

Algebraische Zahlentheorie 2  
Prof. Dr. Werner Bley  
Sommersemester 2017

Pascal Stucky

21. April 2020

Bei gefundenen Fehlern freue ich mich über eine Nachricht – auch im Sinne der anderen Kommilitonen. E-Mail: `vorname.nachname [at] campus.lmu.de`.

# Inhaltsverzeichnis

<b>1</b>	<b>Überblick</b>	<b>1</b>
1.1	Globale Klassenkörpertheorie (idealtheoretisch) . . . . .	1
1.2	Lokale Klassenkörpertheorie . . . . .	12
1.3	Globale Klassenkörpertheorie (ideltheoretisch) . . . . .	14
<b>2</b>	<b>Kohomologie endlicher Gruppen</b>	<b>20</b>
2.1	$G$ -Moduln . . . . .	20
2.2	Definition von (Tate)-Kohomologiegruppen . . . . .	26
2.3	Die lange exakte Kohomologiesequenz . . . . .	30
2.4	$G$ -induzierte Moduln . . . . .	37
2.5	Inflation, Restriktion und Korestriktion . . . . .	41
2.6	Das Cupprodukt . . . . .	49
2.7	Kohomologie zyklischer Gruppen . . . . .	56
2.8	Der Satz von Tate . . . . .	59
<b>3</b>	<b>Lokale Klassenkörpertheorie</b>	<b>64</b>
3.1	Abstrakte Klassenkörpertheorie . . . . .	64
3.2	Abstrakte Galoistheorie . . . . .	66
3.3	Galoiskohomologie . . . . .	78
3.4	Die multiplikative Gruppe von $p$ -adischen Körpern . . . . .	79
3.5	Die Klassenformation der unverzweigten Erweiterungen . . . . .	80
3.6	Das lokale Reziprozitätsgesetz . . . . .	86
3.7	Der Existenzsatz . . . . .	94
	<b>Anmerkungen zur Klausur</b>	<b>98</b>
	<b>Literatur</b>	<b>99</b>

# Literatur

- Grundlage für die Vorlesung: [NS11]
- Grundlage für das Vorwissen (Dedekindringe, Ganzheitsringe, Zerlegungssätze, Dirichletscher Einheitsatz, Endlichkeit der Klassenzahl, quadratische Zahlkörper, Kreisteilungskörper): [Neu06]
- Vorausgesetzt wird:  $p$ -adische Zahlen  $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ , endliche Erweiterungen von  $\mathbb{Q}_p$ , diskrete Bewertungsringe. Dies findet man in [Ser13].

## 1 Überblick

### 1.1 Globale Klassenkörpertheorie (idealthoretisch)

Ziel: Beschreibung aller abelschen, endlichen Erweiterungen eines fixierten Zahlkörpers  $k$  durch Daten in  $k$ .

Vorlage: [Was97, Appendix]

**Notation.** Wir fixieren einen festen Zahlkörper als Grundkörper und bezeichnen ihn mit  $k$ .

**Definition 1.1.** Sei  $\mathfrak{m}_0 \subseteq \mathcal{O}_k$  ein Ideal und  $\mathfrak{m}_\infty$  ein formales quadratfreies Produkt von reellen archimedischen Stellen. Dann nennt man  $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$  einen *Divisor* von  $k$ .

**Erläuterung.** • Hierbei bezeichnen archimedische Stellen (oder auch unendliche Stellen) die Einbettungen von  $k$  in  $\mathbb{C}$  modulo komplexer Konjugation, d.h. jede reelle Einbettung und jedes Paar komplex konjugierter Einbettungen definiert eine archimedische Stelle. Jede archimedische Stelle definiert durch die Einbettung  $\tau$  (bzw. durch  $\sigma, \bar{\sigma}$ ) einen Betrag

$$|\alpha|_\tau := |\tau(\alpha)| \quad \forall \alpha \in k$$

bzw.

$$|\alpha|_\sigma := |\sigma(\alpha)| = |\bar{\sigma}(\alpha)| \quad \forall \alpha \in k.$$

Wir bezeichnen die Menge der archimedischen Stellen mit  $S_{k,\infty}$  und die Menge der nicht-archimedischen (endlichen) Stellen mit  $S_{k,f}$ . Letztere entsprechen den Primidealen von  $\mathcal{O}_k$ .

- Sei  $\mathfrak{p} \subseteq \mathcal{O}_k$  ein Primideal. Dann wird durch

$$|\alpha|_{\mathfrak{p}} := N_{k/\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(\alpha)} \quad \alpha \in k$$

ein Betrag definiert. Hierbei ist  $v_{\mathfrak{p}}(\alpha)$  definiert durch

$$\alpha \mathcal{O}_k = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}.$$

**Beispiele 1.2.** (1) Sei  $k = \mathbb{Q}$ , dann gibt es genau eine reelle Einbettung, die wir mit  $\infty$  bezeichnen. Beispiele für Divisoren sind

$$\begin{aligned}\mathfrak{m} &= (1) = \mathcal{O}_k, \\ \mathfrak{m} &= \infty, \\ \mathfrak{m} &= 2^7 \cdot 3^5 \cdot 17, \\ \mathfrak{m} &= 2^7 \cdot 3^5 \cdot 17 \cdot \infty.\end{aligned}$$

(2) Sei  $k = \mathbb{Q}(\sqrt{d})$  mit  $d < 0$  quadratfrei, dann gibt es keine reellen Einbettungen und Divisoren sind Ideale.

(3) Sei  $k = \mathbb{Q}(\sqrt{d})$  reell-quadratisch, d.h.  $d > 0$  quadratfrei. Dann gibt es zwei reelle Einbettungen, die wir mit  $\infty_1$  und  $\infty_2$  bezeichnen. Beispiele für Divisoren sind

$$\begin{aligned}\mathfrak{m} &= (1), \\ \mathfrak{m} &= \infty_1 \cdot \infty_2, \\ \mathfrak{m} &= \mathfrak{m}_0 \cdot \infty_1, \\ \mathfrak{m} &= \mathfrak{m}_0 \cdot \infty_2, \\ \mathfrak{m} &= \mathfrak{m}_0.\end{aligned}$$

**Definition 1.3.** Sei  $\alpha \in k^\times$  und  $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$  ein Divisor.

(1) Dann schreibt man

$$\alpha \equiv 1 \pmod{* \mathfrak{m}}$$

falls

- (i)  $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0)$  für alle  $\mathfrak{p} | \mathfrak{m}_0$  und
- (ii)  $\sigma(\alpha) > 0$  für alle  $\sigma$  in  $\mathfrak{m}_\infty$ .

(2) Die Gruppe

$$\mathcal{P}_k(\mathfrak{m}) := \{\alpha \mathcal{O}_k \mid \alpha \equiv 1 \pmod{* \mathfrak{m}}\}$$

heißt *Strahl modulo  $\mathfrak{m}$* .

(3) Sei  $\mathcal{I}_k(\mathfrak{m}) = \mathcal{I}_k(\mathfrak{m}_0)$  die Untergruppe von  $\mathcal{I}_k$  (Gruppe der gebrochenen Ideale von  $\mathcal{O}_k$ ) der zu  $\mathfrak{m}_0$  primen gebrochenen Ideale. Dann ist  $\mathcal{P}_k(\mathfrak{m})$  eine Untergruppe von  $\mathcal{I}_k(\mathfrak{m})$  und  $cl_k(\mathfrak{m}) := \mathcal{I}_k(\mathfrak{m}) / \mathcal{P}_k(\mathfrak{m})$  heißt *Strahlklassengruppe modulo  $\mathfrak{m}$* .

**Erläuterung.** • Es gilt wie zuvor für Hauptideale  $\mathfrak{m}_0 = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m}_0)}$ .

- Es ist  $\alpha \mathcal{O}_k \in \mathcal{P}_k(\mathfrak{m})$  genau dann, wenn ein  $\varepsilon \in \mathcal{O}_k^\times$  mit

$$\varepsilon \alpha \equiv 1 \pmod{* \mathfrak{m}}$$

existiert.

- Des Weiteren ist  $\mathfrak{a} \in \mathcal{I}_k(\mathfrak{m})$  genau dann, wenn es teilerfremde ganze Ideale  $\mathfrak{a}_1, \mathfrak{a}_2 \subseteq \mathcal{O}_k$  gibt, sodass  $\mathfrak{a} = \mathfrak{a}_1/\mathfrak{a}_2$  und  $\mathfrak{a}_1 + \mathfrak{m}_0 = (\mathfrak{a}_1, \mathfrak{m}_0) = \mathcal{O}_k = (\mathfrak{a}_2, \mathfrak{m}_0)$ .

**Beispiel 1.4.** Sei  $\mathfrak{m} = (1)$ , dann ist  $cl_k(\mathfrak{m}) = \mathcal{I}_k/\mathcal{P}_k$  die gewöhnliche Idealklassengruppe.

**Beispiele 1.5.** Sei  $k = \mathbb{Q}$ .

- (1) Sei  $\mathfrak{m} = (n) = n\mathbb{Z}$ . Betrachte die Abbildung  $\pi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow cl_{\mathbb{Q}}((n))$  induziert von

$$\bar{a} \mapsto a\mathbb{Z} = (a).$$

Diese ist wohldefiniert:

Angenommen  $a \equiv b \pmod{n}$ . Es gilt

$$\begin{aligned} (a) \equiv (b) \pmod{\mathcal{P}_{\mathbb{Q}}((n))} &\iff \left(\frac{a}{b}\right) \in \mathcal{P}_{\mathbb{Q}}((n)) \\ &\iff v_p\left(\pm\frac{a}{b} - 1\right) \geq v_p(n) \quad \forall p|n. \end{aligned}$$

Man rechnet

$$v_p\left(\frac{a}{b} - 1\right) = v_p(a - b) \geq v_p(n)$$

und erhält Wohldefiniertheit. Weiter ist  $\pi$  offensichtlich ein Homomorphismus. Dieser ist surjektiv, denn:

Sei  $\left(\frac{a_1}{a_2}\right) \in \mathcal{I}_{\mathbb{Q}}((n))$  mit  $a_1, a_2 \in \mathbb{Z}$ ,  $(a_1, a_2) = 1$  und  $(a_1 a_2, n) = 1$ . Dann ist  $\pi(\bar{a}_1 \bar{a}_2^{-1}) = \left(\frac{a_1}{a_2}\right) \mathcal{P}_{\mathbb{Q}}((n))$  und somit ist  $\pi$  surjektiv.

Ein Element  $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$  liegt im Kern von  $\pi$  genau dann, wenn  $v_p(\pm a - 1) \geq v_p(n)$  für alle  $p|n$  gilt, also genau dann, wenn  $a \equiv \pm 1 \pmod{n}$  ist. Somit ist die Sequenz

$$0 \rightarrow \{\pm 1\} \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\pi} cl_{\mathbb{Q}}((n)) \rightarrow 0$$

exakt.

- (2) Sei  $\mathfrak{m} = (n)\infty$ . Betrachte die Abbildung

$$\begin{aligned} \pi : (\mathbb{Z}/n\mathbb{Z})^\times &\rightarrow cl_{\mathbb{Q}}((n)\infty) \\ \bar{a} &\mapsto (a)\mathcal{P}_{\mathbb{Q}}((n)\infty), \end{aligned}$$

wobei o.E.  $a > 0$  ist. Dann ist  $\pi$  ein wohldefinierter Homomorphismus und  $\ker(\pi) = \{\bar{1}\}$ , d.h.  $\pi$  ist ein Isomorphismus.

**Notation.** • Wir schreiben

$$k_{\mathfrak{m}}^\times := \{\alpha \in k^\times \mid \alpha \equiv 1 \pmod{*}\mathfrak{m}\}.$$

Dann ist  $\mathcal{P}_k(\mathfrak{m}) = \{(\alpha) \mid \alpha \in k_{\mathfrak{m}}^\times\}$ .

- Definiere

$$(\mathcal{O}_k/\mathfrak{m})^\times := (\mathcal{O}_k/\mathfrak{m}_0)^\times \times \underbrace{\{\pm 1\} \times \cdots \times \{\pm 1\}}_{\text{einen Faktor für jedes } \sigma \text{ in } \mathfrak{m}_\infty} .$$

- Sei  $\alpha \in k^\times$  prim zu  $\mathfrak{m}_0$ . Dann gibt es  $\beta, \gamma \in \mathcal{O}_k$ , beide prim zu  $\mathfrak{m}_0$ , mit  $\alpha = \beta/\gamma$ .  
Definiere

$$\bar{\alpha} := \bar{\beta}/\bar{\gamma} \in (\mathcal{O}_k/\mathfrak{m}_0)^\times .$$

Dies ist unabhängig von der Wahl von  $\beta$  und  $\gamma$ .

Betrachte nun die Abbildung

$$\begin{aligned} \rho : \{ \alpha \in k^\times \mid (\alpha, \mathfrak{m}_0) = 1 \} &\longrightarrow (\mathcal{O}_k/\mathfrak{m})^\times \\ \alpha &\longmapsto (\bar{\alpha}, (\text{sgn}(\sigma(\alpha)))_{\sigma \in \mathfrak{m}_\infty}) . \end{aligned}$$

Mit Hilfe des starken Approximationsatzes, lässt sich die Surjektivität von  $\rho$  zeigen.

**Übung 1.6** (siehe Blatt 1, Aufgabe 1). *Zeige die Exaktheit der Sequenz*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{O}_k^\times \cap k_m^\times & \longrightarrow & \mathcal{O}_k^\times & \xrightarrow{\rho} & (\mathcal{O}_k/\mathfrak{m})^\times & \longrightarrow & cl_k(\mathfrak{m}) & \longrightarrow & cl_k & \longrightarrow & 0 \\ & & & & u & \longmapsto & (\bar{u}, (\text{sgn}(\sigma(u)))_{\sigma \in \mathfrak{m}_\infty}) & & \alpha \mathcal{P}_k(\mathfrak{m}) & \longmapsto & \alpha \mathcal{P}_k & & \\ & & & & & & \rho(\alpha) & \longmapsto & (\alpha) \mathcal{P}_k(\mathfrak{m}) & & & & \end{array}$$

Tipp: [Coh12, Prop.3.2.3].

**Korollar 1.7.** *Es gilt  $|cl_k(\mathfrak{m})| < \infty$ . Genauer:*

$$|cl_k(\mathfrak{m})| = |cl_k| \cdot \frac{|(\mathcal{O}_k/\mathfrak{m})^\times|}{[\mathcal{O}_k^\times : \mathcal{O}_k^\times \cap k_m^\times]} .$$

*Beweis.* siehe Blatt 1, Aufgabe 2. □

**Erinnerung 1.8.** Sei  $K/k$  eine Galois-Erweiterung von Zahlkörpern mit zugehörigen Ganzheitsringen  $\mathcal{O}_K$  bzw.  $\mathcal{O}_k$ . Sei  $\mathfrak{p} \subseteq \mathcal{O}_k$  ein Primideal und  $\mathfrak{P} \subseteq \mathcal{O}_K$  ein darüber liegendes Primideal. Der Restklassenkörper  $\bar{K} := \kappa(\mathfrak{P}) := \mathcal{O}_K/\mathfrak{P}$  ist eine endliche Erweiterung von  $\bar{k} := \kappa(\mathfrak{p}) := \mathcal{O}_k/\mathfrak{p}$  mit Restklassengrad  $f(\mathfrak{P}|\mathfrak{p}) := [\bar{K} : \bar{k}]$ . Die Galoisgruppe  $G := \text{Gal}(\bar{K}|\bar{k})$  ist zyklisch und wird erzeugt vom *Frobenius*

$$x \longmapsto x^q \quad \forall x \in \bar{K} ,$$

wobei  $q = |\bar{k}| = N_{k/\mathbb{Q}}(\mathfrak{p})$ .

Sei

$$Z := Z(\mathfrak{P}|\mathfrak{p}) := \{ \sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P} \}$$

die Zerlegungsgruppe und

$$T(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in Z \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \quad \forall \alpha \in \mathcal{O}_k\}$$

die Verzweigungsgruppe oder Trägheitsgruppe.

Es gilt: Die Sequenz

$$\begin{aligned} 0 \longrightarrow T(\mathfrak{P}|\mathfrak{p}) \hookrightarrow Z(\mathfrak{P}|\mathfrak{p}) \longrightarrow \text{Gal}(\overline{K}|\overline{k}) \longrightarrow 0 \\ \sigma \longmapsto (\overline{\alpha} \mapsto \overline{\sigma(\alpha)}) \end{aligned}$$

ist exakt. Weiter ist  $\mathfrak{P}|\mathfrak{p}$  genau dann unverzweigt, wenn  $|T(\mathfrak{P}|\mathfrak{p})| = 1$  ist.

Sei nun  $\mathfrak{P}|\mathfrak{p}$  unverzweigt. Dann gibt es einen (globalen) Frobenius  $\sigma_{\mathfrak{P}} \in Z(\mathfrak{P}|\mathfrak{p}) \subseteq G$ , der eindeutig durch

$$\sigma_{\mathfrak{P}}(\alpha) \equiv \alpha^{N_{K/\mathbb{Q}(\mathfrak{p})}} \pmod{\mathfrak{P}} \quad \forall \alpha \in \mathcal{O}_K$$

bestimmt ist.

Seien  $\mathfrak{P}, \mathfrak{P}'$  Primideale über  $\mathfrak{p}$ . Dann gibt es  $\tau \in G$  mit  $\tau(\mathfrak{P}) = \mathfrak{P}'$  und es gilt:

$$Z(\mathfrak{P}'|\mathfrak{p}) = \{\sigma \in G \mid \sigma(\mathfrak{P}') = \mathfrak{P}'\} = \tau Z(\mathfrak{P}|\mathfrak{p}) \tau^{-1}$$

und

$$T(\mathfrak{P}'|\mathfrak{p}) = \tau T(\mathfrak{P}|\mathfrak{p}) \tau^{-1}.$$

Weiter gilt

$$\begin{aligned} \implies \sigma_{\mathfrak{P}}(\tau^{-1}(\alpha)) &\equiv \tau^{-1}(\alpha)^{N_{\mathfrak{p}}} \pmod{\mathfrak{P}} && \forall \alpha \in \mathcal{O}_K \\ \implies (\tau \sigma_{\mathfrak{P}} \tau^{-1})(\alpha) &\equiv \alpha^{N_{\mathfrak{p}}} \pmod{\mathfrak{P}'} && \forall \alpha \in \mathcal{O}_K \\ \implies \sigma_{\mathfrak{P}'} &= \tau \sigma_{\mathfrak{P}} \tau^{-1} \end{aligned}$$

Falls also  $K/k$  abelsch ist, so folgt  $\sigma_{\mathfrak{P}'} = \sigma_{\mathfrak{P}}$  und wir schreiben  $\sigma_{\mathfrak{p}}$  für den Frobenius.

**Definition 1.9** (Artinabbildung). Sei  $K/k$  abelsch. Dann induziert  $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$  einen Homomorphismus

$$\begin{aligned} \mathcal{I}_k(d_{K/k}) &\longrightarrow \text{Gal}(K|k) \\ \mathfrak{a} &\longmapsto (\mathfrak{a}, K/k) = \sigma_{\mathfrak{a}} \end{aligned}$$

durch multiplikative Fortsetzung, die sogenannte *Artinabbildung*.

**Erläuterung.** Falls  $\mathfrak{a} \in \mathcal{I}_k(d_{K/k})$ , so ist  $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ ,  $e_{\mathfrak{p}} \in \mathbb{Z}$  mit fast allen  $e_{\mathfrak{p}} = 0$  und insbesondere  $e_{\mathfrak{p}} = 0$  falls  $\mathfrak{p}$  verzweigt.

Dann gilt:

$$(\mathfrak{a}, K/k) = \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{e_{\mathfrak{p}}}.$$

Dies ist wohldefiniert, da  $\mathcal{I}_k(\mathfrak{b})$  (für ein ganzes Ideal  $\mathfrak{b} \subseteq \mathcal{O}_k$ ) frei von den Primidealen  $\mathfrak{p}$ , die teilerfremd zu  $\mathfrak{b}$  sind, erzeugt wird.

**Satz 1.10.** Sei  $K/k$  abelsch. Dann gibt es einen Divisor  $\mathfrak{f}$  von  $k$  mit folgenden Eigenschaften:

- (1) Eine Stelle  $\mathfrak{p}$  verzweigt in  $K/k$  genau dann, wenn  $\mathfrak{p}|\mathfrak{f}$ .
- (2) Zu jedem Divisor  $\mathfrak{m}$  mit  $\mathfrak{f}|\mathfrak{m}$  gibt es eine eindeutige Untergruppe  $H$  mit  $\mathcal{P}_k(\mathfrak{m}) \leq H \leq \mathcal{I}_k(\mathfrak{m})$ , sodass

$$\begin{aligned} \mathcal{I}_k(\mathfrak{m})/H &\longrightarrow \text{Gal}(K|k) \\ \mathfrak{a}H &\longmapsto (\mathfrak{a}, K/k) \end{aligned}$$

ein Isomorphismus ist.

Genauer gilt:

$$H = \mathcal{P}_k(\mathfrak{m}) \cdot N_{K/k}(\mathcal{I}_K(\mathfrak{m}_0\mathcal{O}_K)).$$

**Erläuterung.** In ((1)) sind auch unendliche Stellen  $\mathfrak{p}$  berücksichtigt. Verzweigung von unendlichen Stellen wird folgendermaßen definiert:

Sei  $v$  eine unendliche Stelle von  $k$ . Dann entspricht  $v$  entweder einer reellen Einbettung  $\tau : k \hookrightarrow \mathbb{R}$  oder einem Paar komplexer Einbettungen  $\tau, \bar{\tau} : k \hookrightarrow \mathbb{C}$  wobei  $\tau(k) \not\subseteq \mathbb{R}$ .

Sei  $w$  eine Stelle über  $v$ , d.h.  $w$  entspricht entweder einer reellen Einbettung  $\sigma : K \hookrightarrow \mathbb{R}$  oder einem Paar komplexer Einbettungen  $\sigma, \bar{\sigma} : K \hookrightarrow \mathbb{C}$  wobei  $\sigma(K) \not\subseteq \mathbb{R}$  und  $\sigma|_k = \tau$ .

**Definition 1.11.** Sei  $K/k$  galoissch,  $G = \text{Gal}(K|k)$  und  $g \in G$ . Dann definiert man  $g(w)$  als die Stelle, die zu  $\sigma \circ g$  korrespondiert.

Dies ist wohldefiniert, denn:

- (1) Falls  $\sigma$  reell ist, ist nichts zu zeigen.
- (2) Falls  $\sigma$  komplex ist, so ist zu zeigen  $\bar{\sigma} \circ g = \overline{\sigma \circ g}$ . Dies gilt offensichtlich.

Betrachte nun eine Stelle  $w|v$  mit korrespondierender Einbettung  $\sigma$  und  $g \in G$ . Dann gilt

$$(\sigma \circ g)|_k = \sigma|_k = \tau$$

und es folgt  $g(w)|v$ .

Weiter wirkt  $G$  transitiv auf den Stellen über  $v$ :

Betrachte

$$\begin{array}{ccc} k(\alpha) = K & \xleftarrow{\sigma} & \mathbb{C} \\ & \downarrow n & \parallel \\ k & \xleftarrow{\tau} & \mathbb{C} \end{array}$$

Aus der Algebra ist bekannt, dass es  $n$  verschiedene Fortsetzungen von  $\tau$  gibt. Falls  $\sigma_0 : K \rightarrow \mathbb{C}$  eine feste Fortsetzung ist, so sind durch  $\sigma_0 \circ g$ ,  $g \in G$ , sämtliche Fortsetzungen definiert.



**Definition 1.12.** Die Zerlegungs- und Trägheitsgruppe für unendliche Stellen  $w|v$  sind

$$T(w|v) = Z(w|v) := \{g \in G \mid g(w) = w\}.$$

**Übung 1.13** (siehe Blatt 2, Aufgabe 2). Sei  $K/k$  galoissch. Zeige:

(1)  $|T(w|v)| \in \{1, 2\}$ .

(2)  $|T(w|v)| = 2 \iff \tau$  ist reell und  $\sigma$  komplex.

Dies beschreibt die Verzweigung der unendlichen Stellen.

**Definition 1.14.** (1) Es gibt ein minimales  $\mathfrak{f}$  mit den Eigenschaften von Satz 1.10. Dieses  $\mathfrak{f}$  heißt *Führer* oder *Konduktor* von  $K/k$ . Wir schreiben  $\mathfrak{f}_{K/k}$ .

(2) Jedes  $\mathfrak{m}$  mit  $\mathfrak{f}_{K/k} | \mathfrak{m}$  nennt man einen *Erklärungsmodul* von  $K/k$ .

**Satz 1.15** (Existenzsatz). Sei  $\mathfrak{m}$  ein Divisor von  $k$  und  $H \leq \mathcal{I}_k(\mathfrak{m})$  mit  $\mathcal{P}_k(\mathfrak{m}) \leq H \leq \mathcal{I}_k(\mathfrak{m})$ . Dann gibt es eine eindeutig bestimmte abelsche Erweiterung  $K/k$  mit:

(1) Ist eine Stelle  $\mathfrak{p}$  verzweigt in  $K/k$ , so folgt  $\mathfrak{p} | \mathfrak{m}$ .

(2) Es gilt  $H = \mathcal{P}_k(\mathfrak{m}) \cdot N_{K/k}(\mathcal{I}_K(\mathfrak{m}_0 \mathcal{O}_K))$  und die Abbildung

$$\begin{aligned} \mathcal{I}_k(\mathfrak{m})/H &\longrightarrow \text{Gal}(K|k) \\ \mathfrak{a}H &\longmapsto (\mathfrak{a}, K/k) \end{aligned}$$

ist ein Isomorphismus.

**Definition 1.16.** Diese eindeutig bestimmte Erweiterung  $K$  heißt der *Klassenkörper* zu  $H$ .

**Satz 1.17.** Seien  $K_1/k$  und  $K_2/k$  zwei abelsche Erweiterungen mit den Führern  $\mathfrak{f}_1$  und  $\mathfrak{f}_2$ . Sei  $\mathfrak{m}$  ein gemeinsames Vielfaches von  $\mathfrak{f}_1$  und  $\mathfrak{f}_2$  und seien  $H_1, H_2 \leq \mathcal{I}_k(\mathfrak{m})$  die zugehörigen Untergruppen gemäß Satz 1.10. Dann gilt:

$$K_1 \subseteq K_2 \iff H_1 \supseteq H_2.$$

**Beispiel 1.18.** Sei  $k = \mathbb{Q}$  und  $K = \mathbb{Q}(\zeta_n)$ . Sei  $p$  prim mit  $p \nmid n$  (d.h.  $p$  ist unverzweigt) und sei  $\sigma_{p\mathbb{Z}}$  der zugehörige Frobenius. Es gilt:

$$\sigma_{p\mathbb{Z}} = (\zeta_n \xrightarrow{\sigma_p} \zeta_n^p)$$

**Erinnerung 1.19.** Für zyklotomische Erweiterungen gilt

$$\begin{aligned} \text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) &\cong (\mathbb{Z}/n\mathbb{Z})^\times \\ (\zeta_n \xrightarrow{\sigma_a} \zeta_n^a) &\longleftarrow \bar{a} \end{aligned}$$

Die Artinabbildung ist von der Form

$$\begin{aligned} \mathcal{I}_{\mathbb{Q}}(n\mathbb{Z}) &\longrightarrow \text{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \\ a\mathbb{Z} &\longmapsto \sigma_{|a|} \end{aligned}$$

Ziel: Finde das zugehörige  $H \leq \mathcal{I}_{\mathbb{Q}}(n\mathbb{Z})$  gemäß Satz 1.10.

Es gilt  $H = \ker(\_, K/k)$ . Sei  $r\mathbb{Z} \in \mathcal{I}_{\mathbb{Q}}(n\mathbb{Z})$  mit  $r = \frac{r_1}{r_2}$ , wobei die  $r_i \in \mathbb{N}$  teilerfremd zu  $n$  sind.

$$\begin{aligned} (r\mathbb{Z}, K/k) = \text{id} &\iff \zeta_n^{|r_1|} = \zeta_n^{|r_2|} \\ &\iff |r_1| \equiv |r_2| \pmod{n} \\ &\iff v_p \left( \left| \frac{r_1}{r_2} \right| - 1 \right) \geq v_p(n) \quad \forall p|n \\ &\iff r\mathbb{Z} \in \mathcal{P}_{\mathbb{Q}}(n\mathbb{Z}\infty) \end{aligned}$$

Also ist  $\mathbb{Q}(\zeta_n)$  der zu  $H = \mathcal{P}_{\mathbb{Q}}(n\mathbb{Z}\infty)$  gehörige Klassenkörper.

**Beispiel 1.20.** Betrachte

$$\begin{array}{ccc} \mathbb{Q}(\zeta_n) & \longleftrightarrow & \mathcal{P}_{\mathbb{Q}}(n\mathbb{Z}\infty) \\ | & & | \\ \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n)^+ & \longleftrightarrow & \mathcal{P}_{\mathbb{Q}}(n\mathbb{Z}) \\ | & & \\ \mathbb{Q} & & \end{array}$$

Der Zwischenkörper korrespondiert zu  $\mathcal{P}_{\mathbb{Q}}(n\mathbb{Z})$ . Dies illustriert Satz 1.17:  
 $\mathcal{P}_{\mathbb{Q}}(n\mathbb{Z}\infty) \subseteq \mathcal{P}_{\mathbb{Q}}(n\mathbb{Z}) \subseteq \mathcal{I}_{\mathbb{Q}}(n\mathbb{Z})$ .

### Konsequenzen

Betrachte  $\mathfrak{m} = (1)$  und  $H = \mathcal{P}_k((1)) = \mathcal{P}_k$  sei die Gruppe der Hauptideale. Sei  $k(1)$  der zugehörige Klassenkörper gemäß Satz 1.15. Dann gilt

**Satz 1.21.**  $k(1)$  ist die maximal unverzweigte abelsche Erweiterung von  $k$ . Insbesondere gilt für jede unverzweigte abelsche Erweiterung  $K/k$ :

- (1)  $[K : k] \leq h_k < \infty$ ,
- (2)  $K \subseteq k(1)$ .

Ferner gilt  $cl_k \cong \text{Gal}(k(1)|k)$  mittels der Artinabbildung.

**Definition 1.22.**  $k(1)$  heißt *Hilbertscher Klassenkörper*.

*Beweis.* Da  $K/k$  endlich, abelsch und unverzweigt ist folgt mit Satz 1.10, dass  $K$  modulo  $\mathfrak{f} = (1)$  definiert ist. Nach Satz 1.17 ist somit  $K \subseteq k(1)$ , da die zugehörige Gruppe  $H$  über  $\mathcal{P}_k((1))$  liegt.  $\square$

**Satz 1.23.** Ein Primideal  $\mathfrak{p}$  ist genau dann voll zerlegt in  $k(1)/k$ , wenn  $\mathfrak{p}$  ein Hauptideal ist.

*Beweis.* Betrachte die bijektive Abbildung

$$\begin{aligned} G/Z(\mathfrak{p}) &\longrightarrow \{\mathfrak{P}|\mathfrak{p}\} \\ gZ(\mathfrak{p}) &\longmapsto g\mathfrak{P}_0 \end{aligned}$$

wobei  $\mathfrak{P}_0|\mathfrak{p}$  fest gewählt sei. Falls  $\mathfrak{p}$  unverzweigt ist, so gilt:

$$\begin{aligned} \mathfrak{p} \text{ voll zerlegt} &\iff Z(\mathfrak{p}) = \{1\} \\ &\iff \sigma_{\mathfrak{p}} = 1 \\ &\iff (\mathfrak{p}, K/k) = 1 \\ &\iff \mathfrak{p} \in H \end{aligned}$$

und  $H$  ist gerade die Gruppe der Hauptideale. □

**Übung 1.24.** Sei  $K/k$  der Klassenkörper zu  $H \leq \mathcal{I}_k(\mathfrak{m})$ . Sei weiter  $\mathfrak{p} \subseteq \mathcal{O}_k$  ein Primideal mit  $(\mathfrak{p}, \mathfrak{m}) = 1$  und  $f_{\mathfrak{p}} = [\mathcal{O}_K/\mathfrak{p} : \mathcal{O}_k/\mathfrak{p}]$  der Restklassengrad. Dann gilt:

$$f_{\mathfrak{p}} = \text{ord}_{\mathcal{I}_k(\mathfrak{m})/H}(\mathfrak{p}H).$$

**Definition 1.25.** Falls  $H = \mathcal{P}_k(\mathfrak{m})$ , so heißt der zu  $H$  gehörige Klassenkörper *Strahlklassenkörper modulo  $\mathfrak{m}$* .

