

# 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 quasi-kompakt (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.*  $\square$

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

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

Dabei ist die Topologie die Unterraumtopologie von  $\prod_i T_i$  mit der Produkttopologie. Sind  $\varphi_k : \varprojlim_i T_i \rightarrow T_k$  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  $i \geq j$ :

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

- 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

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

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  $\prod T_i \implies \varprojlim T_i$  abgeschlossen.

Bleibt zu zeigen  $\varprojlim T_i \neq \emptyset$ . 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.  $\square$

**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

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

ein Homöomorphismus ist.

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

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

**Satz 1.4.** Sei  $1 \rightarrow (G'_i) \rightarrow (G_i) \rightarrow (G''_i) \rightarrow 1$  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

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

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

**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  $\emptyset$  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.

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

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

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

Wir betrachten die Abbildungen

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

die durch

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

und

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

gegeben sind. In der Algebra-Vorlesung wurde bewiesen:

- $\varphi \circ \psi = \text{id}$ , insbesondere ist  $\psi$  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  $\varphi \circ \psi = \text{id}$ , d.h. wir erhalten eine 1-1 Korrespondenz.

Wir betrachten die gerichtete Menge  $L_i$ ,  $K \subset L_i \subset L$  aller endlichen Galoiszweischenerweiterungen. 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

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

Nach 1.6 erhalten wir eine Topologie auf  $G$ .

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

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

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

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

Abstrakter:

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

Behauptung:  $f$  ist ein Homöomorphismus. Es gilt:

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

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

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

eine Umgebungsbasis der 1. Daher ist  $f$  ein Homöomorphismus.  $\square$

**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  $U \implies U$  offen.

(iii) Es gilt

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

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.  $\square$

**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  $\overline{H} \subset \bigcap U$ . Sei  $x \notin \overline{H}$ . Dann existiert ein offener Normalteiler  $U$  mit  $xU \cap H = \emptyset$ .  $\leadsto x \notin UH$  und  $UH$  ist eine offene Untergruppe die  $H$  umfaßt.  $\square$

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

$$\left\{ \begin{array}{l} \text{abgeschl. UG} \\ H \subset G \end{array} \right\} \xrightleftharpoons[\psi]{\varphi} \left\{ \begin{array}{l} \text{Zwischenk.} \\ K \subset M \subset L \end{array} \right\}$$

Es ist  $M|K$  genau dann galoissch, wenn  $H = \psi(M)$  Normalteiler in  $G$  ist. Dann existiert ein natürlicher topologischer Isomorphismus  $\text{Gal}(M|K) \cong G/H$ .  $M|K$  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  $H = \psi(M) = \text{Gal}(L|M)$  nach Definition offen in der Krulltopologie und

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

(siehe Beweis von 1.7).

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

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

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

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

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

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

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

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

$$0 \longrightarrow \text{Gal}(L|M) \longrightarrow \text{Gal}(L|K) \longrightarrow \varprojlim \text{Gal}(M_i|K) \longrightarrow 0$$

$$\parallel$$

$$\text{Gal}(M|K)$$

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

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

Die Gruppen  $\text{Gal}(L|M_i)$  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.  $\square$

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

Es gilt  $G_K \cong \varprojlim \text{Gal}(L|K)$ , 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  $\varphi_g : G \rightarrow G, h \mapsto ghg^{-1}$ , 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  $f_1^*, f_2^* : \text{Gal}(L'|K) \rightarrow \text{Gal}(L|K)$  die induzierten Isomorphismen. Dann existiert ein  $g \in \text{Gal}(L|K)$  mit  $f_2^* = \varphi_g \circ f_1^*$ .

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

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

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

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

□

**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 Isomorphismus

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

Daher erhalten wir einen Isomorphismus projektiver Systeme

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

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

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

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

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

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

welcher  $1 \in \hat{\mathbb{Z}}$  auf den Frobeniushomomorphismus  $F$  von  $K^{\text{nr}}|K$  schickt (dieser ist durch  $F(x) \equiv x^q \pmod{\pi}$  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.



# Algebraische Zahlentheorie II

## Sommersemester 2022

Dr. Katharina Hübner

basierend auf Alexander Schmidts AZT2-Skript von 2014

### Inhaltsverzeichnis

<b>1</b>	<b>Homologische Algebra (Auffrischung)</b>	<b>1</b>
1.1	Injektive und projektive Objekte . . . . .	1
1.2	Adjungierte Funktoren . . . . .	3
1.3	Komplexe . . . . .	4
1.4	Abgeleitete Funktoren . . . . .	7
1.5	Azyklische Objekte . . . . .	8
1.6	Universelle $\delta$ -Funktoren . . . . .	8
1.7	Tor und Ext . . . . .	9

## 1 Homologische Algebra (Auffrischung)

### 1.1 Injektive und projektive Objekte

Sei  $\mathcal{A}$  eine abelsche Kategorie (z.B. die Kategorie der  $R$ -Moduln,  $R$  ein unitärer Ring). Eine Folge

$$M' \xrightarrow{u} M \xrightarrow{v} M''$$

heißt exakt, wenn  $v \circ u = 0$  und der natürliche Homomorphismus  $\text{im}(u) \rightarrow \ker(v)$  ein Isomorphismus ist.

**Satz 1.1.** (i) *Eine Folge  $M' \xrightarrow{u} M \xrightarrow{v} M'' \rightarrow 0$  in  $\mathcal{A}$  ist genau dann exakt, wenn für jedes  $N \in \mathcal{A}$  die Folge abelscher Gruppen*

$$0 \longrightarrow \text{Hom}_{\mathcal{A}}(M'', N) \xrightarrow{v^*} \text{Hom}_{\mathcal{A}}(M, N) \xrightarrow{u^*} \text{Hom}_{\mathcal{A}}(M', N)$$

*exakt ist.*

- (ii) Eine Folge  $0 \rightarrow N' \xrightarrow{u} N \xrightarrow{v} N''$  in  $\mathcal{A}$  ist genau dann exakt, wenn für jedes  $M \in \mathcal{A}$  die Folge abelscher Gruppen

$$0 \longrightarrow \operatorname{Hom}_{\mathcal{A}}(M, N') \xrightarrow{u_*} \operatorname{Hom}_{\mathcal{A}}(M, N) \xrightarrow{v_*} \operatorname{Hom}_{\mathcal{A}}(M, N'')$$

exakt ist.

**Definition.** Ein Funktor zwischen abelschen Kategorien heißt **exakt**, wenn er exakte Folgen in exakte Folgen überführt.

**Definition.**  $I \in \operatorname{ob}(\mathcal{A})$  heißt **injektiv**, falls sich jedes Diagramm

$$\begin{array}{ccc} & B & \\ i \uparrow & \searrow g & \\ A & \xrightarrow{f} & I \end{array}$$

in dem  $i$  ein Monomorphismus ist und  $f$  ein beliebiger Morphismus, kommutativ durch ein  $g$  ergänzen läßt.

$P \in \operatorname{ob}(\mathcal{A})$  heißt **projektiv**, wenn  $P \in \operatorname{ob}(\mathcal{A}^{\operatorname{op}})$  injektiv ist. M.a.W., wenn sich jedes Diagramm

$$\begin{array}{ccc} & B & \\ p \downarrow & \nearrow g & \\ A & \xleftarrow{f} & P \end{array}$$

mit  $p$  Epimorphismus und  $f$  beliebig, durch ein  $g$  kommutativ ergänzen läßt.

**Bemerkung.** Ist  $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$  eine exakte Folge in  $\mathcal{A}$  und  $A'$  injektiv oder  $A''$  projektiv, so zerfällt die Folge.

**Lemma 1.2.** (i)  $I$  ist genau dann injektiv, wenn der Funktor

$$\operatorname{Hom}_{\mathcal{A}}(-, I) : \mathcal{A}^{\operatorname{op}} \longrightarrow \mathcal{A}b$$

exakt ist.

- (ii)  $P$  ist genau dann projektiv, wenn der Funktor  $\operatorname{Hom}_{\mathcal{A}}(P, -) : \mathcal{A} \rightarrow \mathcal{A}b$  exakt ist.

**Bemerkung.** Sei  $A$  ein Hauptidealring. Dann sind die injektiven  $A$ -Moduln genau die teilbaren  $A$ -Moduln, die projektiven genau die freien.

## 1.2 Adjungierte Funktoren

Seien  $\mathcal{C}, \mathcal{D}$  Kategorien und  $F : \mathcal{C} \rightarrow \mathcal{D}$  und  $G : \mathcal{D} \rightarrow \mathcal{C}$  Funktoren.

**Definition.**  $F$  ist **linksadjungiert** zu  $G$  (und  $G$  **rechtsadjungiert** zu  $F$ , Schreibweise:  $F \dashv G$ ), wenn eine natürliche Äquivalenz

$$\text{Mor}_{\mathcal{C}}(-, G-) \cong \text{Mor}_{\mathcal{D}}(F-, -)$$

von Bifunktoren:  $\mathcal{C} \times \mathcal{D} \rightarrow (\text{Mengen})$  existiert.

Sind  $\mathcal{C}, \mathcal{D}$  additive Kategorien und  $F, G$  additive Funktoren, so wird stillschweigend angenommen, dass eine Äquivalenz von Bifunktoren  $\mathcal{C} \times \mathcal{D} \rightarrow \mathcal{A}b$  vorliegt.

**Beispiele.** 1)  $\mathcal{C} = \text{Mod-}R$ ,  $\mathcal{D} = \mathcal{A}b$ . Sei  $B$  ein  $R$ -Linksmodul. Wir betrachten die Funktoren

$$\text{Mod-}R \rightarrow \mathcal{A}b, \quad A \mapsto A \otimes_R B,$$

und

$$\mathcal{A}b \rightarrow \text{Mod-}R, \quad C \mapsto \text{Hom}_{\mathcal{A}b}(B, C).$$

Dann gilt in natürlicher Weise

$$\text{Hom}_{\mathcal{A}b}(A \otimes_R B, C) \cong \text{Hom}_{\text{Mod-}R}(A, \text{Hom}_{\mathcal{A}b}(B, C)).$$

Wir erhalten die Funktorenadjunktion

$$- \otimes_R B \dashv \text{Hom}_{\mathcal{A}b}(B, -).$$

2) Sei  $\mathcal{C} = K\text{-Vec}$ ,  $\mathcal{D} = (\text{Mengen})$ ,  $F : K\text{-Vec} \rightarrow (\text{Mengen})$  der Vergiß-Funktor und  $G : (\text{Mengen}) \rightarrow K\text{-Vec}$ ,  $M \rightarrow K^{(M)} = \text{Vektorraum mit Basis } M$ .

Dann gilt

$$\text{Hom}_{K\text{-Vec}}(GM, V) = \text{Hom}_{(\text{Mengen})}(M, FV)$$

also  $G \dashv F$ .

**Satz 1.3.** Es seien  $\mathcal{A}, \mathcal{B}$  abelsche Kategorien,  $F : \mathcal{A} \rightarrow \mathcal{B}$ ,  $G : \mathcal{B} \rightarrow \mathcal{A}$  additive Funktoren und sei  $F \dashv G$  (im additiven Sinne). Dann gilt

- (i)  $F$  ist rechtsexakt, d.h. ist  $A' \rightarrow A \rightarrow A'' \rightarrow 0$  exakt in  $\mathcal{A}$ , so ist  $FA' \rightarrow FA \rightarrow FA'' \rightarrow 0$  exakt in  $\mathcal{B}$ .
- (ii)  $G$  ist linksexakt.
- (iii) ist  $F$  exakt, so überführt  $G$  Injektive in Injektive.
- (iv) ist  $G$  exakt, so überführt  $F$  Projektive in Projektive.

*Beweis.*  $F$  induziert einen Funktor  $F^{\text{op}} : \mathcal{A}^{\text{op}} \rightarrow \mathcal{B}^{\text{op}}$  und analog  $G^{\text{op}} : \mathcal{B}^{\text{op}} \rightarrow \mathcal{A}^{\text{op}}$ . Es gilt  $G^{\text{op}} \dashv F^{\text{op}}$ . Daher genügt es (i) und (iii) zu zeigen.

(i) Für  $A' \rightarrow A \rightarrow A'' \rightarrow 0$  exakt und  $B \in \text{ob}(\mathcal{B})$  beliebig ist

$$0 \longrightarrow \text{Hom}_{\mathcal{A}}(A'', GB) \longrightarrow \text{Hom}_{\mathcal{A}}(A, GB) \longrightarrow \text{Hom}_{\mathcal{A}}(A', GB)$$

exakt, also auch

$$0 \longrightarrow \text{Hom}_{\mathcal{B}}(FA'', B) \longrightarrow \text{Hom}_{\mathcal{B}}(FA, B) \longrightarrow \text{Hom}_{\mathcal{B}}(FA', B).$$

Hieraus folgt die Exaktheit von

$$FA' \longrightarrow FA \longrightarrow FA'' \longrightarrow 0.$$

(iii) Sei  $I \in \text{ob}(\mathcal{A})$  injektiv. Zu zeigen: der Funktor

$$\text{Hom}_{\mathcal{A}}(-, GI)$$

ist exakt. Nun gilt

$$\text{Hom}_{\mathcal{A}}(-, GI) = \text{Hom}_{\mathcal{B}}(F-, I)$$

und weil  $F$  exakt und  $I$  injektiv ist ... □

### 1.3 Komplexe

Sei  $\mathcal{A}$  eine abelsche Kategorie.

**Definition.** Ein **Komplex**  $A^\bullet$  in  $\mathcal{A}$  ist eine Folge von Objekten und Homomorphismen

$$\dots \longrightarrow A^{-1} \xrightarrow{d_{-1}} A^0 \xrightarrow{d_0} A^1 \xrightarrow{d_1} A^2 \dots$$

so dass  $d_i \circ d_{i-1} = 0$  für alle  $i \in \mathbb{Z}$  gilt.

**Definition.** Ein **Homomorphismus**  $f : A^\bullet \rightarrow B^\bullet$  zwischen zwei Komplexen ist eine Familie  $f = (f_i)_{i \in \mathbb{Z}}$  von Homomorphismen  $f_i : A^i \rightarrow B^i$ , so dass für alle  $i \in \mathbb{Z}$  gilt:  $d_i \circ f_i = f_{i+1} \circ d_i$ , d.h. das Diagramm

$$\begin{array}{ccccccc} \dots & \longrightarrow & A^{i-1} & \xrightarrow{d_{i-1}} & A^i & \xrightarrow{d_i} & A^{i+1} & \longrightarrow & \dots \\ & & f_{i-1} \downarrow & & f_i \downarrow & & f_{i+1} \downarrow & & \\ \dots & \longrightarrow & B^{i-1} & \xrightarrow{d_{i-1}} & B^i & \xrightarrow{d_i} & B^{i+1}(C^\bullet) & \longrightarrow & \dots \end{array}$$

kommutiert.

**Bemerkung.** Komplexe in  $\mathcal{A}$  zusammen mit Homomorphismen von Komplexen bilden wieder eine abelsche Kategorie. Kerne, Kokerne und endliche Produkte bilden sich an jeder Stelle separat.

**Definition.**  $Z^i = \ker(d_i) \subset A^i$  heißen die ***i*-Kozykel** von  $A^\bullet$ .

$B^i = \operatorname{im}(d_{i-1}) \subset A^i$  heißen die ***i*-Koränder**.

$H^i(A^\bullet) = Z^i/B^i$  heißt die ***i*-te Kohomologiegruppe** von  $A^\bullet$ .

**Bemerkung.** Ein Komplexhomomorphismus  $f : A^\bullet \rightarrow B^\bullet$  induziert Homomorphismen  $Z^i(f) : Z^i A^\bullet \rightarrow Z^i B^\bullet$ ,  $B^i(f) : B^i A^\bullet \rightarrow B^i B^\bullet$  und  $H^i(f) : H^i(A^\bullet) \rightarrow H^i(B^\bullet)$  für alle  $i$ .

**Satz 1.4 (Verallgemeinertes Schlangen-Lemma).** Sei  $0 \rightarrow A^\bullet \rightarrow B^\bullet \rightarrow C^\bullet \rightarrow 0$  eine kurze exakte Folge von Komplexen (d.h. für jedes  $i$  ist  $0 \rightarrow A^i \rightarrow B^i \rightarrow C^i \rightarrow 0$  exakt). Dann existiert eine natürliche lange exakte Folge

$$\cdots \rightarrow H^i(A^\bullet) \rightarrow H^i(B^\bullet) \rightarrow H^i(C^\bullet) \rightarrow H^{i+1}(A^\bullet) \rightarrow \cdots$$

**Definition.** Eine **injektive Auflösung** von  $A \in \operatorname{ob}(\mathcal{A})$  ist ein Komplex

$$0 \rightarrow I^0 \xrightarrow{d_0} I^1 \xrightarrow{d_1} I^2 \rightarrow \cdots$$

bestehend aus injektiven Objekten in  $\mathcal{A}$ , mit  $H^i(I^\bullet) = 0$  für  $i \geq 1$  zusammen mit einem Isomorphismus  $A \xrightarrow{\sim} \ker(d_0) = H^0(I^\bullet)$ .

Eine **projektive Auflösung** ist eine injektive Auflösung in  $\mathcal{A}^{\operatorname{op}}$ , d.h. ein Komplex

$$\cdots \rightarrow P^{-2} \rightarrow P^{-1} \rightarrow P^0 \rightarrow 0$$

bestehend aus projektiven Objekten in  $\mathcal{A}$ , mit  $H^i(P^\bullet) = 0$ ,  $i \leq -1$ , zusammen mit einem Isomorphismus  $H^0(P^\bullet) \xrightarrow{\sim} A$ .

**Bemerkung.** Man benutzt gerne die untere Numerierung  $P_i = P^{-i}$  und schreibt dann  $H_i(-) = H^{-i}(-)$ .

**Definition.**  $\mathcal{A}$  hat **genügend viele Injektive**, wenn zu jedem  $A \in \operatorname{ob}(\mathcal{A})$  ein Monomorphismus  $i : A \rightarrow I$  mit  $I$  injektives Objekt existiert.  $\mathcal{A}$  hat **genügend viele Projektive**, wenn  $\mathcal{A}^{\operatorname{op}}$  genügend viele Injektive hat.

**Beispiel.**  $R\text{-Mod}$  hat genügend viele Injektive und genügend viele Projektive.

**Lemma 1.5.** (i) *Hat  $\mathcal{A}$  genügend viele Injektive, so hat jedes Objekt eine injektive Auflösung.*

(ii) *... projektive ...*

*Beweis.* Induktive Konstruktion von  $I^\bullet$

1. Schritt: Wähle  $A \hookrightarrow I^0$

2. Schritt: Wähle

$$I^0/A \hookrightarrow I^1$$

$n$ -ter Schritt: Wähle

$$I^{n-2}/\operatorname{im}(I^{n-3}) \hookrightarrow I^{n-1}$$

□

**Definition.** Seien  $f, g : A^\bullet \rightarrow B^\bullet$  zwei Komplexhomomorphismen  $f$  und  $g$  heißen **homotop**, wenn Homomorphismen  $D^i : A^{i+1} \rightarrow B^i$  für alle  $i \in \mathbb{Z}$  existieren, so dass  $f - g = Dd + dD$  gilt. Schreibweise:  $f \sim g$ .

$$\begin{array}{ccccccc} A^0 & \xrightarrow{d} & A^1 & \xrightarrow{d} & A^2 & \xrightarrow{d} & A^3 \\ f \Downarrow g & \swarrow D & f \Downarrow g & \swarrow D & f \Downarrow g & \swarrow D & f \Downarrow g \\ B^0 & \xrightarrow{d} & B^1 & \xrightarrow{d} & B^2 & \xrightarrow{d} & B^3 \end{array}$$

**Bemerkung.** Homotopie ist eine Äquivalenzrelation.

**Lemma 1.6.** Aus  $f \sim g$  folgt

$$H^i(f) = H^i(g) : H^i(A^\bullet) \longrightarrow H^i(B^\bullet)$$

für alle  $i \in \mathbb{Z}$ .

**Definition.** Ein Komplexhomomorphismus  $f : A^\bullet \rightarrow B^\bullet$  heißt **Homotopieäquivalenz**, wenn  $g : B^\bullet \rightarrow A^\bullet$  existiert mit  $g \circ f \sim \text{id}_A$  und  $f \circ g \sim \text{id}_B$ .

**Bemerkung.** Ist  $f$  eine Homotopieäquivalenz, so ist  $H^i(f) : H^i(A) \rightarrow H^i(B)$  ein Isomorphismus für alle  $i$ . Solche Homomorphismen nennt man **Quasi-Isomorphismen**. Nicht jeder Quasi-Isomorphismus ist eine Homotopieäquivalenz.

**Beispiel.** Betrachte den Komplexhomomorphismus

$$[0 \rightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \rightarrow 0] \rightarrow [0 \rightarrow 0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0].$$

Dieser ist ein Quasiisomorphismus. Wäre er eine Homotopieäquivalenz, so wäre er auch nach Tensorieren mit einer beliebigen abelschen Gruppe wieder eine Homotopieäquivalenz und insbesondere ein Quasisomorphismus. Tensorieren mit  $\mathbb{Z}/2\mathbb{Z}$  gibt aber den Komplexhomomorphismus

$$[0 \rightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \rightarrow 0] \rightarrow [0 \rightarrow 0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0],$$

welcher kein Quasiisomorphismus ist.

**Satz 1.7.** Gegeben seien zwei Komplexe

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & E^0 & \longrightarrow & E^1 & \longrightarrow & \dots \\ & & \varphi \downarrow & & & & & & \\ 0 & \longrightarrow & B & \longrightarrow & I^0 & \longrightarrow & I^1 & \longrightarrow & \dots \end{array}$$

Wir nehmen an:

- die obere Zeile ist exakt.
- alle  $I^i$ ,  $i \geq 0$ , sind injektiv.

Dann existiert ein Komplexhomomorphismus  $f$  von der oberen zur unteren Zeile mit  $f_{-1} = \varphi$ . Beliebige zwei solche  $f$  sind homotop.

**Korollar 1.8** ( $A = B$ ,  $\varphi = \text{id}_A$ ). Zwei injektive Auflösungen desselben Objekts sind homotopieäquivalent, die Homotopieäquivalenz ist wohlbestimmt bis auf Homotopie.

## 1.4 Abgeleitete Funktoren

Sei  $\mathcal{A}$  eine abelsche Kategorie mit genügend vielen Injektiven und sei  $F : \mathcal{A} \rightarrow \mathcal{B}$  ein linksexakter Funktor in eine abelsche Kategorie  $\mathcal{B}$ .

Wir wählen für  $A \in \text{ob}(\mathcal{A})$  eine injektive Auflösung  $A \rightarrow I^\bullet$  und setzen

$$R^i F(A) = H^i(FI^\bullet).$$

Nach 1.8 gibt eine andere injektive Auflösung in kanonischer Weise isomorphe Gruppen  $R^i F(A)$ . Ist nun  $\varphi : A \rightarrow B$  ein Homomorphismus und  $A \rightarrow I^\bullet$  und  $B \rightarrow J^\bullet$  injektive Auflösungen, so existiert nach 1.7 ein bis auf Homotopie eindeutiges  $f : I^\bullet \rightarrow J^\bullet$  mit  $H^0(f) = \varphi$ . So wird für alle  $i \in \mathbb{Z}$  die Zuordnung  $A \mapsto R^i F(A)$  zu einem Funktor  $\mathcal{A} \rightarrow \mathcal{B}$ .

**Definition.**  $R^i F(-) : \mathcal{A} \rightarrow \mathcal{B}$  heißt der  **$i$ -te rechtsabgeleitete Funktor** des linksexakten Funktors  $F$ .

**Lemma 1.9.** Es gilt  $R^i F = 0$  für  $i < 0$  und  $R^0 F = F$ . Ist  $F$  exakt, so gilt  $R^i F = 0$  für  $i > 0$ .

**Satz 1.10.** Für jede exakte Folge  $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$  in  $\mathcal{A}$  existieren natürliche Abbildungen

$$\delta^i : R^i F(A'') \longrightarrow R^{i+1} F(A')$$

für jedes  $i \geq 0$ , so dass die (lange) Folge

$$\begin{aligned} \cdots \rightarrow R^i F A' \rightarrow R^i F A \rightarrow R^i F A'' \\ \rightarrow R^{i+1} F A' \rightarrow R^{i+1} F A \rightarrow R^{i+1} F A'' \rightarrow \cdots \end{aligned}$$

exakt ist. Ist

$$\begin{array}{ccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' \longrightarrow 0 \end{array}$$

ein Homomorphismus exakter Folgen, so kommutiert für alle  $i \geq 0$  das Diagramm

$$\begin{array}{ccc} R^i F(A'') & \xrightarrow{\delta} & R^{i+1} F(A') \\ \downarrow & & \downarrow \\ R^i(FB'') & \xrightarrow{\delta} & R^{i+1} F(B'). \end{array}$$

**Linksabgeleitete Funktoren:** Man drehe alle Pfeile um:

$F : \mathcal{A} \rightarrow \mathcal{B}$  sei rechtsexakter Funktor und  $\mathcal{A}$  habe genügend viele Projektive. Wir wählen für jedes Objekt  $A$  eine projektive Auflösung

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

und setzen  $L_i F(A) := H_i(FP_\bullet)$ .

– alles analog –

## 1.5 Azyklische Objekte

Wie vorher sei  $\mathcal{A}$  abelsche Kategorie mit genügend vielen Injektiven und  $F : \mathcal{A} \rightarrow \mathcal{B}$  linksexakter Funktor.

**Definition.**  $A \in \text{ob}(\mathcal{A})$  heißt  **$F$ -azyklisch**, wenn  $R^i F A = 0$  für alle  $i \geq 1$  gilt.

**Lemma 1.11.** *Injektive sind  $F$ -azyklisch.*

**Satz 1.12.** *Sei  $A \rightarrow I^\bullet$  eine Auflösung durch  $F$ -azyklische, d.h.*

$$0 \longrightarrow A \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \dots$$

*ist exakt und  $I^i$  ist  $F$ -azyklisch für alle  $i \geq 0$ . Dann gibt es kanonische Isomorphismen*

$$R^i F A \cong H^i(F I^\bullet).$$

## 1.6 Universelle $\delta$ -Funktoren

Sei wie vorher  $\mathcal{A}$  eine abelsche Kategorie.

**Definition.** Ein (**exakter**)  **$\delta$ -Funktorkomplex**  $H = (H^n)_{n \in \mathbb{Z}}$  ist eine Familie von Funktoren  $H^n : \mathcal{A} \rightarrow \mathcal{B}$  zusammen mit Homomorphismen  $\delta : H^n(C) \rightarrow H^{n+1}(A)$  für jede kurze exakte Folge  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  in  $\mathcal{A}$ , so dass gilt

(i)  $\delta$  ist funktoriell, d.h. ist

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

ein kommutatives Diagramm mit exakten Zeilen in  $\mathcal{A}$  so kommutiert

$$\begin{array}{ccc} H^n(C) & \xrightarrow{\delta} & H^{n+1}(A) \\ \downarrow & & \downarrow \\ H^n(C') & \xrightarrow{\delta} & H^{n+1}(C) \end{array}$$

in  $\mathcal{B}$ .

(ii) Für jede kurze exakte Folge  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  in  $\mathcal{A}$  ist die lange Folge

$$\dots \longrightarrow H^n(A) \longrightarrow H^n(B) \longrightarrow H^n(C) \longrightarrow H^{n+1}(A) \longrightarrow \dots$$

exakt in  $\mathcal{B}$ .

**Beispiel.**  $\mathcal{A}$  habe genügend viele Injektive und  $F : \mathcal{A} \rightarrow \mathcal{B}$  sei linksexakt. Dann ist  $H^n := R^n F$  ein  $\delta$ -Funktorkomplex.



**Konvention:** Ist ein  $\delta$ -Funktorkur nur für gewisse  $H^n$  gegeben, so setzen wir  $H^m = 0$  für alle anderen Indizes.

**Definition.** Ein  $\delta$ -Funktorkur  $H = (H^n)_{n \geq 0} : \mathcal{A} \rightarrow \mathcal{B}$  heißt *universell*, wenn für jeden  $\delta$ -Funktorkur  $H' = (H'^n)_{n \geq 0} : \mathcal{A} \rightarrow \mathcal{B}$  sich jede natürliche Transformation  $f^0 : H^0 \rightarrow H'^0$  eindeutig zu einem Homomorphismus  $f : H \rightarrow H'$  von  $\delta$ -Funktoren ausdehnt.

**Bemerkung.** Das bedeutet, dass sich jeder linksexakte Funktorkur  $H^0$  höchstens auf eine Weise (d.h. wenn existent, dann bis auf Isomorphie eindeutig) zu einem universellen  $\delta$ -Funktorkur ausdehnen lässt.

**Definition.** Ein Funktorkur  $F$  heißt **auslöschbar**, wenn zu jedem  $A \in \text{ob}(\mathcal{A})$  ein Monomorphismus  $A \xrightarrow{u} A'$  existiert mit  $F(u) = 0$ .

**Satz 1.13.** Ein  $\delta$ -Funktorkur  $H = (H^n)_{n \geq 0}$  ist universell, wenn für jedes  $n \geq 1$  der Funktorkur  $H^n$  auslöschbar ist.

**Korollar 1.14.**  $\mathcal{A}$  habe genügend viele Injektive und  $F : \mathcal{A} \rightarrow \mathcal{B}$  sei linksexakt. Dann ist  $(R^n F)_{n \geq 0}$  ein universeller  $\delta$ -Funktorkur.

## 1.7 Tor und Ext

Sei  $R$  ein Ring. Wir betrachten den Bifunktorkur

$$- \otimes_R - : \text{Mod-}R \times R\text{-Mod} \longrightarrow \mathcal{A}b.$$

Dieser ist in beiden Variablen rechtsexakt.

In  $\text{Mod-}R$  und  $R\text{-Mod}$  existieren genügend viele Projektive, also:

für jeden  $R$ -Linksmodul  $N$  existiert  $L_n(- \otimes_R N) : \text{Mod-}R \rightarrow \mathcal{A}b$ .

für jeden  $R$ -Rechtsmodul  $M$  existiert  $L_n(M \otimes_R -) : R\text{-Mod} \rightarrow \mathcal{A}b$ .

**Satz 1.15.** Es gibt natürliche Isomorphismen

$$L_n(- \otimes_R N)(M) \cong L_n(M \otimes_R -)(N).$$

Man nennt diesen Funktorkur

$$\text{Tor}_n^R(M, N).$$

Er kann durch eine flache Auflösung in der ersten oder in der zweiten Variable berechnet werden.

Analog: Für  $\text{Hom}_R(-, -) : R\text{-Mod} \times R\text{-Mod} \rightarrow \mathcal{A}b$  (oder wahlweise auch Rechtsmoduln).

**Satz 1.16.**

$$R^n \text{Hom}_R(-, N)(M) \cong R^n \text{Hom}_R(M, -)(N)$$

und man bezeichnet diesen Funktor mit

$$\mathrm{Ext}_R^n(M, N).$$

Kann berechnet werden durch projektive Auflösung von  $M$  (= injektive Auflösung in  $(R\text{-Mod})^{\mathrm{op}}$ ) oder injektive Auflösung von  $N$ .

# Algebraische Zahlentheorie II

## Sommersemester 2022

Dr. Katharina Hübner

basierend auf Alexander Schmidts AZT2-Skript von 2014

### Inhaltsverzeichnis

<b>1</b>	<b>Gruppenhomologie</b>	<b>1</b>
1.1	Der Gruppenring . . . . .	1
1.2	$G$ -Moduln . . . . .	3
1.3	Homologie . . . . .	5
1.4	Induzierte Moduln . . . . .	8
1.5	Homologisch triviale Moduln . . . . .	10
1.6	Restriktion und Korestriktion . . . . .	11

## 1 Gruppenhomologie

### 1.1 Der Gruppenring

Sei  $G$  eine Gruppe und  $A$  ein kommutativer Ring.

**Definition.** Der **Gruppenring**  $A[G]$  besteht aus allen formalen Linearkombinationen

$$\sum_{g \in G} a_g \cdot g, \quad a_g = 0 \text{ für fast alle } g \in G.$$

Addition: Komponentenweise.

Multiplikation:  $(ag) \cdot (b \cdot h) = ab \cdot gh$  und linear fortsetzen. Das Element  $1_A \cdot e_G$  ist die 1 im Ring  $A[G]$ . Der Ring  $A[G]$  ist genau dann kommutativ, wenn  $G$  dies ist. Ein Gruppenhomomorphismus  $f : G \rightarrow H$  induziert einen Ringhomomorphismus  $A[G] \rightarrow A[H]$ ,  $\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g f(g)$ . Der Spezialfall  $H = 1$  hat einen eigenen Namen:

**Definition.** Der Ringhomomorphismus

$$\varepsilon_A : A[G] \longrightarrow A, \quad \sum a_g g \longmapsto \sum a_g,$$

heißt die **Augmentation(sabbildung)**.  $I_G^A := \ker(\varepsilon_A)$  heißt das **Augmentationsideal**.

**Lemma 1.1.** *Das Augmentationsideal  $I_G^A \subset A[G]$  ist als  $A$ -Modul frei über der Basis*

$$\{g - 1 \mid g \in G \setminus \{e\}\}.$$

*Ist  $S \subset G$  ein Erzeugendensystem, so erzeugt die Menge  $S - 1 = \{s - 1 \mid s \in S\}$   $I_G^A$  als  $A[G]$ -Links(Rechts-)ideal.*

*Beweis.* Die Elemente  $g - 1$ ,  $g \in G \setminus \{e\}$ , liegen in  $I_G^A$  und sind linear unabhängig über  $A$ . Sei  $\alpha = \sum_{i=1}^n a_i g_i \in I_G^A$ . Dann gilt  $\sum a_i = 0$ , also  $\alpha = \sum a_i (g_i - 1)$ . Wegen  $e - 1 = 0 \in A[G]$  folgt die erste Aussage. Für die zweite genügt es zu zeigen, dass für alle  $g \in G$  das Element  $g - 1$  im von  $S - 1$  erzeugten Linksideal liegt. Wegen  $s_1 s_2 - 1 = s_1(s_2 - 1) + s_1 - 1$  und

$$s^{-1} - 1 = -s^{-1}(s - 1)$$

folgt dies aus der Existenz einer Darstellung

$$g = s_1^{\pm 1} \cdot s_2^{\pm 1} \dots s_n^{\pm 1}, \quad s_i \in S.$$

□

**Definition.** Für  $g, h \in G$  heißt  $[g, h] = ghg^{-1}h^{-1}$  der **Kommutator** von  $g$  und  $h$  (oft in der Literatur auch  $(g, h) = g^{-1}h^{-1}gh$ .) Die durch alle Kommutatoren erzeugte Untergruppe  $[G, G]$  heißt die **Kommutatorgruppe**.

**Lemma 1.2.**  $[G, G]$  ist ein Normalteiler in  $G$ . Die Faktorgruppe  $G^{\text{ab}} = G/[G, G]$  ist abelsch.

*Beweis.* Für  $[G, G] \triangleleft G$  genügt es zu zeigen, dass für  $g, h_1, h_2 \in G$  gilt  $g[h_1, h_2]g^{-1} \in [G, G]$ . Dies ist klar wegen

$$\begin{aligned} g[h_1, h_2]g^{-1} &= gh_1h_2h_1^{-1}h_2^{-1}g^{-1} \\ &= gh_1g^{-1}gh_2g^{-1} \cdot gh_1^{-1}g^{-1}gh_2^{-1}g^{-1} \\ &= [gh_1g^{-1}, gh_2g^{-1}]. \end{aligned}$$

Wegen  $gh(hg)^{-1} = [g, h] \in [G, G]$  ist  $G^{\text{ab}} = G/[G, G]$  abelsch. □

**Bemerkung.** Der Funktor  $G \mapsto G^{\text{ab}}$  ist linksadjungiert zur natürlichen Inklusion  $\text{Ab} \subset (\text{Groups})$ .

Wir betrachten die Untergruppe  $I_G^2 = I_G \cdot I_G$  in  $I_G = I_G^{\mathbb{Z}}$ .

