Algebraische Zahlentheorie II
Sommersemester 2022

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

Inhaltsverzeichnis

1 Unendliche Galoistheorie

1.1 Proendliche Gruppen

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

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

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

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

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

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

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

Beweis. Setze für $i \geq j$:

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

1) die U_{ij} sind offene Teilmengen in $\prod T_k$
2) jede endliche Vereinigung von Mengen der Form U_{ij} ist echt kleiner als $\prod T_k$
Zu 1) ist einfach. Zu 2) wähle ein $n \in I$ größer gleich allen i, j die auftreten. Wähle $x_n \in T_n$ beliebig und setze

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

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

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

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

Definition. Eine Folge topologischer Gruppen und stetiger Homomorphismus

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

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: $\mathrm{im}(\varphi) \to \ker(\psi)$ ist dann bijektiv, stetig und abgeschlossen.

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

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

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

exakt.

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

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

zeigt man vollkommen analog wie bei R-Moduln. Für

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

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

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

Beispiel. Sei K ein lokaler Körper. Dann sind

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

(abelsche) proendliche Gruppen.

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

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

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

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

1.2 Unendliche Galoistheorie

Sei G eine Gruppe und $(U_i)_{i\in I}$ ein durch Inklusion gerichtetes System von Normalteilern (d.h. zu i, j existiert k mit $U_k \subset U_i \cap U_j$). Wir geben G die Topologie mit Basis (von 1-Umgebungen) $\{gU_i \mid g \in G,\ i \in I\}$.

Lemma 1.6. *Wir erhalten eine topologische Gruppe.*

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

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

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

Wir betrachten die Abbildungen

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

die durch

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

und

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

gegeben sind. In der Algebra-Vorlesung wurde bewiesen:

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

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

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

Wir betrachten die Familie von Normalteilern

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

Nach 1.6 erhalten wir eine Topologie auf G.

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

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

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

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

Abstrakter:

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

Behauptung: f ist ein Homöomorphismus. Es gilt:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(siehe Beweis von 1.7).
2) Sei $M|K$ endlich und $\tilde{M} \subset L$ die normale Hülle von M. Dann gilt $H = \psi(M) = \mathrm{Gal}(L|M) \supset \mathrm{Gal}(L|\tilde{M})$ und H ist offen nach 1.8. Wenden wir 1) auf $\mathrm{Gal}(L|K)$ und $\mathrm{Gal}(L|M)$ and erhalten wir mit $\tilde{H} = \psi(\tilde{M})$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

□

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

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

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

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

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

Daher erhalten wir einen Isomorphismus projektiver Systeme

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

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

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

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

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

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

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

Es gilt der folgende tiefliegende

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

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

2 Homologische Algebra (Auffrischung)

2.1 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 $\mathrm{im}(u) \to \ker(v)$ ein Isomorphismus ist.

Satz 2.1. (i) *Eine Folge $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ in $\mathcal{A}$ ist genau dann exakt, wenn für jedes $N \in \mathcal{A}$ die Folge abelscher Gruppen*

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

exakt ist.

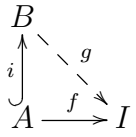
(ii) *Eine Folge* $0 \to N' \xrightarrow{u} N \xrightarrow{v} N''$ *in* $\mathcal{A}$ *ist genau dann exakt, wenn für jedes* $M \in \mathcal{A}$ *die Folge abelscher Gruppen*

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

exakt ist.

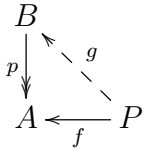
Definition. Ein Funktor zwischen abelschen Kategorien heißt **exakt**, wenn er exakte Folgen in exakte Folgen überführt.

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



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

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



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

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

Lemma 2.2. (i) *I ist genau dann injektiv, wenn der Funktor*

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

exakt ist.

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

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

2.2 Adjungierte Funktoren

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

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

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

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

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

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

$$\mathrm{Mod} - R \to \mathcal{A}b, \quad A \mapsto A \otimes_R B,$$

und

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

Dann gilt in natürlicher Weise

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

Wir erhalten die Funktorenadjunktion

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

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

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

also $G \dashv F$.

Satz 2.3. *Es seien $\mathcal{A}, \mathcal{B}$ abelsche Kategorien, $F : \mathcal{A} \to \mathcal{B}$, $G : \mathcal{B} \to \mathcal{A}$ additive Funktoren und sei $F \dashv G$ (im additiven Sinne). Dann gilt*

(i) *F ist rechtsexakt, d.h. ist $A' \to A \to A'' \to 0$ exakt in $\mathcal{A}$, so ist $FA' \to FA \to FA'' \to 0$ 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 $F^{\mathrm{op}} : \mathcal{A}^{\mathrm{op}} \to \mathcal{B}^{\mathrm{op}}$ und analog $G^{\mathrm{op}} : \mathcal{B}^{\mathrm{op}} \to \mathcal{A}^{\mathrm{op}}$. Es gilt $G^{\mathrm{op}} \dashv F^{\mathrm{op}}$. Daher genügt es (i) und (iii) zu zeigen.

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

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

exakt, also auch

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

Hieraus folgt die Exaktheit von

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

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

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

ist exakt. Nun gilt

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

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

2.3 Komplexe

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

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

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

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

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

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & A^{i-1} & \xrightarrow{d_{i-1}} & A^i & \xrightarrow{d_i} & A^{i+1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{i-1}} & & \downarrow{\scriptstyle f_i} & & \downarrow{\scriptstyle f_{i+1}} & & \\
\cdots & \longrightarrow & B^{i-1} & \xrightarrow{d_{i-1}} & B^i & \xrightarrow{d_i} & B^{i+1} & \longrightarrow & \cdots
\end{array}$$

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 $A^\bullet$.

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

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

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

Satz 2.4 (**Verallgemeinertes Schlangen-Lemma**). *Sei* $0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$ *eine kurze exakte Folge von Komplexen (d.h. für jedes* i *ist* $0 \to A^i \to B^i \to C^i \to 0$ *exakt). Dann existiert eine natürliche lange exakte Folge*

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

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

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

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 $\mathcal{A}^{\mathrm{op}}$, d.h. ein Komplex

$$\longrightarrow P^{-2} \longrightarrow P^{-1} \longrightarrow P^0 \longrightarrow 0$$

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

Beispiel. R-Mod hat genügend viele Injektive und genügend viele Projektive.

Lemma 2.5. (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

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

□

Definition. Seien $f, g : A^\bullet \to B^\bullet$ zwei Komplexhomomorphismen. f und g heißen **homotop**, wenn Homomorphismen $D^i : A^{i+1} \to B^i$ 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 2.6. *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 $f : A^\bullet \to B^\bullet$ heißt **Homotopieäquivalenz**, wenn $g : B^\bullet \to A^\bullet$ existiert mit $g \circ f \sim \mathrm{id}_A$ und $f \circ g \sim \mathrm{id}_B$.

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

Beispiel. Betrachte den Komplexhomomorphismus

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

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

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

welcher kein Quasiisomorphismus ist.

Satz 2.7. *Gegeben seien zwei Komplexe*

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

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

2.4 Abgeleitete Funktoren

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

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

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

Nach 2.8 gibt eine andere injektive Auflösung in kanonischer Weise isomorphe Gruppen $R^iF(A)$. Ist nun $\varphi : A \to B$ ein Homomorphismus und $A \to I^\bullet$ und $B \to J^\bullet$ injektive Auflösungen, so existiert nach 2.7 ein bis auf Homotopie eindeutiges $f : I^\bullet \to J^\bullet$ mit $H^0(f) = \varphi$. So wird für alle $i \in \mathbb{Z}$ die Zuordnung $A \mapsto R^iF(A)$ zu einem Funktor $\mathcal{A} \to \mathcal{B}$.

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

Lemma 2.9. *Es gilt $R^iF = 0$ für $i < 0$ und $R^0F = F$. Ist F exakt, so gilt $R^iF = 0$ für $i > 0$.*

Satz 2.10. *Für jede exakte Folge $0 \to A' \to A \to A'' \to 0$ in $\mathcal{A}$ existieren natürliche Abbildungen*

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

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

$$\cdots \to R^iFA' \to R^iFA \to R^iFA''$$
$$\to R^{i+1}FA' \to R^{i+1}FA \to R^{i+1}FA'' \to \cdots$$

exakt ist. Ist

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

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

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

Linksabgeleitete Funktoren: Man drehe alle Pfeile um:

$F : \mathcal{A} \to \mathcal{B}$ 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 $L_iF(A) := H_i(FP_\bullet)$.

– alles analog –

2.5 Azyklische Objekte

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

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

Lemma 2.11. *Injektive sind F-azyklisch.*

Satz 2.12. *Sei $A \to I^\bullet$ eine Auflösung durch F-azyklische, d.h.*

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

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

$$R^iFA \cong H^i(FI^\bullet).$$

2.6 Universelle δ-Funktoren

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

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

(i) δ 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 $0 \to A \to B \to C \to 0$ in $\mathcal{A}$ ist die lange Folge

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

exakt in $\mathcal{B}$.

Beispiel. $\mathcal{A}$ habe genügend viele Injektive und $F : \mathcal{A} \to \mathcal{B}$ sei linksexakt. Dann ist $H^n := R^nF$ ein δ-Funktor.

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

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

Bemerkung. Das bedeutet, dass sich jeder linksexakte Funktor H^0 höchstens auf eine Weise (d.h. wenn existent, dann bis auf Isomorphie eindeutig) zu einem universellen δ-Funktor ausdehnen läßt.

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

Satz 2.13. *Ein δ-Funktor $H = (H^n)_{n\geq 0}$ ist universell, wenn für jedes $n \geq 1$ der Funktor H^n auslöschbar ist.*

Korollar 2.14. *$\mathcal{A}$ habe genügend viele Injektive und $F : \mathcal{A} \to \mathcal{B}$ sei linksexakt. Dann ist $(R^nF)_{n\geq 0}$ ein universeller δ-Funktor.*

2.7 Tor und Ext

Sei R ein Ring. Wir betrachten den Bifunktor

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

Dieser ist in beiden Variablen rechtsexakt.
In Mod-R und R-Mod existieren genügend viele Projektive, also:
für jeden R-Linksmodul N existiert $L_n(- \otimes_R N) : \text{Mod-}R \to \mathcal{A}b$.
für jeden R-Rechtsmodul M existiert $L_n(M \otimes_R -) : R\text{-Mod} \to \mathcal{A}b$.

Satz 2.15. *Es gibt natürliche Isomorphismen*

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

Man nennt diesen Funktor

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

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

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

Satz 2.16.

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

und man bezeichnet diesen Funktor mit

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

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

3 Gruppenkohomologie

3.1 Der Gruppenring

Sei G eine Gruppe und A ein kommutativer Ring.

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

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

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 $f : G \to H$ induziert einen Ringhomomorphismus $A[G] \to A[H]$, $\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g f(g)$. Der Spezialfall $H = 1$ hat einen eigenen Namen:

Definition. Der Ringhomomorphismus

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

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

Lemma 3.1. *Das Augmentationsideal $I^A_G \subset A[G]$ ist als A-Modul frei über der Basis*

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

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

Beweis. Die Elemente $g-1$, $g \in G\smallsetminus\{e\}$, liegen in I^A_G und sind linear unabhängig über A. Sei $\alpha = \sum_{i=1}^{n} a_i g_i \in I^A_G$. 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 3.2. *$[G,G]$ ist ein Normalteiler in G. Die Faktorgruppe $G^{\mathrm{ab}} = G/[G,G]$ ist abelsch.*

Beweis. Für $[G,G] \lhd G$ 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 $G^{\mathrm{ab}} = G/[G,G]$ abelsch. □

Bemerkung. Der Funktor $G \mapsto G^{\mathrm{ab}}$ ist linksadjungiert zur natürlichen Inklusion $\mathcal{A}b \subset (\mathrm{Groups})$.

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

Satz 3.3. *Für $I_G = I_G^{\mathbb{Z}} \subset \mathbb{Z}[G]$ gilt $I_G/I_G^2 \cong G^{\mathrm{ab}}$.*

Beweis. Wir betrachten die Abbildung

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

Wegen $gh - 1 = (g-1) + (h-1) + \underbrace{(g-1)(h-1)}_{\in I_G^2}$
ist φ ein Gruppenhomomorphismus. Da I_G/I_G^2 abelsch ist, gilt $\varphi([G,G]) = 0$. Dies induziert $\tilde{\varphi}\colon G^{\mathrm{ab}} \to I_G/I_G^2$. Wir konstruieren die inverse Abbildung. Nach 3.1 ist I_G der freie $\mathbb{Z}$-Modul über der Menge $W = \{g-1 \mid g \neq e\}$. Die Abbildung $W \to G^{\mathrm{ab}}$, $(g-1) \mapsto g[G,G]$ setzt sich daher eindeutig zu einem Homomorphismus abelscher Gruppen $\psi\colon I_G \to G^{\mathrm{ab}}$ 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 ψ einen Homomorphismus $\tilde{\psi}\colon I_G/I_G^2 \to G^{\mathrm{ab}}$. Schließlich sind $\tilde{\psi}$ und $\tilde{\varphi}$ zueinander invers. □

3.2 G-Moduln

Definition. Ein ***G*-Links-Modul** A ist eine abelsche Gruppe A zusammen mit einer Operation $G \times A \to A$, $(g, a) \mapsto ga$ 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 $ga \overset{\text{df}}{=} ag^{-1}$ A auch als G-Linksmodul auffassen. M.a.W., es gilt

Lemma 3.4. *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 $L^\times$ $\mathrm{Gal}(L/K)$-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:

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

• Ist A ein G-Linksmodul, so wird $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ 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:** $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ 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 $\mathrm{Hom}_{\mathbb{Z}}(A, B)^G = \mathrm{Hom}_G(A, B)$

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 3.5. (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

$$\mathrm{Res}^G_U \colon G - \mathrm{Mod} \longrightarrow U - \mathrm{Mod}$$

Lemma 3.6. *Res^G_U 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

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

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

$$\mathrm{Res}^G_U \mathbb{Z}[G] \cong \bigoplus_i M_i$$

freier $\mathbb{Z}[U]$-Modul. Da Res^G_U mit der direkten Summe vertauscht, gilt Res^G_U (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 $\mathrm{Res}^G_U P$ direkter Summand im freien U-Modul $\mathrm{Res}^G_U(P \oplus Q)$, also projektiv. □

3.3 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

$$-_G \colon G - \mathrm{Mod} \longrightarrow \mathcal{A}b,\ A \longmapsto A_G,$$

rechtsexakt und es gilt

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

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

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

Wir konstruieren nun eine freie Auflösung von $\mathbb{Z}$.
Setze für $n \geq 0$:

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

mit G-Modulstruktur gegeben durch

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

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

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

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

Lemma 3.7. *$X_\bullet$ ist ein Komplex, d.h. $d \circ d = 0$.*

Beweis. Wir betrachten

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

Es gilt

$$d \circ d((g_0,\ldots,g_{n+2})) = d\left(\sum_{i=0}^{n+2}(-1)^i(g_0,\ldots,\widehat{g_i},\ldots,g_{n+2}\right)$$

$$= \sum_{j=0}^{n+1}(-1)^j \cdot \sum_{i=0}^{n+2}(-1)^i \overbrace{(g_0,\ldots,\widehat{g_i},\ldots,g_{n+2})}^{\text{hieraus die j-te Komp. entfernen}}.$$

Für $j < i$ erhalten wir

$$(g_0,\ldots,\widehat{g_j},\ldots,\widehat{g_i},\ldots,g_{n+2}) \cdot (-1)^{i+j}.$$

Für $j \geq i$

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

M.a.W.: Der Term $(g_0,\ldots,\widehat{g_a},\ldots,\widehat{g_b},\ldots,g_{n+2})$ $a<b$ taucht auf

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

Lemma 3.8. *Es ist* $\varepsilon \circ d_0 \colon X_1 \xrightarrow{d_0} X_0 = \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z}$ *die Nullabbildung.*

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

Satz 3.9. $X_\bullet \to \mathbb{Z}$ *ist eine freie Auflösung von* $\mathbb{Z}$ *als G-Modul.*

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

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

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

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

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

Wir berechnen:

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

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

$$d_0 D_0(g) + D_{-1} d_{-1}(g) = d_0((e, g)) + D_{-1}(1) = g - e + e = g.$$

Für $n \geq 1$:

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

□

Korollar 3.10. *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 3.11. *Es gilt*

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

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

$$0 = H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to$$
$$H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}) \to 0$$

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 3.3 gilt $I_G/I_G^2 \cong G^{\mathrm{ab}}$. □

Lemma 3.12. *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: $H_i(\{1\}, A) = \mathrm{Tor}_i^{\mathbb{Z}}(A, \mathbb{Z}) = 0$ 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 $\Rightarrow\ L_i(-_G) = 0 \quad \forall\, i \geq 1.$ □

3.4 Induzierte Moduln

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

Bemerkung. $\mathrm{Ind}_G : G - \mathrm{Mod} \to G - \mathrm{Mod}$ ist ein exakter Funktor.

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

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

Lemma 3.13. *Es gibt einen natürlichen Isomorphismus* $\mathrm{Ind}_G A^{\mathrm{tr}} \xrightarrow{\sim} \mathrm{Ind}_G A$.

Beweis. Als abelsche Gruppe gilt

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

Daher setzt sich die Abbildung

$$g \otimes a \longmapsto g \otimes ga$$

zu einem Homomorphismus

$$\varphi \colon \mathbb{Z}[G] \otimes A^{\mathrm{tr}} \longrightarrow \mathbb{Z}[G] \otimes A$$

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

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

Daher ist φ ein Homomorphismus von G-Moduln. □

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

Definition.

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

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 3.13 die natürliche Äquivalenz von Funktoren

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

wobei $\mathrm{Res}_{\{1\}}^G \colon G - \mathrm{Mod} \to \{1\} - \mathrm{Mod} = \mathcal{A}b$ der Vergiss-Funktor ist.

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

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

Sei OE $e \in S$. Dann identifizieren wir A mit der Untergruppe $e \cdot A \subseteq \mathrm{Ind}_G^U A$. 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 $eA \subset \mathrm{Ind}_G^U A$ als U-Modul.

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

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

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

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

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

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

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

Satz 3.14 („Frobenius-Reziprozität“)**.** *Es gilt*

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

Beide Funktoren sind exakt. Ind_G^U *überführt projektive* U*-Moduln in projektive* G*-Moduln und* Res_U^G *überführt injektive* G*-Moduln in injektive* U*-Moduln.*

Beweis. Die Adjunktion haben wir gerade bewiesen. Res_U^G ist offensichtlich exakt. $\mathrm{Ind}_G^U A = \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} A$ und weil $\mathbb{Z}[G]$ ein freier $\mathbb{Z}[U]$-Modul ist (siehe 3.6) ist auch Ind_G^U exakt. Die verbleibenden Aussagen folgen aus 2.3. □

Schließlich bemerken wir:

Lemma 3.15. *Sei* G *eine Gruppe und sei* A *ein induzierter* G*-Modul. Dann ist für jede Untergruppe* $U \subset G$ *der Modul* $\mathrm{Res}_U^G A$ *ein induzierter* U*-Modul.*

Beweis. Sei $A = \mathrm{Ind}_G B$ und nach 3.13 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. □

3.5 Homologisch triviale Moduln

Im folgenden lassen wir die Bezeichnung Res^G_U 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 3.6 ist M auch projektiver U-Modul für jedes $U \subset G$).

Satz 3.16. *Induzierte Moduln sind homologisch trivial.*

Beweis. Nach 3.15 und 3.13 g.z.z.: $H_n(G, \mathrm{Ind}_G A) = 0$ für alle $n \geq 1$ und jeden trivialen G-Modul A. Nun gilt:

$$H_n(G, \mathrm{Ind}_G A) = H_n(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}} A)$$

$$= H_n(P_\bullet \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] \otimes_{\mathbb{Z}} A) = H_n(P_\bullet \otimes_{\mathbb{Z}} A)$$

wobei $P_\bullet \to \mathbb{Z}$ eine beliebige projektive Auflösung von $\mathbb{Z}$ als G-Modul ist. Nach 3.6 ist $P_\bullet \to \mathbb{Z}$ insbesondere eine projektive Auflösung in $\mathcal{A}b$. Daher gilt für $n \geq 1$:

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

□

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

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

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

Dieses Vorgehen läßt sich verallgemeinern.

