Inhaltsverzeichnis

Kapitel 1

Topologische Gruppen

1.1 Topologische Gruppen

1.1.1 Definition: Topologische Gruppen

Ein Paar $(G, \mathcal{T})$ einer Gruppe und einer Topologie auf G heißt **topologische Gruppe**, wenn die Abbildungen

$$\begin{aligned} \_ \cdot \_ : G \times G &\longrightarrow G \\ \_^{-1} : G &\longrightarrow G \end{aligned}$$

stetig sind.
Unter einem **Homomorphismus topologischer Gruppen** verstehen wir einen stetigen Gruppenhomomorphismus.

1.1.2 Bemerkung

Seien G, H topologische Gruppen.

- $U \subset G$ heißt **Umgebung** von $g \in G$, falls eine Teilmenge $V \subset_o G$ existiert, sodass $g \in V \subseteq U$.
- $\phi : G \to H$ ist genau ein Homomorphismus, wenn das Urbild jeder Umgebung der 1 in H eine Umgebung der 1 in G ist.

1.1.3 Proposition

Sei G eine topologische Gruppe und $U \subset G$ eine Umgebung der 1.

(i) Es existiert eine offene Umgebung V der 1, sodass $V \cdot V \subset U$ und $V = V^{-1}$.

(ii) Es existiert eine Umgebung V der 1, deren Abschluss $\overline{V}$ in U enthalten ist.

Sei nun $H \leq G$ eine Untergruppe.

(iii) Der Abschluss von H ist ebenfalls eine Untergruppe. Dieser ist insbesondere normal, falls H ebenfalls normal ist.

(iv) Ist $H \leq_o G$ offen, so auch abgeschlossen, also insbesondere eine Zusammenhangkomponente.

Beweis

(i) Definiere

$$f : G \to G, x \mapsto x^2$$
$$V' := f^{-1}(U) \cap U$$
$$V := V' \cap V'^{-1}$$

(ii) Wir geben ohne Beweis einen Satz an, aus dem die Behauptung sofort folgt:

Satz von Weil Eine topologische Gruppe G ist $\mathrm{T}_{3\frac{1}{2}}$, d. h., ist $A \subseteq_a G$ eine Teilmenge, die die 1 nicht enthält, so existiert eine stetige Abbildung $f : G \to [0,1] \subset \mathbb{R}$ mit folgenden Eigenschaften:

- $f(A) = \{1\}$
- $f(1) = 0$

(iii) Seien $a, b \in \overline{H}$, dann existieren Folgen $a_n, b_n \in H$, die gegen a, b konvergieren. Dann ist (a_n, b_n^{-1}) eine Folge in $G \times G$, die gegen (a, b^{-1}) konvergiert. Da Multiplikation stetig ist, konvergiert $a_n b_n^{-1} \in H$ gegen ab^{-1}, ergo liegt ab^{-1} in $\overline{H}$. Analog zeigt man, dass $\overline{H}$ normal ist, falls H normal ist.

(iv) Sei $H \leq_o G$ offen und sei $a \in \overline{H}$. Dann existiert eine Folge $a_n \in H$, die gegen a konvergiert. aH ist eine Umgebung von a, ergo existiert ein $N \in \mathbb{N}$, sodass $a_n \in aH$. Daraus folgt $a \in a_n H^{-1} = H$.

□

1.1.4 Proposition

Sei G eine topologische Gruppe. Dann sind folgende Aussagen äquivalent:

(i) G ist hausdorffsch.

(ii) $\{1\}$ ist abgeschlossen in G.

(iii) $\{g\}$ ist abgeschlossen in G für alle $g \in G$.

Beweis
Es bleibt die Implikation (iii) $\implies$ (i) zu zeigen. Seien $g, h \in G$ verschieden. Dann ist $U = G \setminus \{gh^{-1}\}$ offen in G. Laut Proposition 1.1.3 (i) existiert eine offene Teilmenge V von U mit folgenden Eigenschaften:

- $1 \in V$
- $VV \subset U$
- $V^{-1} = V$

Dann sind Vg, Vh disjunkte Umgebungen von g, h. Denn wäre ihr Schnitt nichtleer, so würden $v, w \in V$ existieren, sodass $vg = wh$, woraus folgt dass gh^{-1} in U liegen würde. □

1.1.5 Proposition

Sei G eine topologische Gruppe und $H \leq G$ eine Untergruppe.

(i) H ist genau dann diskret, wenn H einen isolierten Punkt besitzt.

(ii) Ist G hausdorffsch und H diskret, so ist H abgeschlossen.

Beweis: (ii)
H ist diskret, d. h., es existiert eine offene Teilmenge $V \subseteq_o G$, s. d. $V \cap H = \{1\}$. Ohne Einschränkung darf angenommen werden, dass $V = V^{-1}$.
G ist hausdorffsch, ergo ist $\{1\}$ abgeschlossen in V. Sei $x \in \overline{H}$, dann existiert ein $y \in H$, das in xV liegt. Man erhält durch Umformung

$$x \in yV \cap \overline{H} = \bigcap_{H \subset A \subset_a G} A \cap yV = \bigcap_{\{y\} = H \cap yV \subset A \subset_a yV} A = \{y\}$$

Ergo gilt $x = y \in H$. □

1.1.6 Proposition

Sei G eine topologische Gruppe mit Untergruppe H.

- G operiert stetig auf G/H.
- $\pi_H : G \to G/H$ ist eine offene Abbildung.
- G/H ist genau dann hausdorffsch, wenn H abgeschlossen ist.
- G/H ist genau dann diskret, wenn H offen ist.
- Ist H normal, so ist G/H eine topologische Gruppe und π_H ein Morphismus topologischer Gruppen.

Beweis: (iii)
$\Longrightarrow$: Sei $a \in \overline{H}$, dann existiert eine Folge $a_n \in H$, die gegen a konvergiert. Da π_H stetig ist, gilt

$$\pi_H(a_n) \overset{n \to \infty}{\longrightarrow} \pi_H(a)$$

Da alle a_n in H liegen, gilt aber $\pi_H(a_n) = \pi_H(1)$. Da G/H hausdorffsch ist, besitzt diese Folge höchstens einen Grenzwert, ergo gilt

$$\pi_H(a) = \pi_H(1) \Longrightarrow a \in H$$

$\Longleftarrow$: Seien $\pi_H(b), \pi_H(c) \in G/H$. Ohne Einschränkung nehmen wir an, dass $\pi_H(c) = \pi_H(1)$.
In jeder Umgebung $\widetilde{U}$ von $\pi_H(b)$ sei $\pi_H(1)$ enthalten. Dann ist b im Abschluss von H enthalten, denn ist U eine Umgebung von b, so ist $\pi(U)_H$ eine Umgebung von $\pi_H(b)$. Ergo ist $\pi_H(1) \in \pi_H(U)$, ergo existiert ein $h \in H$, sodass $h \in U$. □

1.1.7 Definition

Ist G eine topologische, so ist $\overline{\{1\}}$ normal. $G/\overline{\{1\}}$ wird als **Hausdorffquotient** von G bezeichnet.

1.1.8 Definition

Ein Homomorphismus $\phi : G \to G'$ topologischer Gruppen heißt **strikt**, falls er den Isomorphiesatz respektiert, d. h., die induzierte Abbildung

$$\phi : G/\mathsf{Kern}\phi \longrightarrow \mathsf{Bild}\phi$$

ist homöomorph.

1.1.9 Definition

Eine kurze exakte Sequenz topologischer Gruppen heißt **topologisch exakt**, falls alle beteiligten Abbildungen strikt sind.

1.2 Lokal-Kompakte Gruppen

1.2.1 Definition

Sei X ein topologischer Raum.

- Wir nennen X **kompakt**, falls er **quasikompakt** ist, d. h., jede offene Überdeckung von X besitzt eine offene Teilüberdeckung.
- X heißt **lokal kompakt**, falls jeder Punkt eine Umgebung enthält, deren Abschluss kompakt ist.

1.2.2 Bemerkung

- Jede abgeschlossene Teilmenge eines kompakten Raumes ist kompakt.
- Jede kompakte Menge eines Hausdorffraums ist abgeschlossen.
- Ist ein Raum kompakt und hausdorffsch, so erfüllt er **T3**, d. h., er ist **regulär**, d. h., jede abgeschlossene Teilmenge und jeder nicht in dieser Teilmenge liegender Punkt könne durch offene Umgebungen getrennt werden.
- Ein Raum ist genau dann regulär, wenn jeder Punkt eine Umgebungsbasis aus abgeschlossenen Umgebungen besitzt.
- In lokal kompakten Räumen hat jeder Punkt eine Umgebungsbasis aus kompakten Umgebungen.
- Ist ein Raum kompakt und hausdorffsch, so erfüllt er **T4**, d. h., er ist **normal**, d. h., disjunkte abgeschlossene Teilmengen werden durch offene Umgebungen getrennt.
- Eine bijektive, stetige Abbildung von einem Kompaktum nach einem Hausdorffraum ist homöomorph.