**Satz 1.3.** Für  $I_G = I_G^{\mathbb{Z}} \subset \mathbb{Z}[G]$  gilt  $I_G/I_G^2 \cong G^{\text{ab}}$ .

*Beweis.* Wir betrachten die Abbildung

$$\varphi: G \longrightarrow I_G/I_G^2, \quad g \longmapsto g - 1.$$

Wegen  $gh - 1 = (g - 1) + (h - 1) + \underbrace{(g - 1)(h - 1)}_{\in I_G^2}$

ist  $\varphi$  ein Gruppenhomomorphismus. Da  $I_G/I_G^2$  abelsch ist, gilt  $\varphi([G, G]) = 0$ . Dies induziert  $\tilde{\varphi}: G^{\text{ab}} \rightarrow I_G/I_G^2$ . Wir konstruieren die inverse Abbildung. Nach 1.1 ist  $I_G$  der freie  $\mathbb{Z}$ -Modul über der Menge  $W = \{g - 1 \mid g \neq e\}$ . Die Abbildung  $W \rightarrow G^{\text{ab}}$ ,  $(g - 1) \mapsto g[G, G]$  setzt sich daher eindeutig zu einem Homomorphismus abelscher Gruppen  $\psi: I_G \rightarrow G^{\text{ab}}$  fort. Wegen  $(g - 1)(h - 1) = (gh - 1) - (g - 1) - (h - 1)$  gilt

$$\psi((g - 1)(h - 1)) = gh[G, G] \cdot (g[G, G])^{-1} \cdot (h[G, G])^{-1} = 1,$$

also induziert  $\psi$  einen Homomorphismus  $\tilde{\psi}: I_G/I_G^2 \rightarrow G^{\text{ab}}$ . Schließlich sind  $\tilde{\psi}$  und  $\tilde{\varphi}$  zueinander invers.  $\square$

## 1.2 $G$ -Moduln

**Definition.** Ein  **$G$ -Links-Modul**  $A$  ist eine abelsche Gruppe  $A$  zusammen mit einer Operation  $G \times A \rightarrow A$ ,  $(g, a) \mapsto ga$  mit  $g(a_1 + a_2) = ga_1 + ga_2$ ,  $gh(a) = g(h(a))$  und  $ea = a$  für alle  $a \in A$ .  $G$ -Rechtsmoduln definiert man analog.

**Bemerkung.** Ein  $G$ -Links(Rechts)modul ist nichts anderes als ein  $\mathbb{Z}[G]$ -Links-(Rechts)modul.

Ist  $A$  ein  $G$ -Rechtsmodul, so können wir durch  $ga \stackrel{\text{df}}{=} ag^{-1}$   $A$  auch als  $G$ -Linksmodul auffassen. M.a.W., es gilt

**Lemma 1.4.** *Die folgenden Kategorien sind natürlich äquivalent:*

- (i)  $\mathbb{Z}[G]$ -Linksmoduln.
- (ii)  $G$ -Linksmoduln.
- (iii)  $G$ -Rechtsmoduln.
- (iv)  $\mathbb{Z}[G]$ -Rechtsmoduln.

**Beispiele.** •  $\mathbb{Z}[G]$  ist ein  $G$ -Modul.

• Sei  $L/K$  eine endliche Galoiserweiterung. Dann sind  $L^+$  und  $L^\times$   $\text{Gal}(L/K)$ -Moduln.

Im folgenden arbeiten wir immer mit Linksmoduln und machen, wann immer nötig, Rechtsmoduln zu Linksmoduln und umgekehrt.

**Beispiele.** • Für  $G$ -Linksmoduln  $A, B$  bilden wir das Tensorprodukt  $A \otimes_G B$  indem wir  $A$  als  $G$ -Rechtsmodul auffassen und dann  $A \otimes_{\mathbb{Z}[G]} B$  bilden. Anders gesagt:

$$A \otimes_G B = (A \otimes_{\mathbb{Z}} B) / ((g^{-1}a, b) - (a, gb)).$$

• Ist  $A$  ein  $G$ -Linksmodul, so wird  $\text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$  zum  $G$ -Linksmodul durch  $(g\varphi)(a) := \varphi(g^{-1}a)$ .

**Definition.** Wir nennen einen  $G$ -Modul **frei**, wenn er frei als  $\mathbb{Z}[G]$ -Modul ist.

### Operationen auf $G$ -Moduln

- 1) **Tensorprodukt:**  $A \otimes_{\mathbb{Z}} B$  wird zum  $G$ -Modul durch  $g(a \otimes b) = ga \otimes gb$ .
- 2) **Homomorphismen:**  $\text{Hom}_{\mathbb{Z}}(A, B)$  wird zum  $G$ -Modul durch  $(g\varphi)(a) = g\varphi(g^{-1}a)$ .
- 3) **Invarianten:**

$$A^G = \{a \in A \mid ga = a \quad \forall g \in G\}$$

heißt die (Unter)Gruppe der **( $G$ -)Invarianten** von  $A$ .

Es gilt  $\text{Hom}_{\mathbb{Z}}(A, B)^G = \text{Hom}_G(A, B)$

- 4) **Koinvarianten:**

$$A_G = A / \{(ga - a), g \in G, a \in A\} = A / I_G \cdot A$$

heißt die Gruppe der **Koinvarianten** von  $A$ .

Es gilt  $(A \otimes_{\mathbb{Z}} B)_G = A \otimes_G B$ .

**Definition.** Wir nennen einen  $G$ -Modul  $A$  **trivial**, wenn  $ga = a \quad \forall g \in G, a \in A$ .

**Lemma 1.5.** (i)  $A^G$  ist der größte triviale Untermodul von  $A$

(ii)  $A_G$  ist der größte triviale Faktormodul von  $A$ .

*Beweis.* Klar. □

Sei nun  $U \subset G$  eine Untergruppe. Wir betrachten den Vergissfunktor

$$\text{Res}_U^G: G\text{-Mod} \longrightarrow U\text{-Mod}$$

**Lemma 1.6.**  $\text{Res}_U^G$  überführt freie in freie und projektive in projektive Moduln.

*Beweis.* Sei  $(x_i)$  ein Repräsentantensystem von Rechtsnebenklassen  $U \backslash G$ . Dann ist  $G$  die disjunkte Vereinigung der Mengen  $Ux_i$ . Für fixiertes  $i$  ist der  $U$ -Untermodul

$$M_i := \left\{ \sum_{g \in Ux_i} a_g g \mid a_g = 0 \text{ für fast alle } g \right\} \subset \mathbb{Z}[G]$$

isomorph zu  $\mathbb{Z}[U]$ , also frei. Daher ist

$$\operatorname{Res}_U^G \mathbb{Z}[G] \cong \bigoplus_i M_i$$

freier  $\mathbb{Z}[U]$ -Modul. Da  $\operatorname{Res}_U^G$  mit der direkten Summe vertauscht, gilt  $\operatorname{Res}_U^G$  (freier  $G$ -Modul) = freier  $U$ -Modul. Ist nun  $P$  ein projektiver  $G$ -Modul so existiert ein (projektiver)  $G$ -Modul  $Q$  mit  $P \oplus Q$  frei. Daher ist  $\operatorname{Res}_U^G P$  direkter Summand im freien  $U$ -Modul  $\operatorname{Res}_U^G(P \oplus Q)$ , also projektiv.  $\square$

### 1.3 Homologie

Wir fassen  $\mathbb{Z}$  als trivialen  $G$ -Modul auf. Dann gilt für jeden  $G$ -Modul  $A$

$$A_G = (A \otimes_{\mathbb{Z}} \mathbb{Z})_G = A \otimes_G \mathbb{Z}.$$

Daher ist der Funktor

$$-_G: G\text{-Mod} \longrightarrow \mathcal{A}b, \quad A \longmapsto A_G,$$

rechtsexakt und es gilt

$$L_n(-_G)(A) = \operatorname{Tor}_n^{\mathbb{Z}[G]}(A, \mathbb{Z}).$$

**Definition.**  $H_n(G, A) \stackrel{\text{df}}{=} L_n(-_G)(A)$  heißt die  **$n$ -te Homologiegruppe von  $G$  mit Werten in  $A$** .

Wegen der Gleichheit  $H_n(G, A) = \operatorname{Tor}_n^{\mathbb{Z}[G]}(A, \mathbb{Z})$  haben wir die folgenden Berechnungsmethoden:

- 1) Wähle projektive Auflösung  $Q_\bullet \rightarrow A$ . Dann gilt  $H_n(G, A) = H_n((Q_\bullet)_G)$
- 2) oder wähle projektive Auflösung  $P^\bullet \rightarrow \mathbb{Z}$ . Dann gilt  $H_n(G, A) = H_n(A \otimes_G P^\bullet)$ .

Wir konstruieren nun eine freie Auflösung von  $\mathbb{Z}$ .

Setze für  $n \geq 0$ :

$$\begin{aligned} X_n &= \mathbb{Z}[G^{n+1}] = \mathbb{Z}[\overbrace{G \times \cdots \times G}^{n+1 \text{ Faktoren}}] \\ &= \{\text{freie ab. Gruppe über } (n+1)\text{-Tupel} \\ &\quad (g_0, \dots, g_n), \quad g_i \in G, \quad i = 0, \dots, n\}, \end{aligned}$$

mit  $G$ -Modulstruktur gegeben durch

$$g(g_0, \dots, g_n) = (gg_0, \dots, gg_n).$$

- $X_n$  ist ein freier  $G$ -Modul, Basis die  $(n+1)$ -Tupel der Form  $(e, g_1, \dots, g_n)$ .
- Wir machen  $X_\bullet$  zu einem Komplex indem wir  $G$ -Modulhomomorphismen

$$d: X_{n+1} \longrightarrow X_n$$

durch  $d((g_0, \dots, g_{n+1})) = \sum_{i=0}^{n+1} (-1)^i (g_0, \dots, g_{i-1}, g_{i+1} \cdots g_{n+1})$  definieren.

**Lemma 1.7.**  $X_\bullet$  ist ein Komplex, d.h.  $d \circ d = 0$ .

*Beweis.* Wir betrachten

$$d \circ d: X_{n+2} \longrightarrow X_n.$$

Es gilt

$$\begin{aligned} d \circ d((g_0, \dots, g_{n+2})) &= d \left( \sum_{i=0}^{n+2} (-1)^i (g_0, \dots, \widehat{g}_i, \dots, g_{n+2}) \right) \\ &= \sum_{j=0}^{n+1} (-1)^j \cdot \sum_{i=0}^{n+2} (-1)^i \overbrace{(g_0, \dots, \widehat{g}_i, \dots, g_{n+2})}^{\text{hieraus die } j\text{-te Komp. entfernen}}. \end{aligned}$$

Für  $j < i$  erhalten wir

$$(g_0, \dots, \widehat{g}_j, \dots, \widehat{g}_i, \dots, g_{n+2}) \cdot (-1)^{i+j}.$$

Für  $j \geq i$

$$(g_0, \dots, \widehat{g}_i, \dots, \widehat{g}_{j+1}, \dots, g_{n+2}) \cdot (-1)^{i+j}.$$

M.a.W.: Der Term  $(g_0, \dots, \widehat{g}_a, \dots, \widehat{g}_b, \dots, g_{n+2})$   $a < b$  taucht auf

für  $j = a, i = b$  mit Vorfaktor  $(-1)^{a+b}$  und

für  $i = a, j = b - 1$  mit Vorfaktor  $(-1)^{a+b-1}$ .  $\square$

**Lemma 1.8.** Es ist  $\varepsilon \circ d_0: X_1 \xrightarrow{d_0} X_0 = \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z}$  die Nullabbildung.

*Beweis.* Für  $g_0, g_1 \in G$  beliebig gilt  $\varepsilon \circ d_0((g_0, g_1)) = \varepsilon(g_1 - g_0) = 1 - 1 = 0$ .  $\square$

**Satz 1.9.**  $X_\bullet \rightarrow \mathbb{Z}$  ist eine freie Auflösung von  $\mathbb{Z}$  als  $G$ -Modul.

*Beweis.* Wir setzen  $d_{-1} = \varepsilon$ . Z.z.: der Komplex

$$\dots \rightarrow X_3 \longrightarrow X_2 \xrightarrow{d_1} X_1 \xrightarrow{d_0} X_0 \xrightarrow{d_{-1}} \mathbb{Z} \longrightarrow 0$$

ist exakt. Zum Beweis geben wir eine Nullhomotopie an, also Abbildungen  $(D_i: X_i \rightarrow X_{i+1}), i \in \mathbb{Z}$ , mit  $d_i \circ D_i + D_{i-1} \circ d_{i-1} = \text{id}_{X_i}$ . Dann induzieren die homotopen Komplexhomomorphismen  $\text{id}$  und  $0$  die gleichen Abbildungen auf der Homologie, weshalb die Homologie Null und somit der Komplex exakt ist.

Nun setze  $D_{-1}: \mathbb{Z} \rightarrow \mathbb{Z}[G], 1 \mapsto 1e$ , und für  $n \geq 0$ :

$$D_n: X_n \longrightarrow X_{n+1}, (g_0, \dots, g_n) \longmapsto (e, g_0, \dots, g_n).$$

Wir berechnen:

$$\begin{array}{ccccccccccc} X_3 & \longrightarrow & X_2 & \longrightarrow & X_1 & \xrightarrow{d_0} & X_0 & \xrightarrow{d_{-1}} & \mathbb{Z} & \longrightarrow & 0 \\ \Downarrow & \swarrow D_2 & \Downarrow & \swarrow D_1 & \Downarrow & \swarrow D_0 & \Downarrow & \swarrow D_{-1} & \Downarrow & & \\ X_3 & \longrightarrow & X_2 & \longrightarrow & X_1 & \xrightarrow{d_0} & X_0 & \xrightarrow{d_{-1}} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$



Zunächst gilt  $d_{-1}D_{-1}(1) = \varepsilon(e) = 1$ . Wir haben für  $g \in G \subset X_0$

$$d_0D_0(g) + D_{-1}d_{-1}(g) = d_0((e, g)) + D_{-1}(1) = g - e + e = g.$$

Für  $n \geq 1$ :

$$\begin{aligned} & d_n \circ D_n((g_0, \dots, g_n)) + D_{n-1} \circ d_{n-1}(g_0, \dots, g_n) \\ &= d_n((e, g_0, \dots, g_n) + D_{n-1} \left( \sum_{i=0}^n (-1)^i (g_0, \dots, \widehat{g}_i, \dots, g_n) \right)) \\ &= \sum_{i=0}^{n+1} (-1)^i \overbrace{(e, g_0, \dots, g_n)}^{i\text{-te Komp. weg}} + \sum_{i=0}^n (-1)^i \overbrace{(e, g_0, \dots, g_n)}^{i+1\text{-te Komp. weg}} \\ &= (g_0, \dots, g_n). \end{aligned}$$

□

**Korollar 1.10.** Es gilt

$$H_n(G, A) = H_n((A \otimes_{\mathbb{Z}} X_{\bullet})_G).$$

**Bemerkung.** Man kann die Folgerung zur Definition machen. Dann muß man aber später vieles mühsam nachrechnen.

**Satz 1.11.** Es gilt

$$H_1(G, \mathbb{Z}) \cong G^{\text{ab}}.$$

*Beweis.* Wir betrachten die exakte Folge

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Da  $\mathbb{Z}[G]$  frei ist, folgt aus der exakten Folge

$$\begin{aligned} 0 = H_1(G, \mathbb{Z}[G]) &\rightarrow H_1(G, \mathbb{Z}) \rightarrow H_0(G, I_G) \rightarrow \\ &H_0(G, \mathbb{Z}[G]) \rightarrow H_0(G, \mathbb{Z}) \rightarrow 0 \end{aligned}$$

die Exaktheit der Folge

$$0 \longrightarrow H_1(G, \mathbb{Z}) \longrightarrow (I_G)_G \longrightarrow (\mathbb{Z}[G])_G \xrightarrow{\bar{\varepsilon}} \mathbb{Z} \longrightarrow 0$$

Nun gilt  $(\mathbb{Z}[G])_G = \mathbb{Z}[G]/I_G\mathbb{Z}[G] = \mathbb{Z}[G]/I_G$  also ist  $\bar{\varepsilon}$  ein Isomorphismus. Wir erhalten

$$H_1(G, \mathbb{Z}) \cong (I_G)_G = I_G/I_G^2$$

und nach 1.3 gilt  $I_G/I_G^2 \cong G^{\text{ab}}$ .

□

**Lemma 1.12.** Für  $G = \{1\}$  gilt

$$H_i(\{1\}, A) = 0 \quad \forall i \geq 1.$$

*Beweis.* Für  $G = \{1\}$  gilt  $\mathbb{Z}[G] = \mathbb{Z}$ . Daher:  $H_i(\{1\}, A) = \text{Tor}_i^{\mathbb{Z}}(A, \mathbb{Z}) = 0$  für  $i \geq 1$ , weil  $\mathbb{Z}$  ein flacher  $\mathbb{Z}$ -Modul ist.

Alternativer Beweis: Für  $G = \{1\}$  ist die Kategorie der  $G$ -Moduln gleich der Kategorie der abelschen Gruppen und  $(-)_G$  ist der identische Funktor, also exakt  $\Rightarrow L_i(-_G) = 0 \quad \forall i \geq 1$ .

□

## 1.4 Induzierte Moduln

**Definition.** Sei  $A$  ein  $G$ -Modul. Dann heißt  $\text{Ind}_G A = \mathbb{Z}[G] \otimes A$  der induzierte Modul zu  $A$ .

**Bemerkung.**  $\text{Ind}_G : G\text{-Mod} \rightarrow G\text{-Mod}$  ist ein exakter Funktor.

**Definition.** Ein  $G$ -Modul  $B$  heißt **induziert**, wenn es einen  $G$ -Modul  $A$  und einen Isomorphismus  $B \cong \text{Ind}_G A$  gibt.

*Bezeichnung:* Mit  $A^{\text{tr}}$  bezeichnen wir den  $G$ -Modul, der die gleiche unterliegende abelsche Gruppe hat wie  $A$ , aber triviale  $G$ -Wirkung.

**Lemma 1.13.** *Es gibt einen natürlichen Isomorphismus  $\text{Ind}_G A^{\text{tr}} \xrightarrow{\sim} \text{Ind}_G A$ .*

*Beweis.* Als abelsche Gruppe gilt

$$\text{Ind}_G A = \mathbb{Z}[G] \otimes A = \bigoplus_{g \in G} gA.$$

Daher setzt sich die Abbildung

$$g \otimes a \mapsto g \otimes ga$$

zu einem Homomorphismus

$$\varphi : \mathbb{Z}[G] \otimes A^{\text{tr}} \longrightarrow \mathbb{Z}[G] \otimes A$$

fort. Dies ist ein Isomorphismus,  $\varphi^{-1}$  ist gegeben durch  $\varphi^{-1}(g \otimes a) = g \otimes g^{-1}a$ . Nun gilt für  $g, h \in G$ ,  $a \in A^{\text{tr}}$ ,

$$g\varphi(h \otimes a) = g(h \otimes ha) = gh \otimes gha = \varphi(gh \otimes a) = \varphi(g(\underbrace{h \otimes a}_{\in \mathbb{Z}[G] \otimes A^{\text{tr}}})).$$

Daher ist  $\varphi$  ein Homomorphismus von  $G$ -Moduln. □

Sei nun  $U \subset G$  eine Untergruppe und sei  $A$  ein  $U$ -Modul.

**Definition.**

$$\text{Ind}_G^U A = \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} A.$$

$\text{Ind}_G^U$  wird zum  $G$ -Modul durch  $g(h \otimes_{\mathbb{Z}[U]} a) = gh \otimes_{\mathbb{Z}[U]} a$ .

**Bemerkung.** Für den Spezialfall  $U = \{1\}$  gibt uns 1.13 die natürliche Äquivalenz von Funktoren

$$\text{Ind}_G \simeq \text{Ind}_G^{\{1\}} \circ \text{Res}_{\{1\}}^G : G\text{-Mod} \longrightarrow G\text{-Mod},$$

wobei  $\text{Res}_{\{1\}}^G : G\text{-Mod} \rightarrow \{1\}\text{-Mod} = \mathcal{A}b$  der Vergiss-Funktor ist.

Sei  $S \subset G$  ein System von Vertretern der Linksnebenklassen  $G/U$ . Dann gilt als abelsche Gruppe

$$\begin{aligned}\text{Ind}_G^U A &= \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} A \\ &= \mathbb{Z}[U]^S \otimes_{\mathbb{Z}[U]} A \\ &= \bigoplus_{s \in S} s \cdot A.\end{aligned}$$

Sei OE  $e \in S$ . Dann identifizieren wir  $A$  mit der Untergruppe  $e \cdot A \subseteq \text{Ind}_G^U A$ . Die  $G$ -Wirkung auf  $\bigoplus_{s \in S} sA$  ist die folgende:

Für  $g \in G$ ,  $s \in S$  existieren eindeutig bestimmte  $s_g \in S$ ,  $u_g \in U$  mit  $gs = s_g u_g$ . Daher gilt

$$g(s \cdot a) = g \cdot s \cdot a = s_g \cdot u_g \cdot a.$$

Für  $u \in U$  gilt daher  $u \cdot e \cdot a = e \cdot ua$ , d.h.  $A$  identifiziert sich mit  $eA \subset \text{Ind}_G^U A$  als  $U$ -Modul.

Ist nun  $B$  ein  $G$ -Modul und  $\varphi : \text{Ind}_G^U A \rightarrow B$  ein  $G$ -Homomorphismus, so ist  $\varphi|_{eA} : A \rightarrow B$  ein  $U$ -Homomorphismus. Ist umgekehrt  $\psi : A \rightarrow B$  ein  $U$ -Homomorphismus, so setze für  $s \in S$

$$\psi(sa) = s\psi(a) \in B.$$

Wir erhalten so eine Ausdehnung von  $\psi : eA \rightarrow B$  zu  $\tilde{\psi} : \bigoplus_{s \in S} sA \rightarrow B$ .

Für  $g \in G$ ,  $s \in S$ ,  $a \in A$  gilt

$$\begin{aligned}\tilde{\psi}(gsa) &= \tilde{\psi}(s_g u_g a) = s_g \psi(u_g a) \\ &= s_g u_g \psi(a) \\ &= gs \psi(a) = g \cdot \tilde{\psi}(sa).\end{aligned}$$

Daher ist  $\tilde{\psi}$  ein  $G$ -Homomorphismus

$$\tilde{\psi} : \text{Ind}_G^U A \longrightarrow B.$$

$\tilde{\psi}$  ist der eindeutige  $G$ -Homomorphismus  $\tilde{\psi} : \text{Ind}_G^U A \rightarrow B$ , der den  $U$ -Homomorphismus  $\psi : eA \rightarrow B$  fortsetzt (gleiche Rechnung rückwärts).

Bezeichnen wir mit  $\text{Res}_U^G : G\text{-Mod} \rightarrow U\text{-Mod}$  den Vergiss-Funktor, so erhalten wir:

**Satz 1.14** („Frobenius-Reziprozität“). *Es gilt*

$$\text{Ind}_G^U \dashv \text{Res}_U^G.$$

Beide Funktoren sind exakt.  $\text{Ind}_G^U$  überführt projektive  $U$ -Moduln in projektive  $G$ -Moduln und  $\text{Res}_U^G$  überführt injektive  $G$ -Moduln in injektive  $U$ -Moduln.

*Beweis.* Die Adjunktion haben wir gerade bewiesen.  $\text{Res}_U^G$  ist offensichtlich exakt.  $\text{Ind}_G^U A = \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} A$  und weil  $\mathbb{Z}[G]$  ein freier  $\mathbb{Z}[U]$ -Modul ist (siehe 1.6) ist auch  $\text{Ind}_G^U$  exakt. Die verbleibenden Aussagen folgen aus ??.

Schließlich bemerken wir:

**Lemma 1.15.** *Sei  $G$  eine Gruppe und sei  $A$  ein induzierter  $G$ -Modul. Dann ist für jede Untergruppe  $U \subset G$  der Modul  $\text{Res}_U^G A$  ein induzierter  $U$ -Modul.*

*Beweis.* Sei  $A = \text{Ind}_G B$  und nach 1.13 sei ohne Einschränkung  $B$  ein trivialer  $G$ -Modul. Dann gilt

$$\begin{aligned} A &= \mathbb{Z}[G] \otimes_{\mathbb{Z}} B \\ &= \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} \mathbb{Z}[U] \otimes_{\mathbb{Z}} B \\ (\text{als } U\text{-Modul}) &\cong \mathbb{Z}[U]^{(S)} \otimes_{\mathbb{Z}[U]} \mathbb{Z}[U] \otimes_{\mathbb{Z}} B \\ &\cong \mathbb{Z}[U]^{(S)} \otimes_{\mathbb{Z}} B \\ &\cong (\mathbb{Z}[U] \otimes_{\mathbb{Z}} B)^{(S)} \\ &= \mathbb{Z}[U] \otimes_{\mathbb{Z}} B^{(S)} \end{aligned}$$

wobei  $S$  ein Repräsentantensystem von  $G/U$  ist.

## 1.5 Homologisch triviale Moduln

Im folgenden lassen wir die Bezeichnung  $\text{Res}_U^G$  weg und fassen, wenn nötig,  $A$  als  $U$ -Modul auf.

**Definition.** Ein  $G$ -Modul  $M$  heißt **homologisch trivial**, wenn  $H_n(U, M) = 0$  für alle  $n \geq 1$  und jede Untergruppe  $U \subset G$ .

**Bemerkung.** Projektive Moduln sind homologisch trivial: (Nach 1.6 ist  $M$  auch projektiver  $U$ -Modul für jedes  $U \subset G$ ).

**Satz 1.16.** *Induzierte Moduln sind homologisch trivial.*

*Beweis.* Nach 1.15 und 1.13 g.z.z.:  $H_n(G, \text{Ind}_G A) = 0$  für alle  $n \geq 1$  und jeden trivialen  $G$ -Modul  $A$ . Nun gilt:

$$\begin{aligned} H_n(G, \text{Ind}_G A) &= H_n(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}} A) \\ &= H_n(P_{\bullet} \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] \otimes_{\mathbb{Z}} A) = H_n(P_{\bullet} \otimes_{\mathbb{Z}} A) \end{aligned}$$

wobei  $P_{\bullet} \rightarrow \mathbb{Z}$  eine beliebige projektive Auflösung von  $\mathbb{Z}$  als  $G$ -Modul ist. Nach 1.6 ist  $P_{\bullet} \rightarrow \mathbb{Z}$  insbesondere eine projektive Auflösung in  $\mathcal{A}b$ . Daher gilt für  $n \geq 1$ :

$$\begin{aligned} H_n(P_{\bullet} \otimes_{\mathbb{Z}} A) &= \text{Tor}_n^{\mathbb{Z}}(\mathbb{Z}, A) \\ &= 0. \end{aligned}$$

□

Sei nun  $A$  ein  $G$ -Modul. Tensoriert man die Augmentation  $\varepsilon: \mathbb{Z}[G] \rightarrow \mathbb{Z}$  mit  $A$  erhält man eine exakte Folge

$$0 \longrightarrow A_1 \longrightarrow \text{Ind}_G A \longrightarrow A \longrightarrow 0.$$

Setzt man mit  $\text{Ind}_G A_1 \rightarrow A_1$  fort, so erhält man induktiv eine natürliche Auflösung von  $A$  durch homologisch triviale Moduln.

Dieses Vorgehen läßt sich verallgemeinern.

**Satz 1.17** (Shapiro-Lemma). *Sei  $U \subset G$  eine Untergruppe und  $A$  ein  $U$ -Modul. Dann gilt*

$$H_n(U, A) \cong H_n(G, \text{Ind}_G^U A)$$

für alle  $n \geq 0$ .

*Beweis.* Sei  $P \rightarrow \mathbb{Z}$  eine Auflösung durch projektive  $G$ -Moduln. Dann gilt

$$\begin{aligned} H_n(G, \text{Ind}_G^U A) &= H_n(P_\bullet \otimes_{\mathbb{Z}[G]} \text{Ind}_G^U A) \\ &= H_n(P_\bullet \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} A) \\ &= H_n(P_\bullet \otimes_{\mathbb{Z}[U]} A) \\ &= H_n(U, A) \end{aligned}$$

weil  $P_\bullet \rightarrow \mathbb{Z}$  auch eine Auflösung durch projektive  $U$ -Moduln ist. □

## 1.6 Restriktion und Korestriktion

Sei  $U \subset G$  eine Untergruppe und  $A$  ein  $G$ -Modul. Wir konstruieren eine natürliche Abbildung  $\text{cor}_G^U: H_n(U, A) \rightarrow H_n(G, A)$  für alle  $n \geq 0$ .

Sei  $M$  ein  $G$ -Modul. Dann haben wir eine natürliche Abbildung  $M_U \xrightarrow{\text{kan}} M_G$ . Ist nun  $P_\bullet \rightarrow \mathbb{Z}$  eine  $G$ -projektive Auflösung, so erhalten wir (setze  $M = P_i \otimes A$ ) eine Abbildung

$$(P_\bullet \otimes A)_U \longrightarrow (P_\bullet \otimes A)_G$$

**Definition.** Die auf der Homologie induzierte Abbildung

$$\text{cor}_G^U: H_n(U, A) \longrightarrow H_n(G, A)$$

heißt die **Korestriktion(sabbildung)**.

**Beispiel.**  $A = \mathbb{Z}$ ,  $n = 1$ .

$$\text{cor}_G^U: U^{\text{ab}} = H_1(U, \mathbb{Z}) \longrightarrow H_1(G, \mathbb{Z}) = G^{\text{ab}}$$

ist die natürliche, durch  $U \hookrightarrow G$  induzierte Abbildung auf den Abelsierungen.

Nun nehmen wir an, dass  $(G : U) < \infty$  gilt. Für jeden  $G$ -Modul  $M$  haben wir die „Norm-Abbildung“

$$M_G \longrightarrow M_U \quad , \quad m \longmapsto \sum_{s \in U \setminus G} sm.$$

Diese ist wohldefiniert, denn für  $u \in U$  gilt  $usm - sm = (u - 1)(sm) \in I_U M$ , d.h. wir erhalten  $M \xrightarrow{N} M_U$ . Für  $g \in G$ ,  $m \in M$  gilt

$$\begin{aligned} N((g - 1)m) &= \sum_{s \in U \setminus G} sgm - sm \\ &= \sum_{s \in U \setminus G} sgm - \sum_{s \in U \setminus G} sm. \end{aligned}$$

Nun ist die Multiplikation von rechts mit  $g$  eine Bijektion  $U \setminus G \rightarrow U \setminus G$ , also gilt  $N((g - 1)m) = 0$ . Wir erhalten  $N : M_G = M/I_G M \rightarrow M_U$ . Angewendet auf eine projektive Auflösung  $P_\bullet \otimes A$  erhalten wir eine Abbildung

$$(P_\bullet \otimes A)_G \longrightarrow (P_\bullet \otimes A)_U.$$

**Definition.** Die auf der Homologie induzierte Abbildung  $\text{res}_U^G : H_n(G, A) \rightarrow H_n(U, A)$  heißt die **Restriktion**.

**Beispiel.** Für  $(G : U) < \infty$ ,  $n = 1$ ,  $A = \mathbb{Z}$ , erhalten wir einen (mysteriösen) Homomorphismus

$$\text{Ver} : G^{\text{ab}} \longrightarrow U^{\text{ab}}.$$

Dieser heißt **Verlagerung**.

Ein der für die Zahlentheorie wichtiger gruppentheoretischer Satz ist der

**Satz 1.18** (Hauptidealsatz). *Sei  $G$  eine endlich erzeugte Gruppe und wir nehmen an, dass die Kommutatorgruppe  $H = [G, G] \subset G$  endlichen Index hat. Dann ist die Verlagerung*

$$\text{Ver} : G^{\text{ab}} \longrightarrow H^{\text{ab}}$$

*die Nullabbildung.*

*Beweis.* Siehe Neukirch: „Zahlentheorie“. □

Zurück zur alten Situation  $(G : U) = n < \infty$ . Die Komposition der konstruierten Abbildungen

$$M_G \xrightarrow{N} M_U \xrightarrow{\text{kan}} M_G$$

ist die Multiplikation mit  $n$ , denn

$$\sum_{s \in U \setminus G} sm - n \cdot m = \sum_{s \in U \setminus G} (s - 1)m \in I_G M.$$

Wir wenden das auf  $P_\bullet \otimes A$  an und erhalten:

**Satz 1.19.** Für  $(G:U) = n < \infty$  gilt  $\text{cor}_G^U \circ \text{res}_U^G = n \cdot \text{id}$ .

**Korollar 1.20.** Sei  $G$  eine endliche Gruppe der Ordnung  $n$  und sei  $A$  ein  $G$ -Modul, so dass die  $n$ -Multiplikation  $A \xrightarrow{\cdot n} A$  ein Isomorphismus ist. Dann gilt

$$H_i(G, A) = 0 \quad \forall i \geq 1.$$

*Beweis.* Nach 1.19 sind die Selbstabbildungen  $\text{cor}_G^{\{1\}} \text{res}_{\{1\}}^G$  und  $\cdot n$  von  $H_i(G, A)$  dieselben. Nach Voraussetzung ist  $\cdot n$  ein Isomorphismus und wegen  $H_i(\{1\}, A) = 0$  für  $i \geq 1$  ist  $\text{cor} \circ \text{res}$  die Nullabbildung. Die Nullabbildung ist aber nur auf der trivialen Gruppe ein Isomorphismus.  $\square$

**Korollar 1.21.** (i) Sei  $G$  eine endliche Gruppe und  $A$  ein  $G$ -Modul der als abelsche Gruppe eindeutig teilbar ist. Dann gilt  $H_i(G, A) = 0 \quad \forall i \geq 1$ .

(ii) Sei  $G$  eine endliche Gruppe und sei  $A$  ein endlicher  $G$ -Modul. Gilt  $(\#G, \#A) = 1$ , so folgt

$$H_i(G, A) = 0$$

für alle  $i \geq 1$ .

# Algebraische Zahlentheorie II

## Sommersemester 2022

Dr. Katharina Hübner

basierend auf Alexander Schmidts AZT2-Skript von 2014

### Inhaltsverzeichnis

<b>1</b>	<b>Gruppenkohomologie</b>	<b>1</b>
1.1	Diskrete $G$ -Moduln . . . . .	1
1.2	Kohomologie . . . . .	3
1.3	Der Kohomologische Standardkomplex . . . . .	7
1.4	Funktorialität . . . . .	10
1.5	Die Korestriktion . . . . .	13
1.6	Das Cup-Produkt . . . . .	15
1.7	Proendliche Gruppen – Reduktion auf endliche Gruppen . . . . .	20
1.8	Abstrakte Gruppen – Beziehung zwischen Homologie und Kohomologie . . . . .	22

## 1 Gruppenkohomologie

### 1.1 Diskrete $G$ -Moduln

Sei  $G$  eine proendliche Gruppe. Mit  $G^{\text{abst}}$  bezeichnen wir die unterliegende Gruppe, d.h. das Bild von  $G$  unter dem Vergissfunktork:

$$(\text{topologische Gruppen}) \rightarrow (\text{Gruppen}).$$

**Definition.** Ein abstrakter  $G$ -Modul ist ein  $G^{\text{abst}}$ -Modul.

**Satz 1.1.** Sei  $G$  eine proendliche Gruppe und  $A$  ein abstrakter  $G$ -Modul. Dann sind die folgenden Bedingungen äquivalent

(i) die  $G$ -Wirkung

$$G \times A \longrightarrow A, (g, a) \longmapsto ga,$$

ist stetig bzgl. der diskreten Topologie auf  $A$ .



- (ii) Für jedes  $a \in A$  ist  $G_a := \{g \in G, ga = a\}$  offen in  $G$ .  
 (iii)  $A = \bigcup_{U \subset G} A^U$ , wobei  $U$  die offenen Normalteiler von  $G$  durchläuft.

*Beweis.* (i)  $\Rightarrow$  (ii) Sei  $a \in A$  beliebig und wir bezeichnen die  $G$ -Wirkung mit

$$m : G \times A \longrightarrow A.$$

Dann sind die Teilmengen

$$m^{-1}(a), G \times \{a\} \subseteq G \times A$$

offen, also auch ihr Durchschnitt

$$\{(g, a) \mid g \in G, ga = a\}.$$

Die Projektion  $p_1 : G \times A \rightarrow G$  ist offen, daher ist

$$G_a = \{g \in G \mid ga = a\} \subset G$$

offen.

(ii)  $\Rightarrow$  (iii) Wegen  $e \in G_a$  folgt die Existenz eines offenen Normalteiler  $U_a \subset G$  mit  $U \subset G_a$  und somit  $a \in A^{U_a}$ . Daher  $A = \bigcup_U A^U$ .

(iii)  $\Rightarrow$  (i) Sei  $(g, a) \in G \times A$ . Es existiert ein offener Normalteiler  $U \subset G$  mit  $a \in A^U$ . Daher gilt

$$m(gU \times \{a\}) = ga,$$

d.h.  $gU \times \{a\}$  ist eine offene Umgebung von  $(g, a)$  in  $m^{-1}(ga)$ . Daher ist  $m$  stetig.  $\square$

**Definition.** Ein diskreter  $G$ -Modul  $A$  ist ein  $G^{\text{abst}}$ -Modul  $A$ , der den äquivalenten Bedingungen von 1.1 genügt. Wir bezeichnen die Kategorie der diskreten  $G$ -Moduln mit (automatisch stetigen)  $G$ -Homomorphismen mit  $G\text{-Mod}$ .

