiserweiterung von K liegt, gilt

$$L = \varinjlim L_i \quad (= \bigcup L_i).$$

Wir betrachten die Familie von Normalteilern

$$U_i = \mathrm{Gal}(L|L_i) \subset G.$$

Nach 1.6 erhalten wir eine Topologie auf G.

Definition. Die durch die U_i auf $G = \mathrm{Gal}(L|K)$ definierte Topologie heißt die **Krull-Topologie**.

Satz 1.7. $\mathrm{Gal}(L|K)$ *mit der Krull-Topologie ist eine proendliche Gruppe.*

Beweis. Jedes $x \in L$ liegt in einem L_i. Daher ist ein $\sigma \in G = \mathrm{Gal}(L|K)$ durch seine Einschränkung auf die L_i eindeutig bestimmt. Jedes kompatible System von Elementen $\sigma_i \in \mathrm{Gal}(L_i|K)$ definiert ein Element in G. Daher haben wir einen bijektiven Homomorphismus.

$$f : G \xrightarrow{\sim} \varprojlim \mathrm{Gal}(L_i|K)$$

Abstrakter:

$$\begin{aligned} G &= \mathrm{Aut}_K(L) = \mathrm{Hom}_K(L, L) \\ &= \mathrm{Hom}_K(\varinjlim L_i, L) \\ &= \varprojlim \mathrm{Hom}_K(L_i, L) \\ &= \varprojlim \mathrm{Aut}_K(L_i) \\ &= \varprojlim \mathrm{Gal}(L_i|K). \end{aligned}$$

Behauptung: f ist ein Homöomorphismus. Es gilt:

$$\ker(f_i : G \longrightarrow \mathrm{Gal}(L_i|K)) = \mathrm{Gal}(L(L_i) = U_i.$$

Die U_i bilden eine Umgebungsbasis der $1 \in G$ nach Definition der Krulltopoplogie. In $\varprojlim \mathrm{Gal}(L_i|K)$ mit der projektiven Limestopologie bilden die Normalteiler

$$f(U_i) = \ker(\varprojlim \mathrm{Gal}(L_j|K) \longrightarrow \mathrm{Gal}(L_i|K))$$

eine Umgebungsbasis der 1. Daher ist f ein Homöomorphismus. □

Lemma 1.8. *Sei G eine topologische Gruppe.*
(i) Jede offene Untergruppe in G ist auch abgeschlossen.
(ii) Ist $U \subset G$ eine Untergruppe und $V \subset G$ eine nichtleere offene Teilmenge mit $V \subset U$, so ist U offen.
(iii) Ist G kompakt, so hat jede offene Untergruppe endlichen Index und jede abgeschlossene Untergruppe von endlichem Index ist offen.

Beweis. (i) Für jedes $g \in G$ ist gU offen und somit ist $U = G \setminus \bigcup_{g \notin U} gU$ abgeschlossen.
(ii) Sei $v \in V$ und $u \in U$ beliebig. Dann ist $uv^{-1} \cdot V$ eine offene Umgebung von u in $U \Longrightarrow U$ offen.
(iii) Es gilt

$$G = \amalg_{g \in G/H} gH.$$

Ist H offen, folgt $(G : H) < \infty$ da G kompakt. Ist $(G : H) < \infty$, so ist $\bigcup_{g \notin H} gH$ abgeschlossen, also H offen als Komplement einer abgeschlossenen Teilmenge. □

Lemma 1.9. *Sei G eine proendliche Gruppe und $H \subset G$ eine Untergruppe. Dann gilt*

$$\overline{H} = \bigcap_{\substack{U \subset G \text{ offen} \\ H \subset U}} U$$

Beweis. Da offene Untergruppen auch abgeschlossen sind, folgt die Inklusion $\overline{H} \subset \cap U$. Sei $x \notin \overline{H}$. Dann existiert ein offener Normalteiler U mit $xU \cap H = \varnothing$. $\rightsquigarrow x \notin UH$ und UH ist eine offene Untergruppe die H umfaßt. □