**Notation.** Wir bezeichnen den Strahlklassenkörper modulo  $\mathfrak{m}$  mit  $k(\mathfrak{m})$ .

**Bemerkung 1.26.** Für  $\mathfrak{m}|\mathfrak{n}$  gilt  $k(\mathfrak{m}) \subseteq k(\mathfrak{n})$ .

*Beweis.*  $k(\mathfrak{m})$  kann nach Satz 1.10 modulo  $\mathfrak{n}$  erklärt werden. Dann korrespondiert  $k(\mathfrak{m})$  nach Satz 1.15 zu  $\mathcal{P}_k(\mathfrak{n})N_{k(\mathfrak{m})/k}(I_{k(\mathfrak{m})}(\mathfrak{n})) \supseteq \mathcal{P}_k(\mathfrak{n})$ . Dann folgt mit Satz 1.17  $k(\mathfrak{m}) \subseteq k(\mathfrak{n})$ . □

**Warnung.** Die Umkehrung gilt nicht!

**Beispiele 1.27.** (1) Sei  $k = \mathbb{Q}$  und  $n \equiv 2 \pmod{4}$ , d.h.  $n = 2n_1$  mit  $n_1$  ungerade. Dann ist  $[k((n)\infty) : k] = \varphi(n)$  ( $\varphi$  bezeichnet die Eulersche  $\varphi$ -Funktion, d.h.  $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ ).

Es gilt  $k((n_1)\infty) \subseteq k((n)\infty)$ , aber wegen  $\varphi(n) = \varphi(2)\varphi(n_1) = \varphi(n_1)$  folgt sogar  $k((n)\infty) = k((n_1)\infty)$ .

(2) Sei  $k$  imaginär-quadratisch. Sei  $\mathfrak{m}$  ein Divisor, d.h.  $\mathfrak{m} = \mathfrak{m}_0$ . Definiere  $w(1) := |\mu_k| \in \{2, 4, 6\}$ , wobei  $\mu_k$  die Gruppe der Einheitswurzeln in  $k$  bezeichnet, und

$$w(\mathfrak{m}) := |\{\zeta \in \mu_k \mid \zeta \equiv 1 \pmod{\mathfrak{m}}\}|$$

**Übung 1.28.** Es gilt

$$[k(\mathfrak{m}) : k] = h_k \frac{w(1)}{w(\mathfrak{m})} \varphi_k(\mathfrak{m})$$

wobei  $\varphi_k(\mathfrak{m}) := |(\mathcal{O}_k/\mathfrak{m})^\times|$ .

Sei nun  $d_k \neq -3, -4$ , dann ist  $w(1) = 2$ . Sei nun  $\mathfrak{m} = (2)$ , dann gilt:

$$[k(2) : k] = h_k \frac{2}{2} \varphi_k(2) = \begin{cases} h_k & 2 = \mathfrak{p}\bar{\mathfrak{p}}, \mathfrak{p} \neq \bar{\mathfrak{p}} \\ 3h_k & 2 = \mathfrak{p} \\ 2h_k & 2 = \mathfrak{p}^2 \end{cases}$$

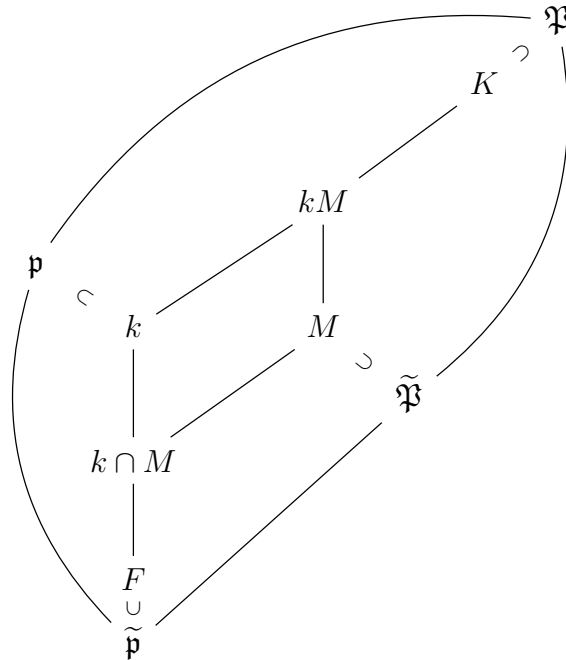
Also gilt  $k(2) = k(1)$  falls 2 zerlegt ist in  $k/\mathbb{Q}$ .

**Korollar 1.29** (zu Satz 1.17). *Jede abelsche Erweiterung  $K/k$  ist in einem Strahlklassenkörper enthalten.*

**Korollar 1.30** (Satz von Kronecker-Weber). *Jede abelsche Erweiterung  $K/\mathbb{Q}$  ist in einem Kreisteilungskörper enthalten.*

### Eine funktorielle Eigenschaft

Betrachte die Situation



wobei das Primideal  $\mathfrak{P}$  fest gewählt ist und die Ideale  $\tilde{\mathfrak{p}}, \mathfrak{p}$  und  $\tilde{\mathfrak{P}}$  unter  $\mathfrak{P}$  liegen. Es seien  $M/F$  und  $K/k$  abelsch, dann ist Abbildung

$$\text{Gal}(K|k) \longrightarrow \text{Gal}(M|k \cap M) \subseteq \text{Gal}(M|F)$$

surjektiv. Weiter seien  $\mathfrak{p}, \tilde{\mathfrak{p}}$  unverzweigt in  $K/k$  bzw.  $M/F$ .

Sei nun  $f = [\bar{k} : \bar{F}]$  mit  $\bar{k} = \mathcal{O}_{K/\mathfrak{p}}$  und  $\bar{F} = \mathcal{O}_{F/\tilde{\mathfrak{p}}}$ . Dann gilt  $N_{k/F}(\mathfrak{p}) = \tilde{\mathfrak{p}}^f$  und

$$\left( \sigma_{\mathfrak{p}}^{K/k} \Big|_M \right) (x) \equiv x^{N_{k/\mathbb{Q}}(\mathfrak{p})} \pmod{\underbrace{\mathfrak{P} \cap \mathcal{O}_M}_{=\tilde{\mathfrak{P}}}}$$

für  $x \in \mathcal{O}_M$ . Andererseits ist

$$(N_{k/F}(\mathfrak{p}), M/F) = (\tilde{\mathfrak{p}}^f, M/F) = (\tilde{\mathfrak{p}}, M/F)^f = \left(\sigma_{\tilde{\mathfrak{p}}}^{M/F}\right)^f$$

und

$$\left(\sigma_{\tilde{\mathfrak{p}}}^{M/F}\right)^f(x) \equiv x^{N_{F/\mathbb{Q}}(\tilde{\mathfrak{p}})^f} \pmod{\tilde{\mathfrak{P}}}.$$

Ferner gilt

$$N_{k/\mathbb{Q}}(\mathfrak{p}) = N_{F/\mathbb{Q}}N_{k/F}(\mathfrak{p}) = N_{F/\mathbb{Q}}(\tilde{\mathfrak{p}})^f.$$

Es folgt also

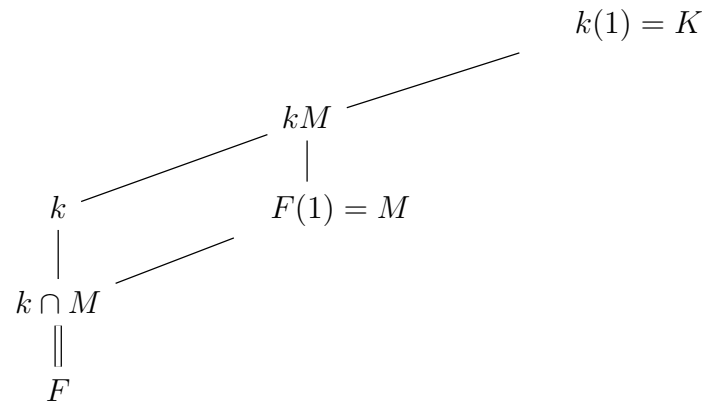
$$(\mathfrak{p}, K/k)|_M = (N_{k/F}(\mathfrak{p}), M/F)$$

oder allgemeiner

$$(\mathfrak{a}, K/k)|_M = (N_{k/F}(\mathfrak{a}), M/F)$$

für alle  $\mathfrak{a}$ , wo dies Sinn ergibt.

**Anwendung.** Betrachte den Fall



Dann ist die Restriktionsabbildung

$$\text{Gal}(K|k) \xrightarrow{\text{res}} \text{Gal}(M|F)$$

surjektiv und das Diagramm

$$\begin{array}{ccc}
 cl_k = \mathcal{I}_k/\mathcal{P}_k & \xrightarrow[\cong]{(-, K/k)} & \text{Gal}(K|k) \\
 \downarrow N_{k/F} & & \downarrow \text{res} \\
 cl_F = \mathcal{I}_F/\mathcal{P}_F & \xrightarrow[\cong]{(-, M/F)} & \text{Gal}(M|F)
 \end{array}$$

kommutiert.

**Satz 1.31.** Falls  $k/F$  keine unverzweigte Erweiterung  $L/F$  mit  $L \neq F$  enthält, so ist  $N_{k/F}$  surjektiv. Insbesondere gilt  $h_F|h_k$ .

**Anwendung.** Hat die Erweiterung  $k/F$  Primzahlgrad und gibt es eine verzweigte Stelle, so folgt  $h_F|h_k$ .

## 1.2 Lokale Klassenkörpertheorie

Ziel: Beschreibung aller abelschen, endlichen Erweiterungen einer fixierten endlichen Erweiterung  $k$  von  $\mathbb{Q}_p$  durch Daten in  $k$ .

**Erinnerung 1.32.**  $\mathbb{Q}_p$  ist der Quotientenkörper vom diskreten Bewertungsring  $\mathbb{Z}_p$  mit maximalem Ideal  $p\mathbb{Z}_p$ , Bewertung  $v_p : \mathbb{Q}_p^\times \rightarrow \mathbb{Z}$  ( $v_p(0) := \infty$ ) und Absolutbetrag  $|\alpha|_p = p^{-v_p(\alpha)}$ . Dann ist

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p \mid v_p(\alpha) \geq 0\}$$

und

$$\mathbb{Z}_p^\times = \{\alpha \in \mathbb{Q}_p \mid v_p(\alpha) = 0\}.$$

Diese Konzepte lassen sich auf eine endliche Erweiterung  $k/\mathbb{Q}_p$  übertragen:

$k$  ist Quotientenkörper des diskreten Bewertungsring  $\mathcal{O}_k$  mit maximalem Ideal  $\mathfrak{p}_k = \pi_k \mathcal{O}_k$ , wobei  $v_k(\pi_k) = 1$ . Die Ideale in  $\mathcal{O}_k$  sind gegeben durch

$$\mathfrak{p}_k^n = \pi_k^n \mathcal{O}_k$$

und für die Bewertung gilt

$$\begin{aligned} v_k : k &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ v_k|_{\mathbb{Q}_p} &= ev_p \end{aligned}$$

mit dem Verzweigungsindex  $e = e_{k/\mathbb{Q}_p}$ , d.h.  $p\mathcal{O}_k = \mathfrak{p}_k^e$ .

Der zugehörige Absolutbetrag ist definiert als

$$|\alpha|_k := (N_{k/\mathbb{Q}_p}(\mathfrak{p}_k))^{-v_k(\alpha)} = p^{-fv_k(\alpha)}$$

für alle  $\alpha \in k$ , wobei

$$f = f_{k/\mathbb{Q}_p} = [\mathcal{O}_k/\mathfrak{p}_k : \underbrace{\mathbb{Z}_p/p\mathbb{Z}_p}_{=\mathbb{F}_p}].$$

**Notation.** Wir definieren die *Einseinheiten  $n$ -ter Stufe* als

$$\begin{aligned} \mathcal{U}_k^n &:= 1 + \mathfrak{p}_k^n, & n \geq 1 \\ \mathcal{U}_k^0 &:= \mathcal{O}_k^\times \end{aligned}$$

Die Gruppe  $k^\times$  ist eine topologische Gruppe, wobei die  $\mathcal{U}_k^n$  eine Umgebungsbasis der 1 darstellen. Explizit ist  $V \subseteq k^\times$  genau dann offen, wenn für alle  $v \in V$  ein  $n \in \mathbb{N}$  existiert, sodass  $v\mathcal{U}_k^n \subseteq V$  ist.

Die Struktur von  $k^\times$  lässt sich nun folgendermaßen beschreiben:

$$k^\times = \langle \pi_k \rangle \times \mathcal{U}_k^0 = \langle \pi_k \rangle \times \mathcal{U}_k^1 \times \mu_{q-1}$$

wobei  $q = |\mathcal{O}_k/\mathfrak{p}_k|$  ist (die Gleichung  $x^{q-1} - 1 = 0$  hat eine Lösung in  $\bar{k} = \mathcal{O}_k/\mathfrak{p}_k$ . Dann folgt mit Hensels Lemma, dass die  $(q-1)$ -ten Einheitswurzeln in  $\mathcal{U}_k^0$  enthalten sind).

**Satz 1.33.** (1) Sei  $K/k$  eine endliche, abelsche Erweiterung. Dann gibt es eine kanonische, surjektive Abbildung, die sogenannte Artinabbildung,

$$(\_, K/k) : k^\times \longrightarrow \text{Gal}(K|k)$$

mit  $\ker((\_, K/k)) = N_{K/k}(K^\times)$  (die Untergruppe  $N_{K/k}(K^\times) \leq k^\times$  ist offen (siehe z.B. [Ser13]).

Falls  $K/k$  unverzweigt ist, so gilt

$$(a, K/k) = \sigma_{K/k}^{v_k(a)}$$

für alle  $a \in k^\times$ , wobei  $\sigma_{K/k}$  den Frobenius bezeichnet.

(2) Sei  $H \leq k^\times$  eine offene Untergruppe von endlichem Index. Dann gibt es eine eindeutig bestimmte abelsche Erweiterung  $K/k$ , sodass  $N_{K/k}(K^\times) = H$ .

**Erläuterung.** Die Situation in Teil ((1)) ist von der folgenden Form:

$$\begin{array}{c} K \supset \mathcal{O}_K \supset \mathfrak{P} \\ | \\ k \supset \mathcal{O}_k \supset \mathfrak{p} \\ | \\ \mathbb{Q}_p \end{array}$$

wobei  $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^e$ . Sei  $\bar{K} := \mathcal{O}_K/\mathfrak{P}$  und  $\bar{k} := \mathcal{O}_k/\mathfrak{p}$ . Die Sequenz

$$\begin{array}{ccccccc} 0 & \longrightarrow & G_0 & \hookrightarrow & G & \longrightarrow & \text{Gal}(\bar{K}|\bar{k}) \longrightarrow 0 \\ & & & & \sigma & \longmapsto & (\bar{a} \mapsto \bar{\sigma}(\bar{a})) \end{array}$$

ist exakt, wobei

$$G_0 := I := \{\sigma \in G \mid \sigma(a) \equiv a \pmod{\mathfrak{P}}, \forall a \in \mathcal{O}_K\}.$$

Es ist  $e = |G_0|$ , d.h.

$$\begin{array}{ccc} G & \xrightarrow{\cong} & \text{Gal}(\bar{K}|\bar{k}) \\ \sigma_{K/k} & \longmapsto & (x \mapsto x^{|\bar{k}|}) \end{array}$$

falls  $K/k$  unverzweigt ist.

**Bemerkung 1.34.** Satz 1.33 definiert eine Bijektion

$$K \longmapsto N_{K/k}(K^\times)$$

zwischen endlichen, abelschen Erweiterungen  $K/k$  und Untergruppen von  $k^\times$ , die offen sind und endlichen Index haben.

**Satz 1.35.** Seien  $H_1, H_2 \leq k^\times$  offen und von endlichem Index. Seien  $K_1, K_2$  die zugehörigen Klassenkörper. Dann gilt:

$$(1) H_1 \leq H_2 \iff K_1 \supseteq K_2,$$

$$(2) H_1 \cap H_2 \iff K_1 K_2,$$

$$(3) H_1 H_2 \iff K_1 \cap K_2.$$

**Satz 1.36.** Sei  $K/k$  eine endliche, abelsche Erweiterung. Dann induziert die Artinabbildung einen Isomorphismus

$$\mathcal{U}_k^0 / N_{K/k}(\mathcal{U}_K^0) \longrightarrow G_0$$

**Korollar 1.37.** Sei  $K/k$  eine endliche, abelsche Erweiterung. Dann ist  $K/k$  genau dann unverzweigt, wenn  $N_{K/k}$  surjektiv auf den Einheiten ist.

### 1.3 Globale Klassenkörpertheorie (ideltheoretisch)

Literatur: [CNT87].

Sei  $k/\mathbb{Q}$  ein Zahlkörper und  $v$  eine Stelle von  $k$ . Wir bezeichnen die Kompletzierung bei  $v$  mit  $k_v$ . Falls  $v$  endlich ist (d.h.  $v$  korrespondiert zu einem Primideal  $\mathfrak{p}$ ), ist  $k_v$  ein  $\mathfrak{p}$ -adischer Körper mit den Einheiten  $\mathcal{U}_v := \mathcal{U}_{k_v} := \mathcal{U}_{k_v}^0$ . Ist  $v$  unendlich, so ist  $k_v = \mathbb{R}$  oder  $k_v = \mathbb{C}$  und wir setzen  $\mathcal{U}_v := \mathcal{U}_{k_v} := k_v^\times$ .

**Definition 1.38.** Die Gruppe

$$\mathcal{J}_k := \{a = (a_v)_v \in \prod_v k_v^\times \mid a_v \in \mathcal{U}_v \text{ für fast alle } v\}$$

heißt die *Idelgruppe von  $k$* . Die Untergruppe

$$\mathcal{U}_k = \prod_v \mathcal{U}_v$$

nennt man die Gruppe der *Einheitsidele*.

$\mathcal{J}_k$  ist eine topologische Gruppe. Eine Umgebungsbasis der 1 ist gegeben durch

$$\prod_{v \in S} W_v \times \prod_{v \notin S} \mathcal{U}_v \leq \mathcal{J}_k,$$

wobei  $S$  alle endlichen Teilmengen von Stellen von  $k$  und  $W_v$  jeweils eine Umgebungsbasis der 1 in  $k_v^\times$  durchläuft.

Betrachte

$$\begin{aligned} \iota_k : k^\times &\hookrightarrow \mathcal{J}_k \\ \alpha &\longmapsto (\iota_v(\alpha))_v \end{aligned}$$



**Erläuterung.** Ist  $v$  endlich, so gibt es eine kanonische Abbildung  $\iota_v : k \hookrightarrow k_v$ , die  $\alpha \in k$  auf die konstante Cauchy-Folge mit Wert  $\alpha$  abbildet. Ist  $v$  unendlich, so korrespondiert  $v$  zu einer Einbettung  $\tau : k \hookrightarrow \mathbb{C}$  und  $\iota_v(\alpha) = \tau(\alpha) \in k_v$ .

**Übung 1.39** (siehe Blatt 3, Aufgabe 1).  $\iota_k(k^\times)$  ist eine diskrete Untergruppe von  $\mathcal{J}_k$ .

Man nennt  $\iota_k(k^\times)$  die Untergruppe der *Hauptidele* von  $k$ .

Sei  $v_0$  eine fixierte Stelle von  $k$ . Dann erhalten wir eine Einbettung

$$\begin{aligned} k_{v_0}^\times &\hookrightarrow \mathcal{J}_k \\ \alpha &\longmapsto (x_v)_v \end{aligned}$$

mit

$$x_v = \begin{cases} 1, & v \neq v_0 \\ \alpha, & v = v_0 \end{cases}$$

Sei  $K/k$  eine Erweiterung von Zahlkörpern. Dann definiert man eine Norm  $N_{K/k} : \mathcal{J}_K \rightarrow \mathcal{J}_k$  durch

$$N_{K/k}((x_w)_w) := (y_v)_v$$

mit

$$y_v := \prod_{w|v} N_{K_w/k_v}(x_w).$$

Es gilt

$$N_{K/k}(\iota_K(\alpha)) = \iota_k(N_{K/k}(\alpha)) \tag{1.1}$$

für  $\alpha \in K^\times$ .

**Definition 1.40.** Sei  $k$  ein Zahlkörper. Dann heißt

$$\mathcal{C}_k := \mathcal{J}_k/k^\times$$

die *Idelklassengruppe*.

Wegen (1.1) induziert die Norm eine Normabbildung  $N_{K/k} : \mathcal{C}_K \rightarrow \mathcal{C}_k$ .

**Definition 1.41.** (1) Sei  $\mathfrak{m}$  ein Divisor von  $k$  und  $\alpha = (\alpha_v)_v \in \mathcal{J}_k$ . Dann schreibt man

$$\alpha \equiv 1 \pmod{*\mathfrak{m}},$$

falls

- (i)  $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}} - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0)$  für alle  $\mathfrak{p}|\mathfrak{m}_0$  und

(ii)  $\alpha_v > 0$  für alle  $v | \mathfrak{m}_\infty$ .

(2) Die Untergruppe

$$\mathcal{J}_k(\mathfrak{m}) := \{\alpha = (\alpha_v)_v \in \mathcal{J}_k \mid \alpha \equiv 1 \pmod{*}\mathfrak{m}\} \leq \mathcal{J}_k$$

heißt *Strahl modulo  $\mathfrak{m}$* .

(3) Die Gruppe  $\mathcal{C}_k(\mathfrak{m}) := \mathcal{J}_k/k^\times \mathcal{J}_k(\mathfrak{m})$  heißt *Strahlklassengruppe modulo  $\mathfrak{m}$* .

**Notation.** Für eine Untergruppe  $V \leq \mathcal{J}_k$  sei  $V_{\mathfrak{m}} := V \cap \mathcal{J}_k(\mathfrak{m})$ .

**Lemma 1.42.** *Es gilt*

$$\mathcal{J}_k(\mathfrak{m})/k_{\mathfrak{m}}^\times \xrightarrow{\cong} \mathcal{J}_k/k^\times.$$

*Beweis.* Es ist zu zeigen, dass

$$\begin{array}{ccccc} \mathcal{J}_k(\mathfrak{m}) & \xrightarrow{\subseteq} & \mathcal{J}_k & \longrightarrow & \mathcal{J}_k/k^\times \\ & & \searrow \psi & \nearrow & \\ & & & & \end{array}$$

surjektiv ist, dann folgt die Aussage mit  $\ker(\psi) = \mathcal{J}_k(\mathfrak{m}) \cap k^\times = k_{\mathfrak{m}}^\times$ . Dazu braucht man den

**Satz 1.43** (Approximationssatz). *Seien  $|\cdot|_1, \dots, |\cdot|_n$  paarweise inäquivalente Beträge auf  $k$ . Seien  $a_1, \dots, a_n \in k$ . Dann gibt es zu jedem  $\varepsilon > 0$  ein  $x \in k$  mit  $|x - a_i|_i < \varepsilon$  für  $1 \leq i \leq n$  (vgl. [Neu06, Kapitel II, Satz (3.4)]).*

Sei  $\alpha = (\alpha_v)_v \in \mathcal{J}_k$ . Zu zeigen: Es gibt ein  $\beta \in k^\times$  mit  $\beta\alpha \in \mathcal{J}_k(\mathfrak{m})$  (dann ist  $\psi(\beta\alpha) = \alpha k^\times$  in  $\mathcal{J}_k/k^\times$ ).

Hierzu ist ein  $\beta \in k^\times$  gesucht mit

$$\begin{aligned} v_{\mathfrak{p}}(\beta\alpha_{\mathfrak{p}} - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0) &\iff N_{k/\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(\beta\alpha_{\mathfrak{p}}-1)} \leq N_{k/\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(\mathfrak{m}_0)} \\ &\iff |\beta\alpha_{\mathfrak{p}} - 1|_{\mathfrak{p}} \leq N_{k/\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(\mathfrak{m}_0)} \\ &\iff |\beta - \alpha_{\mathfrak{p}}^{-1}|_{\mathfrak{p}} \leq \frac{N_{k/\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(\mathfrak{m}_0)}}{|\alpha_{\mathfrak{p}}|_{\mathfrak{p}}} =: \varepsilon_{\mathfrak{p}} \end{aligned}$$

für alle  $v = \mathfrak{p}$  mit  $\mathfrak{p} | \mathfrak{m}_0$ . Falls  $v = \sigma$  eine unendliche Stelle in  $\mathfrak{m}_\infty$  ist, so muss gelten  $\text{sgn}(\sigma(\beta)) = \text{sgn}(\alpha_v)$ . Wähle

$$\varepsilon < \min\{\varepsilon_{\mathfrak{p}}, |\alpha_v|/2 \mid v | \mathfrak{m}_\infty, \mathfrak{p} | \mathfrak{m}_0\}.$$

Für  $v | \mathfrak{m}$  wähle  $a_v \in k$  mit

$$|a_v - \alpha_v^{-1}|_v < \frac{\varepsilon}{2}$$

Finde mit dem Approximationssatz  $\beta \in k$  mit

$$|\beta - a_v| < \frac{\varepsilon}{2}$$

für alle  $v|\mathfrak{m}$ . Dann folgt

$$\begin{aligned} |\beta - \alpha_v^{-1}|_v &= |\beta - a_v + a_v - \alpha_v^{-1}|_v \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \end{aligned}$$

für alle  $v|\mathfrak{m}$ . Somit folgt  $\beta\alpha \in \mathcal{J}_k(\mathfrak{m})$ . □

**Definition 1.44.** Der Homomorphismus

$$\begin{aligned} c : \mathcal{J}_k &\longrightarrow \mathcal{I}_k \\ \alpha = (\alpha_v)_v &\longmapsto \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} =: (\alpha) = c(\alpha) \end{aligned}$$

heißt *Inhalt* (engl. *content*).

**Satz 1.45.** Sei  $K/k$  eine abelsche Erweiterung von Zahlkörpern. Dann induziert der Inhalt  $c$  einen Isomorphismus von Gruppen

$$\mathcal{J}_k(\mathfrak{m}) / (k^\times N_{K/k}(\mathcal{J}_k))_{\mathfrak{m}} \longrightarrow \mathcal{I}_k(\mathfrak{m}) / \mathcal{P}_k(\mathfrak{m}) N_{K/k}(\mathcal{I}_K(\mathfrak{m}_0 \mathcal{O}_K))$$

*Beweis.* Siehe [Lan13, Kapitel VII, §4]. □

Betrachte das kommutative Diagramm

$$\begin{array}{ccc} \mathcal{J}_k(\mathfrak{m}) / (k^\times N_{K/k}(\mathcal{J}_k))_{\mathfrak{m}} & \xrightarrow{\cong} & \mathcal{I}_k(\mathfrak{m}) / \mathcal{P}_k(\mathfrak{m}) N_{K/k}(\mathcal{I}_K(\mathfrak{m}_0 \mathcal{O}_K)) \\ \text{siehe Lemma 1.42} \downarrow \cong & & \cong \downarrow (-, K/k) \\ \mathcal{J}_k / k^\times N_{K/k}(\mathcal{J}_K) & \xrightarrow{\Theta} & \text{Gal}(K|k) \\ \nearrow & \text{---} & \searrow \\ \mathcal{J}_k & & (-, K/k) \end{array}$$

**Bemerkung 1.46.**  $\Theta$  hängt nicht von  $\mathfrak{m}$  ab.

**Definition 1.47.** Die Abbildung  $(-, K/k) : \mathcal{J}_k \longrightarrow \text{Gal}(K|k)$  heißt *Artinabbildung*.

**Bemerkung 1.48.** Sei  $\alpha = (\alpha_v)_v \in \mathcal{J}_k$  und  $K/k$  modulo  $\mathfrak{m}$  definiert. Finde mit dem Approximationsatz  $\beta \in k^\times$  mit  $\beta\alpha \in \mathcal{J}_k(\mathfrak{m})$ . Sei  $\mathfrak{a} = c(\beta\alpha)$ . Dann gilt

$$(\mathfrak{a}, K/k) = (\alpha, K/k).$$

**Satz 1.49.** (1) Sei  $K/k$  eine abelsche Erweiterung von Zahlkörpern. Dann induziert die Artinabbildung  $(-, K/k) : \mathcal{J}_k \longrightarrow \text{Gal}(K|k)$  einen Isomorphismus

$$\mathcal{C}_k / N_{K/k}(\mathcal{C}_K) = \mathcal{J}_k / k^\times N_{K/k}(\mathcal{J}_K) \xrightarrow{\cong} \text{Gal}(K|k)$$

(2) Zu jeder offenen Untergruppe  $k^\times \leq H \leq \mathcal{J}_k$  von endlichem Index gibt es genau eine abelsche Erweiterung  $K/k$  mit  $k^\times N_{K/k}(\mathcal{J}_K) = H$ .

**Bemerkung 1.50.** (1) Oft wird die Artinabbildung aufgefasst als Abbildung

$$(-, K/k) : \mathcal{C}_k = \mathcal{J}_k/k^\times \longrightarrow \text{Gal}(K|k).$$

(2) Mittels der Zuordnung

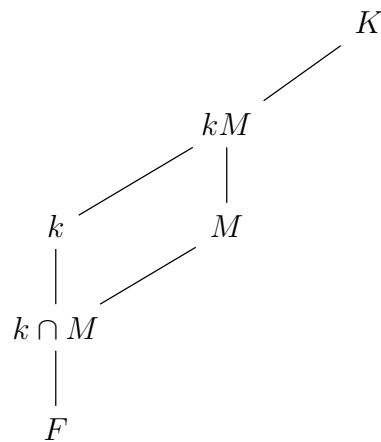
$$\begin{array}{ccc} \mathcal{J}_k & \longrightarrow & \mathcal{C}_k \\ | & & | \\ H & \longrightarrow & U \\ | & & | \\ k^\times & \longrightarrow & 1 \end{array}$$

lassen sich die obigen Resultate auch über die Idelklassengruppe formulieren.

(3) Seien  $k^\times \leq H_1, H_2 \leq \mathcal{J}_k$  offene Untergruppen von endlichem Index und  $K_1, K_2$  die zugehörigen Klassenkörper. Dann gilt

- (i)  $H_1 \leq H_2 \iff K_1 \supseteq K_2$ ,
- (ii)  $H_1 H_2 \longleftrightarrow K_1 \cap K_2$ ,
- (iii)  $H_1 \cap H_2 \longleftrightarrow K_1 K_2$ .

(4) Betrachte die Situation

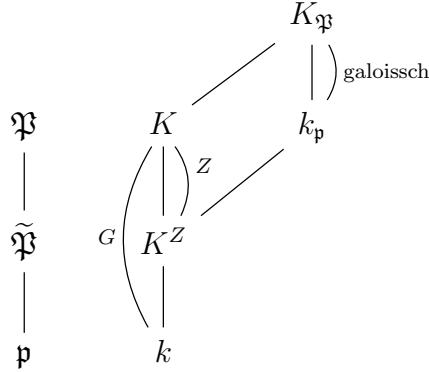


wobei die Erweiterungen  $K/k$  sowie  $M/F$  abelsch sind. Sei  $\alpha \in \mathcal{J}_k$ . Dann ist

$$(\alpha, K/k)|_M = (N_{k/F}(\alpha), M/F)$$

## Zusammenhang zum Lokalen

Sei  $K/k$  eine Galoiserweiterung von Zahlkörpern. Betrachte



wobei

$$Z = Z_{\mathfrak{P}} = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} \leq G$$

die Zerlegungsgruppe von  $\mathfrak{P}$  ist. Es gilt

$$\begin{aligned}
 \varphi : Z &\xrightarrow{\cong} \text{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \\
 \sigma &\longmapsto (\alpha \mapsto \sigma(\alpha))
 \end{aligned}$$

wobei für  $\alpha \in K_{\mathfrak{P}}$  repräsentiert durch die Cauchy-Folge  $(\alpha_n)_n, \alpha_n \in K, \sigma(\alpha)$  durch  $(\sigma(\alpha_n))_n$  repräsentiert ist.