**Bemerkung.**  $G\text{-Mod}$  ist eine abelsche Kategorie.

**Definition.** Für einen abstrakten  $G$ -Modul  $A$  heißt der Modul

$$A^\delta := \bigcup_{\substack{U \subset G \\ \text{offen}}} A^U \subset A$$

der assoziierte diskrete  $G$ -Modul.

**Lemma 1.2.** Der Funktor

$$\begin{aligned} \bullet^\delta : G^{\text{abst}}\text{-Mod} &\longrightarrow G\text{-Mod} \\ A &\longmapsto A^\delta \end{aligned}$$

ist rechtsadjungiert zur Inklusion

$$G\text{-Mod} \hookrightarrow G^{\text{abst}}\text{-Mod}$$

$\bullet^\delta$  ist linksexakt und überführt Injektive in Injektive

*Beweis.* Sei  $A \in G\text{-Mod}$ ,  $B \in G^{\text{abst}}\text{-Mod}$ . und  $f : A \rightarrow B$  ein  $G$ -Homomorphismus. Für  $a \in A$  sei  $U \subset G$  ein offener Normalteiler mit  $a \in A^U$ . Dann gilt für  $u \in U$ :

$$u \cdot f(a) = f(ua) = f(a)$$

also  $f(a) \in B^U$ . Daher gilt

$$\text{im}(f) \subset B^\delta \subset B.$$

Dies zeigt die Funktoradjunktion und nach Satz 1.3 (ii) in Kapitel 2 die Links-exaktheit von  $\delta$ . Da die Inklusion  $G\text{-Mod} \hookrightarrow G^{\text{abst}}\text{-Mod}$  exakt ist, überführt  $\bullet^\delta$  Injektive in Injektive nach Satz 1.3 (iii) in Kapitel 2.  $\square$

**Korollar 1.3.**  $G\text{-Mod}$  hat genügend viele Injektive.

*Beweis.* Für  $A \in G\text{-Mod}$  existiert ein injektives Objekt  $I \in G^{\text{abst}}\text{-Mod}$  und eine Inklusion  $A \hookrightarrow I$ . Nach 1.3 erhalten wir eine Inklusion  $A = A^\delta \hookrightarrow I^\delta$  in das injektive Objekt  $I^\delta \in G\text{-Mod}$ .  $\square$

*Beispiele diskreter Moduln.*

Sei  $L|K$  eine Galoiserweiterung mit Gruppe  $G = \text{Gal}(L|K)$ .

- jedes  $x \in L$  liegt bereits in einer endlich galoisschen Zwischenerweiterung  $L'|K$ . Daher gilt  $gx = x$  für alle  $g$  in  $G(L|L') \subset G(L|K)$ . Daher sind  $L^+$  und  $L^\times$  diskrete  $G$ -Moduln.
- Ist  $K$  ein lokaler Körper, so ist

$$\mathcal{O}_L = \{x \in L \mid |x| \leq 1\}$$

ein diskreter  $G$ -Modul. Analog:

$$\begin{aligned} U_L &= \{x \in L \mid |x| = 1\} \\ U_L^{(1)} &= \{x \in U_L \mid |x - 1| < 1\} \end{aligned}$$

- Ist  $K$  ein globaler Körper, so sind  $\mathcal{O}_L$  und  $E_L = \mathcal{O}_L^\times$  diskrete  $G$ -Moduln.

## 1.2 Kohomologie

Wir behandeln die Fälle  $G$  (abstrakte) Gruppe und  $G$  proendliche Gruppe parallel.

Wörterbuch im proendlichen Fall

$G$ -Modul = diskreter  $G$ -Modul

Untergruppe = abgeschlossene Untergruppe

Untergruppe von endlichem Index = abgeschlossene Untergruppe von endlichem Index (= offene Untergruppe)

Abbildung = stetige Abbildung.

Wir betrachten den linksexakten Funktor

$$\begin{aligned} \bullet^G : G\text{-Mod} &\longrightarrow \mathcal{A}b \\ A &\longmapsto A^G = \{a \in A \mid ga = a \quad \forall g \in G\} \\ &= \text{Hom}_G(\mathbb{Z}, A) \end{aligned}$$

Da  $G\text{-Mod}$  genügend viele Injektive hat, ist die folgende Definition sinnvoll.

**Definition.** Sei  $A$  ein  $G$ -Modul

$$H^i(G, A) := R^i(\bullet^G)(A).$$

Wegen  $A^G = \text{Hom}_G(\mathbb{Z}, A)$  gilt

$$H^i(G, A) = \text{Ext}_G^i(\mathbb{Z}, A).$$

**Bemerkung.** • Ist  $G$  proendlich, so hat  $G\text{-Mod}$  im allgemeinen nicht genügend viele Projektive, so dass man keine Homologie hat und auch  $\text{Ext}$  nicht durch eine projektive Auflösung im ersten Argument berechnen kann.

• Für  $G = \{1\}$  gilt

$$G\text{-Mod} = \mathcal{A}b = \mathbb{Z}\text{-Mod}$$

und

$$H^i(\{1\}, A) = \text{Ext}_{\mathbb{Z}}^i(\mathbb{Z}, A) = 0$$

für  $i \geq 1$ , weil  $\mathbb{Z}$  ein projektiver  $\mathbb{Z}$ -Modul ist.

**Definition.** Sei  $A \in G\text{-Mod}$ .  $\text{Koind}_G A = \text{Abb}(G, A)$  mit Gruppenstruktur

$$(f_1 + f_2)(g) = f_1(g) + f_2(g)$$

und  $G$ -Modulstruktur

$$(gf)(h) = gf(g^{-1}h)$$

heißt der **koinduzierte Modul von  $A$** .

**Bemerkung.** Ist  $G$  proendlich und  $A$  diskret, so ist  $\text{Koind}_G A$  wieder ein diskreter  $G$ -Modul.

Wir erhalten einen Funktor

$$\text{Koind}_G : G\text{-Mod} \longrightarrow G\text{-Mod}.$$

**Definition.** Ein  $G$ -Modul  $B$  heißt **koinduziert**, wenn  $B \cong \text{Koind}_G A$  für ein  $A \in G\text{-Mod}$ .

Sei nun  $H \subset G$  eine Untergruppe und  $A \in H\text{-Mod}$ .

**Definition.**

$$\begin{aligned}\mathrm{Koind}_G^H(A) &= \mathrm{Abb}_H(G, A) \\ &= \{f : G \longrightarrow A, f(hg) = hf(g) \quad \forall h \in H\}\end{aligned}$$

Gruppenstruktur:  $f_1 + f_2(g) = f_1(g) + f_2(g)$ ,

$G$ -Wirkung:  $(gf)(g') = f(g'g)$ .

**Lemma 1.4.** Für  $A \in G\text{-Mod}$  ist  $\mathrm{Koind}_G^H \mathrm{Res}_H^G A$  isomorph zum  $G$ -Modul  $\mathrm{Abb}(G/H, A)$  mit Gruppenstruktur

$$(f_1 + f_2)(gH) = f_1(gH) + f_2(gH),$$

$G$ -Wirkung

$$(gf)(g'H) = gf(g^{-1}g'H).$$

Insbesondere gilt für  $H = \{1\}$

$$\mathrm{Koind}_G^{\{1\}} \mathrm{Res}_{\{1\}}^G A \cong \mathrm{Koind}_G A.$$

*Beweis.* Der Isomorphismus

$$\varphi : \mathrm{Koind}_G^H \mathrm{Res}_H^G A \longrightarrow \mathrm{Abb}(G/H, A)$$

ist gegeben durch  $\varphi(f)(gH) = gf(g^{-1})$ . □

**Lemma 1.5.** Wir haben eine Adjunktion:

$$\mathrm{Res}_H^G \dashv \mathrm{Koind}_G^H.$$

*Beweis.* Wir definieren

$$\varphi : \mathrm{Hom}_H(\mathrm{Res}_H^G A, B) \xrightarrow{\sim} \mathrm{Hom}_G(A, \mathrm{Koind}_G^H B)$$

durch

$$\varphi(f)(a) = (g \mapsto f(ga)) \in \mathrm{Koind}_G^H B.$$

Nachprüfen dass  $\varphi(f)$  ein  $G$ -Homomorphismus ist

$$\begin{aligned}[\varphi(f)(ga)](g') &= f(g'ga) \\ &\parallel? \\ [g\varphi(f)(a)](g') &= \varphi(f)(a)(g'g) = f(g'ga)\end{aligned}$$

Rückabbildung

$$\psi : \mathrm{Hom}_G(A, \mathrm{Koind}_G^H B) \longrightarrow \mathrm{Hom}_H(\mathrm{Res}_H^G A, B)$$

$\psi(f)(a) = f(a)(e)$ . □

**Korollar 1.6.**  $\text{Koind}_G^H$  ist exakt und überführt Injektive in Injektive.

*Beweis.* Die Exaktheit kann man schnell explizit nachrechnen. Da die Linksadjungierte  $\text{Res}_H^G$  exakt ist, werden Injektive in Injektive überführt.  $\square$

**Satz 1.7.** (Shapiro-Lemma).

$$H^i(G, \text{Koind}_G^H A) = H^i(H, A) \quad \forall i \geq 0.$$

*Beweis.* Sei  $A \rightarrow I^\bullet$  eine Auflösung durch  $H$ -Injektive. Dann gilt

$$\begin{aligned} H^i(H, A) &= H^i(I^{\bullet H}) = H^i(\text{Hom}_H(\mathbb{Z}, I^\bullet)) \\ &= H^i(\text{Hom}_G(\mathbb{Z}, \text{Koind}_G^H I^\bullet)) = H^i((\text{Koind}_G^H I^\bullet)^G). \end{aligned}$$

Nun ist nach 1.6

$$\text{Koind}_G^H A \rightarrow \text{Koind}_G^H I^\bullet$$

eine Auflösung durch  $G$ -Injektive.  $\square$

**Definition.** Ein  $G$ -Modul  $A$  heißt **kohomologisch trivial**, wenn

$$H^i(H, A) = 0 \quad \forall i \geq 1 \quad \forall H \subseteq G.$$

**Bemerkung.** Ist  $G$  eine abstrakte Gruppe, so überführt  $\text{Res}_H^G$  Injektive in Injektive (Frobenius-Reziprozität, Satz 1.14 in Kapitel 3.1). Daher sind in diesem Fall Injektive kohomologisch trivial. Das gilt auch für proendliche Gruppen (siehe unten).

**Lemma 1.8.** Sei  $G$  eine proendliche Gruppe und seien  $H_1 \subseteq H_2$  abgeschlossene Untergruppen. Dann hat die Projektion topologischer Räume

$$H_1 \backslash G \twoheadrightarrow H_2 \backslash G$$

einen stetigen Schnitt  $s$ . Ist  $H \subset G$  eine abgeschlossene Untergruppe, so existiert ein Homöomorphismus  $G \cong H \backslash G \times H$ .

*Beweis.* Übungsaufgabe.  $\square$

**Lemma 1.9.** Ein koinduzierter  $G$ -Modul ist auch koinduzierter  $H$ -Modul für alle  $H \subseteq G$ .

*Beweis.*  $\text{Koind}_G A = \text{Abb}(G, A)$  nur als  $H$ -Modul betrachtet:

$$(hf)(g) = h \cdot f(h^{-1}g).$$

Sei nun  $s : H \backslash G \rightarrow G$  ein stetiger Schnitt und  $S = s(H \backslash G)$ , also  $G \cong H \times S$  als topologischer Raum. Dann gilt

$$\begin{aligned} \text{Abb}(G, A) = \text{Abb}(H \times S, A) &= \text{Abb}(H, \text{Abb}(S, A)) \\ f &\longmapsto [h \longmapsto (s \longmapsto f(h \cdot s))]. \end{aligned}$$

Versehen wir  $\text{Abb}(S, A)$  mit der  $H$ -Modulstruktur  $(h\varphi)(s) = h \cdot \varphi(s)$ , so erhalten wir einen Isomorphismus von  $H$ -Moduln

$$\text{Koind}_G A \xrightarrow{\sim} \text{Koind}_H \text{Abb}(S, A).$$

□

**Satz 1.10.**

- (i) *Koinduzierte Moduln sind kohomologisch trivial.*
- (ii) *Injektive Moduln sind kohomologisch trivial.*

*Beweis.* (i) Nach 1.9 gilt zu zeigen

$$H^i(G, \text{Koind}_G A) = 0 \quad \forall i \geq 1.$$

Dies folgt aus

$$\text{Koind}_G A \cong \text{Koind}_G^{\{1\}} \text{Res}_{\{1\}}^G A$$

und

$$0 = H^i(\{1\}, \text{Res}_{\{1\}}^G A) = H^i(G, \text{Koind}_G^{\{1\}} \text{Res}_{\{1\}}^G A)$$

für  $i \geq 1$ .

(ii) Sei  $I$  injektiv. Wir haben eine Inklusion

$$i : I \longrightarrow \text{Koind}_G I, \quad x \longmapsto (g \longmapsto x \quad \forall g \in G).$$

Weil  $I$  injektiv ist, hat  $i$  einen Schnitt. Also ist  $I$  direkter Summand in einem kohomologisch trivialen Modul und daher selbst kohomologisch trivial. □

### 1.3 Der Kohomologische Standardkomplex

Sei  $A \in G\text{-Mod}$ . Wir setzen:

$$X^n(G, A) = \text{Abb}(G^{n+1}, A)$$

mit der  $G$ -Modulstruktur

$$(g\varphi)(g_0, \dots, g_n) = g\varphi(g^{-1}g_0, \dots, g^{-1}g_n).$$

**Bemerkung.**

$$\begin{aligned} X^0(G, A) &= \text{Koind}_G A \quad \text{und} \quad X^n(G, A) = \text{Abb}(G, \text{Abb}(G^n, A)) \\ &= \text{Koind}_G X^{n-1}(G, A). \end{aligned}$$

Daher sind alle  $X^i(G, A)$  kohomologisch trivial. Die Projektionen  $p_i : G^n \rightarrow G^{n-1}$ ,  $i = 0, \dots, n$ , induzieren Abbildungen

$$\delta_i : X^{n-1} \longrightarrow X^n \quad i = 0, \dots, n.$$

Wir setzen

$$d = \sum_{i=0}^n (-1)^i \delta_i : X^{n-1} \longrightarrow X^n.$$

**Lemma 1.11.**  $d \circ d = 0$  und der Komplex  $X^\bullet = X^\bullet(G, A)$  ist eine Auflösung von  $A$  durch kohomologisch triviale  $G$ -Moduln.

*Beweis.* Analog wie bei der homologischen Standardauflösung.  $\square$

**Korollar 1.12.** Sei

$$C^\bullet(G, A) = X^\bullet(G, A)^G.$$

Dann gilt

$$H^i(G, A) = H^i(C^\bullet(G, A)) \quad \forall i.$$

**Definition.** Eine **Derivation**  $D : G \rightarrow A$  ist eine Abbildung, so dass

$$D(gh) = D(g) + g \cdot D(h) \quad \forall g, h \in G$$

gilt. Durch  $(D_1 + D_2)(g) = D_1(g) + D_2(g)$  wird die Menge der Derivationen von  $G$  mit Werten in  $A$  zu einer abelschen Gruppe  $\text{Der}(G, A)$ .

**Bemerkung.** Ist  $A$  ein trivialer  $G$ -Modul, so gilt  $\text{Der}(G, A) = \text{Hom}(G, A)$ .

**Beispiel.** Für jedes  $a \in A$  ist

$$D_a : G \longrightarrow A, \quad g \longmapsto ga - a,$$

eine Derivation wegen

$$gha - a = ga - a + g(ha - a).$$

Solche Derivationen heißen **innere Derivationen** und bilden die Untergruppe  $\text{IDer}(G, A) \subseteq \text{Der}(G, A)$ .

**Bemerkung.** Ist  $A$  ein trivialer  $G$ -Modul, so gilt  $\text{IDer}(G, A) = 0$ .

**Satz 1.13.** Es gibt einen Isomorphismus

$$H^1(G, A) \cong \text{Der}(G, A) / \text{IDer}(G, A).$$

Für einen trivialen Modul  $A$  gilt

$$H^1(G, A) \cong \text{Hom}(G, A).$$

Insbesondere gilt für eine proendliche Gruppe  $G$ :

$$G^{\text{ab}} \cong H^1(G, \mathbb{Q}/\mathbb{Z})^\vee.$$

**Bemerkung.** Das Symbol  $(-)^{\vee}$  im obigen Satz bezeichnet das *Pontrjagindual*. Dieses ist für eine lokal kompakte abelsche Gruppe  $H$  definiert als

$$H^{\vee} := \text{Hom}(H, \mathbb{R}/\mathbb{Z})$$

mit der kompakt-offen-Topologie. Es überführt kompakte Gruppen in diskrete und andersherum. Die *Pontrjagindualität* sagt aus, dass die natürliche Abbildung ins Doppeldual

$$H \longrightarrow H^{\vee\vee}$$

ein Isomorphismus ist, es handelt sich also tatsächlich um eine Dualität. Für endliche Gruppen lässt sich dies elementar nachprüfen, im Allgemeinen ist diese Aussage aber schwieriger zu beweisen. Für die Aussage in Satz 1.13 ist noch anzumerken, dass für eine proendliche Gruppe  $G = \varprojlim_i G_i$  (mit endlichen Gruppen  $G_i$ ) gilt:

$$\begin{aligned} \text{Hom}(G, \mathbb{R}/\mathbb{Z}) &= \text{Hom}(\varprojlim_i G_i, \mathbb{R}/\mathbb{Z}) \\ &= \varinjlim_i \text{Hom}(G_i, \mathbb{R}/\mathbb{Z}) = \varinjlim_i \text{Hom}(G_i, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(G, \mathbb{Q}/\mathbb{Z}). \end{aligned}$$

*Beweis.* Wir betrachten das kommutative Diagramm

$$\begin{array}{ccc} X^0(G, A)^G = C^0(G, A) & \xrightarrow[\varphi \mapsto \varphi(1)]{\sim} & A \\ d^1 \downarrow & & \downarrow \partial^1 \\ C^1(G, A) & \xrightarrow[\varphi \mapsto (g \mapsto \varphi(e, g))]{\sim} & \text{Abb}(G, A) \\ d^2 \downarrow & & \downarrow \partial^2 \\ C^2(G, A) & \xrightarrow[\varphi \mapsto ((g_1, g_2) \mapsto \varphi(e, g_1, g_1 g_2))]{\sim} & \text{Abb}(G^2, A), \end{array}$$

wobei  $\partial^1$  und  $\partial^2$  so gewählt sind, dass das Diagramm kommutiert.

*Behauptung:* (i)  $\partial^1(a) = (g \mapsto ga - a)$

(ii)  $\partial^2(x) = ((g_1, g_2) \mapsto g_1 x(g_2) - x(g_1 g_2) + x(g_1))$

*Stupides Nachrechnen:*

(i) Sei  $a \in A$ . Das Urbild in  $C^0(G, A)$  ist die Kokette

$$\varphi_a = (g \mapsto ga) \in C^0(G, A).$$

*Probe:*  $\varphi_a(g) = ga$  liegt in  $C^0(G, A)$  wegen

$$\begin{aligned} (g' \varphi_a)(g) &= g' \varphi_a(g'^{-1}g) = g'^{-1} g' ga = ga. \\ d^1(\varphi_a)(g_0, g_1) &= g_1 a - g_0 a. \end{aligned}$$

Dies bildet sich in  $\text{Abb}(G, A)$  ab auf

$$g \longmapsto ga - ea = ga - a.$$



(ii) Sei  $x : G \rightarrow A \in \text{Abb}(G, A)$ . Das Urbild in  $C^1(G, A)$  ist

$$\varphi_x : G \times G \longrightarrow A, (g_0, g_1) \longmapsto g_0 \cdot x(g_0^{-1}g_1)$$

*Probe:*

$$\begin{aligned} (g \cdot \varphi_x)(g_0, g_1) &= g\varphi_x(g^{-1}g_0, g^{-1}g_1) \\ &= g(g^{-1}g_0) \cdot x(g^{-1}g_0)^{-1}g^{-1}g_1 = g_0 \cdot x(g_0^{-1}g_1) \end{aligned}$$

also  $\varphi_x \in C^1(G, A)$ .

Nun gilt

$$\begin{aligned} (d^2\varphi_x)((g_0, g_1, g_2)) &= \varphi_x(g_1, g_2) - \varphi_x(g_0, g_2) + \varphi_x(g_0, g_1) \\ &= g_1x(g_1^{-1}g_2) - g_0x(g_0^{-1}g_2) + g_0x(g_0^{-1}g_1). \end{aligned}$$

Dies bildet sich in  $\text{Abb}(G^2, A)$  ab auf

$$\begin{aligned} (g_1, g_2) &\longmapsto d^2\varphi_x(e, g_1, g_1g_2) \\ &= g_1x(g_2) - x(g_1, g_2) + x(g_1) \end{aligned}$$

Wir erhalten:

$$H^1(G, A) = H(A \xrightarrow{\partial^1} \text{Abb}(G, A) \xrightarrow{\partial^2} \text{Abb}(G^2, A))$$

Nun gilt

$$\partial^2x = 0 \iff x(g_1g_2) = g_1x(g_2) + x(g_1) \quad \forall g_1, g_2 \in G$$

Daher  $\ker \partial^2 = \text{Der}(G, A)$  und  $\text{im} \partial^1 = \text{IDer}(G, A)$ . □

## 1.4 Funktorialität

Ein **kompatibles Paar**  $(\varphi, f) : (G, A) \rightarrow (G', A')$  besteht aus:

- Gruppen  $G, G'$ ,
- ein  $G$ -Modul  $A$ , ein  $G'$ -Modul  $A'$ ,
- ein Gruppenhomomorphismus  $\varphi : G' \rightarrow G$ ,
- ein Homomorphismus abelscher Gruppen:  $f : A \rightarrow A'$ .

so dass für  $g' \in G', a \in A$  gilt

$$f(\varphi(g')a) = g'f(a). \tag{*}$$

Ein kompatibles Paar induziert Komplexhomomorphismen

$$(\varphi, f) : X^\bullet(G, A) \longrightarrow X^\bullet(G', A')$$

durch

$$(\varphi, f)(x)(g'_0, \dots, g'_n) = f(x(\varphi(g'_0), \dots, g'_n))$$

und wegen (\*):

$$C^\bullet(G, A) \longrightarrow C^\bullet(G', A').$$

Nimmt man Kohomologie erhält man natürliche Abbildung

$$H^i(G, A) \longrightarrow H^i(G', A') \quad \forall i \geq 0.$$

1. Beispiel:  $\text{res}_H^G$

Sei  $H \subseteq G$  eine Untergruppe und  $A$  ein  $G$ -Modul. Das kompatible Paar  $(G, A) \rightarrow (H, A)$  induziert die Abbildung

$$\text{res}_U^G : H^i(G, A) \longrightarrow H^i(U, A)$$

2. Beispiel: Die Inflation

Sei  $H \subseteq G$  ein Normalteiler. Dann ist  $A^H$  in natürlicher Weise ein  $G/H$ -Modul. Das kompatible Paar

$$(G/H, A^H) \longrightarrow (G, A) \quad (\text{durch } G \twoheadrightarrow G/H, A^H \hookrightarrow A)$$

induziert die **Inflationsabbildung**

$$\text{inf}_G^{G/H} : H^i(G/H, A^H) \longrightarrow H^i(G, A) \quad \forall i$$

**Satz 1.14.** Sei  $H \triangleleft G$  ein Normalteiler und  $A$  ein  $G$ -Modul. Dann ist die Folge

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A)$$

exakt.

*Beweis.* Wir nutzen den Isomorphismus

$$H^1(G, A) = \text{Der}(G, A) / \text{IDer}(G, A).$$

1) Injektivität von  $\text{inf}$ .

Sei  $D : G/H \rightarrow A^H$  eine Derivation so dass  $\text{inf } D : G \twoheadrightarrow G/H \xrightarrow{D} A^H \subset A$  inner ist, d.h. es existiert  $a \in A$  mit  $\text{inf } D(g) = ga - a$  für alle  $g \in G$ .

Zu zeigen  $D$  ist inner. Genügt zu zeigen  $a \in A^H$ . Nun gilt per Konstruktion

$$(\text{inf } D)(h) = D(e) \in A^H \subset A$$

für alle  $h \in H$ . Nach Definition einer Derivation gilt

$$D(e) = D(ee) = e \cdot D(e) + D(e) = D(e) + D(e) \text{ also } D(e) = 0.$$

Also gilt

$$\text{inf } D(h) = 0 \quad \forall h \in H.$$

Folglich

$$ha - a = 0 \quad \rightsquigarrow \quad a \in A^H.$$

2)  $\text{res} \circ \text{inf} = 0$ .

Ist  $D : G/H \rightarrow A^H$  eine Derivation, so ist

$$\text{res} \circ \text{inf} D : H \rightarrow G \rightarrow G/H \rightarrow A^H \subset A$$

die Nullabbildung wegen  $\text{res} \circ \text{inf} D(h) = D(e) = 0$ .

3) Exaktheit bei  $H^1(G, A)$ .

Sei  $D : G \rightarrow A$  eine Derivation so dass

$$\text{res} D : H \hookrightarrow G \rightarrow A$$

inner ist, d.h. es existiert

$$a \in A : D(h) = ha - a \quad \forall h \in H.$$

Zu zeigen es existiert

$$D' \in \text{Der}(G/H, A^H) \text{ und } b \in A \text{ mit } D = \text{inf } D' + D_a.$$

Wir setzen  $b = a$ .

Die Gleichung

$$\begin{aligned} (D - D_a)(gh) &= gD(h) + D(g) - gha + a \\ &= g(ha - a) + D(g) - gha + a = (D - D_a)(g) \end{aligned}$$

zeigt, dass  $D' = D - D_a$  nur von der Restklasse  $\text{mod } H$  abhängt. Außerdem nimmt wegen

$$hD'(g) = hD'g(g) + D'(h) = D'(hg) = D'(gg^{-1}hg) = D'(g)$$

$D'$  Werte in  $A^H$  an. Daher gilt

$$D - D_a = \text{inf}(D').$$

□

**Satz 1.15.** Sei  $H \subseteq G$  ein Normalteiler,  $A$  ein  $G$ -Modul und  $n \geq 1$  eine natürliche Zahl, so dass

$$H^i(H, A) = 0$$

für  $1 \leq i \leq n - 1$ . Dann ist die Folge

$$0 \longrightarrow H^n(G/H, A^H) \xrightarrow{\text{inf}} H^n(G, A) \xrightarrow{\text{res}} H^n(H, A)$$

exakt.

*Beweis.* Per Induktion nach  $n$ .  $n = 1$  ist 1.14.

Sei  $n \geq 2$ . Wir betrachten die kurze exakte Folge

$$0 \longrightarrow A \longrightarrow \text{Koind}_G A \longrightarrow A' \longrightarrow 0.$$

Die lange exakte Folge

$$\begin{aligned} H^i(G, \text{Koind}_G A) &\longrightarrow H^i(G, A') \longrightarrow H^{i+1}(G, A) \\ &\longrightarrow H^{i+1}(G, \text{Koind}_G A) \longrightarrow \dots \end{aligned}$$

zeigt

$$H^i(G, A') \xrightarrow{\sim} H^{i+1}(G, A) \text{ f\"ur } i \geq 1.$$

Analog

$$H^i(H, A) \xrightarrow{\sim} H^{i+1}(H, A').$$

Also insbesondere  $H^i(H, A') = 0$  f\"ur  $i = 1, \dots, n-2$ .

Desweiteren gilt

$$\begin{aligned} (\text{Koind}_G A)^H &\cong (\text{Koind}_G^{\{1\}} A)^H = \text{Abb}_H(G, A^{\text{tr}}) \\ &= \text{Abb}(G/H, A^{\text{tr}}) = \text{Koind}_{G/H}^{\{1\}} A^{\text{tr}}. \end{aligned}$$

Also ist  $(\text{Koind}_G A)^H$  ein kohomologisch trivialer  $G/H$ -Modul. Wegen  $H^1(H, A) = 0$  ist die Folge

$$0 \longrightarrow A^H \longrightarrow (\text{Koind}_G A)^H \longrightarrow A'^H \longrightarrow 0$$

exakt. Wir erhalten

$$H^i(G/H, A'^H) = H^{i+1}(G/H, A^H) \quad \forall i \geq 1.$$

Zusammen ergibt dies ein kommutatives Diagramm

$$\begin{array}{ccccc} 0 \longrightarrow H^n(G/H, A^H) & \xrightarrow{\inf} & H^n(G, A) & \xrightarrow{\text{res}} & H^n(H, A) \\ & \wr & \wr & & \wr \\ 0 \longrightarrow H^{n+1}(G/H, A'^H) & \xrightarrow{\inf} & H^{n-1}(G, A') & \longrightarrow & H^{n-1}(H, A). \end{array}$$

Nach Induktionsvoraussetzung ist die untere Zeile exakt, also auch die obere.  $\square$

## 1.5 Die Korestriktion

Sei  $U \subseteq G$  eine Untergruppe von endlichem Index. Wir haben die Norm-Abbildung

$$\begin{aligned} N : M^U &\longrightarrow M^G \\ m &\longmapsto \sum_{s \in G/U} sm \end{aligned}$$

Angewendet auf eine kohomologisch triviale Aufl\"osung  $A \rightarrow I$  gibt dies die Abbildung

$$\text{cor}_G^U : H^i(U, A) \longrightarrow H^i(G, A), \quad i \geq 0.$$

**Beispiel.** Sei  $L|K$  eine (evtl. unendliche) Galoiserweiterung mit Gruppe  $G$  und sei  $U \subset G$  eine offene Untergruppe. Setze  $K' = L^U$ .

$$\text{auf } H^0\text{-Niveau } \begin{cases} \bullet & A = L^+ : \text{cor} = \text{Spur}_{K'|K} K'^+ \longrightarrow K^+ \\ \bullet & A = L^\times : \text{cor} = \text{Norm}_{K'|K} : K'^\times \longrightarrow K^\times \end{cases}$$

Analog wie bei Homologie erhalten wir

**Lemma 1.16.**

$$\text{cor}_G^U \circ \text{res}_U^G = (G : U).$$

**Korollar 1.17.** Sei  $G$  eine endliche Gruppe der Ordnung  $n$  und  $A$  ein  $G$ -Modul, so dass die  $n$ -Multiplikation  $A \xrightarrow{\cdot n} A$  ein Isomorphismus ist. Dann gilt

$$H^i(G, A) = 0 \quad \forall i \geq 1.$$

#### 4. Konjugation

Sei  $H \subset G$  eine Untergruppe,  $A$  ein  $G$ -Modul und  $B$  ein  $H$ -Untermodul von  $A$ . Für  $g \in G$  ist  $gB = \{gb \mid g \in G\}$  eine Untergruppe und ein  $H^g = gHg^{-1}$ -Modul. Das Paar

$$\begin{aligned} H^g &\longrightarrow H & B &\longrightarrow gB \\ h &\longmapsto g^{-1}hg & b &\longmapsto gb \end{aligned}$$

ist ein kompatibles Paar (von Isomorphismen). Wir erhalten Isomorphismen

$$g_* : H^n(H, B) \xrightarrow{\sim} H^n(H^g, gB) \quad \forall n.$$

Diese heißen **Konjugationsabbildungen**

$$\left. \begin{aligned} \text{Es gilt } e_* &= \text{id} \quad \text{und} \\ (g_1 g_2)_* &= (g_1)_* \circ (g_2)_* \end{aligned} \right\} \quad (*)$$

Nun nehmen wir an:

$H \triangleleft G$ , also  $H^g = H$  und  $B = A$ , also  $gB = A$  und erhalten die Abbildung

$$g_* : H^n(H, A) \rightarrow H^n(H, A)$$

für alle  $g \in G$ ,  $n \geq 0$ . Wegen  $(*)$  wird  $H^n(H, A)$  durch

$$\begin{aligned} G \times H^n(H, A) &\longrightarrow H^n(H, A) \\ (g, x) &\longmapsto g_*(x) \end{aligned}$$

zum  $G$ -Modul.

**Satz 1.18.** Sei  $A$  ein  $G$ -Modul und  $H \subset G$  ein Normalteiler. Dann ist für jedes  $h \in H$  die Abbildung

$$h_* : H^n(H, A) \longrightarrow H^n(H, A)$$

die Identität. Mit anderen Worten: Die  $G$ -Wirkung auf  $H^n(H, A)$  faktorisiert über  $G/H$ , d.h.  $H^n(H, A)$  ist ein  $G/H$ -Modul.

*Beweis.* Auf  $H^0(H, A) = A^H$  ist  $h_*$  trivialerweise die Identität. Der allgemeine Fall folgt durch Anwendung auf eine kohomologisch triviale Auflösung  $A \rightarrow I^\bullet$  aus dem Spezialfall  $H^0$ .  $\square$

## 1.6 Das Cup-Produkt

Seien  $A, B$   $G$ -Moduln. Die natürliche Abbildung

$$A^G \times B^G \longrightarrow (A \otimes B)^G, \quad (a, b) \longmapsto a \otimes b,$$

setzt sich auf die höheren Kohomologiegruppen fort.

Sei  $C^\bullet(G, A) = X^\bullet(G, A)^G$ . Wir betrachten für  $p, q \geq 0$  die Abbildung

$$C^p(G, A) \times C^q(G, B) \xrightarrow{\cup} C^{p+q}(G, A \otimes B)$$

die durch  $a \cup b(g_0, \dots, g_{p+q}) = a(g_0, \dots, g_p) \otimes b(g_p, \dots, g_{p+q})$  gegeben ist.

**Satz 1.19.** Für das Differential  $\partial$  in den verschiedenen Standardkomplexen gilt

$$\partial(a \cup b) = (\partial a) \cup b + (-1)^p(a \cup \partial b).$$

*Beweis.* Es gilt

$$\begin{aligned} & \partial(a \cup b)(g_0, \dots, g_{p+q+1}) \\ &= \sum_{i=0}^{p+q+1} (-1)^i (a \cup b)(g_0, \dots, \widehat{g}_i, \dots, g_{p+q+1}) \\ &= \sum_{i=0}^p (-1)^i a(g_0, \dots, \widehat{g}_i, \dots, g_{p+1}) \otimes b(g_{p+1}, \dots, g_{p+q+1}) \\ &+ \sum_{i=p+1}^{p+q+1} (-1)^i a(g_0, \dots, g_p) \otimes b(g_p, \dots, \widehat{g}_i, \dots, g_{p+q+1}) \end{aligned}$$

Desweiteren

$$\begin{aligned} & (\partial a \cup b)(g_0, \dots, g_{p+q+1}) \\ &= \partial a(g_0, \dots, g_{p+1}) \otimes b(g_{p+1}, \dots, g_{p+q+1}) \\ &= \sum_{i=0}^{p+1} (-1)^i a(g_0, \dots, \widehat{g}_i, \dots, g_{p+1}) \otimes b(g_{p+1}, \dots, g_{p+q+1}) \end{aligned}$$

und

$$\begin{aligned} & (a \cup \partial b)(g_0, \dots, g_{p+q+1}) \\ &= a(g_0, \dots, g_p) \otimes \partial b(g_p, \dots, g_{p+q+1}) \\ &= \sum_{i=0}^{q+1} (-1)^i a(g_0, \dots, g_p) \otimes b(g_p, \dots, \widehat{g}_{p+i}, \dots, g_{p+q+1}) \\ &= (-1)^p \sum_{i=p}^{p+q+1} (-1)^i a(g_0, \dots, g_p) \otimes b(g_p, \dots, \widehat{g}_i, \dots, g_{p+q+1}). \end{aligned}$$

In der zu beweisenden Formel

$$\partial(a \cup b) = \partial a \cup b + (-1)^p(a \cup \partial b)$$

bleibt stehen:

$$\begin{aligned} 0 &= (-1)^{p+1} a(g_0, \dots, g_p) \otimes b(g_{p+1}, \dots, g_{p+q+1}) \\ &+ (-1)^p a(g_0, \dots, g_p) \otimes b(g_{p+1}, \dots, g_{p+q+1}). \end{aligned}$$

□

Wir erhalten somit Abbildungen

$$\begin{aligned} Z^p(G, A) \times Z^q(G, B) &\xrightarrow{\cup} Z^{p+q}(G, A \otimes B), \\ B^p(G, A) \times Z^q(G, B) &\xrightarrow{\cup} B^{p+q}(G, A \otimes B), \\ Z^p(G, A) \times B^q(G, B) &\xrightarrow{\cup} Z^{p+q}(G, A \otimes B). \end{aligned}$$

**Definition.** Die induzierte Abbildung

$$H^p(G, A) \times H^q(G, B) \xrightarrow{\cup} H^{p+q}(G, A \otimes B)$$

heißt das **Cup-Produkt**.

**Bemerkungen.** 1.) Ist  $A \times B \rightarrow C$  eine bilineare Paarung, so wird ein Homomorphismus.  $A \otimes B \rightarrow C$  induziert und wir erhalten eine Abbildung

$$H^p(G, A) \times H^q(G, B) \longrightarrow H^{p+q}(G, A \otimes B) \longrightarrow H^{p+q}(G, C)$$

die auch Cup-Produkt genannt wird.