1.2.3 Proposition

Sei G eine lokal kompakte Gruppe, $H \leq G$ eine abgeschlossene Gruppe.

- G/H ist ein lokal kompakter Raum.
- Jede kompakte Teilmenge von G/H besitzt ein kompaktes Urbild.

1.2.4 Proposition

Sei G lokal kompakt und hausdorffsch, $H \leq G$ eine Untergruppe.
H ist genau dann diskret, wenn $H \cap K$ für alle kompakten Teilmengen von $K \subset G$ endlich ist.

1.3 Zusammenhangkomponenten

1.3.1 Definition

Ein topologischer Raum heißt **zusammenhängend**, wenn er sich nicht in zwei offene, disjunkte, nichtleere Teilräume zerlegen lässt.

1.3.2 Bemerkung

- Ist eine Teilmenge eines Raumes zusammenhängend, so ist es auch ihr Abschluss.
- Seien $A_i \subset X$ jeweils zusammenhängend, dann gilt
$$\bigcap_{i\in I} A_i \neq \emptyset \Longrightarrow \bigcup_{i\in I} A_i \text{ ist zusammenhängend}$$
- Beliebige Produkte zusammenhängender Räume sind zusammenhängend.
- Bilder zusammenhängender Räume bleiben unter stetigen Abbildungen zusammenhängend.

1.3.3 Definition

Sei X ein topologischer Raum.

- Ist $x \in X$ ein Punkt, so verstehen wir unter der **Zusammenhangkomponente** von x die größte, zusammenhängende Teilmenge von X, die x enthält.
- X heißt **total unzusammenhängend**, wenn jede Zusammenhangkomponente genau ein Element enthält.
- Ist G eine topologische Gruppe, so bezeichnen wir mit G^o die Zusammenhangkomponente der Eins.

1.3.4 Proposition

Ist G eine topologische Gruppe, so ist G^o ein abgeschlossener Normalteiler.

1.3.5 Proposition

Sei G eine topologische Gruppe, $H \leq G$ eine Untergruppe. Sind H und G/H zusammenhängend, so auch G.

1.3.6 Proposition

Sei G eine topologische Gruppe, dann ist G/G^o hausdorffsch und total unzusammenhängend.

1.3.7 Bemerkung

Eine total unzusammenhängende Gruppe ist hausdorffsch.

1.4 Total Unzusammenhängende Gruppen

1.4.1 Satz

Eine hausdorffsche Gruppe ist genau dann total unzusammenhängend und lokal kompakt, wenn jede Umgebung der Eins eine offene und kompakte Untergruppe enthält.

1.4.2 Lemma

Sei X ein kompakter und total unzusammenhängender Hausdorffraum. Bezeichnet $\mathcal{W}$ für $x \in X$ die Menge der Umgebungen von x, die zugleich offen und abgeschlossen sind, so gilt
$$\bigcap_{W\in\mathcal{W}} W = \{x\}$$

1.4.3 Lemma

Sei G eine lokal kompakte und total unzusammenhängende Gruppe, U eine offene Umgebung von $x \in G$.
Dann existiert eine offene und kompakte Umgebung von x, die in U enthalten ist.

1.4.4 Korollar

Sei G eine kompakte und total unzusammenhängende Gruppe. Dann enthält jede Umgebung der Eins einen offenen Normalteiler.

1.5 Limiten Topologischer Räume

1.5.1 Definition: Gerichtet Geordnet

Sei I eine nichtleere Menge.

- $(I, \leq)$ heißt **teilgeordnet**, falls $\leq$ auf I eine binäre Relation ist, die reflexiv und transitiv ist.
- Eine teilgeordnete Menge $(I, \leq)$ heißt **gerichtet**, falls für jedes Paar $i, j \in I$ ein $k \in I$ existiert, sodass $i \leq k$ und $j \leq k$.

1.5.2 Definition: Inverses System

Sei I gerichtet.

- Ein **inverses System** (X_i, ϕ_{ij}) topologischer Räume ist ein kontravarianter Funktor $X : I \to$ **Top**, d. h., die X_i sind topologische Räume und für jedes $i \leq j$ ist
$$\phi_{ij} : X_j \longrightarrow X_i$$
eine stetige Abbildung.
- Ein Morphismus inverser Systeme ist eine natürliche Transformation von inversen Systemen.
- Ist X ein topologische Raum, so verstehen wir unter (X, id_X) das **konstante System** zu X.

1.5.3 Definition: Projektiver Limes

Ein **projektiver bzw. inverser Limes** eines inversen Systemes (X_i, ϕ_{ij}) ist ein topologischer Raum
$$X = \lim_{i \in I}(X_i, \phi_{ij}) =: \lim_{i \in I} X_i$$
der den Funktor
$$\begin{aligned} \mathbf{Top} &\longrightarrow \mathbf{Set} \\ Y &\longmapsto \mathsf{Hom}_{\text{inv.Sys.}}\left((Y, \mathsf{id}_Y), (X_i, \phi_{ij})\right) \end{aligned}$$
darstellt, d. h.,
$$\mathsf{Hom}_{\mathbf{Top}}\left(Y, X\right) \cong \mathsf{Hom}_{\text{inv.Sys.}}\left((Y, \mathsf{id}_Y), (X_i, \phi_{ij})\right)$$

1.5.4 Bemerkung

- Ein Limes ist eindeutig bis auf eindeutige Isomorphie.
- Folgendes Konstrukt ist ein Limes von (X_i, ϕ_{ij})

$$X := \left\{ (x_k) \in \prod_{i \in I} X_i \mid \phi_{ij}(x_i) = x_j \forall i \leq j \right\}$$

- Es gilt

$$X = \bigcap_{i \leq j} \left\{ (x_k) \in \prod_{i \in I} X_i \mid \phi_{ij}(x_i) = x_j \right\}$$

1.5.5 Proposition

Sei (X_i, ϕ_{ij}) ein inverses System topologischer Räume mit stetigen Abbildungen

$$\phi_i : X_i \longrightarrow X := \lim_{i \in I} X_i$$

- Die ϕ_i^{-1} bilden für alle i und $U \subseteq_o X_i$ eine Basis der Topologie von X.
- Eine Teilmenge $Y \subset X$ mit $\phi_i(Y) = X_i$ für alle $i \in I$ liegt dicht in X.
- Eine Abbildung $f : X \to Y$ ist genau dann stetig, wenn für alle $i \in I$ $\phi_i \circ f$ stetig ist.

1.5.6 Proposition

Sei (X_i, ϕ_{ij}) ein inverses System topologischer Räume mit Limes X.

- Sind alle X_i hausdorffsch, so ist dies auch X.
- Sind alle X_i total unzusammenhängend, so auch X.
- Sind alle X_i hausdorffsch, so ist

$$\left\{ (x_k) \in \prod_{i \in I} X_i \mid \phi_{ij}(x_i) = x_j \forall i \leq j \right\}$$

  eine abgeschlossene Teilmenge von $\prod_{i \in I} X_i$.
- Sind alle X_i kompakt und hausdorffsch, so ist es auch X.
- Sind alle X_i nichtleer, kompakt und hausdorffsch, so ist dies auch X.

1.5.7 Proposition

Seien folgende Morphismen inverser Systeme von kompakten und hausdorffschen Gruppen gegeben

$$(F_i, \upsilon_{ij}) \xrightarrow{\alpha} (G_i, \phi_{ij}) \xrightarrow{\beta} (H_i, \chi_{ij})$$

Ist diese Sequenz gradweise exakt, d. h., ist für alle $i \in I$

$$F_i \xrightarrow{\alpha_i} G_i \xrightarrow{\beta_i} H_i$$

exakt, so ist auch die Limessequenz

$$\lim_{i \in I} F_i \xrightarrow{\alpha} \lim_{i \in I} G_i \xrightarrow{\beta} \lim_{i \in I} H_i$$

exakt.

1.5.8 Definition: Kolimes

Sei I gerichtet.

- Ein **direktes System** topologischer Räume ist ein kovarianter Funktor

$$X : I \longrightarrow \mathbf{Top}$$

- Morphismen direkter System sind natürliche Transformationen der zugrunde liegenden Funktoren.

- Ein **Kolimes** eines direkten Systemes (X_i, ϕ_{ij}) ist ein topologischer Raum $X = \mathsf{colim}_{i\in I} X_i$, der den Funktor

$$Y \longmapsto \mathsf{Hom}\left((X_i, \phi_{ij}), (Y, \mathsf{id}_Y)\right)$$

  darstellt.

1.5.9 Bemerkung

Ist (X_i, ϕ_{ij}) ein direktes System, so ist folgender Kolimes gegeben

$$\coprod_{i\in I} X_i / \sim$$

wobei

$$x_i \sim x_j \Longleftrightarrow \exists k \geq i, j : \phi_{ik}(x_i) = \phi_{jk}(x_j)$$

1.6 Proendliche Gruppe

1.6.1 Bemerkung

Jede endliche Gruppe wird als eine topologische Gruppe aufgefasst, indem wir sie mit der diskreten Topologie versehen.