Satz 3.17 (Shapiro-Lemma)**.** *Sei $U \subset G$ eine Untergruppe und A ein U-Modul. Dann gilt*

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

für alle $n \geq 0$.

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

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

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

3.6 Restriktion und Korestriktion

Sei $U \subset G$ eine Untergruppe und A ein G-Modul. Wir konstruieren eine natürliche Abbildung $cor_G^U \colon H_n(U, A) \to H_n(G, A)$ 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 $P_\bullet \to \mathbb{Z}$ 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

$$cor_G^U \colon H_n(U, A) \longrightarrow H_n(G, A)$$

heißt die **Korestriktion(sabbildung)**.

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

$$cor_G^U \colon U^{\mathrm{ab}} = H_1(U, \mathbb{Z}) \longrightarrow H_1(G, \mathbb{Z}) = G^{\mathrm{ab}}$$

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

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

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

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

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

Nun ist die Multiplikation von rechts mit g eine Bijektion $U\backslash G \to U\backslash G$, also gilt $N((g-1)m) = 0$. Wir erhalten $N : M_G = M/I_G M \to M_U$. 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 $res^G_U \colon H_n(G, A) \to H_n(U, A)$ heißt die **Restriktion**.

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

$$\mathrm{Ver} \colon G^{\mathrm{ab}} \longrightarrow U^{\mathrm{ab}}.$$

Dieser heißt **Verlagerung**.

Ein der für die Zahlentheorie wichtiger gruppentheoretischer Satz ist der

Satz 3.18 (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*

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

die Nullabbildung.

Beweis. Siehe Neukirch: „Zahlentheorie“. □

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

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

ist die Multiplikation mit n, denn

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

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

Satz 3.19. *Für $(G \colon U) = n < \infty$ gilt $cor^U_G \circ res^G_U = n \cdot \mathrm{id}$.*

Korollar 3.20. *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 3.19 sind die Selbstabbildungen $cor_G^{\{1\}} res_{\{1\}}^G$ 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 $cor \circ res$ die Nullabbildung. Die Nullabbildung ist aber nur auf der trivialen Gruppe ein Isomorphismus. □

Korollar 3.21. (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 $i \geq 1$.

3.7 Diskrete G-Moduln

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

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

Definition. Ein abstrakter G-Modul ist ein G^{abst}-Modul.

Satz 3.22. *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 $p_1 : G \times A \to G$ 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. □

Definition. Ein diskreter G-Modul A ist ein G^{abst}-Modul A, der den äquivalenten Bedingungen von 3.22 genügt. Wir bezeichnen die Kategorie der diskreten G-Moduln mit (automatisch stetigen) G-Homomorphismen mit G-Mod.

Bemerkung. G-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 3.23. *Der Funktor*

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

ist rechtsadjungiert zur Inklusion

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

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

Beweis. Sei $A \in G$-Mod, $B \in G^{\text{abst}}$-Mod. und $f : A \to B$ 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 2.3 (ii) die Linksexaktheit von δ. Da die Inklusion G-Mod $\hookrightarrow G^{\text{abst}}$-Mod exakt ist, überführt $\bullet^\delta$ Injektive in Injektive nach 2.3 (iii). □

Korollar 3.24. *G-Mod hat genügend viele Injektive.*

Beweis. Für $A \in G$-Mod existiert ein injektives Objekt $I \in G^{\text{abst}}$-Mod und eine Inklusion $A \hookrightarrow I$. Nach 3.24 erhalten wir eine Inklusion $A = A^\delta \hookrightarrow I^\delta$ in das injektive Objekt $I^\delta \in G$-Mod. □

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.

3.8 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

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

Da G-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 $A^G = \mathrm{Hom}_G(\mathbb{Z}, A)$ gilt

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

Bemerkung. • Ist G proendlich, so hat G-Mod im allgemeinen nicht genügend viele Projektive, so dass man keine Homologie hat und auch 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

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

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

Definition. Sei $A \in G$-Mod. $\mathrm{Koind}_G A = \mathrm{Abb}\ (G, A)$ 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 $\mathrm{Koind}_G A$ wieder ein diskreter G-Modul.

Wir erhalten einen Funktor

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

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

Sei nun $H \subset G$ eine Untergruppe und $A \in H$-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 3.25. *Für $A \in G$-Mod ist $\mathrm{Koind}_G^H \mathrm{Res}_H^G A$ isomorph zum G-Modul $Abb(G/H, A)$ mit Gruppenstruktur*

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

G-Wirkung

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

Insbesondere gilt für $H = \{1\}$

$$Koind_G^{\{1\}} \mathrm{Res}^G_{\{1\}} A \cong \ Koind_G A.$$

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 3.26. *Wir haben eine Adjunktion:*

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

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

$$\begin{array}{rcl} [\varphi(f)(ga)]\,(g') & = & f(g'ga) \\ \quad \| ? & & \\ [g\varphi(f)(a)]\,(g') & = & \varphi(f)(a)(g'g) = f(g'ga) \end{array}$$

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 3.27. Koind_G^H *ist exakt und überführt Injektive in Injektive.*

Beweis. Die Exaktheit kann man schnell explizit nachrechnen. Da die Linksadjungierte Res_H^G exakt ist, werden Injektive in Injektive überführt. □

Satz 3.28. *(Shapiro-Lemma).*

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

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

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

Nun ist nach 3.27

$$\mathrm{Koind}_G^H A \to \mathrm{Koind}_G^H I^\bullet$$

eine Auflösung durch G-Injektive. □

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 Res^G_H Injektive in Injektive (3.14). Daher sind in diesem Fall Injektive kohomologisch trivial. Das gilt auch für proendliche Gruppen (siehe unten).

Lemma 3.29. *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. □

Lemma 3.30. *Ein koinduzierter G-Modul ist auch koinduzierter H-Modul für alle $H \subseteq G$.*

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

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

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

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

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

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

□

Satz 3.31.

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

Beweis. (i) Nach 3.30 gilt zu zeigen

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

Dies folgt aus

$$\mathrm{Koind}_G A \cong \mathrm{Koind}_G^{\{1\}} \mathrm{Res}^G_{\{1\}} A$$

und

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

für $i \geq 1$.
(ii) Sei I injektiv. Wir haben eine Inklusion

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

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

3.9 Der Kohomologische Standardkomplex

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

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

mit der G-Modulstruktur

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

Bemerkung.

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

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

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

Wir setzen

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

Lemma 3.32. *$d \circ d = 0$ 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. □

Korollar 3.33. *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** $D : G \to A$ 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 $\mathrm{Der}(G, A)$.

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

Beispiel. Für jedes $a \in A$ ist

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

eine Derivation wegen

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

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

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

Satz 3.34. *Es gibt einen Isomorphismus*

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

Für einen trivialen Modul A gilt

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

Insbesondere gilt für eine proendliche Gruppe G:

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

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

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

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 3.34 ist noch anzumerken, dass für eine proendliche Gruppe $G = \varprojlim_i G_i$ (mit endlichen Gruppen G_i) gilt:

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

Beweis. Wir betrachten das kommutative Diagramm

$$\begin{array}{rccc} X^0(G,A)^G = & C^0(G,A) & \xrightarrow[\varphi\mapsto\varphi(1)]{\sim} & A \\ & d^1\downarrow & & \downarrow\partial^1 \\ & C^1(G,A) & \xrightarrow[\varphi\mapsto(g\mapsto\varphi(e,g))]{\sim} & \mathrm{Abb}(G,A) \\ & d^2\downarrow & & \downarrow\partial^2 \\ & C^2(G,A) & \xrightarrow[\varphi\mapsto((g_1,g_2)\mapsto\varphi(e,g_1,g_1g_2))]{\sim} & \mathrm{Abb}(G^2,A), \end{array}$$

wobei ∂^1 und ∂^2 so gewählt sind, dass das Diagramm kommutiert.
Behauptung: (i) $\partial^1(a) = (g \mapsto ga - a)$
(ii) $\partial^2(x) = ((g_1,g_2) \mapsto g_1x(g_2) - x(g_1g_2) + x(g_1))$
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

$$\begin{aligned} (g'\varphi_a)(g) &= g'\varphi_a(g'^{-1}g) = g'^{-1}g'ga = ga. \\ d^1(\varphi_a)(g_0,g_1) &= g_1a - g_0a. \end{aligned}$$

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

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

(ii) Sei $x : G \to A \in \mathrm{Abb}(G,A)$. 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:

$$\begin{aligned} (g\cdot\varphi_x)(g_0,g_1) &= g\varphi_x(g^{-1}g_0, g^{-1}g_1) \\ &= g(g^{-1}g_0)\cdot x(g^{-1}g_0)^{-1}g^{-1}q_1) = g_0 \cdot x(g_0^{-1}g_1) \end{aligned}$$

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

Nun gilt

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

Dies bildet sich in $\mathrm{Abb}(G^2,A)$ 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:

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

Nun gilt

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

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

3.10 Funktorialität

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

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

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

$$f(\varphi(g')a) = g' f(a). \qquad (*)$$

Ein kompatibles Paar induziert Komplexhomomorphismen

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

durch

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

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: res^G_H
Sei $H \subseteq G$ eine Untergruppe und A ein G-Modul. Das kompatible Paar $(G, A) \to (H, A)$ induziert die Abbildung

$$res^G_U : H^i(G, A) \longrightarrow H^i(U, A)$$

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

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

induziert die **Inflationsabbildung**

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

Satz 3.35. *Sei $H \lhd G$ ein Normalteiler und A ein G-Modul. Dann ist die Folge*

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

exakt.

Beweis. Wir nutzen den Isomorphismus

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

1) Injektivität von inf.
Sei $D : G/H \to A^H$ eine Derivation so dass $\inf D : G \twoheadrightarrow G/H \xrightarrow{D} A^H \subset A$ inner ist, d.h. es existiert $a \in A$ mit $\inf D(g) = ga - a$ für alle $g \in G$.
Zu zeigen D ist inner. Genügt zu zeigen $a \in A^H$. Nun gilt per Konstruktion

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

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

$$\inf D(h) = 0 \quad \forall\, h \in H.$$

Folglich

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

2) $res \circ \inf = 0$.
Ist $D : G/H \to A^H$ eine Derivation, so ist

$$res \circ \inf D : H \to G \to G/H \to A^H \subset A$$

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

3) Exaktheit bei $H^1(G,A)$.
Sei $D : G \to A$ eine Derivation so dass

$$resD : H \hookrightarrow G \to A$$

inner ist, d.h. es existiert

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

Zu zeigen es existiert

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

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 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

$$D - D_a = \inf(D').$$

□

Satz 3.36. *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

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

exakt.

Beweis. Per Induktion nach n. $n = 1$ ist 3.35.
Sei $n \geq 2$. Wir betrachten die kurze exakte Folge

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

Die lange exakte Folge

$$H^i(G, \mathrm{Koind}_G A) \longrightarrow H^i(G, A') \longrightarrow H^{i+1}(G, A)$$

$$\longrightarrow H^{i+1}(G, \mathrm{Koind}_G A) \longrightarrow \cdots$$

zeigt

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

Analog

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

Also insbesondere $H^i(H, A') = 0$ für $i = 1, \ldots, n-2$.

Desweiteren gilt

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

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

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

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

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

Nach Induktionsvoraussetzung ist die untere Zeile exakt, also auch die obere. □

3.11 Die Korestriktion

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

$$\begin{array}{rcl} N : M^U & \longrightarrow & M^G \\ m & \longmapsto & \displaystyle\sum_{S \in G/U} sm \end{array}$$

Angewendet auf eine kohomologisch triviale Auflösung $A \to I$ gibt dies die Abbildung

$$cor_G^U : H^i(U, A) \longrightarrow H^i(G, A), \quad i \geq 0.$$

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

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

Analog wie bei Homologie erhalten wir

Lemma 3.37.

$$cor_G^U \circ res_U^G = (G : U).$$

Korollar 3.38. *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*

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

3.12 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

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

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**

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

Nun nehmen wir an:
$H \triangleleft G$, also $H^g = H$ und $B = A$, also $gB = A$ und erhalten die Abbildung

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

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

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

zum G-Modul.

Satz 3.39. *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 $A \to I^\bullet$ aus dem Spezialfall H^0. □

3.13 Das Cup-Produkt

Seien A, B G-Moduln. Die natürliche Abbildung

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

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

Satz 3.40. *Für das Differential ∂ in den verschiedenen Standardkomplexen gilt*

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

Beweis. Es gilt

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

Desweiteren

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

und

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

In der zu beweisenden Formel

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

bleibt stehen:

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

□

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 $A \times B \to C$ eine bilineare Paarung, so wird ein Homomorphismus. $A \otimes B \to C$ 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 $A^G \times B^G \to (A \otimes B)^G$
– es gelten die Eigenschaften, die wir gleich nachweisen werden.

Lemma 3.41. *Für Homomorphismen $A \to A'$, $B \to B'$ 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 3.42. (i) *Seien $0 \to A' \to A \to A'' \to 0$ und $0 \to C' \to C \to C'' \to 0$ exakte Folgen von G-Moduln. Sei B ein weiterer G-Modul und sei $A \times B \to C$ eine bilineare Paarung, die Paarungen $A' \times B \to C'$ und $A'' \times B \to C$ induziert. Dann ist das Diagramm*

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

kommutativ, d.h. $\delta(a'' \cup \beta) = \delta a'' \cup \beta$.
(ii) *Seien $0 \to B' \to B \to B'' \to 0$ und $0 \to C' \to C \to C'' \to 0$ exakte Folgen von G-Moduln und sei $A \times B \to C$ eine Paarung, die Paarungen $A \times B' \to C'$ und $A \times B'' \to C''$ induziert. Dann kommutiert das Diagramm*

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

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

Beweis. Wir zeigen (ii): Sei $\alpha = \overline{a}$, $a \in Z^p(G,A)$, $\beta'' = \overline{b''}$, $b'' \in Z^q(G,B'')$. 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 3.40

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

Übergang zu Kohomologie gibt

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

□

Wir machen die Identifikationen

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

Satz 3.43. *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*

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

Beweis. Seien a, b, c Kozyklen, die α, β, γ repräsentieren. Dann gilt

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

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

$$(\mathrm{Koind}_G A) \otimes B \to \mathrm{Koind}_G(A \otimes B), \; f \otimes b \mapsto [g \mapsto f(g) \otimes b]$$

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

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

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:

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

Dann haben wir eine Surjektion:

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

und Isomorphismen:

$$H^1(G, A_{n-1}) \underset{\delta}{\overset{\sim}{\to}} H^2(G, A_{n-2}) \underset{\delta}{\overset{\sim}{\to}} \dots \underset{\delta}{\overset{\sim}{\to}} H^n(G, A_0).$$

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

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

Nach 3.42 ((i) p mal und (ii) q mal angewendet) erhalten wir ein kommutatives Diagramm

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

andersherum:

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

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

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

Wir betrachten die Paarung

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

Diese induziert das Cup-Produkt

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

Satz 3.44. *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*

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

ist exakt.

Dann ist das Diagramm

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

kommutativ, d.h.

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

für

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

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

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

und analog

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

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. □

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. $\mathrm{Proj}(H^{2*}(G,k))$ ist die assoziierte Kohomologie-Varietät über k.

3.14 Proendliche Gruppen – Reduktion auf endliche Gruppen

Satz 3.45. *Sei G eine proendliche Gruppe und A ein diskreter G-Modul. Dann existiert ein natürlicher Isomorphismus*

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

wobei U die offenen Normalteiler in G durchläuft.

Konstruktion der Abbildung: Für offene Normalteiler $V \lhd U \lhd G$ 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 3.45. Es ist bereits die natürliche Abbildung

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

ein Isomorphismus von Komplexen. Die Injektivität ist klar. Sei $x : G^{n+1} \to A$ 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 $x : G^{n+1} \twoheadrightarrow (G/U_0)^{n+1} \to A$.
Behauptung: $\mathrm{im}(x) \subset A^{U_0}$.

Grund: Für $u_0 \in U_0$ gilt

$$\begin{array}{rcl} (u_0x)(g_0,\ldots,g_n) & = & u_0 \cdot x(u_0^{-1}g_0,\ldots,u_0^{-1}g_n) \\ \| & = & u_0x(g_0,\ldots,g_n) \\ x(g_0,\ldots,g_n) & & \end{array}$$

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

$$\begin{array}{rcl} \varinjlim\limits_U H^n(G/U, A^U) & \cong & H^n\left(\varinjlim\limits_U C^\bullet(G/U, A^U)\right) \\ & = & H^n(C^\bullet(G,A)) = H^n(G,A). \end{array}$$

□

Korollar 3.46. *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 3.37

$$cor_G^U \circ res_U^G = (G:U).$$

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

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

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 3.45 auch $H^n(G,A)$.

□

Korollar 3.47. *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: $((G,U), \mathrm{ord}(a)) = 1$.

Korollar 3.48. *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

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

□

3.15 Abstrakte Gruppen – Beziehung zwischen Homologie und Kohomologie

Sei G eine abstrakte Gruppe.

Lemma 3.49. *Sei B eine abelsche Gruppe. Dann überführt der Funktor*

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

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 3.50.

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

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

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

□

4 Kohomologie endlicher Gruppen

Im ganzen Kapitel sei G stets eine endliche Gruppe.

4.1 Tate-Kohomologiegruppen

Lemma 4.1. *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

$$\begin{array}{rcl} \mathrm{Koind}_G A & \longrightarrow & \mathrm{Ind}_G A \\ \| & & \| \\ \mathrm{Abb}(G, A) & \longrightarrow & \mathbb{Z}[G] \otimes A \\ x & \longmapsto & \sum\limits_{g \in G} g \otimes x(g^{-1}) \end{array}$$

ist ein Isomorphismus von G-Moduln. □

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

Definition. Die Gruppen

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

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

Lemma 4.2. *Für einen (ko)induzierten Modul A gilt*

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

d.h. $\bar{N}_G : A_G \to A^G$ 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 $\hat{H}_0(G, A) = 0$. □

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

$$\begin{array}{rcl} C \otimes A & \xrightarrow{\sim} & \mathrm{Hom}(C^+, A),\ c \otimes a \longmapsto (f \longmapsto f(c) \cdot a) \\ C^+ \otimes A & \xrightarrow{\sim} & \mathrm{Hom}(C, A),\ f \otimes a \longmapsto (c \longmapsto f(c) \cdot a). \end{array}$$

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 $\mathrm{Ind}_G C$ und somit nach 3.49 für jeden G-Modul A der Modul $\mathrm{Hom}(C, A)$ direkter Summand in einem (ko)induzierten Modul. Nach 4.2 erhalten wir somit Isomorphismen

$$(C^+ \otimes A)_G \xrightarrow{\sim} \mathrm{Hom}(C, A)_G \underset{\sim}{\xrightarrow{\bar{N}_G}} \mathrm{Hom}(C, A)^G. \qquad (*)$$

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 3.49). 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

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

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 4.3. *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 $(*)$

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

Nun schauen wir die Mitte an:

$$\begin{array}{ccccc} \mathrm{Hom}(P_{-2}, A)^G & \to & \mathrm{Hom}(P_{-1}, A)^G & \overset{(\varepsilon^+ \circ \varepsilon)^*}{\to} & \mathrm{Hom}(P_0, A)^G \to \mathrm{Hom}(P_1, A)^G \\ \| \wr & & \| \wr & \nearrow \varphi & \\ (P_1 \otimes A)_G & \to & (P_0 \otimes A)_G & & . \end{array}$$

Nach Konstruktion der vertikalen Isomorphismen kommutiert das Diagramm

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

Daher faktorisiert φ in der Form

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

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

Korollar 4.4. *Sei A ein (ko)induzierter G-Modul. Dann gilt*

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

Satz 4.5. *Sei $0 \to A' \to A \to A'' \to 0$ 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

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

die exakte Folge von Komplexen.