2.) Man kann das Cup-Produkt abstrakt charakterisieren durch:

- auf  $H^0$  ist es die natürliche Abbildung  $A^G \times B^G \rightarrow (A \otimes B)^G$
- es gelten die Eigenschaften, die wir gleich nachweisen werden.

**Lemma 1.20.** Für Homomorphismen  $A \rightarrow A'$ ,  $B \rightarrow B'$  ist das induzierte Diagramm

$$\begin{array}{ccccc} H^p(G, A) & \times & H^q(G, B) & \xrightarrow{\cup} & H^{p+q}(G, A \otimes B) \\ \downarrow & & \downarrow & & \downarrow \\ H^p(G, A') & \times & H^q(G, B') & \xrightarrow{\cup} & H^{p+q}(G, A' \otimes B) \end{array}$$

kommutativ.

*Beweis.* Direkt aus der Definitionen. □

**Satz 1.21.** (i) Seien  $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$  und  $0 \rightarrow C' \rightarrow C \rightarrow C'' \rightarrow 0$  exakte Folgen von  $G$ -Moduln. Sei  $B$  ein weiterer  $G$ -Modul und sei  $A \times B \rightarrow C$  eine bilineare Paarung, die Paarungen  $A' \times B \rightarrow C'$  und  $A'' \times B \rightarrow C$  induziert. Dann ist das Diagramm

$$\begin{array}{ccccc} H^p(G, A'') & \times & H^q(G, B) & \xrightarrow{\cup} & H^{p+q}(G, C'') \\ \downarrow \delta & & \downarrow \text{id} & & \downarrow \delta \\ H^{p+1}(G, A') & \times & H^q(G, B) & \xrightarrow{\cup} & H^{p+q+1}(G, C') \end{array}$$

kommutativ, d.h.  $\delta(a'' \cup \beta) = \delta a'' \cup \beta$ .

(ii) Seien  $0 \rightarrow B' \rightarrow B \rightarrow B'' \rightarrow 0$  und  $0 \rightarrow C' \rightarrow C \rightarrow C'' \rightarrow 0$  exakte Folgen von  $G$ -Moduln und sei  $A \times B \rightarrow C$  eine Paarung, die Paarungen  $A \times B' \rightarrow C'$  und  $A \times B'' \rightarrow C''$  induziert. Dann kommutiert das Diagramm

$$\begin{array}{ccccc} H^p(G, A) & \times & H^q(G, B'') & \xrightarrow{\cup} & H^{p+q}(G, C'') \\ \downarrow \text{id} & & \downarrow \delta & & \downarrow (-1)^p \delta \\ H^p(G, A) & \times & H^{q+1}(G, B') & \xrightarrow{\cup} & H^{p+q+1}(G, C'), \end{array}$$

d.h.  $(-1)^p \delta(\alpha \cup \beta'') = \alpha \cup \delta \beta''$ .

*Beweis.* Wir zeigen (ii): Sei  $\alpha = \bar{a}$ ,  $a \in Z^p(G, A)$ ,  $\beta'' = \bar{b''}$ ,  $b'' \in Z^q(G, B'')$ . Sei  $b \in C^q(G, B)$  ein Urbild von  $b''$ . Wir identifizieren  $B'$  mit seinem Bild in  $B$ . Dann wird nach Definition  $\delta\beta''$  durch den Kozyklus  $\partial b \in Z^{q+1}(G, B')$  repräsentiert und  $\delta(\alpha \cup \beta'')$  durch  $\partial(a \cup b) \in Z^{p+q+1}(G, C)$ . Wegen  $\partial a = 0$  erhalten wir nach 1.19

$$\begin{aligned}\partial(a \cup b) &= (\partial a) \cup b + (-1)^p(a \cup \partial b) \\ &= (-1)^p(a \cup \partial b).\end{aligned}$$

Übergang zu Kohomologie gibt

$$\delta(\alpha \cup \beta'') = (-1)^p \delta\alpha \cup \beta''.$$

□

Wir machen die Identifikationen

$$(A \otimes B) \otimes C \cong A \otimes (B \otimes C) \quad \text{und} \quad A \otimes B \cong B \otimes A.$$

**Satz 1.22.** *Das Cup-Produkt ist assoziativ und graduiert-kommutativ, d.h. für  $\alpha \in H^p(G, A)$ ,  $\beta \in H^q(G, B)$ ,  $\gamma \in H^r(G, C)$  gilt*

$$(\alpha \cup \beta) \cup \gamma = \alpha \cup (\beta \cup \gamma) \quad \text{und} \quad \alpha \cup \beta = (-1)^{pq}(\beta \cup \alpha).$$

*Beweis.* Seien  $a, b, c$  Kozyklen, die  $\alpha, \beta, \gamma$  repräsentieren. Dann gilt

$$\begin{aligned}& (a \cup b) \cup c(g_0, \dots, g_{p+q+r}) \\ &= a \cup b(g_0, \dots, g_{p+q}) \otimes c(g_{p+q}, \dots, g_{p+q+r}) \\ &= a(g_0, \dots, g_p) \otimes b(g_p, \dots, g_{p+q}) \otimes c(g_{p+q}, \dots, g_{p+q+r}) \\ &= a(g_0, \dots, g_p) \otimes (b \cup c)(g_p, \dots, g_{p+q+r}) \\ &= a \cup (b \cup c)(g_0, \dots, g_{p+q+r}).\end{aligned}$$

Übergang zur Kohomologie zeigt die Assoziativität.

Die graduierte Kommutativität ist auf Kozykelniveau schwierig einzusehen. Für  $p = q = 0$  gilt offensichtlich  $\alpha \cup \beta = \beta \cup \alpha$ .

Wir beschränken uns im Beweis für allgemeine  $p, q$  auf den Fall, dass  $G$  proendlich ist. Wir nutzen, dass für beliebige diskrete  $G$ -Moduln  $A, B$  die Abbildung

$$(\text{Koind}_G A) \otimes B \rightarrow \text{Koind}_G(A \otimes B), \quad f \otimes b \mapsto [g \mapsto f(g) \otimes b]$$

ein Isomorphismus von  $G$  Moduln ist. Das sieht man für endliches  $G$  wegen

$$\text{Koind}_G A = \text{Abb}(G, A) = \bigoplus_G A,$$

und weil Tensorprodukt und direkte Summe kommutieren. Für beliebiges  $G$  folgt die Aussage per Limesübergang aus der Aussage für  $G/U$  für beliebige offene Normalteiler  $U$  von  $G$ .



Nun machen wir Dimensionsverschiebung: Für einen  $G$ -Modul  $A$  setzen wir induktiv:

$$A_0 = A, A_{i+1} = \text{coker}(A_i \rightarrow \text{Koind}_G A_i).$$

Dann haben wir eine Surjektion:

$$H^0(G, A_n) \xrightarrow{\delta} H^1(G, A_{n-1})$$

und Isomorphismen:

$$H^1(G, A_{n-1}) \xrightarrow[\delta]{\sim} H^2(G, A_{n-2}) \xrightarrow[\delta]{\sim} \dots \xrightarrow[\delta]{\sim} H^n(G, A_0).$$

Die Komposition  $\delta^n$  dieser  $n$  Randabbildungen ist eine Surjektion  $H^0(G, A_n) \xrightarrow{\delta^n} H^n(G, A)$ . Wegen  $\text{Koind}_G A \otimes B \cong \text{Koind}_G(A \otimes B)$  haben wir

$$A_1 \otimes B \cong (A \otimes B)_1 \cong A \otimes B_1.$$

Nach 1.21 ((i)  $p$  mal und (ii)  $q$  mal angewendet) erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccccc} H^0(G, A_p) & \times & H^0(G, B_q) & \xrightarrow{\cup} & H^0(G, A_p \otimes B_q) = H^0(G, (A \otimes B)_p) \\ \delta^p \downarrow & & \text{id} \downarrow & & \swarrow \delta^p \\ H^p(G, A) & \times & H^0(G, B_q) & \xrightarrow{\cup} & H^p(G, A \otimes B_q) = H^p(G, (A \otimes B)_q) \\ \text{id} \downarrow & & \delta^q \downarrow & & \swarrow (-1)^{pq} \delta^q \\ H^p(G, A) & \times & H^q(G, B) & \xrightarrow{\cup} & H^{p+q}(G, A \otimes B). \end{array}$$

andersherum:

$$\begin{array}{ccccc} H^0(G, B_q) & \times & H^0(G, A_p) & \xrightarrow{\cup} & H^0(G, B_q \otimes A_p) = H^0(G, (B \otimes A)_p) \\ \text{id} \downarrow & & \delta^p \downarrow & & \swarrow \delta^p \\ H^0(G, B_q) & \times & H^p(G, A) & \xrightarrow{\cup} & H^p(G, B_q \otimes A) = H^p(G, (B \otimes A)_q) \\ \delta^q \downarrow & & \text{id} \downarrow & & \swarrow \delta^q \\ H^p(G, B) & \times & H^q(G, A) & \xrightarrow{\cup} & H^{p+q}(G, A \otimes B). \end{array}$$

Weil das Cup-Produkt auf  $H^0$ -Niveau kommutiert, erhalten wir das behauptete Vorzeichen.  $\square$

Seien  $A, B$  diskrete  $G$ -Moduln und sei eine der folgenden Bedingungen erfüllt  
(a)  $G$  endlich; oder  
(b)  $A$  ist endlich erzeugt als abelsche Gruppe.

Dann ist  $\text{Hom}(A, B)$  mit der  $G$ -Wirkung  $(g\varphi)(a) = g \cdot \varphi(g^{-1}a)$  ein diskreter  $G$ -Modul.

Wir betrachten die Paarung

$$\text{Hom}(A, B) \times A \longrightarrow B, \quad (\varphi, a) \longmapsto \varphi(a).$$

Diese induziert das Cup-Produkt

$$H^p(G, \text{Hom}(A, B)) \times H^q(G, A) \longrightarrow H^{p+q}(G, B)$$

**Satz 1.23.** Es sei

$$0 \longrightarrow A' \xrightarrow{i} A \xrightarrow{j} A'' \longrightarrow 0$$

eine exakte Folge von  $G$ -Moduln und  $B$  ein  $G$ -Modul, so dass

- (i)  $G$  endlich, oder  $A$  endlich erzeugte abelsche Gruppe, und
- (ii) Die Folge

$$0 \longrightarrow \text{Hom}(A'', B) \xrightarrow{\hat{\gamma}} \text{Hom}(A, B) \xrightarrow{\hat{i}} \text{Hom}(A', B) \longrightarrow 0$$

ist exakt.

Dann ist das Diagramm

$$\begin{array}{ccccc} H^p(G, \text{Hom}(A', B)) & \times & H^q(G, A') & \xrightarrow{\cup} & H^{p+q}(G, B) \\ \delta \downarrow & & \uparrow \delta & & \downarrow (-1)^{p+1} \\ H^{p+1}(G, \text{Hom}(A'', B)) & \times & H^{q-1}(G, A'') & \xrightarrow{\cup} & H^{p+q}(G, B) \end{array}$$

kommutativ, d.h.

$$(\delta \hat{\alpha}) \cup \alpha + (-1)^p (\hat{\alpha} \cup \delta \alpha) = 0$$

für

$$\hat{\alpha} \in H^p(G, \text{Hom}(A', B)), \quad \alpha \in H^{q-1}(G, A'').$$

*Beweis.* Seien  $\hat{a}' \in Z^p(G, \text{Hom}(A', B))$  und  $a'' \in Z^{q-1}(G, A'')$  repräsentierende Kozykel von  $\hat{\alpha}$  und  $\alpha$ . Seien  $\hat{a} \in C^p(G, \text{Hom}(A, B))$  und  $a \in C^{q-1}(G, A)$  Urbilder. Dann existieren  $\hat{a}'' \in C^{p+1}(G, \text{Hom}(A'', B))$  und  $a' \in C^q(G, A')$  mit  $\hat{j}\hat{a}'' = \partial\hat{a}$  und  $ia' = \partial a$ . Diagramm ( $G$  weglassen)

$$\begin{array}{ccccccc} 0 & \longrightarrow & C^p(\text{Hom}(A'', B)) & \xrightarrow{\hat{j}} & C^p(\text{Hom}(A, B)) & \xrightarrow{\hat{i}} & C^p(\text{Hom}(A', B)) \longrightarrow 0 \\ & & & & \hat{a} \longmapsto & \hat{a}' & \\ \partial \downarrow & & \hat{a}'' \longmapsto & \bullet & & \downarrow & \partial \downarrow \\ & & & & & 0 & \\ 0 & \longrightarrow & C^{p+1}(\text{Hom}(A'', B)) & \xrightarrow{\hat{j}} & C^{p+1}(\text{Hom}(A, B)) & \longrightarrow & C^{p+1}(\text{Hom}(A', B)) \longrightarrow 0 \end{array}$$

und analog

$$\begin{array}{ccccccc} 0 & \longrightarrow & C^{q-1}(A') & \xrightarrow{i} & C^{q-1}(A) & \xrightarrow{j} & C^{q-1}(A'') \longrightarrow 0 \\ & & & & a \longmapsto & a'' & \\ \partial \downarrow & & a' \longmapsto & \bullet & & \downarrow & \partial \downarrow \\ & & & & & 0 & \\ 0 & \longrightarrow & C^q(A') & \xrightarrow{i} & C^q(A) & \xrightarrow{j} & C^q(A'') \longrightarrow 0 \end{array}$$

Dann ist  $\delta \hat{\alpha}$  durch  $\hat{a}''$  und  $\delta \alpha$  durch  $a'$  repräsentiert.

Folglich gilt

$$(\delta\hat{\alpha}) \cup \alpha + (-1)^p(\hat{\alpha} \cup \delta\alpha) = 0,$$

da diese Klasse durch die Kokette

$$\begin{aligned} \hat{a}'' \cup a'' + (-1)^p(\hat{a}' \cup a') &= \hat{a}'' \cup ja + (-1)^p(\hat{i}\hat{a} \cup a') \\ &= \hat{j}\hat{a}'' \cup a + (-1)^p(\hat{a} \cup ia') \\ &= \partial\hat{a} \cup a + (-1)^p(\hat{a} \cup \partial a) \\ &= \partial(\hat{a} \cup a) \end{aligned}$$

repräsentiert wird, die ein Korand ist.  $\square$

**Bemerkung.** Sei  $k$  ein Körper (mit trivialer  $G$ -Wirkung). Dann ist  $H^*(G, k)$  ein graduiert-kommutativer Ring und  $H^{2*}(G, k)$  ein kommutativer graduierter Ring.  $\text{Proj}(H^{2*}(G, k))$  ist die assoziierte Kohomologie-Varietät über  $k$ .

## 1.7 Proendliche Gruppen – Reduktion auf endliche Gruppen

**Satz 1.24.** Sei  $G$  eine proendliche Gruppe und  $A$  ein diskreter  $G$ -Modul. Dann existiert ein natürlicher Isomorphismus

$$\lim_{\substack{\longrightarrow \\ U}} H^n(G/U, A^U) \xrightarrow{\sim} H^n(G, A),$$

wobei  $U$  die offenen Normalteiler in  $G$  durchläuft.

*Konstruktion der Abbildung:* Für offene Normalteiler  $V \triangleleft U \triangleleft G$  haben wir die Inflationsabbildung

$$H^n(G/U, A^U) \longrightarrow H^n(G/V, A^V) \longrightarrow H^n(G, A)$$

Die Gruppen  $H^n(G/U, A^U)$  bilden ein direktes System und wir erhalten die Abbildung im Satz nach der Universaleigenschaft des direkten Limes.

*Beweis von 1.24.* Es ist bereits die natürliche Abbildung

$$\lim_{\substack{\longrightarrow \\ U}} C^\bullet(G/U, A^U) \longrightarrow C^\bullet(G, A)$$

ein Isomorphismus von Komplexen. Die Injektivität ist klar. Sei  $x : G^{n+1} \rightarrow A$  eine  $n$ -Kokette. Da  $A$  diskret ist, ist  $x$  lokal konstant auf  $G^{n+1}$ . Daher existiert ein offener Normalteiler  $U_0 \subset G$  so dass  $x$  konstant auf den Nebenklassen von  $U_0^{n+1}$  in  $G^{n+1}$  ist. D.h.  $x$  faktorisiert in der Form  $x : G^{n+1} \twoheadrightarrow (G/U_0)^{n+1} \rightarrow A$ .

*Behauptung:*  $\text{im}(x) \subset A^{U_0}$ .

*Grund:* Für  $u_0 \in U_0$  gilt

$$\begin{aligned} (u_0 x)(g_0, \dots, g_n) &= u_0 \cdot x(u_0^{-1} g_0, \dots, u_0^{-1} g_n) \\ &\parallel \\ &= u_0 x(g_0, \dots, g_n) \\ x(g_0, \dots, g_n) & \end{aligned}$$

Daher liegt  $x$  schon im Bild von  $C^n(G/U_0, A^U) \rightarrow C^n(G, A)$ . Wir erhalten:

$$\begin{aligned} \lim_{\overrightarrow{U}} H^n(G/U, A^U) &\cong H^n \left( \lim_{\overrightarrow{U}} C^\bullet(G/U, A^U) \right) \\ &= H^n(C^\bullet(G, A)) = H^n(G, A). \end{aligned}$$

□

**Korollar 1.25.** Sei  $G$  eine proendliche Gruppe und  $A$  ein diskreter  $G$ -Modul. Dann sind für  $n \geq 1$  die Gruppen  $H^n(G, A)$  Torsionsgruppen.

*Beweis.* Für jeden offenen Normalteiler  $U \subset G$  ist nach 1.16

$$\text{cor}_G^U \circ \text{res}_U^G = (G : U).$$

Daher faktorisiert die  $(G : U)$ -Multiplikation

$$\begin{array}{ccccc} H^n(G/U, A^U) & \xrightarrow{\text{res}} & H^n(\{1\}, A^U) & \xrightarrow{\text{cor}} & H^n(G/U, A^U) \\ & & \parallel & & \\ & & 0 & & \end{array}$$

über 0, d.h.  $(G : U)H^n(G/U, A^U) = 0$ .

Insbesondere ist  $H^n(G/U, A^U)$  eine Torsionsgruppe und nach 1.24 auch  $H^n(G, A)$ .

□

**Korollar 1.26.** Ist  $A$  eindeutig teilbar, so gilt

$$H^n(G, A) = 0 \quad \forall n \geq 1$$

*Beweis.*  $H^n(G, A)$  ist eine eindeutig teilbare Torsionsgruppe.

□

**Notation:** Sei  $A$  ein diskreter  $G$ -Torsionsmodul. Wir sagen  $(\#G, \#A) = 1$  wenn für jedes  $a \in A$ , und jeden offenen Normalteiler  $U \subset G$  gilt:  $((G, U), \text{ord}(a)) = 1$ .

**Korollar 1.27.** Gilt  $(\#G, \#A) = 1$ , so folgt

$$H^n(G, A) = 0 \quad \forall n \geq 1.$$

*Beweis.* Für jedes  $U \subset G$  ist die  $(G : U)$ -Multiplikation auf  $A^U$  ein Isomorphismus

$$\begin{aligned} \implies H^n(G/U, A^U) &= 0 \quad \forall U, \\ \implies H^n(G, A) &= 0. \end{aligned}$$

□

## 1.8 Abstrakte Gruppen – Beziehung zwischen Homologie und Kohomologie

Sei  $G$  eine abstrakte Gruppe.

**Lemma 1.28.** *Sei  $B$  eine abelsche Gruppe. Dann überführt der Funktor*

$$\mathrm{Hom}(-, B) : G - \mathrm{Mod} \longrightarrow G - \mathrm{Mod}.$$

*induzierte in koinduzierte Moduln.*

*Beweis.* Sei  $A$  eine abelsche Gruppe. Dann gilt

$$\begin{aligned} \mathrm{Hom}(\mathrm{Ind}_G A, B) &= \mathrm{Hom}(\mathbb{Z}[G] \otimes A, B) \\ &= \mathrm{Hom}(\mathbb{Z}[G], \mathrm{Hom}(A, B)) \\ &= \mathrm{Koind}_G \mathrm{Hom}(A, B). \end{aligned}$$

□

**Erinnerung:**  $\mathbb{Q}/\mathbb{Z}$  ist eine teilbare, d.h. injektive abelsche Gruppe, daher ist der Funktor

$$\begin{aligned} * : G - \mathrm{Mod} &\longrightarrow G - \mathrm{Mod} \\ A &\longmapsto \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}) \end{aligned}$$

exakt.

**Satz 1.29.**

$$H_n(G, A)^* \cong H^n(G, A^*).$$

*Beweis.* Sei  $P_\bullet \rightarrow A$  eine Auflösung durch induzierte Moduln. Dann ist  $A^* \rightarrow (P_\bullet)^*$  eine Auflösung durch koinduzierte. Wir erhalten

$$\begin{aligned} H_n(G, A)^* &= \mathrm{Hom}(H_n(G, A), \mathbb{Q}/\mathbb{Z}) \\ &= \mathrm{Hom}(H_n(P_{\bullet_G}), \mathbb{Q}/\mathbb{Z}) \\ &= H^n(\mathrm{Hom}(P_{\bullet_G}, \mathbb{Q}/\mathbb{Z})) \\ &= H^n(\mathrm{Hom}(P_\bullet, \mathbb{Q}/\mathbb{Z})^G) \\ &= H^n(G, A^*). \end{aligned}$$

□

# Algebraische Zahlentheorie II

## Sommersemester 2022

Dr. Katharina Hübner

basierend auf Alexander Schmidts AZT2-Skript von 2014

### Inhaltsverzeichnis

<b>1</b>	<b>Kohomologie endlicher Gruppen</b>	<b>1</b>
1.1	Tate-Kohomologiegruppen . . . . .	1
1.2	Res, Kores und Cup-Produkt . . . . .	5
1.3	Kohomologie der zyklischen Gruppen . . . . .	7
1.4	Kohomologische Trivialität . . . . .	10

## 1 Kohomologie endlicher Gruppen

Im ganzen Kapitel sei  $G$  stets eine endliche Gruppe.

### 1.1 Tate-Kohomologiegruppen

**Lemma 1.1.** *Ist  $G$  eine endliche Gruppe, so ist jeder induzierte Modul koinduziert und jeder koinduzierte Modul induziert. Insbesondere sind koinduzierte Moduln homologisch trivial und induzierte Moduln kohomologisch trivial.*

*Beweis.* Die Abbildung

$$\begin{array}{ccc}
 \text{Koind}_G A & \longrightarrow & \text{Ind}_G A \\
 \parallel & & \parallel \\
 \text{Abb}(G, A) & \longrightarrow & \mathbb{Z}[G] \otimes A \\
 x & \longmapsto & \sum_{g \in G} g \otimes x(g^{-1})
 \end{array}$$

ist ein Isomorphismus von  $G$ -Moduln. □

Die Normabbildung  $N_G : A \rightarrow A$ ,  $a \mapsto \sum_{g \in G} a$  induziert eine Abbildung  $\bar{N}_G : A_G \rightarrow A^G$ .

**Definition.** Die Gruppen

$$\hat{H}_0(G, A) = \ker(\bar{N}_G) \subset H_0(G, A)$$

und  $\hat{H}^0(G, A) = H^0(G, A)/\text{im}(\bar{N}_G)$  heißen die **modifizierten (Ko)Homologiegruppen** in Dimension 0.

**Lemma 1.2.** Für einen (ko)induzierten Modul  $A$  gilt

$$\hat{H}_0(G, A) = 0 = \hat{H}^0(G, A),$$

d.h.  $\bar{N}_G : A_G \rightarrow A^G$  ist ein Isomorphismus.

*Beweis.* Sei  $A = \mathbb{Z}[G] \otimes B$  mit einer abelschen Gruppe  $B$ . Jedes Element in  $x \in \mathbb{Z}[G] \otimes B$  hat eine eindeutige Darstellung der Form  $x = \sum_{g \in G} g \otimes x_g$ . Für  $x \in A^G$  folgt, dass alle  $x_g$  gleich sind, und somit gilt  $x = N_G(1 \otimes x_1)$ . Dies zeigt  $\hat{H}^0(G, A) = 0$ .

Aus  $N_G(x) = 0$  folgt  $\sum x_g = 0$ , also  $x = \sum_{g \in G} (g - 1)(1 \otimes x_g)$ , und somit  $\hat{H}_0(G, A) = 0$ .  $\square$

Für eine endlich erzeugte freie abelsche Gruppe  $C$  setzen wir  $C^+ = \text{Hom}(C, \mathbb{Z})$ . Ist  $C$  ein  $G$ -Modul, so auch  $C^+$  und es gilt:  $C \xrightarrow{\sim} C^{++}$ .

Für eine abelsche Gruppe  $A$  haben wir Isomorphismen

$$\begin{aligned} C \otimes A &\xrightarrow{\sim} \text{Hom}(C^+, A), \quad c \otimes a \mapsto (f \mapsto f(c) \cdot a) \\ C^+ \otimes A &\xrightarrow{\sim} \text{Hom}(C, A), \quad f \otimes a \mapsto (c \mapsto f(c) \cdot a). \end{aligned}$$

Nun sei  $C$  ein endlich erzeugter projektiver  $G$ -Modul, insbesondere ist  $C$  endlich erzeugt und frei als abelsche Gruppe. Dann ist  $C$  direkter Summand in  $\text{Ind}_G C$  und somit nach Lemma 1.28 in Kapitel 3.2 für jeden  $G$ -Modul  $A$  der Modul  $\text{Hom}(C, A)$  direkter Summand in einem (ko)induzierten Modul. Nach 1.2 erhalten wir somit Isomorphismen

$$(C^+ \otimes A)_G \xrightarrow{\sim} \text{Hom}(C, A)_G \xrightarrow[\sim]{\bar{N}_G} \text{Hom}(C, A)^G. \quad (*)$$

Sei nun  $P_\bullet \xrightarrow{\varepsilon} \mathbb{Z}$  eine Auflösung von  $\mathbb{Z}$  durch endlich erzeugte projektive  $G$ -Moduln. Dann ist  $\mathbb{Z} \xrightarrow{\varepsilon^+} P_\bullet^+$  eine Auflösung durch kohomologisch triviale Moduln (Lemma 1.28 in Kapitel 3.2). Für  $n \leq -1$  setzen wir  $P_n := (P_{-n-1})^+$  und kleben die Komplexe zu einem exakten Komplex

$$\longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\varepsilon^+ \circ \varepsilon} P_{-1} \longrightarrow P_{-2} \longrightarrow \dots$$

zusammen.

**Definition.** Für einen  $G$ -Modul  $A$  setzt man

$$\hat{X}^\bullet(G, A) = \text{Hom}(P_\bullet, A) \text{ und } \hat{C}^\bullet(G, A) = \hat{X}^\bullet(G, A)^G$$

und definiert die  $n$ -te **Tate-Kohomologiegruppe** ( $n \in \mathbb{Z}$ ) durch

$$\hat{H}^n(G, A) = H^n(\hat{C}^\bullet(G, A)).$$

**Satz 1.3.** *Es gilt*

$$\hat{H}^n(G, A) = \begin{cases} H^n(G, A) & \text{für } n \geq 1 \\ \hat{H}^0(G, A) & n = 0 \\ \hat{H}_0(G, A) & n = -1 \\ H_{-n-1}(G, A) & n \leq -2. \end{cases}$$

*Beweis.* Für  $n \geq 1$  gilt

$$H^n(\hat{C}(G, A)) = H^n(C^\bullet(G, A)) = H^n(G, A).$$

Für  $n \leq -2$  gilt unter Benutzung von  $(*)$

$$\begin{aligned} \hat{H}^n(\hat{C}(G, A)) &= H^{n+1}(\text{Hom}(P_\bullet^+, A)^G) \cong H_{-n-1}((P_\bullet \otimes A)_G) \\ &= H_{-n-1}(G, A). \end{aligned}$$

Nun schauen wir die Mitte an:

$$\begin{array}{ccccc} \text{Hom}(P_{-2}, A)^G & \rightarrow & \text{Hom}(P_{-1}, A)^G & \xrightarrow{(\varepsilon^+_{\circ\varepsilon})^*} & \text{Hom}(P_0, A)^G \rightarrow \text{Hom}(P_1, A)^G \\ \parallel \wr & & \parallel \wr & \nearrow \varphi & \\ (P_1 \otimes A)_G & \rightarrow & (P_0 \otimes A)_G & & \end{array} .$$

Nach Konstruktion der vertikalen Isomorphismen kommutiert das Diagramm

$$\begin{array}{ccccc} \text{Hom}(P_{-1}, A)^G & \xrightarrow{(\varepsilon^+)^*} & \text{Hom}(\mathbb{Z}, A)^G & \xrightarrow{\varepsilon^*} & \text{Hom}(P_0, A)^G \\ \parallel \wr & & \parallel \wr & & \\ (P_0 \otimes A)_G & \xrightarrow{\varepsilon_*} & (\mathbb{Z} \otimes A)_G & & \end{array} .$$

Daher faktorisiert  $\varphi$  in der Form

$$(P_0 \otimes A)_G \xrightarrow{\varepsilon_*} (\mathbb{Z} \otimes A)_G = A_G \xrightarrow{\bar{N}_G} A^G = \text{Hom}(\mathbb{Z}, A)^G \xrightarrow{\varepsilon^*} \text{Hom}(P_0, A)^G$$

und wir erhalten  $\hat{H}^{-1}(G, A) = \ker(\bar{N}_G) = \hat{H}_0(G, A)$  und  $\hat{H}^0(G, A) = \text{coker}(\bar{N}_G)$ . □

**Korollar 1.4.** *Sei  $A$  ein (ko)induzierter  $G$ -Modul. Dann gilt*

$$\hat{H}^n(G, A) = 0 \quad \forall n \in \mathbb{Z}.$$



**Satz 1.5.** Sei  $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$  eine exakte Folge von  $G$ -Moduln. Dann existiert eine natürliche exakte Folge

$$\cdots \longrightarrow \hat{H}^i(G, A') \longrightarrow \hat{H}^i(G, A) \longrightarrow \hat{H}^i(G, A'') \longrightarrow \cdots.$$

*Beweis.* Die  $\hat{X}^n(G, -)$  sind direkte Summanden in induzierten  $G$ -Moduln, insbesondere gilt  $H^1(G, \hat{X}^n(G, A')) = 0$ . Daher erhalten wir aus den kurzen exakten Folgen

$$0 \rightarrow \hat{X}^n(G, A') \rightarrow \hat{X}^n(G, A) \rightarrow \hat{X}^n(G, A'') \rightarrow 0$$

die exakte Folge von Komplexen.

$$0 \rightarrow \hat{C}^\bullet(G, A') \rightarrow \hat{C}^\bullet(G, A) \rightarrow \hat{C}^\bullet(G, A'') \rightarrow 0.$$

Die assoziierte lange exakte Kohomologiefolge zeigt das gewünschte.  $\square$

Definiert man wie vorher für einen  $G$ -Modul  $A$  induktiv für  $i \geq 0$ :

$$A_0 = A, \quad A_{i+1} = \text{coker}(A_i \rightarrow \text{Koind}_G A_i),$$

und induktiv für  $i \leq 0$ :  $A_0 = A$

$$A_i = \ker(\text{Ind}_G A_{i+1} \longrightarrow A_{i+1})$$

so erhält man **Dimensionsverschiebung**:

$$\hat{H}^n(G, A_i) = \hat{H}^{n+i}(G, A) \quad \forall n, i \in \mathbb{Z}.$$

Nun betrachten wir den Fall, dass  $P_\bullet$  der homologische Standardkomplex  $X_\bullet$  ist, d.h.  $X_n = \mathbb{Z}[G^{n+1}]$  mit den vorher definierten Differentialen. Sei für  $(g_0, \dots, g_n) \in G^{n+1}$  das Element  $\varphi_{g_0, \dots, g_n} \in \mathbb{Z}[G^{n+1}]^+$  gegeben durch

$$\varphi_{g_0, \dots, g_n}(\sigma_0, \dots, \sigma_n) = \begin{cases} 1 & \text{falls } (g_0, \dots, g_n) = (\sigma_0, \dots, \sigma_n) \\ 0 & \text{sonst.} \end{cases}$$

Dann bilden die  $\varphi_{g_0, \dots, g_n}$  eine  $\mathbb{Z}$ -Basis von  $\mathbb{Z}[G^{n+1}]^+$ . Wir erhalten einen  $G$ -Modulisomorphismus

$$\begin{aligned} \mathbb{Z}[G^{n+1}]^+ &\xrightarrow{\sim} \mathbb{Z}[G^{n+1}], \\ \varphi_{g_0, \dots, g_n} &\longmapsto (g_0^{-1}, \dots, g_n^{-1}). \end{aligned}$$

Bezüglich dieses Isomorphismus erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccc} \mathbb{Z}[G^{n+1}]^+ & \xrightarrow{\sim} & \mathbb{Z}[G^{n+1}] \\ \uparrow \partial^+ & & \uparrow \Delta \\ \mathbb{Z}[G^n]^+ & \xrightarrow{\sim} & \mathbb{Z}[G^n], \end{array}$$

wobei

$$\Delta(g_0, \dots, g_{n-1}) = \sum_{\tau \in G} \sum_{i=0}^n (-1)^i (g_0, \dots, \tau, \dots, g_{n-1})$$

gilt. Wir rechnen das nach:

$$\begin{aligned}
\partial^+ \varphi_{g_0, \dots, g_{n-1}}(\sigma_0, \dots, \sigma_n) &= \varphi_{g_0, \dots, g_{n-1}}(\partial(\sigma_0, \dots, \sigma_n)) \\
&= \varphi_{g_0, \dots, g_{n-1}} \left( \sum_{i=0}^n (-1)^i (\sigma_0, \dots, \hat{\sigma}_i, \dots, \sigma_n) \right) \\
&= \sum_{i=0}^n (-1)^i \sum_{\tau \in G} \varphi_{g_0, \dots, \tau, \dots, g_{n-1}}(\sigma_0, \dots, \sigma_n).
\end{aligned}$$

Explizite Rechnungen in der „Mitte“ ergeben dann die folgende alternative Definition von Tate-Kohomologie.

**Definition.** Der Komplex  $\hat{X}_\bullet$  mit

$$\hat{X}_n = \mathbb{Z}[G^{n+1}] \quad \text{für } n \geq 0$$

und

$$\hat{X}_n = \mathbb{Z}[G^{-n}] \quad \text{für } n \leq -1$$

mit den Differentialen:

$n \geq 1$ :

$$\begin{aligned}
\partial_n(g_0, \dots, g_n) &= \sum_{i=0}^n (-1)^i (g_0, \dots, \hat{g}_i, \dots, g_n) \\
\partial_{-n}(g_0, \dots, g_{n-1}) &= \sum_{\tau \in G} \sum_{i=0}^n (-1)^i (g_0, \dots, \tau, \dots, g_{n-1})
\end{aligned}$$

und  $\partial_0$ :

$$\begin{array}{ccc}
X_0 & \longrightarrow & X_{-1} \\
\parallel & & \parallel \\
\mathbb{Z}[G] & & \mathbb{Z}[G]
\end{array}$$

ist die Abbildung, die jedes  $g \in G$  auf  $\sum_{\tau \in G} \tau \in \mathbb{Z}[G]$  abbildet, heißt die **vollständige Standardauflösung** von  $\mathbb{Z}$ . Es gilt

$$\hat{H}^n(G, A) = H^n(\text{Hom}(X_\bullet, A)^G).$$

## 1.2 Res, Kores und Cup-Produkt

Sei  $H \subset G$  eine Untergruppe und  $A$  ein  $G$ -Modul. Für  $n \leq -2$ ,  $n \geq 1$  haben wir die Abbildung

$$res : \hat{H}^n(G, A) \longrightarrow \hat{H}^n(H, A).$$

Für  $n = 0$  ist  $res : H^0(G, A) \rightarrow H^0(H, A)$  die natürliche Inklusion  $A^G \hookrightarrow A^H$ . Für  $a \in A$  gilt  $\sum_{g \in G} ga = \sum_s \sum_{h \in H} h \cdot sa$  wobei  $s$  ein Vertretersystem von  $H \backslash G$  durchläuft. Daher gilt  $N_G(A) \subset N_H(A)$  und  $res$  faktorisiert zu einer Abbildung

$$res : \hat{H}^0(G, A) \longrightarrow \hat{H}^0(H, A).$$

Analog:  $res : H_0(G, A) \rightarrow H_0(H, A)$  ist definiert durch  $a \mapsto \sum_{s \in H \backslash G} sa$ .