1.6.2 Definition

Eine topologische Gruppe heißt **proendlich**, wenn sie ein projektiver Limes eines inversen Systems endlicher Gruppen ist.

1.6.3 Satz

Sei G eine topologische Gruppe. Folgende Aussagen sind äquivalent:

- G ist proendlich.

- G ist kompakt und total unzusammenhängend.

- G ist kompakt und

$$\bigcap_{N \trianglelefteq_o G} N = \{1\}$$

1.6.4 Lemma

Sei G eine topologische Gruppe, I eine Familie abgeschlossener Normalteiler, sodass gilt

$$N_1, N_2 \in I \Longrightarrow \exists N_3 \in I : N_3 \subseteq N_1 \cap N_2$$

- Definiere für $N_1, N_2 \in I$
$$N_1 \preceq N_2 \Longleftrightarrow N_1 \supseteq N_2$$
Dann ist $(I, \preceq)$ gerichtet.
- Setzt man für $N_i \preceq N_j$
$$\phi_{ij} : G/N_j \longrightarrow G/N_i$$
so ist $(G/N_i, \phi_{ij})$ ein inverses System.
Definiere
$$\widehat{G} := \lim_{N \in I} G/N$$
Es existiert ein kanonischer Morphismus stetiger Gruppen
$$\upsilon : G \longrightarrow \widehat{G}$$
mit Kern
$$\mathsf{Kern}\upsilon = \bigcap_{N \in I} N$$
- Ist G kompakt, so ist υ surjektiv.

1.7 Unendliche Galoistheorie

1.7.1 Satz

Sei $L|K$ eine galoissche, nicht notwendigerweise endliche Körpererweiterung. Definiere

$$G(L|K) := \mathsf{Aut}_{K-\text{Alg.}}(L)$$

$G(L|K)$ erhält eine Topologie als Gruppe, indem wir Untergruppen der Gestalt

$$G(L|E)$$

für alle endlichen, galoisschen Teilerweiterungen $E|K$ zu einer Umgebungsbasis der Eins in $G(L|K)$ zusammenfassen. Es gilt dann

$$G = \lim_{\substack{L|E|K \\ E|K \text{ endl., gal.}}} G(E|K)$$

1.7.2 Satz: Satz der Unendlichen Galoistheorie

Für eine galoissche Körpererweiterung K herrschen folgende Dualitäten vor

$$\begin{array}{ccc}
\{L|E|K \text{ galoissche Zwischenerweiterung}\} & \longleftrightarrow & \{U \subseteq_{\text{abg}} G\} \\
\uparrow & & \uparrow \\
\{L|E|K\text{endliche, galoissche Zwischenerweiterung}\} & \longleftrightarrow & \{U \subseteq_o G\}
\end{array}$$

durch

$$E \longmapsto G(L|E)$$
$$H \longmapsto L^H$$

Kapitel 2

Klassenkörpertheorie – Motivation und Hauptresultate

2.1 Abelsche Erweiterungen von $\mathbb{Q}$

2.1.1 Satz: Kroncker-Weber

Sei $L|\mathbb{Q}$ eine endliche Erweiterung. Folgende Aussagen sind äquivalent:

- $L|\mathbb{Q}$ ist abelsch.
- L ist enthalten in einem Kreisteilungskörper $\mathbb{Q}(\mu_n)$.

2.1.2 Satz

Sei $N \in \mathbb{N}$, $L|\mathbb{Q}$ endlich. Folgende Aussagen sind äquivalent:

- $L \subseteq \mathbb{Q}(\mu_N)$.
- Ob eine Primzahl p in L voll zerlegt ist, hängt nur von $p \mod n$ ab.

2.1.3 Satz

Sei $L|\mathbb{Q}$ abelsch und N minimal mit

$$L \subseteq \mathbb{Q}(\mu_N)$$

Für jede Primzahl p gilt

$$p \text{ ist in } L \text{ verzweigt} \Longleftrightarrow p|N$$

2.1.4 Satz

Sei $N \in \mathbb{N}$ und $H \subseteq (\mathbb{Z}/N\mathbb{Z})^\times \cong G(\mathbb{Q}(\mu_N)/\mathbb{Q})$ beliebig. Es bezeichne $L = \mathbb{Q}(\mu_N)^H$.
Für $p \not| N$ prim gilt:

- p ist unverzweigt in L.
- p ist genau dann voll zerlegt in L, wenn $p \mod N \in H$.
- Ist f die kleinste natürliche Zahl, die

  $$p^f \mod N \in H$$

  erfüllt, so ist $p\mathcal{O}_L$ ein Produkt von $[L : \mathbb{Q}]/f$ verschiedenen Primidealen.

2.1.5 Proposition

Sei $L|K$ galoissch und $\mathfrak{P}|\mathfrak{p}$ unverzweigte Stellen in $\mathcal{O}_L|\mathcal{O}_K$. Es bezeichne $\lambda = \mathcal{O}_L/\mathfrak{P}$ und $\kappa = \mathcal{O}_K/\mathfrak{p}$ die korrespondierenden Restklassenkörper. Dann ist $G_{\mathfrak{P}} := G(\lambda|\kappa) \overset{\iota}{\hookrightarrow} G(L|K)$ zyklisch und wird vom **Frobeniusautomorphismus**

$$\begin{aligned} \phi_q : \lambda &\longrightarrow \lambda \\ x &\longmapsto x^q \end{aligned}$$

erzeugt, wobei $q = \#\kappa$. Definiere für $\sigma \in G(L|K)$

$$\mathsf{Frob}_{\mathfrak{p},\mathfrak{P}} := \iota(\phi_q) \text{ und } \mathsf{Frob}_{\mathfrak{p},\sigma(\mathfrak{P})} := \sigma \mathsf{Frob}_{\mathfrak{p},\mathfrak{P}} \sigma^{-1}$$

und folgende Äquivalenzklasse

$$\mathsf{Frob}_{\mathfrak{p}} := \mathsf{Frob}_{\mathfrak{p},L} := \left\{ \mathsf{Frob}_{\mathfrak{p},\sigma(\mathfrak{P})} \mid \sigma \in G(L|K) \right\} \subset G(L|K)$$

Dann gilt

- Es gilt $\mathsf{Frob}_{\mathfrak{p}} = \{1\}$ genau dann, wenn $\mathfrak{p}$ total zerlegt in $L|K$ ist.
- Es gilt
$$\#\{\mathfrak{P}'|\mathfrak{p}\} = \frac{\#G(L|K)}{\#G_{\mathfrak{P}'}}$$
- Ist $L|K$ abelsch, so besteht $\mathsf{Frob}_{\mathfrak{p}}$ aus dem eindeutig bestimmten Element, das auf λ die Abbildung $x \mapsto x^q$ induziert.
- Ist $L'|K$ eine galoissche Zwischenerweiterung, so gilt
$$\mathsf{Frob}_{\mathfrak{p},L} \overset{res}{\twoheadrightarrow} \mathsf{Frob}_{\mathfrak{p},L'}$$

2.1.6 Proposition

Es gelte $p \nmid N$. Dann ist p unverzweigt in $\mathbb{Q}(\mu_N)$ und es herrscht folgende Isomorphie vor

$$\begin{aligned} \chi_{cyc,N} : G(\mathbb{Q}(\mu_N)|\mathbb{Q}) &\xrightarrow{\cong} (\mathbb{Z}/NZ)^\times \\ \mathsf{Frob}_p &\longmapsto p \mod N \end{aligned}$$

2.2 Quadratische Erweiterungen

2.2.1 Proposition

Sei m eine quadratfreie ganze Zahl. Dann ist $\mathbb{Q}(\sqrt{m})|\mathbb{Q}$ abelsch. Setzt man

$$N := \begin{cases} |m| & m \equiv 1 \mod 4 \\ 4\,|m| & m \equiv 2,3 \mod 4 \end{cases}$$

so ist N minimal mit der Eigenschaft

$$\mathbb{Q}(\sqrt{m}) \subset \mathbb{Q}(\mu_N)$$

2.2.2 Definition: Legendre-Symbol

Sei $p > 2$ eine ungerade Primzahl und $a \in \mathbb{Z}$ beliebig. Definiere das **Legendre-Symbol** durch

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & p \nmid a \text{ und } a \in (\mathbb{Z}/p\mathbb{Z}^\times)^2 \\ 0 & p \mid a \\ -1 & p \nmid a \text{ und } a \notin (\mathbb{Z}/p\mathbb{Z}^\times)^2 \end{cases}$$

wobei $(\mathbb{Z}/p\mathbb{Z}^\times)^2 = \left\{x^2 \mid 0 \neq x \in \mathbb{Z}/p\mathbb{Z}\right\}$ die Quadratzahlen modulo p bezeichnet.
Die Abbildung $\left(\frac{\cdot}{p}\right) : \mathbb{Z}/p\mathbb{Z}^\times \to \{\pm 1\}$ ist multiplikativ, weswegen folgende kurze exakte Sequenz vorliegt

$$1 \longrightarrow (\mathbb{Z}/p\mathbb{Z}^\times)^2 \hookrightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{\left(\frac{\cdot}{p}\right)} \{\pm 1\} \longrightarrow 1$$