Satz 1.10 (Hauptsatz der Galoistheorie, allgemeine Version)**.** *Die Abbildungen φ, ψ definieren eine $1:1$ Korrespondenz zwischen*

$$\left\{ \begin{array}{c} \textit{abgeschl. UG} \\ H \subset G \end{array} \right\} \underset{\psi}{\overset{\varphi}{\longleftrightarrow}} \left\{ \begin{array}{c} \textit{Zwischenk.} \\ K \subset M \subset L \end{array} \right\}$$

Es ist $M|K$ genau dann galoissch, wenn $H = \psi(M)$ Normalteiler in G ist. Dann existiert ein natürlicher topologisches Isomorphismus $\mathrm{Gal}(M|K) \cong G/H$. $M|K$ ist genau dann endlich, wenn $H = \psi(M)$ eine offene Untergruppe ist. Dann gilt $[M : K] = (G : H)$.

Beweis. 1) Sei $M|K$ endlich galoissch. Dann ist $H = \psi(M) = \mathrm{Gal}(L|M)$ nach Definition offen in der Krulltopologie und

$$G/H = \mathrm{Gal}(L|K)/\mathrm{Gal}(L|M) \cong \mathrm{Gal}(M|K)$$

(siehe Beweis von 1.7).
2) Sei $M|K$ endlich und $\tilde{M} \subset L$ die normale Hülle von M. Dann gilt $H = \psi(M) =$

$\mathrm{Gal}(L|M) \supset \mathrm{Gal}(L|\tilde{M})$ und H ist offen nach 1.8. Wenden wir 1) auf $\mathrm{Gal}(L|K)$ und $\mathrm{Gal}(L|M)$ and erhalten wir mit $\tilde{H} = \psi(\tilde{M})$

$$\begin{aligned}(G:H) &= \frac{(G:\tilde{H})}{(\tilde{H}:H)} = \frac{\#\mathrm{Gal}\,(\tilde{M}|K)}{\#\mathrm{Gal}(\tilde{M}|M)} \\ &= \frac{[\tilde{M}:K]}{[\tilde{M}:M]} = [M:K].\end{aligned}$$

3) Sei $M|K$ beliebig und $M = \bigcup M_i$ mit $M_i|K$ endlich. Dann gilt

$$\begin{aligned}H = \psi(M) &= \mathrm{Gal}(L|M) \\ &= \bigcap_i \mathrm{Gal}(L|M_i) \\ &= \text{abgeschlossene Untergruppe.}\end{aligned}$$

4) Ist $M|K$ galoissch und $M = \bigcup M_i$ mit $M_i|K$ endlich galoissch, so haben wir exakte Folgen:

$$0 \longrightarrow \mathrm{Gal}(L|M_i) \longrightarrow \mathrm{Gal}(L|K) \longrightarrow \mathrm{Gal}(M_i|K) \longrightarrow 0.$$

Durch Übergang zum projektiven Limes erhalten wir, da alle Gruppen kompakt sind, die exakte Folge

$$0 \longrightarrow \mathrm{Gal}(L|M) \longrightarrow \mathrm{Gal}(L|K) \longrightarrow \underset{\longleftarrow}{\lim}\,\mathrm{Gal}(M_i|K) \longrightarrow 0$$
$$\underset{\longleftarrow}{\lim}\,\mathrm{Gal}(M_i|K) = \mathrm{Gal}(M|K)$$

5) Sei $H \subset G$ eine beliebige Untergruppe und $M = \varphi(H) = L^H$. Sei $M = \bigcup M_i$, $M_i|K$ endlich. Dann gilt

$$\psi(M) = \mathrm{Gal}(L|M) = \bigcap_i \mathrm{Gal}(L|M_i).$$

Die Gruppen $\mathrm{Gal}(L|M_i)$ durchlaufen alle offenen Untergruppen in G, die H umfassen.

Nach 1.9 folgt $\psi(\varphi(H)) = \overline{H}$. Insbesondere gilt $\psi \circ \varphi(H) = H$ falls H abgeschlossene Untergruppe. □

Definition. Sei K ein Körper und K^s ein separabler Abschluß von K. Dann heißt $G_K = \mathrm{Gal}(K^s|K)$ die **absolute Galoisgruppe** von K.

Es gilt $G_K \cong \underset{\longleftarrow}{\lim}\,\mathrm{Gal}(L|K)$, wobei L die endlichen Galoiserweiterungen von K in K^s durchläuft.