Wegen

$$\sum_{h \in H} h \left( \sum_s sa \right) = \sum_{g \in G} ga$$

induziert  $res$  eine Abbildung

$$res : \hat{H}^{-1}(G, A) \longrightarrow \hat{H}^{-1}(H, A).$$

**Satz 1.6.**  $res$  ist ein Homomorphismus von  $\delta$ -Funktoren d.h. für jede exakte Folge  $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$  von  $G$ -Moduln und alle  $n \in \mathbb{Z}$  kommutiert das Diagramm

$$\begin{array}{ccc} \hat{H}^n(G, A'') & \xrightarrow{\delta} & \hat{H}^{n+1}(G, A') \\ res \downarrow & & \downarrow res \\ \hat{H}^n(H, A'') & \xrightarrow{\delta} & \hat{H}^{n+1}(H, A'). \end{array}$$

*Beweis.* Für  $n \neq -1$  klar.  $n = -1$  Übungsaufgabe. □

Analog setzt sich die Abbildung

$$cor : \hat{H}^n(H, A) \rightarrow \hat{H}^n(H, A),$$

die bereits für  $n \leq -2$ ,  $n \geq 1$  definiert, ist auf alle  $n \in \mathbb{Z}$  fort und es gilt

**Satz 1.7.**  $cor$  ist ein Homomorphismus von  $\delta$ -Funktoren.

**Satz 1.8.** Es gilt

$$cor_G^H \cdot res_H^G = (G : H).$$

Seien  $A, B$   $G$ -Moduln. Die natürliche Abbildung

$$A^G \times B^G \longrightarrow (A \otimes B)^G$$

setzt sich fort zu

$$\hat{H}^0(G, A) \times \hat{H}^0(G, B) \longrightarrow \hat{H}^0(G, A \otimes B).$$

Wir definieren (entsprechend Satz 1.21 in Kapitel 3.2) das Cup-Produkt

$$\hat{H}^p(G, A) \times \hat{H}^q(G, B) \longrightarrow \hat{H}^{p+q}(G, A \otimes B)$$

durch das kommutative Diagramm

$$\begin{array}{ccccc} \hat{H}^p(G, A) & \times & \hat{H}^q(G, B) & \xrightarrow{\cup} & \hat{H}^{p+q}(G, A \otimes B) \\ | \wr & & | \wr & & | \wr (-1)^{pq} \\ \hat{H}^0(G, A_p) & \times & \hat{H}^0(G, B_q) & \xrightarrow{\cup} & \hat{H}^{p+q}(G, A_p \otimes B_q). \end{array}$$

Beachte

$$\begin{aligned}\hat{H}^{p+q}(G, A \otimes B) &\cong \hat{H}^p(G, (A \otimes B)_q) \cong \hat{H}^p(G, A \otimes B_q) \\ &\cong \hat{H}^0(G, (A \otimes B_q)_p) \cong \hat{H}^0(G, A_p \otimes B_q).\end{aligned}$$

Man kann auch explizite Formeln für das Cup-Produkt auf dem vollständigen Standardkomplex geben.

Schließlich passen auch das homologische und das kohomologische Shapiro-Lemma zusammen, d.h. es gilt

**Satz 1.9.** *Sei  $H \subset G$  eine Untergruppe und  $A$  ein  $H$ -Modul. Dann gilt*

$$\hat{H}^n(H, A) \cong \hat{H}^n(G, \text{Ind}_G^H A)$$

für alle  $n \in \mathbb{Z}$ .

*Beweis.* Lassen wir weg. □

### 1.3 Kohomologie der zyklischen Gruppen

Sei  $G$  eine zyklische Gruppe der Ordnung  $n$  und  $\sigma \in G$  ein Erzeuger. Setze

$$\begin{aligned}N_G A &= \text{im}(N_G : A \rightarrow A), \\ {}_N G A &= \ker(N_G : A \rightarrow A).\end{aligned}$$

Dann gilt nach Definition:

$$\hat{H}^0(G, A) = A^G / N_G A, \quad \hat{H}^{-1}(G, A) = {}_N G A / I_G A.$$

Wegen

$$\sigma^i - 1 = (\sigma - 1)(\sigma^{i-1} + \dots + 1)$$

gilt  $I_G A = (\sigma - 1) \cdot A$ .

**Satz 1.10.** *Sei  $G$  eine endliche zyklische Gruppe. Dann ist  $\hat{H}^2(G, \mathbb{Z})$  zyklisch von der gleichen Ordnung wie  $G$ . Sei  $\chi \in H^2(G, \mathbb{Z})$  ein Erzeuger. Dann induziert das Cup-Produkt*

$$\chi \cup - : \hat{H}^n(G, A) \xrightarrow{\sim} \hat{H}^{n+2}(G, A)$$

*Isomorphismen für alle  $n \in \mathbb{Z}$  und jeden  $G$ -Modul  $A$ . Insbesondere gilt:*

$$\hat{H}^{2n}(G, A) \cong \hat{H}^0(G, A)$$

und

$$\hat{H}^{2n-1}(G, A) \cong \hat{H}^{-1}(G, A)$$

für alle  $n \in \mathbb{Z}$ .

*Beweis.* Sei  $\langle \sigma \rangle = G$  und  $N = \#G$ . Wir betrachten die exakte Folge

$$(*) \quad 0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} \mathbb{Z}[G] \xrightarrow{(\sigma-1)} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

wobei  $\varepsilon$  die Augmentation  $\sum a_i \sigma^i \mapsto \sum a_i$  und

$$\mu(a) = a(1 + \sigma + \cdots + \sigma^{N-1})$$

ist. Wir erhalten (aufbrechen in zwei kurze exakte Folgen) einen Isomorphismus

$$\delta^2 : \hat{H}^0(G, \mathbb{Z}) \xrightarrow{\sim} \hat{H}^2(G, \mathbb{Z}).$$

Wegen

$$\begin{aligned} \hat{H}^0(G, \mathbb{Z}) &= \mathbb{Z}/N_G \mathbb{Z} \\ &= \mathbb{Z}/(1 + \cdots + \sigma^{N-1})\mathbb{Z} = \mathbb{Z}/N\mathbb{Z} \end{aligned}$$

erhalten wir die erste Aussage. Außerdem ist jeder Erzeuger  $\chi$  von der Form

$$\chi = \delta^2(m), \quad m \in (\mathbb{Z}/N\mathbb{Z})^\times.$$

Da alle Objekte in  $(*)$   $\mathbb{Z}$ -frei sind, bleibt  $(*)$  nach Tensorieren mit jedem  $G$ -Modul  $A$  exakt. Daher erhalten wir für jedes  $A$  einen Isomorphismus

$$\delta^2 : \hat{H}^n(G, A) \xrightarrow{\sim} \hat{H}^{n+2}(G, A),$$

der in ein kommutatives Diagramm

$$\begin{array}{ccc} \hat{H}^n(G, A) & \xlongequal{\quad} & \hat{H}^n(G, A) \\ \downarrow \cdot m & & \chi \cup \downarrow \\ \hat{H}^n(G, A) & \xrightarrow[\delta^2]{\sim} & \hat{H}^{n+2}(G, A) \end{array}$$

passt.

Um zu zeigen, dass  $\chi \cup -$  ein Isomorphismus ist, genügt es zu zeigen, dass  $\cdot m$  ein Isomorphismus ist. Dies folgt aus  $m \in (\mathbb{Z}/N\mathbb{Z})^\times$  und weil  $\hat{H}^n(G, A)$  ein  $\mathbb{Z}/N\mathbb{Z}$ -Modul ist.  $\square$

**Bemerkung.** Nach Wahl eines Erzeugers  $\sigma$  von  $G$  werden wir stets den Isomorphismus  $\delta^2(1) \cup - : \hat{H}^n(G, A) \xrightarrow{\sim} \hat{H}^{n+2}(G, A)$  als „kanonische“ Identifikation verwenden.

**Korollar 1.11.** Sei  $G$  endlich zyklisch. Ist  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  eine kurze exakte Folge von  $G$ -Moduln, so erhalten wir ein exaktes Hexagon

$$\begin{array}{ccccc} & & \hat{H}^0(G, A) & \longrightarrow & \hat{H}^0(G, B) \\ & \nearrow & & & \searrow \\ \hat{H}^{-1}(G, C) & & & & \hat{H}^0(G, C) \\ & \nwarrow & & & \swarrow \\ & & \hat{H}^{-1}(G, B) & \longleftarrow & \hat{H}^{-1}(G, A). \end{array}$$

*Beweis.* Alle Abbildungen sind die offensichtlichen, bis auf  $\hat{H}^0(G, C) \rightarrow \hat{H}^{-1}(G, A)$ . Dies ist die Komposition von  $\hat{H}^0(G, C) \xrightarrow{\delta} \hat{H}^1(G, A)$  mit dem Inversen des Isomorphismus

$$\delta^2(1) \cup - : \hat{H}^{-1}(G, A) \xrightarrow{\sim} \hat{H}^1(G, A)$$

aus 1.10. Dieser hängt von der Wahl eines Erzeugers  $\sigma$  von  $G$  ab, ist aber kanonisch im Modul. Daher kommutiert das Diagramm:

$$\begin{array}{ccc} \hat{H}^{-1}(G, A) & \longrightarrow & \hat{H}^{-1}(G, B) \\ \downarrow \wr & & \downarrow \wr \\ \hat{H}^1(G, A) & \longrightarrow & \hat{H}^1(G, B) \end{array}$$

was die Exaktheit des Hexagons auch bei  $\hat{H}^0(G, C)$  zeigt.  $\square$

**Definition.** Ist sowohl  $\hat{H}^0(G, A)$  als auch  $\hat{H}^{-1}(G, A)$  endlich, so heißt

$$h(G, A) := \frac{\#\hat{H}^0(G, A)}{\#\hat{H}^1(G, A)}$$

der **Herbrand-Index** von  $A$ .

Sei  $\sigma$  ein Erzeuger von  $G$  und  $D = \sigma - 1 : A \rightarrow A$ . Dann gilt  $D \circ N_G = 0 = N_G \circ D$  und

$$\begin{aligned} \hat{H}^0(G, A) &= \ker(D)/\text{im}(N_G) \\ \hat{H}^{-1}(G, A) &= \ker(N_G)/\text{im}(D) \end{aligned}$$

**Satz 1.12.** Sei  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  eine exakte Folge von  $G$ -Moduln. Dann gilt

$$h(G, B) = h(G, A) \cdot h(G, C)$$

in dem Sinne: Sind zwei der Indizes definiert, so auch der dritte und Gleichheit gilt.

*Beweis.* Dies folgt direkt aus dem Hexagon in 1.11.  $\square$

**Satz 1.13.** Ist  $A$  endlich, so gilt

$$h(G, A) = 1.$$

*Beweis.* Der Homomorphiesatz liefert

$$\#\ker(D) \cdot \#\text{im}(D) = \#A = \#\ker(N_G) \cdot \#\text{im}(N_G).$$

Dies zeigt

$$\frac{\#\hat{H}^0(G, A)}{\#\hat{H}^1(G, A)} = 1$$

$\square$

## 1.4 Kohomologische Trivialität

Erinnerung.

**Definition.** Ein  $G$ -Modul  $A$  heißt **kohomologisch trivial**, wenn  $H^n(H, A) = 0$  für alle  $n \geq 1$ ,  $H \subseteq G$ .

Ist  $A$  eine Torsionsgruppe, und  $p$  eine Primzahl, so bezeichnet  $A(p)$  den  $p$ -primären Anteil. Es gilt  $A \cong \bigoplus_p A(p)$ .

**Satz 1.14.** Sei  $A$  ein  $G$ -Modul und  $G_p$  eine  $p$ -Sylowgruppe von  $G$ . Dann ist für alle  $n \in \mathbb{Z}$

$$res : \hat{H}^n(G, A)(p) \longrightarrow \hat{H}^n(G_p, A)$$

injektiv und

$$cor : \hat{H}^n(G_p, A) \longrightarrow \hat{H}^n(G, A)(p)$$

surjektiv.

*Beweis.* Es gilt  $cor \circ res = (G : G_p)$  und dies ist eine natürliche Zahl prim zu  $p$ . Daher ist

$$cor \circ res : \hat{H}^n(G, A)(p) \longrightarrow \hat{H}^n(G, A)(p)$$

ein Isomorphismus. □

**Korollar 1.15.**

- (i) Gilt  $\hat{H}^n(G_p, A) = 0$  für alle Primzahlen  $p$  dann gilt  $\hat{H}^n(G, A) = 0$ .
- (ii) Ein  $G$ -Modul  $A$  ist genau dann kohomologisch trivial, wenn er ein kohomologisch trivialer  $G_p$ -Modul für jedes  $p$  ist.

*Beweis.* (i) Nach 1.14 haben wir eine Injektion

$$\hat{H}^n(G, A) \rightarrow \bigoplus_p \hat{H}^n(G_p, A).$$

Daher gilt

$$\hat{H}^n(G_p, A) = 0 \quad \forall p \implies \hat{H}^n(G, A) = 0.$$

(ii) Aus (i) folgt  $A$  kohomologisch trivialer  $G_p$ -Modul  $\forall p \implies A$  kohomologisch trivialer  $G$ -Modul.

Die andere Richtung ist trivial, weil eine Untergruppe von  $G_p$  auch eine Untergruppe von  $G$  ist. □

**Satz 1.16.** Sei  $G$  eine  $p$ -Gruppe und sei  $A$  ein  $p$ -primärer  $G$ -Modul.

- (i) Gilt  $H_0(G, A) = 0$  oder  $H^0(G, A) = 0$ , so folgt  $A = 0$ .
- (ii) Gilt  $pA = 0$  und  $\hat{H}^n(G, A) = 0$  für ein  $n \in \mathbb{Z}$ , dann ist  $A$  induziert.

*Beweis.* Jedes  $a \in A$  erzeugt einen endlichen  $G$ -Untermodul von  $A$ . Daher können wir im Beweis der Implikation  $H^0(G, A) = 0 \implies A = 0$  annehmen, dass  $A$  endlich ist. Das Komplement  $A \setminus A^G$  ist disjunkte Vereinigung von nichttrivialen  $G$ -Bahnen  $Ga$ ,  $a \in A \setminus A^G$ . Es gilt:  $\#Ga = \#(G/G_a)$ , wobei  $G_a$  die Standgruppe von  $a$  ist. Daher gilt

$$p \mid \#Ga \quad \forall a \in A \setminus A^G.$$

Daher gilt  $p \mid \#(A \setminus A^G)$ . Gilt nun  $A^G = 0$  so folgt  $\#A \equiv 1 \pmod{p}$ . Da  $\#A$  eine  $p$ -Potenz ist, folgt  $\#A = 1$ .

Ist  $H_0(G, A) = 0$ , so folgt  $0 = H_0(G, A)^* = H^0(G, A^*)$ . Also  $A^* = 0 \implies A = 0$ . Dies zeigt (i).

(ii) Wegen  $pA = 0$  ist  $A$  ein  $\mathbb{F}_p[G]$ -Modul. Sei  $\Lambda = \mathbb{F}_p[G]$ ,  $I$  eine  $\mathbb{F}_p$ -Basis von  $A^G$  und  $V = \bigoplus_I \Lambda$ . Dann ist  $\text{Hom}(A, V)$  für jeden Modul  $A$  ein induzierter Modul, denn

$$\text{Hom}(A, \Lambda) = \text{Hom}(A, \mathbb{F}_p[G]) = \text{Hom}(A, \mathbb{F}_p) \otimes_{\mathbb{Z}} \mathbb{Z}[G].$$

Daher besteht die exakte Folge

$$0 \longrightarrow \text{Hom}(A/A^G, V) \longrightarrow \text{Hom}(A, V) \longrightarrow \text{Hom}(A^G, V) \longrightarrow 0$$

aus induzierten  $G$ -Moduln und folglich ist

$$\text{Hom}_G(A, V) \longrightarrow \text{Hom}_G(A^G, V) = \text{Hom}(A^G, V^G)$$

surjektiv. Außerdem gilt  $\Lambda^G = \mathbb{F}_p$ , also  $V^G = \bigoplus_I \mathbb{F}_p$ . Daher gibt es einen Isomorphismus  $A^G \cong V^G$  der sich wegen der Surjektivität zu einem  $G$ -Homomorphismus  $j : A \rightarrow V$  ausdehnt.  $j$  ist injektiv wegen  $\ker(j)^G = \ker(j|_{A^G}) = 0$  und (i). Nun setze  $C = \text{coker}(j)$ . Wir erhalten eine exakte Folge

$$0 \longrightarrow A^G \xrightarrow{\sim} V^G \longrightarrow C^G \longrightarrow H^1(G, A).$$

Daher gilt:

$$H^1(G, A) = 0 \implies C^G = 0 \implies C = 0 \implies j \text{ ist Isomorphismus}$$

$$\implies A \cong V = \bigoplus_I \mathbb{F}_p[G] = \text{Ind}_G \left( \bigoplus_I \mathbb{F}_p \right).$$

Gilt nun  $\hat{H}^n(G, A) = 0$  für ein  $n \in \mathbb{Z}$ , so folgt  $H^1(G, A_{n-1}) = \hat{H}^n(G, A) = 0$ , und  $A_{n-1}$  ist induziert. Daraus folgt:

$$H^1(G, A) = \hat{H}^{2-n}(G, A_{n-1}) = 0.$$

Daher ist  $A$  induziert. □



**Erinnerung:** Ein  $G$ -Modul  $A \neq 0$  heißt **einfach**, wenn es keinen  $G$ -Modul  $B$ , mit  $0 \subsetneq B \subsetneq A$  gibt.

**Lemma 1.17.** *Ein einfacher  $G$ -Modul  $A$  ist endlich. Es gibt eine eindeutig bestimmte Primzahl  $p$  mit  $pA = 0$ .*

*Beweis.* Sei  $A$  einfach und  $a \in A, a \neq 0$ . Dann ist  $A$  als  $G$ -Modul durch  $a$  erzeugt, also ist  $A$  endlich erzeugte abelsche Gruppe. Dann existiert eine Primzahl  $p$  so dass die  $p$ -Multiplikation  $A \xrightarrow{p} A$  nicht surjektiv ist. Daher gilt  $pA \subsetneq A$ , also  $pA = 0$ . Die Eindeutigkeit von  $p$  ist klar, da aus  $qA = 0$  für ein  $q \neq p$  folgen würde  $A = 0$ .  $\square$

**Satz 1.18.** *Sei  $G$  eine  $p$ -Gruppe. Dann ist jeder einfache  $p$ -primäre  $G$ -Modul  $A$  isomorph zu  $\mathbb{Z}/p\mathbb{Z}$  mit trivialer  $G$ -Wirkung.*

*Beweis.* Nach 1.17 gilt  $pA = 0$ . Wegen  $A \neq 0$  und  $A$  einfach folgt  $A^G = A$  ( $A^G = 0$  würde nach 1.16  $A = 0$  implizieren). Daher ist  $A$  ein  $\mathbb{F}_p$ -Vektorraum mit trivialer  $G$ -Wirkung. Da  $A$  einfach ist, folgt  $\dim_{\mathbb{F}_p} A = 1$ .  $\square$

Da jeder endliche  $G$ -Modul  $A$  eine Kompositionsreihe  $0 = A_0 \subseteq A_1 \subseteq \dots \subseteq A_n = A$  mit  $A_i/A_{i-1}$  einfach für  $i = 1, \dots, n$  besitzt (siehe Algebra-Vorlesung) erhalten wir

**Korollar 1.19.** *Ist  $G$  eine  $p$ -Gruppe, so hat jeder endliche  $p$ -primäre  $G$ -Modul  $A$  eine Kompositionsreihe in der die Graduierten isomorph zu  $\mathbb{Z}/p\mathbb{Z}$  mit trivialer  $G$ -Wirkung sind.*

**Satz 1.20.** *Sei  $G$  eine endliche Gruppe und sei  $A$  ein  $G$ -Modul, so dass für jede Primzahl  $p$  ein  $n_p \in \mathbb{Z}$  mit*

$$\hat{H}^{n_p}(G_p, A) = 0 = \hat{H}^{n_p+1}(G_p, A)$$

*existiert. Dann ist  $A$  kohomologisch trivial. Ist  $A$   $\mathbb{Z}$ -frei, so ist  $A$  ein direkter Summand in einem freien  $\mathbb{Z}[G]$ -Modul.*

*Für jeden kohomologisch trivialen Modul  $A$  gilt*

$$\hat{H}^n(H, A) = 0 \quad \forall n \in \mathbb{Z} \quad \forall H \subseteq G.$$

*Beweis.* Sei  $0 \rightarrow R \rightarrow F \rightarrow A \rightarrow 0$  eine exakte Folge mit einem freien  $\mathbb{Z}[G]$ -Modul  $F$ .

Behauptung: Für jede Primzahl  $p$  ist  $R/pR$  ein induzierter  $G_p$ -Modul.

Beweis der Behauptung.  $F$  ist induzierter  $G_p$ -Modul. Aus

$$\hat{H}^{n_p}(G_p, A) = 0 = \hat{H}^{n_p+1}(G_p, A), \quad \hat{H}^i(G_p, F) = 0 \quad \forall i \in \mathbb{Z}$$

und der langen exakten Folge erhalten wir

$$\hat{H}^{n_p+1}(G_p, R) = 0 = \hat{H}^{n_p+2}(G_p, R). \quad (2)$$

Die exakte Folge

$$0 \longrightarrow R \xrightarrow{p} R \longrightarrow R/pR \longrightarrow 0 \quad (3)$$

gibt uns

$$\hat{H}^{n_p+1}(G_p, R/pR) = 0.$$

Nach 1.16 (ii) ist  $R/pR$  induziert. Dies zeigt die Behauptung.

Wir nehmen nun an, dass  $A$   $\mathbb{Z}$ -frei ist. Dann ist  $\text{Ext}^1(A, A) = 0$  und Anwenden von  $\text{Hom}(A, -)$  auf die kurze exakte Folge  $0 \rightarrow R \rightarrow F \rightarrow A$  liefert die kurze exakte Folge

$$0 \longrightarrow \text{Hom}(A, R) \longrightarrow \text{Hom}(A, F) \longrightarrow \text{Hom}(A, A) \longrightarrow 0.$$

Wäre  $H^1(G, \text{Hom}(A, R)) = 0$ , so wäre  $\text{Hom}_G(A, F) \rightarrow \text{Hom}_G(A, A)$  surjektiv und ein Urbild von  $\text{id}_A$  in  $\text{Hom}_G(A, F)$  realisiert  $A$  als direkten Summanden in  $F$ .

Daher genügt zu zeigen:  $H^1(G, M) = 0$  für  $M = \text{Hom}(A, R)$ . Aus (3) erhalten wir die exakte Folge

$$0 \longrightarrow M \xrightarrow{p} M \longrightarrow \text{Hom}(A, R/pR) \longrightarrow 0.$$

Daher ist  $M/pM = \text{Hom}(A, R/pR)$  ein induzierter  $G_p$ -Modul. Dies impliziert, dass

$$H^1(G_p, M) \xrightarrow{p} H^1(G_p, M)$$

ein Isomorphismus ist, also  $H^1(G_p, M) = 0$  für alle  $p$ . Nach 1.15 (i) folgt  $H^1(G, M) = 0$ . Folglich ist  $A$  direkter Summand in  $F$ .

Nun sei  $A$  beliebig. Der erste Teil des Beweises angewendet auf den  $\mathbb{Z}$ -freien  $G$ -Modul  $R$  zeigt, dass  $R$  direkter Summand in einem freien  $\mathbb{Z}[G]$ -Modul ist. Daher ist  $R$  kohomologisch trivial und da  $F$  kohomologisch trivial ist, ist auch  $A$  kohomologisch trivial.

Sei nun  $A$  kohomologisch trivial. Dann ist nach dem eben bewiesenen  $R$  direkter Summand in einem freien. Daher gilt für jede Untergruppe  $H$  von  $G$

$$\hat{H}^i(H, F) = 0 = \hat{H}^i(H, R) \quad \forall i$$

und deshalb  $\hat{H}^i(H, A) = 0 \quad \forall i$ . □

**Korollar 1.21.** *Sei  $G$  eine endliche Gruppe und  $A, B$   $G$ -Moduln. Ist  $A$  kohomologisch trivial und  $B$  teilbar, oder  $A$   $\mathbb{Z}$ -frei und  $B$  kohomologisch trivial, so ist  $\text{Hom}(A, B)$  kohomologisch trivial.*

*Beweis.* Sei  $A$  kohomologisch trivial und  $B$  teilbar. Wir betrachten eine exakte Folge

$$0 \longrightarrow R \longrightarrow F \longrightarrow A \longrightarrow 0$$

mit einem freien  $G$ -Modul  $F$ . Da  $F$  und  $A$  kohomologisch trivial sind, gilt dies auch für  $R$ . Außerdem ist  $R$   $\mathbb{Z}$ -frei, und folglich nach 1.20 direkter Summand in einem freien  $\mathbb{Z}[G]$ -Modul  $F'$ . Folglich ist  $\text{Hom}(R, B)$  direkter Summand im induzierten  $G$ -Modul  $\text{Hom}(F', B)$  und daher kohomologisch trivial. Da  $B$  teilbar ist, ist die Folge

$$0 \longrightarrow \text{Hom}(A, B) \longrightarrow \text{Hom}(F, B) \longrightarrow \text{Hom}(R, B) \longrightarrow 0$$

exakt und da die letzten beiden Moduln kohomologisch trivial sind, gilt dies auch für  $\text{Hom}(A, B)$ . Der Fall dass  $A$   $\mathbb{Z}$ -frei und  $B$  kohomologisch trivial ist wird analog behandelt.  $\square$

# Algebraische Zahlentheorie II

## Sommersemester 2022

Dr. Katharina Hübner

basierend auf Alexander Schmidts AZT2-Skript von 2014

### Inhaltsverzeichnis

<b>1</b>	<b>Galoiskohomologie</b>	<b>1</b>
1.1	Die Abhängigkeit von der Auswahl des separablen Abschlusses . .	1
1.2	Additive Theorie . . . . .	2
1.3	Multiplikative Theorie – Hilberts Satz 90 . . . . .	4
1.4	Multiplikative Theorie – die Brauergruppe . . . . .	5
1.5	Die Brauergruppe eines lokalen Körpers . . . . .	7

## 1 Galoiskohomologie

Wir untersuchen Kohomologie der additiven und der multiplikativen Gruppe des separablen Abschlusses als Modul unter der absoluten Galoisgruppe.

### 1.1 Die Abhängigkeit von der Auswahl des separablen Abschlusses

Sei  $K$  ein Körper und  $\overline{K}_1, \overline{K}_2$  zwei separable Abschlüsse von  $K$ . Dann existiert ein (unkanonischer)  $K$ -Isomorphismus

$$\varphi : \overline{K}_1 \xrightarrow{\sim} \overline{K}_2.$$

Dieser induziert einen Isomorphismus

$$\begin{aligned} \varphi^* : G_2 = G(\overline{K}_2/K) &\xrightarrow{\sim} G_1 = G(\overline{K}_1/K), \\ \sigma &\longmapsto \varphi^{-1} \circ \sigma \circ \varphi. \end{aligned}$$

Nun sei  $\dagger \in \{+, \times\}$ . Dann ist  $\overline{K}_i^\dagger$  ein diskreter  $G(\overline{K}_i/K)$ -Modul,  $i = 1, 2$ . Das Paar  $\varphi^* : G_2 \xrightarrow{\sim} G_1$ ,  $\varphi : \overline{K}_1 \rightarrow \overline{K}_2$  ist kompatibel und wir erhalten einen Isomorphismus

$$H^i(G_1, \overline{K}_1^\dagger) \xrightarrow{\sim} H^i(G_2, \overline{K}_2^\dagger) \quad \forall i.$$

Ist nun

$$\varphi' : \overline{K}_1 \xrightarrow{\sim} \overline{K}_2$$

ein weiterer  $K$ -Isomorphismus, so erhalten wir das kommutative Diagramm

$$\begin{array}{ccc} H^i(G_1, \overline{K}_1^\dagger) & \xrightarrow{(\varphi^*, \varphi)} & H^i(G_2, \overline{K}_2^\dagger) \\ \parallel & & \downarrow ((\varphi' \circ \varphi^{-1})^*, \varphi' \circ \varphi^{-1}) \\ H^i(G_1, \overline{K}_1^\dagger) & \xrightarrow{(\varphi'^*, \varphi')} & H^i(G_2, \overline{K}_2^\dagger) \end{array}$$

Nun ist  $(\varphi' \circ \varphi^{-1})^*$  ein innerer Automorphismus von  $G_2$ , also gilt nach Satz 1.18 in Kapitel 3.2:

$$((\varphi' \circ \varphi^{-1})^*, \varphi' \circ \varphi^{-1}) = \text{id}_{H^i(G_2, \overline{K}_2^\dagger)}.$$

Wir erhalten daher einen *kanonischen* Isomorphismus

$$H^i(G(\overline{K}_1/K_1), \overline{K}_1^\dagger) \xrightarrow{\sim} H^i(G(\overline{K}_2/K_2), \overline{K}_2^\dagger)$$

für alle  $i$ .

Man benutzt oft die invarianten Schreibweisen

$$\begin{aligned} H^i(K, \mathbb{G}_a) &= H^i(G(\overline{K}/K), \overline{K}^+) \\ H^i(K, \mathbb{G}_m) &= H^i(G(\overline{K}/K), \overline{K}^\times). \end{aligned}$$

## 1.2 Additive Theorie

**Satz 1.1.** Sei  $L|K$  eine Galoiserweiterung mit Gruppe  $G$ . Dann gilt

$$H^i(G, L^+) = 0 \quad \forall i \geq 1.$$

*Beweis.* Wegen

$$H^i(G, L^+) = \varinjlim_{K \subset K' \subset L} H^i(G(K'|K), K'^+)$$

sei ohne Einschränkung  $L|K$  endlich. Dann ist wegen der Existenz einer Normalbasis  $L^+$  ein induzierter  $G$ -Modul.  $\square$

**Korollar 1.2.** Ist  $L|K$  endlich, so gilt  $\hat{H}^i(G, L^+) = 0 \quad \forall i \in \mathbb{Z}$ .

*Beweis.*  $L^+$  ist induziert, also kohomologisch trivial.  $\square$

Sei nun  $K$  ein Körper der Charakteristik  $p > 0$  und  $\overline{K}$  ein separabler Abschluss. Das Polynom  $f(X) = X^p - X$  ist separabel, daher ist der Homomorphismus(!)

$$\begin{aligned} \wp : \overline{K} &\longrightarrow \overline{K} \\ x &\longmapsto x^p - x \end{aligned}$$

surjektiv. Der Kern von  $\wp$  besteht aus den Nullstellen von  $f$ , d.h.

$$\ker(\wp) = \mathbb{F}_p \subset \overline{K}^+$$

(der Primkörper). Wir erhalten somit eine kurze exakte Folge von  $G_K$ -Moduln

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \overline{K}^+ \xrightarrow{\wp} \overline{K}^+ \longrightarrow 0$$

Aus der langen exakten Kohomologiefolge und 1.1 erhalten wir

**Korollar 1.3.** („Artin-Schreier-Theorie“). Sei  $K$  ein Körper der Charakteristik  $p > 0$ . Dann gilt

$$H^i(G_K, \mathbb{Z}/p\mathbb{Z}) = \begin{cases} \mathbb{Z}/p\mathbb{Z} & i = 0 \\ K^+/\wp K^+ & i = 1 \\ 0 & i \geq 2. \end{cases}$$

**Bemerkung.** Es gilt

$$H^1(G_K, \mathbb{Z}/p\mathbb{Z}) = \text{Hom}(G_K, \mathbb{Z}/p\mathbb{Z}).$$

D.h. die Elemente  $\neq 0$  in  $H^1(G_K, \mathbb{Z}/p\mathbb{Z})$  entsprechen surjektiven Homomorphismen

$$G_K \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Dies entspricht den folgenden Daten:

- eine zyklische Teilerweiterung  $K'|K$  von  $\overline{K}|K$  vom Grad  $p$
- ein Isomorphismus  $G(K'|K) \cong \mathbb{Z}/p\mathbb{Z}$ , d.h. ein ausgezeichneter Erzeuger von  $G(K'|K)$ .

Daher misst  $\dim_{\mathbb{F}_p} H^1(G_K, \mathbb{Z}/p\mathbb{Z})$  die maximale Anzahl linear unabhängiger zyklischer Erweiterungen vom Grad  $p$ .

**Beispiel.** Sei  $\mathbb{F}_q$ ,  $q = p^f$ , ein endlicher Körper. Dimensionszählung in der exakten Folge

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{F}_q \xrightarrow{\wp} \mathbb{F}_q \longrightarrow H^1(G_{\mathbb{F}_q}, \mathbb{Z}/p\mathbb{Z}) \longrightarrow 0$$

liefert

$$\dim_{\mathbb{F}_q} H^1(G_{\mathbb{F}_q}, \mathbb{Z}/p\mathbb{Z}) = 1,$$

d.h.  $\mathbb{F}_q$  hat genau eine zyklische Erweiterung vom Grad  $p$ . (Das wußten wir sowieso schon).

**Bemerkung.** Dies läßt sich von  $\mathbb{Z}/p\mathbb{Z}$  auf  $\mathbb{Z}/p^n\mathbb{Z}$  verallgemeinern. Die Rolle von  $\overline{K}^+$  wird dann von den „Wittvektoren“ übernommen.

### 1.3 Multiplikative Theorie – Hilberts Satz 90

**Satz 1.4.** (Hilberts Satz 90)

Sei  $L|K$  eine Galoiserweiterung mit Gruppe  $G$ . Dann gilt

$$H^1(G, L^\times) = 0.$$

*Beweis.* Wie vorher reduziert man auf den Fall  $L|K$  endlich. Sei  $a : G \rightarrow L^\times$  eine Derivation. Für  $c \in L^\times$  setzen wir

$$b = \sum_{g \in G} a(g) \cdot g(c).$$

Wegen der linearen Unabhängigkeit der Charaktere

$$L^\times \rightarrow L^\times, \quad c \mapsto gc$$

für  $g \in G$  (siehe Algebra-Vorlesung) existiert ein  $c \in L^\times$ , so dass  $b \neq 0$ . Für  $\tau \in G$  erhalten wir

$$a(\tau g) = a(\tau) \cdot \tau(a(g))$$

also

$$a(\tau)^{-1} a(\tau g) = \tau(a(g)).$$

Und daher:

$$\begin{aligned} \tau(b) &= \sum_{g \in G} \tau(a(g)) \cdot \tau g(c) \\ &= \sum_{g \in G} a(\tau)^{-1} a(\tau g) \cdot \tau g(c) \\ &= a(\tau)^{-1} b. \end{aligned}$$

$\rightsquigarrow a(\tau) = b/\tau(b) \quad \forall \tau \rightsquigarrow a$  ist innere Derivation. □

**Korollar 1.5** (klassischer Hilbertscher Satz 90). Sei  $L|K$  eine endliche Galoiserweiterung mit zyklischer Gruppe  $G$ . Sei  $\sigma$  ein Erzeuger von  $G$ . Dann ist jedes  $x \in L^\times$  mit  $N_{L|K}(x) = 1$  von der Form  $x = y/\sigma y$  für ein  $y \in L^\times$ .

*Beweis.*  $G$  zyklisch  $\implies$

$$\hat{H}^{-1}(G, L^\times) \cong H^1(G, L^\times) = 0.$$

Es folgt  $\ker(N_G) = I_G L^\times = (1 - \sigma) \cdot L^\times$ . □

Sei  $n$  eine natürliche Zahl prim zu  $\text{char}(K)$ . Dann ist das Polynom  $x^n - a$  für jedes  $a \in \bar{K}^\times$  separabel, also der Homomorphismus  $\bar{K}^\times \xrightarrow{\cdot n} \bar{K}^\times, x \mapsto x^n$ , surjektiv. Wir erhalten eine exakte Folge (die „Kummer-Folge“) von  $G_K$ -Moduln

$$0 \longrightarrow \mu_n \longrightarrow \bar{K}^\times \xrightarrow{\cdot n} \bar{K}^\times \longrightarrow 0.$$

Nach Hilberts Satz 90 folgt

**Korollar 1.6** („Kummer-Theorie“).

$$H^1(G_K, \mu_n) \cong K^\times / K^{\times n}.$$

Nun nehmen wir an, dass eine primitive  $n$ -te Einheitswurzel  $\zeta_n$  in  $K$  liegt.