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

Die assoziierte lange exakte Kohomologiefolge zeigt das gewünschte. □

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

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

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

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

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 $(g_0, \ldots, g_n) \in G^{n+1}$ das Element $\varphi_{g_0,\ldots,g_n} \in \mathbb{Z}[G^{n+1}]^+$ gegeben durch

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

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

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

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

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

gilt. Wir rechnen das nach:

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

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

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

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

und

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

mit den Differentialen:
$n \geq 1$:

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

und ∂_0:

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

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

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

4.2 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 $res : H^0(G, A) \to H^0(H, A)$ 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 $H \setminus G$ 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: $res : H_0(G, A) \to H_0(H, A)$ ist definiert durch $a \mapsto \sum_{s \in H \setminus G} sa$.

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

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

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

Analog setzt sich die Abbildung

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

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

Satz 4.7. *cor ist ein Homomorphismus von δ-Funktoren.*

Satz 4.8. *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 3.42) 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

$$\begin{array}{ccccc} \hat{H}^p(G, A) & \times & \hat{H}^q(G, B) & \stackrel{\cup}{\longrightarrow} & \hat{H}^{p+q}(G, A \otimes B) \\ \big| \wr & & \big| \wr & & \big| \wr \, (-1)^{pq} \\ \hat{H}^0(G, A_p) & \times & \hat{H}^0(G, B_q) & \stackrel{\cup}{\longrightarrow} & \hat{H}^{p+q}(G, A_p \otimes B_q). \end{array}$$

Beachte

$$\begin{array}{rcl} \hat{H}^{p+q}(G, A \otimes B) & \cong & \hat{H}^p(G, (A \otimes B)_q) \cong \hat{H}^p(G, A \otimes B_q) \\ & \cong & \hat{H}^0(G, (A \otimes B_q)_p) \cong \hat{H}^0(G, A_p \otimes B_q). \end{array}$$

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 4.9. *Sei $H \subset G$ eine Untergruppe und A ein H-Modul. Dann gilt*

$$\hat{H}^n(H, A) \cong \hat{H}^n(G, \mathrm{Ind}_G^H A)$$

für alle $n \in \mathbb{Z}$.

Beweis. Lassen wir weg. □

4.3 Kohomologie der zyklischen Gruppen

Sei G eine zyklische Gruppe der Ordnung n und $\sigma \in G$ ein Erzeuger. Setze

$$N_G A = \mathrm{im}(N_G : A \to A),$$
$$_{N_G}A = \ker(N_G : A \longrightarrow A).$$

Dann gilt nach Definition:

$$\hat{H}^0(G, A) = A^G/N_G A,\ \hat{H}^{-1}(G, A) = {}_{N_G}A/I_G A.$$

Wegen

$$\sigma^i - 1 = (\sigma - 1)(\sigma^{i-1} + \cdots + 1)$$

gilt $I_G A = (\sigma - 1) \cdot A$.

Satz 4.10. *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

$$(*) \qquad 0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} \mathbb{Z}[G] \xrightarrow{\cdot(\sigma-1)} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

wobei ε die Augmentation $\Sigma\ a_i\sigma^i \mapsto \Sigma\ a_i$ 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 χ 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

$$\begin{array}{ccc} \hat{H}^n(G,A) & = & \hat{H}^n(G,A) \\ \downarrow \cdot m & & \chi\cup \downarrow \\ \hat{H}^n(G,A) & \xrightarrow[\delta^2]{\sim} & \hat{H}^{n+2}(G,A) \end{array}$$

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. □

Bemerkung. Nach Wahl eines Erzeugers σ 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 4.11. *Sei G endlich zyklisch. Ist $0 \to A \to B \to C \to 0$ 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 $\hat{H}^0(G,C) \to \hat{H}^{-1}(G,A)$. 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 4.10. Dieser hängt von der Wahl eines Erzeugers σ 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. □

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 σ ein Erzeuger von G und $D = \sigma - 1 : A \to A$. Dann gilt $D \circ N_G = 0 = N_G \circ D$ und

$$\begin{aligned} \hat{H}^0(G, A) &= \ker(D)/\mathrm{im}(N_G) \\ \hat{H}^{-1}(G, A) &= \ker(N_G)/\mathrm{im}(D) \end{aligned}$$

Satz 4.12. *Sei $0 \to A \to B \to C \to 0$ 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 4.11. □

Satz 4.13. *Ist A endlich, so gilt*

$$h(G, A) = 1.$$

Beweis. Der Homomorphiesatz liefert

$$\#\ker(D) \cdot \#\mathrm{im}(D) = \#A = \#\ker(N_G) \cdot \#\mathrm{im}(N_G).$$

Dies zeigt

$$\frac{\#\hat{H}^0(G, A)}{\#\hat{H}^1(G, A)} = 1$$

□

4.4 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 4.14. *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 4.15.

(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 4.14 haben wir eine Injektion

$$\hat{H}^n(G, A) \to \bigoplus_p \hat{H}^n(G_p, A).$$

Daher gilt

$$\hat{H}^n(G_p, A) = 0 \quad \forall\, p \Longrightarrow \hat{H}^n(G, A) = 0.$$

(ii) Aus (i) folgt A kohomologisch trivialer G_p-Modul $\forall\, p \Longrightarrow A$ kohomologisch trivialer G-Modul.

Die andere Richtung ist trivial, weil eine Untergruppe von G_p auch eine Untergruppe von G ist. □

Satz 4.16. *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 $H^0(G, A) = 0 \Longrightarrow A = 0$ annehmen, dass A endlich ist. Das Komplement $A \smallsetminus A^G$ ist disjunkte Vereinigung von nichttrivialen G-Bahnen Ga, $a \in A \smallsetminus A^G$. Es gilt: $\#Ga = \#(G/G_a)$, wobei G_a die Standgruppe von a ist. Daher gilt

$$p \mid \#Ga \quad \forall\, a \in A \smallsetminus A^G.$$

Daher gilt $p \mid \#(A \smallsetminus A^G)$. Gilt nun $A^G = 0$ so folgt $\#A \equiv 1 \bmod p$. 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 $A^* = 0 \Longrightarrow A = 0$. 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 $\mathrm{Hom}(A, V)$ für jeden Modul A ein induzierter Modul, denn

$$\mathrm{Hom}(A, \Lambda) = \mathrm{Hom}(A, \mathbb{F}_p[G]) = \mathrm{Hom}(A, \mathbb{F}_p) \otimes_{\mathbb{Z}} \mathbb{Z}[G].$$

Daher besteht die exakte Folge

$$0 \longrightarrow \mathrm{Hom}(A/A^G, V) \longrightarrow \mathrm{Hom}(A, V) \longrightarrow \mathrm{Hom}(A^G, V) \longrightarrow 0$$

aus induzierten G-Moduln und folglich ist

$$\mathrm{Hom}_G(A, V) \longrightarrow \mathrm{Hom}_G(A^G, V) = \mathrm{Hom}(A^G, V^G)$$

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 $j : A \to V$ ausdehnt. j ist injektiv wegen $\ker(j)^G = \ker(j|_{A^G}) = 0$ und (i). Nun setze $C = \mathrm{coker}(j)$. Wir erhalten eine exakte Folge

$$0 \longrightarrow A^G \xrightarrow{\sim} V^G \longrightarrow C^G \longrightarrow H^1(G, A).$$

Daher gilt:

$$H^1(G, A) = 0 \Longrightarrow C^G = 0 \Longrightarrow C = 0 \Longrightarrow j \text{ ist Isomorphismus}$$

$$\Longrightarrow A \cong V = \bigoplus_I \mathbb{F}_p[G] = \mathrm{Ind}_G \left(\bigoplus_I \mathbb{F}_p \right).$$

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 $0 \subsetneqq B \subsetneqq A$ gibt.

Lemma 4.17. *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. $A \xrightarrow{\cdot p} A$ nicht surjektiv ist. Daher gilt $pA \subsetneqq A$, also $pA = 0$. Die Eindeutigkeit von p ist klar, da aus $qA = 0$ für ein $q \neq p$ folgen würde $A = 0$. □

Satz 4.18. *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 4.17 gilt $pA = 0$. Wegen $A \neq 0$ und A einfach folgt $A^G = A$ ($A^G = 0$ würde nach 4.16 $A = 0$ implizieren). Daher ist A ein $\mathbb{F}_p$-Vektorraum mit trivialer G-Wirkung. Da A einfach ist, folgt $\dim_{\mathbb{F}_p} A = 1$. □

Da jeder endliche G-Modul A eine Kompositionsreihe $0 = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_n = A$ mit A_i/A_{i-1} einfach für $i = 1, \ldots, n$ besitzt (siehe Algebra-Vorlesung) erhalten wir

Korollar 4.19. *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 4.20. *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

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

Beweis. Sei $0 \to R \to F \to A \to 0$ 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

$$\hat{H}^{n_p}(G_p, A) = 0 = \hat{H}^{n_p+1}(G_p, A),\ \hat{H}^i(G_p, F) = 0 \quad \forall\, i \in \mathbb{Z}$$

und der langen exakten Folge erhalten wir

$$\hat{H}^{n_p+1}(G_p, R) = 0 = \hat{H}^{n_p+2}(G_p, R). \tag{2}$$

Die exakte Folge

$$0 \longrightarrow R \xrightarrow{\cdot p} R \longrightarrow R/pR \longrightarrow 0 \tag{3}$$

gibt uns

$$\hat{H}^{n_p+1}(G_p, R/pR) = 0.$$

Nach 4.16 (ii) ist R/pR induziert. Dies zeigt die Behauptung.

Wir nehmen nun an, dass A $\mathbb{Z}$-frei ist. Dann ist $\mathrm{Ext}^1(A, A) = 0$ und Anwenden von $\mathrm{Hom}(A, -)$ auf die kurze exakte Folge $0 \to R \to F \to A$ liefert die kurze exakte Folge

$$0 \longrightarrow \mathrm{Hom}(A, R) \longrightarrow \mathrm{Hom}(A, F) \longrightarrow \mathrm{Hom}(A, A) \longrightarrow 0.$$

Wäre $H^1(G, \mathrm{Hom}(A, R)) = 0$, so wäre $\mathrm{Hom}_G(A, F) \to \mathrm{Hom}_G(A, A)$ surjektiv und ein Urbild von id_A in $\mathrm{Hom}_G(A, F)$ realisiert A als direkten Summanden in F.

Daher genügt zu zeigen: $H^1(G, M) = 0$ für $M = \mathrm{Hom}(A, R)$. Aus (3) erhalten wir die exakte Folge

$$0 \longrightarrow M \xrightarrow{\cdot p} M \longrightarrow \mathrm{Hom}(A, R/pR) \longrightarrow 0.$$

Daher ist $M/pM = \mathrm{Hom}(A, R/pR)$ ein induzierter G_p-Modul. Dies impliziert, dass

$$H^1(G_p, M) \xrightarrow{\cdot p} H^1(G_p, M)$$

ein Isomorphismus ist, also $H^1(G_p, M) = 0$ für alle p. Nach 4.15 (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 4.21. *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* $\mathrm{Hom}(A, B)$ *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 4.20 direkter Summand in einem freien $\mathbb{Z}[G]$-Modul F'. Folglich ist $\mathrm{Hom}(R, B)$ direkter Summand im induzierten G-Modul $\mathrm{Hom}(F', B)$ und daher kohomologisch trivial. Da B teilbar ist, ist die Folge

$$0 \longrightarrow \mathrm{Hom}(A, B) \longrightarrow \mathrm{Hom}(F, B) \longrightarrow \mathrm{Hom}(R, B) \longrightarrow 0$$

exakt und da die letzten beiden Moduln kohomologisch trivial sind, gilt dies auch für $\mathrm{Hom}(A, B)$. Der Fall dass A $\mathbb{Z}$-frei und B kohomologisch trivial ist wird analog behandelt. □

5 Galoiskohomologie

Wir untersuchen Kohomologie der additiven und der multiplikativen Gruppe des separablen Abschlusses als Modul unter der absoluten Galoisgruppe.

5.1 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

$$\begin{array}{rcl} \varphi^* : G_2 = G(\overline{K}_2/K) & \xrightarrow{\sim} & G_1 = G(\overline{K}_1/K), \\ \sigma & \longmapsto & \varphi^{-1} \circ \sigma \circ \varphi. \end{array}$$

Nun sei $\dagger \in \{+, \times\}$. Dann ist $\overline{K}_i^\dagger$ ein diskreter $G(\overline{K}_i/K)$-Modul, $i = 1, 2$. Das Paar $\varphi^* : G_2 \xrightarrow{\sim} G_1$, $\varphi : \overline{K}_1 \to \overline{K}_2$ 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

$$\begin{array}{ccc} H^i(G_1, \overline{K}_1^\dagger) & \xrightarrow{(\varphi^*, \varphi)} & H^i(G_2, \overline{K}_2^\dagger) \\ \| & & \downarrow {\scriptstyle ((\varphi' \circ \varphi^{-1})^*, \varphi' \circ \varphi^{-1})} \\ H^i(G_1, \overline{K}_1^\dagger) & \xrightarrow{(\varphi'^*, \varphi')} & H^i(G_2, \overline{K}_2^\dagger) \end{array}$$

Nun ist $(\varphi' \circ \varphi^{-1})^*$ ein innerer Automorphismus von G_2, also gilt nach 3.39:

$$((\varphi' \circ \varphi^{-1})^*, \varphi' \circ \varphi^{-1}) = \mathrm{id}_{H^i(G_2, \overline{K}_2^\dagger)}.$$

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

$$\begin{array}{rcl} H^i(K, \mathbb{G}_a) & = & H^i(G(\overline{K}/K), \overline{K}^+) \\ H^i(K, \mathbb{G}_m) & = & H^i(G(\overline{K}/K), \overline{K}^\times). \end{array}$$

5.2 Additive Theorie

Satz 5.1. *Sei $L|K$ eine Galoiserweiterung mit Gruppe G. Dann gilt*

$$H^i(G, L^+) = 0 \qquad \forall\, i \geq 1.$$

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. □

Korollar 5.2. *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. □

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(!)
$$\begin{array}{rcl} \wp : \overline{K} & \longrightarrow & \overline{K} \\ x & \longmapsto & x^p - x \end{array}$$
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 5.1 erhalten wir

Korollar 5.3. *(„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
$$H^1(G_K, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(G_K, \mathbb{Z}/p\mathbb{Z}).$$
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.

5.3 Multiplikative Theorie – Hilberts Satz 90

Satz 5.4. *(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 $a : G \to L^\times$ 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

$$L^\times \to L^\times, \quad c \mapsto gc$$

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:

$$\begin{aligned} \tau(b) &= \sum_{g \in G} \tau(a(g)) \cdot \tau g(c) \\ &= \sum_{g \in G} a(\tau)^{-1} a(\tau g) \cdot \tau g(c) \\ &= a(\tau)^{-1}\, b. \end{aligned}$$

$\rightsquigarrow \quad a(\tau) = b/\tau(b) \quad \forall\, \tau \rightsquigarrow \quad a$ ist innere Derivation. □

Korollar 5.5 (klassischer Hilbertscher Satz 90)**.** *Sei $L|K$ eine endliche Galoiserweiterung mit zyklischer Gruppe G. Sei σ 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 $\Longrightarrow$

$$\hat{H}^{-1}(G, L^\times) \cong H^1(G, L^\times) = 0.$$

Es folgt $\ker(N_G) = I_G L^\times = (1 - \sigma) \cdot L^\times$. □

Sei n eine natürliche Zahl prim zu $\mathrm{char}(K)$. Dann ist das Polynom $x^n - a$ für jedes $a \in \overline{K}^\times$ separabel, also der Homomorphismus $\overline{K}^\times \xrightarrow{\cdot n} \overline{K}^\times$, $x \mapsto x^n$, surjektiv. Wir erhalten eine exakte Folge (die „Kummer-Folge“) von G_K-Moduln

$$0 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow{\cdot n} \overline{K}^\times \longrightarrow 0.$$

Nach Hilberts Satz 90 folgt

Korollar 5.6 („Kummer-Theorie“)**.**

$$H^1(G_K, \mu_n) \cong K^\times / K^{\times n}.$$

Nun nehmen wir an, dass eine primitive n-te Einheitswurzel ζ_n in K liegt.

Wir erhalten einen Isomorphismus von G_K-Moduln

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mu_n, \quad 1 + n\mathbb{Z} \longmapsto \zeta_n,$$

und folglich einen (von der Wahl von ζ 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 $\overline{x} \in K^\times / K^{\times n}$ sei $\varphi_{\overline{x}} : G_K \to \mathbb{Z}/n\mathbb{Z}$ der assoziierte Homomorphismus. $U_{\overline{x}} := \ker(\varphi_{\overline{x}}) \subset G_K$ ist ein offener Normalteiler und es gilt

$$\begin{array}{rcl} G_K/U_{\bar{x}} \xrightarrow{\sim} & \frac{n}{d}\mathbb{Z}/n\mathbb{Z} \subset \mathbb{Z}/n\mathbb{Z} \\ & \wr| \\ & \mathbb{Z}/d\mathbb{Z} \end{array}$$

für einen Teiler $d \mid n$. Nun gilt

$$\overline{K}^{U_{\overline{x}}} = K\left(\sqrt[n]{x}\right)$$

wobei $x \in K^\times$ ein Vertreter von $\overline{x} \in K^\times / K^{\times n}$ ist. Der zu $\frac{n}{d} + n\mathbb{Z}$ zugehörige Erzeuger der zyklischen Gruppe $G_K/U_{\bar{x}}$ ist der Körperautomorphismus

$$\begin{array}{rcl} K\left(\sqrt[n]{x}\right) & \longrightarrow & K\left(\sqrt[n]{x}\right), \\ \sqrt[n]{x} & \longmapsto & \zeta_n^{\frac{n}{d}} \cdot \sqrt[n]{x}. \end{array}$$

D.h: Der Körper zu $\overline{x} \in K^\times/K^{\times n}$ ist kanonisch, der assoziierte Erzeuger der zyklischen Gruppe $G\left(K\left(\sqrt[n]{x}\right)|K\right)$ hängt von der Wahl der primitiven Einheitswurzel ζ_n ab.

Übungsaufgabe: Man verifiziere diese Behauptungen und überlege sich, wie die Situation im Fall der Artin-Schreier-Theorie

$$\mathrm{Hom}(G_K, \mathbb{Z}/p\mathbb{Z}) \Longrightarrow K/\wp K, \quad p = \mathrm{char}(K) > 0$$

aussieht.

5.4 Multiplikative Theorie – die Brauergruppe

Definition. Sei $L|K$ eine Galoiserweiterung mit Gruppe G. Die Gruppe

$$Br(L|K) = H^2(G, L^\times).$$

heißt **relative Brauergruppe** von L/K und

$$Br(K) = Br(\overline{K}|K) = H^2(G_K, \overline{K}^\times)$$

heißt die **(absolute) Brauergruppe** von K.

Erinnerung: Ist G eine Gruppe, $H \subset G$ ein Normalteiler und A ein G-Modul mit $H^i(H, A) = 0$, $i = 1, \ldots, n-1$, so haben wir eine exakte Folge

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

Ist nun $M|L|K$ ein Turm von Galoiserweiterungen und $A = M^\times$, so folgt mit Hilberts Satz 90, dass die Inflation

$$Br(L|K) \longrightarrow Br(M|K)$$

injektiv ist. Wir können die Formel

$$H^2(G_K, \overline{K}^\times) = \varinjlim_{K \subseteq L \subset \overline{K}} H^2(G(L|K), L^\times)$$

daher in der Form

$$Br(K) = \varinjlim_{K \subseteq L \subset \overline{K}} Br(L|K) = \bigcup_{K \subseteq L \subset \overline{K}} Br(L|K)$$

schreiben. Die obige exakte Folge liest sich

$$0 \longrightarrow Br(L|K) \longrightarrow Br(K) \longrightarrow Br(L).$$

Definition. Man sagt, dass ein $x \in Br(K)$ in einer Erweiterung $L|K$ **zerfällt**, wenn das Bild von x in $Br(L)$ gleich 0 ist.

Bemerkungen. Ist $L|K$ galoissch, so besteht $Br(L|K)$ gerade aus den $x \in Br(K)$, die über L zerfallen.

– Jedes $x \in Br(K)$ zerfällt in einer endlichen Erweiterung.