Ferner gilt

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$$

2.2.3 Proposition: Trivialer Zerlegungssatz

Sei m quadratfrei und p eine ungerade Primzahl, die teilerfremd zu p ist. Es gilt

$$p \text{ ist voll zerlegt in } \mathbb{Q}(\sqrt{m}) \Longleftrightarrow \left(\frac{m}{p}\right) = 1$$

2.2.4 Definition: Dirichlet-Charaktere

Sei m quadratfrei. Setze

$$N := \begin{cases} |m| & m \equiv 1 \mod 4 \\ 4\,|m| & m \equiv 2,3 \mod 4 \end{cases}$$

- Unter einem **Dirichlet-Charakter** verstehen wir einen Gruppenhomomorphismus

  $$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

- Ein Dirichlet-Charakter χ heißt **primitiv**, falls es kein $d \in \{1, \dots, m-1\}$ gibt, für welches χ über

  $$(\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/d\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$$

  faktorisiert.

- Definiere

  $$\begin{aligned} \chi_m : (\mathbb{Z}/N\mathbb{Z})^\times &\longrightarrow \{\pm 1\} \subset \mathbb{C}^\times \\ a &\longmapsto \Theta_m(a) \cdot \prod_{\substack{e \mid m \\ e>2 \text{ prim}}} \left(\frac{a}{e}\right) \end{aligned}$$

  wobei

  $$\Theta_m(a) := \begin{cases} 1 & m \equiv 1 \mod 4 \\ 1 & m \equiv 3 \mod 4 \text{ und } a \equiv 1 \mod 4 \\ -1 & m \equiv 3 \mod 4 \text{ und } a \not\equiv 1 \mod 4 \\ 1 & m \equiv 2 \mod 4 \text{ und } a \equiv 1 \text{ oder } 1-m \mod 4 \\ -1 & m \equiv 2 \mod 4 \text{ und } a \not\equiv 1 \text{ oder } 1-m \mod 4 \end{cases}$$

2.2.5 Lemma

Sei m quadratfrei. Setze

$$N := \begin{cases} |m| & m \equiv 1 \mod 4 \\ 4\,|m| & m \equiv 2,3 \mod 4 \end{cases}$$

Dann gilt

- χ_m ist primitiv.
- $$\chi_m(-1) = \begin{cases} 1 & m > 0 \\ -1 & m < 0 \end{cases}$$

2.2.6 Definition: Gaußsche Summen

Sei $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ ein Dirichlet-Charakter und ζ_N eine primitive N-te Einheitswurzel. Definiere die **Gaußsche Summe** von χ und ζ_N durch

$$G(\chi, \zeta_N) := \sum_{a \in \mathbb{Z}/N\mathbb{Z}^\times} \chi(a)\zeta_N^a$$

Bezeichne mit $\overline{\chi}$ den komplex konjugierten Charakter von χ.

2.2.7 Satz

Sei χ primitiv. Dann gilt

- Für alle $n \in \mathbb{Z}$ gilt
$$G(\chi, \zeta_N^n) = \overline{\chi}(n) G(\chi, \zeta_N)$$
- $|G(\chi, \zeta_N)| = \sqrt{N}$
- Ist m quadratfrei und gilt für N
$$N = \begin{cases} |m| & m \equiv 1 \mod 4 \\ 4\,|m| & m \equiv 2,3 \mod 4 \end{cases}$$
dann folgt
$$G(\chi_m, \zeta_N)^2 = \begin{cases} m & m \equiv 1 \mod 4 \\ 4m & m \equiv 2,3 \mod 4 \end{cases}$$

2.2.8 Satz

Sei m quadratfrei und $N = \begin{cases} |m| & m \equiv 1 \mod 4 \\ 4\,|m| & m \equiv 2,3 \mod 4 \end{cases}$. Dann kommutiert folgendes Diagramm

$$\begin{tikzcd} G(\mathbb{Q}(\mu_N)|\mathbb{Q}) \arrow[r, "\chi_{cyc,N}", "\cong"'] \arrow[d, two heads, "res"'] & (\mathbb{Z}/N\mathbb{Z})^\times \arrow[d, "\chi_m"] \\ G(\mathbb{Q}(\sqrt{m})/\mathbb{Q}) \arrow[r, "\sigma \mapsto \frac{\sigma(\sqrt{m})}{\sqrt{m}}"] & \{\pm 1\} \end{tikzcd}$$

2.2.9 Satz

Sei m quadratfrei und $N = \begin{cases} |m| & m \equiv 1 \mod 4 \\ 4\,|m| & m \equiv 2,3 \mod 4 \end{cases}$
p sei eine zu N teilerfremde Primzahl. Es gilt

$$p \text{ ist voll zerlegt in } \mathbb{Q}(\sqrt{m}) \Longleftrightarrow \chi_m(p) = 1$$

2.2.10 Satz: Gaußsches Quadratisches Reziprozitätsgesetz

Für zwei ungerade, verschiedene Primzahlen p, q gilt

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} \left(\frac{p}{q}\right)$$

Ergänzungssätze

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ und } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

2.2.11 Definition

Sei K ein Zahlkörper. Ein Element $a \in K^\times$ heißt **total positiv**, falls für alle reellen Stellen $\iota : K \hookrightarrow \mathbb{R}$ gilt

$$\iota(a) > 0$$

2.2.12 Satz: Strahlklassenkörper

Sei K ein Zahlkörper und $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal.

- Es existiert genau eine endliche Körpererweiterung $K(\mathfrak{a})|K$, die folgende Eigenschaften für jedes Ideal $\mathfrak{p} \subset \mathcal{O}_K$ erfüllt

  - $\mathfrak{p} \nmid \mathfrak{a} \Longrightarrow \mathfrak{p}$ ist unverzweigt in $K(\mathfrak{a})$.
  - $\mathfrak{p}$ zerlegt sich voll in $K(\mathfrak{a}) \Longleftrightarrow$ es existiert ein total positives $\alpha \in 1 + \mathfrak{a}$ mit $\mathfrak{p} = (\alpha)$.

  Wir nennen in diesem Fall $K(\mathfrak{a})$ den **Strahlklassenkörper** $\mod \mathfrak{a}$.

- $K(\mathfrak{a})/K$ ist abelsch und jede endliche abelsche Erweiterung ist in einem Strahlklassenkörper enthalten.

- $\mathfrak{b} \subset \mathfrak{a} \Longleftrightarrow K(\mathfrak{b}) \supset K(\mathfrak{a})$

- Für jede endliche abelsche Erweiterung $L|K$ existiert ein Ideal $\mathfrak{f} \subset \mathcal{O}_K$, das maximal ist mit der Eigenschaft $L \subset K(\mathfrak{f})$. Dieses Ideal nennen wir den **Führer** der Erweiterung $L|K$.
  Für jedes Ideal $\mathfrak{p} \subset \mathcal{O}_K$ gilt:
  $$\mathfrak{p} \text{ verzweigt in } L \Longleftrightarrow \mathfrak{p}|\mathfrak{f}$$

2.3 Abstrakte bzw. Axiomatische Klassenkörpertheorie

2.3.1 Definition: Stetiger G-Modul

Sei K ein Körper und $G := G_K := G(\overline{K}|K)$ die Galoisgruppe der maximalen separablen Erweiterung von K.
Eine abelsche, multiplikativ geschriebene Gruppe A heißt **stetiger G-Modul**, falls eine stetige Rechtswirkung von G

$$\begin{aligned} G \times A &\longrightarrow A \\ (\sigma, a) &\longmapsto a^\sigma \end{aligned}$$

gegeben ist, wobei A hierbei mit der diskreten Topologie und G mit der proendlichen Topologie ausgestattet wird, sodass folgende Eigenschaften erfüllt werden:

- $a^1 = a$
- $(ab)^\sigma = a^\sigma b^\sigma$
- $(a^\sigma)^\tau = a^{\sigma\tau}$
- $A = \bigcup_{L|K \text{ endl.}} A_L$ wobei

$$A_L := A^{G_L} = \left\{a \in A \mid a^\sigma = a \forall \sigma \in G_L = G(\overline{L}|L)\right\}$$

2.3.2 Definition: Normabbildung

Sei eine endliche Körpererweiterung $L'|L$ galoissch über K gegeben. Definiere folgende **Normabbildung**

$$\begin{aligned} N_{L'|L} : A_{L'} &\longrightarrow A_L \\ a &\longmapsto \prod_{\sigma \in G_L/G_{L'}} a^\sigma \end{aligned}$$

Ist $L'|L$ galoissch, so ist $A_{L'}$ ein $G(L'|L)$-Modul und es gilt

$$A_{L'}^{G(L'|L)} = A_L$$

2.3.3 Definition: Kohomologie

Sei eine endliche, galoissche Körpererweiterung $L'|L$ galoissch über K gegeben. Definiere folgende **Tate-Kohomologiegruppen**

$$\begin{aligned} H^0(G(L'|L), A_{L'}) &:= A_L / N_{L'|L} A_{L'} \\ H^{-1}(G(L'|L), A_{L'}) &:= {}_{N_{L'|L}} A_{L'} / I_{G(L'|L)} A_{L'} \end{aligned}$$

wobei

$$\begin{aligned} {}_{N_{L'|L}} A_{L'} &:= \{a \in A_{L'} \mid N_{L'|L}(a) = 1\} \\ I_{G(L'|L)} A_{L'} &:= \{a^{\sigma - 1} \mid a \in A_{L'}, \sigma \in G(L'|L)\} \end{aligned}$$

${}_{N_{L'|L}} A_{L'}$ nennen wir auch die **Normrestgruppe**.