Sei  $K/k$  abelsch und

$$\begin{aligned}
 \iota_v : k_v &\hookrightarrow \mathcal{J}_k \\
 \xi &\longmapsto (\dots, 1, \underbrace{\xi}_{v\text{-te Stelle}}, 1, \dots)
 \end{aligned}$$

Dann kann man zeigen:

$$(\iota_v(\xi), K/k) \in Z_v,$$

wobei  $Z_v$  die Zerlegungsgruppe zu  $v$  bezeichnet, und

$$\varphi((\iota_v(\xi), K/k)) = (\xi, K_w/k_v)$$

für alle  $\xi \in k_v^\times$ .

**Satz 1.51.** *Eine Stelle  $v = \mathfrak{p}$  ist genau dann unverzweigt in  $K/k$ , wenn  $\iota_{\mathfrak{p}}(\mathcal{U}_{\mathfrak{p}}) \subseteq k^\times N_{K/k}(\mathcal{J}_K)$ .*

*"Beweis".  $\implies$ :*  $\mathfrak{p}$  ist genau dann unverzweigt, wenn  $K_{\mathfrak{P}}/k_{\mathfrak{p}}$  für alle  $\mathfrak{P}|\mathfrak{p}$  unverzweigt ist. Dies ist genau dann der Fall, wenn  $\mathcal{U}_{\mathfrak{p}} = N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U_{\mathfrak{P}})$  für alle  $\mathfrak{P}|\mathfrak{p}$ . Daraus folgt, dass  $\iota_{\mathfrak{p}}(\mathcal{U}_{\mathfrak{p}}) \subseteq N_{K/k}(\mathcal{J}_K)$ .

*$\impliedby$ :* Sei  $\xi \in \mathcal{U}_{\mathfrak{p}}$ . Dann gilt

$$(\iota_{\mathfrak{p}}(\xi), K/k) = 1$$

d.h.

$$(\xi, K_{\mathfrak{P}}/k_{\mathfrak{p}}) = 1$$

und  $\xi \in \ker((-, K_{\mathfrak{P}}/k_{\mathfrak{p}})) = N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(K_{\mathfrak{P}}^\times)$ . Somit folgt  $\xi \in N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(U_{\mathfrak{P}})$ .  $\square$

## 2 Kohomologie endlicher Gruppen

### 2.1 $G$ -Moduln

Literatur: Dieses Kapitel folgt [NS11].

$G$  sei stets eine endliche Gruppe. Der *ganzzahlige Gruppenring* ist definiert als

$$\mathbb{Z}[G] := \left\{ \sum_{g \in G} a_g g \mid a_g \in \mathbb{Z} \right\}.$$

$\mathbb{Z}[G]$  ist ein Ring mittels komponentenweiser Addition und

$$\begin{aligned} \left( \sum_{g \in G} a_g g \right) \cdot \left( \sum_{h \in G} b_h h \right) &= \sum_{g, h} a_g b_h gh \\ &= \sum_{z \in G} \left( \sum_{gh=z} a_g b_h \right) z \end{aligned}$$

Es ist klar, dass  $\mathbb{Z}[G]$  genau dann kommutativ ist, wenn  $G$  abelsch ist.

Analog lässt sich  $R[G]$  für jeden kommutativen Ring  $R$  definieren.

Wir wollen  $\mathbb{Z}[G]$ -Moduln ( $G$ -Moduln), also  $G$ -Mengen, die zugleich eine abelsche Gruppe sind, studieren.

**Beispiel 2.1.** (1) Sei  $L/K$  eine Galoiserweiterung mit Galoisgruppe  $G$ . Dann gilt für  $\alpha \in L$

$$\left( \sum_{g \in G} a_g g \right) \alpha := \sum_{g \in G} a_g g(\alpha)$$

und somit ist  $L$  ein  $\mathbb{Z}[G]$ -Modul. Analog ist  $L$  auch ein  $K[G]$ - und ein  $\mathcal{O}_K[G]$ -Modul. Der Ganzheitsring  $\mathcal{O}_L$  ist ein  $\mathbb{Z}[G]$ - und ein  $\mathcal{O}_K[G]$ -Modul, jedoch kein  $K[G]$ -Modul.

Sei nun  $\alpha \in L^\times$ , dann ist  $L^\times$  mittels

$$\left( \sum_{g \in G} a_g g \right) \cdot \alpha := \prod_{g \in G} g(\alpha)^{a_g}$$

ein  $\mathbb{Z}[G]$ -Modul und analog sind auch  $\mathcal{O}_L^\times$  und  $\mathcal{I}_L$   $\mathbb{Z}[G]$ -Moduln, letzteres mittels

$$\left( \sum_{g \in G} a_g g \right) \cdot \mathfrak{a} := \prod_{g \in G} g(\mathfrak{a})^{a_g}.$$

Dann ist  $\mathcal{P}_L$  ein  $\mathbb{Z}[G]$ -Teilmodul von  $\mathcal{I}_L$  und somit auch  $cl_L = \mathcal{I}_L/\mathcal{P}_L$  ein  $\mathbb{Z}[G]$ -Modul. Ebenfalls ist die Gruppe der Einheitswurzeln  $\mu_L$  ein  $\mathbb{Z}[G]$ -Modul.

(2) Es seien  $A, G$  endliche Gruppen und  $A$  zusätzlich abelsch. Die Sequenz

$$1 \longrightarrow A \hookrightarrow E \begin{array}{c} \xrightarrow{\pi} \\ \xleftarrow{\sigma} \end{array} G \longrightarrow 1.$$

sei exakt. Dann können wir  $A$  als  $G$ -Modul betrachten mittels:

Wähle eine mengentheoretische Abbildung  $\sigma$  mit  $\pi\sigma(g) = g$ . Dann definiere

$$g \cdot a := \sigma(g)a\sigma(g)^{-1}$$

für  $g \in G, a \in A$ .

**Übung 2.2.** Die Gruppenwirkung ist unabhängig von der Wahl von  $\sigma$ .

**Definition 2.3.** (1) Die Abbildung

$$\begin{aligned} \varepsilon : \mathbb{Z}[G] &\longrightarrow \mathbb{Z} \\ \sum_{g \in G} a_g g &\longmapsto \sum_{g \in G} a_g \end{aligned}$$

heißt *Augmentation*. Der Kern von  $\varepsilon$  heißt *Augmentationsideal* und wird mit  $I_G$  bezeichnet.

(2) Das Element  $N_G := \sum_{g \in G} g$  heißt *Normelement* oder *Spurelement*. Die Abbildung

$$\begin{aligned} \mu : \mathbb{Z} &\hookrightarrow \mathbb{Z}[G] \\ n &\longmapsto nN_G \end{aligned}$$

heißt *Koaugmentation*. Wir setzen  $J_G := \text{coker}(\mu) = \mathbb{Z}[G]/\mathbb{Z} \cdot N_G$ .

Wir haben also die exakten Sequenzen

$$\begin{array}{ccccccc} 0 & \longrightarrow & I_G & \hookrightarrow & \mathbb{Z}[G] & \xrightarrow{\varepsilon} & \mathbb{Z} \longrightarrow 0 \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\mu} & \mathbb{Z}[G] & \longrightarrow & J_G \longrightarrow 0 \end{array}$$

**Satz 2.4.** (1)  $I_G$  hat die  $\mathbb{Z}$ -Basis

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

(2)  $J_G$  hat die  $\mathbb{Z}$ -Basis

$$\{g + \mathbb{Z} \cdot N_G \mid g \in G \setminus \{1\}\}.$$

(3) Die Sequenzen zerfallen als  $\mathbb{Z}$ -Moduln, d.h.

$$\begin{aligned} \mathbb{Z}[G] &\cong \mathbb{Z} \oplus I_G, \\ \mathbb{Z}[G] &\cong \mathbb{Z} \oplus J_G. \end{aligned}$$

*Beweis.* Übung. □

**Übung 2.5.** Es gilt  $I_G = \text{Ann}_{\mathbb{Z}[G]}(\mathbb{Z} \cdot N_G)$  und  $\mathbb{Z} \cdot N_G = \text{Ann}_{\mathbb{Z}[G]}(I_G)$ .

Sei nun  $A$  ein  $G$ -Modul.

**Definition 2.6.** Die Menge

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

heißt der *Fixmodul* und die Teilmenge

$$N_G A := \{N_G a \mid a \in A\}$$

heißt die *Normengruppe* von  $A$ . Weiter ist

$${}_N A := \{a \in A \mid N_G a = 0\}$$

der Kern der Norm und wir definieren den Teilmodul

$$I_G A := \left\{ \sum_{g \neq 1} a_g (ga - a) \mid a \in A, a_g \in \mathbb{Z} \right\} \subseteq {}_N A$$

**Beispiel 2.7.** Sei  $L/K$  eine Galoiserweiterung von lokalen Körpern über  $\mathbb{Q}_p$ . Für  $A = L^\times$  ist

$$(L^\times)^G = K^\times \supseteq N_G A = N_{L/K}(L^\times)$$

und falls  $L/K$  abelsch ist folgt

$$H^{-2}(G, \mathbb{Z}) \cong \text{Gal}(L/K) \stackrel{\text{Artin}}{\cong} K^\times / N_{L/K}(L^\times) \cong H^0(G, L^\times).$$

Etwas ausführlicher:  $\text{Gal}(L/K)$  ist kanonisch isomorph zur Kohomologiegruppe  $H^{-2}(G, \mathbb{Z})$ ,  $K^\times / N_{L/K}(L^\times)$  ist kanonisch isomorph zu  $H^0(G, L^\times)$  und wir werden die Artinabbildung als Inverse zu einem kanonischen Isomorphismus

$$\text{inv}_{L/K}: H^{-2}(G, \mathbb{Z}) \longrightarrow H^0(G, L^\times)$$

definieren.

Seien  $A, B$   $G$ -Moduln. Dann wird  $\text{Hom}_{\mathbb{Z}}(A, B)$  zu einem  $G$ -Modul mittels

$$(gf)(a) := g(f(g^{-1}a)),$$

d.h.  $gf := g \circ f \circ g^{-1}$ , wobei  $f \in \text{Hom}_{\mathbb{Z}}(A, B)$ ,  $g \in G$ ,  $a \in A$ .

Es ist klar, dass

$$\text{Hom}_G(A, B) := \text{Hom}_{\mathbb{Z}[G]}(A, B) = \text{Hom}_{\mathbb{Z}}(A, B)^G$$

gilt.

Ebenso wird  $A \otimes_{\mathbb{Z}} B$  zum  $G$ -Modul mittels

$$g(a \otimes b) := ga \otimes gb.$$



**Warnung.** Es ist  $A^G \otimes B^G \subseteq (A \otimes B)^G$ . Im Allgemeinen gilt hier keine Gleichheit.

**Definition 2.8.** Ein  $\mathbb{Z}[G]$ -Modul  $A$  heißt *frei*, falls es einen  $\mathbb{Z}[G]$ -Isomorphismus

$$f : A \longrightarrow \bigoplus_{i \in I} \mathbb{Z}[G]$$

gibt, wobei  $I$  eine beliebige Indexmenge ist.

**Übung 2.9.** (1) Sei  $L/K$  eine Galoiserweiterung von Zahlkörpern mit Galoisgruppe  $G$ . Dann besagt der Satz von der Normalbasis, dass ein  $\Theta \in L$  existiert, sodass  $\{g(\Theta) \mid g \in G\}$  eine  $K$ -Basis von  $L$  ist.

Mit anderen Worten ist  $L$   $K[G]$ -frei, denn

$$\begin{aligned} K[G] &\longrightarrow L \\ \sum_g a_g g &\longmapsto \sum_g a_g g(\Theta) \end{aligned}$$

ist ein Isomorphismus.

Sei nun  $\omega_1, \dots, \omega_n$  mit  $n = [K : \mathbb{Q}]$  eine  $\mathbb{Q}$ -Basis von  $K$ . Dann ist  $L$  auch  $\mathbb{Q}[G]$ -frei, denn

$$\begin{aligned} \mathbb{Q}[G]^n &\longrightarrow L \\ (\lambda_i)_{i=1, \dots, n} &\longmapsto \sum_{i=1}^n \omega_i \lambda_i(\Theta) \end{aligned}$$

ist ein Isomorphismus von  $\mathbb{Q}[G]$ -Moduln.

Es stellt sich die

Frage (A. Fröhlich): Ist  $\mathcal{O}_L$  ein freier  $\mathbb{Z}[G]$ -Modul?

Diese Frage wurde 1981 von M. Taylor gelöst:

$\mathcal{O}_L$  ist genau dann (stabil) frei, wenn die Wurzelzahlklasse trivial ist.

(2)  $I_G$  und  $J_G$  sind nicht frei.

(3) Sei  $p$  eine Primzahl, dann ist  $\mathcal{O}_{\mathbb{Q}(\zeta_p)} \mathbb{Z}[G]$ -frei (Hilberts Satz 132, siehe Blatt 4, Aufgabe 3).

**Satz 2.10.** Sei  $X$   $\mathbb{Z}[G]$ -frei und

$$0 \longrightarrow A \xrightarrow{h} B \xrightarrow{g} C \longrightarrow 0$$

eine kurze exakte Sequenz von  $G$ -Moduln. Dann ist die Sequenz

$$0 \longrightarrow \text{Hom}_G(X, A) \xrightarrow{h} \text{Hom}_G(X, B) \xrightarrow{g} \text{Hom}_G(X, C) \longrightarrow 0$$

exakt.

*Beweis.* Falls  $X = \mathbb{Z}[G]$ , so gilt: Das Diagramm

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}_G(\mathbb{Z}[G], A) & \xleftarrow{h^*} & \text{Hom}_G(\mathbb{Z}[G], B) & \xrightarrow{g^*} & \text{Hom}_G(\mathbb{Z}[G], C) \longrightarrow 0 \\ & & \cong \downarrow f \mapsto f(1) & & h \circ f \mapsto h(f(1)) \downarrow \cong & & \downarrow \cong \\ 0 & \longrightarrow & A & \xleftarrow{\quad} & B & \xrightarrow{\quad} & C \longrightarrow 0 \end{array}$$

ist kommutativ, wobei  $h^*(f) = h \circ f$  (analog für  $g^*$ ).

Sei allgemein  $X \cong \bigoplus_{i \in I} \mathbb{Z}[G]$ . Dann folgt die Behauptung aus der Additivität von  $\text{Hom}_G(X, -)$ .

Genauer sei  $X = \bigoplus_{j \in J} X_j$  für  $G$ -Moduln  $X_j$ . Dann ist

$$\begin{array}{ccc} \text{Hom}_G\left(\bigoplus_{j \in J} X_j, A\right) & \longrightarrow & \prod_{j \in J} \text{Hom}_G(X_j, A) \\ & & f \mapsto (f|_{X_j})_{j \in J} \\ \left(\sum_{j \in J} x_j \mapsto \sum_{j \in J} f_j(x_j)\right) & \longleftarrow & (f_j)_{j \in J} \end{array}$$

ein Isomorphismus. □

**Bemerkung 2.11.** (1) Der Funktor  $\text{Hom}_G(X, -)$  ist stets linksexakt, d.h.

$$0 \longrightarrow \text{Hom}_G(X, A) \xleftarrow{h^*} \text{Hom}_G(X, B) \xrightarrow{g^*} \text{Hom}_G(X, C)$$

ist exakt.

(2) Man kann  $\mathbb{Z}[G]$ -frei durch  $\mathbb{Z}[G]$ -projektiv ersetzen (siehe Übungsblatt).

*Beweis zu (1).* Sei  $f \in \text{Hom}_G(X, A)$ , dann ist  $(g^* \circ h^*)(f) = g \circ h \circ f = 0$ , d.h.  $\text{im}(h^*) \subseteq \ker(g^*)$ .

Sei nun  $f_2 \in \text{Hom}_G(X, B)$  und es gelte  $g \circ f_2 = 0$ , d.h.  $\text{im}(f_2) \subseteq \ker(g) = \text{im}(h)$ . Wir suchen  $f_1$ , sodass

$$\begin{array}{ccc} X & \xrightarrow{f_2} & B \\ & \searrow f_1 & \uparrow h \\ & & A \end{array}$$

kommutiert. Dazu sei  $x \in X$ . Dann gibt es genau ein  $a \in A$  mit  $f_2(x) = h(a)$ . Setze nun  $f_1(x) := a$ . □

**Definition 2.12.** Ein  $G$ -Modul  $X$  ist *projektiv*, falls für alle Diagramme der Form

$$\begin{array}{ccccc} & & X & & \\ & \swarrow \exists & \downarrow & & \\ V & \longrightarrow & W & \longrightarrow & 0 \end{array}$$

mit exakter Zeile ein  $\mathbb{Z}[G]$ -Modulhomomorphismus  $X \rightarrow V$  existiert, sodass das Diagramm kommutiert (hierbei sind die Abbildungen jeweils  $\mathbb{Z}[G]$ -Modulhomomorphismen).

Falls  $X$  projektiv ist, so ist  $\text{Hom}_G(X, -)$  exakt.

*Beweis.* Nach Definition von Projektivität gibt es zu einem  $f_3 \in \text{Hom}_G(X, W)$  ein  $f_2 \in \text{Hom}_G(X, V)$  sodass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} & X & \\ & \swarrow f_2 & \downarrow f_3 \\ V & \xrightarrow{h} & W \longrightarrow 0 \end{array}$$

Dann ist  $f_2$  ein Urbild von  $f_3$  und somit ist  $h^*$  surjektiv.  $\square$

**Übung 2.13** (siehe Blatt 4, Aufgabe 4). Sei  $X$  ein  $G$ -Modul. Folgende Aussagen sind äquivalent:

- (1)  $X$  ist projektiv,
- (2)  $\text{Hom}_G(X, -)$  ist exakt,
- (3)  $X$  ist direkter Summand eines freien  $G$ -Moduls, d.h. es existiert ein  $G$ -Modul  $Y$ , sodass  $X \oplus Y$  ein freier  $G$ -Modul ist.
- (4) Jede exakte Sequenz

$$0 \longrightarrow A \hookrightarrow B \xrightarrow{\pi} X \longrightarrow 0$$

$\swarrow \sigma$

von  $G$ -Moduln zerfällt, d.h. es gibt einen  $G$ -Modulhomomorphismus  $\sigma : X \rightarrow B$  mit  $\pi \circ \sigma = \text{id}_X$ .

### Drei Lemmata (ohne Beweis)

**Lemma 2.14.** Ist

$$\dots \longleftarrow X_{q-1} \longleftarrow X_q \longleftarrow X_{q+1} \longleftarrow \dots$$

eine exakte Sequenz von freien  $\mathbb{Z}$ -Moduln und  $D$  ein beliebiger  $\mathbb{Z}$ -Modul. Dann ist

$$\dots \longrightarrow \text{Hom}_{\mathbb{Z}}(X_{q-1}, D) \longrightarrow \text{Hom}_{\mathbb{Z}}(X_q, D) \longrightarrow \text{Hom}_{\mathbb{Z}}(X_{q+1}, D) \longrightarrow \dots$$

exakt.

**Lemma 2.15.** Ist

$$0 \longrightarrow A \hookrightarrow B \twoheadrightarrow C \longrightarrow 0$$

eine exakte Sequenz von freien  $\mathbb{Z}$ -Moduln und  $X$  ein beliebiger Modul. Dann ist

$$0 \longrightarrow X \otimes A \hookrightarrow X \otimes B \twoheadrightarrow X \otimes C \longrightarrow 0$$

exakt.

**Lemma 2.16.** *Ist*

$$0 \longrightarrow A \hookrightarrow B \twoheadrightarrow C \longrightarrow 0$$

eine exakte Sequenz von  $\mathbb{Z}$ -Moduln und  $X$  ein freier  $\mathbb{Z}$ -Modul, dann ist

$$0 \longrightarrow X \otimes A \hookrightarrow X \otimes B \twoheadrightarrow X \otimes C \longrightarrow 0$$

exakt.

**Beispiele 2.17.** (1) Betrachte

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \twoheadrightarrow & \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \\ & & & & a & \longmapsto & na \end{array}$$

für ein  $n \in \mathbb{N}$ .

Wende  $-\otimes \mathbb{Z}/n\mathbb{Z}$  an, dann folgt

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} & \xrightarrow{n} & \mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \\ & & \parallel & & \parallel & & \parallel \\ 0 & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \xrightarrow{n} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \end{array}$$

Die untere Multiplikation mit  $n$  ist die Nullabbildung, also insbesondere nicht injektiv. Somit ist die Sequenz nicht mehr exakt und dies ist ein Gegenbeispiel zu Lemma 2.15 und Lemma 2.16.

(2) Betrachte

$$\dots \longleftarrow 0 \longleftarrow \mathbb{Z}/n\mathbb{Z} \longleftarrow \mathbb{Z} \xleftarrow{n} \mathbb{Z} \longleftarrow 0 \longleftarrow \dots$$

Wende  $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$  an, dann folgt

$$\dots \longrightarrow 0 \longrightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \longrightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \longrightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \longrightarrow 0 \longrightarrow \dots$$

also

$$\dots \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \longrightarrow 0 \longrightarrow \dots$$

und die Multiplikation mit  $n$  ist nicht surjektiv, d.h. die Sequenz ist nicht exakt und dies ist ein Gegenbeispiel zu Lemma 2.14.

## 2.2 Definition von (Tate)-Kohomologiegruppen

Sei  $G$  eine endliche Gruppe.

**Definition 2.18.** Unter einer *vollständigen freien Auflösung* von  $\mathbb{Z}$  versteht man einen unendlichen Komplex

$$\begin{array}{ccccccccccc} \dots & \longleftarrow & X_{-2} & \xleftarrow{d_{-1}} & X_{-1} & \xleftarrow{d_0} & X_0 & \xleftarrow{d_1} & X_1 & \xleftarrow{d_2} & X_2 & \longleftarrow & \dots \\ & & & & \swarrow \mu & & \searrow \varepsilon & & & & & & \\ & & & & \mathbb{Z} & & & & & & & & \\ & & & & \swarrow & & \searrow & & & & & & \\ & & & & 0 & & & & & & & & 0 \end{array}$$

sodass

- (1) die  $X_q$  sind freie  $\mathbb{Z}[G]$ -Moduln,
- (2)  $\mu\varepsilon = d_0$ ,
- (3)  $\mu, \varepsilon, d_q$  sind  $G$ -Modulhomomorphismen,
- (4) Exaktheit an jeder Stelle.

Wir wollen nun die *Standardauflösung von  $\mathbb{Z}$*  definieren:

Für  $q \geq 1$  definiert man

$$X_q = X_{-q-1} = \bigoplus \mathbb{Z}[G](\sigma_1, \dots, \sigma_q)$$

wobei sich die direkte Summe über alle  $q$ -Zellen  $(\sigma_1, \dots, \sigma_q)$ ,  $\sigma_i \in G$ , erstreckt.

**Beispiel.**  $X_1 = X_{-2} \cong \mathbb{Z}[G]^{|G|}$ . Ein Element von  $X_1$  ist von der Form  $\sum_{\sigma \in G} \lambda_\sigma(\sigma)$  für  $\lambda_\sigma \in \mathbb{Z}[G]$ .

Setze  $X_0 = X_{-1} = \mathbb{Z}[G]$  und definiere

$$\begin{aligned} \varepsilon : X_0 = \mathbb{Z}[G] &\longrightarrow \mathbb{Z} \\ \sigma &\longmapsto 1 \end{aligned}$$

und

$$\begin{aligned} \mu : \mathbb{Z} &\longrightarrow X_{-1} = \mathbb{Z}[G] \\ 1 &\longmapsto N_G \end{aligned}$$

Weiter sei

$$\begin{aligned} d_0(1) &:= N_G, \\ d_1((\sigma)) &:= \sigma - 1, \\ d_q((\sigma_1, \dots, \sigma_q)) &:= \sigma_1(\sigma_2, \dots, \sigma_q) \\ &\quad + \sum_{i=1}^{q-1} (-1)^i (\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma_{i+1}, \sigma_{i+2}, \dots, \sigma_q) \\ &\quad + (-1)^q (\sigma_1, \dots, \sigma_{q-1}), \end{aligned} \quad q > 1.$$

Die Formeln für  $d_q, q < 0$  findet man in [NS11, S. 13].

**Lemma 2.19.** *Die Standardauflösung ist eine vollständige freie Auflösung von  $\mathbb{Z}$ .*

*Beweis.* Die Eigenschaften (1)-(3) gelten per Definition. Die Exaktheit von

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\varepsilon} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \longleftarrow \dots \quad (2.1)$$

zeigt man durch Rechnung und Induktion. Wende auf (2.1) den Funktor  $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$  an. Dann folgt mit Lemma 2.14

$$0 \longrightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \longrightarrow \text{Hom}_{\mathbb{Z}}(X_0, \mathbb{Z}) \longrightarrow \text{Hom}_{\mathbb{Z}}(X_1, \mathbb{Z}) \longrightarrow \dots \quad (2.2)$$

ist exakt.

Sei  $x = (\sigma_1, \dots, \sigma_q)$  eine  $q$ -Zelle. Definiere  $x^* \in \text{Hom}_{\mathbb{Z}}(X_q, \mathbb{Z})$  durch

$$x^*(\sigma(\tau_1, \dots, \tau_q)) := \begin{cases} 1, & \sigma = 1 \text{ und } x = (\tau_1, \dots, \tau_q) \\ 0, & \text{sonst} \end{cases}$$

Die Abbildung

$$\begin{aligned} X_q &\longrightarrow \text{Hom}_{\mathbb{Z}}(X_q, \mathbb{Z}) \\ x &\longmapsto x^* \end{aligned}$$

kann  $\mathbb{Z}[G]$ -linear fortgesetzt werden und wird ein Isomorphismus von  $\mathbb{Z}[G]$ -Moduln. Zur Bijektivität:

$$\begin{aligned} (\tau x^*)(\sigma(\tau_1, \dots, \tau_q)) &= \tau(x^*(\tau^{-1}\sigma(\tau_1, \dots, \tau_q))) \\ &= \begin{cases} 1, & \tau = \sigma \text{ und } x = (\tau_1, \dots, \tau_q) \\ 0, & \text{sonst} \end{cases} \end{aligned}$$

Also ist  $\tau(\sigma_1, \dots, \sigma_n)^*$  genau die  $\mathbb{Z}$ -duale Basis zu

$$\{\sigma(\tau_1, \dots, \tau_q) \mid \sigma \in G, (\tau_1, \dots, \tau_q) \text{ } q\text{-Zelle}\}.$$

Somit wird aus (2.2) durch diese Dualisierung

$$0 \longrightarrow \mathbb{Z} \longrightarrow X_0 \longrightarrow X_1 \longrightarrow \dots$$

und es gilt  $X_0 = X_{-1}, X_1 = X_{-2}$ , etc.

Die expliziten Formeln ergeben sich ebenfalls aus (2.1) durch dualisieren.  $\square$

Sei nun  $A$  ein  $G$ -Modul. Wende den Funktor  $\text{Hom}_G(-, A)$  auf die Standardauflösung an, dann folgt

$$\dots \longrightarrow \text{Hom}_G(X_{-2}, A) \xrightarrow{\partial_{-1}} \text{Hom}_G(X_{-1}, A) \xrightarrow{\partial_0} \text{Hom}_G(X_0, A) \longrightarrow \dots$$

ist eine Sequenz von  $G$ -Moduln mit

$$(\partial_{q+1} \circ \partial_q)(f) = 0$$

für alle  $q$ , d.h.  $\text{im}(\partial_q) \subseteq \ker(\partial_{q+1})$ .

**Notation.** Definiere

$$\begin{aligned} A_q &:= \text{Hom}_G(X_q, A), \\ Z_q = Z_q(A) &:= \ker(\partial_{q+1}), \\ B_q = B_q(A) &:= \text{im}(\partial_q). \end{aligned}$$

Man nennt  $A_q$  die  $q$ -Koketten,  $Z_q$  die  $q$ -Kozyklen und  $B_q$  die  $q$ -Koränder.

**Definition 2.20.** Die Gruppe

$$H^q(G, A) := Z_q(A)/B_q(A)$$

heißt die  $q$ -te (Tate)-Kohomologiegruppe.

Sei  $x \in A_q = A_{-q-1} = \text{Hom}_G(X_q, A)$  eine  $q$ -Kokette.  $X_q$  ist  $\mathbb{Z}[G]$ -frei erzeugt von den  $q$ -Zellen  $(\sigma_1, \dots, \sigma_q)$  für  $q \geq 1$ . Also ist  $x$  eindeutig bestimmt durch seine Werte auf  $(\sigma_1, \dots, \sigma_q)$ . Man kann  $x$  als Abbildung

$$x : G^q \longrightarrow A$$

auffassen. Also gilt

$$A_q = A_{-q-1} = \{x : G^q \longrightarrow A\}$$

für  $q \geq 1$  und

$$A_0 = A_{-1} = \text{Hom}_G(\mathbb{Z}[G], A) \cong A$$

mittels  $f \mapsto f(1)$ . Die Formeln für die  $d_q$  liefern nun für die  $\partial_q$  die Formeln

$$\begin{aligned} \partial_0 x &= N_G x & x \in A_{-1} &= A, \\ (\partial_1 x)(\sigma) &= \sigma x - x & x \in A_0 &= A, \\ (\partial_q x)(\sigma_1, \dots, \sigma_q) &= \sigma_1(x(\sigma_2, \dots, \sigma_q)) \\ &+ \sum_{i=1}^{q-1} (-1)^i x(\sigma_1, \dots, \sigma_i \sigma_{i+1}, \dots, \sigma_q) \\ &+ (-1)^q x(\sigma_1, \dots, \sigma_{q-1}) & x \in A_{q-1}, q \geq 2, \\ \partial_{-1} x &= \sum_{\sigma \in G} \sigma^{-1}(x(\sigma)) - x(\sigma) & x \in A_{-2} &= \{x : G \longrightarrow A\}, \end{aligned}$$

(siehe [NS11, S. 17] für die restlichen Formeln).

Beispielsweise hat man für  $q = 0$

$$\begin{array}{ccc} A_{-1} = A \cong \text{Hom}_G(\mathbb{Z}[G], A) & \ni & f \\ \downarrow \partial_0 & & \downarrow \\ A_0 = A \cong \text{Hom}_G(\mathbb{Z}[G], A) & \ni & f \circ d_0 \end{array}$$

und die Formel für  $\partial_0$  folgt aus

$$f(d_0(1)) = f(N_G) = N_G f(1).$$

Ebenso hat man für  $q = 1$

$$\begin{array}{ccc} A_0 = A \cong \text{Hom}_G(\mathbb{Z}[G], A) & \ni & f \\ \downarrow \partial_1 & & \downarrow \\ A_1 = \{x : G \longrightarrow A\} = \text{Hom}_G(X_1, A) & \ni & f \circ d_1 \end{array}$$

und die Formel für  $\partial_1$  folgt aus

$$f(d_1(\sigma)) = f(\sigma - 1) = (\sigma - 1)f(1).$$

Die restlichen Formeln folgen analog.