Zwischenbemerkung: Woher die Terminologie? Es gibt einen Isomorphismus

$$Br(K) \cong \left\{ \begin{array}{l} \text{endlich-dimensionale zentrale} \\ \text{einfache } K - \text{Algebren} \end{array} \right\} / \text{gewisse Äquivalenzrelation } \sim$$

Ein $A \in Br(K)$ zerfällt über L wenn $A \otimes_K L \sim M_n(L)$ für ein n.
Trivialerweise gilt falls $K = \overline{K}$:

$$Br(K) = H^2(G_K, \overline{K}^\times) = H^2(\{1\}, \overline{K}^\times) = 0.$$

Satz 5.7. *Sei K ein endlicher Körper. Dann gilt $Br(K) = 0$.*

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.

5.5 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

$$inv_K : Br(K) \to \mathbb{Q}/\mathbb{Z},$$

der sogenannten *Invariantenabbildung*.

Lemma 5.8. *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 5.9. *Sei L/K eine endliche zyklische Erweiterung und $G = \mathrm{Gal}(L/K)$. Dann gilt*

$$\mid \hat{H}^n(G, L^\times) \mid = \begin{cases} [L:K], & n \text{ gerade} \\ 1 & n \text{ ungerade} \end{cases}$$

Insbesondere ist $\mid Br(L|K) \mid = [L:K]$.

Beweis. Nach Satz 4.10 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 is $\mid \hat{H}^1(G, L^\times) \mid = 1$ Es reicht also zu zeigen, dass der Herbrandindex

$$h(G, L^\times) = \frac{\mid \hat{H}^0(G, L^\times) \mid}{\mid \hat{H}^1(G, L^\times) \mid}$$

gleich $[L:K]$ ist.

Sei σ in Erzeuger von G und es sei $|G| = n$ also $G = \{1, \sigma, \ldots, \sigma^{n-1}\}$. Nach dem Satz vom primitiven Element gibt es $a \in L^\times$ mit $L = K(a)$. Dann ist $\{\sigma^i a\}_{i=1,\ldots n-1}$ 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 π_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

$$0 \to A_i/A_{i+} \to A_0/A_{i+1} \to A_0/A_i \to 0$$

und Induktion schließen wir, dass A_0/A_i für alle i kohomologisch trivial ist. Wegen Lemma 5.8 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 4.12), bekommen wir aus der exakten Folge

$$0 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0$$

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 4.13). 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 5.10. *Sei L/K eine unverzweigte Erweiterung und $G = \mathrm{Gal}(L/K)$. Dann sind $\mathcal{O}_L^\times$ und $U_L^{(1)}$ kohomologisch triviale G-Moduln.*

Beweis. Für eine abgeschlossene Untergruppe $H \subseteq G$ ist

$$H^i(H, \mathcal{O}_L^\times) = H^i(\mathrm{Gal}(L/L^H), \mathcal{O}_L^\times) = \varprojlim_{L/M/L^H} H^i(\mathrm{Gal}(M/L^H), \mathcal{O}_M^\times),$$

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 ℓ/k die zu L/K gehörige Restklassenkörpererweiterung. Wir betrachten die Filtrierung

$$\ldots \subset U_L^{(2)} \subset U_L^{(1)} \subset \mathcal{O}_L^\times$$

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 $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(\ell/k)$. Damit ist $U_L^{(i-1)}/U_L^{(i)}$ induziert, also kohomologisch trivial. Per Induktion folgt mithilfe der exakten Folge

$$1 \to U_L^{(i-1)}/U_L^{(i)} \to U_L^{(1)}/U_L^{(i)} \to U_L^{(1)}/U_L^{(i-1)} \to 1,$$

dass $U_L^{(1)}/U_L^{(i)}$ kohomologisch trivial ist für alle $i \geq 1$ und damit nach Lemma 5.8 auch $U_L^{(1)}$.

Um einzusehen, dass $\mathcal{O}_L^\times$ kohomologisch trivial ist, untersuchen wir die exakte Folge

$$1 \to U_L^{(1)} \to \mathcal{O}_L^\times \to \ell^\times \to 1.$$

Wir wissen schon, dass $U_L^{(1)}$ kohomologisch trivial ist. Außerdem ist $\ell^\times$ kohomologisch trivial, denn $H^1(G, \ell^\times) = H^1(\mathrm{Gal}(\ell/k), \ell^\times) = 0$ 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 4.13). 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. □

Korollar 5.11. *Sei L/K eine endliche unverzweigte Erweiterung. Dann ist die Norm*

$$N_{L/K} : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$$

surjektiv.

Beweis. Weil $\mathcal{O}_L^\times$ kohomologisch trivial ist, gilt

$$0 = \hat{H}^0(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) = \mathcal{O}_K^\times / N_{L/K}\mathcal{O}_L^\times.$$

□

Für eine unverzweigte Erweiterung L/K mit Galoisgruppe $G = \mathrm{Gal}(L/K)$ und Bewertung $v : L^\times \to \mathbb{Z}$ konstruieren wir nun die Invariantenabbildung

$$inv_{L/K} : Br(L/K) \to \mathbb{Q}/\mathbb{Z}.$$

Die exakte Folge

$$1 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v} \mathbb{Z} \to 0$$

diskreter G-Moduln gibt uns wegen der kohomologischen Trivialität von $\mathcal{O}_L^\times$ einen Isomorphismus

$$Br(L/K) = H^2(G, L^\times) \xrightarrow{\sim} H^2(G, \mathbb{Z}).$$

Nun betrachten wir die exakte Folge

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0.$$

Weil $\mathbb{Q}$ eindeutig teilbar ist, ist es kohomologisch trivial und wir erhalten einen Isomorphismus

$$H^2(G, \mathbb{Z}) \xleftarrow{\sim} H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$

Weil L/K unverzweigt ist, haben wir $G = \mathrm{Gal}(\ell/k)$ und $\mathrm{Gal}(\ell/k)$ wird topologisch erzeugt vom Frobeniusautomorphismus, der $x \in \ell$ auf x^q schickt, wobei $q = \#k$. Es gibt also einen eindeutig bestimmten Frobeniusautomorphismus $\mathrm{Frob}_{L/K}$ auf L, der den Frobeniusautomorphismus auf ℓ induziert und dieser ist ein topologischer Erzeuger der Gruppe G. Wir definieren

$$\eta : H^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}, \qquad \varphi \mapsto \varphi(\mathrm{Frob}_{L/K}).$$

Diese Abbildung ist injektiv, da $\mathrm{Frob}_{L/K}$ die Gruppe G topologisch erzeugt und mit $\mathrm{Hom}(G, -)$ die stetigen Homomorphismen gemeint sind.

Definition. Die Komposition

$$inv_{L/K} : Br(L/K) = H^2(G, L^\times) \cong H^2(G, \mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

heißt Invariantenabbildung.

Lemma 5.12. *Sei $M/L/K$ ein Turm unverzweigter Erweiterungen. Dann kommutiert das Diagramm*

$$\begin{array}{ccc} Br(L|K) & \xrightarrow{inv_{L/K}} & \mathbb{Q}/\mathbb{Z} \\ \big\downarrow{\scriptstyle \inf} & & \big\| \\ Br(M/K) & \xrightarrow{invM/K} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Beweis. Alle in der Definition der Invariantenabbildung vorkommenden Abbildungen sind funktoriell, ebenso die Inflation. □

Satz 5.13. *Es existiert ein eindeutig bestimmter Isomorphismus*

$$inv_K : Br(K^{\mathrm{nr}}|K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

(nämlich $inv_K = inv_{k^{\mathrm{nr}}/K}$), so dass für alle endlichen Galoiserweiterungen L/K in K^{nr} das Diagramm

$$\begin{array}{ccc} Br(L|K) & \xrightarrow{inv_{L|K}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ \big\downarrow{\scriptstyle \inf} & & \big\downarrow \\ Br(K^{\mathrm{nr}}|K) & \xrightarrow[inv_K]{\sim} & \mathbb{Q}/\mathbb{Z} \end{array}$$

kommutiert.

Beweis. Für eine endliche unverzweigte Erweiterung L/K ist die Galoisgruppe $G = \mathrm{Gal}(L/K)$ endlich zyklisch und wird vom Frobeniusautomorphismus $\mathrm{Frob}_{L/K}$ erzeugt. Wir können somit einen Homomorphismus $f \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$ definieren dadurch, dass

$$f(\mathrm{Frob}_{L/K}) = \frac{1}{[L:K]} + \mathbb{Z}.$$

Insbesondere ist das Bild von $inv_{L/K}$ gleich $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. Da $\inf_{L/K}$ injektiv ist, ist

$$\mathrm{im}(inv_{L/K}) \cong Br(L|K) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(\mathbb{Z}/[L:K]\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/[L:K]\mathbb{Z},$$

das heißt

$$\mathrm{im}(inv_{L|K}) = \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

Das Diagramm in der Aussage des Satzes kommutiert wegen Bemerkung 5.12. Außerdem ist inv_K surjektiv, da

$$Br(K^{\mathrm{nr}}|K) = \bigcup_{K^{\mathrm{nr}}/L/K \text{ endl.}} Br(L|K)$$

und es zu jedem $n \in \mathbb{N}$ eine unverzweigte Erweiterung L/K vom Grad n gibt. Außerdem folgt daraus, dass inv_K durch $inv_{L/K}$ für endliche unverzweigte Erweiterungen L/K eindeutig bestimmt ist. □

Theorem 5.14. *Sei L/K eine endliche separable Erweiterung. Dann existiert ein kanonischer Homomorphismus*

$$res : Br(K^{\mathrm{nr}}|K) \to Br(L^{\mathrm{nr}}|L),$$

so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} Br(K^{\mathrm{nr}}|K) & \xrightarrow{res} & Br(L^{\mathrm{nr}}|L) \\ \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Ist L/K galoissch, so kann der Kern von res kanonisch mit einer zyklischen Untergruppe der Ordnung $[L:K]$ von $Br(L|K)$ identifiziert werden.

Beweis. Wir setzen $\Gamma_K := \mathrm{Gal}(K^{\mathrm{nr}}/K)$ und $\Gamma_L := \mathrm{Gal}(L^{\mathrm{nr}}/L)$. Es ist $L^{\mathrm{nr}} = LK^{\mathrm{nr}}$. Insbesondere haben wir eine natürliche Inklusion $\varphi : \Gamma_L \hookrightarrow \Gamma_K$. Wir betrachten das Diagramm

$$\begin{array}{ccccccc} Br(K^{\mathrm{nr}}|K) & \xrightarrow[\sim]{v_K} & H^2(\Gamma_K, \mathbb{Z}) & \xrightarrow[\sim]{\delta^{-1}} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\eta_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle res} & & \downarrow{\scriptstyle e_{L/K}\cdot res} & & \downarrow{\scriptstyle e_{L/K}\cdot res} & & \downarrow{\scriptstyle e_{L/K}f_{L/K}=[L:K]} \\ Br(L^{\mathrm{nr}}|L) & \xrightarrow[\sim]{v_L} & H^2(\Gamma_L, \mathbb{Z}) & \xrightarrow[\sim]{\delta^{-1}} & H^1(\Gamma_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\eta_L} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Dieses kommutiert wegen $v_L|_{K^{\mathrm{nr}}} = e_{L/K} v_K$ und $\mathrm{Frob}_L|_{K^{\mathrm{nr}}} = \mathrm{Frob}_K^{f_{L/K}}$. Daraus folgt die erste Behauptung.

Für eine endliche Galoiserweiterung L/K ist L^{nr}/K galoissch (das liegt an der Maximalität von L^{nr}/L; für $\sigma \in G_K$ ist σL^{nr} unverzweigt über $\sigma L = L$ und somit enthalten in L^{nr}). Wir erhalten ein kommutatives Diagramm mit exakten Zeilen

$$\begin{array}{ccccccc}
0 & \longrightarrow & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \mathbb{Q}/\mathbb{Z} \\
 & & \sim\uparrow & & inv_K\uparrow\sim & & inv_L\uparrow\sim \\
0 & \longrightarrow & \ker(res) & \longrightarrow & Br(K^{\mathrm{nr}}|K) & \xrightarrow{res} & Br(L^{\mathrm{nr}}|L) \\
 & & \downarrow & & \downarrow\inf & & \| \\
0 & \longrightarrow & Br(L|K) & \xrightarrow{\inf} & Br(L^{\mathrm{nr}}|K) & \xrightarrow{res} & Br(L^{\mathrm{nr}}|L),
\end{array}$$

woraus sich die zweite Behauptung ergibt. □

Korollar 5.15. *Sei L/K eine endliche Galoiserweiterung. Dann ist $Br(L|K)$ 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 5.14 und Satz 5.9. Falls L/K nicht zyklisch ist, finden wir eine nichttiviale galoissche Zwischenerweiterung $L/M/K$, denn die absolute Galoisgruppe eines lokalen Körpers ist auflösbar. Nach Induktionsvoraussetzung ist $|Br(L|M)| = [L:M]$ und $|Br(M|K)| = [M:K]$. Außerdem haben wir die exakte Folge

$$0 \to Br(M|K) \to Br(L|K) \to Br(L|M),$$

also

$$|Br(L|K)| \leq |Br(M|K)| \cdot |Br(L|M)| = [M:K] \cdot [L:M] = [L:K].$$

Wegen Satz 5.14 enthält $Br(L|K)$ aber eine zyklische Untergruppe der Ordnung $[L:K]$, muss also gleich dieser zyklischen Untergruppe sein. □

Theorem 5.16. *Es existiert ein eindeutig bestimmer Isomorphismus*

$$inv_K : Br(K) \to \mathbb{Q}/\mathbb{Z},$$

so dass für jede endliche separable Erweiterung $L|K$ das Diagramm

$$\begin{array}{ccc}
Br(K) & \xrightarrow{res} & Br(L) \\
\downarrow inv_K & & \downarrow inv_L \\
\mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

kommutiert und für jede endliche Galoiserweiterung L/K das Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & Br(L/K) & \xrightarrow{\inf} & Br(K) & \xrightarrow{res} & Br(L) \\ & & \downarrow{\scriptstyle inv_{L/K}} & & \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_L} \\ 0 & \longrightarrow & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \mathbb{Q}/\mathbb{Z} \end{array}$$

kommutiert.

Beweis. Wegen Korollar 5.15 ist für eine endliche galoissche Erweiterung L/K der Kern der Restriktion

$$res : Br(K^{\mathrm{nr}}|K) \to Br(L^{\mathrm{nr}}|L),$$

gleich $Br(L/K)$ (siehe Theorem 5.14). Das heißt wir können $Br(L/K)$ kanonisch als Untergruppe von $Br(K^{\mathrm{nr}}|K)$ auffassen. Außerdem ist

$$Br(K) = \bigcup_{L/K \text{ endl. gal.}} Br(L|K),$$

das heißt inf : $Br(K^{\mathrm{nr}}|K) \to Br(K)$ is ein Isomorphismus. Wir können also in Satz 5.13 die maximal unverzweigte Erweiterung K^{nr} von K durch einen separablen Abschluss K^{sep} von K ersetzen. Dann folgt die Behauptung. □

Korollar 5.17. *Sei L/K endlich separabel. Dann kommutiert das Diagramm*

$$\begin{array}{ccc} Br(L) & \xrightarrow{cor} & Br(K) \\ {\scriptstyle inv_L}\downarrow & & \downarrow{\scriptstyle inv_K} \\ \mathbb{Q}/\mathbb{Z} & = & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Beweis. Betrachte das Diagramm

$$\begin{array}{ccccc} Br(K) & \xrightarrow{res} & Br(L) & \xrightarrow{cor} & Br(K) \\ \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_L} & & \downarrow{\scriptstyle inv_K} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Q}/\mathbb{Z}, \end{array}$$

wobei φ so gewählt ist, dass das Diagramm kommutiert. Da $cor \circ res = [L : K]$, muss φ die Identität sein. □

Korollar 5.18. *Sei $M/L/K$ ein Turm endlicher Galoiserweiterungen. Dann kommutiert das Diagramm*

$$\begin{array}{ccccc} Br(L|K) & \xhookrightarrow{\inf} & Br(M|K) & \xrightarrow{res} & Br(M|L) \\ \downarrow{\scriptstyle inv_{L/K}} & & \downarrow{\scriptstyle inv_{M/K}} & & \downarrow{\scriptstyle inv_{M/L}} \\ \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \hookrightarrow & \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\cdot[L:K]} & \frac{1}{[M:L]}\mathbb{Z}/\mathbb{Z}. \end{array}$$

Beweis. Das rechte Quadrat kommutiert wegen Theorem 5.16 und das linke wegen Bemerkung 5.12. □

Definition. Sei L/K eine endliche Galoiserweiterung. Das Element

$$inv_{L/K}^{-1}(\frac{1}{[L:K]} + \mathbb{Z}) \in Br(L|K)$$

heißt Fundamentalklasse von L/K.

6 Klassenformationen

6.1 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 6.1. *Sei G eine endliche Gruppe und sei A ein G-Modul. Die durch die Paarung $A^* \times A \to \mathbb{Q}/\mathbb{Z}$ 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 $f : A \to \mathbb{Q}/\mathbb{Z}$ 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 $f : A \to \mathbb{Q}/\mathbb{Z}$ den assoziierten Homomorphismus $\tilde{f} : A/I_G A \to \mathbb{Q}/\mathbb{Z}$ 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

$$\begin{array}{rccc} \varphi: & A^*G/N_GA^* & \twoheadrightarrow & (N_GA/I_GA)^* \\ & \| & & \| \\ & \hat{H}^0(G,A^*) & & \hat{H}^{-1}(G,A)^*. \end{array}$$

Nun habe $f \in A^{*G}$ triviales Bild, d.h. $f(N_GA) = 0$. Da

$$N_G : A/_{N_G}A \xrightarrow{\sim} N_GA$$

ein Isomorphismus ist, existiert ein Homomorphismus $\tilde{f} : N_GA \to \mathbb{Q}/\mathbb{Z}$ mit $f(a) = \tilde{f}(N_Ga)$ für alle $a \in A$. Da $\mathbb{Q}/\mathbb{Z}$ $\mathbb{Z}$-injektiv ist, können wir $\tilde{f}$ zu einem Homomorphismus $\tilde{f} : A \to \mathbb{Q}/\mathbb{Z}$ 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

$$N_G\tilde{f}(a) = \sum_{g\in G} \tilde{f}(g^{-1}a) = \tilde{f}(N_Ga) = f(a).$$

Dies zeigt die Injektivität von φ 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

$$\begin{array}{ccccc} \hat{H}^i(G,\mathrm{Hom}(A,\mathbb{Q}/\mathbb{Z})) & \times & \hat{H}^{-i-1}(G,A) & \xrightarrow{\cup} & \hat{H}^{-1}(G,\mathbb{Q}/\mathbb{Z}) \\ {\scriptstyle \delta^i}\uparrow\wr & & {\scriptstyle \delta^i}\downarrow\wr & & {\scriptstyle (-1)^{\frac{i(i+1)}{2}}}\downarrow \\ \hat{H}^0(G,\mathrm{Hom}(A,\mathbb{Q}/\mathbb{Z})_i) & \times & \hat{H}^{-i-1}(G,A_{-i}) & \longrightarrow & \hat{H}^{-1}(G,\mathbb{Q}/\mathbb{Z}) \end{array}$$

unter Beachtung von

$$\mathrm{Hom}(A,\mathbb{Q}/\mathbb{Z})_i = \mathrm{Hom}(A_{-i},\mathbb{Q}/\mathbb{Z})$$

□

Lemma 6.2. *Ist G eine endliche Gruppe und A ein $\mathbb{Z}$-freier G-Modul, so induziert für alle $i \in \mathbb{Z}$ die Cup-Produktpaarung*

$$\hat{H}^i(G,\mathrm{Hom}(A,\mathbb{Z})) \times \hat{H}^{-i}(G,A) \xrightarrow{\cup} \hat{H}^0(G,\mathbb{Z}) = \mathbb{Z}/\#G\mathbb{Z}$$

einen Isomorphismus

$$\hat{H}^i(G,\mathrm{Hom}(A,\mathbb{Z})) \cong \hat{H}^{-i}(G,A)^*.$$

Beweis. Da A $\mathbb{Z}$-frei ist, ist die Folge

$$0 \longrightarrow \mathrm{Hom}(A,\mathbb{Z}) \longrightarrow \mathrm{Hom}(A,\mathbb{Q}) \longrightarrow \mathrm{Hom}(A,\mathbb{Q}/\mathbb{Z}) \longrightarrow 0$$

exakt. Nun ist $\mathrm{Hom}(A,\mathbb{Q})$ eindeutig teilbar, also kohomologisch trivial und wir erhalten das kommutative Diagramm

$$\begin{array}{ccccc} \hat{H}^{i-1}(G,\mathrm{Hom}(A,\mathbb{Q}/\mathbb{Z})) & \times & \hat{H}^{-i}(G,A) & \xrightarrow{\cup} & \hat{H}^{-1}(G,\mathbb{Q}/\mathbb{Z}) \\ \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \delta} \\ \hat{H}^i(G,\mathrm{Hom}(A,\mathbb{Z})) & \times & \hat{H}^{-i}(G,A) & \xrightarrow{\cup} & \hat{H}^0(G,\mathbb{Z}) \end{array}$$

wobei die vertikalen Abbildungen Isomorphismen sind. Daher folgt die Aussage aus 6.1. □

6.2 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 γ von $H^2(G, C)$ heißt **Fundamentalklasse**.