2.3.4 Definition: Verlagerung

Sei G eine Gruppe und H eine Untergruppe mit endlichen Index. $R = G/H$ bezeichne ein Repräsentantensystem der Linksnebenklassen von H, welches die 1 enthält.
Definiere die **Verlagerung** durch

$$\begin{aligned} Ver : G^{ab} &\longrightarrow H^{ab} \\ [g] &\longmapsto \left[\prod_{r\in R} g_r\right] \end{aligned}$$

wobei die g_r hinreichend wohldefiniert sind durch

$$gr = r' g_r$$

für ein $r' \in R$.

2.3.5 Definition: Normrestsymbol

Sei eine endliche, galoissche Körpererweiterung $L|K$ gegeben. Definiere das **Normrestsymbol** durch

$$(\_, L|K) : A_K \twoheadrightarrow A_K/NL|KA_L \overset{\cong}{\to} G(L|K)^{ab}$$

Das Normrestsymbol erfüllt folgende Eigenschaften:

(A1) Für alle $\sigma \in G_K$ kommutiert

$$\begin{tikzcd} A_K \arrow[r, "(\_, L|E)"] \arrow[d, two heads, "\sigma"'] & G(L|K)^{ab} \arrow[d, "\sigma^* : g \mapsto \sigma g \sigma^{-1}"] \\ A_{K^\sigma} \arrow[r, "(\_, L^\sigma|K^\sigma)"] & G(L^\sigma|K^\sigma)^{ab} \end{tikzcd}$$

(A2) Sei $K'|K$ eine endliche Erweiterung und setze $L' = K'L$. Dann kommutiert

$$\begin{tikzcd} A_{K'} \arrow[r, "(\_, L'|K')"] \arrow[d, two heads, "N_{L'|L}"'] & G(L'|K')^{ab} \arrow[d, "\sigma \mapsto \sigma_{|L}"] \\ A_K \arrow[r, "(\_, L|K)"] & G(L|K)^{ab} \end{tikzcd}$$

(A3) Liegen endliche Körpererweiterungen $L|K'|K$ vor, sodass L und K' galoissch über K sind, so kommutiert

$$\begin{tikzcd} A_{K'} \arrow[r, "(\_, L|K')"] & G(L|K')^{ab} \\ A_K \arrow[r, "(\_, L|K)"] \arrow[u, hook] & G(L|K)^{ab} \arrow[u, "Ver"'] \end{tikzcd}$$

2.4 Haupttheoreme der Klassenkörpertheorie

2.4.1 Definition: Lokaler Körper

Unter einem **lokalen Körper** verstehen wir $\mathbb{R}$ oder $\mathbb{C}$ oder einen vollständigen, diskret bewerteten Körper mit endlichem Restklassenkörper.

2.4.2 Satz: Lokale Klassenkörpertheorie

Sei K ein lokaler Körper.

- Es existiert genau ein stetiger Gruppenhomomorphismus

$$\phi_K : K^\times \longrightarrow G_K^{ab}$$

  der folgende Eigenschaften erfüllt:

  - Für jede endliche, abelsche Erweiterung $L|K$ induziert ϕ_K einen Isomorphismus

$$K^\times / N_{L|K} L^\times \xrightarrow{\cong} G(L|K)$$

  - Ist $K \neq \mathbb{R}, \mathbb{C}$ und besitzt den endlichen Restklassenkörper κ, so kommutiert folgendes Diagramm

$$\begin{tikzcd}
K^\times \arrow[r, "\phi_K"] \arrow[d, "v_K : \pi_K \mapsto 1"'] & G(K^{ab}|K) \arrow[d] \arrow[dr, "res"] & \\
\mathbb{Z} \arrow[r, "\phi_\kappa : 1 \mapsto \phi_{\#\kappa}"] & G(\overline{\kappa}|\kappa) \arrow[r, "\cong"] & G(K^{uv}|K)
\end{tikzcd}$$

    wobei K^{ab} die maximale abelsche Erweiterung von K und K^{uv} ihre maximale unverzweigte Teilerweiterung ist.

- Es ergeben sich folgende Korrespondenzen

$$\begin{tikzcd}
\{H \leq_o G(K^{ab}|K)\} \arrow[r, leftrightarrow, "1:1"] \arrow[d, leftrightarrow, "1:1"'] & \{U \subseteq_o K^\times \text{ von endlichem Index}\} \\
\{L|K \text{ endlich, abelsch}\} &
\end{tikzcd}$$

2.4.3 Definition: Globale Körper

Unter einem **globalen Körper** verstehen wir einen Zahl- bzw. Funktionenkörper.

2.4.4 Satz: Globale Klassenkörpertheorie

Sei K ein globaler Körper, C_K bezeichne seien Idelegruppe.

- Es existiert genau ein stetiger Gruppenhomomorphismus

$$\phi_K : C_K \longrightarrow G_K^{ab}$$

  sodass für jede Stelle v von K folgendes Diagramm kommutiert

$$\begin{tikzcd} K_v^\times \arrow[r, "\phi_{K_v}"] \arrow[d, hook, "\pi_v \mapsto ?"'] & G(K_v^{ab}|K_v) \arrow[d, hook] \\ C_K \arrow[r, "\phi_K : ? \mapsto \mathsf{Frob}_v"] & G(K^{ab}|K) \end{tikzcd}$$

wobei K_v die Komplettierung von K bzgl. v bezeichnet.

- Für jede endliche, abelsche Erweiterung $L|K$ induziert ϕ_K einen Isomorphismus

$$C_K/N_{L|K}C_L \xrightarrow{\cong} G(L|K)$$

- Es ergeben sich folgende Korrespondenzen

$$\begin{tikzcd} \{H \leq_o G(K^{ab}|K)\} \arrow[r, leftrightarrow, "1:1"] \arrow[d, leftrightarrow, "1:1"'] & \{U \subseteq_o C_K \text{ von endlichem Index}\} \\ \{L|K \text{ endlich, abelsch}\} & \end{tikzcd}$$

2.5 Was besagt die Klassenkörpertheorie? Erste Folgerungen der Hauptresultate

2.5.1 Satz

Sei $L|K$ eine endliche, abelsche Erweiterung globaler Körper. v sei eine Stelle von K, $\pi_v \in \mathcal{O}_{K_v} \subset K_v$ die zugehörige lokale Stelle. Definiere folgende Abbildung

$$\Theta : K_v^\times \hookrightarrow C_K \longrightarrow C_K/N_{L|K}C_L$$

Dann gilt

- v zerlegt sich voll in $L \iff \Theta(K_v^\times) = \{1\}$
- Ist v endlich, so gilt
$$v \text{ ist unverzweigt in } L \iff \Theta(\mathcal{O}_{K_v}^\times) = \{1\}$$
- Sei v endlich und unverzweigt in L. Dann liegt folgende Isomorphie vor

$$\begin{aligned} C_K/N_{L|K}C_L &\longrightarrow G(L|K) \\ \Theta(\pi_v) &\longmapsto \mathsf{Frob}_v \end{aligned}$$

Kapitel 3

Adele, Idele und Verallgemeinerte Idealklassengruppen

3.1 Eingeschränkte Produkte

3.1.1 Bemerkung

Ab sofort heißt ein topologischer Raum *kompakt*, falls er *quasikompakt* und *hausdorffsch* ist.
Ein Raum heißt ferner ab jetzt *lokal kompakt*, falls er *hausdorffsch* und *lokal quasikompakt* ist.