Wir erhalten einen Isomorphismus von  $G_K$ -Moduln

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mu_n, \quad 1 + n\mathbb{Z} \mapsto \zeta_n,$$

und folglich einen (von der Wahl von  $\zeta$  abhängenden) Isomorphismus

$$\mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}) \cong H^1(G_K, \mu_n) = K^\times / K^{\times n}.$$

Für ein  $\bar{x} \in K^\times / K^{\times n}$  sei  $\varphi_{\bar{x}} : G_K \rightarrow \mathbb{Z}/n\mathbb{Z}$  der assoziierte Homomorphismus.  $U_{\bar{x}} := \ker(\varphi_{\bar{x}}) \subset G_K$  ist ein offener Normalteiler und es gilt

$$\begin{array}{ccc} G_K/U_{\bar{x}} & \xrightarrow{\sim} & \frac{n}{d}\mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z} \\ & & \downarrow \\ & & \mathbb{Z}/d\mathbb{Z} \end{array}$$

für einen Teiler  $d \mid n$ . Nun gilt

$$\overline{K}^{U_{\bar{x}}} = K(\sqrt[n]{x})$$

wobei  $x \in K^\times$  ein Vertreter von  $\bar{x} \in K^\times / K^{\times n}$  ist. Der zu  $\frac{n}{d} + n\mathbb{Z}$  zugehörige Erzeuger der zyklischen Gruppe  $G_K/U_{\bar{x}}$  ist der Körperautomorphismus

$$\begin{array}{ccc} K(\sqrt[n]{x}) & \longrightarrow & K(\sqrt[n]{x}), \\ \sqrt[n]{x} & \longmapsto & \zeta_n^{\frac{n}{d}} \cdot \sqrt[n]{x}. \end{array}$$

D.h: Der Körper zu  $\bar{x} \in K^\times / K^{\times n}$  ist kanonisch, der assoziierte Erzeuger der zyklischen Gruppe  $G(K(\sqrt[n]{x})|K)$  hängt von der Wahl der primitiven Einheitswurzel  $\zeta_n$  ab.

*Übungsaufgabe:* Man verifiziere diese Behauptungen und überlege sich, wie die Situation im Fall der Artin-Schreier-Theorie

$$\mathrm{Hom}(G_K, \mathbb{Z}/p\mathbb{Z}) \implies K/\wp K, \quad p = \mathrm{char}(K) > 0$$

aussieht.

## 1.4 Multiplikative Theorie – die Brauergruppe

**Definition.** Sei  $L|K$  eine Galoiserweiterung mit Gruppe  $G$ . Die Gruppe

$$\mathrm{Br}(L|K) = H^2(G, L^\times).$$

heißt **relative Brauergruppe** von  $L|K$  und

$$\mathrm{Br}(K) = \mathrm{Br}(\overline{K}|K) = H^2(G_K, \overline{K}^\times)$$

heißt die **(absolute) Brauergruppe** von  $K$ .



**Erinnerung:** Ist  $G$  eine Gruppe,  $H \subset G$  ein Normalteiler und  $A$  ein  $G$ -Modul mit  $H^i(H, A) = 0$ ,  $i = 1, \dots, n-1$ , so haben wir eine exakte Folge

$$0 \longrightarrow H^n(G/H, A^H) \xrightarrow{\text{inf}} H^n(G, A) \xrightarrow{\text{res}} H^n(H, A).$$

Ist nun  $M|L|K$  ein Turm von Galoiserweiterungen und  $A = M^\times$ , so folgt mit Hilberts Satz 90, dass die Inflation

$$\text{Br}(L|K) \longrightarrow \text{Br}(M|K)$$

injektiv ist. Wir können die Formel

$$H^2(G_K, \overline{K}^\times) = \varinjlim_{K \subseteq L \subseteq \overline{K}} H^2(G(L|K), L^\times)$$

daher in der Form

$$\text{Br}(K) = \varinjlim_{K \subseteq L \subseteq \overline{K}} \text{Br}(L|K) = \bigcup_{K \subseteq L \subseteq \overline{K}} \text{Br}(L|K)$$

schreiben. Die obige exakte Folge liest sich

$$0 \longrightarrow \text{Br}(L|K) \longrightarrow \text{Br}(K) \longrightarrow \text{Br}(L).$$

**Definition.** Man sagt, dass ein  $x \in \text{Br}(K)$  in einer Erweiterung  $L|K$  **zerfällt**, wenn das Bild von  $x$  in  $\text{Br}(L)$  gleich 0 ist.

**Bemerkungen.** Ist  $L|K$  galoissch, so besteht  $\text{Br}(L|K)$  gerade aus den  $x \in \text{Br}(K)$ , die über  $L$  zerfallen.

– Jedes  $x \in \text{Br}(K)$  zerfällt in einer endlichen Erweiterung.

**Zwischenbemerkung:** Woher die Terminologie? Es gibt einen Isomorphismus

$$\text{Br}(K) \cong \left\{ \begin{array}{l} \text{endlich-dimensionale zentrale} \\ \text{einfache } K\text{-Algebren} \end{array} \right\} / \text{gewisse Äquivalenzrelation } \sim$$

Ein  $A \in \text{Br}(K)$  zerfällt über  $L$  wenn  $A \otimes_K L \sim M_n(L)$  für ein  $n$ .

Trivialerweise gilt falls  $K = \overline{K}$ :

$$\text{Br}(K) = H^2(G_K, \overline{K}^\times) = H^2(\{1\}, \overline{K}^\times) = 0.$$

**Satz 1.7.** Sei  $K$  ein endlicher Körper. Dann gilt  $\text{Br}(K) = 0$ .

*Beweis.* Sei  $L|K$  eine endliche Erweiterung. Dann ist  $G = G(L|K)$  zyklisch. Weil  $L^\times$  endlich ist, gilt

$$h(G, L^\times) = 1;$$

also

$$\#H^2(G, L^\times) = \#H^1(G, L^\times) = 1.$$

Dies zeigt  $Br(L|K) = 0$  für jede endliche Erweiterung  $L|K$  und somit

$$Br(K) = \bigcup_L Br(L|K) = 0.$$

□

**Bemerkung.** Verschieben in die andere Richtung liefert:  $\hat{H}^0(G, L^\times) = 0$ , d.h.  $K^\times = L^{\times G} = N_G L^\times$ . Mit anderen Worten: Für jede endliche Erweiterung  $L|K$  endlicher Körper ist die Normabbildung

$$N_{L|K} : L^\times \longrightarrow K^\times$$

surjektiv.

## 1.5 Die Brauergruppe eines lokalen Körpers

Dieser Abschnitt ist angelehnt an Denis Vogels Zahlentheorievorlesung vom Sommersemester 2021. Es sei  $K$  ein nichtarchimedischer lokaler Körper. Unser Ziel ist die Konstruktion eines natürlichen Isomorphismus

$$inv_K : Br(K) \rightarrow \mathbb{Q}/\mathbb{Z},$$

der sogenannten *Invariantenabbildung*.

**Lemma 1.8.** Für eine endliche Gruppe  $G$  und ein projektives System  $(A_i)_{i \in \mathbb{N}}$  kohomologisch trivialer  $G$ -Moduln ist auch  $\varprojlim_i A_i$  kohomologisch trivial.

*Beweis.* Übung. □

**Satz 1.9.** Sei  $L/K$  eine endliche zyklische Erweiterung und  $G = \text{Gal}(L/K)$ . Dann gilt

$$|\hat{H}^n(G, L^\times)| = \begin{cases} [L : K], & n \text{ gerade} \\ 1 & n \text{ ungerade} \end{cases}$$

Insbesondere ist  $|Br(L|K)| = [L : K]$ .

*Beweis.* Nach Satz 1.10 in Kapitel 4 ist  $\hat{H}^n(G, L^\times) \cong \hat{H}^{n+2}(G, L^\times)$  für alle  $n \in \mathbb{Z}$ . Nach Hilberts Satz 90 ist  $|\hat{H}^1(G, L^\times)| = 1$ . Es reicht also zu zeigen, dass der Herbrandindex

$$h(G, L^\times) = \frac{|\hat{H}^0(G, L^\times)|}{|\hat{H}^1(G, L^\times)|}$$

gleich  $[L : K]$  ist.

Sei  $\sigma$  in Erzeuger von  $G$  und es sei  $|G| = n$  also  $G = \{1, \sigma, \dots, \sigma^{n-1}\}$ . Nach dem Satz vom primitiven Element gibt es  $a \in L^\times$  mit  $L = K(a)$ . Dann ist  $\{\sigma^i a\}_{i=1, \dots, n-1}$  eine Basis von  $L$  und insbesondere sind die  $\sigma^i a$  linear unabhängig über  $\mathcal{O}_K$ . Nach Multiplikation mit einem Element von  $K$  können wir annehmen, dass  $a \in \mathcal{O}_L$ . Wir betrachten den  $G$ -Untermodul

$$M := \bigoplus_{i=0}^{n-1} \sigma^i a \mathcal{O}_K \subseteq \mathcal{O}_L.$$

Es ist  $M \cong \mathcal{O}_K[G]$ . Außerdem ist  $M$  abgeschlossen in  $\mathcal{O}_L$  und  $(\mathcal{O}_L : M) < \infty$ , denn  $M$  und  $\mathcal{O}_L$  haben beide Rang  $n$  und  $\mathcal{O}_L$  ist endlich erzeugt. Daraus folgt, dass  $M$  offen in  $\mathcal{O}_L$  ist. Das bedeutet, dass es  $N \in \mathbb{N}$  gibt mit  $\pi_K^N \mathcal{O}_L \subseteq M$ , wobei  $\pi_K$  eine Uniformisierende von  $K$  ist.

Wir setzen für  $i \geq 0$

$$A_i := 1 + \pi_K^{N+i} M \subseteq \mathcal{O}_L^\times.$$

Die  $A_i$  bilden eine offene Umgebungsbasis der 1 in  $\mathcal{O}_L^\times$ . Wir behaupten, dass  $A_i$  ein  $G$ -Untermodul von endlichem Index ist. Um zu zeigen, dass es ein  $G$ -Untermodul ist, berechnen wir für  $x, y \in M$  und  $\sigma \in G$ :

$$\begin{aligned} (1 + \pi_K^{N+i} x)(1 + \pi_K^{N+i} y) &= 1 + \pi_K^{N+i} (x + y + \pi_K^{N+i} xy) \in A_i \\ (1 - \pi_K^{N+i} x)^{-1} &= 1 + \pi_K^{N+i} (x + \sum_{j=1}^{\infty} x^{j+1} (\pi_K^{N+i})^j) \in A_i \quad (\mathcal{O}_L \text{ vollständig}) \\ \sigma(1 + \pi_K^{N+i} x) &= 1 + \pi_K^{N+i} \sigma(x) \in A_i \end{aligned}$$

Außerdem ist  $(\mathcal{O}_L^\times : A_i) < \infty$ , da  $A_i$  offen in  $\mathcal{O}_L^\times$  und  $\mathcal{O}_L^\times$  kompakt ist.

Die  $G$ -Moduln  $A_i/A_{i+1}$  sind kohomologisch trivial, da wir folgende Isomorphismen haben ( $k$  ist der Restklassenkörper von  $K$ ):

$$\begin{aligned} A_i/A_{i+1} &\xrightarrow{\sim} M/\pi_K M \\ 1 + \pi_K^{N+i} x + A_{i+1} &\mapsto x + \pi_K M, \end{aligned}$$

$$\begin{aligned} M/\pi_K M &\xrightarrow{\sim} k[G] \\ \sigma^i a + \pi_K M &\mapsto \sigma^i. \end{aligned}$$

Mithilfe der exakten Folgen

$$0 \rightarrow A_i/A_{i+} \rightarrow A_0/A_{i+1} \rightarrow A_0/A_i \rightarrow 0$$

und Induktion schließen wir, dass  $A_0/A_i$  für alle  $i$  kohomologisch trivial ist. Wegen Lemma 1.8 ist daher  $A_0 = \varprojlim_i A_0/A_i$  kohomologisch trivial.

Wir wollen nun den Herbrandindex  $h(G, L^\times) = h(L^\times)$  bestimmen. Weil er multiplikativ in kurzen exakten Folgen ist (Satz 1.12 aus Kapitel 4), bekommen wir aus der exakten Folge

$$0 \rightarrow \mathcal{O}_L^\times \rightarrow L^\times \xrightarrow{v_L} \mathbb{Z} \rightarrow 0$$

die Gleichung

$$h(L^\times) = h(\mathcal{O}_L^\times)h(\mathbb{Z}) = h(\mathcal{O}_L)[L : K].$$

Außerdem ist  $h(\mathcal{O}_L/A_0) = 1$ , da  $A_0$  endlichen Index in  $\mathcal{O}_L$  hat (siehe Satz 1.13 aus Kapitel 4). Deshalb ist  $h(\mathcal{O}_L^\times) = h(A_0)$  und das ist 1, weil  $A_0$  kohomologisch trivial ist. Daraus folgt

$$h(G, L^\times) = [L : K].$$

□

**Lemma 1.10.** *Sei  $L/K$  eine unverzweigte Erweiterung und  $G = \text{Gal}(L/K)$ . Dann sind  $\mathcal{O}_L^\times$  und  $U_L^{(1)}$  kohomologisch triviale  $G$ -Moduln.*

*Beweis.* Für eine abgeschlossene Untergruppe  $H \subseteq G$  ist

$$H^i(H, \mathcal{O}_L^\times) = H^i(\text{Gal}(L/L^H), \mathcal{O}_L^\times) = \varprojlim_{L/M/L^H} H^i(\text{Gal}(M/L^H), \mathcal{O}_M^\times),$$

wobei der projektive Limes über alle Zwischenerweiterungen  $L/M/L^H$  läuft mit  $M/L^H$  endlich. Die analoge Aussage gilt für  $U_L^{(1)}$ . Damit haben wir uns auf den Fall endlicher Erweiterungen zurückgezogen. Wir können also im Folgenden annehmen, dass  $L/K$  endlich ist.

Sei  $\ell/k$  die zu  $L/K$  gehörige Restklassenkörpererweiterung. Wir betrachten die Filtrierung

$$\dots \subset U_L^{(2)} \subset U_L^{(1)} \subset \mathcal{O}_L^\times$$

Es ist

$$U_L^{(i-1)}/U_L^{(i)} \cong \ell^+ \cong k^+[G],$$

wobei wir für den zweiten Isomorphismus benutzt haben, dass  $L/K$  unverzweigt ist und damit  $G = \text{Gal}(L/K) = \text{Gal}(\ell/k)$ . Damit ist  $U_L^{(i-1)}/U_L^{(i)}$  induziert, also kohomologisch trivial. Per Induktion folgt mithilfe der exakten Folge

$$1 \rightarrow U_L^{(i-1)}/U_L^{(i)} \rightarrow U_L^{(1)}/U_L^{(i)} \rightarrow U_L^{(1)}/U_L^{(i-1)} \rightarrow 1,$$

dass  $U_L^{(1)}/U_L^{(i)}$  kohomologisch trivial ist für alle  $i \geq 1$  und damit nach Lemma 1.8 auch  $U_L^{(1)}$ .

Um einzusehen, dass  $\mathcal{O}_L^\times$  kohomologisch trivial ist, untersuchen wir die exakte Folge

$$1 \rightarrow U_L^{(1)} \rightarrow \mathcal{O}_L^\times \rightarrow \ell^\times \rightarrow 1.$$

Wir wissen schon, dass  $U_L^{(1)}$  kohomologisch trivial ist. Außerdem ist  $\ell^\times$  kohomologisch trivial, denn  $H^1(G, \ell^\times) = H^1(\text{Gal}(\ell/k), \ell^\times) = 0$  nach Hilberts Satz 90. Weil  $G$  zyklisch ist, reicht es daher zu zeigen, dass der Herbrandindex

$$h(G, \ell^\times) = \frac{|\hat{H}^0(G, \ell^\times)|}{|\hat{H}^1(G, \ell^\times)|}$$

trivial ist. Dies ist der Fall, weil  $\ell^\times$  endlich ist (siehe Satz 1.13 aus Kapitel 4). Das gleiche Argument zeigt, dass die Kohomologiegruppen  $H^i(H, \ell^\times)$  für jede Untergruppe  $H$  von  $G$  verschwinden. Insgesamt schließen wir mit obiger exakter Folge, dass  $\mathcal{O}_L^\times$  kohomologisch trivial ist.  $\square$

**Korollar 1.11.** *Sei  $L/K$  eine endliche unverzweigte Erweiterung. Dann ist die Norm*

$$N_{L/K} : \mathcal{O}_L^\times \rightarrow \mathcal{O}_K^\times$$

*surjektiv.*

*Beweis.* Weil  $\mathcal{O}_L^\times$  kohomologisch trivial ist, gilt

$$0 = \hat{H}^0(\text{Gal}(L/K), \mathcal{O}_L^\times) = \mathcal{O}_K^\times / N_{L/K} \mathcal{O}_L^\times.$$

$\square$

Für eine unverzweigte Erweiterung  $L/K$  mit Galoisgruppe  $G = \text{Gal}(L/K)$  und Bewertung  $v : L^\times \rightarrow \mathbb{Z}$  konstruieren wir nun die Invariantenabbildung

$$\text{inv}_{L/K} : \text{Br}(L/K) \rightarrow \mathbb{Q}/\mathbb{Z}.$$

Die exakte Folge

$$1 \rightarrow \mathcal{O}_L^\times \rightarrow L^\times \xrightarrow{v} \mathbb{Z} \rightarrow 0$$

diskreter  $G$ -Moduln gibt uns wegen der kohomologischen Trivialität von  $\mathcal{O}_L^\times$  einen Isomorphismus

$$\text{Br}(L/K) = H^2(G, L^\times) \xrightarrow{\sim} H^2(G, \mathbb{Z}).$$

Nun betrachten wir die exakte Folge

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0.$$

Weil  $\mathbb{Q}$  eindeutig teilbar ist, ist es kohomologisch trivial und wir erhalten einen Isomorphismus

$$H^2(G, \mathbb{Z}) \xleftarrow{\sim} H^1(G, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$

Weil  $L/K$  unverzweigt ist, haben wir  $G = \text{Gal}(\ell/k)$  und  $\text{Gal}(\ell/k)$  wird topologisch erzeugt vom Frobeniusautomorphismus, der  $x \in \ell$  auf  $x^q$  schickt, wobei  $q = \#k$ . Es gibt also einen eindeutig bestimmten Frobeniusautomorphismus  $\text{Frob}_{L/K}$  auf  $L$ , der den Frobeniusautomorphismus auf  $\ell$  induziert und dieser ist ein topologischer Erzeuger der Gruppe  $G$ . Wir definieren

$$\eta : H^1(G, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \rightarrow \mathbb{Q}/\mathbb{Z}, \quad \varphi \mapsto \varphi(\text{Frob}_{L/K}).$$

Diese Abbildung ist injektiv, da  $\text{Frob}_{L/K}$  die Gruppe  $G$  topologisch erzeugt und mit  $\text{Hom}(G, -)$  die stetigen Homomorphismen gemeint sind.

**Definition.** Die Komposition

$$\text{inv}_{L/K} : Br(L/K) = H^2(G, L^\times) \cong H^2(G, \mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

heißt Invariantenabbildung.

**Lemma 1.12.** Sei  $M/L/K$  ein Turm unverzweigter Erweiterungen. Dann kommutiert das Diagramm

$$\begin{array}{ccc} Br(L|K) & \xrightarrow{\text{inv}_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow \text{inf} & & \parallel \\ Br(M/K) & \xrightarrow{\text{inv}_{M/K}} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

*Beweis.* Alle in der Definition der Invariantenabbildung vorkommenden Abbildungen sind funktoriell, ebenso die Inflation.  $\square$

**Satz 1.13.** Es existiert ein eindeutig bestimmter Isomorphismus

$$\text{inv}_K : Br(K^{\text{nr}}|K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

(nämlich  $\text{inv}_K = \text{inv}_{K^{\text{nr}}/K}$ ), so dass für alle endlichen Galoiserweiterungen  $L/K$  in  $K^{\text{nr}}$  das Diagramm

$$\begin{array}{ccc} Br(L|K) & \xrightarrow{\text{inv}_{L/K}} & \frac{1}{[L:K]} \mathbb{Z}/\mathbb{Z} \\ \downarrow \text{inf} & & \downarrow \\ Br(K^{\text{nr}}|K) & \xrightarrow[\text{inv}_K]{\sim} & \mathbb{Q}/\mathbb{Z} \end{array}$$

kommutiert.

*Beweis.* Für eine endliche unverzweigte Erweiterung  $L/K$  ist die Galoisgruppe  $G = \text{Gal}(L/K)$  endlich zyklisch und wird vom Frobeniusautomorphismus  $\text{Frob}_{L/K}$  erzeugt. Wir können somit einen Homomorphismus  $f \in \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$  definieren dadurch, dass

$$f(\text{Frob}_{L/K}) = \frac{1}{[L : K]} + \mathbb{Z}.$$

Insbesondere ist das Bild von  $\text{inv}_{L/K}$  gleich  $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ . Da  $\text{inf}_{L/K}$  injektiv ist, ist  $\text{im}(\text{inv}_{L/K}) \cong \text{Br}(L|K) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \text{Hom}(\mathbb{Z}/[L : K]\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/[L : K]\mathbb{Z}$ , das heißt

$$\text{im}(\text{inv}_{L|K}) = \frac{1}{[L : K]}\mathbb{Z}/\mathbb{Z}.$$

Das Diagramm in der Aussage des Satzes kommutiert wegen Bemerkung 1.12. Außerdem ist  $\text{inv}_K$  surjektiv, da

$$\text{Br}(K^{\text{nr}}|K) = \bigcup_{K^{\text{nr}}/L/K \text{ endl.}} \text{Br}(L|K)$$

und es zu jedem  $n \in \mathbb{N}$  eine unverzweigte Erweiterung  $L/K$  vom Grad  $n$  gibt. Außerdem folgt daraus, dass  $\text{inv}_K$  durch  $\text{inv}_{L/K}$  für endliche unverzweigte Erweiterungen  $L/K$  eindeutig bestimmt ist.  $\square$

**Theorem 1.14.** *Sei  $L/K$  eine endliche separable Erweiterung. Dann existiert ein kanonischer Homomorphismus*

$$\text{res} : \text{Br}(K^{\text{nr}}|K) \rightarrow \text{Br}(L^{\text{nr}}|L),$$

so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} \text{Br}(K^{\text{nr}}|K) & \xrightarrow{\text{res}} & \text{Br}(L^{\text{nr}}|L) \\ \downarrow \text{inv}_K & & \downarrow \text{inv}_L \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot [L:K]} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Ist  $L/K$  galoissch, so kann der Kern von  $\text{res}$  kanonisch mit einer zyklischen Untergruppe der Ordnung  $[L : K]$  von  $\text{Br}(L|K)$  identifiziert werden.

*Beweis.* Wir setzen  $\Gamma_K := \text{Gal}(K^{\text{nr}}/K)$  und  $\Gamma_L := \text{Gal}(L^{\text{nr}}/L)$ . Es ist  $L^{\text{nr}} = LK^{\text{nr}}$ . Insbesondere haben wir eine natürliche Inklusion  $\varphi : \Gamma_L \hookrightarrow \Gamma_K$ . Wir betrachten das Diagramm

$$\begin{array}{ccccccc} \text{Br}(K^{\text{nr}}|K) & \xrightarrow[\sim]{v_K} & H^2(\Gamma_K, \mathbb{Z}) & \xrightarrow[\sim]{\delta^{-1}} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\eta_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow \text{res} & & \downarrow e_{L/K} \cdot \text{res} & & \downarrow e_{L/K} \cdot \text{res} & & \downarrow e_{L/K} f_{L/K} = [L:K] \\ \text{Br}(L^{\text{nr}}|L) & \xrightarrow[\sim]{v_L} & H^2(\Gamma_L, \mathbb{Z}) & \xrightarrow[\sim]{\delta^{-1}} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\eta_L} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Dieses kommutiert wegen  $v_L|_{K^{\text{nr}}} = e_{L/K}v_K$  und  $\text{Frob}_L|_{K^{\text{nr}}} = \text{Frob}_K^{f_{L/K}}$ . Daraus folgt die erste Behauptung.

Für eine endliche Galoiserweiterung  $L/K$  ist  $L^{\text{nr}}/K$  galoissch (das liegt an der Maximalität von  $L^{\text{nr}}/L$ ; für  $\sigma \in G_K$  ist  $\sigma L^{\text{nr}}$  unverzweigt über  $\sigma L = L$  und somit enthalten in  $L^{\text{nr}}$ ). Wir erhalten ein kommutatives Diagramm mit exakten Zeilen

$$\begin{array}{ccccccc}
0 & \longrightarrow & \frac{1}{[L:K]} \mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \mathbb{Q}/\mathbb{Z} \\
& & \uparrow \sim & & \uparrow \sim \text{inv}_K & & \uparrow \sim \text{inv}_L \\
0 & \longrightarrow & \ker(\text{res}) & \longrightarrow & \text{Br}(K^{\text{nr}}|K) & \xrightarrow{\text{res}} & \text{Br}(L^{\text{nr}}|L) \\
& & \downarrow & & \downarrow \text{inf} & & \parallel \\
0 & \longrightarrow & \text{Br}(L|K) & \xrightarrow{\text{inf}} & \text{Br}(L^{\text{nr}}|K) & \xrightarrow{\text{res}} & \text{Br}(L^{\text{nr}}|L),
\end{array}$$

woraus sich die zweite Behauptung ergibt.  $\square$

**Korollar 1.15.** *Sei  $L/K$  eine endliche Galoiserweiterung. Dann ist  $\text{Br}(L|K)$  zyklisch der Ordnung  $[L : K]$ .*

*Beweis.* Wir beweisen das per Induktion nach  $n = [L : K]$ . Für  $n = 1$  ist die Aussage klar und für  $n > 1$  und  $L/K$  zyklisch folgt sie aus dem Satz 1.14 und Satz 1.9. Falls  $L/K$  nicht zyklisch ist, finden wir eine nichttriviale galoissche Zwischenerweiterung  $L/M/K$ , denn die absolute Galoisgruppe eines lokalen Körpers ist auflösbar. Nach Induktionsvoraussetzung ist  $|\text{Br}(L|M)| = [L : M]$  und  $|\text{Br}(M|K)| = [M : K]$ . Außerdem haben wir die exakte Folge

$$0 \rightarrow \text{Br}(M|K) \rightarrow \text{Br}(L|K) \rightarrow \text{Br}(L|M),$$

also

$$|\text{Br}(L|K)| \leq |\text{Br}(M|K)| \cdot |\text{Br}(L|M)| = [M : K] \cdot [L : M] = [L : K].$$

Wegen Satz 1.14 enthält  $\text{Br}(L|K)$  aber eine zyklische Untergruppe der Ordnung  $[L : K]$ , muss also gleich dieser zyklischen Untergruppe sein.  $\square$

**Theorem 1.16.** *Es existiert ein eindeutig bestimmter Isomorphismus*

$$\text{inv}_K : \text{Br}(K) \rightarrow \mathbb{Q}/\mathbb{Z},$$

so dass für jede endliche separable Erweiterung  $L|K$  das Diagramm

$$\begin{array}{ccc}
\text{Br}(K) & \xrightarrow{\text{res}} & \text{Br}(L) \\
\downarrow \text{inv}_K & & \downarrow \text{inv}_L \\
\mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \mathbb{Q}/\mathbb{Z}
\end{array}$$



kommutiert und für jede endliche Galoiserweiterung  $L/K$  das Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & Br(L/K) & \xrightarrow{\inf} & Br(K) & \xrightarrow{res} & Br(L) \\ & & \downarrow \text{inv}_{L/K} & & \downarrow \text{inv}_K & & \downarrow \text{inv}_L \\ 0 & \longrightarrow & \frac{1}{[L:K]} \mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \mathbb{Q}/\mathbb{Z} \end{array}$$

kommutiert.

*Beweis.* Wegen Korollar 1.15 ist für eine endliche galoissche Erweiterung  $L/K$  der Kern der Restriktion

$$res : Br(K^{\text{nr}}|K) \rightarrow Br(L^{\text{nr}}|L),$$

gleich  $Br(L/K)$  (siehe Theorem 1.14). Das heißt wir können  $Br(L/K)$  kanonisch als Untergruppe von  $Br(K^{\text{nr}}|K)$  auffassen. Außerdem ist

$$Br(K) = \bigcup_{L/K \text{ endl. gal.}} Br(L|K),$$

das heißt  $\inf : Br(K^{\text{nr}}|K) \rightarrow Br(K)$  ist ein Isomorphismus. Wir können also in Satz 1.13 die maximal unverzweigte Erweiterung  $K^{\text{nr}}$  von  $K$  durch einen separablen Abschluss  $K^{\text{sep}}$  von  $K$  ersetzen. Dann folgt die Behauptung.  $\square$

**Korollar 1.17.** Sei  $L/K$  endlich separabel. Dann kommutiert das Diagramm

$$\begin{array}{ccc} Br(L) & \xrightarrow{cor} & Br(K) \\ \text{inv}_L \downarrow & & \downarrow \text{inv}_K \\ \mathbb{Q}/\mathbb{Z} & \xlongequal{\quad} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

*Beweis.* Betrachte das Diagramm

$$\begin{array}{ccccc} Br(K) & \xrightarrow{res} & Br(L) & \xrightarrow{cor} & Br(K) \\ \downarrow \text{inv}_K & & \downarrow \text{inv}_L & & \downarrow \text{inv}_K \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Q}/\mathbb{Z}, \end{array}$$

wobei  $\varphi$  so gewählt ist, dass das Diagramm kommutiert. Da  $cor \circ res = [L : K]$ , muss  $\varphi$  die Identität sein.  $\square$

**Korollar 1.18.** Sei  $M/L/K$  ein Turm endlicher Galoiserweiterungen. Dann kommutiert das Diagramm

$$\begin{array}{ccccc} Br(L|K) & \xhookrightarrow{\inf} & Br(M|K) & \xrightarrow{res} & Br(M|L) \\ \downarrow \text{inv}_{L/K} & & \downarrow \text{inv}_{M/K} & & \downarrow \text{inv}_{M/L} \\ \frac{1}{[L:K]} \mathbb{Z}/\mathbb{Z} & \hookrightarrow & \frac{1}{[M:K]} \mathbb{Z}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \frac{1}{[M:L]} \mathbb{Z}/\mathbb{Z}. \end{array}$$

*Beweis.* Das rechte Quadrat kommutiert wegen Theorem 1.16 und das linke wegen Bemerkung 1.12.  $\square$

**Definition.** Sei  $L/K$  eine endliche Galoiserweiterung. Das Element

$$\text{inv}_{L/K}^{-1}\left(\frac{1}{[L:K]} + \mathbb{Z}\right) \in \text{Br}(L|K)$$

heißt Fundamentalklasse von  $L/K$ .

# Algebraische Zahlentheorie II

## Sommersemester 2022

Dr. Katharina Hübner

basierend auf Alexander Schmidts AZT2-Skript von 2014

### Inhaltsverzeichnis

<b>1</b>	<b>Klassenformationen</b>	<b>1</b>
1.1	Dualität für endliche Gruppen . . . . .	1
1.2	Klassenmoduln . . . . .	3
1.3	Nakayama-Tate Dualität . . . . .	7
1.4	Klassenformationen . . . . .	10

## 1 Klassenformationen

### 1.1 Dualität für endliche Gruppen

Erinnerung:

- $H^n(G, A^*) \cong H_n(G, A)^*$
- $\hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) = \ker(N_G)/I_G\mathbb{Q}/\mathbb{Z} = \frac{1}{\#G} \cdot \mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ .

**Lemma 1.1.** Sei  $G$  eine endliche Gruppe und sei  $A$  ein  $G$ -Modul. Die durch die Paarung  $A^* \times A \rightarrow \mathbb{Q}/\mathbb{Z}$  induzierte Cup-Produktpaarung

$$\hat{H}^i(G, A^*) \times \hat{H}^{-i-1}(G, A) \longrightarrow H^{-1}(G, \mathbb{Q}/\mathbb{Z}) = \frac{1}{\#G} \mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$$

induziert einen Isomorphismus

$$\hat{H}^i(G, A^*) \xrightarrow{\sim} \hat{H}^{-i-1}(G, A)^*$$

für alle  $i \in \mathbb{Z}$ .

*Beweis.* Sei zunächst  $i = 0$ . Ein Homomorphismus  $f : A \rightarrow \mathbb{Q}/\mathbb{Z}$  ist ein  $G$ -Homomorphismus, d.h.  $f \in H^0(G, A^*)$ , gdw.  $f(I_G A) = 0$ . Daher ist die Abbildung

$$H^0(G, A^*) \longrightarrow H_0(G, A)^*$$

die einem  $G$ -Homomorphismus  $f : A \rightarrow \mathbb{Q}/\mathbb{Z}$  den assoziierten Homomorphismus  $\tilde{f} : A/I_G A \rightarrow \mathbb{Q}/\mathbb{Z}$  zuordnet, ein Isomorphismus. (Das hatten wir schon beim Beweis von  $H^n(G, A)^* \cong H_n(G, A)^*$  gesehen).

Ist  $f \in N_G A^*$ , d.h.  $f = \sum_{g \in G} gF$  für ein  $F \in A^*$ , dann gilt für  $a \in N_G A$ :

$$f(a) = \sum_{g \in G} g \cdot F(a) = \sum_{g \in G} F(g^{-1}a) = F(N_G a) = 0.$$

Daher faktorisiert der Homomorphismus

$$H^0(G, A^*) \longrightarrow H_0(G, A)^* = (A/I_G A)^* \twoheadrightarrow (N_G A/I_G A)^*$$

zu einem Homomorphismus

$$\begin{array}{ccc} \varphi : & A^* G / N_G A^* & \twoheadrightarrow & (N_G A / I_G A)^* \\ & \parallel & & \parallel \\ & \hat{H}^0(G, A^*) & & \hat{H}^{-1}(G, A)^*. \end{array}$$

Nun habe  $f \in A^{*G}$  triviales Bild, d.h.  $f(N_G A) = 0$ . Da

$$N_G : A/N_G A \xrightarrow{\sim} N_G A$$

ein Isomorphismus ist, existiert ein Homomorphismus  $\tilde{f} : N_G A \rightarrow \mathbb{Q}/\mathbb{Z}$  mit  $f(a) = \tilde{f}(N_G a)$  für alle  $a \in A$ . Da  $\mathbb{Q}/\mathbb{Z}$   $\mathbb{Z}$ -injektiv ist, können wir  $\tilde{f}$  zu einem Homomorphismus  $\tilde{f} : A \rightarrow \mathbb{Q}/\mathbb{Z}$  fortsetzen und es gilt  $f = \tilde{f} \circ N_G$ . Hieraus folgt aber  $f = N_G \tilde{f}$  weil für alle  $a \in A$  gilt

$$N_G \tilde{f}(a) = \sum_{g \in G} \tilde{f}(g^{-1}a) = \tilde{f}(N_G a) = f(a).$$

Dies zeigt die Injektivität von  $\varphi$  und damit die Behauptung für  $i = 0$  (dass der Isomorphismus vom Cup-Produkt induziert ist, lassen wir hier weg). Der allgemeine Fall folgt durch Dimensionsverschiebung mit Hilfe von

$$\begin{array}{ccccc} \hat{H}^i(G, \text{Hom}(A, \mathbb{Q}/\mathbb{Z})) & \times & \hat{H}^{-i-1}(G, A) & \xrightarrow{\cup} & \hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \\ \delta^i \uparrow \wr & & \delta^i \downarrow \wr & & (-1)^{\frac{i(i+1)}{2}} \downarrow \\ \hat{H}^0(G, \text{Hom}(A, \mathbb{Q}/\mathbb{Z})_i) & \times & \hat{H}^{-i-1}(G, A_{-i}) & \longrightarrow & \hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \end{array}$$

unter Beachtung von

$$\text{Hom}(A, \mathbb{Q}/\mathbb{Z})_i = \text{Hom}(A_{-i}, \mathbb{Q}/\mathbb{Z})$$

□

**Lemma 1.2.** Ist  $G$  eine endliche Gruppe und  $A$  ein  $\mathbb{Z}$ -freier  $G$ -Modul, so induziert für alle  $i \in \mathbb{Z}$  die Cup-Produktpaarung

$$\hat{H}^i(G, \text{Hom}(A, \mathbb{Z})) \times \hat{H}^{-i}(G, A) \xrightarrow{\cup} \hat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/\#G\mathbb{Z}$$

einen Isomorphismus

$$\hat{H}^i(G, \text{Hom}(A, \mathbb{Z})) \cong \hat{H}^{-i}(G, A)^*.$$

*Beweis.* Da  $A$   $\mathbb{Z}$ -frei ist, ist die Folge

$$0 \longrightarrow \text{Hom}(A, \mathbb{Z}) \longrightarrow \text{Hom}(A, \mathbb{Q}) \longrightarrow \text{Hom}(A, \mathbb{Q}/\mathbb{Z}) \longrightarrow 0$$

exakt. Nun ist  $\text{Hom}(A, \mathbb{Q})$  eindeutig teilbar, also kohomologisch trivial und wir erhalten das kommutative Diagramm

$$\begin{array}{ccccc} \hat{H}^{i-1}(G, \text{Hom}(A, \mathbb{Q}/\mathbb{Z})) & \times & \hat{H}^{-i}(G, A) & \xrightarrow{\cup} & \hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \\ \downarrow \delta & & \downarrow \text{id} & & \downarrow \delta \\ \hat{H}^{-i}(G, \text{Hom}(A, \mathbb{Z})) & \times & \hat{H}^{-i}(G, A) & \xrightarrow{\cup} & \hat{H}^0(G, \mathbb{Z}) \end{array}$$

wobei die vertikalen Abbildungen Isomorphismen sind. Daher folgt die Aussage aus 1.1.  $\square$

## 1.2 Klassenmoduln

**Definition.** Sei  $G$  eine endliche Gruppe. Ein  $G$ -Modul  $C$  heißt **Klassenmodul**, wenn für jede Untergruppe  $H$  von  $G$  gilt:

- (i)  $H^1(H, C) = 0$
- (ii)  $H^2(H, C)$  ist zyklisch von Ordnung  $\#H$ .