Bemerkung. C ist offenbar auch Klassenmodul für jede Untergruppe $H \subset G$. Ist γ ein Erzeuger von $H^2(G, C)$, so ist $\gamma_H = res^G_H \gamma$ ein Erzeuger von $H^2(H, C)$.

Grund: Wegen $cor\gamma_H = cor \cdot res\gamma = (G : H) \cdot \gamma$ ist die Ordnung von γ_H durch $\#H$ teilbar.

Beispiel. 1) Ist G zyklisch, so ist $C = \mathbb{Z}$ ein Klassenmodul. In der Tat gilt

$$H^1(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z}) = 0$$

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:

$$\begin{aligned} H^1(G, L^\times) &= 0 \qquad \text{(Hilberts Satz 90)} \\ H^2(G, L^\times) &= Br(L|K) \cong \mathbb{Z}/[L : K]\mathbb{Z}. \end{aligned}$$

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 3.34 ($H^1 = Der/\mathrm{I}Der$) und erweitern es ein wenig:

$$\begin{array}{ccc} C^0(G, A) & \xrightarrow[\varphi \mapsto \varphi(1)]{\sim} & A = \mathcal{C}^0(G, A) \\ {\scriptstyle d^1}\downarrow & & \downarrow{\scriptstyle \partial^1} \\ C^1(G, A) & \xrightarrow[\varphi \mapsto (g \mapsto \varphi(1,g))]{\sim} & \mathrm{Abb}(G, A) = \mathcal{C}^1(G, A) \\ {\scriptstyle d^2}\downarrow & & \downarrow{\scriptstyle \partial^2} \\ C^2(G, A) & \xrightarrow[\varphi \mapsto ((g_1,g_2) \mapsto \varphi(1,g_1,g_1g_2))]{\sim} & \mathrm{Abb}(G^2, A) = \mathcal{C}^2(G, A) \\ {\scriptstyle d^3}\downarrow & & \downarrow{\scriptstyle \partial^3} \\ C^3(G, A) & \xrightarrow[\varphi \mapsto ((g_1,g_2,g_3) \mapsto \varphi(1,g_1,g_1g_2,g_1g_2g_3))]{\sim} & \mathrm{Abb}(G^3, A) = \mathcal{C}^3(G, A), \end{array}$$

wobei:

- $\partial^1(a) = (g \mapsto ga - a)$
- $\partial^2(x) = ((g_1, g_2) \mapsto g_1 x(g_2) - x(g_1 g_2) + x(g_1)$

und (einfach nachrechnen)

$$\partial^3(x) = (g_1, g_2, g_3) \longmapsto g_1 x(g_2, g_3) - x(g_1 g_2, g_3) + x(g_1, g_2 g_3) - x(g_1, g_2)$$

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 **Zerfällungsmodul** $C(\gamma)$ 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 γ 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: $1 b_\tau = b_\tau$ 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 $i : C \to C(\gamma)$. Betrachtet man die Abbildung: $b : G \to C(\gamma)$, $\sigma \mapsto b_\sigma$, $b \in \mathrm{Abb}(G, C(\gamma)) = \mathcal{C}^1(G, C(\gamma))$ so gilt $\partial^2 b = i(c) \in \mathcal{C}^2(G, C(\gamma))$. D.h. c wird zum Korand in $C(\gamma)$, also $H^2(G, C) \to H^2(G, C(\gamma))$ schickt γ auf Null, d.h. γ „zerfällt“.

Bemerkung. Eine andere Wahl der Repräsentanten c von γ 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 φ 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

$$0 \longrightarrow C \xrightarrow{i} C(\gamma) \xrightarrow{\varphi} I_G \longrightarrow 0,$$
$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Bemerkung. Die obere Folge entspricht gerade dem Element

$$\gamma \in H^2(G, C) = \mathrm{Ext}^2_{\mathbb{Z}[G]}(\mathbb{Z}, C) = \mathrm{Ext}^1_{\mathbb{Z}[G]}(I_G, C).$$

unter der Identifikation zwischen Elementen in 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 6.3. *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 $\gamma_H = res^G_H\ \gamma \in H^2(H,C)$. Die folgenden Bedingungen sind äquivalent

(i) *$C(\gamma)$ ist ein kohomologisch trivialer G-Modul.*
(ii) *C ist ein Klassenmodul mit Fundamentalklasse γ.*
(iii) *δ^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

$$\begin{array}{rcl}(\delta^2)^{-1} : H^2(H,C) & \xrightarrow{\sim} & \frac{1}{\#H}\mathbb{Z}/\mathbb{Z} \\ \gamma_H & \longmapsto & \frac{1}{\#H}\mathbb{Z} + \mathbb{Z}.\end{array}$$

Diese heißen die **Invariantenabbildungen** (bzgl. γ) und werden mit inv bezeichnet.

Beweis. Die Abbildung δ^2 entsteht aus den exakten Folgen

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0 \tag{1}$$

$$0 \longrightarrow C \xrightarrow{i} C(\gamma) \xrightarrow{\varphi} I_G \longrightarrow 0 \tag{2}$$

und ist das Kompositum der Abbildung

$$\hat{H}^n(G,\mathbb{Z}) \xrightarrow[\sim]{\delta_1} \hat{H}^{n+1}(G,I_G) \xrightarrow{\delta_2} \hat{H}^{n+2}(G,C), \tag{3}$$

wobei δ_1 stets ein Isomorphismus ist. Für $n = 0$ haben wir die Abbildung

$$\mathbb{Z}/\#H\mathbb{Z} = \hat{H}^0(H,\mathbb{Z}) \xrightarrow[\sim]{\delta_1} H^1(H,I_G) \xrightarrow{\delta_2} H^2(H,C) \tag{4}$$

Behauptung: Für $\overline{1} = 1 + \#H\mathbb{Z}$ gilt

$$\delta_2\delta_1\overline{1} = \gamma_H = res^G_H\gamma. \tag{5}$$

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 $\delta_1\overline{1} \in H^1(H,I_G)$ ist durch den inhomogenen 1-Kozykel $(\partial 1)(\sigma) = \sigma - 1$ repräsentiert (eine Derivation $H \to I_G$). Ein Urbild von $\partial 1$ in $\mathcal{C}^1(H,C(\gamma))$ ist durch die Abbildung

$$x : H \to C(\gamma),\ x(\sigma) = b_\sigma$$

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 3.42 (Verhalten von $\cup$ unter Randabbildung, die Variante für Tate-Kohomologie) auf die exakten Folgen (1) und (2) an, erhält man

$$\delta^2\beta = \delta_2\delta_1(\overline{1} \cup \beta) = \delta_2(\delta_1\overline{1} \cup \beta) = \delta_2\delta_1\overline{1} \cup \beta = \gamma_H \cup \beta.$$

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

$$\mathbb{Z}/\#H\mathbb{Z} = \hat{H}^0(H,\mathbb{Z}) \xrightarrow[\sim]{\delta_1} H^1(H,I_G) \xrightarrow[\sim]{\delta_2} H^2(H,C)$$

ist ein Isomorphismus, der $\overline{1}$ auf γ_H schickt. Daher ist C ein Klassenmodul mit Fundamentalklasse γ, d.h. (i) $\Rightarrow$ (ii) ist gezeigt. Gilt umgekehrt (ii), so ist $H^1(H,C) = 0$ und $H^1(H,I_G) \xrightarrow[\sim]{\delta} H^2(H,C)$ ist ein Isomorphismus. Wir erhalten

$$H^n(H,C(\gamma)) = 0 \quad \text{für} \quad n = 1, 2$$

und jede Untergruppe H von G (insbesondere für jede p-Sylowgruppe). Nach 3.4.7 ist $C(\gamma)$ kohomologisch trivial. Wir erhalten (i) $\Longleftrightarrow$ (ii). Die Äquivalenz (i) $\Longleftrightarrow$ (iii) folgt aus (3) und der langen exakten Folge

$$\begin{aligned}\cdots \;&\longrightarrow \hat{H}^n(H,C) \longrightarrow \hat{H}^n(H,C(\gamma)) \longrightarrow \hat{H}^n(H,I_G)\\ &\xrightarrow{\delta} \hat{H}^{n+1}(H,C) \longrightarrow \hat{H}^{n+1}(H,C(\gamma)) \longrightarrow \cdots.\end{aligned}$$

□

6.3 Nakayama-Tate Dualität

Satz 6.4. *(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*

$$\hat{H}^i(G, \mathrm{Hom}(A,C)) \times \hat{H}^{2-i}(G,A) \xrightarrow{\cup} H^2(G,C) \cong \frac{1}{\#G}\mathbb{Z}/\mathbb{Z},$$

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*

$$\hat{H}^i(G, \mathrm{Hom}(A,C)) \xrightarrow{\sim} \hat{H}^{2-i}(G,A)^*$$

endlicher abelscher Gruppen.

Beweis. Sei

$$0 \longrightarrow C \longrightarrow C(\gamma) \longrightarrow I_G \longrightarrow 0$$

die exakte Folge aus dem Beweis von 6.3. Da A $\mathbb{Z}$-frei ist, sind die Folgen

$$\begin{aligned} 0 &\longrightarrow \mathrm{Hom}(A,C) \longrightarrow \mathrm{Hom}(A,C(\gamma)) \longrightarrow \mathrm{Hom}(A,I_G) \longrightarrow 0 \\ 0 &\longrightarrow \mathrm{Hom}(A,I_G) \longrightarrow \mathrm{Hom}(A,\mathbb{Z}[G]) \longrightarrow \mathrm{Hom}(A,\mathbb{Z}) \longrightarrow 0 \end{aligned}$$

exakt und die G-Moduln in der Mitte sind jeweils kohomologisch trivial (nach 4.21). Wir erhalten somit für alle $i \in \mathbb{Z}$ ein kommutatives Diagramm:

$$\begin{array}{ccccc} \hat{H}^{i-2}(G,\mathrm{Hom}(A,\mathbb{Z})) & \times & \hat{H}^{2-i}(G,A) & \xrightarrow{\cup} & \hat{H}^0(G,\mathbb{Z}) \\ {\scriptstyle\delta}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle\delta} \\ \hat{H}^{i-1}(G,\mathrm{Hom}(A,I_G)) & \times & \hat{H}^{2-i}(G,A) & \longrightarrow & \hat{H}^1(G,I_G) \\ {\scriptstyle\delta}\downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle\delta} \\ \hat{H}^i(G,\mathrm{Hom}(A,C)) & \times & \hat{H}^{2-i}(G,A) & \longrightarrow & \hat{H}^2(G,C) \end{array}$$

in dem die vertikalen Abbildungen Isomorphismen sind. Nach 6.2 erhalten wir den Isomorphismus

$$\hat{H}^i(G,\mathrm{Hom}(A,C)) \xrightarrow{\sim} \hat{H}^{2-i}(G,A)^*.$$

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. □

Bemerkung. Für eine Untergruppe $H \subset G$ haben wir zwei kommutative Diagramme

$$\begin{array}{ccc} \hat{H}^i(H,\mathrm{Hom}(A,C)) & \xrightarrow{\sim} & \hat{H}^{2-i}(H,A)^* \\ {\scriptstyle res}\uparrow\downarrow{\scriptstyle cor} & & {\scriptstyle cor^*}\uparrow\downarrow{\scriptstyle res^*} \\ \hat{H}^i(G,\mathrm{Hom}(A,C)) & \xrightarrow{\sim} & \hat{H}^{2-i}(G,A) \end{array}$$

wobei cor^* und res^* die zu cor und res dualen Abbildungen sind. Die Kommutativität folgt aus $cor(\alpha \cup res\beta) = cor(\alpha) \cup \beta$ (Übungsaufgabe).

Setzt man in 6.4 $i = 0$ und $A = \mathbb{Z}$ und erinnert sich an

$$H^2(G,\mathbb{Z})^* \cong H^1(G,\mathbb{Q}/\mathbb{Z})^* \cong G^{\mathrm{ab}},$$

erhält man

Satz 6.5. *Ist C ein Klassenmodul für die endliche Gruppe G, so erhält man einen Isomorphismus*

$$\rho = \rho_G : G^{\mathrm{ab}} \xrightarrow{\sim} C^G/N_G C.$$

Dieser heißt **Nakayama-Abbildung**, *hängt von der Wahl einer Fundamentalklasse $\gamma \in H^2(G, C)$ ab und es gilt*

$$\chi(\sigma) = inv(\rho(\sigma) \cup \delta\chi)$$

für jedes

$$\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\sim]{\delta} H^2(G, \mathbb{Z}).$$

Beweis. Die Existenz des Isomomorphismus ρ folgt direkt aus Satz 6.4. Um die Formel $\chi(\sigma) = inv(\rho(\sigma) \cup \delta\chi)$ zu zeigen erinnern wir uns an die Konstruktion von ρ.

$$\begin{array}{ccccccc}
 & & & \overset{\rho}{\frown} & & & \\
\hat{H}^0(G,C) & \xrightarrow{\sim} & H^2(G,\mathbb{Z})^* & \xrightarrow[\delta^*]{\sim} & H^1(G,\mathbb{Q}/\mathbb{Z})^* & \xleftarrow[\sim]{} & G^{\mathrm{ab}} \\
c & \longmapsto & (\alpha \mapsto inv(\alpha \cup c)) & \longmapsto & (\chi \mapsto inv(\delta\chi \cup c)) & & \\
 & & & & (\chi \mapsto \chi(\sigma)) & \longmapsto & \sigma
\end{array}$$

Ist nun $c = \rho(\sigma)$, erhalten wir $\chi(\sigma) = inv(\rho(\sigma) \cup \delta\chi)$ für alle $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$. □

Bemerkung. Wir können die Formel $\chi(\sigma) = inv(\rho(\sigma) \cup \delta\chi)$ auch anders ausdrücken, indem wir sagen, dass das Diagramm

$$\begin{array}{ccccc}
G^{\mathrm{ab}} & \times & H^1(G,\mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\
{\scriptstyle rec}\uparrow & & \downarrow{\scriptstyle \delta} & & \uparrow{\scriptstyle inv} \\
\hat{H}^0(G,C) & \times & H^2(G,\mathbb{Z}) & \xrightarrow{\cup} & H^2(G,C).
\end{array}$$

kommutiert, wobei wir uns daran erinnern, das der Reziprozitätshomomorphismus invers zu ρ ist.

Definition. Die Komposition

$$rec_G : C^G \twoheadrightarrow C^G/N_G C \xrightarrow[\sim]{\rho^{-1}} G^{\mathrm{ab}}$$

heißt **Reziprozitätshomomorphismus**. Ein alternativer Name ist „Normenrestsymbol“ und für $\alpha \in C^G$ schreibt man auch $(\alpha, G) := rec(\alpha)$. Der Name rührt daher, dass (α, G) dann und nur dann trivial ist, wenn $\alpha \in N_G C$ gilt.

Schließlich erinnern wir uns an den Isomorphismus

$$\Phi : G^{\mathrm{ab}} \xrightarrow{\sim} H_1(G,\mathbb{Z}) \xrightarrow{\sim} \hat{H}^{-2}(G,\mathbb{Z}).$$

Zusammen mit dem Isomorphismus aus 6.2 erhalten wir den Isomorphismus

$$\rho' : G^{\mathrm{ab}} \xrightarrow{\sim} \hat{H}^{-2}(G,\mathbb{Z}) \xrightarrow{\gamma\cup -} \hat{H}^0(G,C) \cong C^G/N_G C,$$

der in der Literatur oft zur Definition der Nakayama-Abbildung herangezogen wird.

Satz 6.6. $\rho = \rho'$.

Beweis. Wir betrachten das Diagramm

$$\begin{array}{ccccc}
G^{\mathrm{ab}} & \times & H^1(G,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\cup} & \frac{1}{\#G}\mathbb{Z}/\mathbb{Z} \\
{\scriptstyle rec}\uparrow & & \downarrow{\scriptstyle \delta} & & \uparrow{\scriptstyle inv} \\
\hat{H}^0(G,C) & \times & H^2(G,\mathbb{Z}) & \xrightarrow{\cup} & H^2(G,C) \\
{\scriptstyle \gamma\cup}\uparrow & & \downarrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle \gamma\cup} \\
\hat{H}^{-2}(G,\mathbb{Z}) & \times & \hat{H}^2(G,\mathbb{Z}) & \xrightarrow{\cup} & \frac{1}{\#G}\mathbb{Z}/\mathbb{Z}
\end{array}$$

Für $\rho = \rho'$ ist zu zeigen, dass für jedes $\sigma \in G^{\mathrm{ab}}$ und jedes $\chi \in H^1(G,\mathbb{Q}/\mathbb{Z})$ gilt

$$inv(\gamma \cup \Phi(\sigma) \cup \delta\chi) = \chi(\sigma)$$

Nach Definition von *inv* ist die Komposition der rechten vertikalen Pfeile die Identität. Wir erhalten

$$inv(\gamma \cup \Phi(\sigma) \cup \delta\chi) = \Phi(\sigma) \cup \delta\chi.$$

Dass dies gleich $\chi(\sigma)$ ist, ist eine Übungsaufgabe. □

6.4 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

$$inv_{U/V} : H^2(U/V, C^V) \xrightarrow{\sim} \frac{1}{(U:V)}\mathbb{Z}/\mathbb{Z}$$

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

$$\begin{array}{ccccc} H^2(U/V, C^V) & \xrightarrow{\inf} & H^2(U/W, C^W) & \xrightarrow{res} & H^2(V/W, C^W) \\ \wr \downarrow inv & & \wr \downarrow inv & & \wr \downarrow inv \\ \frac{1}{(U:V)}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\text{inkl}} & \frac{1}{(U:W)}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\cdot(U:V)} & \frac{1}{(V:W)}\mathbb{Z}/\mathbb{Z}. \end{array}$$

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

$$\begin{array}{ccc} H^2(V/W, C^W) & \xrightarrow{inv} & \frac{1}{(V:W)}\mathbb{Z}/\mathbb{Z} \\ cor \downarrow & & \downarrow \cap \\ H^2(U/W, C^W) & \xrightarrow{inv} & \frac{1}{(U:W)}\mathbb{Z}/\mathbb{Z}, \end{array}$$

da $cor_U^V \cdot res_V^U = (U : V)$.
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

$$\frac{1}{\#G}\mathbb{Z}/\mathbb{Z} := \varinjlim_V \frac{1}{(G:V)}\mathbb{Z}/\mathbb{Z}.$$

4) für jeden offenen Normalteiler $U \subset G$ ist C^U ein Klassenmodul für G/U. Die Elemente $inv_{G/U}^{-1}\left(\frac{1}{(G:U)} \mod \mathbb{Z}\right) \in H^2(G/U, C^U)$ bilden ein kompatibles System von Fundamentalklassen bei variierendem U. Daher erhalten wir kompatible Homomorphismen

$$rec_{G/U} : C^G \twoheadrightarrow C^G/N_{G/U}C^U \xrightarrow{\sim} (G/U)^{\text{ab}}.$$

Im Limes erhalten wir den **Reziprozitätshomomorphismus**

$$rec : C^G \longrightarrow G^{\text{ab}}.$$

Dieser hat dichtes Bild: Ist $U \subset G^{\text{ab}}$ eine offene Untergruppe und bezeichnen wir das Urbild von U unter der kanonischen Projektion $\pi : G \to G^{\text{ab}}$ mit $\tilde{U}$, so gilt $G^{\text{ab}}/U \cong G/\tilde{U} = (G/\tilde{U})^{\text{ab}}$, weshalb die Komposition $rec : C^G \to G^{\text{ab}} \twoheadrightarrow G^{\text{ab}}/U$ surjektiv ist.