3.1.2 Definition: Eingeschränkte Produkte

Sei I eine Indexmenge, $(G_i)_{i\in I}$ eine Familie lokal kompakter, abelscher Gruppen und $(U_i)_{i\in I}$ eine Familie jeweils kompakter, offener Untergruppen.
Definiere das **restringierte Produkt** bzw. **eingeschränkte Produkt** von $(G_i)_i$ bzgl. $(U_i)_i$ durch

$$\prod_{i\in I}{}' G_i := \left\{ (x_i)_i \in \prod_{i\in I} G_i \mid x_i \in U_i \text{ ffa } i \in I \right\}$$

Definiere für eine endliche Menge $J \subset I$

$$G_J := \prod_{i\in J} G_i \times \prod_{i\in I\setminus J} G_i$$

Dann gilt

$$\prod_{i\in I}{}' G_i = \bigcup_{J \text{ endlich}} G_J$$

Jedes G_J trägt die Produkttopologie und ist lokal kompakt; das restringierte Produkt $\prod'_{i\in I} G_i$ wird nun mit der dadurch induzierten Kolimestopologie versehen. Dadurch ist $\prod'_{i\in I} G_i$ ebenfalls lokal kompakt und für jedes $V \subset \prod'_{i\in I} G_i$ gilt insbesondere

$$V \subset_o G \Longleftrightarrow V \cap G_J \subset_o G_J \text{ für alle } J \text{ endlich}$$

Die Menge

$$\left\{ \prod_{i\in J} O_i \times \prod_{i\in I\setminus J} U_i \mid J \subset I \text{ endlich und } 1 \in O_i \subset_o G_i \right\}$$

bilde eine Umgebungsbasis der Eins in $\prod'_{i\in I} G_i$.
Ferner wird folgende universelle Abbildungseigenschaft für jede hausdorffsche, abelsche Gruppe Z erfüllt

$$\mathsf{Hom}_{cts}\left(\prod_{i\in I}{}' G_i, Z\right) = \left\{(f_i)_i \in \prod_{i\in I} \mathsf{Hom}_{cts}\left(G_i, Z\right) \;\middle|\; \text{ffa } i\in I \text{ ist } f_i(U_i) \text{ in jedem } 1\in U\subset_o Z \text{ enthalten}\right\}$$

3.2 Adele und Idele

3.2.1 Definition: Adelering und Idelering

Sei K ein globaler Körper, S die Menge aller Stellen von K. Definiere den **Adelering** von K durch das restringierte Produkt

$$\mathbb{A}_K := \prod_{v\in S}{}' K_v \text{ bzgl. } (\mathcal{O}_v)_{v\in S}$$

und die **Idelegruppe** durch

$$\mathbb{A}_K^\times := \prod_{v\in S}{}' K_v^\times \text{ bzgl. } (\mathcal{O}_v^\times)_{v\in S}$$

3.2.2 Bemerkung

$$(\mathbb{A}_K)^\times = \mathbb{A}_K^\times$$

3.2.3 Definition: Hauptadele und Hauptidele

Es liegen folgende Homomorphismen vor

$$\begin{aligned} K &\hookrightarrow \mathbb{A}_K \\ a &\longmapsto (a)_v \end{aligned} \qquad\qquad \begin{aligned} K^\times &\hookrightarrow \mathbb{A}_K^\times \\ a &\longmapsto (a)_v \end{aligned}$$

Die Bilder dieser Inklusionen nennen wir **Hauptadele** bzw. **Hauptidele**.
Die **Idele-Klassengruppe** ist definiert durch

$$C_K := \mathbb{A}_K^\times / K^\times$$

Ferner liegt folgender stetiger multiplikativer Monoid-Homomorphismus vor

$$\begin{aligned} |\cdot| : \mathbb{A}_K &\longrightarrow \mathbb{R}_{\geq 0} \\ (a_v)_v &\longmapsto |a| := \prod_v |a|_v \end{aligned}$$

3.2.4 Satz: Produktformel

Sei K global, dann gilt für alle $a \in K^\times$

$$|a| = 1$$

3.2.5 Satz

Sei K global.

- K liegt in $\mathbb{A}_K$ diskret und $\mathbb{A}_K/K$ ist kompakt.
- Definiere
$$\mathbb{A}_K^1 := \left\{a \in \mathbb{A}_K^\times \;|\; |a| = 1\right\}$$
$K^\times$ liegt in $\mathbb{A}_K^1$ diskret und $C_K^1 := \mathbb{A}_K^1/K^\times$ ist kompakt.

3.2.6 Bemerkung

$C_K = \mathbb{A}_K^\times / K^\times$ ist im Allgemeinem nicht kompakt.

3.2.7 Bemerkung: Idealklassengruppe

Sei K ein Zahlkörper, $\mathcal{I}$ bezeichne die Menge der gebrochenen Ideale von K, $\mathcal{P}$ die Menge der gebrochenen Hauptideale.
Die **Idealklassengruppe** ist definiert durch

$$Cl(K) = \mathcal{I}/\mathcal{P}$$

Bezeichnet S_f die Menge der endlichen Stellen von K und S_∞ die Menge der unendlichen Stellen von K, so definiere

$$\mathcal{U} := \prod_{v \in S_\infty} K_v^\times \times \prod_{v \in S_f} \mathcal{O}_v^\times \subset \mathbb{A}_K^\times$$

Es gilt

$$\mathbb{A}_K^\times / \mathcal{U} \cong \bigoplus_{v \in S_f} K_v^\times / \mathcal{O}_v^\times \cong \mathcal{I}$$

Definiert man ferner $\overline{\mathcal{U}} := K^\times \cdot \mathcal{U}/K^\times$, so gilt

$$C_K/\overline{\mathcal{U}} \cong Cl(K)$$

3.2.8 Definition: Verallgemeinerte Idealklassengruppe

Sei K ein Zahlkörper.
Definiere für ein Ideal $0 \neq \mathfrak{a} \subset \mathcal{O}_K$

$$\mathcal{U}(\mathfrak{a}) := \prod_{v \in S} U_v(\mathfrak{a}) \subset \mathcal{U}$$

wobei

$$U_v(\mathfrak{a}) := \begin{cases} \{x \in \mathcal{O}_{K_v} \mid x \equiv 1 \mod \mathfrak{a}\mathcal{O}_{K_v}\} = 1 + \mathfrak{m}_v^{n_v(\mathfrak{a})} = 1 + \mathfrak{a}\mathcal{O}_{K_v} & v \in S_f \\ K_v^\times & v \text{ komplex} \\ \mathbb{R}_{>0} \cap K_v^\times & v \text{ reell} \end{cases}$$

Die **verallgemeinerte Idealklassengruppe** ist definiert durch

$$Cl(K, \mathfrak{a}) = C_K / \overline{\mathcal{U}(\mathfrak{a})}$$

Es gilt für Ideale $\mathfrak{a}, \mathfrak{b}$

$$\mathfrak{a} \leq \mathfrak{b} \Longleftrightarrow \mathcal{U}(\mathfrak{a}) \leq \mathcal{U}(\mathfrak{b}) \Longleftrightarrow Cl(K, \mathfrak{a}) \twoheadrightarrow Cl(K, \mathfrak{b})$$

und

$$Cl(K, \mathcal{O}_K) = Cl(K)$$

3.2.9 Bemerkung: Alternative Beschreibung der Idealklassengruppe

Sei K ein Zahlkörper, $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal.
Es sei

$$S(\mathfrak{a}) := \{v \in S_f \mid n_v(\mathfrak{a}) \neq 0\}$$

Definiere für ein Ideal $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ die Gruppe der zu $\mathfrak{a}$ teilerfremden gebrochenen Ideale

$$\mathcal{I}(\mathfrak{a}) := \left\{\mathfrak{b}^{-1}\mathfrak{c} \mid \mathfrak{b}, \mathfrak{c} \trianglelefteq \mathcal{O}_K \text{ teilerfremd zu } \mathfrak{a}\right\} \cong \bigoplus_{v \in S_f \setminus S(\mathfrak{a})} \mathbb{Z}$$

und die Gruppe der $\mathfrak{a}$ teilerfremden gebrochenen Hauptideale

$$\mathcal{P}(\mathfrak{a}) := \left\{(\alpha) \in K^\times \mid \alpha \text{ ist lokal positiv und } \forall v \in S(\mathfrak{a}) : \alpha \in 1 + \mathfrak{a}\mathcal{O}_{K_v}\right\}$$

3.2.10 Bemerkung

Im Allgemeinem gilt

$$\mathcal{P}(\mathfrak{a}) \subsetneq \mathcal{P} \cap \mathcal{I}(\mathfrak{a})$$

In jedem Fall gilt wegen dem Approximationsatz

$$\mathcal{I}(\mathfrak{a})/\mathcal{P} \cap \mathcal{I}(\mathfrak{a}) = \mathcal{I}/\mathcal{P} = Cl(K)$$

3.2.11 Satz

Sei K ein Zahlkörper, $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal.
Setze

$$S := S_\infty \cup S(\mathfrak{a})$$

Beachte, dass für $v \notin S$ $U_v(\mathfrak{a}) = \mathcal{O}_{K_v}^\times$ gilt. Wir erklären folgenden Homomorphismus

$$\phi : \mathcal{I}(\mathfrak{a}) \cong \bigoplus_{v \notin S} \mathbb{Z} \cong \bigoplus_{v \notin S} K_v^\times / U_v(\mathfrak{a}) \subset \mathbb{A}_K^\times / \mathcal{U}(\mathfrak{a}) \twoheadrightarrow C_K / \overline{\mathcal{U}(\mathfrak{a})} = Cl(K, \mathfrak{a})$$

Es gilt

- ϕ induziert einen Isomorphismus

$$\phi : \mathcal{I}(\mathfrak{a})/\mathcal{P}(\mathfrak{a}) \longrightarrow Cl(K, \mathfrak{a})$$

- Es liegt folgende kurze exakte Sequenz vor

$$1 \longrightarrow \left(\bigoplus_{v \text{ reell}} \mathbb{R}^\times/\mathbb{R}_{>0} \oplus (\mathcal{O}_K/\mathfrak{a})^\times\right)/\mathcal{O}_K^\times \longrightarrow Cl(K, \mathfrak{a}) \longrightarrow Cl(K) \longrightarrow 1$$

  Insbesondere ist $Cl(K, \mathfrak{a})$ endlich.