## Explizite Beschreibung der Kohomologiegruppen für $q = -1, 0, 1$

Es gilt für  $q = -1$ :

$$\begin{aligned} Z_{-1} &= \ker(N_G) = {}_G A, \\ B_{-1} &= \text{im}(\partial_{-1}) = I_G A = \left\{ \sum_{\sigma \neq 1} n_\sigma (\sigma(a) - a) \mid a \in A, n_\sigma \in \mathbb{Z} \right\}, \\ H^{-1}(G, A) &= {}_G A / I_G A. \end{aligned}$$

Für  $q = 0$  ergibt sich

$$\begin{aligned} Z_0 &= \ker(\partial_1) = A^G, \\ B_0 &= \text{im}(\partial_0) = N_G A, \\ H^0(G, A) &= A^G / N_G A. \end{aligned}$$

Für  $q = 1$  erhalten wir

$$\begin{aligned} Z_1 &= \ker(\partial_2) = \{x : G \longrightarrow A \mid x(\sigma\tau) = \sigma x(\tau) + x(\sigma), \forall \sigma, \tau \in G\}, \\ B_1 &= \text{im}(\partial_1) = \{x : G \longrightarrow A \mid \exists a \in A : x(\sigma) = \sigma(a) - a\}, \\ H^1(G, A) &= Z_1 / B_1. \end{aligned}$$

**Bemerkungen 2.21.** (1) Elemente in  $Z_1$  heißen *gekreuzte Homomorphismen*.

(2) Falls  $G$  trivial auf  $A$  wirkt, d.h.  $\sigma a = a$  für alle  $\sigma \in G$  und  $a \in A$ , so ist

$$\begin{aligned} Z_1 &= \text{Hom}_{\mathbb{Z}}(G, A), \\ B_1 &= 0, \\ \implies H^1(G, A) &= \text{Hom}_{\mathbb{Z}}(G, A). \end{aligned}$$

(3) Falls

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

eine exakte Sequenz von  $G$ -Moduln ist, so ist

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G$$

exakt (siehe Blatt 5, Aufgabe 2a)). Falls  $H^1(G, A) = 0$ , so ist auch

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow 0$$

exakt.

## 2.3 Die lange exakte Kohomologiesequenz

Sei  $f : A \longrightarrow B$  ein Homomorphismus von  $G$ -Moduln. Dann induziert  $f$  Abbildungen

$$\begin{aligned} f_q : A_q &\longrightarrow B_q \\ x &\longmapsto fx \end{aligned}$$



wobei  $(fx)(\sigma_1, \dots, \sigma_q) := f(x(\sigma_1, \dots, \sigma_q))$  für  $q \geq 1$ . Das unendliches Diagramm

$$\begin{array}{ccccccc} \dots & \longrightarrow & A_{q-1} & \xrightarrow{\partial_q} & A_q & \xrightarrow{\partial_{q+1}} & A_{q+1} & \longrightarrow & \dots \\ & & \downarrow f_{q-1} & & \downarrow f_q & & \downarrow f_{q+1} & & \\ \dots & \longrightarrow & B_{q-1} & \xrightarrow{\partial_q} & B_q & \xrightarrow{\partial_{q+1}} & B_{q+1} & \longrightarrow & \dots \end{array}$$

kommutiert. Somit folgt

$$\begin{aligned} f_q &: Z_q(A) \longrightarrow Z_q(B), \\ f_q &: B_q(A) \longrightarrow B_q(B). \end{aligned}$$

Insgesamt induziert also der Homomorphismus  $f : A \longrightarrow B$  Abbildungen

$$\bar{f}_q : H^q(G, A) \longrightarrow H^q(G, B).$$

Explizit sei  $\bar{c} \in H^q(G, A) = Z_q(A)/B_q(A)$  die Restklasse von  $c \in Z_q(A)$ . Dann wird  $\bar{f}_q(\bar{c})$  repräsentiert von  $fc$  in  $Z_q(B)/B_q(B)$ .

**Satz 2.22.** *Sei*

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$$

eine exakte Sequenz von  $G$ -Moduln. Dann gibt es einen kanonischen Homomorphismus von  $G$ -Moduln für alle  $q \in \mathbb{Z}$

$$\delta_q : H^q(G, C) \longrightarrow H^{q+1}(G, A),$$

sodass die unendliche Sequenz

$$\dots \longrightarrow H^q(G, A) \xrightarrow{\bar{i}_q} H^q(G, B) \xrightarrow{\bar{j}_q} H^q(G, C) \xrightarrow{\delta_q} H^{q+1}(G, A) \xrightarrow{\bar{i}_{q+1}} \dots \quad (2.3)$$

exakt ist.

**Definition 2.23.** Die Abbildung  $\delta_q$  heißt *Verbindungshomomorphismus*, die Sequenz 2.3 heißt *lange exakte Kohomologiesequenz*.

*Beweis.* Betrachte

$$\begin{array}{ccccccc} 0 & \longrightarrow & A_{q-1} & \xrightarrow{i_{q-1}} & B_{q-1} & \xrightarrow{j_{q-1}} & C_{q-1} & \longrightarrow & 0 \\ & & \downarrow \partial_q & & \downarrow \partial_q & & \downarrow \partial_q & & \\ 0 & \longrightarrow & A_q & \xrightarrow{i_q} & B_q & \xrightarrow{j_q} & C_q & \longrightarrow & 0 \\ & & \downarrow \partial_{q+1} & & \downarrow \partial_{q+1} & & \downarrow \partial_{q+1} & & \\ 0 & \longrightarrow & A_{q+1} & \xrightarrow{i_{q+1}} & B_{q+1} & \xrightarrow{j_{q+1}} & C_{q+1} & \longrightarrow & 0 \end{array}$$

Die Zeilen sind exakt, da sie aus

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

durch Anwendung von  $\text{Hom}_G(X_i, -)$  für  $i = q - 1, q, q + 1$  entstehen und da die  $X_i$   $\mathbb{Z}[G]$ -frei sind.

Sei  $\bar{c}_q \in H^q(G, C) = Z_q(C)/B_q(C) \subseteq C_q/B_q(C)$ . Es gilt  $\partial_{q+1}(c_q) = 0$ . Sei  $b_q \in B_q$  mit  $j_q(b_q) = c_q$ . Dann ist  $\partial_{q+1}(b_q) \in \ker(j_{q+1}) = \text{im}(i_{q+1})$  und es existiert ein eindeutiges Urbild  $a_{q+1} \in A_q$ , d.h.  $i_{q+1}(a_{q+1}) = \partial_{q+1}(b_q)$ . Es gilt

$$i_{q+2}(\partial_{q+2}(a_{q+1})) = \partial_{q+2}(i_{q+1}(a_{q+1})) = \partial_{q+2}(\partial_{q+1}(b_q)) = 0$$

und somit folgt  $\partial_{q+2}(a_{q+1}) = 0$ . Dann ist  $a_{q+1} \in Z_{q+1}(A)$  und wir definieren

$$\delta_q(\bar{c}_q) := \bar{a}_{q+1},$$

(man nennt das hier angewendete Verfahren *Diagrammjagd*).

Wohldefiniertheit: Folgt ebenfalls mittels Diagrammjagd:

Sei  $\bar{c}_q = \bar{c}'_q$ , d.h.  $c_q - c'_q \in B_q(C)$ . Also existiert ein  $c_{q-1} \in C_{q-1}$  mit  $\partial_q(c_{q-1}) = c_q - c'_q$  und wir können ein Urbild  $b_{q-1}$  von  $c_{q-1}$  unter  $j_{q-1}$  wählen. Dann unterscheiden sich die  $b_q, b'_q$  in der vorherigen Konstruktion gerade um  $\partial_q(b_{q-1})$  und es folgt  $\partial_{q+1}(b_q - b'_q) = 0$ , also  $a_{q+1} = a'_{q+1}$ .

Sei nun  $j_q(b_q) = c_q = j_q(b'_q)$ , dann ist  $b_q - b'_q \in \ker(j_q) = \text{im}(i_q)$  und es existiert ein eindeutiges  $a_q$  mit  $i_q(a_q) = b_q - b'_q$ . Dann ist aber

$$\begin{aligned} i_{q+1}(\partial_{q+1}(a_q)) &= \partial_{q+1}(i_q(a_q)) = \partial_{q+1}(b_q) - \partial_{q+1}(b'_q) \\ &= i_{q+1}(a_{q+1}) - i_{q+1}(a'_{q+1}) \end{aligned}$$

und somit folgt  $a_{q+1} - a'_{q+1} \in B_{q+1}(A)$ .

Exaktheit bei  $H^q(G, C)$ : Betrachte

$$H^q(G, B) \xrightarrow{\bar{j}_q} H^q(G, C) \xrightarrow{\delta_q} H^{q+1}(G, A)$$

Die Inklusion  $\text{im}(\bar{j}_q) \subseteq \ker(\delta_q)$  folgt aus der Konstruktion. Sei umgekehrt  $\delta_q(\bar{c}_q) = 0$ . Dann gibt es  $a_{q+1}$  und  $b_q$  mit

$$\begin{aligned} \delta_q(\bar{c}_q) &= \bar{a}_{q+1}, \\ j_q(b_q) &= c_q, \\ i_{q+1}(a_{q+1}) &= \partial_{q+1}(b_q). \end{aligned}$$

Es gilt nun  $\bar{a}_{q+1} = 0$ , d.h.  $a_{q+1} = \partial_{q+1}(a_q)$ . Dann folgt

$$\partial_{q+1}(b_q) = i_{q+1}(a_{q+1}) = i_{q+1}(\partial_{q+1}(a_q)) = \partial_{q+1}(i_q(a_q))$$

und somit

$$\partial_{q+1}(b_q - i_q(a_q)) = 0.$$

Ferner gilt

$$c_q = j_q(b_q - i_q(a_q))$$

und da  $b_q - i_q(a_q)$  ein Kozykel ist, folgt

$$\bar{c}_q = \bar{j}_q(\overline{b_q - i_q(a_q)}) \in \text{im}(\bar{j}_q).$$

Der Rest des Beweises ist eine Übung (siehe Blatt 5, Aufgabe 1). □

**Korollar 2.24.** Falls  $H^q(G, A) = 0$  (bzw.  $H^q(G, B) = 0$  bzw.  $H^q(G, C) = 0$ ) für alle  $q \in \mathbb{Z}$  gilt, so erhält man Isomorphismen

$$\bar{j}_q : H^q(G, B) \cong H^q(G, C)$$

bzw.

$$\delta : H^q(G, C) \cong H^{q+1}(G, A)$$

bzw.

$$\bar{i}_q : H^q(G, A) \cong H^q(G, B).$$

**Satz 2.25.** Falls

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{j} & C & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{j'} & C' & \longrightarrow & 0 \end{array}$$

ein kommutatives Diagramm von  $G$ -Moduln mit exakten Zeilen ist, so kommutiert

$$\begin{array}{ccc} H^q(G, C) & \xrightarrow{\delta} & H^{q+1}(G, A) \\ \downarrow \bar{h}_q & & \downarrow \bar{f}_{q+1} \\ H^q(G, C') & \xrightarrow{\delta} & H^{q+1}(G, A') \end{array}$$

*Beweis.* Das folgt direkt aus der Konstruktion von  $\delta$ . □

**Satz 2.26.** Sei

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \xrightarrow{f_1} & A & \xrightarrow{f_2} & A'' & \longrightarrow & 0 \\ & & \downarrow i' & & \downarrow i & & \downarrow i'' & & \\ 0 & \longrightarrow & B' & \xrightarrow{g_1} & B & \xrightarrow{g_2} & B'' & \longrightarrow & 0 \\ & & \downarrow j' & & \downarrow j & & \downarrow j'' & & \\ 0 & \longrightarrow & C' & \xrightarrow{h_1} & C & \xrightarrow{h_2} & C''' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

ein kommutatives Diagramm von  $G$ -Moduln mit exakten Zeilen und Spalten. Dann kommutiert

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

*Beweis.* Sei

$$D := \ker \left( B \xrightarrow{g_2} B'' \xrightarrow{j''} C'' \right) = \ker \left( B \xrightarrow{j} C \xrightarrow{h_2} C'' \right).$$

Dann ist die Sequenz

$$0 \longrightarrow D \longrightarrow B \longrightarrow C'' \longrightarrow 0$$

exakt. Sei weiter

$$\begin{aligned} I : A' &\longrightarrow A \oplus B' \\ a' &\longmapsto (f_1(a'), i'(a')) \end{aligned}$$

und

$$\begin{aligned} J : A \oplus B' &\longrightarrow D \subseteq B \\ (a, b') &\longmapsto i(a) - g_1(b') \end{aligned}$$

**Behauptung 1.** *Die Sequenz*

$$0 \longrightarrow A' \xrightarrow{I} A \oplus B' \xrightarrow{J} D \longrightarrow 0$$

*ist exakt.*

*Beweis.* • Exaktheit bei  $D$ :

Sei  $b \in D$ . Dann ist  $j''(g_2(b)) = 0$  und somit gibt es ein eindeutiges  $a'' \in A''$ , sodass  $i''(a'') = g_2(b)$ . Sei nun  $a \in A$  mit  $f_2(a) = a''$ . Dann gilt

$$g_2(i(a)) = i''(f_2(a)) = i''(a'') = g_2(b).$$

Es folgt  $i(a) - b \in \ker(g_2) = \text{im}(g_1)$ , d.h. es gibt ein eindeutiges  $b' \in B'$ , sodass  $g_1(b') = i(a) - b$ , und wir erhalten

$$b = i(a) - g_1(b') \in \text{im}(J).$$

• Exaktheit bei  $A \oplus B'$ :

Es gilt

$$J(I(a')) = J((f_1(a'), i'(a'))) = i(f_1(a')) - g_1(i'(a')) = 0,$$

d.h.  $\text{im}(I) \subseteq \ker(J)$ . Sei nun  $(a, b') \in \ker(J)$ . Dies ist genau dann der Fall, wenn  $i(a) = g_1(b')$  ist. Es gilt

$$i''(f_2(a)) = g_2(i(a)) = g_2(g_1(b')) = 0,$$

d.h.  $f_2(a) = 0$ . Dann gibt es ein eindeutiges  $a' \in A'$ , sodass  $f_1(a') = a$ . Es ist noch zu zeigen, dass  $i'(a') = b'$  ist. Dazu betrachte

$$g_1(i'(a')) = i(f_1(a')) = i(a) = g_1(b').$$

Da  $g_1$  injektiv ist, folgt  $i'(a') = b'$ .

• Exaktheit bei  $A'$

Es gilt

$$\begin{aligned} I(a') = 0 &\iff f_1(a') = 0 \text{ und } i'(a') = 0 \\ &\iff a' = 0. \end{aligned}$$

□

**Behauptung 2.** *Das folgende Diagramm ist kommutativ:*

$$\begin{array}{ccccccccc} A' & \xrightarrow{f_1} & A & \xrightarrow{f_2} & A'' & \xrightarrow{i''} & B'' & \xrightarrow{j''} & C'' \\ \text{id} \uparrow & & (\text{id}, 0) \uparrow & & \uparrow & & g_2 \uparrow & & \text{id} \uparrow \\ A' & \xrightarrow{I} & A \oplus B' & \xrightarrow{J} & D & \xrightarrow{\subseteq} & B & \xrightarrow{j'' \circ g_2} & C'' \\ -\text{id} \downarrow & & (0, -\text{id}) \downarrow & & \downarrow & & j \downarrow & & \text{id} \downarrow \\ A' & \xrightarrow{i'} & B' & \xrightarrow{j'} & C' & \xrightarrow{h_1} & C & \xrightarrow{h_2} & C'' \end{array}$$

**Bemerkungen.** • Die einzelnen Rechtecke innerhalb des Diagramms werden jeweils mit der Zeile und Spalte indiziert, also z.B. hat das Rechteck

$$\begin{array}{ccc} B'' & \xrightarrow{j''} & C'' \\ g_2 \uparrow & & \text{id} \uparrow \\ B & \xrightarrow{j'' \circ g_2} & C'' \end{array}$$

die Bezeichnung (1, 4). Dies gilt auch für alle folgenden Diagramme.

- Die gestrichelten Pfeile sind für Behauptung 2 zu ignorieren, d.h. hier wird die Kommutativität des großen Rechtecks (1, 2 + 3), das die Rechtecke (1, 2) und (1, 3) umfasst, behauptet (analog für die unteren Rechtecke).

*Beweis.* Wir geben hier eine Kostprobe, indem wir die Kommutativität im Rechteck (2, 1) nachrechnen:

$$\begin{aligned} (0, -\text{id})(I(a')) &= -i'(a'), \\ i'((-\text{id})(a')) &= -i'(a'). \end{aligned}$$

Die Kommutativität der restlichen Rechtecke folgt analog. □

**Behauptung 3.** *Das Diagramm lässt sich kommutativ vervollständigen.*

*Beweis.* Betrachte zuerst  $D \dashrightarrow A''$ :

Da  $J$  surjektiv ist, kann man ein Urbild  $(a, b')$  von  $d \in D$  wählen und somit das Bild von  $d$  als  $f_2(a)$  definieren. Dies ist wohldefiniert, da  $\ker(J) = \text{im}(I)$  und  $f_2 \circ f_1 = 0$  ist. Dann ist das Rechteck (1, 2) per Konstruktion kommutativ.

Es ist noch zu zeigen, dass das Rechteck (1, 3) ebenfalls kommutiert. Dies folgt aus der Surjektivität von  $J$  und der Kommutativität der Rechtecke (1, 2) und (1, 2 + 3).

Der Beweis für  $D \dashrightarrow C'$  funktioniert analog. □

Das Diagramm

$$\begin{array}{ccccc}
 H^{q-1}(G, C'') & \longrightarrow & H^q(G, A'') & \longrightarrow & H^{q+1}(G, A') \\
 \parallel & & \uparrow & & \text{id} \uparrow \\
 H^{q-1}(G, C'') & \longrightarrow & H^q(G, D) & \longrightarrow & H^{q+1}(G, A') \\
 \parallel & & \downarrow & & -\text{id} \downarrow \\
 H^{q-1}(G, C'') & \longrightarrow & H^q(G, C') & \longrightarrow & H^{q+1}(G, A')
 \end{array}$$

kommutiert wegen der Funktorialität des Verbindungshomomorphismus  $\delta$ . Das ist die Aussage des Satzes. □

**Satz 2.27.** Sei  $\{A_i \mid i \in I\}$  eine Familie von  $G$ -Moduln. Dann gilt

$$\begin{aligned}
 H^q(G, \bigoplus_{i \in I} A_i) &\cong \bigoplus_{i \in I} H^q(G, A_i), \\
 H^q(G, \prod_{i \in I} A_i) &\cong \prod_{i \in I} H^q(G, A_i).
 \end{aligned}$$

*Beweis.* Sei  $A = \bigoplus_{i \in I} A_i = \{(a_i)_{i \in I} \in \prod_{i \in I} A_i \mid a_i = 0 \text{ für fast alle } i\}$ . Es ist

$$\begin{aligned}
 A_q &= \text{Hom}_G(X_q, A) \cong \bigoplus_{i \in I} \text{Hom}_G(X_q, A_i) = \bigoplus_{i \in I} (A_i)_q \\
 f &\mapsto (\pi_i \circ f)_{i \in I} \\
 (x \mapsto \sum_{i \in I} f_i(x)) &\leftrightarrow (f_i)_{i \in I}
 \end{aligned}$$

(wohldefiniert, da die  $X_q$  endlich erzeugt sind).

Damit erhalten wir das unendliche kommutative Diagramm

$$\begin{array}{ccccccc}
 \dots & \longrightarrow & A_{q-1} & \longrightarrow & A_q & \longrightarrow & A_{q+1} & \longrightarrow & \dots \\
 & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \\
 \dots & \longrightarrow & \bigoplus_{i \in I} (A_i)_{q-1} & \longrightarrow & \bigoplus_{i \in I} (A_i)_q & \longrightarrow & \bigoplus_{i \in I} (A_i)_{q+1} & \longrightarrow & \dots
 \end{array}$$

Die Aussage für das Produkt folgt analog. □

**Anwendung.** Wir werden zeigen, dass  $H^q(G, \mathbb{Z}[G]) = 0$  für alle  $q \in \mathbb{Z}$ . Es folgt, dass  $H^q(G, P) = 0$  für alle  $q \in \mathbb{Z}$  und für alle projektiven  $G$ -Moduln  $P$  (siehe Blatt 5, Aufgabe 2c).

## 2.4 $G$ -induzierte Moduln

**Definition 2.28.** Ein  $G$ -Modul  $A$  heißt  $G$ -induziert, falls es eine Untergruppe  $D \leq A$  gibt, sodass

$$A = \bigoplus_{\sigma \in G} \sigma D$$

(hierbei wird  $D$  als trivialer Modul betrachtet).

**Beispiel 2.29.** Es ist

$$\mathbb{Z}[G] = \bigoplus_{\sigma \in G} \sigma \mathbb{Z},$$

wobei wir  $\mathbb{Z}$  für die Untergruppe  $\mathbb{Z} \cdot 1_G$  von  $\mathbb{Z}[G]$  schreiben.

**Satz 2.30.** Sei  $A$   $G$ -induziert und  $H \leq G$ . Dann ist  $A$   $H$ -induziert. Falls  $H \trianglelefteq G$  ein Normalteiler ist, so ist  $A^H$   $G/H$ -induziert.

*Beweis.* Sei  $A = \bigoplus_{\sigma \in G} \sigma D$ . Dann gilt

$$A = \bigoplus_{\tau \in H \backslash G} \bigoplus_{\sigma \in H} \sigma \tau D = \bigoplus_{\sigma \in H} \sigma \left( \bigoplus_{\tau \in H \backslash G} \tau D \right)$$

Sei nun  $H \trianglelefteq G$ .

**Behauptung.**  $A^H = \bigoplus_{\tau \in G/H} \tau N_H D$ .

*Beweis.* Die Summe ist tatsächlich direkt, da

$$\bigoplus_{\tau \in G/H} \tau N_H D \subseteq \bigoplus_{\sigma \in G} \sigma D.$$

Für die Inklusion „ $\supseteq$ “ sei  $\tau N_H d \in \tau N_H D$  und  $h \in H$ . Dann gilt

$$h \tau N_H d = \tau \underbrace{(\tau^{-1} h \tau)}_{\in H} N_H d = \tau N_H d.$$

Für die andere Inklusion „ $\subseteq$ “ sei  $a \in A^H$ . Sei

$$a = \sum_{\tau \in G} \tau d_\tau$$

mit  $d_\tau \in D$ . Dann gilt für alle  $\sigma \in H$

$$\sum_{\tau \in G} \sigma \tau d_{\sigma \tau} = a = \sigma a = \sum_{\tau \in G} \sigma \tau d_\tau$$

und es folgt  $d_{\sigma \tau} = d_\tau$  für alle  $\sigma \in H$  und  $\tau \in G$ . Wir erhalten

$$\begin{aligned} a &= \sum_{\tau \in G/H} \sum_{\sigma \in H} \tau \sigma d_{\tau \sigma} = \sum_{\tau \in G/H} \tau \sum_{\sigma \in H} \sigma d_{\tau \sigma \tau^{-1}} \\ &= \sum_{\tau \in G/H} \tau \left( \sum_{\sigma \in H} \sigma \right) d_\tau \in \sum_{\tau \in G/H} \tau N_H D \end{aligned}$$

□

Der Satz ist mit der Behauptung bewiesen.  $\square$

**Satz 2.31.** Sei  $X$   $G$ -induziert und  $A$  ein beliebiger  $G$ -Modul. Dann ist  $X \otimes A = X \otimes_{\mathbb{Z}} A$  ebenfalls  $G$ -induziert.

*Beweis.* Es ist

$$\begin{aligned} X \otimes A &= \left( \bigoplus_{\sigma \in G} \sigma D \right) \otimes A = \bigoplus_{\sigma \in G} (\sigma D \otimes A) \\ &= \bigoplus_{\sigma \in G} (\sigma D \otimes \sigma A) = \bigoplus_{\sigma \in G} \sigma (D \otimes A) \end{aligned}$$

und somit ist  $X \otimes A$   $G$ -induziert.  $\square$

**Definition 2.32.** Ein  $G$ -Modul  $A$  hat *triviale Kohomologie* (oder ist *kohomologisch trivial*), falls für alle  $U \leq G$  und  $q \in \mathbb{Z}$  gilt

$$H^q(U, A) = 0$$

**Satz 2.33.** Jeder  $G$ -induzierte Modul hat triviale Kohomologie.

**Beispiel 2.34.** Das zeigt  $H^q(U, \mathbb{Z}[G]) = 0$  für alle  $q \in \mathbb{Z}$  und alle Untergruppen  $U \leq G$ . Eine Konsequenz hieraus ist, dass jeder projektive  $G$ -Modul triviale Kohomologie hat (siehe Blatt 5, Aufgabe 2c)).

*Beweis.* Ohne Einschränkung genügt es  $U = G$  zu betrachten. Es ist zu zeigen, dass die Sequenz

$$\dots \longrightarrow \underbrace{\text{Hom}_G(X_q, A)}_{=A_q} \xrightarrow{\partial_{q+1}} \underbrace{\text{Hom}_G(X_{q+1}, A)}_{=A_{q+1}} \longrightarrow \dots \quad (2.4)$$

exakt ist.

Sei  $A = \bigoplus_{\sigma \in G} \sigma D$  und  $\pi : A \rightarrow D$  die Projektion auf die Komponente der 1. Dann ist

$$\begin{aligned} \text{Hom}_G(X_q, A) &\cong \text{Hom}_{\mathbb{Z}}(X_q, D) & (2.5) \\ f &\mapsto \pi \circ f \\ \left( x \xrightarrow{f_h} \sum_{\sigma \in G} \sigma^{-1} f(\sigma x) \right) &\leftrightarrow h \end{aligned}$$

ein Isomorphismus.

**Übung 2.35.** Es gilt:

- $f_h$  ist  $G$ -verträglich,
- $f(x) = \sum_{\sigma \in G} \sigma^{-1} (\pi \circ f)(\sigma x)$ ,
- $\pi \circ f_h = h$ .



Identifiziert man gemäß (2.5), so wird aus (2.4)

$$\dots \longrightarrow \text{Hom}_{\mathbb{Z}}(X_q, D) \longrightarrow \text{Hom}_{\mathbb{Z}}(X_{q+1}, D) \longrightarrow \dots \quad (2.6)$$

Da die Sequenz

$$\dots \longleftarrow X_q \longleftarrow X_{q+1} \longleftarrow \dots$$

exakt ist und  $X_q$   $\mathbb{Z}$ -frei ist, ist auch (2.6) exakt.  $\square$

Betrachte

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

und

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\mu} & \mathbb{Z}[G] & \longrightarrow & J_G \longrightarrow 0 \\ & & & & 1 & \longmapsto & N_G \end{array}$$

Sei  $A$  ein  $G$ -Modul. Anwendung von  $- \otimes A$  liefert die exakten Sequenzen

$$0 \longrightarrow I_G \otimes A \longrightarrow \mathbb{Z}[G] \otimes A \longrightarrow A \longrightarrow 0$$

und

$$0 \longrightarrow A \longrightarrow \mathbb{Z}[G] \otimes A \longrightarrow J_G \otimes A \longrightarrow 0.$$

Da  $\mathbb{Z}[G] \otimes A$   $G$ -induziert ist, erhalten wir aus der langen exakten Kohomologiesequenz die Isomorphismen

$$\begin{aligned} \delta &: H^{q-1}(U, J_G \otimes A) \longrightarrow H^q(U, A), \\ \delta^{-1} &: H^{q+1}(U, I_G \otimes A) \longrightarrow H^q(U, A) \end{aligned}$$

für alle  $q \in \mathbb{Z}$  und alle Untergruppen  $U \leq G$ .

**Definition 2.36.** Wir definieren

$$\begin{aligned} A^m &:= \underbrace{J_G \otimes J_G \otimes \dots \otimes J_G}_{m \text{ Faktoren}} \otimes A, & m \geq 0, \\ A^m &:= \underbrace{I_G \otimes I_G \otimes \dots \otimes I_G}_{|m| \text{ Faktoren}} \otimes A, & m \leq 0. \end{aligned}$$

Für  $m \geq 0$  erhält man

$$\delta^m : H^{q-m}(U, A^m) \xrightarrow{\delta} H^{q-m+1}(U, A^{m-1}) \longrightarrow \dots \longrightarrow H^q(U, A)$$

und für  $m \leq 0$

$$\delta^m : H^{q-m}(U, A^m) \xrightarrow{\delta^{-1}} H^{q-m-1}(U, A^{m+1}) \longrightarrow \dots \longrightarrow H^q(U, A).$$

**Bemerkungen 2.37.** (1)  $\delta^m$  ist ein Isomorphismus für alle  $m \in \mathbb{Z}$ .

- (2) Mit der *Methode der Dimensionsverschiebung* kann man Resultate für Kohomologiegruppen kleiner Dimension auf beliebige Dimensionen übertragen.

Ein Beispiel für die Dimensionsverschiebung ist der folgende

**Satz 2.38.** *Es gilt  $|G| H^q(G, A) = 0$  für alle  $q \in \mathbb{Z}$ .*

*Beweis.* Sei  $C$  ein beliebiger  $G$ -Modul.

**Behauptung.** *Es gilt  $|G| H^0(G, C) = 0$ .*

*Beweis.* Es ist  $H^0(G, C) = C^G/N_G C$ . Sei  $c + N_G C \in C^G/N_G C$  beliebig. Dann gilt

$$|G| (c + N_G C) = |G| c + N_G C = N_G c + N_G C = 0.$$

□

Wähle nun  $C = A^q$  und  $m = q$ . Dann folgt mit

$$\delta^q : H^0(G, A^q) \xrightarrow{\cong} H^q(G, A),$$

dass  $|G| H^q(G, A) = 0$  ist.

□

**Korollar 2.39.** *Falls  $A$  ein endlich erzeugter  $G$ -Modul ist, so ist  $H^q(G, A)$  endlich für alle  $q \in \mathbb{Z}$ .*

*Beweis.* Der Modul  $A_q = \text{Hom}_G(X_q, A)$  ist endlich erzeugt. Somit ist auch  $H^q(G, A) = Z_q(A)/B_q(A)$  endlich erzeugt. Da  $H^q(G, A)$  von  $|G|$  annulliert wird, ist  $H^q(G, A)$  also endlich.

□

**Definition 2.40.** Eine abelsche Gruppe  $A$  hat *uneingeschränkte und eindeutige Division*, falls es zu jedem  $n \in \mathbb{N}$  und allen  $a \in A$  genau ein  $a_1 \in A$  mit  $na_1 = a$  gibt.

**Beispiele 2.41.** (1)  $\mathbb{Q}$  hat uneingeschränkte und eindeutige Division.

(2)  $\mathbb{Q}/\mathbb{Z}$  hat uneingeschränkte Division. Diese ist aber nicht eindeutig!

**Satz 2.42.** *Falls  $A$  uneingeschränkte und eindeutige Division hat, so ist  $A$  kohomologisch trivial.*

*Beweis.* Sei

$$n \cdot \text{id} : A \longrightarrow A$$

die Multiplikation mit  $n$ . Da  $A$  uneingeschränkte und eindeutige Division hat, ist dies ein Isomorphismus, wie auch die induzierte Abbildung

$$n \cdot \text{id} : H^q(U, A) \longrightarrow H^q(U, A).$$

Also ist  $H^q(U, A) \cong nH^q(U, A)$  für alle  $n \in \mathbb{N}$  und durch die Wahl  $n = |G|$  erhalten wir  $H^q(U, A) = 0$  für alle  $q \in \mathbb{Z}$ .

□

**Beispiele 2.43.** (1)  $\mathbb{Q}$  ist kohomologisch trivial.

(2) Betrachte die exakte Sequenz

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0. \quad (2.7)$$

Dann ist  $H^q(G, \mathbb{Q}/\mathbb{Z}) \cong H^{q+1}(G, \mathbb{Z})$  und insbesondere  $H^{-1}(G, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/|G|\mathbb{Z}$ .

(3) Falls  $A$   $m$ -Torsion ist für ein  $m \in \mathbb{N}$  und  $(m, |G|) = 1$ , so ist  $H^q(U, A) = 0$  für alle  $q \in \mathbb{Z}$ .

*Beweis.* Übung (zeige  $mH^q(U, A) = 0$ ). □

**Bemerkung 2.44.** Es gilt

$$\begin{aligned} H^{-2}(G, \mathbb{Z}) &\cong G^{\text{ab}}, \\ H^{-1}(G, \mathbb{Z}) &= 0, \\ H^0(G, \mathbb{Z}) &= \mathbb{Z}/|G|\mathbb{Z}, \\ H^1(G, \mathbb{Z}) &= \text{Hom}(G, \mathbb{Z}) = 0. \end{aligned}$$

Wir können nun zeigen

$$H^2(G, \mathbb{Z}) = \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \text{Hom}(G, \mathbb{C}^\times),$$

denn wir erhalten aus (2.7)

$$\text{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{Z})$$

und die Abbildung

$$\begin{aligned} \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) &\longrightarrow \text{Hom}(G, \mathbb{C}^\times) \\ f &\longmapsto (\sigma \mapsto e^{2\pi i f(\sigma)}) \end{aligned}$$

ist ein Isomorphismus.