Nach Definition (und Linksexaktheit des projektiven Limes) gilt

$$\ker(rec) = N_G C := \bigcap_{U \lhd G} N_{G/U} C^U \subset C^G.$$

Man nennt $N_G C$ die **Gruppe der universellen Normen** von C.

Schließlich schreibt man für $\alpha \in C^G$ auch $(\alpha, G) := rec(\alpha)$ und nennt dies das **Normrestsymbol**.

6.5 Normengruppen

Sei (G, C) eine Klassenformation. Um suggestiver zu werden, stellen wir uns G als Galoisgruppe einer Körpererweiterung vor. Wir benutzen die inklusionsumkehrende 1:1-Korrespondenz der Galoistheorie und ordnen jeder abgeschlossenen Untergruppe $H \subset G$ einen „Körper“ E zu. Wir schreiben $E_1 \supset E_2 \Longleftrightarrow H_1 \subset H_2$. Nennen $E_1|E_2$ endlich, wenn $(H_2 : H_1) < \infty$ ist und galoissch, wenn $H_1 \lhd H_2$. Für $g \in G$ setzen wir gE mit der konjugierten Untergruppe gHg^{-1} gleich. Wir schreiben

$$C_E := C^H.$$

Dies dient der besseren Orientierung, da man typischerweise besser in Körpern als in Gruppen denken kann.

Die Buchstaben K und L reservieren wir für „Körper“ deren assoziierte Untergruppen G_K bzw. G_L in G offen sind. (Dies sind die endlichen Erweiterungen des „Grundkörpers“, d.h. des Körpers der zur ganzen Gruppe G gehört.

Für jede endliche Erweiterung $L'|L$ und jedes $s \in G_L$ haben wir die Abbildung: $s : C_{L'} \to C_{sL'}$, $x \mapsto sx$. Diese Abbildung hängt nur von der Restklasse von s in $G_L/G_{L'}$ ab. Summiert man über alle Restklassen, erhält man die Normabbildung

$$N_{L'|L} : C_{L'} \longrightarrow C_L, \quad x \longmapsto \sum_{s \in G_L/G_{L'}} sx.$$

Ist $L'|L$ galoissch, d.h. $G_{L'} \lhd G_L$, mit Galoisgruppe $G(L'|L) \equiv G_L/G_{L'}$ so haben wir den Reziprozitätsisomorphismus

$$C_L/N_{L'|L} C_{L'} \xrightarrow[\sim]{(-,L'|L)} G(L'|L)^{\mathrm{ab}}$$

Definition. Die Untergruppen in C_L der Form $N_{L'|L} C_{L'}$ für eine endliche nicht notwendig galoissche Erweiterung heißen die **Normengruppen** in C_L.

Lemma 6.7. *Die Normengruppen haben endlichen Index.*

Beweis. Sei $L'|L$ endlich und $L''|L$ eine endliche galoissche Erweiterung die L' enthält. Dann gilt

$$\begin{aligned} N_{L''|L}C_{L''} &= N_{L'|L}N_{L''|L'}C_{L''} \\ &\subseteq N_{L'|L}C_{L'}. \end{aligned}$$

Außerdem gilt

$$C_L/N_{L''|L}C_{L''} \cong G(L''|L)^{\mathrm{ab}}$$

und dies ist eine endliche Gruppe. □

Definition. Wir nennen eine Erweiterung $L|K$ **abelsch**, wenn sie galoissch mit abelscher Galoisgruppe ist.

Bemerkung. Das Kompositum abelscher Erweiterungen ist abelsch. Daher enthält jede Erweiterung $L|K$ eine maximale abelsche Teilerweiterung $K'|K$.

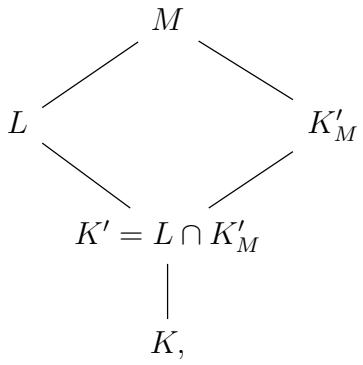
Satz 6.8. *Sei $L|K$ eine endliche Erweiterung und sei $K' \subset L$ die maximale abelsche Teilerweiterung. Dann gilt*

$$N_{L|K}C_L = N_{K'|K}C_{K'}.$$

Beweis. Wir haben die Inklusion

$$\begin{aligned} N_{L|K}C_L &= N_{K'|K}N_{L|K'}C_L \\ &\subseteq N_{K'|K}C_{K'}. \end{aligned}$$

Nun sei M eine galoissche Hülle von $L|K$. Wir betrachten folgendes Diagramm von Körpererweiterungen:



wobei K'_M die maximale abelsche Teilerweiterung von M/K ist. Dann gilt

$$G(M|K') = G(M|L) \cdot [G(M|K), G(M, K)].$$

Die exakte Folge

$$\begin{aligned} &G(M|L)/[G(M|L), G(M|L)] \longrightarrow G(M|K)/[(G(M|K), G(M|K)] \\ &\longrightarrow G(M|K)/G(M|L) \cdot [G(M|K), G(M|K)] \longrightarrow 0 \end{aligned}$$

liest sich daher als

$$G(M|L)^{\mathrm{ab}} \longrightarrow G(M|K)^{\mathrm{ab}} \longrightarrow G(K'|K) \longrightarrow 0.$$

Nun betrachten wir das kommutative Diagramm

$$\begin{array}{ccc} C_L/N_{M|L}C_M & \xrightarrow[\sim]{(-,M|L)} & G(M|L)^{\mathrm{ab}} \\ \downarrow N_{L|K} & & \downarrow \\ C_K/N_{M|K}C_M & \xrightarrow[\sim]{(-,M|K)} & G(M|K)^{\mathrm{ab}} \\ \downarrow & & \downarrow \\ C_K/N_{K'|K}C_{K'} & \xrightarrow[\sim]{(-,K'|K)} & G(K'|K) \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array}$$

Sei $x \in N_{K'|K}C_{K'} \subset C_K$. Dann bildet sich $(x, M|K) \in G(M|K)^{\mathrm{ab}}$ auf $0 \in G(K'|K)$ ab. Daher existiert ein $y \in C_L$ mit $x - N_{L|K}(y) \in N_{M|K}C_M$. Also $x \in N_{L|K}(y) + N_{M|K}C_M \subset N_{L|K}C_L$. □

Wir erhalten

Korollar 6.9. *Der Index $(C_K : N_{L|K}C_L)$ teilt den Grad $[L : K]$. Es gilt genau dann Gleichheit, wenn $L|K$ eine abelsche Erweiterung ist.*

Satz 6.10. *Die Zuordnung*

$$L \longmapsto I_L := N_{L|K}C_L \subset C_K$$

definiert eine inklusionsumkehrende Bijektion zwischen der Menge der endlichen abelschen Erweiterungen von K und der Menge der Normengruppen in C_K. Es gilt

$$I_{L\cdot L'} = I_L \cap I_{L'},\ I_{L\cap L'} = I_L + I_{L'}.$$

Jede Gruppe, die eine Normengruppe enthält, ist selbst Normengruppe.

Beweis. Sind $L|K$ und $L'|K$ abelsch, so auch $LL'|K$ und es gilt

$$I_{LL'} = N_{LL'|K}C_{LL'} \subset I_L \cap I_{L'}.$$

Ist $x \in I_L \cap I_{L'}$, so bildet sich $(x, LL'|K) \in G(LL'|K)$ auf 0 ab in $G(L|K)$ und $G(L'|K)$, ist also selbst 0. Daher gilt $x \in I_{LL'}$.

Gilt nun $L \subset L'$ so folgt $I_{L'} \subset I_L$. Aus $I_{L'} = I_L$ folgt

$$\begin{aligned} I_{LL'} &= I_{L'} \cap I_L \\ &= I_L \end{aligned}$$

und daher

$$[LL' : K] = (C_K : I_{LL'}) = (C_K : I_L) = [L : K].$$

Also $LL' = L \Longrightarrow L' \subset L$. Analog folgt $L \subset L'$, also ist die Zuordnung eine Bijektion.

Schließlich gilt offenbar

$$I_{L\cap L'} \supset I_L + I_{L'}.$$

Weiterhin gilt

$$\begin{aligned}(C_K : I_{L\cap L'}) &= [L \cap L' : K] \\ &= \frac{[L : K] \cdot [L' : K]}{[LL' : K]} \\ &= \frac{(C_K : I_L) \cdot (C_K : I_{L'})}{(C_K : (I_L \cap I_{L'}))} \\ &= (C_K : (I_L + I_{L'})).\end{aligned}$$

Nun gelte $U \supset I_L$ für eine abelsche Erweiterung $L|K$. Dann ist C_K/U eine Faktorgruppe von C_K/I_L und wir erhalten ein kommutatives Diagramm

$$\begin{array}{ccc} C_K/I_L & \xrightarrow[\sim]{(\quad,L'|K)} & G(L|K) \\ \downarrow & & \downarrow \\ C_K/U & \underset{\sim}{\to} & G(L'|K). \end{array}$$

Daher folgt

$$U = \ker(rec : C_K \longrightarrow G(L'|K)) = I_{L'}.$$

□

Korollar 6.11. *Die Gruppe C_K wird zur topologischen Gruppe indem man die Normengruppen als Umgebungsbasis der 0 erklärt. Die Reziprozitätsabbildung*

$$rec : C_K \longrightarrow G^{\mathrm{ab}}$$

induziert einen Isomorphismus $\hat{C}_K \xrightarrow{\sim} G^{\mathrm{ab}}$, wobei $\hat{C}_K$ die Vervollständigung bezeichnet.

Beweis. Läuft L über die endlichen abelschen Erweiterungen des Grundkörpers K der zu G gehört, so erhalten wir

$$\hat{C}_K = \varprojlim_{I \text{ Normgr.}} C_K/I \xrightarrow{\sim} \varinjlim_{L|K \text{ endlich ab.}} G(L|K) = G^{\mathrm{ab}}.$$

□

6.6 Der Existenzsatz

Welches sind die Normengruppen in C_K?

Wir machen zusätzliche Annahmen und fordern 3 Axiome.

- Für jedes L sei C_L mit der Struktur einer abelschen topologischen Gruppe versehen.
- Für $L \subset L'$ stimmt die Topologie von C_L mit der Topologie als Unterraum in $C_{L'}$ überein.
- Für jedes $g \in G$ ist die Abbildung

$$C_L \longrightarrow C_{gL}, \quad x \longmapsto gx$$

stetig.

Hieraus folgt, dass für $L \subset L'$ die Normabbildung $N_{L'|L} : C_{L'} \to C_L$ stetig ist.

Axiom I: Für jede Erweiterung $L'|L$ hat die Normabbildung $N_{L'|L} : C_{L'} \to C_L$ abgeschlossenes Bild und kompakten Kern.

Bemerkung. Da $N_{L'|L}C_{L'}$ endlichen Index in C_L hat folgt, dass $N_{L'|L}C_{L'}$ offen in C_L ist. D.h.: Die Topologie auf C_L ist *feiner* als die Normtopologie.

Notation:

$$D_L = N_{G_L}C = \bigcap_{L'|L \text{ endl.}} N_{L'|L}C_{L'} \subset C_L$$

(Gruppe der universellen Normen in C_L).

Satz 6.12. *Für jede endliche Erweiterung $L'|L$ gilt $N_{L'|L}D_{L'} = D_L$.*

Beweis. Die Inklusion $N_{L'|L}D_{L'} \subset D_L$ ist offensichtlich. Sei umgekehrt $x \in D_L$ und $L''|L'$ eine endliche Erweiterung. Setze

$$K(L'') = N_{L''|L'}C_{L''} \cap N^{-1}_{L'|L}(x),$$

d.h. $K(L'')$ besteht aus den Elementen in $C_{L'}$ der Norm x, die Norm eines Elements in L'' sind. Nun ist $N_{L''|L'}C_{L''}$ abgeschlossen und $N^{-1}_{L'|L}(x)$ kompakt (Axiom I). Daher ist $K(L'')$ kompakt.

Behauptung: $K(L'') \neq \emptyset$.

Grund: Nach Voraussetzung gilt $x \in D_L$, daher existiert ein $y \in L''$ mit $N_{L''|L}(y) = x$ und somit $N_{L''|L'}(y) \in K(L'') \subset C_{L'}$.

Nun lassen wir L'' laufen. Es gilt

$$\bigcap_{L''} K(L'') = \varprojlim_{L''} K(L'') \neq \emptyset$$

weil der projektive Limes nichtleerer Kompakta ein nichtleeres Kompaktum ist. Für $y \in \bigcap_{L''} K(L'')$ gilt $y \in D_{L'}$ und $N_{L'|L}(y) = x$. □

Axiom II. Für jede Primzahl p existiert ein Körper L_p, endlich über K, so dass für $L \supset L_p$ die p-Multiplikationsabbildung $m_p : C_L \to C_L$, $x \mapsto px$ der folgenden Bedingung genügt

$$(*) \qquad \ker(m_p) \text{ ist kompakt und } \mathrm{im}(m_p) \supset D_L.$$

(Dieses Axiom ist das, welches in der Anwendung am schwierigsten nachzuweisen ist.)

Satz 6.13. *Für jedes L ist D_L teilbar und gleich $\bigcap_n n \cdot C_L$.*

Beweis. Wir zeigen zunächst: Für jede Primzahl p und jedes L gilt $D_L = pD_L$. Sei $x \in D_L$ und L' eine endliche Erweiterung von L, die L_p enthält. ("L' hinreichend groß"). Sei

$$E(L') = \{y \in C_L \mid py = x \text{ und } y \in N_{L'|L}C_{L'}\}.$$

Dann gilt $E(L') \neq \emptyset$: Nach 6.12 gilt $x = N_{L'|L}z'$ für ein $z' \in D_{L'}$ und nach Axiom II gilt $z' = pz$ für ein $z \in C_{L'}$. Dann gilt $N_{L'|L}(z) \in E(L')$.

Nun gilt: $E(L') = m_p^{-1}(x) \cap N_{L'|L}C_{L'}$. Daher ist $E(L')$ kompakt. Wie vorher lassen wir nun L' laufen und erhalten $\bigcap_{L'} E(L') \neq \emptyset$. Für $y \in \bigcap_{L'} E(L')$ gilt $y \in D_L$ und $py = x$. Daher ist D_L teilbar also $D_L \subset \bigcap_n nC_L$. Gilt umgekehrt $x \in \bigcap_n nC_L$ und hat $L'|L$ den Grad n, so gilt: $x \in nC_L \subset N_{L'|L}C_{L'}$. Folglich $x \in D_L = \bigcap_{L'} N_{L'|L}C_{L'}$. □

Axiom III. Es existiert eine kompakte Untergruppe $\tilde{C}_L \subset C_L$, so dass jede Untergruppe von endlichem Index in C_L, die $\tilde{C}_L$ enthält, Normengruppe ist.

Theorem 6.14. *Gelten Axiome I, II und III so sind die Normengruppen genau die abgeschlossenen Untergruppen von endlichem Index.*

Beweis. Normengruppen sind abgeschlossen und haben endlichen Index nach Axiom I. Sei $U \subset C_L$ abgeschlossen und von endlichem Index. Gilt $(C_L : U) = n$, so gilt $n \cdot C_L \subset U$, also $D_L \subset U$ nach 6.13. Nun durchlaufe N alle Normengruppen. Dann gilt

$$\bigcap (N \cap \tilde{C}_L) = \bigcap N \cap \tilde{C}_L = D_L \cap \tilde{C}_L \subset U.$$

Da die Gruppen $N \cap \tilde{C}_L$ kompakt sind, und U offen, existiert ein N mit $N \cap \tilde{C}_L \subset U$:

$$\left(\bigcap_N (N \cap \tilde{C}_L) \right) \smallsetminus U) = \varnothing \Longrightarrow$$

eines der Elemente dieser Familie muss leer sein. (beachte: endliche Durchschnitte von Normengruppen sind Normengruppen, daher ist dieser projektive Limes gefiltert).

Aus $N \cap \tilde{C}_L \subset U$ folgt

$$N \cap (\tilde{C}_L + (N \cap U)) \subset U.$$

Grund: Liegt x im Durchschnitt, so können wir schreiben: $x = x' + x''$ mit $x' \in \tilde{C}_L$ und $x'' \in N \cap U$. Es gilt $x' = x - x'' \in N$, also

$$x' \in \tilde{C}_L \cap N \subset U \quad \rightsquigarrow \quad x = x' + x'' \in U.$$

Die Gruppe $N \cap U$ ist abgeschlossen von endlichem Index, weil N und U dies sind. Daher ist auch $\tilde{C}_L + (N \cap U)$ abgeschlossen von endlichem Index und nach Axiom III eine Normengruppe. Nach 6.10 ist damit auch $N \cap (\tilde{C}_L + (N \cap U))$ eine Normengruppe und damit (wieder 6.10) auch ihre Obergruppe U. □

7 Lokale Klassenkörpertheorie

Es sei k ein lokaler Körper, $\overline{k}$ ein separabler Abschluss und $G = G_k = \mathrm{Gal}(\overline{k}|k)$. In Kapitel 4 haben wir einen Isomorphismus

$$inv_K : H^2(G_k, \overline{k}^\times) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

konstruiert, so dass für $k \subset K \subset L \subset \overline{k}$ mit L/k endlich das Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L|K, L^\times) & \xrightarrow{\inf} & H^2(K, \overline{k}^\times) & \xrightarrow{res} & H^2(L, \overline{k}^\times) \\ & & \downarrow {\scriptstyle inv_{L|K}} & & \downarrow {\scriptstyle inv_K} & & \downarrow {\scriptstyle inv_L} \\ 0 & \longrightarrow & \frac{1}{(L:K)}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z} \end{array}$$

kommutiert. Außerdem gilt für jeden Zwischenkörper $k \subset K \subset \overline{k}$ nach Hilberts Satz 90, dass $H^1(G_K, \overline{k}^\times) = 0$. Wir erhalten

Satz 7.1. *Das Paar $(G_k, \overline{k}^\times)$ ist eine Klassenformation.*

Korollar 7.2. *Wir erhalten einen Reziprozitätshomomorphismus*

$$rec : k^\times \longrightarrow G_k^{\mathrm{ab}}$$

mit dichtem Bild.

Ziele:

1.) Verstehe die Normengruppe in $k^\times$.
2.) Verstehe das Bild von *rec*.
3.) Welche Rolle spielt das Bild $rec(U_k)$?

7.1 Der Existenzsatz

Satz 7.3. *Die Normengruppen in $k^\times$ sind genau die offenen Untergruppen von endlichem Index.*

Wir brauchen zunächst:

Satz 7.4. *Sei $(n, \mathrm{char}\ k) = 1$ 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 $\overline{k}^{\ker(\varphi)} = k(\sqrt[n]{x})$. Daher ist K das Kompositum aller zyklischen Erweiterungen von k, deren Ordnung n teilt. Wir erhalten einen Isomorphismus

$$\begin{aligned} G(K|k) \cong \mathrm{Hom}(G(K|k), \mathbb{Z}/n\mathbb{Z})^\vee &= \mathrm{Hom}(G_k^{\mathrm{ab}}/n, \mathbb{Z}/n)^\vee \\ &= H^1(G_k, \mathbb{Z}/n)^\vee = (k^\times/k^{\times n})^\vee. \end{aligned}$$

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 6.9 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 7.3. Wir versehen für jede endliche Erweiterung $K|k$ die Gruppe $K^\times$ mit ihrer natürlichen Topologie. Nach Abschnitt 6.6. 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 $N_{L'|L} : L'^\times \to L^\times$ 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 $m_p : L^\times \to L^\times$ der folgenden Bedingung genügt

$(*)$ $\ker(m_p)$ ist kompakt und $\mathrm{im}(m_p) \supset D_L$

Beweis von Axiom II. Der Kern von m_p ist endlich. Wir zeigen die Aussage über $\mathrm{im}(m_p)$ im Fall $p \neq \mathrm{char}\ k$. Setze $L_p = k(\mu_p)$. Dann gilt für jedes $L \supset L_p$ nach 7.4:

$$N(L(\sqrt[p]{L^\times})/L) = L^{\times p} = \mathrm{im}(m_p)$$

also $D_L \subset \mathrm{im}(m_p)$

• für $p = \mathrm{char}\ k$, 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 7.5. *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 π 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 π eine Uniformisierende von L_n und

$$N_{L_n|L}(\pi) = \pi^n \Longrightarrow (\pi^n) \times U_L \subset N_{L_n|L}(L_n^\times).$$

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 $L^\times/U_L \xrightarrow[\sim]{v} \mathbb{Z}$ genau die Untergruppen der Form $(\pi^n) \times U_L$ und diese sind nach 7.5 Normengruppen. Dies zeigt Satz 7.3. □

Korollar 7.6. *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. □

Korollar 7.7. *Die Reziprozitätsabbildung*

$$rec : k^\times \longrightarrow G(k^{\mathrm{ab}}|k)$$

ist stetig und injektiv.