3.2.12 Satz: Approximationssatz

Sei K ein Zahlkörper, S eine endliche Stellenmenge. Für jedes $v \in S$ sei ein $x_v \in K$ vorgegeben. Dann existiert für jedes $\epsilon > 0$ ein $x \in K$, sodass für alle $v \in S$ gilt

$$|x - x_v|_v < \epsilon$$

3.2.13 Definition

Sei K ein Zahlkörper, $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ ein Ideal, $S = S_\infty \cup S(\mathfrak{a})$.
Definiere

$$K_\mathfrak{a}^\times := \mathsf{Kern}\left(K^\times \to \bigoplus_{v \in S} K_v^\times / U_v(\mathfrak{a})\right)$$

und

$$\mathcal{O}_{K,\mathfrak{a}}^\times := K_\mathfrak{a}^\times \cap \mathcal{O}_K^\times$$

Dann liegt folgende Isomorphie vor

$$K_\mathfrak{a}^\times / \mathcal{O}_{K,\mathfrak{a}}^\times = \mathcal{P}(\mathfrak{a})$$

3.2.14 Lemma

Folgende Sequenz ist exakt

$$1 \longrightarrow K_{\mathfrak{a}}^{\times} \longrightarrow K^{\times} \longrightarrow \bigoplus_{v \in S} K_v^{\times}/U_v(\mathfrak{a}) \longrightarrow 1$$

3.2.15 Satz: Schlangenlemma

Sei folgendes kommutative Diagramm von R-Moduln gegeben

$$\begin{tikzcd} & A \arrow[r] \arrow[d, "a"'] & B \arrow[r] \arrow[d, "b"'] & C \arrow[r] \arrow[d, "c"'] & 0 \\ 0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' & \end{tikzcd}$$

Es liegt folgende exakte Sequenz vor

$$\mathsf{Kern} a \longrightarrow \mathsf{Kern} b \longrightarrow \mathsf{Kern} c \xrightarrow{\delta} \mathsf{Kokern} a \longrightarrow \mathsf{Kokern} b \longrightarrow \mathsf{Kokern} c$$

3.2.16 Bemerkung

Definiere

$$\mathbb{A}_{K,\mathfrak{a}}^{\times} := \prod_{v \in S} U_v(\mathfrak{a}) \times \prod_{v \notin S}{}' K_v^{\times}$$

dann liegt folgende Isomorphie vor

$$\mathbb{A}_{K,\mathfrak{a}}^{\times} \xrightarrow{\cong} \mathbb{A}_K^{\times}/K^{\times}$$

und folgende surjektive Abbildung

$$\begin{aligned} \Psi_{\mathfrak{a}} : \mathbb{A}_{K,\mathfrak{a}}^{\times} &\longrightarrow \mathcal{I}(\mathfrak{a}) \\ (a)_v &\longmapsto (a) := \prod_{v \in S_f} \mathfrak{p}_v^{v(a_v)} \end{aligned}$$

3.3 Normgruppen

3.3.1 Definition: Spur und Norm

Sei $L|K$ eine endliche, galoissche Erweiterung globaler Körper.
Definiere die **Spurabbildung** auf den Adelen durch

$$\begin{aligned} Tr_{L|K} : \mathbb{A}_L &\longrightarrow \mathbb{A}_K \\ (x_w)_w &\longmapsto \left(\sum_{w|v} Tr_{L_w|K_v}(x_w) \right)_v \end{aligned}$$

und die **Normabbildung** durch

$$\begin{aligned} N_{L|K} : \mathbb{A}_L^{\times} &\longrightarrow \mathbb{A}_K^{\times} \\ (x_w)_w &\longmapsto \left(\prod_{w|v} N_{L_w|K_v}(x_w) \right)_v \end{aligned}$$

$G(L|K)$ operiert auf den Adelen bzw. Idelen durch

$$((x_w)_w)^\sigma := (x_w^\sigma)_{w^\sigma} = (x^\sigma_{w^{\sigma^{-1}}})_w$$

für $(x_w)_w \in \mathbb{A}_L$. Es gilt ferner

$$\mathbb{A}_L^{G(L|K)} = \mathbb{A}_K \text{ und } (\mathbb{A}_L^\times)^{G(L|K)} = \mathbb{A}_K^\times$$

3.3.2 Bemerkung

Es bezeichne $G = G(L|K)$. Da $L^\times \hookrightarrow \mathbb{A}_L^\times$ eine Inklusion von G-Moduln ist, ist auch $C_L = \mathbb{A}_L^\times / L^\times$ ein G-Modul.
Da die erste Kohomologiegruppe $H^1(G, L^\times) = 1$ verschwindet laut Hilbert '90, ist der Invariantenfunktor

$$\begin{aligned} G - \mathbf{Mod} &\longrightarrow \mathbf{Ab} \\ M &\longmapsto M^G := \{m \in M \mid \forall g \in G : m^g = m\} \end{aligned}$$

exakt, ergo ergibt sich folgendes kommutative Diagramm

$$\begin{tikzcd} 1 \arrow[r] & L^\times \arrow[r] \arrow[d, "N_{L|K}"'] & \mathbb{A}_L^\times \arrow[r] \arrow[d, "N_{L|K}"'] & C_L \arrow[r] \arrow[d, "N_{L|K}"'] & 1 \\ 1 \arrow[r] & K^\times \arrow[r] & \mathbb{A}_K^\times \arrow[r] & C_L^G = C_K \arrow[r] & 1 \end{tikzcd}$$

Es folgt nun

- $N_{L|K} C_L = K^\times N_{L|K} \mathbb{A}_L^\times \ / \ K^\times$
- $C_K / N_{L|K} C_L = \mathbb{A}_K^\times \ / \ (K^\times N_{L|K} \mathbb{A}_L^\times)$

3.3.3 Definition: Zulässige Ideale

Sei K ein Zahlkörper. Ein Ideal $0 \neq \mathfrak{a} \subset \mathcal{O}_K$ heißt **zulässig** für eine endliche, galoissche Erweiterung $L|K$, falls für alle Stellen v von K und allen w über v gilt

$$U_v(\mathfrak{a}) \subseteq N_{L_w|K_v} L_w^\times$$

Bemerkung Für unendliche Stellen ist diese Bedingung immer erfüllt.
Für endliche, unverzweigte Stellen ist diese Bedingung ebenfalls immer erfüllt.
Bezeichnet S die Menge aller Stellen, die in L verzweigen, so wähle $\mathfrak{a}$ dergestalt, dass für alle $v \in S$ und w über v gilt

$$[L_w : K_v] \mid v(\mathfrak{a})$$

Es gilt in diesem Fall

$$U_v(\mathfrak{a}) = 1 + \mathfrak{a}\mathcal{O}_{K_v} = 1 + \mathfrak{m}_v^{v(\mathfrak{a})} \subset (K_v^\times)^{v(\mathfrak{a})} \subset (K_v^\times)^{[L_w:K_v]} = N_{L_w|K_v} K_v^\times \subset N_{L_w|K_v} L_w^\times$$

Bezüglich Teilbarkeit existiert für $L|K$ ferner stets ein kleinstes zulässiges Ideal $\mathfrak{f}$.

3.3.4 Satz

- Ist $L|K$ eine endliche, unverzweigte Erweiterung lokaler Körper, so ist folgende Norm
$$N_{L|K} : \mathcal{O}_L^\times \longrightarrow \mathcal{O}_K^\times$$
surjektiv.