**Definition 2.45.** Die Gruppe

$$\chi(G) := \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

heißt *Gruppe der (abelschen) Charaktere von  $G$* .

## 2.5 Inflation, Restriktion und Korestriktion

**Motivation.** Ist  $A$  ein  $G$ -Modul und  $U \leq G$  eine Untergruppe, so ist  $A$  auch ein  $U$ -Modul. Ist  $U \trianglelefteq G$  ein Normalteiler, so ist  $A^U$  ein  $G/U$ -Modul. Wir wollen nun die Zusammenhänge zwischen  $H^q(G/U, A^U)$ ,  $H^q(G, A)$  und  $H^q(U, A)$  studieren.

Sei ab jetzt  $q \geq 1$ .

**Definition 2.46.** Sei  $U \trianglelefteq G$  ein Normalteiler und

$$x : G/U \times \cdots \times G/U \longrightarrow A^U$$

eine  $q$ -Kokette, d.h. ein Element von  $(A^U)_q$ . Dann wird eine  $q$ -Kokette  $y \in A$  definiert durch

$$\begin{aligned} y : G \times \cdots \times G &\longrightarrow A \\ y(\sigma_1, \dots, \sigma_q) &:= x(\sigma_1 U, \dots, \sigma_q U) \end{aligned}$$

Man schreibt  $y = \inf x = \inf_{G/U}^G x$ .

Das Diagramm

$$\begin{array}{ccc} (A^U)_q & \xrightarrow{\partial_{q+1}} & (A^U)_{q+1} \\ \downarrow \inf & & \downarrow \inf \\ A_q & \xrightarrow{\partial_{q+1}} & A_{q+1} \end{array}$$

kommutiert, d.h. Zyklen gehen auf Zyklen und Ränder auf Ränder über.

**Definition 2.47.** Die induzierte Abbildung

$$\text{Inf}_q : H^q(G/U, A^U) \longrightarrow H^q(G, A)$$

heißt *Inflation*.

**Satz 2.48.** Sei  $U \trianglelefteq G$  ein Normalteiler und  $A$  ein  $G$ -Modul. Dann ist die folgende Sequenz exakt:

$$0 \longrightarrow H^1(G/U, A^U) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(U, A)$$

Wir erinnern uns, dass für  $\bar{x} \in H^1(G/U, A^U)$  repräsentiert durch  $x : G/U \longrightarrow A^U$  das Bild  $\text{Inf}(\bar{x})$  repräsentiert wird durch

$$\begin{aligned} \text{inf}(x) : G &\longrightarrow A \\ g &\longmapsto x(gU) \end{aligned}$$

Das Bild von  $\bar{y} \in H^1(G, A)$  unter der *Restriktion* wird repräsentiert durch

$$\begin{aligned} \text{res}(y) : U &\longrightarrow A \\ u &\longmapsto y(u) \end{aligned}$$

*Beweis.* • Exaktheit bei  $H^1(G/U, A^U)$ :

Sei  $x : G/U \longrightarrow A^U$  ein 1-Kozyklus mit  $\text{Inf}(\bar{x}) = 0$ . Dann ist  $\text{inf}(x)$  ein 1-Korand, d.h.

$$\text{inf}(x)(\sigma) = x(\sigma U) = \sigma a - a$$

für ein  $a \in A$  für alle  $\sigma \in G$ .

Es genügt zu zeigen, dass  $a \in A^U$  ist. Für alle  $\tau \in U$  gilt wegen

$$\sigma a - a = x(\sigma U) = x(\sigma \tau U) = \text{inf}(x)(\sigma \tau) = \sigma \tau a - a,$$

dass  $\tau a = a$  für alle  $\tau \in U$  ist. Damit folgt aber  $a \in A^U$  und  $x$  ist ein 1-Korand.

- Exaktheit bei  $H^1(G, A)$ :

Sei  $x : G/U \rightarrow A^U$  ein 1-Kozyklus. Dann gilt

$$\text{res}(\text{inf}(x))(\tau) = \text{inf}(x)(\tau) = x(\tau U) = x(\bar{1}) = 0,$$

denn  $x(\bar{1}) = x(\bar{1} \cdot \bar{1}) = x(\bar{1}) + x(\bar{1})$ . Also ist  $\text{im}(\text{Inf}) \subseteq \text{ker}(\text{Res})$ .

Sei umgekehrt  $x : G \rightarrow A$  ein 1-Kozyklus mit  $\text{Res}(\bar{x}) = 0$ . Dann ist  $\text{res}(x)$  ein 1-Korand, d.h. es gibt ein  $a \in A$  mit

$$x(\tau) = \tau a - a$$

für alle  $\tau \in U$ . Betrachte den 1-Korand

$$\begin{aligned} \rho : G &\rightarrow A \\ \sigma &\mapsto \sigma a - a \end{aligned}$$

in  $B_1(G, A)$ . Dann gilt für  $x' := x - \rho$ :

$$x'(\tau) = 0$$

für alle  $\tau \in U$  und  $\bar{x}' = \bar{x}$  in  $H^1(G, A)$ . Es gilt weiter

$$x'(\sigma\tau) = x'(\sigma) + \sigma x'(\tau) = x'(\sigma) \tag{2.8}$$

$$x'(\tau\sigma) = x'(\tau) + \tau x'(\sigma) = \tau x'(\sigma) \tag{2.9}$$

für alle  $\sigma \in G$  und  $\tau \in U$ .

Definiere

$$\begin{aligned} y : G/U &\rightarrow A^U \\ \sigma U &\mapsto x'(\sigma) \end{aligned}$$

Wegen (2.8) ist dies wohldefiniert und wegen

$$\tau x'(\sigma) \stackrel{(2.9)}{=} x'(\tau\sigma) = x'(\underbrace{\sigma \sigma^{-1} \tau \sigma}_{\in U}) \stackrel{(2.8)}{=} x'(\sigma)$$

für alle  $\tau \in U$ , ist  $x'(\sigma) \in A^U$ . Es ist klar, dass  $\text{Inf}(\bar{y}) = \bar{x}' = \bar{x}$  gilt und somit folgt  $\text{ker}(\text{Res}) = \text{im}(\text{Inf})$ . □

**Satz 2.49.** Sei  $U \trianglelefteq G$  ein Normalteiler und  $A$  ein  $G$ -Modul. Sei  $q \geq 1$  und es gelte  $H^i(U, A) = 0$  für  $i = 1, \dots, q - 1$ . Dann ist die Sequenz

$$0 \rightarrow H^q(G/U, A^U) \xrightarrow{\text{Inf}} H^q(G, A) \xrightarrow{\text{Res}} H^q(U, A)$$

exakt.

*Beweis.* Dies folgt leicht mit Dimensionsverschiebung (siehe [NS11, Kapitel I, Satz (4.7)]). □

## Die Restriktion für $q = 0$

Betrachte

$$\begin{aligned} A^G/N_G A &= H^0(G, A) \xrightarrow{\text{Res}_0} H^0(U, A) = A^U/N_U A \\ a + N_G A &\longmapsto a + N_U A \end{aligned}$$

Dies ist wohldefiniert, da  $N_G A = N_{G/U} N_U A = N_U N_{G/U} A \subseteq N_U A$ .

**Übung 2.50** (siehe Blatt 7, Aufgabe 1). *Ist*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

eine exakte Sequenz von  $G$ -Moduln, so kommutiert

$$\begin{array}{ccc} H^0(G, C) & \xrightarrow{\text{Res}_0} & H^0(U, C) \\ \downarrow \delta & & \downarrow \delta \\ H^1(G, A) & \xrightarrow{\text{Res}_1} & H^1(U, A) \end{array}$$

**Bemerkung 2.51.** Man kann die Restriktion auf alle Dimensionen  $q \in \mathbb{Z}$  mittels Dimensionsverschiebung fortsetzen (siehe [NS11, Kapitel I, Definition (4.9)]).

## Die Korestriktion

Ziel: Für eine Untergruppe  $U \leq G$  und einen  $G$ -Modul  $A$  konstruiere

$$H^q(U, A) \longrightarrow H^q(G, A)$$

für alle  $q \in \mathbb{Z}$ .

$q = -1$  Definiere

$$\begin{aligned} H^{-1}(U, A) &= N_U A / I_U A \xrightarrow{\text{Kor}_{-1}} N_G A / I_G A = H^{-1}(G, A) \\ a + I_U A &\longmapsto a + I_G A \end{aligned}$$

Dies ist wohldefiniert, da

$$I_U A = \langle \tau a - a \mid \tau \in U, a \in A \rangle \subseteq I_G A.$$

$q = 0$  Definiere

$$\begin{aligned} H^0(U, A) &= A^U / N_U A \xrightarrow{\text{Kor}_0} A^G / N_G A = H^0(G, A) \\ a + N_U A &\longmapsto N_{G/U} a + N_G A \end{aligned}$$

wobei  $N_{G/U} = \sum_{\sigma \in G/U} \sigma$ .

**Lemma 2.52.** *Sei*

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$$

eine exakte Sequenz von  $G$ -Moduln. Dann kommutiert

$$\begin{array}{ccc} H^{-1}(U, C) & \xrightarrow{\delta} & H^0(U, A) \\ \downarrow \text{Kor}_{-1} & & \downarrow \text{Kor}_0 \\ H^{-1}(G, C) & \xrightarrow{\delta} & H^0(G, A) \end{array}$$

*Beweis.* Sei  $\bar{c} \in H^{-1}(U, C) = N_U C / I_U C$ . Wir berechnen zuerst  $\text{Kor}_0 \circ \delta$ . Betrachte hierfür das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{-1} & \xrightarrow{i} & B_{-1} & \xrightarrow{j} & C_{-1} & \longrightarrow & 0 \\ & & \downarrow \partial & & \downarrow \partial & & \downarrow \partial & & \\ 0 & \longrightarrow & A_0 & \xrightarrow{i} & B_0 & \xrightarrow{j} & C_0 & \longrightarrow & 0 \end{array}$$

wobei  $A_{-1} = A_0 = A$  und  $\partial = N_U$  (analog für  $B$  und  $C$ ).

Sei  $b \in B_{-1} = B$  mit

$$j(b) = c. \tag{2.10}$$

Dann folgt  $j(\partial b) = 0$ , d.h. es existiert ein eindeutiges  $a \in A_0 = A$  mit

$$i(a) = \partial b = N_U b. \tag{2.11}$$

Dann gilt

$$\delta(\bar{c}) = \bar{a} = a + N_U A$$

(leichte Übung:  $a \in A^U$ ). Also folgt

$$\text{Kor}_0(\delta(\bar{c})) = N_{G/U} a + N_G A.$$

Berechne nun  $\delta \circ \text{Kor}_{-1}$ :

Es gilt  $\delta(\text{Kor}_{-1}(\bar{c})) = \delta(c + I_G(C))$ . Betrachte das obige Diagramm als Diagramm von  $G$ -Moduln und  $\partial = N_G$ . Man nehme  $b$  wie in (2.10). Dann folgt:

$$\partial b = N_G b = N_{G/U} N_U b \stackrel{(2.11)}{=} N_{G/U}(i(a)) = i(N_{G/U} a)$$

Also ist

$$\delta(\text{Kor}_{-1}(\bar{c})) = N_{G/U} a + N_G A$$

(leichte Übung:  $N_{G/U} a \in A^G$ ). □

**Definition 2.53.** Sei  $U \leq G$  eine Untergruppe. Unter der *Korestriktion* versteht man die eindeutig bestimmte Familie von Homomorphismen

$$\text{Kor}_q : H^q(U, A) \longrightarrow H^q(G, A), \quad q \in \mathbb{Z}$$

mit:

- (1)  $\text{Kor}_0(a + N_U A) = N_{G/U} a + N_G A$ ,
- (2) Für jede exakte Sequenz von  $G$ -Moduln

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

kommutiert für alle  $q \in \mathbb{Z}$

$$\begin{array}{ccc} H^q(U, C) & \xrightarrow{\delta} & H^{q+1}(U, A) \\ \downarrow \text{Kor}_q & & \downarrow \text{Kor}_{q+1} \\ H^q(G, C) & \xrightarrow{\delta} & H^{q+1}(G, A) \end{array}$$

*Beweisansatz.* Wir betrachten hier nur die Konstruktion der Homomorphismen. Betrachte

$$\begin{aligned} \delta_G^q : H^0(G, A^q) &\xrightarrow{\cong} H^q(G, A) \\ \delta_U^q : H^0(U, A^q) &\xrightarrow{\cong} H^q(U, A) \end{aligned}$$

$\text{Kor}_q$  wird definiert durch

$$\begin{array}{ccc} H^0(U, A^q) & \xrightarrow[\cong]{\delta_U^q} & H^q(U, A) \\ \downarrow \text{Kor}_0 & & \downarrow \text{Kor}_q \\ H^0(G, A^q) & \xrightarrow[\cong]{\delta_G^q} & H^q(G, A) \end{array}$$

□

**Bemerkung 2.54.** Der Modul  $A^q$  ist hierbei stets definiert als

$$A^q := I_G \otimes \cdots \otimes I_G \otimes A$$

für  $q < 0$  bzw.

$$A^q := J_G \otimes \cdots \otimes J_G \otimes A$$

für  $q > 0$ , d.h. unabhängig von  $U$ . Wir erhalten dennoch Isomorphismen

$$H^0(U, A^q) \cong H^q(U, A)$$

für jede Untergruppe  $U \leq G$  (vgl. Definition 2.36 und Bemerkungen 2.37 bzw. [NS11, Kapitel I, Satz (3.15)]).



**Übung 2.55** (siehe Blatt 7, Aufgabe 2). *Es gilt*

$$\begin{aligned} \text{Kor}_{-2} : U/U' = U^{ab} \cong H^{-2}(U, \mathbb{Z}) &\longrightarrow H^{-2}(G, \mathbb{Z}) \cong G^{ab} = G/G' \\ uU' &\longmapsto uG' \end{aligned}$$

wobei  $U'$  bzw.  $G'$  die jeweilige Kommutatoruntergruppe bezeichnet.

**Satz 2.56.** *Es gilt*

$$\text{Kor} \circ \text{Res} = (G : U) \cdot \text{id} .$$

*Beweis.* Sei  $\bar{a} = a + N_G A \in H^0(G, A)$ . Dann ist

$$\begin{aligned} \text{Kor}_0(\text{Res}_0(\bar{a})) &= \text{Kor}_0(a + N_U A) = N_{G/U} a + N_G A \\ &\stackrel{a \in A^G}{=} (G : U)(a + N_G A) . \end{aligned}$$

Der allgemeine Fall folgt mittels Dimensionsverschiebung:  
Betrachte

$$\begin{array}{ccc} H^0(G, A^q) & \xrightarrow{\text{Kor}_0 \circ \text{Res}_0} & H^0(G, A^q) \\ \delta^q \downarrow \cong & & \delta^q \downarrow \cong \\ H^q(G, A) & \xrightarrow{\text{Kor}_q \circ \text{Res}_q} & H^q(G, A) \end{array}$$

Dann gilt

$$(\text{Kor}_q \circ \text{Res}_q)(\bar{x}) = \delta^q((G : U)(\delta^q)^{-1}(\bar{x})) = (G : U)(\bar{x}) .$$

□

**Satz 2.57.** *Res und Kor sind funktoriell im folgenden Sinn: Ist  $f : A \longrightarrow B$  ein Homomorphismus von  $G$ -Moduln, so ist*

$$\begin{array}{ccc} H^q(G, A) & \xrightarrow{\bar{f}} & H^q(G, B) \\ \text{Kor} \uparrow \downarrow \text{Res} & & \text{Kor} \uparrow \downarrow \text{Res} \\ H^q(U, A) & \xrightarrow{\bar{f}} & H^q(G, B) \end{array}$$

*kommutativ.*

*Beweis.* Leicht mit Dimensionsverschiebung (siehe [NS11, Kapitel I, Satz (4.15)]). □

**Definition 2.58.** Für eine Primzahl  $p$  bezeichnet  $H^q(G, A)_p$  die  $p$ -Sylowuntergruppe von  $H^q(G, A)$ . Man nennt  $H^q(G, A)_p$  oft den  $p$ -primären Teil.

Die folgenden Aussagen sind klar:

- $H^q(G, A) = \bigoplus_{p \mid |G|} H^q(G, A)_p$ ,

- $H^q(G, A)_p = \{\bar{x} \in H^q(G, A) \mid \text{ord}(\bar{x}) = p^n \text{ für ein } n \in \mathbb{N}\}$ ,
- $H^q(G, A)_p = H^q(G, A) \otimes \mathbb{Z}_p = H^q(G, A \otimes \mathbb{Z}_p)$ . Letztere Gleichheit gilt, da  $- \otimes \mathbb{Z}_p$  exakt ist (Übung).

**Satz 2.59.** Sei  $A$  ein  $G$ -Modul und  $G_p \leq G$  eine  $p$ -Sylowuntergruppe. Dann gilt

$$\begin{aligned} \text{Res} : H^q(G, A)_p &\hookrightarrow H^q(G_p, A), \\ \text{Kor} : H^q(G_p, A) &\twoheadrightarrow H^q(G, A)_p. \end{aligned}$$

*Beweis.* Betrachte

$$\begin{array}{ccc} H^q(G, A)_p & \xrightarrow[\cong]{(G:G_p)} & H^q(G, A)_p \\ & \searrow \text{Res} & \nearrow \text{Kor} \\ & H^q(G_p, A) & \end{array}$$

Die Korestriktion bildet in den  $p$ -primären Teil ab, da  $|G_p| H^q(G_p, A) = 0$  gilt. Daraus folgt die Behauptung.  $\square$

**Korollar 2.60.** Ist für jede Primzahl  $p$  die Gruppe  $H^q(G_p, A)$  trivial für eine  $p$ -Sylowuntergruppe  $G_p \leq G$ , so ist  $H^q(G, A)$  trivial.

### Shapiros Lemma

**Definition 2.61.** Sei  $U \leq G$  eine Untergruppe. Ein  $G$ -Modul  $A$  heißt  $G/U$ -induziert, falls

$$A = \bigoplus_{\sigma \in G/U} \sigma D$$

mit einem  $U$ -Modul  $D$ .

**Beispiel 2.62.** Es gilt

$$\mathbb{Z}[G/U] = \bigoplus_{\sigma \in G/U} \sigma \cdot \mathbb{Z} = \mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} \mathbb{Z}.$$

**Bemerkung 2.63.** Die  $G/U$ -induzierten Moduln sind genau die Moduln der Form

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}[U]} X$$

mit einem  $U$ -Modul  $X$  (Übung).

**Satz 2.64** (Lemma von Shapiro). Sei  $A$  ein  $G/U$ -induzierter Modul,

$$A = \bigoplus_{\sigma \in G/U} \sigma D$$

mit einem  $U$ -Modul  $D$ . Dann gilt

$$H^q(G, A) \cong H^q(U, D)$$

für alle  $q \in \mathbb{Z}$ . Dieser Isomorphismus ist gegeben durch

$$H^q(G, A) \xrightarrow{\text{Res}} H^q(U, A) \xrightarrow{\bar{\pi}} H^q(U, D),$$

wobei  $\pi : A \rightarrow D$  kanonisch ist.

**Bemerkung 2.65.** Ist  $U = 1$ , so folgt

$$H^q(G, A) \cong H^q(1, D) = 0.$$

**Beispiel 2.66.** Sei  $L/K$  eine Galoiserweiterung von Zahlkörpern mit Galoisgruppe  $G$ . Sei  $I_L$  die Gruppe der gebrochenen Ideale.

Ziel: Berechne  $H^q(G, I_L)$  für  $q = -1, 0, 1$ .

Seien  $\mathfrak{p} \subseteq \mathcal{O}_K$ ,  $\mathfrak{P} \subseteq \mathcal{O}_L$  Primideale sodass  $\mathfrak{P}|\mathfrak{p}$ . Sei weiter

$$I_L(\mathfrak{p}) := \{\mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_r^{a_r} \mid a_i \in \mathbb{Z}\}$$

mit

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$$

Dann gilt:

- $I_L = \bigoplus_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ prim}}} I_L(\mathfrak{p})$ ,
- Es ist

$$I_L(\mathfrak{p}) \cong \mathbb{Z}[G/G_{\mathfrak{P}}]$$

$$\prod_{\sigma} \sigma(\mathfrak{P})^{a_{\sigma}} \leftrightarrow \sum_{\sigma \in G/G_{\mathfrak{P}}} a_{\sigma} \sigma$$

mit der Zerlegungsgruppe  $G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ .

Also folgt:

$$\begin{aligned} H^q(G, I_L) &= \bigoplus_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ prim}}} H^q(G, I_L(\mathfrak{p})) \\ &= \bigoplus_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ prim}}} H^q(G, \mathbb{Z}[G/G_{\mathfrak{P}}]) \\ &= \bigoplus_{\substack{\mathfrak{p} \subseteq \mathcal{O}_K \\ \mathfrak{p} \text{ prim}}} H^q(G_{\mathfrak{P}}, \mathbb{Z}) \\ &= \begin{cases} 0, & q = -1, \\ \bigoplus_{\mathfrak{p}} \mathbb{Z}/|G_{\mathfrak{P}}|\mathbb{Z}, & q = 0, \\ 0, & q = 1. \end{cases} \end{aligned}$$

## 2.6 Das Cupprodukt

Seien  $A, B$  zwei  $G$ -Moduln. Dann ist auch  $A \otimes B$  ein  $G$ -Modul mit

$$\sigma(a \otimes b) = \sigma(a) \otimes \sigma(b).$$

Für

$$\begin{aligned} A \times B &\longrightarrow A \otimes B \\ (a, b) &\longmapsto a \otimes b \end{aligned}$$

gilt:

$$\begin{aligned} A^G \times B^G &\longrightarrow (A \otimes B)^G, \\ N_G A \times N_G B &\longrightarrow N_G(A \otimes B), \end{aligned}$$

denn:

$$\begin{aligned} (N_G a, N_G b) &\longmapsto N_G a \otimes N_G b = \sum_{\sigma \in G} \sigma(a) \otimes N_G b \\ &= \sum_{\sigma \in G} \sigma(a \otimes N_G b) \\ &= N_G(a \otimes N_G b) \end{aligned}$$

Also induziert  $(a, b) \longmapsto a \otimes b$  eine bilineare Abbildung

$$\begin{aligned} H^0(G, A) \times H^0(G, B) &\longrightarrow H^0(G, A \otimes B) \\ (\bar{a}, \bar{b}) &\longmapsto \overline{a \otimes b} \end{aligned}$$

Diese Abbildung

$$\bar{a} \cup \bar{b} := \overline{a \otimes b} \in (A \otimes B)^G / N_G(A \otimes B)$$

heißt *Cupprodukt* in Dimension 0.

**Definition 2.67.** Es gibt eine eindeutig bestimmte Familie von bilinearen Abbildungen

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

mit:

- (1) Für  $p = q = 0$  ist  $\bar{a} \cup \bar{b} = \overline{a \otimes b}$ ,
- (2) Sind

$$0 \longrightarrow A \longrightarrow A' \longrightarrow A'' \longrightarrow 0$$

und

$$0 \longrightarrow A \otimes B \longrightarrow A' \otimes B \longrightarrow A'' \otimes B \longrightarrow 0$$

exakte Sequenzen von  $G$ -Moduln so kommutiert

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

d.h.  $\delta(\bar{a}'') \cup \bar{b} = \delta(\overline{a'' \otimes b})$ .

(3) Sind

$$0 \longrightarrow B \longrightarrow B' \longrightarrow B'' \longrightarrow 0$$

und

$$0 \longrightarrow A \otimes B \longrightarrow A \otimes B' \longrightarrow A \otimes B'' \longrightarrow 0$$

exakte Sequenzen von  $G$ -Moduln, so kommutiert

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

Zur Konstruktion:

$$\begin{array}{ccc} H^0(G, A^p) \times H^0(G, B^q) & \xrightarrow{\cup} & H^0(G, A^p \otimes B^q) = H^0(G, (A \otimes B^q)^p) \\ \downarrow (\delta^p, \text{id}) & & \downarrow \delta^p \\ H^p(G, A) \times H^0(G, B^q) & \dashrightarrow & H^p(G, A \otimes B^q) = H^p(G, (A \otimes B)^q) \\ \downarrow (\text{id}, \delta^q) & & \downarrow (-1)^{p\delta^q} \\ H^p(G, A) \times H^q(G, B) & \dashrightarrow & H^{p+q}(G, A \otimes B) \end{array}$$

**Motivation.** Sei  $K/\mathbb{Q}_p$  eine endliche Körpererweiterung und  $L/K$  eine abelsche Erweiterung mit Galoisgruppe  $G$ . Wir werden zeigen, dass  $H^2(G, L^\times)$  eine zyklische Gruppe ist und eine speziellen Erzeuger  $\alpha_{L/K}$  definieren, die *Fundamentalklasse*. Dann erhalten wir einen Isomorphismus

$$- \cup \alpha_{L/K} : G = G^{ab} = H^{-2}(G, \mathbb{Z}) \longrightarrow H^0(G, L^\times) = K^\times / N_{L/K} L^\times$$

Dieser ist das Inverse zur Artinabbildung.

Sei  $b_q : \underbrace{G \times \cdots \times G}_{q\text{-mal}} \longrightarrow B$  ein  $q$ -Kozyklus. Dann ist auch

$$\begin{aligned} a_0 \otimes b_q : G \times \cdots \times G &\longrightarrow A \otimes B \\ (\sigma_1, \dots, \sigma_q) &\longmapsto a_0 \otimes (b_q(\sigma_1, \dots, \sigma_q)) \end{aligned}$$

für  $a_0 \in A^G$  ein  $q$ -Kozyklus.

**Satz 2.68.** *Es gilt*

$$\begin{aligned} \bar{a}_0 \cup \bar{b}_q &= \overline{a_0 \otimes b_q}, \\ \bar{a}_p \cup \bar{b}_0 &= \overline{a_p \otimes b_0}. \end{aligned}$$

## Eigenschaften des Cupprodukts

- (1) Seien  $f : A \rightarrow A'$  und  $g : B \rightarrow B'$  jeweils  $G$ -Modulhomomorphismen. Weiter sei

$$\begin{aligned} f \otimes g : A \otimes B &\rightarrow A' \otimes B' \\ a \otimes b &\mapsto f(a) \otimes g(b) \end{aligned}$$

die induzierte Abbildung und  $\bar{a} \in H^p(G, A)$ ,  $\bar{b} \in H^q(G, B)$ . Dann gilt

$$\overline{f(\bar{a})} \cup \overline{g(\bar{b})} = \overline{f \otimes g(\bar{a} \cup \bar{b})}.$$

- (2) Seien  $A$  und  $B$  zwei  $G$ -Moduln und  $U \leq G$  eine Untergruppe. Sind  $\bar{a} \in H^p(G, A)$  und  $\bar{b} \in H^q(G, B)$ , so gilt

$$\text{Res}(\bar{a} \cup \bar{b}) = \text{Res}(\bar{a}) \cup \text{Res}(\bar{b}) \in H^{p+q}(U, A \otimes B).$$

- (3) Sei  $\bar{a} \in H^p(G, A)$ ,  $\bar{b} \in H^q(U, B)$ . Dann gilt

$$\text{Kor}(\text{Res}(\bar{a}) \cup \bar{b}) = \bar{a} \cup \text{Kor}(\bar{b}).$$

- (4) Für  $\bar{a} \in H^p(G, A)$  und  $\bar{b} \in H^q(G, B)$  gilt

$$\bar{a} \cup \bar{b} = (-1)^{pq} \bar{b} \cup \bar{a} \in H^{p+q}(G, A \otimes B) = H^{p+q}(G, B \otimes A) \quad (\text{Antikommutativität}).$$

- (5) Das Cupprodukt ist assoziativ.

**Lemma 2.69.** Sei  $\bar{a}_1 \in H^1(G, A)$  und  $\bar{b}_{-1} \in H^{-1}(G, B) = {}_{N_G}B / I_G B$ . Dann gilt

$$\bar{a}_1 \cup \bar{b}_{-1} = \bar{x}_0 \in H^0(G, A \otimes B) = (A \otimes B)^G / N_G(A \otimes B)$$

mit

$$x_0 = \sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1}.$$

*Beweis.* Aus

$$0 \rightarrow \mathbb{Z} \xrightarrow{N_G} \mathbb{Z}[G] \rightarrow J_G \rightarrow 0$$

folgt

$$0 \rightarrow A \rightarrow \underbrace{\mathbb{Z}[G] \otimes A}_{=: A'} \rightarrow \underbrace{J_G \otimes A}_{=: A''} \rightarrow 0$$

und

$$0 \rightarrow A \otimes B \rightarrow A' \otimes B \rightarrow A'' \otimes B \rightarrow 0.$$

Diese Sequenzen sind exakt.  $A'$  ist  $G$ -induziert, also kohomologisch trivial. Insbesondere ist also  $H^1(G, A') = 0$  und somit gibt es eine 0-Kokette  $a'_0 \in A'$  mit

$$a_1(\tau) = \tau a'_0 - a'_0 \quad (2.12)$$

für alle  $\tau \in G$ . Sei  $a''_0 \in (A'')^G$  das Bild von  $a'_0$  in  $A''$ . Betrachte dazu

$$\begin{array}{ccccccc} 0 & \longrightarrow & A_0 & \longrightarrow & A'_0 & \xrightarrow{a'_0 \mapsto a''_0} & A''_0 & \longrightarrow & 0 \\ & & \downarrow \partial & & \downarrow \partial & & \downarrow \partial & & \\ 0 & \longrightarrow & A_1 & \longrightarrow & A'_1 & \longrightarrow & A''_1 & \longrightarrow & 0 \end{array}$$

Es gilt  $\partial(a''_0)(\sigma) = \sigma a''_0 - a''_0$  und  $\bar{a}_1 = \delta(\overline{a''_0})$ . Damit folgt

$$\begin{aligned} \bar{a}_1 \cup \bar{b}_{-1} &= \delta(\overline{a''_0}) \cup \bar{b}_{-1} = \delta(\overline{a''_0 \cup \bar{b}_{-1}}) \\ &= \delta(\overline{a''_0 \otimes b_{-1}}) = \partial(\underbrace{a''_0 \otimes b_{-1}}_{\in H^{-1}(G, A \otimes B)}) \\ &\stackrel{\partial=N_G}{=} \overline{N_G(a''_0 \otimes b_{-1})} = \overline{\sum_{\tau \in G} \tau a''_0 \otimes \tau b_{-1}} \\ &\stackrel{(2.12)}{=} \overline{\sum_{\tau \in G} (a_1(\tau) + a'_0) \otimes \tau b_{-1}} \\ &= \overline{\sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1}} + \overline{a'_0 \otimes \underbrace{N_G b_{-1}}_{=0}} \end{aligned}$$

□

Sei nun  $B = \mathbb{Z}$ . Wir identifizieren  $A \otimes \mathbb{Z}$  und  $A$ .