Beweis. Nach 7.6 gilt $\ker(rec) = 0$. Nun faktorisiert rec als

$$k^\times \xrightarrow{\alpha} \varprojlim_{\substack{U\subset k^\times \\ \text{off. von endl. Index}}} k^\times/U \xrightarrow[\sim]{\beta} \varinjlim_{\substack{U\subset G(k^{\mathrm{ab}}|k) \text{ off.} \\ \text{von endl. Index}}} G(k^{\mathrm{ab}}|k)/U \quad \begin{array}{c} \\ \| \wr \\ G(k^{\mathrm{ab}}|k) \end{array}$$

α ist stetig, da die Projektionen $k^\times \to k^\times/U$ stetig sind und β ist der projektive Limes von Isomorphismen endlicher Gruppen, also ein topologischer Isomorphismus. □

7.2 Verzweigung für Erweiterungen lokaler Körper

Dieser Abschnitt ist eine Wiederholung aus Algebraischer Zahlentheorie I.

Satz 7.8. *Sei $L|K$ eine endliche separable Erweiterung lokaler Körper. Dann existiert ein $x \in \mathcal{O}_L$, so dass*

$$\mathcal{O}_L = \mathcal{O}_K[x].$$

Wir können nun unverzweigte Erweiterungen charakterisieren.

Satz 7.9. *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) *$v_L(F'(x)) = 0$.*

Erinnerung: $F \in \mathcal{O}_K[X]$ heißt *Eisensteinpolynom*, wenn

$$F = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

mit $\pi_K \mid a_i$, $i = 0, \ldots, a_{n-1}$ und $\pi_K^2 \nmid a_0$. Eisensteinpolynome sind irreduzibel.

Satz 7.10. *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.*

Umgekehrt gilt

Satz 7.11. *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 π über K ist ein Eisensteinpolynom.*

Erinnerung: $L|K$ heißt zahm verzweigt, falls $p \nmid e$ mit $e = e(L|K)$ und $p = \mathrm{char}(k)$.

Lemma 7.12. (i) *Für einen Turm $M|L|K$ gilt*

$$M|K \quad z.v. \quad \Longleftrightarrow M|L \quad z.v. \quad + \quad L|K \quad z.v.$$

(ii) *Ist $L_1|K$ unverzweigt und $L_2|K$ separabel, so gilt*

$$L_2|K \text{ z.v.} \iff L_1L_2|L_1 \text{ z.v.}$$

Satz 7.13. *Sei $\pi \in K$ eine Uniformisierende. Für eine Erweiterung $L|K$ sind äquivalent:*

(i) *$L|K$ ist zahm verzweigt.*
(ii) *Es existiert eine unverzweigte Erweiterung $M|K$ so dass $LM = M(\sqrt[e]{\pi})$, wobei $(e, p) = 1$.*

Definition. Wir nennen eine unendliche, separable algebraische Erweiterung L eines lokalen Körpers K **zahm verzweigt**, wenn jede endliche Teilerweiterung zahm verzweigt ist. Die maximal zahm verzweigte Teilerweiterung von K in einem gegebenen separablen Abschluß $\overline{K}$ von K wird mit K^{tr} bezeichnet.

Satz 7.14. *$K^{tr}|K$ ist galoissch. K^{tr} entsteht aus K durch Adjunktion aller prim-zu-p Einheitswurzeln und aller prim-zu-p-ten Wurzeln aus π.*

Setzt man $\hat{\mathbb{Z}}^{(p')} = \prod_{\ell \neq p} \mathbb{Z}_p$, so erhalten wir eine exakte Folge

$$1 \to \hat{\mathbb{Z}}^{(p')} \to G(K^{tr}|K) \to \hat{\mathbb{Z}} \to 1.$$

7.3 Trägheits- und Verzweigungsgruppen

Sei $L|K$ eine Galoiserweiterung lokaler oder globaler Körper, und sei v eine nichtarchimedische Bewertung auf K und w eine Fortsetzung auf L.

Definition. • $T_w(L|K) = \{\sigma \in G_w(L|K) \mid \sigma x \equiv x \mod \mathfrak{P}_w \quad \forall\, x \in \mathcal{O}_w\}$ 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
• $V_w(L|K) = \{\sigma \in G_w(L|K) \mid \frac{\sigma x}{x} \equiv 1 \mod \mathfrak{P}_w \quad \forall\, x \in L^\times\}$
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 $\sigma x \equiv x \mod \mathfrak{P}_w$. Daher gilt

$$V_w \subset T_w.$$

Lemma 7.15. (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 7.16. *V_w und T_w sind Normalteiler in G_w.*

Beweis. $T_w = \ker(G_w \longrightarrow G(\ell|k))$ 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 $\tau\sigma\tau^{-1} \in T_w$ und $V_w \subset G_w$ ist Normalteiler. □

Lemma 7.17. *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 7.18. *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 7.19. *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 φ 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. $X_w(L|K) = \mathrm{Hom}(w(L^\times)/v(K^\times), \ell^\times)$.

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 $\overline{x} \in w(L^\times)/w(K^\times)$ wähle einen Vertreter $x \in L^\times$. Dann setze

$$\chi_\sigma(\overline{x}) = \overline{\left(\frac{\sigma x}{x}\right)} \in \ell^\times.$$

Satz 7.20. *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 χ_σ 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 $T_w \to X_w$ ein Homomorphismus ist: Für $\sigma, \tau \in T_w$ gilt

$$\chi_{\sigma\tau}(\overline{x}) = \overline{\left(\frac{\sigma\tau x}{x}\right)} = \overline{\frac{\sigma x}{x} \cdot \frac{\tau x}{x} \cdot \frac{\sigma(\tau(x)/x)}{\tau(x)/x}}.$$

Wegen $u := \frac{\tau(x)}{x} \in U_w$ folgt

$$\overline{\left(\frac{\sigma u}{u}\right)} = 1 \in \ell^\times.$$

□

Satz 7.21. *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

$$X = \mathrm{Hom}(w(L^\times)/v(K^\times), \ell^\times).$$

(Erinnerung: $(w(L^\times) : v(K^\times)) = e(L|K) < \infty$ und $w(L^\times) \cong \mathbb{Z} \cong v(K^\times)$.)
Nach 7.20 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 7.19 ist $L|L^{\langle\sigma\rangle}$ eine rein zahm verzweigte Galoiserweiterung vom Grad q. Sei π_L eine Uniformisierende von L und π 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 7.13 folgt $\zeta \in L^{\langle\sigma\rangle}$ und $L = L^{\langle\sigma\rangle}(\sqrt[q]{\pi\zeta})$. Ersetzen wir π 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

$$\frac{\sigma(\sqrt[q]{\pi})}{\sqrt[q]{\pi}} = \zeta_q \not\equiv 1 \mod \mathfrak{P}$$

wegen $(p, q) = 1$. Widerspruch □

Korollar 7.22. *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 $\overset{7.12}{\iff} K'L^T|L^T$ zahm verzweigt
$\iff [K'L^T : L^T]$ ist prim zu p
$\iff (T : U \cap T)$ 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 7.23. *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 7.15. □

Satz 7.24. *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 7.18 können wir uns für den Beweis der Exaktheit der beiden weiteren Folgen auf den Fall lokaler Körper beschränken. Im kommutativen Diagramm

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & T(M|L) & \longrightarrow & G(M|L) & \longrightarrow & G(m|\ell) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & T(M|K) & \longrightarrow & G(M|K) & \longrightarrow & G(m|k) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & T(L|K) & \longrightarrow & G(L|K) & \longrightarrow & G(\ell|k) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

sind alle Zeilen und die 2. + 3. Spalte exakt, also auch die erste Spalte. Nach 7.23 erhalten wir die exakte Folge

$$\begin{array}{ccccccccc} 1 & \longrightarrow & V(L|K) & \longrightarrow & V(M|K) & \longrightarrow & V(L|K) & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & T(L|K) & \longrightarrow & T(M|K) & \longrightarrow & T(L|K) & \longrightarrow & 0. \end{array}$$

Es bleibt zu zeigen, dass $V(M|K) \to V(L|K)$ 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 σ. Wähle $m \in \mathbb{N}$ mit $n \cdot m \equiv 1 \mod o(\sigma)$. Dann gilt $\tau^{m\cdot n} = (\tau^n)^m \in V(M|K)$ und $\tau^{m\cdot n}|_L = \sigma^{m\cdot n} = \sigma$. □

Satz 7.25. *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. □

7.4 Das Bild der Einheiten unter Reziprozität

Satz 7.26. *Die Einschränkung von rec auf U_K definiert einen Isomorphismus $rec|_{U_K} : U_K \xrightarrow{\sim} T(K^{\mathrm{ab}}|K)$. Die induzierte Abbildung*

$$rec^{\mathrm{nr}} : K^\times/U_K \longrightarrow G(K^{\mathrm{nr}}|K)$$

ist injektiv und das Bild besteht aus allen ganzzahligen Potenzen des Frobeniusautomorphismus. Es gilt

$$rec^{\mathrm{nr}}(x) = \mathrm{Frob}^{v(x)}.$$

Beweis. Wir haben die induzierte Klassenformation $(G(K^{\mathrm{nr}}|K),\ K^{\mathrm{nr}\times})$. Da $U_{K^{\mathrm{nr}}}$ ein kohomologisch trivialer Modul ist, gibt die exakte Folge $0 \to U_{K^{\mathrm{nr}}} \to K^{\mathrm{nr}\times} \xrightarrow{v} \mathbb{Z} \to 0$ einen Isomorphismus zur Klassenformation

$$(\hat{\mathbb{Z}}, \mathbb{Z})$$

wobei die Invariantenabbildung gegeben ist durch den natürlichen Homomorphismus

$$\begin{array}{rcl} H^2(\hat{\mathbb{Z}}, \mathbb{Z}) \xrightarrow{\sim} H^1(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z}, \\ \varphi & \longmapsto & \varphi(1). \end{array}$$

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

$$\mathbb{Z}/n\mathbb{Z} = \hat{H}^0(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}) \to \mathrm{Hom}(H^2(\mathbb{Z}/n\mathbb{Z},\mathbb{Z}), H^2(\mathbb{Z}/n\mathbb{Z},\mathbb{Z})),$$

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 $rec^{\mathrm{nr}}(x) = \mathrm{Frob}^{v(x)}$. Wir erhalten das kommutative Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_K & \longrightarrow & K^\times & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 0 \\
 & & {\scriptstyle rec|_{U_K}}\downarrow & & \downarrow{\scriptstyle rec} & & \downarrow & & \\
0 & \longrightarrow & T(K^{\mathrm{ab}}|K) & \longrightarrow & G(K^{\mathrm{ab}}|K) & \longrightarrow & G(K^{\mathrm{nr}}|K) & \longrightarrow & 0.
\end{array}$$

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 7.5 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

$$\begin{array}{ccccccccc}
0 & \longrightarrow & I_L U_K/U_K & \longrightarrow & K^\times/I_L & \longrightarrow & K^\times/I_L U_K & \longrightarrow & 0 \\
 & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\
0 & \longrightarrow & T(L|K) & \longrightarrow & G(L|K) & \longrightarrow & G(K'|K) & \longrightarrow & 0.
\end{array}$$

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 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

$$U_K \xrightarrow{\sim} T(K^{\mathrm{ab}}|K). \qquad \square$$

Moral: Bezüglich der exakten Folge

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_K & \longrightarrow & K^\times & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \wr\downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & T(K^{\mathrm{ab}}|K) & \longrightarrow & G(K^{\mathrm{ab}}|K) & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

sieht man, dass $G(K^{\mathrm{ab}}|K)$ aus $K^\times$ entsteht „indem man $\mathbb{Z}$ durch $\hat{\mathbb{Z}}$ ersetzt“.

Korollar 7.27. *Das Bild von U_K^1 unter rec ist $V(K^{\mathrm{ab}}|K)$.*

Beweis. U_K^1 bzw. $V(K^{\mathrm{ab}}|K)$ sind jeweils die p-Sylowuntergruppen von U_K bzw. $T(K^{\mathrm{ab}}|K)$. □

7.5 Führer

Definition. Sei $L|K$ eine endliche abelsche Erweiterung lokaler Körper. Es sei $n \in \mathbb{N} \cup \{0\}$ die kleinste Zahl so dass $U_K^{(n)} \subseteq N_{L|K}L^\times$. Dann heißt das Ideal

$$\mathfrak{p}_K^n =: f_{L|K}$$

der **Führer** der Erweiterung $L|K$.

Bemerkung. n existiert, weil $N_{L|K}L^\times$ in $K^\times$ offen ist und die Gruppen $U_K^{(n)}$ eine Umgebungsbasis der 1 bilden.

Korollar 7.28. *Eine endliche abelsche Erweiterung $L|K$ ist genau dann unverzweigt, wenn ihr Führer gleich* 1 *ist.*

Beweis. Dies folgt aus 7.26. □

7.6 Der archimedische Fall

Ist $K = \mathbb{R}$ oder $\mathbb{C}$, so ist $(G_K, \overline{K}^\times)$ eine Klassenformation. Die Reziprozitätsabbildung hat die folgende Gestalt:

$$K = \mathbb{R}: \quad rec : \mathbb{R}^\times \longrightarrow \{\pm 1\}, \quad x \longmapsto \mathrm{sgn}(x).$$

Die Gruppe der universellen Normen ist gleich $\mathbb{R}^\times_{>0}$.

$$K = \mathbb{C}: \quad rec : \mathbb{C}^\times \longrightarrow 1.$$

Die Gruppe der universellen Normen ist gleich $\mathbb{C}^\times$.

7.7 Der Satz von Kronecker-Weber

Satz 7.29. *Sei p eine Primzahl und $n \in \mathbb{N}$. Die Normengruppe der Erweiterung $\mathbb{Q}_p(\mu_{p^n})|\mathbb{Q}_p$ ist die Gruppe*

$$(p) \times U^{(n)}_{\mathbb{Q}_p} \subset \mathbb{Q}_p^\times.$$

Beweis. Sei $K = \mathbb{Q}_p$, $L = \mathbb{Q}_p(\mu_{p^n})$. Nach Zahlentheorie I ist $L|K$ rein verzweigt vom Grad $p^{n-1}(p-1)$. Bezeichnet ζ eine primitive p^n-te Einheitswurzel in L, so ist $1-\zeta$ ein Primelement in $\mathcal{O}_L$ der Norm $N_{L|K}(1-\zeta) = p$. Nun erinnern wir uns an die Exponentialabbildung. Sie definiert einen Isomorphismus

$$\exp : \mathfrak{p}_K^i \underset{\sim}{\to} U_K^{(i)}$$

für $i > \frac{1}{p-1}$, also für $i \geq 1$, wenn $p \neq 2$, und für $i \geq 2$, wenn $p = 2$.

Sei zunächst $p \neq 2$. Dann kommutiert für $i \geq 1$, $j \geq 1$ das Diagramm

$$\begin{array}{ccc} \mathfrak{p}_K^i & \xrightarrow[\sim]{\exp} & U_K^{(i)} \\ \Big\downarrow x & & \Big\downarrow x \\ \mathfrak{p}_K^{i+j-1} & \xrightarrow[\sim]{\exp} & U_K^{(i+j-1)} \end{array} \qquad \begin{array}{c} \\ \\ x^{p^{(j-1)}(p-1)} \\ \\ . \end{array}$$

$\Big\downarrow p^{(j-1)}(p-1)x$

Daher gilt: $(i = 1, j = n)$:

$$\begin{array}{rcll} U_K^{(n)} & = & (U_K^{(1)})^{p^{(n-1)}(p-1)} & \leftarrow \text{ Der Exponent ist gleich } [L:K] \\ & \subseteq & N_{L|K}L^\times. & \end{array}$$

Insgesamt erhalten wir

$$(p) \times U_K^{(n)} \subseteq N_{L|K}L^\times.$$

Wegen

$$p^{n-1}(p-1) = (K^\times : (p) \times U_K^{(n)}) = [L:K] = (K^\times : N_{L|K}L^\times)$$

folgt Gleichheit.

Für $p = 2$ haben wir das folgende Bild:

$$U_K^{(2)} = U_K^{(3)} \cup 5U_K^{(3)},$$

weil eine Zahl $\equiv 1 \bmod 4$ stets entweder $\equiv 1$ oder $5 \bmod 8$ ist.

Die Exponentialabbildung gibt $U_K^{(3)} = (U_K^{(2)})^2$ und wir erhalten:

$$U_K^{(n)} = (U_K^{(2)})^{2^{n-1}} \cup 5^{2^{n-2}}(U_K^{(2)})^{2^{n-1}}.$$

Wegen (Rechnung) $N_{L|K}(2+i) = 5^{2^{n-2}}$ folgt $U_K^{(n)} \subset N_{L|K}L^\times$. Wir erhalten wieder die Inklusion

$$(p) \times U_K^{(n)} \subset N_{L|K}L^\times$$

und aus Gradgründen folgt Gleichheit. □

Satz 7.30. *Jede endliche abelsche Erweiterung $L|\mathbb{Q}_p$ ist in einem Körper $\mathbb{Q}_p(\zeta)$ enthalten, wobei ζ eine Einheitswurzel ist. Mit anderen Worten: Die maximale abelsche Erweiterung $\mathbb{Q}_p^{\mathrm{ab}}|\mathbb{Q}$ entsteht durch Adjunktion aller Einheitswurzeln.*

Beweis. Die Untergruppen $(p^m) \times U_K^{(n)}$, $K = \mathbb{Q}_p$, $n, m \in \mathbb{N}$ bilden eine Umgebungsbasis der 1 in $K^\times$. Daher gilt für m, n geeignet

$$(p^m) \times U_K^{(n)} \subset N_{L|K} L^\times.$$

Nun ist $(p^m) \times U_K$ die Normengruppe der unverzweigten Erweiterung vom Grad m und diese entsteht durch Adjunktion der $(p^m - 1)$-ten Einheitswurzel. Es ist $(p) \times U_K^{(n)}$ die Normengruppe von $\mathbb{Q}_p(\zeta_{p^n})|\mathbb{Q}_p$. Daher ist

$$(p^m) \times U_K^{(n)} = ((p^m) \times U_K) \cap ((p) \times U_K^{(n)})$$

die Normengruppe von

$$\mathbb{Q}_p(\zeta_{p^n}) \cdot \mathbb{Q}_p(\zeta_{p^m-1}) = \mathbb{Q}_p(\zeta_{p^n(p^m-1)}).$$

Daher gilt $L \subset \mathbb{Q}_p(\zeta_{p^n(p^m-1)})$. □

Im Globalen erhalten wir den

Satz 7.31 (Kronecker-Weber)**.** *Jede endliche abelsche Erweiterung $L|\mathbb{Q}$ ist in einem Kreisteilungskörper $\mathbb{Q}(\zeta)$ enthalten.*

Beweis. Sei S die (endliche) Menge der in $L|\mathbb{Q}$ verzweigten Primzahlen und es bezeichne L_p die Vervollständigung von L bezüglich einer gewählten Stelle von L über p. Dann ist $L_p|\mathbb{Q}_p$ abelsch und nach 7.30 gilt $L_p \subset \mathbb{Q}_p(\mu_{n_p})$ für ein passend gewähltes n_p. Sei p^{e_p} die genaue in n_p aufgehende p-Potenz und

$$n = \prod_{p \in S} p^{e_p}.$$

Wir zeigen $L \subset \mathbb{Q}(\mu_n)$. Setze $M = L(\mu_n)$, dann ist zu zeigen $M = \mathbb{Q}(\mu_n)$.