Ein Erzeuger  $\gamma$  von  $H^2(G, C)$  heißt **Fundamentalklasse**.

**Bemerkung.**  $C$  ist offenbar auch Klassenmodul für jede Untergruppe  $H \subset G$ . Ist  $\gamma$  ein Erzeuger von  $H^2(G, C)$ , so ist  $\gamma_H = \text{res}_H^G \gamma$  ein Erzeuger von  $H^2(H, C)$ . Grund: Wegen  $\text{cor} \gamma_H = \text{cor} \cdot \text{res} \gamma = (G : H) \cdot \gamma$  ist die Ordnung von  $\gamma_H$  durch  $\#H$  teilbar.

**Beispiel.** 1) Ist  $G$  zyklisch, so ist  $C = \mathbb{Z}$  ein Klassenmodul. In der Tat gilt

$$H^1(G, \mathbb{Z}) = \text{Hom}(G, \mathbb{Z}) = 0$$

und

$$H^2(G, \mathbb{Z}) \cong \hat{H}^0(G, \mathbb{Z}) \cong \mathbb{Z}/\#G\mathbb{Z}.$$

2) Sei  $L|K$  eine endliche Galoiserweiterung lokaler Körper mit Gruppe  $G$ . Dann ist  $L^\times$  ein Klassenmodul.

Grund:

$$\begin{aligned} H^1(G, L^\times) &= 0 && (\text{Hilberts Satz 90}) \\ H^2(G, L^\times) &= \text{Br}(L|K) \cong \mathbb{Z}/[L : K]\mathbb{Z}. \end{aligned}$$

**Bemerkung.** Im Beispiel 1 haben wir gezeigt: Ist  $\gamma \in H^2(G, \mathbb{Z})$  eine Fundamentalklasse, so ist das Cup-Produkt

$$\gamma \cup - : \hat{H}^n(G, A) \longrightarrow \hat{H}^{n+2}(G, A)$$

ein Isomorphismus für jeden  $G$ -Modul  $A$  und alle  $n \in \mathbb{Z}$ . Dies wollen wir auf beliebige Klassenmoduln verallgemeinern.

Wir erinnern uns zunächst an das kommutative Diagramm im Beweis von Satz 1.13 in Kapitel 3.2 ( $H^1 = \text{Der}/\text{IDer}$ ) und erweitern es ein wenig:

$$\begin{array}{ccc} C^0(G, A) & \xrightarrow[\varphi \mapsto \varphi(1)]{\sim} & A = \mathcal{C}^0(G, A) \\ d^1 \downarrow & & \downarrow \partial^1 \\ C^1(G, A) & \xrightarrow[\varphi \mapsto (g \mapsto \varphi(1, g))]{\sim} & \text{Abb}(G, A) = \mathcal{C}^1(G, A) \\ d^2 \downarrow & & \downarrow \partial^2 \\ C^2(G, A) & \xrightarrow[\varphi \mapsto ((g_1, g_2) \mapsto \varphi(1, g_1, g_2))]{\sim} & \text{Abb}(G^2, A) = \mathcal{C}^2(G, A) \\ d^3 \downarrow & & \downarrow \partial^3 \\ C^3(G, A) & \xrightarrow[\varphi \mapsto ((g_1, g_2, g_3) \mapsto \varphi(1, g_1, g_2, g_3))]{\sim} & \text{Abb}(G^3, A) = \mathcal{C}^3(G, A), \end{array}$$

wobei:

- $\partial^1(a) = (g \mapsto ga - a)$
- $\partial^2(x) = ((g_1, g_2) \mapsto g_1x(g_2) - x(g_1g_2) + x(g_1))$

und (einfach nachrechnen)

$$\partial^3(x) = (g_1, g_2, g_3) \mapsto g_1x(g_2, g_3) - x(g_1g_2, g_3) + x(g_1, g_2g_3) - x(g_1, g_2)$$

**Bemerkung.** Die Elemente in  $\mathcal{C}^\bullet(G, A)$  heißen **inhomogene Koketten**.

**Definition.** Sei  $G$  eine endliche Gruppe und  $C$  ein  $G$ -Modul. Sei  $\gamma \in H^2(G, C)$ . Der **Zerfallungsmodul**  $C(\gamma)$  ist wie folgt definiert:

Sei  $B = \bigoplus_{g \neq 1} \mathbb{Z}b_g$  die freie abelsche Gruppe mit Basis  $b_g$ ,  $g \in G \setminus \{1\}$ . Wir setzen  $C(\gamma) = C \oplus B$  und lassen  $G$  wie folgt operieren: Wähle ein  $c \in \mathcal{C}^2(G, A)$ , das  $\gamma$  repräsentiert. Wir setzen  $b_1 = c(1, 1)$  und definieren

$$\sigma b_\tau = b_{\sigma\tau} - b_\sigma + c(\sigma, \tau).$$

Dies ist in der Tat eine  $G$ -Wirkung.

Nachzurechnen sind:  $1b_\tau = b_\tau$  und  $(\rho\sigma)(b_\tau) = \rho(\sigma b_\tau)$ .

Dies folgt aus  $\partial^3(c) = 0$ , d.h. aus der Relation

$$\rho c(\sigma, \tau) - c(\rho\sigma, \tau) + c(\rho, \tau\sigma) - c(\rho, \sigma) = 0.$$

**Erklärung:** Wir haben die natürliche Inklusion  $i : C \rightarrow C(\gamma)$ . Betrachtet man die Abbildung:  $b : G \rightarrow C(\gamma)$ ,  $\sigma \mapsto b_\sigma$ ,  $b \in \text{Abb}(G, C(\gamma)) = \mathcal{C}^1(G, C(\gamma))$  so gilt  $\partial^2 b = i(c) \in \mathcal{C}^2(G, C(\gamma))$ . D.h.  $c$  wird zum Korand in  $C(\gamma)$ , also  $H^2(G, C) \rightarrow H^2(G, C(\gamma))$  schickt  $\gamma$  auf Null, d.h.  $\gamma$  „zerfällt“.

**Bemerkung.** Eine andere Wahl der Repräsentanten  $c$  von  $\gamma$  liefert einen isomorphen  $G$ -Modul.

Wir erhalten eine exakte Folge

$$0 \longrightarrow C \xrightarrow{i} C(\gamma) \xrightarrow{\varphi} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

in der  $\varphi$  durch  $\varphi(c) = 0$  für  $c \in C$  und  $\varphi(b_\sigma) = \sigma - 1$ ,  $\sigma \neq 1$ , definiert ist. Diese 4er Folge kann man in zwei 3-er Folgen spalten

$$\begin{aligned} 0 \longrightarrow C &\xrightarrow{i} C(\gamma) \xrightarrow{\varphi} I_G \longrightarrow 0, \\ 0 \longrightarrow I_G &\longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0. \end{aligned}$$

**Bemerkung.** Die obere Folge entspricht gerade dem Element

$$\gamma \in H^2(G, C) = \text{Ext}_{\mathbb{Z}[G]}^2(\mathbb{Z}, C) = \text{Ext}_{\mathbb{Z}[G]}^1(I_G, C).$$

unter der Identifikation zwischen Elementen in  $\text{Ext}^1$  und Isomorphieklassen von Erweiterungen.

Für jede Untergruppe  $H \subset G$  liefern die zwei exakten Folgen einen Homomorphismus

$$\delta^2 : \hat{H}^n(H, \mathbb{Z}) \longrightarrow \hat{H}^{n+2}(H, C)$$

für alle  $n \in \mathbb{Z}$ .

**Satz 1.3.** Sei  $G$  eine endliche Gruppe,  $C$  ein  $G$ -Modul und  $\gamma \in H^2(G, C)$ . Dann ist für jedes  $n \in \mathbb{Z}$  und jede Untergruppe  $H \subset G$  die Abbildung

$$\delta^2 : \hat{H}^n(H, \mathbb{Z}) \longrightarrow \hat{H}^{n+2}(H, C)$$

gegeben durch  $\beta \mapsto \gamma_H \cup \beta$ , wobei  $\gamma_H = \text{res}_H^G \gamma \in H^2(H, C)$ . Die folgenden Bedingungen sind äquivalent

- (i)  $C(\gamma)$  ist ein kohomologisch trivialer  $G$ -Modul.
- (ii)  $C$  ist ein Klassenmodul mit Fundamentalklasse  $\gamma$ .
- (iii)  $\delta^2$  ist ein Isomorphismus für alle  $H$  und alle  $n \in \mathbb{Z}$ .

**Bemerkung.** Ist  $C$  ein Klassenmodul für  $G$ , dann haben wir nach dem obigen Satz Isomorphismen

$$\begin{aligned} (\delta^2)^{-1} : H^2(H, C) &\xrightarrow{\sim} \frac{1}{\#H} \mathbb{Z} / \mathbb{Z} \\ \gamma_H &\longmapsto \frac{1}{\#H} \mathbb{Z} + \mathbb{Z}. \end{aligned}$$

Diese heißen die **Invariantenabbildungen** (bzgl.  $\gamma$ ) und werden mit  $\text{inv}$  bezeichnet.

*Beweis.* Die Abbildung  $\delta^2$  entsteht aus den exakten Folgen

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \quad (1)$$

$$0 \longrightarrow C \xrightarrow{i} C(\gamma) \xrightarrow{\varphi} I_G \longrightarrow 0 \quad (2)$$

und ist das Kompositum der Abbildung

$$\hat{H}^n(G, \mathbb{Z}) \xrightarrow[\sim]{\delta_1} \hat{H}^{n+1}(G, I_G) \xrightarrow{\delta_2} \hat{H}^{n+2}(G, C), \quad (3)$$

wobei  $\delta_1$  stets ein Isomorphismus ist. Für  $n = 0$  haben wir die Abbildung

$$\mathbb{Z}/\#H\mathbb{Z} = \hat{H}^0(H, \mathbb{Z}) \xrightarrow[\sim]{\delta_1} H^1(H, I_G) \xrightarrow{\delta_2} H^2(H, C) \quad (4)$$

*Behauptung:* Für  $\bar{1} = 1 + \#H\mathbb{Z}$  gilt

$$\delta_2 \delta_1 \bar{1} = \gamma_H = \text{res}_H^G \gamma. \quad (5)$$

*Beweis der Behauptung.* Ein Urbild des inhomogenen 0-Kozykels  $1 \in \mathcal{Z}^0(H, \mathbb{Z})$  in  $\mathcal{C}^0(H, \mathbb{Z}[G])$  ist  $1 \in \mathbb{Z}[G]$  und  $\delta_1 \bar{1} \in H^1(H, I_G)$  ist durch den inhomogenen 1-Kozykel  $(\partial 1)(\sigma) = \sigma - 1$  repräsentiert (eine Derivation  $H \rightarrow I_G$ ). Ein Urbild von  $\partial 1$  in  $\mathcal{C}^1(H, C(\gamma))$  ist durch die Abbildung

$$x : H \rightarrow C(\gamma), \quad x(\sigma) = b_\sigma$$

gegeben und deshalb wird  $\delta_2 \delta_1(\bar{1})$  durch die Abbildung

$$\begin{aligned} \partial(x) : H^2 &\longrightarrow C \\ \partial(x)(\sigma, \tau) &= \sigma b_\tau - b_{\sigma\tau} + b_\sigma = c(\sigma, \tau) \end{aligned}$$

repräsentiert. Dies zeigt die Behauptung.

Nun sei  $\beta \in \hat{H}^n(H, \mathbb{Z})$  wobei  $n \in \mathbb{Z}$  beliebig ist. Wendet man nun Satz 1.21 aus Kapitel 3.2 (Verhalten von  $\cup$  unter Randabbildung, die Variante für Tate-Kohomologie) auf die exakten Folgen (1) und (2) an, erhält man

$$\delta^2 \beta = \delta_2 \delta_1(\bar{1} \cup \beta) = \delta_2(\delta_1 \bar{1} \cup \beta) = \delta_2 \delta_1 \bar{1} \cup \beta = \gamma_H \cup \beta.$$

Dies zeigt die erste Aussage.

Nun gilt

$$\hat{H}^i(H, I_G) \cong \hat{H}^{i-1}(H, \mathbb{Z}) = 0 \quad \text{für} \quad i = 0, 2.$$

Daher liefert (2) die exakte Folge

$$\begin{aligned} 0 &\longrightarrow H^1(H, C) \longrightarrow H^1(H, C(\gamma)) \longrightarrow H^1(H, I_G) \\ &\xrightarrow{\delta_2} H^2(H, C) \longrightarrow H^2(H, C(\gamma)) \longrightarrow 0. \end{aligned}$$



Ist nun  $C(\gamma)$  kohomologisch trivial, so folgt  $H^1(H, C) = 0$  und das Kompositum

$$\mathbb{Z}/\#H\mathbb{Z} = \hat{H}^0(H, \mathbb{Z}) \xrightarrow{\delta_1} H^1(H, I_G) \xrightarrow{\delta_2} H^2(H, C)$$

ist ein Isomorphismus, der  $\bar{1}$  auf  $\gamma_H$  schickt. Daher ist  $C$  ein Klassenmodul mit Fundamentalklasse  $\gamma$ , d.h. (i)  $\Rightarrow$  (ii) ist gezeigt. Gilt umgekehrt (ii), so ist  $H^1(H, C) = 0$  und  $H^1(H, I_G) \xrightarrow{\delta} H^2(H, C)$  ist ein Isomorphismus. Wir erhalten

$$H^n(H, C(\gamma)) = 0 \quad \text{für } n = 1, 2$$

und jede Untergruppe  $H$  von  $G$  (insbesondere für jede  $p$ -Sylowgruppe). Nach 3.4.7 ist  $C(\gamma)$  kohomologisch trivial. Wir erhalten (i)  $\iff$  (ii). Die Äquivalenz (i)  $\iff$  (iii) folgt aus (3) und der langen exakten Folge

$$\begin{aligned} \cdots &\longrightarrow \hat{H}^n(H, C) \longrightarrow \hat{H}^n(H, C(\gamma)) \longrightarrow \hat{H}^n(H, I_G) \\ &\xrightarrow{\delta} \hat{H}^{n+1}(H, C) \longrightarrow \hat{H}^{n+1}(H, C(\gamma)) \longrightarrow \cdots \end{aligned}$$

□

### 1.3 Nakayama-Tate Dualität

**Satz 1.4.** (Nakayama-Tate). Sei  $G$  eine endliche Gruppe,  $C$  ein Klassenmodul und  $\gamma \in H^2(G, C)$  eine Fundamentalklasse. Sei  $A$  ein endlich erzeugter  $\mathbb{Z}$ -freier  $G$ -Modul. Dann induziert für alle  $i \in \mathbb{Z}$  das Cup-Produkt

$$\hat{H}^i(G, \text{Hom}(A, C)) \times \hat{H}^{2-i}(G, A) \xrightarrow{\cup} H^2(G, C) \cong \frac{1}{\#G} \mathbb{Z}/\mathbb{Z},$$

wobei  $H^2(G, C) \cong \frac{1}{\#G} \mathbb{Z}/\mathbb{Z}$  durch  $\gamma \mapsto \frac{1}{\#G} + \mathbb{Z}$  gegeben ist, einen Isomorphismus

$$\hat{H}^i(G, \text{Hom}(A, C)) \xrightarrow{\sim} \hat{H}^{2-i}(G, A)^*$$

endlicher abelscher Gruppen.

*Beweis.* Sei

$$0 \longrightarrow C \longrightarrow C(\gamma) \longrightarrow I_G \longrightarrow 0$$

die exakte Folge aus dem Beweis von 1.3. Da  $A$   $\mathbb{Z}$ -frei ist, sind die Folgen

$$\begin{aligned} 0 &\longrightarrow \text{Hom}(A, C) \longrightarrow \text{Hom}(A, C(\gamma)) \longrightarrow \text{Hom}(A, I_G) \longrightarrow 0 \\ 0 &\longrightarrow \text{Hom}(A, I_G) \longrightarrow \text{Hom}(A, \mathbb{Z}[G]) \longrightarrow \text{Hom}(A, \mathbb{Z}) \longrightarrow 0 \end{aligned}$$

exakt und die  $G$ -Moduln in der Mitte sind jeweils kohomologisch trivial (nach Korollar 1.21 in Kapitel 4). Wir erhalten somit für alle  $i \in \mathbb{Z}$  ein kommutatives

Diagramm:

$$\begin{array}{ccccc}
\hat{H}^{i-2}(G, \text{Hom}(A, \mathbb{Z})) & \times & \hat{H}^{2-i}(G, A) & \xrightarrow{\cup} & \hat{H}^0(G, \mathbb{Z}) \\
\delta \downarrow & & \downarrow \text{id} & & \downarrow \delta \\
\hat{H}^{i-1}(G, \text{Hom}(A, I_G)) & \times & \hat{H}^{2-i}(G, A) & \longrightarrow & \hat{H}^1(G, I_G) \\
\delta \downarrow & & \downarrow \text{id} & & \downarrow \delta \\
\hat{H}^i(G, \text{Hom}(A, C)) & \times & \hat{H}^{2-i}(G, A) & \longrightarrow & \hat{H}^2(G, C)
\end{array}$$

in dem die vertikalen Abbildungen Isomorphismen sind. Nach 1.2 erhalten wir den Isomorphismus

$$\hat{H}^i(G, \text{Hom}(A, C)) \xrightarrow{\sim} \hat{H}^{2-i}(G, A)^*.$$

Schließlich ist  $A$  endlich erzeugt und  $G$  endlich. Daher sind die Kohomologiegruppen  $\hat{H}^i(G, A)$  endlich erzeugte abelsche Gruppen die durch  $\#G$  annulliert werden, also endlich.  $\square$

**Bemerkung.** Für eine Untergruppe  $H \subset G$  haben wir zwei kommutative Diagramme

$$\begin{array}{ccc}
\hat{H}^i(H, \text{Hom}(A, C)) & \xrightarrow{\sim} & \hat{H}^{2-i}(H, A)^* \\
\text{res} \uparrow \downarrow \text{cor} & & \text{cor}^* \uparrow \downarrow \text{res}^* \\
\hat{H}^i(G, \text{Hom}(A, C)) & \xrightarrow{\sim} & \hat{H}^{2-i}(G, A)
\end{array}$$

wobei  $\text{cor}^*$  und  $\text{res}^*$  die zu  $\text{cor}$  und  $\text{res}$  dualen Abbildungen sind. Die Kommutativität folgt aus  $\text{cor}(\alpha \cup \text{res}\beta) = \text{cor}(\alpha) \cup \beta$  (Übungsaufgabe).

Setzt man in 1.4  $i = 0$  und  $A = \mathbb{Z}$  und erinnert sich an

$$H^2(G, \mathbb{Z})^* \cong H^1(G, \mathbb{Q}/\mathbb{Z})^* \cong G^{\text{ab}},$$

erhält man

**Satz 1.5.** Ist  $C$  ein Klassenmodul für die endliche Gruppe  $G$ , so erhält man einen Isomorphismus

$$\rho = \rho_G : G^{\text{ab}} \xrightarrow{\sim} C^G / N_G C.$$

Dieser heißt **Nakayama-Abbildung**, hängt von der Wahl einer Fundamentalklasse  $\gamma \in H^2(G, C)$  ab und es gilt

$$\chi(\sigma) = \text{inv}(\rho(\sigma) \cup \delta\chi)$$

für jedes

$$\chi \in \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G, \mathbb{Z}).$$

*Beweis.* Die Existenz des Isomorphismus  $\rho$  folgt direkt aus Satz 1.4. Um die Formel  $\chi(\sigma) = \text{inv}(\rho(\sigma) \cup \delta\chi)$  zu zeigen erinnern wir uns an die Konstruktion von  $\rho$ .

$$\begin{array}{ccccccc}
 & & & \rho & & & \\
 & \nearrow & & \searrow & & & \\
 \hat{H}^0(G, C) & \xrightarrow{\sim} & H^2(G, \mathbb{Z})^* & \xrightarrow[\delta^*]{\sim} & H^1(G, \mathbb{Q}/\mathbb{Z})^* & \xleftarrow{\sim} & G^{\text{ab}} \\
 c \longmapsto & (\alpha \mapsto \text{inv}(\alpha \cup c)) & \longmapsto & (\chi \mapsto \text{inv}(\delta\chi \cup c)) & & & \\
 & & & & (\chi \mapsto \chi(\sigma)) & \longleftarrow & \sigma
 \end{array}$$

Ist nun  $c = \rho(\sigma)$ , erhalten wir  $\chi(\sigma) = \text{inv}(\rho(\sigma) \cup \delta\chi)$  für alle  $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$ .  $\square$

**Bemerkung.** Wir können die Formel  $\chi(\sigma) = \text{inv}(\rho(\sigma) \cup \delta\chi)$  auch anders ausdrücken, indem wir sagen, dass das Diagramm

$$\begin{array}{ccccc}
 G^{\text{ab}} & \times & H^1(G, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\
 \uparrow \text{rec} & & \downarrow \delta & & \uparrow \text{inv} \\
 \hat{H}^0(G, C) & \times & H^2(G, \mathbb{Z}) & \xrightarrow{\cup} & H^2(G, C).
 \end{array}$$

kommutiert, wobei wir uns daran erinnern, dass der Reziprozitätshomomorphismus invers zu  $\rho$  ist.

**Definition.** Die Komposition

$$\text{rec}_G : C^G \twoheadrightarrow C^G / N_G C \xrightarrow[\sim]{\rho^{-1}} G^{\text{ab}}$$

heißt **Reziprozitätshomomorphismus**. Ein alternativer Name ist „Normenrestsymbol“ und für  $\alpha \in C^G$  schreibt man auch  $(\alpha, G) := \text{rec}(\alpha)$ . Der Name rührt daher, dass  $(\alpha, G)$  dann und nur dann trivial ist, wenn  $\alpha \in N_G C$  gilt.

Schließlich erinnern wir uns an den Isomorphismus

$$\Phi : G^{\text{ab}} \xrightarrow{\sim} H_1(G, \mathbb{Z}) \xrightarrow{\sim} \hat{H}^{-2}(G, \mathbb{Z}).$$

Zusammen mit dem Isomorphismus aus 1.2 erhalten wir den Isomorphismus

$$\rho' : G^{\text{ab}} \xrightarrow{\sim} \hat{H}^{-2}(G, \mathbb{Z}) \xrightarrow{\gamma \cup -} \hat{H}^0(G, C) \cong C^G / N_G C,$$

der in der Literatur oft zur Definition der Nakayama-Abbildung herangezogen wird.

**Satz 1.6.**  $\rho = \rho'$ .

*Beweis.* Wir betrachten das Diagramm

$$\begin{array}{ccccc}
G^{\text{ab}} & \times & H^1(G, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\cup} & \frac{1}{\#G} \mathbb{Z}/\mathbb{Z} \\
\text{rec} \uparrow & & \downarrow \delta & & \uparrow \text{inv} \\
\hat{H}^0(G, C) & \times & H^2(G, \mathbb{Z}) & \xrightarrow{\cup} & H^2(G, C) \\
\gamma \cup \uparrow & & \downarrow \text{id} & & \uparrow \gamma \cup \\
\hat{H}^{-2}(G, \mathbb{Z}) & \times & \hat{H}^2(G, \mathbb{Z}) & \xrightarrow{\cup} & \frac{1}{\#G} \mathbb{Z}/\mathbb{Z}
\end{array}$$

Für  $\rho = \rho'$  ist zu zeigen, dass für jedes  $\sigma \in G^{\text{ab}}$  und jedes  $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$  gilt

$$\text{inv}(\gamma \cup \Phi(\sigma) \cup \delta\chi) = \chi(\sigma)$$

Nach Definition von  $\text{inv}$  ist die Komposition der rechten vertikalen Pfeile die Identität. Wir erhalten

$$\text{inv}(\gamma \cup \Phi(\sigma) \cup \delta\chi) = \Phi(\sigma) \cup \delta\chi.$$

Dass dies gleich  $\chi(\sigma)$  ist, ist eine Übungsaufgabe. □

## 1.4 Klassenformationen

Sei  $G$  eine proendliche Gruppe. Offene Untergruppen bezeichnen wir mit den Buchstaben  $U, V, W$ .

**Definition.** Ein **Formationsmodul** für  $G$  ist ein diskreter  $G$ -Modul  $C$  zusammen mit einem System von Isomorphismen

$$\text{inv}_{U/V} : H^2(U/V, C^V) \xrightarrow{\sim} \frac{1}{(U:V)} \mathbb{Z}/\mathbb{Z}$$

für jedes Paar  $V \subset U$  offener Untergruppen mit  $V$  Normalteiler in  $U$ , so dass die folgenden Bedingungen gelten

- (i)  $H^1(U/V, C^V) = 0$
- (ii) Für offene Normalteiler  $W \subset V$  von  $U$  kommutiert das Diagramm

$$\begin{array}{ccccc}
H^2(U/V, C^V) & \xrightarrow{\text{inf}} & H^2(U/W, C^W) & \xrightarrow{\text{res}} & H^2(V/W, C^W) \\
\wr \downarrow \text{inv} & & \wr \downarrow \text{inv} & & \wr \downarrow \text{inv} \\
\frac{1}{(U:V)} \mathbb{Z}/\mathbb{Z} & \xrightarrow{\text{inkl}} & \frac{1}{(U:W)} \mathbb{Z}/\mathbb{Z} & \xrightarrow{\cdot(U:V)} & \frac{1}{(V:W)} \mathbb{Z}/\mathbb{Z}.
\end{array}$$

Das Paar  $(G, C)$  heißt **Klassenformation**.

**Bemerkung.** 1) Auch für endliche Gruppen ist der Begriff Formationsmodul stärker als der des Klassenmoduls, da bei diesem keine Bedingung für den Übergang zu Quotienten gefordert ist.

2) Aus (ii) folgt die Kommutativität des Diagramms

$$\begin{array}{ccc} H^2(V/W, C^W) & \xrightarrow{inv} & \frac{1}{(V:W)} \mathbb{Z}/\mathbb{Z} \\ \text{cor} \downarrow & & \downarrow \\ H^2(U/W, C^W) & \xrightarrow{inv} & \frac{1}{(U:W)} \mathbb{Z}/\mathbb{Z}, \end{array}$$

da  $\text{cor}_U^V \cdot \text{res}_V^U = (U : V)$ .

3) Die Isomorphismen

$$inv : H^2(G/V, C^V) \xrightarrow{\sim} \frac{1}{(G : V)} \mathbb{Z}/\mathbb{Z}$$

bilden ein gerichtetes System. Im direkten Limes erhält man eine Injektion

$$inv : H^2(G, C) \hookrightarrow \mathbb{Q}/\mathbb{Z},$$

die **Invariantenabbildung** heißt. Das Bild von  $inv$  ist

$$\frac{1}{\#G} \mathbb{Z}/\mathbb{Z} := \lim_{\substack{\rightarrow \\ V}} \frac{1}{(G : V)} \mathbb{Z}/\mathbb{Z}.$$

4) für jeden offenen Normalteiler  $U \subset G$  ist  $C^U$  ein Klassenmodul für  $G/U$ . Die Elemente  $inv_{G/U}^{-1} \left( \frac{1}{(G:U)} \bmod \mathbb{Z} \right) \in H^2(G/U, C^U)$  bilden ein kompatibles System von Fundamentalklassen bei variierendem  $U$ . Daher erhalten wir kompatible Homomorphismen

$$\text{rec}_{G/U} : C^G \rightarrow C^G / N_{G/U} C^U \xrightarrow{\sim} (G/U)^{\text{ab}}.$$

Im Limes erhalten wir den **Reziprozitätshomomorphismus**

$$\text{rec} : C^G \longrightarrow G^{\text{ab}}.$$

Dieser hat dichtes Bild: Ist  $U \subset G^{\text{ab}}$  eine offene Untergruppe und bezeichnen wir das Urbild von  $U$  unter der kanonischen Projektion  $\pi : G \rightarrow G^{\text{ab}}$  mit  $\tilde{U}$ , so gilt  $G^{\text{ab}}/U \cong G/\tilde{U} = (G/\tilde{U})^{\text{ab}}$ , weshalb die Komposition  $\text{rec} : C^G \rightarrow G^{\text{ab}} \twoheadrightarrow G^{\text{ab}}/U$  surjektiv ist.

Nach Definition (und Linksexaktheit des projektiven Limes) gilt

$$\ker(\text{rec}) = N_G C := \bigcap_{U \triangleleft G} N_{G/U} C^U \subset C^G.$$

Man nennt  $N_G C$  die **Gruppe der universellen Normen** von  $C$ .

Schließlich schreibt man für  $\alpha \in C^G$  auch  $(\alpha, G) := \text{rec}(\alpha)$  und nennt dies das **Normrestsymbol**.

# Algebraische Zahlentheorie II

## Sommersemester 2022

Dr. Katharina Hübner

basierend auf Alexander Schmidts AZT2-Skript von 2014

### Inhaltsverzeichnis

<b>1</b>	<b>Lokale Klassenkörpertheorie</b>	<b>1</b>
1.1	Der Existenzsatz . . . . .	2
1.2	Primitive Erzeugung . . . . .	4
1.3	Zahm verzweigte Erweiterungen . . . . .	6
1.4	Trägheits- und Verzweigungsgruppen . . . . .	8
1.5	Das Bild der Einheiten unter Reziprozität . . . . .	13

## 1 Lokale Klassenkörpertheorie

Es sei  $k$  ein lokaler Körper,  $\bar{k}$  ein separabler Abschluss und  $G = G_k = \text{Gal}(\bar{k}|k)$ . In Kapitel 4 haben wir einen Isomorphismus

$$\text{inv}_K : H^2(G_k, \bar{k}^\times) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

konstruiert, so dass für  $k \subset K \subset L \subset \bar{k}$  mit  $L/k$  endlich das Diagramm

$$\begin{array}{ccccccc}
 0 & \longrightarrow & H^2(L|K, L^\times) & \xrightarrow{\text{inf}} & H^2(K, \bar{k}^\times) & \xrightarrow{\text{res}} & H^2(L, \bar{k}^\times) \\
 & & \downarrow \text{inv}_{L|K} & & \downarrow \text{inv}_K & & \downarrow \text{inv}_L \\
 0 & \longrightarrow & \frac{1}{(L:K)} \mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z}
 \end{array}$$

kommutiert. Außerdem gilt für jeden Zwischenkörper  $k \subset K \subset \bar{k}$  nach Hilberts Satz 90, dass  $H^1(G_K, \bar{k}^\times) = 0$ . Wir erhalten

**Satz 1.1.** *Das Paar  $(G_k, \bar{k}^\times)$  ist eine Klassenformation.*

**Korollar 1.2.** *Wir erhalten einen Reziprozitätshomomorphismus*

$$\text{rec} : k^\times \longrightarrow G_k^{\text{ab}}$$

*mit dichtem Bild.*

### Ziele:

- 1.) Verstehe die Normengruppe in  $k^\times$ .
- 2.) Verstehe das Bild von  $rec$ .
- 3.) Welche Rolle spielt das Bild  $rec(U_k)$ ?

## 1.1 Der Existenzsatz

**Satz 1.3.** Die Normengruppen in  $k^\times$  sind genau die offenen Untergruppen von endlichem Index.

Wir brauchen zunächst:

**Satz 1.4.** Sei  $(n, \text{char } k) = 1$  und  $\mu_n \subset k$ . Sei  $K = k(\sqrt[n]{k^\times})$  die Erweiterung, die man durch Adjunktion der  $n$ -ten Wurzel aus allen Elementen in  $k^\times$  erhält. Dann ist  $K|k$  endlich und

$$N_{K|k}K^\times = k^{\times n}$$

*Beweis.* Wir fixieren eine primitive  $n$ -te Einheitswurzel in  $k$ , d.h. einen Isomorphismus  $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mu_n$  und erhalten nach Kummer-Theorie

$$H^1(G_k, \mathbb{Z}/n\mathbb{Z}) \cong H^1(G_k, \mu_n) \cong k^\times / k^{\times n}.$$

Nach Zahlentheorie I, 8.54, ist  $k^\times / k^{\times n}$  endlich. Entspricht  $\varphi \in H^1(G_k, \mathbb{Z}/n\mathbb{Z})$  bzgl. dieses Isomorphismus dem Element  $x \in k^\times / k^{\times n}$ , so ist  $\bar{k}^{\ker(\varphi)} = k(\sqrt[n]{x})$ . Daher ist  $K$  das Kompositum aller zyklischen Erweiterungen von  $k$ , deren Ordnung  $n$  teilt. Wir erhalten einen Isomorphismus

$$\begin{aligned} G(K|k) &\cong \text{Hom}(G(K|k), \mathbb{Z}/n\mathbb{Z})^\vee = \text{Hom}(G_k^{\text{ab}}/n, \mathbb{Z}/n)^\vee \\ &= H^1(G_k, \mathbb{Z}/n)^\vee = (k^\times / k^{\times n})^\vee. \end{aligned}$$

Daher ist  $K|k$  endlich (und abelsch sowieso). Nun hat die Gruppe  $G(K|k)$  den Exponenten  $n$ . Daher gilt  $n \cdot \hat{H}^i(G(K|k), A) = 0$  für jeden  $G(K|k)$ -Modul  $A$ . Für  $i = 0$  und  $A = K^\times$  erhalten wir  $k^{\times n} \subseteq N_{K|k}K^\times$ .

Nach Korollar 9 in Kapitel 6 gilt nun aber

$$(k^\times : N_{K|k}K^\times) = [K : k] = \#k^\times / k^{\times n}$$

und wir erhalten  $N_{K|k}K^\times = k^{\times n}$ . □

*Beweis von Satz 1.3.* Wir versehen für jede endliche Erweiterung  $K|k$  die Gruppe  $K^\times$  mit ihrer natürlichen Topologie. Nach Abschnitt 6 in Kapitel 6 müssen wir die folgenden Axiome verifizieren:

Axiom I. Für jede endliche Erweiterung  $L'|L$  hat die Normabbildung abgeschlossenes Bild und kompakten Kern.

Beweis von Axiom I. Die Normabbildung  $N_{L'|L} : L'^{\times} \rightarrow L^{\times}$  ist eigentlich, siehe Übungsaufgabe.

Axiom II. Für jede Primzahl  $p$  existiert ein Körper  $L_p$  so dass für  $L \supset L_p$  die  $p$ -Potenzierung  $m_p : L^{\times} \rightarrow L^{\times}$  der folgenden Bedingung genügt

$$(*) \quad \ker(m_p) \text{ ist kompakt und } \text{im}(m_p) \supset D_L$$

Beweis von Axiom II. Der Kern von  $m_p$  ist endlich. Wir zeigen die Aussage über  $\text{im}(m_p)$  im Fall  $p \neq \text{char } k$ . Setze  $L_p = k(\mu_p)$ . Dann gilt für jedes  $L \supset L_p$  nach 1.4:

$$N(L(\sqrt[p]{L^{\times}})/L) = L^{\times p} = \text{im}(m_p)$$

also  $D_L \subset \text{im}(m_p)$

- für  $p = \text{char } k$ , siehe Serre: Local fields.

Axiom III. Es existiert eine kompakte Untergruppe  $U \subset L^{\times}$ , so dass jede Untergruppe von endlichem Index in  $L^{\times}$ , die  $U$  enthält, Normengruppe ist.

Zum Beweis brauchen wir:

**Lemma 1.5.** *Sei  $L_n|L$  die unverzweigte Erweiterung vom Grad  $n$ . Dann gilt*

$$N_{L_n|L}(L_n^{\times}) = \ker(L^{\times} \xrightarrow{v} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}) = (\pi^n) \times U_L$$

wobei  $\pi$  eine Uniformisierende von  $L$  ist.