**Erinnerung 2.70.** Es gilt

$$\begin{aligned} H^{-2}(G, \mathbb{Z}) &\cong G^{ab} \\ \bar{\sigma} &\leftrightarrow \sigma G' \end{aligned}$$

Der Isomorphismus folgt aus der Sequenz

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

und ist gegeben durch

$$\begin{aligned} H^{-2}(G, \mathbb{Z}) &\xrightarrow{\cong} H^{-1}(G, I_G) \xlongequal{\quad} I_G/I_G^2 \longrightarrow G^{ab} \\ \bar{\sigma} &\longmapsto (\sigma - 1) + I_G^2 \longmapsto \sigma G' \end{aligned} \quad (2.13)$$

**Lemma 2.71.** *Es gilt*

$$\bar{a}_1 \cup \bar{\sigma} = \overline{a_1(\sigma)} \in H^{-1}(G, A \otimes \mathbb{Z}) = H^{-1}(G, A).$$

**Bemerkung 2.72.** Es gilt  $N_G a_1(\sigma) = 0$  (leichte Übung).

*Beweis.* Aus

$$0 \longrightarrow A \otimes I_G \longrightarrow A \otimes \mathbb{Z}[G] \longrightarrow A \longrightarrow 0$$

erhält man

$$\delta : H^{-1}(G, A) \xrightarrow{\cong} H^0(G, A \otimes I_G).$$

Es genügt zu zeigen:

$$\delta(\bar{a}_1 \cup \bar{\sigma}) = \delta(\overline{a_1(\sigma)}).$$

Zur rechten Seite betrachte

$$\begin{array}{ccccccc} & & a_1(\sigma) \otimes 1 & \longmapsto & a_1(\sigma) & & \\ & & & & & & \\ 0 & \longrightarrow & A \otimes I_G & \longrightarrow & A \otimes \mathbb{Z}[G] & \longrightarrow & A \longrightarrow 0 & q = -1 \\ & & \downarrow \partial & & \downarrow \partial & & \downarrow \partial & \\ 0 & \longrightarrow & A \otimes I_G & \longrightarrow & A \otimes \mathbb{Z}[G] & \longrightarrow & A \longrightarrow 0 & q = 0 \end{array}$$

mit  $\partial = N_G$ . Aus der Konstruktion von  $\delta$  folgt

$$\begin{aligned} \delta(\overline{a_1(\sigma)}) &= \overline{N_G(a_1(\sigma) \otimes 1)} \\ &= \overline{\sum_{\tau \in G} \tau a_1(\sigma) \otimes \tau} =: \bar{x}_0 \end{aligned}$$

Für die linke Seite gilt

$$\begin{aligned} \delta(\bar{a}_1 \cup \bar{\sigma}) &= -(\bar{a}_1 \cup \delta \bar{\sigma}) \\ &\stackrel{(2.13)}{=} -\bar{a}_1 \cup \overline{(\sigma - 1)} =: \bar{y}_0, \end{aligned}$$

wobei das erste  $\delta$  den Verbindungshomomorphismus zur Sequenz

$$0 \longrightarrow A \otimes I_G \longrightarrow A \otimes \mathbb{Z}[G] \longrightarrow A \longrightarrow 0$$

bezeichnet, während das zweite  $\delta$  für den Verbindungshomomorphismus zur Sequenz

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

steht.

Es gilt wegen Lemma 2.69

$$\begin{aligned} y_0 &= - \sum_{\tau \in G} a_1(\tau) \otimes \tau(\sigma - 1) \\ &= \sum_{\tau \in G} a_1(\tau) \otimes \tau - \sum_{\tau \in G} a_1(\tau) \otimes \tau\sigma \\ &= \sum_{\tau \in G} a_1(\tau) \otimes \tau - \sum_{\tau \in G} (a_1(\tau\sigma) - \tau a_1(\sigma)) \otimes \tau\sigma \\ &= \sum_{\tau \in G} \tau a_1(\sigma) \otimes \tau\sigma \end{aligned}$$



und somit folgt

$$\begin{aligned} y_0 - x_0 &= \sum_{\tau \in G} \tau a_1(\sigma) \otimes \tau(\sigma - 1) \\ &= N_G(a_1(\sigma) \otimes (\sigma - 1)). \end{aligned}$$

Also ist  $\bar{y}_0 = \bar{x}_0 \in H^0(G, A \otimes I_G)$ . □

**Anwendung.** Sei  $\bar{a}_2 \in H^2(G, A)$ . Dann ist

$$\bar{a}_2 \cup \_ : H^{-2}(G, \mathbb{Z}) \longrightarrow H^0(G, A)$$

ein Gruppenhomomorphismus.

**Satz 2.73.** *Es gilt*

$$\bar{a}_2 \cup \bar{\sigma} = \overline{\sum_{\tau \in G} a_2(\tau, \sigma)}$$

**Bemerkung 2.74.** Es gilt  $\sum_{\tau \in G} a_2(\tau, \sigma) \in A^G$  (leichte Übung).

*Beweis.* Betrachte

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}[G] & \longrightarrow & J_G \longrightarrow 0 \\ 0 & \longrightarrow & A & \longrightarrow & \underbrace{A \otimes \mathbb{Z}[G]}_{=: A'} & \longrightarrow & \underbrace{A \otimes J_G}_{=: A''} \longrightarrow 0 \end{array}$$

Wegen  $H^2(G, A') = 0$  gibt es eine 1-Kokette  $a'_1 \in A'_1$  mit  $a_2 = \partial a'_1$ , d.h.

$$a_2(\tau, \sigma) = \tau a'_1(\sigma) - a'_1(\tau\sigma) + a'_1(\tau) \quad (2.14)$$

für alle  $\tau, \sigma \in G$ . Betrachte

$$\begin{array}{ccccccc} & & & & a'_1 & \longmapsto & a''_1 \\ 0 & \longrightarrow & A_1 & \longrightarrow & A'_1 & \longrightarrow & A''_1 \longrightarrow 0 \\ & & \downarrow \partial & & \downarrow \partial & & \downarrow \partial \\ 0 & \longrightarrow & A_2 & \longrightarrow & A'_2 & \longrightarrow & A''_2 \longrightarrow 0 \end{array}$$

Dann ist  $a'_1$  ein 1-Kozyklus, da  $a_2$  eine 2-Kokette mit Werten in  $A$  ist. Es gilt  $\delta \bar{a}''_1 = \bar{a}_2$  und man berechnet

$$\begin{aligned} \bar{a}_2 \cup \bar{\sigma} &= \delta \bar{a}''_1 \cup \bar{\sigma} = \delta(\bar{a}''_1 \cup \bar{\sigma}) \\ &\stackrel{2.71}{=} \overline{\delta(a''_1(\sigma))} = \overline{\partial(a'_1(\sigma))} \\ &= \overline{\sum_{\tau \in G} \tau a_1(\sigma)} \stackrel{(2.14)}{=} \overline{\sum_{\tau \in G} a_2(\tau, \sigma) + a'_1(\tau\sigma) - a'_1(\tau)} \\ &= \overline{\sum_{\tau \in G} a_2(\tau, \sigma)} \end{aligned}$$

□

## 2.7 Kohomologie zyklischer Gruppen

**Satz 2.75.** Sei  $G = \langle \sigma \rangle$  eine endliche zyklische Gruppe und  $A$  ein  $G$ -Modul. Dann gilt

$$H^q(G, A) \cong H^{q+2}(G, A)$$

für alle  $q \in \mathbb{Z}$ .

*Beweis.* Wir werden zeigen  $H^{-1}(G, A) \cong H^1(G, A)$ . Der allgemeine Fall folgt mittels Dimensionsverschiebung:

$$H^q(G, A) \cong H^{-1}(G, A^{q+1}) \cong H^1(G, A^{q+1}) \cong H^{q+2}(G, A)$$

Wir wollen zunächst eine Abbildung

$$Z_1(G, A)/B_1(G, A) \longrightarrow N_G A/I_G A$$

definieren. Hierzu sei  $x \in Z_1(G, A)$ . Dann ist

$$\begin{aligned} x(\sigma^k) &= \sigma x(\sigma^{k-1}) + x(\sigma) \\ &= \sigma(\sigma x(\sigma^{k-2}) + x(\sigma)) + x(\sigma) = \cdots \\ &= \sum_{i=0}^{k-1} \sigma^i x(\sigma) \end{aligned}$$

Es folgt mit  $n = |G|$ :

$$N_G x(\sigma) = \sum_{i=0}^{n-1} \sigma^i x(\sigma) = x(\sigma^n) = x(1) = 0,$$

d.h.  $x(\sigma) \in N_G A$ . Wir haben also

$$\begin{aligned} Z_1(G, A) &\longrightarrow N_G A \\ x &\longmapsto x(\sigma) \end{aligned} \tag{2.15}$$

Umgekehrt sei  $a \in N_G A$ . Dann wird durch  $x(\sigma) := a$  ein 1-Kozyklus definiert vermöge

$$x(\sigma^k) := \sum_{i=0}^{k-1} \sigma^i x(\sigma) = \sum_{i=0}^{k-1} \sigma^i a,$$

da die einzige Relation durch

$$0 = x(\sigma^n) = \sum_{i=0}^{n-1} \sigma^i a$$

erfüllt ist. Somit ist (2.15) eine Bijektion.

Für ein  $x \in Z_1(G, A)$  gilt:

$$\begin{aligned} x \in B_1(G, A) &\iff \exists a \in A : x(\sigma^k) = \sigma^k a - a \\ &\iff \exists a \in A : x(\sigma) = \sigma a - a \\ &\iff x(\sigma) \in I_G A = (\sigma - 1)A \end{aligned}$$

(Übung:  $I_G = (\sigma - 1)\mathbb{Z}[G]$ ).

□

**Bemerkung 2.76.** Sei  $G = \langle \sigma \rangle$  zyklisch mit der Ordnung  $n$ . Sei

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

eine exakte Sequenz von  $G$ -Moduln. Dann wird aus der langen exakten Kohomologiesequenz ein exaktes Hexagon

$$\begin{array}{ccccc}
 H^2(G, A) & \xrightarrow{\cong} & H^0(G, A) & \longrightarrow & H^0(G, B) \\
 \uparrow & \nearrow & \uparrow & & \searrow \\
 H^1(G, C) & \xrightarrow{\cong} & H^{-1}(G, C) & & H^0(G, C) \\
 & \nwarrow & & & \swarrow \\
 & & H^1(G, B) & \longleftarrow & H^1(G, A)
 \end{array}$$

**Übung 2.77.** Zeige die Exaktheit bei  $H^0(G, A)$ .

### Der Herbrandquotient

**Definition 2.78.** Sei  $G$  zyklisch und  $H^0(G, A)$  und  $H^1(G, A)$  seien endlich. Dann nennt man

$$h(A) := \frac{|H^0(G, A)|}{|H^1(G, A)|}$$

den *Herbrandquotienten* von  $A$ .

**Satz 2.79.** Sei

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

exakt und  $G$  zyklisch. Sei der Herbrandquotient für zwei der Moduln definiert. Dann ist der Herbrandquotient auch für den dritten definiert und es gilt

$$h(B) = h(A) \cdot h(C).$$

*Beweis.* Die Aussage folgt aus

$$\frac{h_0(A) \cdot h_0(C) \cdot h_1(B)}{h_0(B) \cdot h_1(A) \cdot h_1(C)} = 1,$$

was wiederum aus der Exaktheit des Hexagon folgt. □

**Satz 2.80.** Sei  $|A| < \infty$ . Dann gilt  $h(A) = 1$ .

*Beweis.* Die Sequenz

$$\begin{array}{ccccccc}
 0 & \longrightarrow & A^G & \longrightarrow & A & \xrightarrow{\sigma-1} & A & \longrightarrow & A/I_G A & \longrightarrow & 0 \\
 & & & & & & a & \longmapsto & \sigma a - a & & 
 \end{array}$$

ist exakt. Also folgt  $|A^G| = |A/I_G A|$ . Aus

$$\begin{array}{ccccccc}
 0 & \longrightarrow & H^{-1}(G, A) & \longrightarrow & A/I_G A & \xrightarrow{N_G} & A^G & \longrightarrow & H^0(G, A) & \longrightarrow & 0 \\
 & & & & & & a + I_G A & \longmapsto & N_G a & & 
 \end{array}$$

folgt nun  $|H^1(G, A)| = |H^{-1}(G, A)| = |H^0(G, A)|$ . □

**Korollar 2.81.** Sei  $f : A \rightarrow B$  ein  $G$ -Modulhomomorphismus mit endlichem Kern und Kokern. Dann gilt:

(1) Falls  $h(A)$  definiert ist, so auch  $h(B)$  und umgekehrt.

(2) Es gilt dann  $h(A) = h(B)$ .

*Beweis.* Betrachte die exakte Sequenz

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \ker(f) & \longrightarrow & A & \xrightarrow{f} & B & \longrightarrow & \operatorname{coker}(f) & \longrightarrow & 0 \\
 & & & & & \searrow f & & \nearrow & & & \\
 & & & & & & W & & & & 
 \end{array}$$

mit  $W = \operatorname{im}(f)$ . Wir betrachten den Fall in dem  $h(A)$  definiert ist. Da der Kern von  $f$  endlich ist, ist auch  $h(W)$  definiert. Dann ist aber auch  $h(B)$  definiert. Es gilt

$$h(A) = h(\ker(f))h(W) = h(W) = h(W)h(\operatorname{coker}(f)) = h(B).$$

Der andere Fall geht genauso. □

### Der Herbrandquotient für Gruppen von Primzahlordnung

Sei  $|G| = p$  für eine Primzahl  $p$ .

**Definition 2.82.** Sei  $A$  eine abelsche Gruppe. Dann setzt man

$$\varphi(A) := \frac{|A/pA|}{|\ker(A \xrightarrow{p} A)|},$$

falls Zähler und Nenner endlich sind.

**Bemerkung 2.83.** Falls  $A$  eine endlich erzeugte abelsche Gruppe ist, so sind sowohl  $h(A)$  als auch  $\varphi(A)$  definiert.

*Beweis.* Da  $A$  endlich erzeugt ist, gilt

$$A \cong A_{\operatorname{tor}} \oplus \mathbb{Z}^r$$

mit  $A_{\operatorname{tor}}$  endlich und  $r \geq 0$ . □

**Definition 2.84.** Für jeden  $G$ -Modul  $A$  ist

$$A_G := A/I_G A.$$

**Bemerkung 2.85.** Die Sequenz

$$0 \longrightarrow H^{-1}(G, A) \longrightarrow A_G \xrightarrow{N_G} A^G \longrightarrow H^0(G, A) \longrightarrow 0$$

ist exakt.

**Satz 2.86.** Sei  $A$  ein  $G$ -Modul,  $|G| = p$ . Seien  $\text{coker}(p), \text{ker}(p)$  endlich. Dann sind auch  $\varphi(A^G), \varphi(A_G)$  und  $h(A)$  definiert und es gilt

$$h(A)^{p-1} = \frac{\varphi(A^G)^p}{\varphi(A)}.$$

*Beweis.* Siehe Blatt 9). □

**Satz 2.87** (Chevalley). Sei  $|G| = p$  und  $A$  ein endlich erzeugter  $G$ -Modul. Seien  $\alpha$  und  $\beta$  die Ränge von  $A$  und  $A^G$ , d.h.  $A \cong A_{\text{tor}} \oplus \mathbb{Z}^\alpha$  und  $A^G \cong (A^G)_{\text{tor}} \oplus \mathbb{Z}^\beta$ . Dann gilt

$$h(A) = p^{(p\beta - \alpha)/(p-1)}$$

*Beweis.* Betrachte

$$0 \longrightarrow A_{\text{tor}} \longrightarrow A \longrightarrow A_{tf} \longrightarrow 0$$

mit  $A_{tf} := A/A_{\text{tor}}$ . Daraus erhalten wir die exakte Sequenz

$$0 \longrightarrow (A_{\text{tor}})^G \longrightarrow A^G \longrightarrow (A_{tf})^G \longrightarrow H^1(G, A_{\text{tor}}).$$

Damit folgt  $\text{rg}(A^G) = \text{rg}((A_{tf})^G)$  und ferner gilt

$$h(A) = h(A_{\text{tor}} \cdot) h(A_{tf}) = h(A_{tf}).$$

Es folgt

$$h(A)^{p-1} = h(A_{tf})^{p-1} \stackrel{2.86}{=} \frac{\varphi((A_{tf})^G)^p}{\varphi(A_{tf})}.$$

Nach Definition erhalten wir

$$\varphi(A_{tf}) = \frac{|A_{tf}/pA_{tf}|}{|\ker(A_{tf} \xrightarrow{p} A_{tf})|} = |A_{tf}/pA_{tf}| = p^\alpha$$

und analog  $\varphi((A_{tf})^G) = p^\beta$ . □

## 2.8 Der Satz von Tate

**Satz 2.88.** Sei  $G$  eine endliche Gruppe und  $A$  ein  $G$ -Modul. Dann sind äquivalent:

- (1)  $A$  ist kohomologisch trivial.
- (2) Es gibt ein  $q_0 \in \mathbb{Z}$ , sodass für alle  $U \leq G$  gilt

$$H^{q_0}(U, A) = 0 = H^{q_0+1}(U, A).$$

*Beweis.* Die Richtung (1)  $\implies$  (2) ist offensichtlich. Für (2)  $\implies$  (1) genügt es zu zeigen:

$$H^{q_0}(U, A) = 0 = H^{q_0+1}(U, A) \implies H^{q_0-1}(U, A) = 0 = H^{q_0+2}(U, A)$$

für alle  $U \leq G$ . Mittels Dimensionsverschiebung reicht es den Fall  $q_0 = 1$  zu betrachten, denn:

$$\left. \begin{array}{l} 0 = H^{q_0}(U, A) \cong H^1(U, A^{q_0-1}) \\ 0 = H^{q_0+1}(U, A) \cong H^2(U, A^{q_0-1}) \end{array} \right\} \implies \left\{ \begin{array}{l} 0 = H^0(U, A^{q_0-1}) \cong H^{q_0-1}(U, A) \\ 0 = H^3(U, A^{q_0-1}) \cong H^{q_0+2}(U, A) \end{array} \right.$$

Sei also ohne Einschränkung

$$H^1(U, A) = 0 = H^2(U, A)$$

für alle Untergruppen  $U \leq G$ . Es ist zu zeigen

$$H^0(U, A) = 0 = H^3(U, A)$$

für alle  $U \leq G$ . Hierfür benutzen wir Induktion über  $|G|$ :

Induktionsanfang: Für  $|G| = 1$  ist die Aussage klar.

Induktionsschritt: Aus der Induktionsannahme folgt  $H^0(U, A) = 0 = H^3(U, A)$  für alle echten Untergruppen  $U \leq G$ .

Es bleibt also zu zeigen:  $H^0(G, A) = 0 = H^3(G, A)$ .

1. Fall  $G$  ist keine  $p$ -Gruppe:

Dann sind alle  $p$ -Sylowuntergruppen *echte* Untergruppen. Die Behauptung folgt dann aus

$$H^q(G, A)_p \xrightarrow{\text{Res}} H^q(G_p, A) = 0$$

für  $q = 0, 3$  und  $H^q(G, A) = \bigoplus_p H^q(G, A)_p$ .

2. Fall  $G$  ist eine  $p$ -Gruppe:

Jede  $p$ -Gruppe ist auflösbar, d.h. es gibt einen Normalteiler  $H \trianglelefteq G$  mit  $|G/H| = p$ . Nach Induktionsvoraussetzung gilt

$$H^0(H, A) = H^3(H, A) = 0$$

und nach Grundannahme

$$H^1(H, A) = H^2(H, A) = 0.$$

Aus der Inflations-Restriktions-Sequenz erhalten wir

$$H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A)$$

für  $q = 1, 2, 3$  (beachte für  $q = 2$  bzw.  $q = 3$ , dass  $H^1(H, A) = 0$  bzw.  $H^1(H, A) = H^2(H, A) = 0$ ).

Jetzt folgt

$$H^1(G, A) = 0 \implies H^1(G/H, A^H) = 0.$$

Da  $G/H$  zyklisch ist, folgt  $H^3(G/H, A^H) = 0$  und somit  $H^3(G, A) = 0$ .

Ferner folgt aus  $H^2(G, A) = 0$ , dass  $H^2(G/H, A^H) = 0$  ist und somit  $H^0(G/H, A^H) = 0$ . D.h.

$$A^G = (A^H)^{G/H} = N_{G/H}A^H = N_{G/H}(N_H A) = N_G A$$

und es folgt  $H^0(G, A) = 0$ .

□

Seien  $A, B$  zwei  $G$ -Moduln und  $a \in H^p(G, A)$ . Dann liefert

$$a \cup \_ : H^q(G, B) \longrightarrow H^{p+q}(G, A \otimes B)$$

für alle  $q \in \mathbb{Z}$  Gruppenhomomorphismen.

**Satz 2.89.** *Sei  $A$  ein  $G$ -Modul mit folgender Eigenschaft. Für alle Untergruppen  $U \leq G$  ist*

$$(1) \ H^{-1}(U, A) = 0,$$

$$(2) \ H^0(U, A) \text{ ist zyklisch von der Ordnung } |U|.$$

Sei  $a \in H^0(G, A)$  ein Erzeuger. Dann ist

$$a \cup \_ : H^q(G, \mathbb{Z}) \longrightarrow H^q(G, A)$$

ein Isomorphismus für alle  $q \in \mathbb{Z}$ .

*Beweis.* Sei  $B := A \oplus \mathbb{Z}[G]$ . Sei

$$\begin{aligned} i : A &\longrightarrow B \\ a &\longmapsto (a, 0) \end{aligned}$$

Dann ist

$$\bar{i} : H^q(U, A) \longrightarrow H^q(U, B) = H^q(U, A) \oplus \underbrace{H^q(U, \mathbb{Z}[G])}_{=0}$$

ein Isomorphismus für alle  $U \leq G$  und alle  $q \in \mathbb{Z}$ .

Sei  $a = a_0 + N_G A$  mit  $a_0 \in A^G$ . Betrachte den  $G$ -Modulhomomorphismus

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow B = A \oplus \mathbb{Z}[G] \\ 1 &\longmapsto (a_0, N_G) \end{aligned}$$

$f$  ist offensichtlich injektiv. Sei  $\bar{f} : H^q(U, \mathbb{Z}) \rightarrow H^q(U, B)$ . Dann kommutiert

$$\begin{array}{ccc} H^q(U, \mathbb{Z}) & \xrightarrow{a \cup -} & H^q(U, A) \\ & \searrow \bar{f} & \downarrow \bar{i} \\ & & H^q(U, B) \end{array}$$

denn: Sei

$$\begin{aligned} b_q &: G \times \cdots \times G \rightarrow \mathbb{Z} \\ \sigma = (\sigma_1, \dots, \sigma_q) &\mapsto b_q(\sigma) \end{aligned}$$

ein  $q$ -Kozyklus. Es gilt

$$\begin{array}{ccc} H^q(U, \mathbb{Z}) \ni \bar{b}_q & \xrightarrow{a \cup -} & \overline{a_0 \otimes b_q} \in H^q(U, A) \\ & \searrow & \downarrow \bar{i} \\ & & \overline{(\sigma \mapsto (b_q(\sigma)a_0, b_q(\sigma)N_G))} = \overline{(\sigma \mapsto (b_q(\sigma)a_0, 0))} \end{array}$$

Es ist noch zu zeigen, dass  $\bar{f}$  ein Isomorphismus ist. Betrachte dazu

$$0 \rightarrow \mathbb{Z} \xrightarrow{f} B \rightarrow C \rightarrow 0, \quad (2.16)$$

mit  $C = \text{coker}(f)$ . Dann folgt

$$0 \rightarrow H^{-1}(U, C) \rightarrow H^0(U, \mathbb{Z}) \xrightarrow{\bar{f}} H^0(U, B) \rightarrow H^0(U, C) \rightarrow 0,$$

da  $H^1(U, \mathbb{Z}) = \text{Hom}_{\mathbb{Z}}(U, \mathbb{Z}) = 0$ .

**Behauptung** (Beweis am Ende).  $\bar{f}$  ist ein Isomorphismus für alle  $U \leq G$ .

Aus der Behauptung folgt, dass  $H^{-1}(U, C) = H^0(U, C) = 0$  für alle  $U \leq G$ . Somit ist nach Satz 2.88  $C$  kohomologisch trivial. Damit folgt  $\bar{f}$  ist ein Isomorphismus für alle  $q \in \mathbb{Z}$  und alle  $U \leq G$ , wegen der langen exakten Kohomologiesequenz zu (2.16).

*Beweis der Behauptung.* Betrachte

$$\begin{array}{ccccc} H^0(G, A) & \xrightarrow{\text{Res}} & H^0(U, A) & \xrightarrow{\text{Kor}} & H^0(G, A) \\ & & \searrow & \nearrow & \\ & & & & |G/U| \cdot \text{id} \end{array}$$

Sei  $m := \text{ord}(\text{Res}_U^G(a))$  ( $\text{Res}_U^G(a) \in H^0(U, A)$ ). Dann gilt

$$0 = \text{Kor}(\text{Res}(ma)) = m \cdot \frac{|G|}{|U|} a.$$

Es folgt  $|U|$  teilt  $m$  und  $\text{Res}_U^G(a)$  ist somit ein Erzeuger von  $H^0(U, A)$ .

Wegen  $\bar{f}(1 + |U|\mathbb{Z}) = a_0 + N_U A = \text{Res}_U^G(a)$  ist  $\bar{f} : H^0(U, \mathbb{Z}) \rightarrow H^0(U, B)$  surjektiv. Wegen

$$|H^0(U, \mathbb{Z})| = |U| = |H^0(U, A)| = |H^0(U, B)|$$

ist  $\bar{f}$  ein Isomorphismus. □



Somit ist der Beweis von Satz 2.89 vollständig.  $\square$

**Satz 2.90** (Satz von Tate). *Sei  $A$  ein  $G$ -Modul mit der folgenden Eigenschaft. Für alle Untergruppen  $U \leq G$  ist*

$$(1) H^1(U, A) = 0,$$

$$(2) H^2(U, A) \text{ ist zyklisch von der Ordnung } |U|.$$

*Dann ist für jeden Erzeuger  $a$  von  $H^2(G, A)$  die Abbildung*

$$a \cup \_ : H^q(G, \mathbb{Z}) \longrightarrow H^{q+2}(G, A)$$

*ein Isomorphismus.*

Zusatz:  $\text{Res}_U^G(a)$  erzeugt  $H^2(U, A)$  für alle Untergruppen  $U \leq G$  und man erhält Isomorphismen

$$\text{Res}_U^G(a) \cup \_ : H^q(U, \mathbb{Z}) \longrightarrow H^{q+2}(U, A).$$

*Beweis.* Betrachte  $\delta : H^q(U, A^2) \longrightarrow H^{q+2}(U, A)$ . Dann folgt  $H^{-1}(U, A^2) = 0$  und  $H^0(U, A^2)$  ist zyklisch von der Ordnung  $|U|$ . Das Diagramm

$$\begin{array}{ccc} H^q(U, \mathbb{Z}) & \xrightarrow{\delta^{-1}a \cup \_} & H^q(U, A^2) \\ \downarrow \text{id} & & \downarrow \delta \\ H^q(U, \mathbb{Z}) & \xrightarrow{a \cup \_} & H^{q+2}(U, A) \end{array}$$

kommutiert wegen  $\delta(\delta^{-1}a \cup x) = \delta(\delta^{-1}a) \cup x$ . Nach Satz 2.89 ist  $\delta^{-1}a \cup \_$  ein Isomorphismus und somit folgt die Behauptung.

Der Zusatz folgt aus  $\text{Kor} \circ \text{Res} = |G/U| \cdot \text{id}$ .

$\square$

### 3 Lokale Klassenkörpertheorie

#### 3.1 Abstrakte Klassenkörpertheorie

##### Einschub: Unendliche Galoistheorie

Literatur: [NS11, Kapitel IV, §1]

Sei  $k$  ein Körper und  $\bar{k}$  der separable Abschluss. Sei  $G_k := \text{Gal}(\bar{k}|k)$  die absolute Galoisgruppe.

**Definition 3.1.** Sei  $\Omega/k$  eine Galoiserweiterung mit Galoisgruppe  $G$ . Dann wird für jedes  $\sigma \in G$  durch die Nebenklassen

$$\sigma \text{Gal}(\Omega|K)$$

für endliche, galoissche Erweiterungen  $K/k$  eine Umgebungsbasis von  $\sigma$  definiert. Die so erzeugte Topologie auf  $G$  heißt *Krulltopologie*.

Die Situation wird in folgendem Bild veranschaulicht:

$$G \left( \begin{array}{c} \Omega \\ \left| \right. \\ \left| \right. \\ K \\ \left| \right. \\ \left| \right. \\ k \end{array} \right) \begin{array}{l} \text{Gal}(\Omega|K) \\ < \infty, \text{ gal.} \end{array}$$

**Bemerkung 3.2.** Eine Teilmenge  $U \subseteq G$  ist offen, wenn es zu jedem  $\sigma \in U$  eine endliche Galoiserweiterung  $K/k$  gibt mit  $\sigma \text{Gal}(\Omega|K) \subseteq U$ .

**Satz 3.3.** Für jede Galoiserweiterung  $\Omega/k$  ist  $G = \text{Gal}(\Omega|k)$  hausdorffsch und kompakt.

*Beweisskizze.* Zu „hausdorffsch“:

Sei  $\sigma \neq \tau$ ,  $\sigma, \tau \in G$ . Dann gibt es eine endliche Galoiserweiterung  $K/k$  mit  $\sigma|_K \neq \tau|_K$ . Dies gilt genau dann, wenn  $\sigma \text{Gal}(\Omega|K) \neq \tau \text{Gal}(\Omega|K)$  und ist somit äquivalent zu

$$\sigma \text{Gal}(\Omega|K) \cap \tau \text{Gal}(\Omega|K) = \emptyset.$$

Zu „kompakt“:

Betrachte

$$h : G \longrightarrow \prod_{\substack{K/k \\ \text{endl., gal.}}} \text{Gal}(K|k)$$

$$\sigma \longmapsto (\sigma|_K)_K$$

Es gilt:

- $h$  ist injektiv,
- $h$  ist ein Homöomorphismus auf  $h(G)$ ,
- $h(G) \subseteq \prod_K \text{Gal}(K|k)$  ist abgeschlossen, wobei jede der endlichen Gruppen  $\text{Gal}(K|k)$  mit der diskreten Topologie versehen wird und das Produkt die Produkttopologie trägt.
- $\prod_K \text{Gal}(K|k)$  ist kompakt nach dem Satz von Tychonoff.

Damit folgt  $h(G) \cong G$  ist kompakt. □

**Bemerkung 3.4.** Es ist

$$h(G) = \varprojlim_{\substack{K/k \\ \text{endl., gal.}}} \text{Gal}(K|k)$$

mit Elementen der Form

$$\left\{ (\sigma_K)_K \in \prod_K \text{Gal}(K|k) \mid \sigma_L|_K = \sigma_K \text{ für alle } L/K/k \right\}.$$

Explizit: Für  $\alpha \in \Omega$ ,  $\sigma \in G$  ist  $\sigma(\alpha) = \sigma_K(\alpha)$  für eine endliche Galoiserweiterung  $K/k$ , sodass  $\alpha \in K$ .

**Beispiele 3.5.** (1) Sei  $k = \mathbb{F}_q$  und  $\Omega = \bar{k}$ . Betrachte

$$\begin{array}{c} N \\ \left| \right. \\ K \\ \left. \left| \right. \right)_m \\ n \left( \left| \right. \right) \\ k \end{array}$$

mit  $n|m$ . Dann gilt

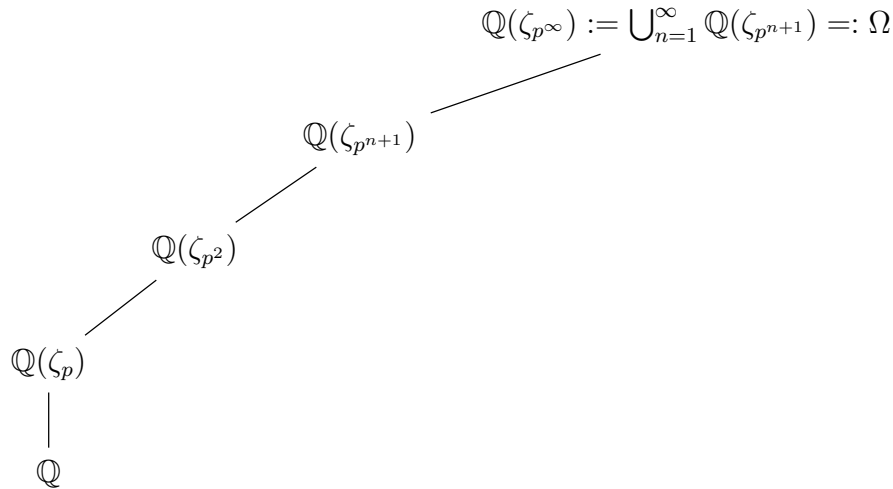
$$\begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \cong \text{Gal}(N|k) & \xrightarrow{\text{res}} & \text{Gal}(K|k) \cong \mathbb{Z}/n\mathbb{Z} \\ & & \varphi \longmapsto \varphi \end{array}$$

wobei  $\varphi$  den Frobenius bezeichnet. Dann gilt

$$\text{Gal}(\bar{k}|k) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}}.$$

$\widehat{\mathbb{Z}}$  wird als der *Prüferring* bezeichnet.