Zunächst ist $M|\mathbb{Q}$ abelsch und nur Primzahlen aus S verzweigen in $M|\mathbb{Q}$. Sei M_p die Vervollständigung von M bezüglich einer Stelle in M die über der gewählten Stelle in L über p liegt. nach Konstruktion gilt

$$M_p = L_p(\mu_n) \subseteq \mathbb{Q}_p(\mu_{p^{e_p}})(\mu_{n'})$$

mit geeignetem $(n', p) = 1$.

Die Erweiterung $\mathbb{Q}_p(\mu_{p^{e_p}})$ ist rein verzweigt und $\mathbb{Q}_p(\mu_{n'})|\mathbb{Q}_p$ ist unverzweigt, also die maximale unverzweigte Teilerweiterung von $\mathbb{Q}_p(\mu_n)|\mathbb{Q}_p$. Die Trägheitsgruppe T_p von $M_p|\mathbb{Q}_p$ ist daher ein Quotient von $G(\mathbb{Q}_p(\mu_{p^{e_p}})|\mathbb{Q}_p)$ und ihre Ordnung teilt

somit $\varphi(p^{e_p})$ (Eulersche φ-Funktion). Sei T die durch die Gruppe T_p, $p \in S$, erzeugte Untergruppe in $G(M|\mathbb{Q})$. Die Erweiterung $M^T|\mathbb{Q}$ ist dann (überall) unverzweigt (siehe ÜA), also $M^T = \mathbb{Q}$, $T = G(M|\mathbb{Q})$. Andererseits gilt

$$\#T \leq \prod_{p \in S} \#T_p \leq \prod_{p \in S} \varphi(p^{e_p}) = \varphi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}].$$

Es folgt $[M : \mathbb{Q}] = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$, also $M = \mathbb{Q}(\mu_n)$ und schließlich $L \subset \mathbb{Q}(\mu_n)$. □

Korollar 7.32. *Der zyklotomische Charakter χ_{cycl} definiert einen Isomorphismus:*

$$G(\mathbb{Q}^{\mathrm{ab}}|\mathbb{Q}) \xrightarrow{\sim} \hat{\mathbb{Z}}^\times$$

Beweis. Den Isomorphismus $G(\mathbb{Q}(\mu)|\mathbb{Q}) \xrightarrow{\sim} \hat{\mathbb{Z}}^\times$ hatten wir in der Algebra-Vorlesung bewiesen. Daher folgt alles aus 7.31. □

7.8 Das Hilbert-Symbol

Sei n eine natürliche Zahl und K ein lokaler Körper, der eine primitive n-te Einheitswurzel enthält. Sei $K'|K$ die maximal abelsche Erweiterung vom Exponent n. Es gilt $N_{K'|K}K'^\times = K^{\times n}$, also $G(K'|K) \xrightarrow{\sim} K^\times/K^{\times n}$. Andererseits gilt nach Kummer-Theorie:

$$\mathrm{Hom}(G(K'|K), \mu_n) = H^1(G_K, \mu_n) \cong K^\times/K^{\times n}.$$

Wir erhalten eine perfekte Paarung

$$\begin{array}{ccccc} G(K'|K) & \times & \mathrm{Hom}(G(K'|K), \mu_n) & \longrightarrow & \mu_n \\ |\wr & & \|\wr & & \| \\ K^\times/K^{\times n} & \times & K^\times/K^{\times n} & \longrightarrow & \mu_n \end{array}$$

Definition. Die untere Paarung heißt das **Hilbert-Symbol**. Es wird für $a, b \in K^\times$ durch

$$(a, b) \longmapsto \left(\frac{a, b}{\mathfrak{p}}\right) \in \mu_n$$

bezeichnet (und hängt nur von der Restklasse modulo $K^{\times n}$ ab).

Satz 7.33. *Für $a, b \in K^\times$ gilt*

$$(a, K(\sqrt[n]{b})|K)(\sqrt[n]{b}) = \left(\frac{a, b}{\mathfrak{p}}\right) \cdot \sqrt[n]{b}.$$

Beweis. Nach Definition ist $(a, K'|K)$ gleich dem Bild von a unter $rec : K^\times/K^{\times n} \xrightarrow{\sim} G(K'|K)$, wobei K' wieder die maximale abelsche Erweiterung vom Exponent n ist. Das Bild von b unter dem Isomorphismus $K^\times/K^{\times n} \xrightarrow{\sim} \mathrm{Hom}(G(K'|K), \mu_n)$

ist der Charakter χ_b der durch $\chi_b(g) = \frac{g(\sqrt[n]{b})}{\sqrt[n]{b}}$ gegeben ist. Nach Definition des Hilbert-Symbols gilt

$$\left(\frac{a,b}{\mathfrak{p}}\right) = \chi_b((a,K'|K)) = \frac{(a,K'|K)\sqrt[n]{b}}{\sqrt[n]{b}} = \frac{(a,K(\sqrt[n]{b})|K)\sqrt[n]{b}}{\sqrt[n]{b}}.$$

□

Satz 7.34. *(Eigenschaften des Hilbertsymbols)*

(i) $\left(\frac{aa',b}{\mathfrak{p}}\right) = \left(\frac{a,b}{\mathfrak{p}}\right) \cdot \left(\frac{a',b}{\mathfrak{p}}\right)$

(ii) $\left(\frac{a,b\cdot b'}{\mathfrak{p}}\right) = \left(\frac{a,b}{\mathfrak{p}}\right) \cdot \left(\frac{a,b}{\mathfrak{p}}\right)$

(iii) $\left(\frac{a,b}{\mathfrak{p}}\right) = 1 \iff a$ *ist eine Norm der Erweiterung* $K(\sqrt[n]{b})/K$

(iv) $\left(\frac{a,b}{\mathfrak{p}}\right) = \left(\frac{b,a}{\mathfrak{p}}\right)^{-1}$

(v) $\left(\frac{a,-a}{\mathfrak{p}}\right) = 1$ *und gilt* $1-a \in K^\times$, *so gilt* $\left(\frac{a,1-a}{\mathfrak{p}}\right) = 1$

(vi) *Ist* $\left(\frac{a,b}{\mathfrak{p}}\right) = 1$ *für alle* $b \in K^\times$, *so gilt* $a \in K^{\times n}$.

Beweis. (i) und (ii) folgen aus der Definition.
(iii) folgt aus 7.33, denn nach lokaler Klassenkörpertheorie gilt

$$\begin{aligned} a \in N_{K(\sqrt[n]{b})/K} K(\sqrt[n]{b})^\times &\iff (a, K(\sqrt[n]{b})/K) = 1 \\ &\iff (a, K(\sqrt[n]{b})/K) \cdot (\sqrt[n]{b}) = \sqrt[n]{b} \\ &\iff \left(\frac{a,b}{\mathfrak{p}}\right) = 1 \end{aligned}$$

Aussage (vi) beschreibt die Vollkommenheit der Paarung.

Um (v) zu zeigen nehmen wir $b \in K^\times$ und $x \in K^\times$ mit $x^n - b \neq 0$. Dann gilt in K':

$$x^n - b = \prod_{i=0}^{n-1}(x - \zeta^i\beta), \quad \beta^n = b$$

mit einer primitiven n-ten Einheitswurzel ζ. Sei d der größte Teiler von n so dass $y^d = b$ eine Lösung in K hat und sei $m = n/d$. Die Erweiterung $K(\beta)/K$ ist dann zyklisch vom Grad m und die Konjugierten von $x - \zeta^i\beta$ sind die Elemente $x - \zeta^j\beta$ mit $j \equiv i \mod d$. Daher gilt

$$x^n - b = \prod_{i=0}^{d-1} N_{K(\beta)/K}(x - \zeta^i\beta).$$

Deshalb ist für jedes $x \in K^\times$ mit $x^n - b \neq 0$ das Element $x^n - b$ eine Norm in $K(\sqrt[n]{b})/K$, also $\left(\frac{x^n-b,b}{\mathfrak{p}}\right) = 1$.

$x = 0$, $b = -a$ liefert $\left(\frac{a,-a}{\mathfrak{p}}\right) = 1$
und $x = 1$, $b = 1 - a$ liefert $\left(\frac{a,1-a}{\mathfrak{p}}\right) = 1$.

Es verbleibt (iv). Dies folgt aus

$$\begin{aligned}\left(\frac{a,b}{\mathfrak{p}}\right)\left(\frac{b,a}{\mathfrak{p}}\right) &= \left(\frac{a,-a}{\mathfrak{p}}\right)\left(\frac{a,b}{\mathfrak{p}}\right)\left(\frac{b,a}{\mathfrak{p}}\right)\left(\frac{b,-b}{\mathfrak{p}}\right) \\ &= \left(\frac{a,-ab}{\mathfrak{p}}\right)\left(\frac{b,-ab}{\mathfrak{p}}\right) = \left(\frac{ab,-ab}{\mathfrak{p}}\right) = 1.\end{aligned}$$

□

Im archimedischen Fall muss für $n > 2$ K schon $\mathbb{C}$ sein und wegen $\mathbb{C}^\times/\mathbb{C}^{\times n} = 1$ ist das Hilbert-Symbol einfach die triviale Paarung. Der Fall $n = 1$ ist uninteressant. Im Fall $K = \mathbb{R}$, $n = 2$ ist das Hilbert-Symbol gegeben durch

$$\left(\frac{a,b}{\infty}\right) = \begin{cases} -1 & \text{wenn} \quad a,b < 0 \\ 1 & \text{sonst.} \end{cases}$$

Grund: sind $a, b < 0$, so ist a keine Norm in $K(\sqrt{b})/K = \mathbb{C}/\mathbb{R}$. Ansonsten ist a stets Norm.

Lemma 7.35. *Sei $(n,p) = 1$ und $x \in K^\times$. Die Erweiterung $K(\sqrt[n]{x})/K$ ist genau dann unverzweigt, wenn $x \in U_K \cdot K^{\times n}$ gilt.*

Beweis. Gilt $x = u \cdot y^n$ und $u \in U_K$ so gilt $K(\sqrt[n]{x}) = K(\sqrt[n]{u})$ und diese Erweiterung ist nach Zahlentheorie I, Kor. 8.62 unverzweigt. Sei $L = K(\sqrt[n]{x})$ unverzweigt über K. Dann gilt $v_K = v_L|_K$ und somit $v_L(\sqrt[n]{x}) = \frac{1}{n}v_K(x) \in \mathbb{Z}$, also $n \mid v_K(x)$. Hieraus folgt $x \in U_K \cdot K^{\times n}$. □

Wir haben die Zerlegung $U_K = \mu_{q-1} \times U_K^1$ wobei q die Anzahl der Elemente im Restklassenkörper ist und schreiben

$$u = \omega(u) \cdot \langle u \rangle$$

Satz 7.36. *Gilt $(n,p) = 1$, so gilt für $a, b \in K^\times$:*

$$\left(\frac{a,b}{\mathfrak{p}}\right) = \omega\left((-1)^{\alpha\beta} \cdot \frac{b^\alpha}{a^\beta}\right)^{\frac{q-1}{n}}$$

wobei $\alpha = v(a)$, $\beta = v(b)$.

Beweis. Der Ausdruck

$$\langle a, b\rangle = \omega\left((-1)^{\alpha\beta} \cdot \frac{b^\alpha}{a^\beta}\right)^{\frac{q-1}{n}}$$

ist bilinear und antisymmetrisch auf $K^\times \times K^\times$. Daher genügt es, die Aussagen für $(a = \pi, b = -\pi)$ $(a = \pi, b \in U_K)$ und $a, b \in U_K$ zu zeigen. Für $a = \pi$, $b = -\pi$ gilt $\left(\frac{a,b}{\mathfrak{p}}\right) = 1$ nach 7.35 und $\langle a, b\rangle = 1$.

Für $a, b \in U_K$ ist $K(\sqrt[n]{b})/K$ unverzweigt, also a eine Norm und somit $\left(\frac{a,b}{\mathfrak{p}}\right) = 1$. Es gilt offenbar auch $\langle a, b\rangle = 1$.

Bleibt der Fall $a = \pi$, $b \in U_l$. Dann ist $(a, K(\sqrt[n]{b})/K)$ nach 7.26 gerade der Frobeniushomomorphismus der unverzweigten Erweiterung $K(\sqrt[n]{b})/K$. Daher gilt

$$(a, K(\sqrt[n]{b})/K)(\sqrt[n]{b}) = \mathrm{Frob}(\sqrt[n]{b}) \equiv (\sqrt[n]{b})^q \mod \mathfrak{p}$$

also $\left(\frac{a,b}{\mathfrak{p}}\right) \equiv (\sqrt[n]{b})^{q-1} \mod \mathfrak{p}$ und folglich

$$\left(\frac{a, b}{\mathfrak{p}}\right) = \omega(b)^{\frac{q-1}{n}}.$$

□

Im Spezialfall $a = \pi$, $b = u \in U_K$ sehen wir, dass

$$\left(\frac{\pi, u}{\mathfrak{p}}\right) = \omega(u)^{\frac{q-1}{n}}$$

nicht von der Auswahl der Uniformisierenden π abhängt.

Definition.

$$\left(\frac{u}{\mathfrak{p}}\right) := \left(\frac{\pi, u}{\mathfrak{p}}\right) = u^{\frac{q-1}{n}} \mod \mathfrak{p}$$

heißt das **Legendre** oder auch das ***n*-te Potenzrestsymbol** von u.

Der Name rechtfertigt sich durch

Lemma 7.37. . *Sei $(n, p) = 1$ und $u \in U_K$. Es gilt*

$$\left(\frac{u}{\mathfrak{p}}\right) = 1 \iff u \quad \textit{ist eine } n\textit{-te Potenz} \mod \mathfrak{p}.$$

Beweis. Der Restklassenkörper κ von K hat Ordnung q und $\kappa^\times$ ist zyklisch von der Ordnung $q - 1$. □

Bemerkung. Für $K = \mathbb{Q}_p$, $p \neq 2$, und $n = 2$ erhalten wir das klassische Legendre-Symbol. Im Fall $(p, n) \neq 1$ ist das Hilbert-Symbol schwierig auszurechnen. Für $n = 2$, $K = \mathbb{Q}_2$ gilt der folgende

Satz 7.38. *Für $a, b \in U_{\mathbb{Q}_2}$ gilt*

- $\left(\frac{2,2}{2}\right) = 1$
- $\left(\frac{2,a}{2}\right) = (-1)^{\frac{a^2-1}{8}}$
- $\left(\frac{a,b}{2}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$.

(Die Exponenten liegen in $\mathbb{Z}_2$, die Potenzen sind wohldefiniert.)

Beweis. Es gilt

$$\frac{(a_1a_2)^2-1}{8} \equiv \frac{a_1^2-1}{8} + \frac{a_2^2-1}{8} \mod 2$$

und

$$\frac{a_1a_2-1}{2} \equiv \frac{a_1-1}{2} + \frac{a_2-1}{2} \mod 2.$$

Daher sind die Ausdrücke auf der rechten Seite bilinear und antisymmetrisch. Das gleiche gilt für die linke Seite wegen 7.34. Wir müssen die Formeln also nur für Erzeuger von $U_{\mathbb{Q}_2}/U_{\mathbb{Q}_2}^2$ prüfen.

Wir behaupten, dass $\{-1, 5\}$ die Gruppe $U_{\mathbb{Q}_2}/U_{\mathbb{Q}_2}^2$ erzeugt. Dazu betrachten wir das Diagramm

$$\begin{array}{ccc} 2^2\mathbb{Z}_2 & \xrightarrow[\exp]{\sim} & U_{\mathbb{Q}_2}^{(2)} \\ {\scriptstyle \cdot 2}\downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle ()^2} \\ 2^3\mathbb{Z}_2 & \xrightarrow[\exp]{\sim} & U_{\mathbb{Q}_2}^{(3)}. \end{array}$$

Die Exponentialabbildungen sind Isomorphismen und die Multiplikation mit 2 auf der linken Seite auch. Deshalb ist die Potenzierung mit 2 auf der rechten Seite in Isomorphismus. Insbesondere gilt

$$U_{\mathbb{Q}_2}^{(3)} \subseteq U_{\mathbb{Q}_2}^2.$$

Wir haben

$$U_{\mathbb{Q}_2} = U_{\mathbb{Q}_2}^{(1)} = \{\pm 1\} \times U_{\mathbb{Q}_2}^{(2)}.$$

und -1 erzeugt $\{\pm 1\}$ und 5 erzeugt $U_{\mathbb{Q}_2}^{(2)}/U_{\mathbb{Q}_2}^{(3)}$.

Sei $x \in \mathbb{Q}_2^\times$. Nach 7.34 ist $\left(\frac{-1,x}{2}\right)$ genau dann 1, wenn x eine Norm der Erweiterung $\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2$ ist, das heißt wenn $x = y^2 + z^2$ für gewisse $y, z \in \mathbb{Q}_2$ gilt. Wir haben

$$5 = 1^2 + 2^2 \Rightarrow \left(\frac{-1,5}{2}\right) = 1$$

$$1 = 1^2 + 1^2 \Rightarrow \left(\frac{-1,2}{2}\right) = 1.$$

Daraus können wir berechnen:

$$\left(\frac{2,2}{2}\right) = \left(\frac{2,-2}{2}\right)\left(\frac{2,-1}{2}\right) = 1,$$
$$\left(\frac{5,5}{2}\right) = \left(\frac{5,-5}{2}\right)\left(\frac{5,-1}{2}\right) = 1.$$

Wäre $\left(\frac{-1,-1}{2}\right) = 1$, so wäre $\left(\frac{-1,x}{2}\right) = 1$ für alle x. Das würde wegen 7.34 implizieren, dass -1 eine Quadratwurzel in $\mathbb{Q}_2$ ist, was nicht stimmt. Also gilt

$$\left(\frac{-1,-1}{2}\right) = -1$$

Die gleich Argumentation ergibt

$$\left(\frac{2,5}{2}\right) = -1.$$

Direktes Nachrechnen ergibt, dass die rechte Seite der Gleichungen jeweils die gleichen Werte annimmt. □

Ist nun K ein Zahlkörper und $n \in \mathbb{N}$ mit $\mu_n \subset K$, so gilt für $a, b \in K^\times$ die fundamentale Produktformel

$$\prod_{\text{alle } \mathfrak{p}} \left(\frac{a,b}{\mathfrak{p}}\right) = 1.$$

Aus dieser erhält man für $K = \mathbb{Q}$ und $n = 2$ das Quadratische Reziprozitätsgesetz: Seien p, q ungerade Primzahlen. Dann gilt

$$\prod_{\text{alle } v} \left(\frac{p,q}{v}\right) = 1.$$

- Für $v = \infty$ gilt $\left(\frac{p,q}{\infty}\right) = 1$ da $p, q > 0$
- Für $\ell \neq 2$ Primzahl gilt nach 7.36

$$\begin{aligned}\left(\frac{p,q}{\ell}\right) &= \omega\left((-1)^{v_\ell(p)v_\ell(q)} \cdot \frac{q^{v_\ell(p)}}{p^{v_\ell(q)}}\right)^{\frac{\ell-1}{2}} \\ &= \begin{cases} 1 & \text{für} \quad \ell \neq p, q \\ \left(\frac{p,q}{p}\right) = \left(\frac{q}{p}\right) & \text{für} \quad \ell = p \\ \left(\frac{p,q}{q}\right) = \left(\frac{q,p}{q}\right)^{-1} = \left(\frac{p}{q}\right)^{-1} & \text{für} \quad \ell = q. \end{cases}\end{aligned}$$

und unter Beachtung von 7.38 für $\ell = 2$:

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

Das Produkt

$$\prod_{\text{alle } v} \left(\frac{p,q}{v}\right) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^{-1}(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ist nach Produktformel gleich 1, worin wir das quadratische Reziprozitätsgesetz wiederfinden.