- Sei $L|K$ eine endliche, galoissche Erweiterung globaler Körper, $\mathfrak{a}$ ein zulässiges Ideal und $\mathfrak{f}$ das kleinste zulässige Ideal für $L|K$.
Definiere die Menge der gebrochenen Ideale in L mit zu $\mathfrak{a}$ teilerfremden Träger durch
$$\mathcal{I}_L(\mathfrak{a}) := \{\mathfrak{b} \in \mathcal{I}_L \mid \mathfrak{P}|\mathfrak{b} \Rightarrow \mathfrak{P} \nmid \mathfrak{a}\mathcal{O}_L\}$$
und
$$\mathcal{N}(\mathfrak{a}) := N_{L|K}\mathcal{I}_L(\mathfrak{a}) = \left\{N_{L|K}\mathfrak{b} \mid \mathfrak{b} \in \mathcal{I}_L(\mathfrak{a})\right\} \subset \mathcal{I}(\mathfrak{a})$$
Die Inklusion
$$\mathcal{I}(\mathfrak{a}) \hookrightarrow \mathcal{I}(\mathfrak{f})$$
induziert einen Isomorphismus
$$\mathcal{I}(\mathfrak{a})/(\mathcal{P}(\mathfrak{a})\mathcal{N}(\mathfrak{a})) \cong \mathcal{I}(\mathfrak{f})/(\mathcal{P}(\mathfrak{f})\mathcal{N}(\mathfrak{f}))$$
Insbesondere gilt
$$\mathcal{P}(\mathfrak{f})\mathcal{N}(\mathfrak{f}) \cap \mathcal{I}(\mathfrak{a}) = \mathcal{P}(\mathfrak{a})\mathcal{N}(\mathfrak{a})$$
Ist
$$\mathsf{supp}(\mathfrak{a}) := \{\mathfrak{p} \in \mathsf{Spec}\mathcal{O}_K \mid \mathfrak{p} \text{ teilt } \mathfrak{a}\} = \mathsf{supp}(\mathfrak{f})$$
d. h., es gilt
$$\mathcal{I}(\mathfrak{a}) = \mathcal{I}(\mathfrak{f}) \text{ und } \mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{f})$$
so gilt insbesondere
$$\mathcal{P}(\mathfrak{f})\mathcal{N}(\mathfrak{f}) = \mathcal{P}(\mathfrak{a})\mathcal{N}(\mathfrak{a})$$

- Gilt in obiger Situation folgende Isomorphie
$$\mathbb{A}_K^\times/K^\times \cong \mathbb{A}_{K,\mathfrak{a}}^\times/K_\mathfrak{a}^\times$$
so induziert $\Psi_\mathfrak{a}$ folgende Isomorphie
$$C_K/N_{L|K}C_L \cong \mathbb{A}_K^\times/K^\times N_{L|K}\mathbb{A}_L^\times \xrightarrow{\cong,\Psi_\mathfrak{a}} \mathcal{I}(\mathfrak{a})/(\mathcal{P}(\mathfrak{a})\mathcal{N}(\mathfrak{a}))$$

3.3.5 Lemma

Sei $\lambda|\kappa$ eine Erweiterung endlicher Körper.

- $N_{\lambda|\kappa} : \lambda^\times \longrightarrow \kappa^\times$ ist surjektiv.
- $T_{\lambda|\kappa} : \lambda \longrightarrow \kappa$ ist surjektiv.

Kapitel 4

Norm-Index-Berechnungen

4.1 Hilbert ’90

4.1.1 Definition: Gruppenkohomologiegruppen

Sei G eine endliche Gruppe, A ein multiplikativ geschriebener G-Modul.
Definiere die Gruppe der 1-**Kozykel** durch

$$Z^1(G, A) := \{f : G \to A \mid \forall \sigma, \tau \in G : f(\sigma\tau) = (f(\sigma))^\tau \cdot f(\tau)\}$$

und die Gruppe der 1-**Koränder** durch

$$B^1(G, A) := \left\{f \in Z^1(G, A) \mid \exists a \in A : f(\sigma) = a^{\sigma - 1}\right\}$$

Definiere die erste **Gruppenkohomologiegruppe** von G mit Koeffizienten in A durch

$$H^1(G, A) := Z^1(G, A)/B^1(G, A)$$

4.1.2 Satz: Hilbert ’90

- Ist $L|K$ eine zyklische, galoissche Erweiterung beliebiger Körper, so gilt

$$H^{-1}(G(L|K), L^\times) = 1$$

- Ist $L|K$ eine endliche, galoissche Erweiterung beliebiger Körper, so gilt

$$H^1(G(L|K), L^\times) = 1$$

Beweis

- Da

$$H^{-1}(G(L|K), L^\times) = {}_{N_{L|K}}L^\times / I_{G(L|K)} L^\times$$

ist die Behauptung äquivalent zur Aussage, dass zu jedem $\alpha \in L^\times$ mit

$$N_{L|K}(\alpha) = 1$$

ein $\beta \in L^\times$ existiert, so dass

$$\alpha = \beta^{\sigma - 1}$$

wobei σ einen Erzeuger der zyklischen Gruppe $G(L|K)$ bezeichnet.
Es bezeichne $n = [L : K]$ den Grad der zyklischen Erweiterung. Die Automorphismen

$$\mathsf{id}_{L^\times}, \sigma, \dots, \sigma^{n-1} : L^\times \longrightarrow L^\times$$

stellen n verschiedene Charaktere da und sind deswegen linear unabhängig. Insbesondere verschwindet folgende Linearkombination nicht

$$\sum_{i=0}^{n-1} \left(\alpha^{\sum_{j=0}^{i-1} \sigma^j} \right) \sigma^i = \mathsf{id}_{L^\times} + \alpha\sigma + \alpha^{1+\sigma}\sigma^2 + \dots + \alpha^{1+\sigma+\dots+\sigma^{n-2}}\sigma^{n-1}$$

Ergo existiert ein $\gamma \in L^\times$, sodass

$$\beta := \gamma + \alpha\gamma^\sigma + \alpha^{1+\sigma}\gamma^{\sigma^2} + \dots + \alpha^{1+\sigma+\dots+\sigma^{n-2}}\gamma^{\sigma^{n-1}} \neq 0$$

Es gilt nun

$$\alpha\beta^\sigma = \alpha(\gamma^\sigma + \dots + \alpha^{\sigma+\dots+\sigma^{n-1}}\gamma^{\sigma^n}) = \beta$$

da

$$\alpha^{\sigma+\dots+\sigma^{n-1}}\gamma^{\sigma^n} = \frac{N_{L|K}(\alpha)}{\alpha}\gamma = \alpha^{-1}\gamma$$

- Sei $f \in Z^1(G(L|K), A)$. Aufgrund der Unabhängigkeit der Charaktere existiert ein $\gamma \in L^\times$ mit

$$\alpha := \sum_{\sigma \in G} f(\sigma)\gamma^\sigma \neq 0$$

Für beliebige $\tau \in G$ gilt nun

$$\alpha^\tau = \sum_{\sigma \in G(L|K)} f(\sigma)^\tau \gamma^{\sigma\tau} \sum_{\sigma \in G(L|K)} f(\sigma\tau) f(\tau^{-1})\gamma^{\sigma\tau} = f(\tau^{-1})\alpha$$

Daraus folgt nun

$$f(\tau) = \alpha^{1-\tau} = \beta^{\tau-1}$$

für $\beta := \alpha^{-1}$. Ergo $f \in B^1(G(L|K), A)$

□

4.1.3 Satz: Gruppenkohomologie ist auch wirklich eine Kohomologietheorie

Zu jeder exakten Sequenz von G-Moduln

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

existiert folgende lange exakte Kohomologiesequenz

$$1 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C) \longrightarrow \dots$$

4.2 Herbrand-Quotient

4.2.1 Lemma

Sei $f : A \to C$ ein Homomorphismus abelscher Gruppen und $B \leq A$ eine Untergruppe. Setze

$${}_fA := A_f := \{a \in A \mid f(a) = 1\} = \mathsf{Kern} f_{|A} \text{ und } A^f := f(A) = \mathsf{Bild} f_{|A}$$

Es gilt

$$(A : B) = (A^f : B^f) \cdot (A_f : B_f)$$

4.2.2 Definition: Herbrand-Quotient

Für Morphismen $f, g : A \to A$ einer Gruppe A definiere den Herbrand-Quotienten durch

$$Q(A) := Q_{f,g}(A) := \frac{(A_f : A^g)}{(A_g : A^f)}$$

4.2.3 Lemma

Seien $f, g : A \to A$ Homomorphismen einer abelschen Gruppe. $B \leq A$ sei eine Untergruppe, sodass $f(B), g(B) \subset B$.
Dann gilt

$$Q(A) = Q(B) \cdot Q(A/B)$$

Ist ferner A endlich, so ist $Q(A) = 1$.

4.2.4 Bemerkung

Sei $G = \langle\sigma\rangle$ zyklisch, A ein multiplikativer G-Modul und $f = 1 - \sigma$ und $g = N = \prod_{\sigma \in G} \sigma$ zwei Selbstabbildungen von A. Es gilt dann

$$Q(G, A) := Q_{f,g}(A) = \frac{(A_f : A^g)}{(A_g : A^f)} = \frac{(A^G : NA)}{(N_A : I_G A)} = \frac{\#H^0(G, A)}{\#H^{-1}(G, A)}$$