(2) Sei  $k = \mathbb{Q}(\zeta_p)$  für eine Primzahl  $p \neq 2$ . Betrachte



Dann gilt

$$\varprojlim_n \underbrace{\text{Gal}(\mathbb{Q}(\zeta_{p^{n+1}}) | \mathbb{Q}(\zeta_p))}_{\cong \frac{1+p\mathbb{Z}}{1+p^{n+1}\mathbb{Z}} \hookrightarrow (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times} = \varprojlim_n \frac{1+p\mathbb{Z}}{1+p^{n+1}\mathbb{Z}} \stackrel{\log_p}{\cong} \varprojlim_n \frac{p\mathbb{Z}}{p^{n+1}\mathbb{Z}} \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

**Satz 3.6** (Hauptsatz der Galoistheorie). Sei  $\Omega/k$  eine Galoiserweiterung. Dann ist die Zuordnung  $K \mapsto \text{Gal}(\Omega|K)$  eine 1 : 1-Korrespondenz zwischen den Teilerweiterungen  $K/k$  von  $\Omega/k$  und den abgeschlossenen Untergruppen von  $\text{Gal}(\Omega|k)$ . Die offenen Untergruppen entsprechen den endlichen Erweiterungen  $K/k$ .

**Bemerkung 3.7.** Für jede topologische Gruppe  $G$  gilt:

- (1) Ist  $U \leq G$  offen, so ist  $U$  auch abgeschlossen.
- (2) Ist  $U \leq G$  abgeschlossen und von endlichem Index, so ist  $U$  auch offen.
- (3) Falls  $G$  kompakt ist und  $U \leq G$ , so gilt

$$U \text{ offen} \iff U \text{ abgeschlossen und } (G : U) < \infty.$$

*Beweis.* Siehe Blatt 10, Aufgabe 1. □

## 3.2 Abstrakte Galoistheorie

**Definition 3.8.** Eine topologische Gruppe  $G$  heißt pro-endlich, falls gilt:

- (1)  $G$  ist hausdorffsch und kompakt.
- (2) Die Identität hat eine Umgebungsbasis bestehend aus offenen Normalteilern.

**Beispiel 3.9** (Standardbeispiel).  $G = \text{Gal}(\Omega|k)$ .

**Sprechweisen.** •  $\{G_K | K \in X\}$  sei die Menge der offenen Untergruppen von  $G$ .

- Die Elemente  $K \in X$  nennen wir *Körper*.
- Das Element  $K_0$  mit  $G_{K_0} = G$  heißt *Grundkörper*.
- Falls  $G_K \supseteq G_L$ , so schreibt man  $L/K$  und wir definieren  $[L : K] := (G_K : G_L)$ .
- $L/K$  ist *normal*, falls  $G_L \trianglelefteq G_K$ . Man setzt dann  $G_{L/K} = G_K/G_L$ .
- Man setzt

$$K = \bigcap_{i=1}^n K_i \iff G_K = \overline{\langle G_{K_i} : i = 1, \dots, n \rangle},$$

$$K = \prod_{i=1}^n K_i \iff G_K = \bigcap_{i=1}^n G_{K_i}.$$

- Falls  $G_{L'} = \sigma G_L \sigma^{-1}$  für ein  $\sigma \in G$ , so schreibt man  $L' = \sigma L$ .  $L$  und  $L'$  heißen *konjugiert*.

Sei  $G$  eine pro-endliche Gruppe und  $A$  ein  $G$ -Modul.

**Beispiel 3.10.** Sei  $\Omega/k$  eine Galoiserweiterung,  $G = \text{Gal}(\Omega|k)$  und  $A = \Omega^\times$ .

**Lemma 3.11.** *Folgende Aussagen sind äquivalent:*

- (1)  $G \times A \rightarrow A$  ist stetig, wobei  $A$  mit der diskreten Topologie versehen ist.
- (2) Für jedes  $a \in A$  ist

$$G_a := \{\sigma \in G \mid \sigma(a) = a\}$$

eine offene Untergruppe von  $G$ .

- (3)  $A = \bigcup_U A^U$ , wobei  $U$  die Menge der offenen Untergruppen durchläuft.

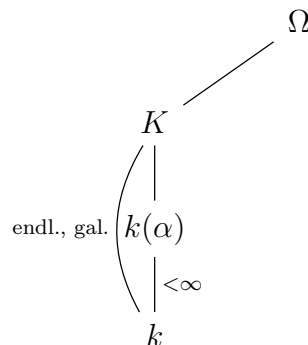
*Beweis.* Siehe Blatt 10, Aufgabe 2. □

**Bemerkung 3.12.** Ein  $G$ -Modul  $A$ , der die obigen Bedingungen erfüllt heißt *stetiger  $G$ -Modul*.

**Definition 3.13.** Sei  $A$  ein stetiger  $G$ -Modul, dann nennt man  $(G, A)$  eine *Formation*.

**Beispiel 3.14.** Sei  $G = \text{Gal}(\Omega|k)$ . Dann ist  $(G, \Omega^\times)$  eine Formation.

*Beweis.* Sei  $\alpha \in \Omega^\times$ . Betrachte



Dann gilt

$$G_\alpha = \text{Gal}(\Omega|k(\alpha)) = \bigcup_{\sigma \in \text{Gal}(\Omega|k(\alpha))/\text{Gal}(\Omega|K)} \sigma \text{Gal}(\Omega|K)$$

ist offen. □

**Definition 3.15.** Sei  $(G, A)$  eine Formation und  $K \in X$ . Dann setzt man

$$A_K := A^{G_K}.$$

Im Standardbeispiel:  $A_K = K^\times$ .

**Bemerkungen 3.16.** Sei  $(G, A)$  eine Formation.

- (1)  $L/K \iff G_L \leq G_K$  impliziert  $A_K \subseteq A_L$ .
- (2) Ist  $L/K$  normal ( $\iff G_L \trianglelefteq G_K$ ), so ist  $A_L = A^{G_L}$  ein  $G_K/G_L = G_{L/K}$ -Modul.

Im Standardbeispiel:

$$\begin{array}{c} \Omega \\ \left. \begin{array}{c} | \\ L \\ | \\ K \end{array} \right) \begin{array}{l} G_L \\ \\ G_K \end{array} \\ \text{gal.} \\ \left. \begin{array}{c} | \\ K \\ | \\ k \end{array} \right) \end{array}$$

$G_{L/K} = G_K/G_L$  und  $A_L = L^\times$  ist ein  $G_{L/K}$ -Modul.

**Fazit.** Zu jeder normalen Erweiterung  $L/K$  haben wir einen  $G_{L/K}$ -Modul  $A_L$  und Kohomologiegruppen  $H^q(G_{L/K}, A_L)$  für alle  $q \in \mathbb{Z}$ .

**Definition 3.17.** Setze

$$H^q(L|K) = H^q(L/K, A_L) := H^q(G_{L/K}, A_L)$$

falls  $L/K$  normal ist.

Sei  $N/L/K$  und  $N/K$  und  $L/K$  seien normal. Dann hat man die Inflationsabbildung

$$\begin{array}{ccc} H^q(L|K) & \xrightarrow{\text{Inf}_N} & H^q(N|K) \\ \parallel & & \parallel \\ H^q(G_{L/K}, A_L) & \xrightarrow{\text{Inf}} & H^q(G_{N/K}, A_N) \end{array}$$

für  $q \geq 1$ , da

$$A_L = A^{G_L} = (A^{G_N})^{G_L/G_N} = A_N^{G_{N/L}}.$$

Ebenso hat man falls  $N/K$  normal ist

$$\begin{array}{ccc} H^q(N|K) & \begin{array}{c} \xrightarrow{\text{Res}_L} \\ \xleftarrow{\text{Kor}_K} \end{array} & H^q(N|L) \\ \parallel & & \parallel \\ H^q(G_{N/K}, A_N) & \begin{array}{c} \xrightarrow{\text{Res}} \\ \xleftarrow{\text{Kor}} \end{array} & H^q(G_{N/L}, A_N) \end{array}$$

eine Restriktion und eine Korestriktion.

Falls  $N/K$  und  $L/K$  normal sind, so hat man exakte Inflations-Restriktions-Sequenzen

$$1 \longrightarrow H^q(L|K) \xrightarrow{\text{Inf}_N} H^q(N|K) \xrightarrow{\text{Res}_L} H^q(N|L)$$

falls  $H^i(N|L) = 1$  für  $1 \leq i \leq q-1$ .

Im Standardbeispiel:

$$H^0(N|K) = K^\times / N_{N/K}(N^\times) \xrightarrow{\text{Res}_L} H^0(N|L) = L^\times / N_{N/L}(N^\times)$$

ist induziert von der Inklusion  $K^\times \subseteq L^\times$ .

$$L^\times / N_{N/L}(N^\times) = H^0(N|L) \xrightarrow{\text{Kor}_K} H^0(N|K) = K^\times / N_{N/K}(N^\times)$$

ist induziert von der körpertheoretischen Norm  $N_{L/K}$ .

**Definition 3.18.** Eine Formation  $(G, A)$  heißt *Körperformation*, falls für jede normale Erweiterung  $L/K$  die erste Kohomologiegruppe  $H^1(L|K) = 1$  ist.

Im Standardbeispiel:

**Satz 3.19.** Sei  $\Omega/k$  galoissch und  $A = \Omega^\times$ . Dann ist  $(\text{Gal}(\Omega|k), \Omega^\times)$  eine Körperformation.

*Beweis.*  $H^1(L|K) = H^1(\text{Gal}(L|K), L^\times) = 1$  nach Hilberts Satz 90 (siehe Blatt 8, Aufgabe 1).  $\square$

**Bemerkung 3.20.** In einer Körperformation ist

$$1 \longrightarrow H^2(L|K) \xrightarrow{\text{Inf}_N} H^2(N|K) \xrightarrow{\text{Res}_L} H^2(N|L)$$

stets exakt.

**Definition 3.21.** Definiere

$$H^2(K) = H^2(K, A) = H^2(G_K, A) := \varinjlim_L H^2(L|K),$$

wobei  $L/K$  die normalen Erweiterungen von  $K$  durchläuft. Der direkte Limes ist bzgl. der Inflation gebildet.

Anschaulich:

$$H^2(K) = \bigcup_L H^2(L|K),$$

wenn man sich die Inflation als Identität vorstellt, d.h.  $H^2(L|K) \subseteq H^2(N|K)$  bedeutet eigentlich  $\text{Inf}_N(H^2(L|K)) \subseteq H^2(N|K)$ .

**Bemerkung 3.22.** Für pro-endliche Gruppen  $G$  und stetige  $G$ -Moduln  $A$  kann man wie bei endlichen Gruppen für  $q \geq 0$  Kohomologiegruppen  $H^q(G, A)$  definieren, indem man als  $q$ -Koketten die *stetigen* Abbildungen

$$x : G \times \cdots \times G \longrightarrow A, \quad q \geq 1$$

zulässt (siehe [NSW13, Chapter I]). Es gilt dann

$$H^q(G, A) \cong \varinjlim_U H^q(G/U, A^U)$$

(siehe [NSW13, Theorem 1.5.1]), wobei  $U \trianglelefteq G$  die offenen Normalteiler durchläuft.

**Satz 3.23.** Sei  $(G, A)$  eine Körperformation und  $K'/K$  normal. Dann ist die Sequenz

$$1 \longrightarrow H^2(K'|K) \xrightarrow{\text{Inf}} H^2(K) \xrightarrow{\text{Res}} H^2(K')$$

exakt.

*Beweis.* Zu zeigen ist die Exaktheit bei  $H^2(K)$ . Sei hierfür  $c \in H^2(L|K) \subseteq H^2(K)$ . Es gelte  $\text{Res}_{K'}(c) = 0$  in  $H^2(L|K')$ . Dabei ist  $L$  groß genug, sodass  $L/K'/K$  und  $L/K$  normal ist. Aus der Inflations-Restriktions-Sequenz für  $L/K'/K$  folgt  $c \in \text{im}(\text{Inf}_L)$ .  $\square$

Ziel: Finde  $G_{L|K}^{\text{ab}} \cong A_K/N_{L/K}A_L$ . Dies liefert der Satz von Tate, wenn man an  $(G, A)$  die folgenden Bedingungen stellt:

- I.  $H^1(L|K) = 1$ ,
- II.  $H^2(L|K)$  ist zyklisch von der Ordnung  $[L : K]$ .

Dann erhalten wir den gewünschten Isomorphismus

$$a \cup - : G_{L/K}^{\text{ab}} = H^{-2}(G_{L/K}, \mathbb{Z}) \xrightarrow{\cong} H^0(G_{L/K}, A_L) = A_K/N_{L/K}A_L$$

falls  $\langle a \rangle = H^2(L|K)$ .

Ziel: Spezifiziere  $a$  eindeutig (durch eine Verschärfung von II.).

**Definition 3.24.** Eine Formation  $(G, A)$  heißt *Klassenformation*, falls

- I.  $H^1(L|K) = 1$  für alle normalen  $L/K$ .
- II. Zu jeder normalen Erweiterung  $L/K$  gibt es einen Isomorphismus, die *Invariantenabbildung*,

$$\text{inv}_{L/K} : H^2(L|K) \xrightarrow{\cong} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

mit folgenden Eigenschaften



(1) Falls  $N/L/K$  mit  $N/K$  und  $L/K$  normal, so gilt:

$$\text{inv}_{L/K} = \text{inv}_{N/K} \Big|_{H^2(L|K)}$$

bzw. das Diagramm

$$\begin{array}{ccc} H^2(L|K) & \xrightarrow{\text{inv}_{L/K}} & \frac{1}{[L:K]} \mathbb{Z}/\mathbb{Z} \\ \downarrow \text{Inf} & & \downarrow \subseteq \\ H^2(N|K) & \xrightarrow{\text{inv}_{N/K}} & \frac{1}{[N:K]} \mathbb{Z}/\mathbb{Z} \end{array}$$

kommutiert.

(2) Falls  $N/L/K$  mit  $N/K$  normal, so kommutiert das Diagramm

$$\begin{array}{ccc} H^2(N|K) & \xrightarrow{\text{inv}_{N/K}} & \frac{1}{[N:K]} \mathbb{Z}/\mathbb{Z} \\ \downarrow \text{Res}_L & & \downarrow [L:K] \\ H^2(N|L) & \xrightarrow{\text{inv}_{N/L}} & \frac{1}{[N:L]} \mathbb{Z}/\mathbb{Z} \end{array}$$

Wegen 3.24.II.(1) erhält man einen injektiven Homomorphismus

$$\begin{aligned} \text{inv}_K : H^2(K) &\hookrightarrow \mathbb{Q}/\mathbb{Z} \\ a &\longmapsto \text{inv}_{L/K}(a), \quad a \in H^2(L|K) \end{aligned}$$

**Satz 3.25.** Sei  $N/L/K$  und  $N/K$  normal. Dann gilt:

- (1)  $\text{inv}_{N/K}(c) = \text{inv}_{L/K}(c)$  falls  $L/K$  normal ist und  $c \in H^2(L|K) \subseteq H^2(N|K)$ .
- (2)  $\text{inv}_{N/L}(\text{Res}_L(c)) = [L:K] \text{inv}_{N/K}(c)$  für  $c \in H^2(N|K)$ .
- (3)  $\text{inv}_{N/K}(\text{Kor}_K(c)) = \text{inv}_{N/L}(c)$  für  $c \in H^2(N|L)$ .
- (4)  $\text{inv}_{\sigma L/\sigma K}(\sigma^*c) = \text{inv}_{L/K}(c)$  für  $c \in H^2(N|K)$ ,  $\sigma \in G$ .

**Erläuterung** (zu (4)). Betrachte

$$\begin{aligned} G_K/G_L &= G_{L/K} \xrightarrow{c_\sigma} G_{\sigma L/\sigma K} = \sigma G_K \sigma^{-1} / \sigma G_L \sigma^{-1} = G_{\sigma K}/G_{\sigma L} \\ \gamma G_L &\longmapsto \sigma \gamma \sigma^{-1} (\sigma G_L \sigma^{-1}) \end{aligned}$$

und

$$\begin{aligned} A^{G_L} &= A_L \xrightarrow{m_\sigma} A_{\sigma L} = A^{G_{\sigma L}} \\ a &\longmapsto \sigma a \end{aligned}$$

Wegen  $m_\sigma(\gamma a) = c_\sigma(\gamma)(m_\sigma(a))$  erhält man einen Isomorphismus

$$\sigma^* : H^q(L|K) \longrightarrow H^q(\sigma L|\sigma K).$$

Auf  $q$ -Koketten für  $q \geq 1$  gilt

$$\begin{array}{c} x : G_{L/K} \times \cdots \times G_{L/K} \rightarrow A_L \\ \downarrow \\ \sigma^* x := m_\sigma \circ x \circ c_\sigma^{-1} \end{array}$$

*Beweis von Satz 3.25.* (1) und (2) sind Definition.

Zu (3): Wegen 3.24.II.(2) ist

$$\text{Res}_L : H^2(N|K) \longrightarrow H^2(N|L)$$

surjektiv. Sei  $\tilde{c} \mapsto c$ . Dann folgt

$$\text{Kor}_K(c) = \text{Kor}_K(\text{Res}_L(\tilde{c})) = \tilde{c}^{[L:K]}$$

und somit

$$\text{inv}_{N/K}(\text{Kor}_K(c)) = \text{inv}_{N/K}(\tilde{c}^{[L:K]}) = [L : K] \text{inv}_{N/K}(\tilde{c}) = \text{inv}_{N/L}(c).$$

Für (4) siehe [NS11, Kapitel II, Satz (1.4)]. □

**Definition 3.26.** Das durch

$$\text{inv}_{L/K}(u_{L/K}) = \frac{1}{[L : K]} + \mathbb{Z}$$

eindeutig bestimmte Element  $u_{L/K} \in H^2(L|K)$  heißt *Fundamentalklasse*. Hierbei ist  $L/K$  stets normal.

Fast formale Konsequenzen aus Satz 3.25:

**Satz 3.27.** *Sei  $N/L/K$  und  $N/K$  normal. Dann gilt:*

(1)  $u_{L/K} = u_{N/K}^{[N:L]}$ , falls  $L/K$  normal ist.

(2)  $\text{Res}_L(u_{N/K}) = u_{N/L}$ .

(3)  $\text{Kor}_K(u_{N/L}) = u_{N/K}^{[L:K]}$ .

(4)  $\sigma^*(u_{N/K}) = u_{\sigma N/\sigma K}$  für  $\sigma \in G$ .

*Beweiskostprobe.* Zu (1): Es gilt

$$\begin{aligned} \text{inv}_{N/K} \left( u_{N/K}^{[N:L]} \right) &= [N : L] \text{inv}_{N/K}(u_{N/K}) \\ &= \frac{[N : L]}{[N : K]} + \mathbb{Z} = \frac{1}{[L : K]} + \mathbb{Z} \\ &= \text{inv}_{L/K}(u_{L/K}) \end{aligned}$$

und somit folgt  $u_{L/K} = u_{N/K}^{[N:L]}$  (beachte  $u_{L/K} \in H^2(L|K) \hookrightarrow H^2(N|K) \ni u_{N/K}$ ).

Für den Rest siehe [NS11, Kapitel II, Satz (1.6)]. □

**Satz 3.28** (Hauptsatz über Klassenformationen). *Sei  $(G, A)$  eine Klassenformation. Dann ist für jede normale Erweiterung  $L/K$  die Abbildung*

$$u_{L/K} \cup - : H^q(G_{L/K}, \mathbb{Z}) \longrightarrow H^{q+2}(G_{L/K}, A_L) = H^{q+2}(L|K)$$

für  $q \in \mathbb{Z}$  ein Isomorphismus.

*Beweis.* Die Aussage gilt nach Satz 2.90 (Satz von Tate). □

Für  $q = -2$  erhält man das *allgemeine Reziprozitätsgesetz*:

**Satz 3.29.** *Sei  $(G, A)$  eine Klassenformation. Dann liefert für jede normale Erweiterung  $L/K$  die Abbildung*

$$u_{L/K} \cup - : G_{L/K}^{\text{ab}} \cong H^{-2}(G_{L/K}, \mathbb{Z}) \longrightarrow H^0(L|K) = A_K/N_{L/K}A_L$$

einen kanonischen Isomorphismus

$$\Theta_{L/K} : G_{L/K}^{\text{ab}} \longrightarrow A_K/N_{L/K}A_L.$$

**Definition 3.30.** •  $\Theta_{L/K}$  heißt *Nakayamaabbildung*.

- Die zu  $\Theta_{L/K}$  inverse Abbildung heißt *Reziprozitätsisomorphismus*.
- Das *Normrestsymbol* ist

$$\begin{array}{ccc} (\_, L/K) : A_K & \xrightarrow{\quad} & G_{L/K}^{\text{ab}} \\ & \searrow & \nearrow \Theta_{L/K}^{-1} \\ & & A_K/N_{L/K}A_L \end{array}$$

### In der lokalen Klassenkörpertheorie

Sei  $k/\mathbb{Q}_p$  eine endliche Erweiterung und  $G = G_k = \text{Gal}(\bar{k}|k)$ . Dann ist  $(G, \bar{k}^\times)$  eine Klassenformation (siehe [NS11, Kapitel II, Satz (5.6)]).

### Im Globalen

Sei  $k$  ein Zahlkörper und  $G = G_k = \text{Gal}(\bar{k}|k)$ . Dann ist  $(G, \mathcal{C}_{\bar{k}})$  eine Klassenformation (siehe [NS11, Kapitel III, Satz (6.9)]). Hierbei ist

$$\mathcal{C}_{\bar{k}} := \varinjlim_L \mathcal{C}_L$$

mit  $\mathcal{C}_L = \mathcal{J}_{L/L^\times}$ . Für endliche Körpererweiterungen  $L'/L/k$  ist dabei  $\mathcal{C}_L \longrightarrow \mathcal{C}_{L'}$  induziert von

$$\begin{aligned} \mathcal{J}_L &\longrightarrow \mathcal{J}_{L'} \\ \alpha = (\alpha_v)_v &\longmapsto \beta = (\beta_w)_w \end{aligned}$$

mit  $\beta_w = \alpha_v$  für  $w|v$ .

**Übung 3.31.** Diese Abbildung ist eine Inklusion  $\mathcal{C}_L \hookrightarrow \mathcal{C}_{L'}$ .

**Bemerkung 3.32.** Die Sequenz

$$0 \longrightarrow N_{L/K}A_L \longrightarrow A_K \xrightarrow{(-, L/K)} G_{L/K}^{\text{ab}} \longrightarrow 0$$

ist exakt, d.h.

$$(a, L/K) = 1 \iff a \in N_{L/K}A_L.$$

**Satz 3.33** (ohne Beweis). Sei  $N/L/K$  und  $N/K$  normal. Dann sind folgende Diagramme kommutativ:

(1) Falls zusätzlich  $L/K$  normal ist:

$$\begin{array}{ccc} A_K & \xrightarrow{(-, N/K)} & G_{N/K}^{\text{ab}} \\ \parallel & & \downarrow \pi \\ A_K & \xrightarrow{(-, L/K)} & G_{L/K}^{\text{ab}} \end{array}$$

wobei

$$\begin{aligned} \pi : G_{N/K}/G'_{N/K} = G_{N/K}^{\text{ab}} &\longrightarrow G_{L/K}^{\text{ab}} = \frac{(G_{N/K}/G_{N/L})}{(G_{N/K}/G_{N/L})'} \\ \tau G'_{N/K} &\longmapsto (\tau G_{N/L})(G_{N/K}/G_{N/L})' \end{aligned}$$

(2)

$$\begin{array}{ccc} A_K & \xrightarrow{(-, N/K)} & G_{N/K}^{\text{ab}} \\ \downarrow \subseteq & & \downarrow \text{Ver} \\ A_L & \xrightarrow{(-, N/L)} & G_{N/L}^{\text{ab}} \end{array}$$

Hierbei ist Ver induziert von

$$H^{-2}(G_{N/K}, \mathbb{Z}) \xrightarrow{\text{Res}} H^{-2}(G_{N/L}, \mathbb{Z}).$$

**Bemerkung.** Ver hat auch eine rein gruppentheoretische Definition, siehe [Neu06, Kapitel IV, §5] und [Ser13].

(3)

$$\begin{array}{ccc} A_L & \xrightarrow{(-, N/L)} & G_{N/L}^{\text{ab}} \\ \downarrow N_{L/K} & & \downarrow \kappa \\ A_K & \xrightarrow{(-, N/K)} & G_{N/K}^{\text{ab}} \end{array}$$

wobei

$$\begin{aligned} \kappa : G_{N/L}/G'_{N/L} = G_{N/L}^{\text{ab}} &\longrightarrow G_{N/K}^{\text{ab}} = G_{N/K}/G'_{N/K} \\ \tau G'_{N/L} &\longmapsto \tau G'_{N/K} \end{aligned}$$

(4)

$$\begin{array}{ccc} A_K & \xrightarrow{(-, N/K)} & G_{N/K}^{\text{ab}} \\ \downarrow \sigma & & \downarrow \sigma^* \\ A_{\sigma K} & \xrightarrow{(-, \sigma N/\sigma K)} & G_{\sigma N/\sigma K}^{\text{ab}} \end{array}$$

Hierbei ist  $\sigma^*$  induziert durch die Konjugation

$$\tau \longmapsto \sigma \tau \sigma^{-1}.$$

**Beispiel 3.34.** Sei  $k/\mathbb{Q}_p$  endlich,  $\bar{k}$  der algebraische Abschluss von  $k$  und  $G_k = \text{Gal}(\bar{k}|k)$ . Dann folgt mit Hilberts Satz 90, dass  $(G_k, \bar{k}^\times)$  eine Körperformation ist.

**Bemerkung 3.35.** Falls  $L/K$  normal, so ist  $G_{L/K}^{\text{ab}} = G_{L/K}/G'_{L/K}$  die Galoisgruppe der maximal abelschen Teilerweiterung  $L^{\text{ab}}/K$  von  $L/K$ , denn für  $H \trianglelefteq G_{L/K}$  gilt:

$$G_{L/K}/H \text{ abelsch} \iff G'_{L/K} \subseteq H.$$

Das Reziprozitätsgesetz ist also ein Isomorphismus

$$G_{L^{\text{ab}}/K} \cong A_K/N_{L/K}A_L.$$

**Definition 3.36.** Eine Untergruppe  $I \leq A_K$  heißt *Normengruppe*, falls es eine normale Erweiterung  $L/K$  gibt mit  $I = N_{L/K}A_L$ .

**Satz 3.37.** Sei  $L/K$  normal und  $L^{\text{ab}}/K$  die maximal abelsche Teilerweiterung. Dann gilt:

$$N_{L/K}A_L = N_{L^{\text{ab}}/K}A_{L^{\text{ab}}}.$$

*Beweis.* Es gilt

$$N_{L/K}A_L = N_{L^{\text{ab}}/K} \underbrace{N_{L/L^{\text{ab}}}A_L}_{\subseteq A_{L^{\text{ab}}}},$$

d.h.  $N_{L/K}A_L \subseteq N_{L^{\text{ab}}/K}A_{L^{\text{ab}}} \subseteq A_K$ . Aus dem Reziprozitätsgesetz erhalten wir

$$A_K/N_{L/K}A_L \cong G_{L/K}^{\text{ab}} \cong G_{L^{\text{ab}}/K} \cong A_K/N_{L^{\text{ab}}/K}A_{L^{\text{ab}}}$$

und somit folgt Gleichheit. □

**Korollar 3.38.**  $(A_K : N_{L/K}A_L)$  teilt  $[L : K]$ . Es gilt genau dann Gleichheit, wenn  $G_{L/K}$  abelsch ist.

**Satz 3.39.** Die Zuordnung

$$L \longmapsto I_L := N_{L/K}A_L$$

ist eine inklusionsumkehrende Bijektion zwischen den abelschen Erweiterungen  $L/K$  und den Normenuntergruppen  $I$  von  $A_K$ . Es gilt:

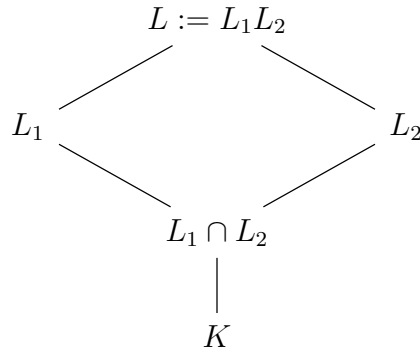
$$(1) I_{L_1} \supseteq I_{L_2} \iff L_1 \subseteq L_2,$$

$$(2) I_{L_1 L_2} = I_{L_1} \cap I_{L_2},$$

$$(3) I_{L_1} I_{L_2} = I_{L_1 \cap L_2}.$$

Falls  $N_{L/K} A_L \leq I \leq A_K$  für eine normale Erweiterung  $L/K$ , so ist auch  $I$  eine Normengruppe.

*Beweis.* Seien  $L_1$  und  $L_2$  abelsche Oberkörper von  $K$ . Die Situation wird in folgendem Bild veranschaulicht:



Wir zeigen zunächst (2). Es gilt:

$$I_L = N_{L/K} A_L = N_{L_i/K} N_{L/L_i} A_L \subseteq N_{L_i/K} A_{L_i} = I_{L_i}$$

für  $i = 1, 2$ . Somit folgt  $I_L \subseteq I_{L_1} \cap I_{L_2}$ .

Sei umgekehrt  $a \in I_{L_1} \cap I_{L_2}$ . Dann folgt aus

$$\begin{array}{ccc}
 A_K & \xrightarrow{(-, L/K)} & G_{L/K}^{\text{ab}} \\
 \parallel & & \downarrow \pi_i \\
 A_K & \xrightarrow{(-, L_i/K)} & G_{L_i/K}^{\text{ab}}
 \end{array}$$

und da  $a \in N_{L_i/K} A_{L_i}$

$$\pi_i((a, L/K)) = (a, L_i/K) = 1.$$

Somit folgt  $(a, L/K) = 1$  und daher gilt  $a \in N_{L/K} A_L = I_L$ .

Es folgt (1):

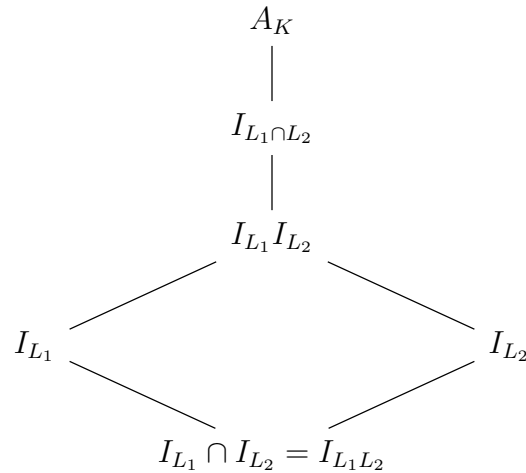
$$\begin{aligned}
 I_{L_1} \supseteq I_{L_2} &\iff I_{L_1} \cap I_{L_2} = I_{L_2} \iff I_{L_1 L_2} = I_{L_2} \\
 &\iff [L_1 L_2 : K] = [L_2 : K] \iff L_1 L_2 = L_2 \\
 &\iff L_1 \subseteq L_2.
 \end{aligned}$$

Die Surjektivität der Zuordnung  $L \mapsto I_L$  folgt aus Satz 3.37, die Injektivität aus (1).