Erinnerung: K^s ist wohlbestimmt bis auf *unkanonischen* Isomorphismus. Wie kanonisch ist G_K?

Definition. Ein Automorphismus der Form $\varphi_g : G \to G,\ h \mapsto ghg^{-1}$, heißt **innerer Automorphismus** der Gruppe G.

Satz 1.11. *G_K ist kanonisch bis auf innere Automorphismen. D.h.:*
Seien L, L' zwei separable Abschlüsse von K und

$$f_1, f_2 : L \xrightarrow{\sim} L'$$

zwei Isomorphismen. Seien $f_1^*, f_2^* : \mathrm{Gal}(L'|K) \longrightarrow \mathrm{Gal}(L|K)$ die induzierten Isomorphismen. Dann existiert ein $g \in \mathrm{Gal}(L|K)$ mit $f_2^* = \varphi_g \circ f_1^*$.

Beweis. Nach Definition gilt für $x \in L$ und $\sigma \in \mathrm{Gal}(L'|K)$:

$$f_i^*(\sigma)(x) = f_i^{-1}(\sigma(f_i(x)).$$

Sei nun $g = f_2^{-1} \circ f_1 \in \mathrm{Aut}_K(L) = \mathrm{Gal}(L|K)$. Dann gilt für jedes $\sigma \in \mathrm{Gal}(L'|K)$:

$$\begin{aligned} f_2^*(\sigma) &= f_2^{-1} \circ \sigma \circ f_2 \\ &= f_2^{-1} \circ f_1 \circ f_1^{-1} \circ \sigma \circ f_1 \circ f_1^{-1} \circ f_2 \\ &= g \cdot f_1^*(\sigma) g^{-1} = \varphi_g(f_1^*(\sigma)) \end{aligned}$$

□

Satz 1.12. *Sei $\mathbb{F}_q$, $q = p^f$, ein endlicher Körper. Dann gibt es einen kanonischen Isomorphismus*

$$\varphi : \hat{\mathbb{Z}} \xrightarrow{\sim} G_{\mathbb{F}_q},$$

der $1 \in \hat{\mathbb{Z}}$ auf den Frobeniusautomorphismus F_q abbildet ($F_q(x) = x^q$).

Beweis. Sei $\overline{\mathbb{F}}_q$ ein separabler Abschluß von $\mathbb{F}_q$. Nach Algebra-Vorlesung gibt es zu jedem $n \in \mathbb{N}$ genau eine Zwischenerweiterung $\mathbb{F}_{q^n} \subset \overline{\mathbb{F}}_q$ vom Grad n, sowie einen natürlichen Isomomorphismus

$$\varphi_n : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q), 1 + n\mathbb{Z} \longmapsto F_q : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}.$$

Daher erhalten wir einen Isomorphismus projektiver Systeme

$$(\mathbb{Z}/n\mathbb{Z})_{n\in\mathbb{N}} \xrightarrow{(\varphi_n)}_{\sim} (\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}))_{n\in\mathbb{N}},$$

wobei $\mathbb{N}$ multiplikativ geordnet ist. Der Übergang zum projektiven Limes gibt uns den Isomorphismus

$$\varphi : \hat{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q).$$

Da $\hat{\mathbb{Z}}$ und daher auch $\mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$ kommutativ ist und also keine inneren Automorphismen hat, ist φ nach 1.11 kanonisch. □

Korollar 1.13 (siehe AZTI, 8.64)**.** *Sei K ein lokaler Körper und K^{nr} die maximale unverzweigte Erweiterung von K. Dann gibt es einen Isomorphismus proendlicher Gruppen*

$$\hat{\mathbb{Z}} \xrightarrow{\sim} G(K^{\mathrm{nr}}|K),$$

welcher $1 \in \hat{\mathbb{Z}}$ auf den Frobeniushomomorphismus F von $K^{\mathrm{nr}}|K$ schickt (dieser ist durch $F(x) \equiv x^q \bmod \pi$ charakterisiert, wobei $q = \#\mathcal{O}_K/\pi$).

Es gilt der folgende tiefliegende

Satz (Neukirch/Uchida). Sind K, L Zahlkörper und $G_K \cong G_L$, so gilt $K \cong L$.

Moral: G_K „kennt“ K und enthält wichtige arithmetische Informationen.