*Beweis.*  $U_{L_n}$  ist ein kohomologisch trivialer  $G(L_n|L)$ -Modul, insbesondere

$$\hat{H}^0(G(L_n|L), U_{L_n}) = 0, \text{ d.h. } N_{L_n|L}(U_{L_n}) = U_L,$$

d.h.  $N_{L_n|L}(L_n^{\times}) \supset U_L$ . Es ist  $\pi$  eine Uniformisierende von  $L_n$  und

$$N_{L_n|L}(\pi) = \pi^n \implies (\pi^n) \times U_L \subset N_{L_n|L}(L_n^{\times}).$$

Nun gilt aber

$$(L^{\times} : (\pi^n) \times U_L) = n = (L^{\times} : N_{L_n|L}(L_n^{\times})),$$

also  $(\pi^n) \times U_L = N_{L_n|L}(L_n^{\times})$ . □

Beweis von Axiom III. Wir setzen  $U = U_L$ . Die offenen Untergruppen von endlichem Index in  $L^{\times}$ , die  $U_L$  enthalten, sind wegen  $L^{\times}/U_L \xrightarrow{v} \mathbb{Z}$  genau die Untergruppen der Form  $(\pi^n) \times U_L$  und diese sind nach 1.5 Normengruppen. Dies zeigt Satz 1.3. □

**Korollar 1.6.** *Die Gruppe der universellen Normen ist trivial.*



*Beweis.* Nach Zahlentheorie I, 8.54, ist der Durchschnitt aller offenen Untergruppen von endlichem Index in  $L^\times$  trivial.  $\square$

**Korollar 1.7.** *Die Reziprozitätsabbildung*

$$\text{rec} : k^\times \longrightarrow G(k^{\text{ab}}|k)$$

*ist stetig und injektiv.*

*Beweis.* Nach 1.6 gilt  $\ker(\text{rec}) = 0$ . Nun faktorisiert  $\text{rec}$  als

$$k^\times \xrightarrow{\alpha} \varprojlim_{\substack{U \subset k^\times \\ \text{off. von endl. Index}}} k^\times/U \xrightarrow[\sim]{\beta} \varprojlim_{\substack{U \subset G(k^{\text{ab}}|k) \text{ off.} \\ \text{von endl. Index}}} G(k^{\text{ab}}|k)/U \quad \parallel \wr \quad G(k^{\text{ab}}|k)$$

$\alpha$  ist stetig, da die Projektionen  $k^\times \rightarrow k^\times/U$  stetig sind und  $\beta$  ist der projektive Limes von Isomorphismen endlicher Gruppen, also ein topologischer Isomorphismus.  $\square$

## 1.2 Primitive Erzeugung

Wir erinnern uns an AZT I, Lemma 8.55

**Lemma 1.8.** *Sei  $A$  ein kommutativer Ring, und  $M$  ein freier  $A$ -Modul vom endlichen Rang  $n$ . Dann ist jedes Erzeugendensystem  $x_1, \dots, x_n$  der Länge  $n$  von  $M$  eine Basis.*

**Satz 1.9.** *Sei  $L|K$  eine endliche separable Erweiterung lokaler Körper. Dann existiert ein  $x \in \mathcal{O}_L$ , so dass*

$$\mathcal{O}_L = \mathcal{O}_K[x].$$

*Beweis.* Sei  $e = e(L|K)$ ,  $f = f(L|K)$  und  $n = [L : K]$ , also  $n = ef$ . Sei  $\pi = \pi_L$  eine Uniformisierende von  $L$  und sei  $x \in \mathcal{O}_L$  so gewählt, dass  $\ell = k(\bar{x})$ .

Behauptung 1. Die Produkte

$$x^i \pi^j, \quad 0 \leq i < f, \quad 0 \leq j < e,$$

sind eine  $\mathcal{O}_K$ -Basis von  $\mathcal{O}_L$ .

Beweis der Behauptung 1. Diese Elemente erzeugen offenbar  $\mathcal{O}_L/\pi^e \mathcal{O}_L$ . Nun gilt  $\mathfrak{p}_K \cdot \mathcal{O}_L = \pi^e \mathcal{O}_L$ , d.h. diese Elemente erzeugen  $\mathcal{O}_L/\mathfrak{p}_K \mathcal{O}_L$ . Nach Nakayama erzeugen sie  $\mathcal{O}_L$  und nach 1.8 sind sie eine Basis.

Behauptung 2. Man kann  $x$  so wählen, dass ein normales Polynom

$$F \in \mathcal{O}_K[x], \quad \deg F = f,$$

existiert, so dass  $F(x) \in \mathcal{O}_L$  eine Uniformisierende ist.

Beweis von Behauptung 2. Sei  $F \in \mathcal{O}_K[x]$  ein normiertes Polynom vom Grad  $f$ , dessen Reduktion  $\overline{F} \in k[x]$  das Minimalpolynom von  $\overline{x} \in \ell$  über  $k$  ist. Wegen  $\overline{F}(\overline{x}) = 0$  folgt  $v_L(F(x)) \geq 1$ . Gilt „=“, sind wir fertig. Ansonsten gilt  $v_L(F(x)) \geq 2$ . Sei  $h \in \mathcal{O}_L$  irgendein Element mit  $v_L(h) = 1$ . Taylor:

$$F(x+h) = F(x) + h \cdot F'(x) + h^2 \cdot r, \quad r \in \mathcal{O}_L.$$

Da  $\overline{F}$  separabel ist, gilt  $\overline{F}'(\overline{x}) \neq 0$ , also

$$v_L(F'(x)) = 0, \quad v_L(F'(x)h) = 1.$$

Wir erhalten  $v_L(F(x+h)) = 1$  und  $x+h$  erfüllt das Gewünschte.

Nun wählen wir  $x$  wie in Behauptung 2 und setzen  $\pi = F(x)$ . Nach Behauptung 1 ist  $x^i F(x)^j$ ,  $0 \leq i < f$ ,  $0 \leq j < e$ , eine  $\mathcal{O}_K$ -Basis von  $\mathcal{O}_L$ . Also wird  $\mathcal{O}_L$  über  $\mathcal{O}_K$  durch  $1, x, \dots, x^{n-1}$  erzeugt und nach 1.8 ist auch dies eine Basis.  $\square$

**Satz 1.10.** Sei  $L|K$  eine endliche separable Erweiterung lokaler Körper. Sei  $x \in \mathcal{O}_L$ , so dass  $\mathcal{O}_L = \mathcal{O}_K[x]$ , und sei  $F \in \mathcal{O}_K[X]$  das Minimalpolynom von  $x$ . Dann sind äquivalent:

- (i)  $L|K$  ist unverzweigt,
- (ii)  $\overline{F} \in k[X]$  ist separabel,
- (iii)  $\overline{F} \in k[X]$  ist irreduzibel,
- (iv)  $v_L(F'(x)) = 0$ .

*Beweis.* Sei  $\overline{F} = G_1^{e_1} \dots G_g^{e_g}$  die Primzerlegung von  $\overline{F} \in k[X]$ . Dann gibt es  $g$  Primideale in  $\mathcal{O}_L$  über  $\mathfrak{p}_K$ . Da  $\mathcal{O}_L$  ein diskreter Bewertungsring ist, gilt  $g = 1$ , d.h.  $\overline{F} = G^e$  für ein irreduzibles normales Polynom  $G \in k[X]$  und  $e = e(L|K)$ .

Da  $k$  vollkommen ist, ist  $G$  separabel. Nun gilt in dieser Situation

$$\overline{F} \text{ irreduzibel} \iff e = 1 \iff \overline{F} \text{ separabel} \iff (\overline{F}, \overline{F}') = 1 \implies \overline{F}'(\overline{x}) \neq 0$$

$$\iff \overline{x} \text{ einfache Nullstelle von } \overline{F} \implies e = 1$$

$$\text{Außerdem gilt } \overline{F}'(\overline{x}) \neq 0 \iff v_L(F'(x)) = 0. \quad \square$$

Erinnerung:  $F \in \mathcal{O}_K[X]$  heißt *Eisensteinpolynom*, wenn

$$F = X^n + a_{n-1}X^{n-1} + \dots + a_0$$

mit  $\pi_K \mid a_i$ ,  $i = 0, \dots, n-1$  und  $\pi_K^2 \nmid a_0$ . Eisensteinpolynome sind irreduzibel.

**Satz 1.11.** Sei  $K$  ein lokaler Körper und  $F \in \mathcal{O}_K[X]$  ein Eisensteinpolynom. Sei  $L = K[X]/F$ . Dann ist  $L|K$  rein verzweigte Erweiterung (d.h.  $e(L|K) = [L : K]$ ) vom Grad  $n = \deg F$  und das Bild von  $X$  in  $L$  ist eine Uniformisierende von  $L$ .

*Beweis.* Da  $F$  irreduzibel ist, ist  $L|K$  eine Körpererweiterung vom Grad  $n = \deg F$ . Sei  $F = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ , und sei  $\alpha$  die tautologische Nullstelle von  $F$  in  $L$  ( $\alpha$  ist das Bild von  $X$  unter  $K[X] \rightarrow K[X]/F = L$ ). Dann gilt:

$$-\alpha^n = a_{n-1}\alpha^{n-1} + \cdots + a_0$$

und daher  $v_L(\alpha) \geq 1$ .

Es gilt auch

$$\begin{aligned} e = v_L(a_0) &= v_L(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha) \\ &\geq \min(nv_L(\alpha), e + v_L(\alpha)). \end{aligned}$$

Daher gilt  $e = n \cdot v_L(\alpha)$ , also

$$v_L(\alpha) = 1 \quad \text{und} \quad e = n. \quad \square$$

Umgekehrt gilt

**Satz 1.12.** Sei  $L|K$  eine rein verzweigte endliche separable Erweiterung lokaler Körper, und sei  $\pi = \pi_L$  eine Uniformisierende von  $L$ . Dann gilt  $\mathcal{O}_L = \mathcal{O}_K[\pi]$ , und das Minimalpolynom  $F$  von  $\pi$  über  $K$  ist ein Eisensteinpolynom.

*Beweis.* Nach Behauptung 1 im Beweis von 1.9 (wähle  $x = 1$ ) ist  $1, \pi, \dots, \pi^{e-1}$  eine  $\mathcal{O}_K$ -Basis von  $\mathcal{O}_L$ . Für das Minimalpolynom  $F \in \mathcal{O}_K[x]$  von  $\pi$  gilt wegen  $\bar{\pi} = 0$  und  $e = n$ :  $\bar{F} = X^e$  und daher

$$F = X^e + a_{e-1}X^{e-1} + \cdots + a_0$$

mit  $\bar{a}_i = 0$ , also  $\pi_K \mid a_i$ , also  $\pi^e \mid a_i$  für  $i = 0, \dots, e-1$ . Wir erhalten  $-a_0 = \pi^e + a_{e-1}\pi^{e-1} + \cdots + a_1\pi$  und daher  $v_L(a_0) = v_L(\pi^e) = e$  und  $v_K(a_0) = 1$ .  $\square$

### 1.3 Zahm verzweigte Erweiterungen

Erinnerung:  $L|K$  heißt zahm verzweigt, falls  $p \nmid e$  mit  $e = e(L|K)$  und  $p = \text{char}(k)$ .

**Lemma 1.13.** Sei  $(n, p) = 1$  und  $\pi \in K$  eine Uniformisierende. Dann ist die Erweiterung  $K(\sqrt[n]{\pi})|K$  rein zahm verzweigt vom Grad  $n$ , d.h.  $e(K(\sqrt[n]{\pi})|K) = n$ .

*Beweis.* Wegen  $v(\pi) = 1$  existiert in  $K$  für kein  $m \geq 2$  eine  $n$ -te Wurzel aus  $\pi$ . Das Minimalpolynom  $F$  von  $\sqrt[n]{\pi}$  ist ein Teiler des Eisensteinpolynoms  $X^n - \pi \implies F = X^n - \pi$ . Jetzt folgt alles aus 1.11.  $\square$

**Lemma 1.14.** (i) Für einen Turm  $M|L|K$  gilt

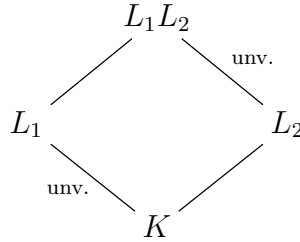
$$M|K \text{ z.v.} \iff M|L \text{ z.v.} + L|K \text{ z.v.}$$

(ii) Ist  $L_1|K$  unverzweigt und  $L_2|K$  separabel, so gilt

$$L_2|K \text{ z.v.} \iff L_1L_2|L_1 \text{ z.v.}$$

*Beweis.* (i) folgt aus der Multiplikativitat der Verzweigungsindizes in Korperturmen.

(ii)



Nach (i) folgt nun

$$L_2|K \text{ z.v.} \iff L_1L_2|K \text{ z.v.} \iff L_1L_2|L_1 \text{ z.v.} \quad \square$$

**Satz 1.15.** Sei  $\pi \in K$  eine Uniformisierende. Fur eine Erweiterung  $L|K$  sind aquivalent:

- (i)  $L|K$  ist zahm verzweigt.
- (ii) Es existiert eine unverzweigte Erweiterung  $M|K$  so dass  $LM = M(\sqrt[e]{\pi})$ , wobei  $(e, p) = 1$ .

*Beweis.* (ii)  $\implies$  (i). Nach 1.13 ist  $LM|M$  zahm verzweigt. Nach 1.14 folgt  $L|K$  ist zahm verzweigt.

(i)  $\implies$  (ii). Sei  $L|K$  zahm verzweigt und  $\pi_L$  eine Uniformisierende von  $L$ . Sei  $K'$  die maximal unverzweigte Teilerweiterung und  $\pi$  eine Uniformisierende von  $K$  und damit auch von  $K'$ . Es gilt

$$\pi_L^e = \pi \cdot \zeta \cdot u$$

mit  $\zeta \in \mu'(L) = \mu'(K')$  und  $u \in U_L^1$ . Wegen  $1/e \in \mathbb{Z}_p$  existiert  $\sqrt[e]{\pi\zeta'} \in L$ , also  $L = K'(\sqrt[e]{\pi\zeta'})$ . Mit  $M := K'(\sqrt[e]{\zeta})$  erhalten wir  $LM = M(\sqrt[e]{\pi})$ .  $\square$

**Korollar 1.16.** Das Kompositum zahm verzweigter Erweiterungen ist zahm verzweigt.

*Beweis.* Sei  $e_1 = e(L_1|K)$ ,  $e_2 = e(L_2|K)$ . Fur geeignetes  $M|K$  unverzweigt gilt:

$$\begin{aligned}
 & L_1M = M(\sqrt[e_1]{\pi}), \quad L_2M = M(\sqrt[e_2]{\pi}) \\
 \implies & L_1L_2M = M(\sqrt[e]{\pi}) \text{ mit } e = \text{kgV}(e_1, e_2) \\
 \implies & L_1L_2M|M \text{ zahm verzweigt} \\
 \implies & L_1L_2|K \text{ zahm verzweigt.}
 \end{aligned}$$

$\square$

**Definition.** Wir nennen eine unendliche, separable algebraische Erweiterung  $L$  eines lokalen Körpers  $K$  **zahn verzweigt**, wenn jede endliche Teilerweiterung zahn verzweigt ist. Die maximal zahn verzweigte Teilerweiterung von  $K$  in einem gegebenen separablen Abschluß  $\overline{K}$  von  $K$  wird mit  $K^{tr}$  bezeichnet.

**Satz 1.17.**  $K^{tr}|K$  ist galoissch.  $K^{tr}$  entsteht aus  $K$  durch Adjunktion aller prim-zu- $p$  Einheitswurzeln und aller prim-zu- $p$ -ten Wurzeln aus  $\pi$ .

Setzt man  $\hat{\mathbb{Z}}^{(p')} = \prod_{\ell \neq p} \mathbb{Z}_\ell$ , so erhalten wir eine exakte Folge

$$1 \rightarrow \hat{\mathbb{Z}}^{(p')} \rightarrow G(K^{tr}|K) \rightarrow \hat{\mathbb{Z}} \rightarrow 1.$$

## 1.4 Trägheits- und Verzweigungsgruppen

Sei  $L|K$  eine Galoiserweiterung lokaler oder globaler Körper, und sei  $v$  eine nicht-archimedische Bewertung auf  $K$  und  $w$  eine Fortsetzung auf  $L$ .

**Definition.** •  $T_w(L|K) = \{\sigma \in G_w(L|K) \mid \sigma x \equiv x \pmod{\mathfrak{P}_w} \quad \forall x \in \mathcal{O}_w\}$  heißt die **Trägheitsgruppe** von  $w$  in  $L|K$ . Hierbei ist  $\mathcal{O}_w$  der Bewertungsring von  $w$  in  $L$  und  $\mathfrak{P}_w \subset \mathcal{O}_w$  das Maximalideal

•  $V_w(L|K) = \{\sigma \in G_w(L|K) \mid \frac{\sigma x}{x} \equiv 1 \pmod{\mathfrak{P}_w} \quad \forall x \in L^\times\}$  heißt die **Verzweigungsgruppe** von  $w$  in  $L|K$ .

**Bemerkungen.** 1) Für  $\sigma \in G_w$  und  $x \in L^\times$  gilt  $v_L(\sigma x) = v_L(x)$ , also  $\sigma x/x \in \mathcal{O}_w$ . Daher ist die Definition von  $V_w$  sinnvoll.

2) Für  $\sigma \in V_w$  und  $x \in \mathcal{O}_w$  gilt  $\sigma x \equiv x \pmod{\mathfrak{P}_w}$ . Daher gilt

$$V_w \subset T_w.$$

**Lemma 1.18.** (i) Es gilt  $\sigma \in T_w(L|K)$  (bzw.  $V_w(L|K)$ ) dann und nur dann, wenn für jede endliche galoissche Teilerweiterung  $K' \subset L$  gilt  $\sigma|_{K'} \in T_w(K'|K)$  (bzw.  $V_w(K'|K)$ ).

(ii) Es gilt

$$T_w(L|K) = \varprojlim_{K \subset K' \subset L} T_w(K'|K)$$

und analog für  $V_w$ .

(iii)  $V_w$  und  $T_w$  sind abgeschlossene Untergruppen in  $G(L|K)$ .

*Beweis.* Standard. □

**Lemma 1.19.**  $V_w$  und  $T_w$  sind Normalteiler in  $G_w$ .

*Beweis.*  $T_w = \ker(G_w \rightarrow G(\ell|k))$  ist offensichtlich ein NT.

Sei  $\sigma \in V_w$  und  $\tau \in G_w$ . Dann gilt für jedes  $x \in L^\times$

$$\frac{\tau \sigma \tau^{-1} x}{x} - 1 = \frac{\tau \sigma \tau^{-1} x}{\tau \tau^{-1} x} - 1 = \tau \left( \frac{\sigma \tau^{-1} x}{\tau^{-1} x} - 1 \right) \in \tau(\mathfrak{P}_L) = \mathfrak{P}_L.$$

Also gilt  $\tau \sigma \tau^{-1} \in V_w$  und  $V_w \subset G_w$  ist Normalteiler. □

**Lemma 1.20.** Sei  $M|K$  eine Galoiserweiterung,  $w$  eine nicht-archimedische Bewertung auf  $M$  und  $L \subset M$  eine Zwischenerweiterung. Dann gilt

$$\begin{aligned} T_w(M|L) &= T_w(M|K) \cap G(M|L) \\ V_w(M|L) &= V_w(M|K) \cap G(M|K) \end{aligned}$$

*Beweis.* direkt aus Definition. □

**Satz 1.21.** Sei  $K$  ein globaler Körper. Dann gilt

$$\begin{aligned} T_w(L|K) &= T(L_w|K_v) \\ V_w(L|K) &= V(K_w|K_v). \end{aligned}$$

*Beweis.* Es gilt  $G_w(L|K) = G(L_w|K_v)$ . Aus Stetigkeitsgründen genügt es die definierenden Bedingungen für Elemente in  $T_w$  bzw.  $V_w$  auf einer dichten Teilmenge zu prüfen. Da  $\mathcal{O}_w \subset \mathcal{O}_{L_w}$  und  $L^\times$  in  $L_w^\times$  dicht sind, folgt das Ergebnis. □

**Satz 1.22.** Sei  $K$  ein lokaler Körper und  $L|K$  galoissch. Dann ist  $L^T$  die maximal unverzweigte Teilerweiterung von  $L|K$ .

*Beweis.* Nach Definition gilt

$$T(L|K) = \ker(\varphi : G(L|K) \longrightarrow G(\ell|k)).$$

Nach Konstruktion faktorisiert  $\varphi$  in der Form

$$G(L|K) \twoheadrightarrow G(K'|K) \xrightarrow{\sim} G(\ell|k),$$

wobei  $K'|K$  die maximal unverzweigte Teilerweiterung ist. Nach Galoistheorie folgt  $L^T = K'$ . □

So wie  $T_w$  der Kern des natürlichen Homomorphismus  $\phi : G_w \longrightarrow G(\ell|k)$  ist, so ist auch  $V_w$  der Kern eines natürlichen Homomorphismus von  $T_w$  in eine abelsche Gruppe.

**Definition.**  $X_w(L|K) = \text{Hom}(w(L^\times)/w(K^\times), \ell^\times)$ .

Für  $\sigma \in T_w$  definieren wir ein Element  $\chi_\sigma \in X_w(L|K)$ , d.h. einen Homomorphismus

$$\chi_\sigma : w(L^\times)/w(K^\times) \longrightarrow \ell^\times$$

wie folgt: Zu  $\bar{x} \in w(L^\times)/w(K^\times)$  wähle einen Vertreter  $x \in L^\times$ . Dann setze

$$\chi_\sigma(\bar{x}) = \overline{\left(\frac{\sigma x}{x}\right)} \in \ell^\times.$$

**Satz 1.23.** Die obige Zuordnung ist wohldefiniert und induziert einen Homomorphismus  $T_w \longrightarrow X_w$  mit Kern  $V_w$ .

*Beweis.* Wohldefiniertheit. Ist  $x' \in L^\times$  weiterer Vertreter, so gilt  $w(x') = w(xa)$  mit  $a \in K^\times$ , also  $x' = xa \cdot u$  mit  $u \in U_w = \mathcal{O}_w^\times$ . Für  $\sigma \in T_w$  gilt  $\overline{\left(\frac{\sigma u}{u}\right)} = 1 \in \ell^\times$  und deshalb

$$\overline{\left(\frac{\sigma x'}{x'}\right)} = \overline{\left(\frac{\sigma x}{x}\right) \left(\frac{\sigma a}{a}\right) \left(\frac{\sigma u}{u}\right)} = \overline{\left(\frac{\sigma x}{x}\right)}.$$

Dies zeigt die Wohldefiniertheit. Ist nun  $\chi_\sigma$  die Nullabbildung, so gilt

$$\overline{\left(\frac{\sigma x}{x}\right)} = 1 \quad \forall x \in L^\times,$$

also  $\sigma \in V_w$  und umgekehrt. Bleibt zu zeigen, dass  $T_w \rightarrow X_w$  ein Homomorphismus ist: Für  $\sigma, \tau \in T_w$  gilt

$$\chi_{\sigma\tau}(\bar{x}) = \overline{\left(\frac{\sigma\tau x}{x}\right)} = \overline{\frac{\sigma x}{x} \cdot \frac{\tau x}{x} \cdot \frac{\sigma(\tau(x)/x)}{\tau(x)/x}}.$$

Wegen  $u := \frac{\tau(x)}{x} \in U_w$  folgt

$$\overline{\left(\frac{\sigma u}{u}\right)} = 1 \in \ell^\times.$$

□

**Satz 1.24.** Sei  $L|K$  eine endliche Galoiserweiterung. Dann ist  $V_w$  eine  $p$ -Gruppe und  $T_w/V_w$  ist von prim-zu- $p$ -Ordnung. D.h.  $V_w$  ist die einzige  $p$ -Sylowgruppe in  $T_w$ .

*Beweis.* Ohne Einschränkung sei  $L|K$  eine Erweiterung lokaler Körper. Dann ist  $\ell^\times$  eine endliche Gruppe von prim-zu- $p$  Ordnung und dasselbe gilt für die endliche abelsche Gruppe

$$X = \text{Hom}(w(L^\times)/v(K^\times), \ell^\times).$$

(Erinnerung:  $(w(L^\times) : v(K^\times)) = e(L|K) < \infty$  und  $w(L^\times) \cong \mathbb{Z} \cong v(K^\times)$ .)

Nach 1.23 haben wir eine Inklusion

$$T/V \hookrightarrow X$$

also ist  $\#T/V$  prim zu  $p$ .

Bleibt zu zeigen, dass  $V$  eine  $p$ -Gruppe ist. Angenommen nicht. Dann existiert eine Primzahl  $q \neq p$  und ein Element  $\sigma \in V$  der Ordnung  $q$ . Nach 1.22 ist  $L|L^{\langle\sigma\rangle}$  eine rein zahn verzweigte Galoiserweiterung vom Grad  $q$ . Sei  $\pi_L$  eine Uniformisierende von  $L$  und  $\pi$  eine Uniformisierende von  $L^{\langle\sigma\rangle}$ . Es gilt

$$\pi_L^q = \pi \cdot \zeta \cdot u$$

mit  $\zeta \in \mu'(L)$  und  $u \in U_L^{(1)}$ .

Wie im Beweis von 1.15 folgt  $\zeta \in L^{\langle \sigma \rangle}$  und  $L = L^{\langle \sigma \rangle}(\sqrt[q]{\pi\zeta})$ . Ersetzen wir  $\pi$  durch  $\pi\zeta$  erhalten wir  $L = L^{\langle \sigma \rangle}(\sqrt[q]{\pi})$ . Da  $L|L^{\langle \sigma \rangle}$  galoissch ist, folgt die Existenz einer primitiven  $q$ -ten Erweiterung  $\zeta_q \in L^{\langle \sigma \rangle}$  so dass gilt:

$$\sigma(\sqrt[q]{\pi}) = \zeta_q \cdot \sqrt[q]{\pi}.$$

Folglich gilt

$$\frac{\sigma(\sqrt[q]{\pi})}{\sqrt[q]{\pi}} = \zeta_q \not\equiv 1 \pmod{\mathfrak{P}}$$

wegen  $(p, q) = 1$ . Widerspruch □

**Korollar 1.25.** *Ist  $L|K$  eine endliche Galoiserweiterung lokaler Körper so ist  $L^V$  die maximal zahm verzweigte Teilerweiterung von  $L|K$ .*

*Beweis.* Da  $L^T|K$  die maximal unverzweigte Teilerweiterung ist, ist  $L|L^T$  rein verzweigt.

Für eine Zwischenerweiterung  $K'|K$  die der Untergruppe  $U \subset G$  entspricht gilt daher  $K'|K$  zahm verzweigt  $\stackrel{1.14}{\iff} K'L^T|L^T$  zahm verzweigt

$$\iff [K'L^T : L^T] \text{ ist prim zu } p$$

$$\iff (T : U \cap T) \text{ ist prim zu } p$$

$$\iff U \supset V$$

□

Wir erweitern dies auf proendliche Gruppen durch die folgende Definition.

**Definition.** Eine proendliche Gruppe  $G$  heißt **pro- $p$ -Gruppe**, wenn sie projektiver Limes endlicher  $p$ -Gruppen ist, d.h. wenn für jede offene Untergruppe  $U \subseteq G$  der Index  $(G : U)$  eine  $p$ -Potenz ist. Wir sagen, dass eine abgeschlossene Untergruppe  $H \subset G$  einen **prim-zu- $p$ -Index** hat, wenn für jede offene Untergruppe  $U \subset G$ ,  $U \supseteq H$  der Index  $(G : U)$  prim zu  $p$  ist.

Eine abgeschlossene Untergruppe  $G_p \subset G$  heißt  **$p$ -Sylowgruppe**, wenn

- $G_p$  ist eine pro- $p$ -Gruppe
- $(G : G_p)$  ist prim zu  $p$ .

Fakten:

- $p$ -Sylowgruppen existieren.
- beliebige zwei  $p$ -Sylowgruppen sind konjugiert.
- ist eine  $p$ -Sylowgruppe Normalteiler, so ist sie die einzige  $p$ -Sylowgruppe.

**Satz 1.26.** *Sei  $K$  ein lokaler Körper und  $L|K$  galoissch. Dann ist  $V$  die einzige  $p$ -Sylowgruppe in  $T$  und  $L^V$  ist die maximal zahm verzweigte Erweiterung von  $K$  in  $L$ .*

*Beweis.* Dies folgt per Limesbildung aus dem Fall endlicher Erweiterungen und Lemma 1.18. □



**Satz 1.27.** Sei  $K$  ein lokaler oder globaler Körper und sei  $M|L|K$  ein Turm von Galoiserweiterungen. Sei  $w$  die bzw. eine nicht-archimedische Bewertung auf  $M$ . Dann haben wir exakte Folgen

$$\begin{aligned} 1 &\longrightarrow G_w(M|L) \longrightarrow G_w(M|K) \longrightarrow G_w(L|K) \longrightarrow 1, \\ 1 &\longrightarrow T_w(M|L) \longrightarrow T_w(M|K) \longrightarrow T_w(L|K) \longrightarrow 1, \\ 1 &\longrightarrow V_w(M|L) \longrightarrow V_w(M|K) \longrightarrow V_w(L|K) \longrightarrow 1. \end{aligned}$$

*Beweis.* Wegen der Exaktheit des projektiven Limes sei ohne Einschränkung  $M|K$  endlich. Wegen  $G_w(L|K) = G(L_w|K_w)$  folgt die Exaktheit der ersten Folge und nach 1.21 können wir uns für den Beweis der Exaktheit der beiden weiteren Folgen auf den Fall lokaler Körper beschränken. Im kommutativen Diagramm

$$\begin{array}{ccccccc} & & 1 & & 1 & & 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & T(M|L) & \longrightarrow & G(M|L) & \longrightarrow & G(m|\ell) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & T(M|K) & \longrightarrow & G(M|K) & \longrightarrow & G(m|k) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & T(L|K) & \longrightarrow & G(L|K) & \longrightarrow & G(\ell|k) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 1 & & 1 & & 1 \end{array}$$

sind alle Zeilen und die 2. + 3. Spalte exakt, also auch die erste Spalte. Nach 1.26 erhalten wir die exakte Folge

$$\begin{array}{ccccccc} 1 & \longrightarrow & V(L|K) & \longrightarrow & V(M|K) & \longrightarrow & V(L|K) \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & T(L|K) & \longrightarrow & T(M|K) & \longrightarrow & T(L|K) \longrightarrow 0. \end{array}$$

Es bleibt zu zeigen, dass  $V(M|K) \rightarrow V(L|K)$  surjektiv ist. Sei  $\sigma \in V(L|K)$  beliebig und  $\tau \in T(M|K)$  mit  $\tau|_L = \sigma$ . Da  $T(M|K)/V(M|K)$  von prim-zu- $p$  Ordnung ist, existiert ein  $n \in \mathbb{N}$ ,  $(n, p) = 1$  mit  $\tau^n \in V(M|K)$ .

Sei  $o(\sigma) = p^s$  die Ordnung von  $\sigma$ . Wähle  $m \in \mathbb{N}$  mit  $n \cdot m \equiv 1 \pmod{o(\sigma)}$ . Dann gilt  $\tau^{m \cdot n} = (\tau^n)^m \in V(M|K)$  und  $\tau^{m \cdot n}|_L = \sigma^{m \cdot n} = \sigma$ .  $\square$

**Satz 1.28.** Die Galoisgruppe einer endlichen Galoiserweiterung eines lokalen Körpers ist auflösbar. Ist  $L|K$  eine unendliche Galoiserweiterung eines lokalen Körpers  $K$ , so ist  $G(L|K)$  pro-auflösbar, d.h. projektiver Limes endlicher auflösbarer Gruppen.

*Beweis.* Ist  $L|K$  endlich Galoissch, so haben wir in  $G = G(L|K)$  die Folge von Normalteilern

$$1 \subseteq V \subseteq T \subseteq G.$$

Es sind  $G|T$  und  $T|V$  abelsch (sogar zyklisch) und  $V$  ist eine  $p$ -Gruppe. Da  $p$ -Gruppen nilpotent, also insbesondere auflösbar sind, folgt das Ergebnis.  $\square$

## 1.5 Das Bild der Einheiten unter Reziprozität

**Satz 1.29.** *Die Einschränkung von  $rec$  auf  $U_K$  definiert einen Isomorphismus  $rec|_{U_K} : U_K \xrightarrow{\sim} T(K^{\text{ab}}|K)$ . Die induzierte Abbildung*

$$rec^{\text{nr}} : K^\times / U_K \longrightarrow G(K^{\text{nr}}|K)$$

*ist injektiv und das Bild besteht aus allen ganzzahligen Potenzen des Frobeniusautomorphismus. Es gilt*

$$rec^{\text{nr}}(x) = \text{Frob}^{v(x)}.$$

*Beweis.* Wir haben die induzierte Klassenformation  $(G(K^{\text{nr}}|K), K^{\text{nr}\times})$ . Da  $U_{K^{\text{nr}}}$  ein kohomologisch trivialer Modul ist, gibt die exakte Folge  $0 \rightarrow U_{K^{\text{nr}}} \rightarrow K^{\text{nr}\times} \xrightarrow{v} \mathbb{Z} \rightarrow 0$  einen Isomorphismus zur Klassenformation

$$(\hat{\mathbb{Z}}, \mathbb{Z})$$

wobei die Invariantenabbildung gegeben ist durch den natürlichen Homomorphismus

$$\begin{aligned} H^2(\hat{\mathbb{Z}}, \mathbb{Z}) &\xrightarrow{\sim} H^1(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathbb{Q}/\mathbb{Z}, \\ \varphi &\longmapsto \varphi(1). \end{aligned}$$

Die Reziprozitätsabbildung wird auf endlichem Level von der Cupproduktpaarung

$$\hat{H}^0(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \times H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \longrightarrow H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

induziert, wobei der rechte Isomorphismus die Fundamentalklasse auf die 1 schickt. Da Cupprodukt mit  $H^0$  einfach Multiplikation ist, ist die endliche Reziprozitätsabbildung der Homomorphismus

$$\mathbb{Z}/n\mathbb{Z} = \hat{H}^0(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \rightarrow \text{Hom}(H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}), H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})),$$

der die 1 auf die Identität schickt. Die rechte Seite identifizieren wir kanonisch mit  $\mathbb{Z}/n\mathbb{Z}$  und damit ist die Reziprozitätsabbildung die Identität auf  $\mathbb{Z}/n\mathbb{Z}$ . Im Limes über alle  $n$  erhalten wir die natürliche Inklusion  $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$ . Dies zeigt  $rec^{\text{nr}}(x) = \text{Frob}^{v(x)}$ . Wir erhalten das kommutative Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K & \longrightarrow & K^\times & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \text{rec}|_{U_K} & & \downarrow \text{rec} & & \downarrow & & \\ 0 & \longrightarrow & T(K^{\text{ab}}|K) & \longrightarrow & G(K^{\text{ab}}|K) & \longrightarrow & G(K^{\text{nr}}|K) & \longrightarrow & 0. \end{array}$$

Bleibt zu zeigen, dass  $rec|_{U_K}$  ein topologischer Isomorphismus ist. Nun sei  $L|K$  eine endliche abelsche Erweiterung und  $I_L \subset K^\times$  die Normengruppe. Nach 1.5 sind die Normengruppen der unverzweigten Erweiterungen gerade die von der Form  $(\pi^n) \cdot U_K$ . Andererseits ist jede Untergruppe von endlichem Index, die  $U_K$

enthält von dieser Form. Daher gilt für die maximal unverzweigte Teilerweiterung  $K'$  von  $L|K$

$$I_{K'} = I_L \cdot U_k.$$

Wir erhalten das kommutative Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & I_L U_K / U_K & \longrightarrow & K^\times / I_L & \longrightarrow & K^\times / I_L U_K \longrightarrow 0 \\ & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr \\ 0 & \longrightarrow & T(L|K) & \longrightarrow & G(L|K) & \longrightarrow & G(K'|K) \longrightarrow 0. \end{array}$$

und somit einen Isomorphismus:

$$U_K / I_L \cap U_K \xrightarrow{\sim} I_L U_K / U_K \xrightarrow{\sim} T(L|K).$$

Durchläuft  $L$  alle endlichen abelschen Erweiterungen, so durchläuft  $I_L$  wegen des Existenzsatzes alle abgeschlossenen Untergruppen von endlichem Index in  $K^\times$  und  $I_L \cap U_K$  alle abgeschlossenen Untergruppen von endlichem Index in  $U_K$ . Da  $U_K$  proendlich ist, erhalten wir im projektiven Limes den Isomorphismus

$$U_K \xrightarrow{\sim} T(K^{\text{ab}}|K). \quad \square$$

**Moral:** Bezüglich der exakten Folge

$$\begin{array}{ccccccc} 0 & \longrightarrow & U_K & \longrightarrow & K^\times & \longrightarrow & \mathbb{Z} \longrightarrow 0 \\ & & \wr \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & T(K^{\text{ab}}|K) & \longrightarrow & G(K^{\text{ab}}|K) & \longrightarrow & \hat{\mathbb{Z}} \longrightarrow 0 \end{array}$$

sieht man, dass  $G(K^{\text{ab}}|K)$  aus  $K^\times$  entsteht „indem man  $\mathbb{Z}$  durch  $\hat{\mathbb{Z}}$  ersetzt“.

**Korollar 1.30.** Das Bild von  $U_K^1$  unter  $\text{rec}$  ist  $V(K^{\text{ab}}|K)$ .

*Beweis.*  $U_K^1$  bzw.  $V(K^{\text{ab}}|K)$  sind jeweils die  $p$ -Sylowuntergruppen von  $U_K$  bzw.  $T(K^{\text{ab}}|K)$ .  $\square$