Zu (3): Es gilt

$$L_1 \cap L_2 \subseteq L_i \xrightarrow{(1)} I_{L_i} \subseteq I_{L_1 \cap L_2} \implies I_{L_1} I_{L_2} \subseteq I_{L_1 \cap L_2}.$$

Betrachte



Dann folgt

$$\begin{aligned}
 |^{A_K/I_{L_1 L_2}}| &= [L_1 L_2 : K] = \frac{[L_1 : K][L_2 : K]}{[L_1 \cap L_2 : K]} \\
 &= \frac{|^{A_K/I_{L_1}}| |^{A_K/I_{L_2}}|}{|^{A_K/I_{L_1 \cap L_2}}|} \\
 &= \frac{|^{A_K/I_{L_1}}| |^{A_K/I_{L_1} I_{L_2}}| |^{I_{L_1} I_{L_2}/I_{L_2}}|}{|^{A_K/I_{L_1 \cap L_2}}|} \\
 &= \frac{|^{A_K/I_{L_1}}| |^{I_{L_1}/I_{L_1} \cap I_{L_2}}| |^{A_K/I_{L_1} I_{L_2}}|}{|^{A_K/I_{L_1 \cap L_2}}|} \\
 &= |^{A_K/I_{L_1} \cap I_{L_2}}| \frac{|^{A_K/I_{L_1} I_{L_2}}|}{|^{A_K/I_{L_1 \cap L_2}}|}
 \end{aligned}$$

Damit folgt  $|^{A_K/I_{L_1} I_{L_2}}| = |^{A_K/I_{L_1 \cap L_2}}|$  und wegen  $I_{L_1} I_{L_2} \subseteq I_{L_1 \cap L_2}$  folgt (3).

Sei  $N_{L/K} A_L \leq I \leq A_K$ , ohne Einschränkung sei  $L/K$  abelsch. Dann ist

$$^{A_K/N_{L/K} A_L} \geq I/N_{L/K} A_L.$$

Betrachte

$${}^{I/N_{L/K} A_L} \left( \begin{array}{c} L \\ | \\ M \\ | \\ K \end{array} \right)^{A_K/N_{L/K} A_L}$$

Dann gilt  $I = N_{M/K} A_M$  (Übung). □

Ziel: Charakterisierung der Normengruppen durch innere Eigenschaften von  $A_K$ .

**Beispiel 3.40** (lokale Klassenkörpertheorie). Sei  $K/\mathbb{Q}_p$  endlich und  $A_K = K^\times$ . Dann gilt:

$$I \leq K^\times \text{ ist Normengruppe} \iff I \text{ ist abgeschlossen von endlichem Index.}$$

Die Richtung „ $\implies$ “ ist relativ leicht. Die Richtung „ $\impliedby$ “ ist schwer, dies ist der sogenannte *Existenzsatz*.

### 3.3 Galoiskohomologie

Sei  $L/K$  eine endliche Galoiserweiterung mit Galoisgruppe  $G$ .

**Satz 3.41.**  $H^q(G, L) = 0$  für alle  $q \in \mathbb{Z}$ .

*Beweis.* Aus dem Satz von der Normalbasis folgt  $L \cong K[G]$  als  $G$ -Modul. Weiter ist  $K[G] = \bigoplus_{\sigma \in G} \sigma K$   $G$ -induziert und somit kohomologisch trivial.  $\square$

**Satz 3.42.** *Es gilt*

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

(2) Falls  $G = \langle \tau \rangle$ , so gilt für  $\alpha \in L^\times$ :

$$N_{L/K}(\alpha) = 1 \iff \exists \beta \in L^\times : \alpha = \frac{\tau(\beta)}{\beta}.$$

Dabei ist  $\beta$  modulo  $K^\times$  eindeutig bestimmt.

*Beweis.* (1) Dies ist Hilberts Satz 90 (siehe Blatt 8, Aufgabe 1).

(2) Dies folgt aus

$$1 = H^1(G, L^\times) \cong H^{-1}(G, L^\times) = {}_G L^\times / ({}_{\tau-1} L^\times).$$

$\square$

**Korollar 3.43.** Falls  $|L| < \infty$ , so ist  $L^\times$  kohomologisch trivial, d.h.  $H^q(U, L^\times) = 1$  für alle  $q \in \mathbb{Z}$  und  $U \leq G$ .

*Beweis.* Es gilt  $H^1(U, L^\times) = 1$  für alle  $U$  und

$$1 = h(L^\times) = \frac{|H^0(U, L^\times)|}{|H^1(U, L^\times)|}.$$

Somit ist  $H^0(U, L^\times) = 1$  für alle  $U$  und  $L^\times$  ist kohomologisch trivial.  $\square$

**Definition 3.44.** Die *Brauergruppe von  $K$*  ist definiert als

$$Br(K) := H^2(K) := \bigcup_L H^2(\text{Gal}(L|K), L^\times).$$

Hierbei durchläuft  $L/K$  die endlichen Galoiserweiterungen von  $K$  in  $\overline{K}/K$  und für  $N/L/K$  mit endlichen Galoiserweiterungen  $N/K$  und  $L/K$  liefert die Inflation  $H^2(\text{Gal}(L|K), L^\times) \subseteq H^2(\text{Gal}(N|K), N^\times)$ .



### 3.4 Die multiplikative Gruppe von $p$ -adischen Körpern

Sei  $K/\mathbb{Q}_p$  eine endliche Erweiterung.

**Notation.** •  $v = v_K$  ist die normierte Bewertung von  $K$ .

- Der Bewertungsring ist

$$\mathcal{O} = \mathcal{O}_K = \{\alpha \in K \mid v_K(\alpha) \geq 0\}.$$

- Das maximale Ideal ist

$$\mathfrak{p} = \mathfrak{p}_K = \{\alpha \in K \mid v_K(\alpha) > 0\}.$$

- Der Restklassenkörper ist  $\overline{K} = \mathcal{O}_K/\mathfrak{p}$ .
- $U = U_K = \mathcal{O}_K^\times$  sind die Einheiten von  $K$ .
- $U^n = U_K^n = 1 + \mathfrak{p}_K^n$  sind die  $n$ -Einheiten für  $n \geq 1$ .
- Wir setzen  $U^0 = U$ .
- Wir setzen  $q = q_K = |\overline{K}| = p^f$ , wobei  $f = [\overline{K} : \mathbb{F}_p]$  der Trägheitsgrad ist.
- Wir wählen einen Erzeuger  $\pi = \pi_K$  von  $\mathfrak{p}_K$ , d.h.  $\mathfrak{p}_K = (\pi_K)$  bzw.  $v_K(\pi_K) = 1$ .

Es gilt

$$K^\times = \langle \pi_K \rangle \times U_K.$$

**Satz 3.45.** *Es gilt*

$$U/U^1 \cong \overline{K}^\times, \quad U^n/U^{n+1} \cong \overline{K}.$$

*Beweis.* Die surjektive Abbildung

$$\begin{aligned} U &\longrightarrow \overline{K}^\times \\ u &\longmapsto \bar{u} \end{aligned}$$

hat den Kern  $U^1$ .

Die Abbildung

$$\begin{aligned} U^n &\longrightarrow \overline{K} \\ 1 + a\pi_K^n &\longmapsto \bar{a}, \quad a \in \mathcal{O}_K \end{aligned}$$

ist ein Homomorphismus, denn

$$(1 + a\pi_K^n)(1 + b\pi_K^n) = 1 + (a + b + ab\pi_K^n)\pi_K^n \longmapsto \overline{a + b} = \bar{a} + \bar{b}.$$

Der Kern ist  $U^{n+1}$ . □

**Lemma 3.46.** Sei  $m \in \mathbb{N}$ . Dann induziert die Abbildung

$$x \longmapsto x^m$$

für genügend große  $n$  einen Isomorphismus

$$U^n \xrightarrow{\cong} U^{n+v(m)}.$$

*Beweis.* Sei  $x = 1 + a\pi^n \in U^n$  mit  $a \in \mathcal{O}_K$ . Dann ist

$$\begin{aligned} x^m &= 1 + ma\pi^n + \binom{m}{2} a^2 \pi^{2n} + \dots \\ &\equiv 1 \pmod{\mathfrak{p}^{n+v(m)}} \end{aligned}$$

falls  $2n \geq n + v(m)$ , also genau dann, wenn  $n \geq v(m)$  (denn:  $v(ma\pi^n) \geq v(m) + n$ ).

Surjektivität: Sei  $1 + a\pi^{n+v(m)}$  mit  $a \in \mathcal{O}_K$ . Finde  $x \in \mathcal{O}_K$  mit

$$1 + a\pi^{n+v(m)} = (1 + x\pi^n)^m = 1 + mx\pi^n + \pi^{2n}f(x), \quad f \in \mathcal{O}_K[X].$$

Schreibe  $m = u\pi^{v(m)}$  mit  $u \in U$ . Es ist zu lösen:

$$\begin{aligned} 1 + ux\pi^{n+v(m)} + \pi^{2n}f(x) &= 1 + a\pi^{n+v(m)} \\ \iff ux + \pi^{n-v(m)}f(x) - a &= 0 \end{aligned}$$

Falls  $n > v(m)$ , so ist  $\bar{x} := \bar{u}^{-1}\bar{a}$  eine Lösung modulo  $\mathfrak{p}$ . Diese kann man mit Hensels Lemma liften.

Injektivität: Es ist  $|\mu_m(K)| < \infty$ . Die  $U^n$  bilden eine Basis der offenen Umgebungen der 1. Da  $\bar{K}$  hausdorffsch ist, folgt die Injektivität.  $\square$

### 3.5 Die Klassenformation der unverzweigten Erweiterungen

Sei  $K/\mathbb{Q}_p$  eine endliche Erweiterung und  $L/K$  unverzweigt. Wir bezeichnen den Frobenius von  $L/K$  mit  $\varphi_{L/K}$ . Dieser ist eindeutig bestimmt durch

$$\varphi_{L/K}(x) \equiv x^{q_K} \pmod{\mathfrak{p}_L}$$

und es gilt

$$\langle \varphi_{L/K} \rangle = \text{Gal}(L|K).$$

Es gilt für unverzweigte  $N/L/K$

$$\begin{aligned} \varphi_{N/K}^{[L:K]} &= \varphi_{N/L}, \\ \varphi_{L/K} &= \varphi_{N/K}|_L = \varphi_{N/K} \text{Gal}(N|L), \end{aligned}$$

wobei  $\text{Gal}(L|K) \cong \text{Gal}(N|K)/\text{Gal}(N|L)$ .

**Satz 3.47.** *Sei  $L/K$  unverzweigt. Dann gilt*

$$H^q(\text{Gal}(L|K), U_L) = 1$$

für alle  $q \in \mathbb{Z}$ , d.h. die  $U_L$  sind kohomologisch trivial.

*Beweis.* Wir identifizieren

$$\begin{aligned} G &:= \text{Gal}(L|K) \cong \text{Gal}(\bar{L}|\bar{K}) \\ &\sigma \mapsto \bar{\sigma} \end{aligned}$$

mit

$$\bar{\sigma}(\bar{\alpha}) := \overline{\sigma(\alpha)}, \quad \alpha \in \mathcal{O}_L.$$

Dann ist

$$0 \longrightarrow U_L^1 \longrightarrow U_L \longrightarrow \bar{L}^\times \longrightarrow 0$$

eine exakte Sequenz von  $G$ -Moduln. Da  $\bar{L}^\times$  kohomologisch trivial ist, folgt

$$H^q(G, U_L^1) \cong H^q(G, U_L)$$

für alle  $q \in \mathbb{Z}$ . Sei  $\pi = \pi_K$ . Da  $L/K$  unverzweigt ist, ist  $v_L(\pi) = v_K(\pi) = 1$ . Betrachte für  $n \geq 2$

$$\begin{aligned} U_L^{n-1} &\longrightarrow \bar{L} \\ 1 + a\pi^{n-1} &\longmapsto \bar{a}, \quad a \in \mathcal{O}_L \end{aligned}$$

Dies ist ein Homomorphismus von  $G$ -Moduln:

$$\sigma(1 + a\pi^{n-1}) = 1 + \sigma(a)\pi^{n-1} \longmapsto \overline{\sigma(a)} = \bar{\sigma}(\bar{a}).$$

Aus der exakten Sequenz

$$0 \longrightarrow U_L^n \longrightarrow U_L^{n-1} \longrightarrow \bar{L} \longrightarrow 0$$

und  $H^q(G, \bar{L}) = 0$  folgt

$$H^q(G, U_L^n) \cong H^q(G, U_L^1) \cong H^q(G, U_L).$$

Die Abbildung  $x \mapsto x^m$  liefert für alle  $m \geq 1$  einen Homomorphismus  $U_L \longrightarrow U_L$  und einen Isomorphismus

$$U_L^n \xrightarrow{\cong} U_L^{n+v_L(m)}.$$

Das Diagramm

$$\begin{array}{ccc} H^q(G, U_L^n) & \xrightarrow[\cong]{\subseteq} & H^q(G, U_L) \\ \cong \downarrow m & & \downarrow m \\ H^q(G, U_L^{n+v_L(m)}) & \xrightarrow[\cong]{\subseteq} & H^q(G, U_L) \end{array}$$

kommutiert. Dann ist

$$H^q(G, U_L) \xrightarrow{m} H^q(G, U_L)$$

ein Isomorphismus für alle  $m \geq 1$ . Da  $|G| H^q(G, U_L) = 0$  folgt  $H^q(G, U_L) = 1$ .  $\square$

**Korollar 3.48.** Sei  $L/K$  unverzweigt. Dann ist  $N_{L/K}(U_L) = U_K$ .

*Beweis.* Dies folgt sofort aus  $H^0(G, U_L) = U_K/N_{L/K}(U_L) = 0$ . □

Ziel: Sei  $T := \bigcup_{n \geq 1} K_n$  der maximal unverzweigte Teilkörper von  $K_0^c|K_0$ . Dabei ist  $[K_n : K_0] = n$ . Wir wollen zeigen, dass

$$(\text{Gal}(T|K_0), T^\times)$$

eine Klassenformation ist.

Dazu ist

$$\text{inv}_{L/K} : H^2(\text{Gal}(L|K), L^\times) \longrightarrow \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

für eine Erweiterung  $L/K$  in  $T/K_0$  zu definieren.

**Bemerkung 3.49.** Es ist  $\text{Gal}(T|K_0) \cong \widehat{\mathbb{Z}}$ .

Sei

$$0 \longrightarrow U_L \longrightarrow L^\times \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0.$$

Dann erhalten wir einen Isomorphismus

$$H^2(G, L^\times) \xrightarrow[\cong]{\overline{v_L}} H^2(G, \mathbb{Z}).$$

Betrachte

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

Daraus folgt

$$\text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\cong]{\delta} H^2(G, \mathbb{Z}).$$

Betrachte noch

$$\text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\cong]{\varphi} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

$$\chi \longmapsto \chi(\varphi_{L/K})$$

Zusammenfassend:

$$\begin{array}{ccc} H^2(G, L^\times) & \xrightarrow{\text{inv}_{L/K}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ \downarrow \overline{v_L} & & \uparrow \varphi \\ H^2(G, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G, \mathbb{Q}/\mathbb{Z}) \end{array}$$

Setze wieder  $H^q(L|K) := H^q(\text{Gal}(L|K), L^\times)$ .

**Satz 3.50.**  $(\text{Gal}(T|K_0), T^\times)$  ist eine Klassenformation für  $K_0/\mathbb{Q}_p$  endlich.

*Beweis.* Es ist die Kommutativität von

$$\begin{array}{ccccccc}
H^2(L|K) & \xrightarrow{\overline{v_L}} & H^2(G_{L/K}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\
\downarrow \text{Inf}=\subseteq & & \downarrow \text{Inf} & & \downarrow \text{Inf} & & \downarrow \subseteq \\
H^2(N|K) & \xrightarrow{\overline{v_N}} & H^2(G_{N/K}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{N/K}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z}
\end{array} \quad (3.1)$$

bzw.

$$\begin{array}{ccccccc}
H^2(N|K) & \xrightarrow{\overline{v_N}} & H^2(G_{N/K}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{N/K}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} \\
\downarrow \text{Res} & & \downarrow \text{Res} & & \downarrow \text{Res} & & \downarrow [L:K] \\
H^2(N|L) & \xrightarrow{\overline{v_N}} & H^2(G_{N/L}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{N/L}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z}
\end{array} \quad (3.2)$$

zu zeigen.

Zum linken Rechteck in Diagramm 3.1: Sei  $\bar{x} \in H^2(G_{L/K}, L^\times)$ . Dann gilt

$$\begin{array}{ccc}
\bar{x} & \xrightarrow{\overline{v_L}} & \overline{v_L} \circ \bar{x} \\
\downarrow & & \downarrow \\
\text{Inf } \bar{x} & \xrightarrow{\quad} & ((\sigma_1, \sigma_2) \mapsto v_L(x(\overline{\sigma_1}, \overline{\sigma_2}))) \\
& & \parallel \\
& & ((\sigma_1, \sigma_2) \mapsto v_N(x(\overline{\sigma_1}, \overline{\sigma_2})))
\end{array}$$

Die Bilder stimmen überein, da  $v_N(\alpha) = v_L(\alpha)$  für alle  $\alpha \in L^\times$ .

Das linke Rechteck in Diagramm 3.2 ist offensichtlich.

Die mittleren Rechtecke in beiden Diagrammen folgen aus der Vertauschbarkeit von  $\delta$  mit Inf und Res.

Zum rechten Rechteck in Diagramm 3.1: Sei  $\chi \in H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(G_{L/K}, \mathbb{Q}/\mathbb{Z})$ . Dann gilt

$$\begin{array}{ccc}
\chi & \xrightarrow{\quad} & \chi(\varphi_{L/K}) \\
\downarrow & & \downarrow \\
\text{Inf } \chi & \xrightarrow{\quad} & (\text{Inf } \chi)(\varphi_{N/K}) \\
& & \parallel \\
& & \chi(\varphi_{L/K})
\end{array}$$

Die Bilder sind gleich, da

$$(\text{Inf } \chi)(\varphi_{N/K}) = \chi(\varphi_{N/K}|_L) = \chi(\varphi_{L/K}).$$

Das rechte Rechteck in Diagramm 3.2 folgt aus  $\varphi_{N/K}^{[L:K]} = \varphi_{N/L}$ . □

**Satz 3.51.** *Die Abbildung*

$$H^2(T|K) = \bigcup_{L/K \text{ unverzweigt}} H^2(L|K) \xrightarrow{\text{inv}_{T/K}} \mathbb{Q}/\mathbb{Z}$$

ist ein Isomorphismus (hierbei ist  $\text{inv}_{T/K}|_L = \text{inv}_{L/K}$ ).

*Beweis.* Injektivität ist eine allgemeine Tatsache aus der Theorie der Klassenformationen. Surjektivität folgt aus

$$\mathbb{Q}/\mathbb{Z} = \bigcup_{n \geq 1} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

und weil es zu jedem  $n \geq 1$  eine unverzweigte Erweiterung  $L$  mit  $[L : K] = n$  gibt.  $\square$

**Satz 3.52.** *Für  $a \in K^\times$  gilt*

$$(a, L/K) = \varphi_{L/K}^{v_K(a)}.$$

Für den Beweis benötigen wir das folgende

**Lemma 3.53.** *Sei  $(G, A)$  eine Klassenformation,  $L/K$  normal,  $a \in A_K$  und  $\bar{a} \in H^0(L|K) = A_K/N_{L/K}A_L$ . Dann gilt für jedes  $\chi \in H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z})$*

$$\chi((a, L/K)) = \text{inv}_{L/K}(\bar{a} \cup \delta\chi).$$

Hierbei ist  $\delta$  der Verbindungshomomorphismus zur exakten Sequenz

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

*Beweis von Satz 3.52.* Es gilt mit Lemma 3.53

$$\begin{aligned} \chi((a, L/K)) &= \text{inv}_{L/K}(\bar{a} \cup \delta\chi) = (\varphi \circ \delta^{-1} \circ \bar{v}_L)(\bar{a} \cup \delta\chi) \\ &\stackrel{(*)}{=} (\varphi \circ \delta^{-1})(v_L(a)\delta\chi) = \varphi(v_L(a)\chi) \\ &= \varphi(v_K(a)\chi) = v_K(a)\chi(\varphi_{L/K}) \\ &= \chi(\varphi_{L/K}^{v_K(a)}) \end{aligned}$$

Da dies für alle  $\chi$  gilt, folgt  $(a, L/K) = \varphi_{L/K}^{v_K(a)}$ . Hierbei folgt  $(*)$  aus Eigenschaften des Cupprodukts.  $\square$

*Beweis von Lemma 3.53.* Setze  $\sigma_a := (a, L/K) \in G_{L/K}^{\text{ab}}$ . Sei  $\bar{\sigma}_a$  das Bild von  $\sigma_a$  unter

$$\begin{aligned} G_{L/K}^{\text{ab}} &\cong H^{-2}(G_{L/K}, \mathbb{Z}) \\ \sigma_a &\mapsto \bar{\sigma}_a \end{aligned}$$

Wegen

$$\begin{array}{ccccc}
 \overline{\sigma}_a & H^{-2}(G_{L/K}, \mathbb{Z}) & \xrightarrow{u_{L/K} \cup -} & H^0(L|K) = A_K/N_{L/K}A_L & \overline{a} \\
 \uparrow & \cong \uparrow & & \uparrow & \uparrow \\
 \sigma_a & G_{L/K}^{\text{ab}} & \xleftarrow{(-, L/K)} & A_K & a
 \end{array}$$

gilt  $\overline{a} = u_{L/K} \cup \overline{\sigma}_a$ . Also ist

$$\overline{a} \cup \delta\chi = (u_{L/K} \cup \overline{\sigma}_a) \cup \delta\chi = u_{L/K} \cup (\overline{\sigma}_a \cup \delta\chi) = u_{L/K} \cup \delta(\overline{\sigma}_a \cup \chi).$$

Die Rechenregel aus [NS11, Kapitel I, Lemma (5.7)] bzw. Lemma 2.71 impliziert

$$\overline{\sigma}_a \cup \chi = \chi \cup \overline{\sigma}_a \stackrel{2.71}{=} \chi(\sigma_a) \stackrel{(*)}{=} \frac{r}{n} + \mathbb{Z},$$

wobei  $n = [L : K]$  und  $r$  durch  $(*)$  definiert wird. Also folgt

$$\delta(\overline{\sigma}_a \cup \chi) = \delta\left(\frac{r}{n} + \mathbb{Z}\right) = r + n\mathbb{Z} \in H^0(G_{L/K}, \mathbb{Z})$$

da

$$\begin{aligned}
 \delta : \frac{1}{n}\mathbb{Z}/\mathbb{Z} = H^{-1}(G_{L/K}, \mathbb{Q}/\mathbb{Z}) &\longrightarrow H^0(G_{L/K}, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} \\
 \frac{s}{n} + \mathbb{Z} &\longmapsto s + n\mathbb{Z}
 \end{aligned}$$

Zusammenfassend erhalten wir

$$\overline{a} \cup \delta\chi = u_{L/K} \cup (r + n\mathbb{Z}) = \underbrace{(r + n\mathbb{Z})}_{\in H^0(G_{L/K}, \mathbb{Z})} \cup \underbrace{u_{L/K}}_{\in H^{-2}(G_{L/K}, \mathbb{Z})} = u_{L/K}^r.$$

Damit folgt

$$\text{inv}_{L/K}(\overline{a} \cup \delta\chi) = r \text{inv}_{L/K}(u_{L/K}) = \frac{r}{n} + \mathbb{Z} = \chi(\sigma_a).$$

□

**Satz 3.54.** Sei  $L/K$  unverzweigt von Grad  $f = [L : K]$ . Dann ist

$$N_{L/K}(L^\times) = \langle \pi_K^f \rangle \times U_K.$$

*Beweis.* Es gilt

$$\begin{aligned}
 a \in N_{L/K}(L^\times) &\iff (a, L/K) = 1, \\
 &\iff \varphi_{L/K}^{v_K(a)} = 1, \\
 &\iff f|v_K(a), \\
 &\iff a \in \langle \pi_K^f \rangle \times U_K.
 \end{aligned}$$

□

### 3.6 Das lokale Reziprozitätsgesetz

Sei  $K_0/\mathbb{Q}_p$  endlich,  $\Omega = K_0^c$  und  $G_{K_0} = \text{Gal}(\Omega|K_0)$ .

Ziel:  $(G_{K_0}, \Omega^\times)$  ist Klassenformation.

Dazu ist für  $L/K$  normal,  $K/K_0$  endlich, ein Invarianten-Isomorphismus

$$\text{inv}_{L/K} : H^2(\text{Gal}(L|K), L^\times) \longrightarrow \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

zu definieren.

**Lemma 3.55** (Zweite fundamentale Ungleichung). *Für jede normale Erweiterung  $L/K$  gilt  $|H^2(L|K)|$  teilt  $[L:K]$ .*

*Beweis.* Sei zunächst  $L/K$  zyklisch von Primzahlgrad  $l$ .

**Behauptung.** *Es gilt*

$$h(L^\times) = \frac{|H^2(L|K)|}{|H^1(L|K)|} = |H^2(L|K)| = l.$$

*Beweis der Behauptung.*

**Erinnerung 3.56.** Es ist

$$q_{f,g}(A) = \frac{(\ker(f) : \text{im}(g))}{(\ker(g) : \text{im}(f))}$$

für  $f, g : A \longrightarrow A$  mit  $f \circ g = g \circ f = 0$  (vgl. Blatt 9). In Blatt 9, Aufgabe 5 wurde gezeigt:

$$h(L^\times)^{l-1} = q_{0,l}(K^\times)^l / q_{0,l}(L^\times), \tag{3.3}$$

wobei

$$q_{0,l}(K^\times) = \frac{(K^\times : (K^\times)^l)}{|\mu_l(K)|},$$

$$q_{0,l}(L^\times) = \frac{(L^\times : (L^\times)^l)}{|\mu_l(L)|}.$$

Wir brauchen den

**Satz 3.57** (Beweis am Ende). *Sei  $K/\mathbb{Q}_p$  endlich. Dann gilt für  $m \geq 1$*

$$(K^\times : (K^\times)^m) = m q_K^{v_K(m)} |\mu_m(K)|$$

mit  $q_K = |\overline{K}|$ .



Also erhalten wir

$$\begin{aligned} q_{0,l}(K^\times) &= lq_K^{v_K(l)}, \\ q_{0,l}(L^\times) &= lq_L^{v_L(l)}. \end{aligned}$$

Sei  $l = ef$  mit dem Verzweigungsindex  $e$  und Restklassengrad  $f$ . Dann gilt  $q_L = q_K^f$  und  $v_L(l) = ev_K(l)$ .

Aus (3.3) erhalten wir

$$h(L^\times)^{l-1} = \frac{l^l q_K^{lv_K(l)}}{lq_L^{v_L(l)}} = \frac{l^{l-1} q_K^{lv_K(l)}}{q_K^{f ev_K(l)}} = l^{l-1}$$

und somit folgt  $h(L^\times) = l$ . □

Zum allgemeinen Fall:  $G_{L/K}$  ist auflösbar, denn:

Definieren wir die *höheren Verzweigungsgruppen*

$$G_i = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{p}_L^{i+1}}\}$$

und betrachten  $G \supseteq G_0 \supseteq G_1$ , so folgt die Auflösbarkeit aus

$$\begin{array}{c} L \\ \left| \right. G_1 \text{ ist } p\text{-Gruppe} \\ L^{G_1} \\ \left| \right. \begin{array}{l} G_0/G_1 \hookrightarrow \bar{L}^\times \\ \bar{\sigma} \mapsto \frac{\sigma(\pi_L)}{\pi_L} \end{array} \\ L^{G_0} \\ \left| \right. \text{zyklisch von der Ordnung } f \\ K \end{array}$$

(siehe [Ser13, Chapter IV, §2, Prop. 7 bzw. Cor. 5]).

Also gilt  $K \stackrel{l}{\subseteq} K' \subseteq L$ . Wegen  $H^1(K'|K) = 1$  ist

$$0 \longrightarrow H^2(K'|K) \xrightarrow{\text{Inf}} H^2(L|K) \xrightarrow{\text{Res}} H^2(L|K')$$

exakt. Damit folgt

$$|H^2(L|K)| \mid \underbrace{|H^2(K'|K)|}_{=l=[K':K]} \mid |H^2(L|K')|.$$

Mit Induktion folgt nun  $|H^2(L|K')|$  teilt  $[L : K']$  und insgesamt ergibt sich die Behauptung. □

*Beweis von Satz 3.57.* Es gilt

$$\begin{aligned} q_{0,m}(K^\times) &= \frac{(K^\times : (K^\times)^m)}{|\mu_m(K)|} \\ \iff (K^\times : (K^\times)^m) &= |\mu_m(K)| q_{0,m}(K^\times) \end{aligned}$$

Aus

$$0 \longrightarrow U_K \longrightarrow K^\times \xrightarrow{v_K} \mathbb{Z} \longrightarrow 0$$

folgt

$$q_{0,m}(K^\times) = q_{0,m}(U_K) \underbrace{q_{0,m}(\mathbb{Z})}_{=m}.$$

Also ist noch zu zeigen, dass  $q_{0,m}(U_K) = q_K^{v_K(m)}$ .

Sei  $n$  groß genug, sodass

$$U_K^n \xrightarrow[\cong]{m} U_K^{n+v_K(m)}.$$

Betrachte

$$0 \longrightarrow U_K^n \longrightarrow U_K \longrightarrow U_K/U_K^n \longrightarrow 0.$$

Damit folgt

$$\begin{aligned} q_{0,m}(U_K) &= q_{0,m}(U_K^n) \underbrace{q_{0,m}(U_K/U_K^n)}_{\stackrel{3.58_1}{\cong} 1} \\ &= \frac{(U_K^n : (U_K^n)^m)}{|\mu_m(K) \cap U_K^n|} \\ &= (U_K^n : U_K^{n+v_K(m)}) = q_K^{v_K(m)} \end{aligned}$$

da

$$\begin{aligned} U_K^i/U_K^{i+1} &\cong \mathfrak{p}_K^i/\mathfrak{p}_K^{i+1} \cong \mathcal{O}_K/\mathfrak{p}_K \\ (1+a)U_K^{i+1} &\leftarrow a + \mathfrak{p}_K^{i+1} \end{aligned}$$

□

Seien  $f, g : A \longrightarrow A$  mit  $f \circ g = g \circ f = 0$  und

$$q_{f,g}(A) := \frac{(\ker(f) : \operatorname{im}(g))}{(\ker(g) : \operatorname{im}(f))}.$$

**Lemma 3.58.** *Ist  $|A| < \infty$ , so folgt  $q_{f,g}(A) = 1$ .*

*Beweis.* Betrachte

$$\begin{aligned} 0 &\longrightarrow \ker(f) \longrightarrow A \longrightarrow \operatorname{im}(f) \longrightarrow 0, \\ 0 &\longrightarrow \ker(g) \longrightarrow A \longrightarrow \operatorname{im}(g) \longrightarrow 0. \end{aligned}$$

Dann folgt

$$|A| = |\ker(f)| |\operatorname{im}(f)| = |\ker(g)| |\operatorname{im}(g)|$$

und somit

$$\frac{|\ker(f)|}{|\operatorname{im}(g)|} = \frac{|\ker(g)|}{|\operatorname{im}(f)|}.$$

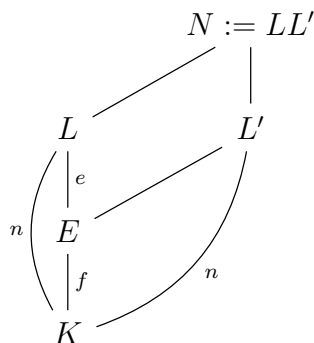
□

**Satz 3.59.** Sei  $L/K$  normal und  $L'/K$  die unverzweigte Erweiterung mit

$$[L' : K] = [L : K].$$

Dann ist  $H^2(L|K) = H^2(L'|K)$  in  $H^2(K)$ .

Genauer: Betrachte



mit  $E = L \cap L'$ . Dann gilt

$$\operatorname{Inf}_{G_{L/K}}^{G_{N/K}} H^2(L|K) = \operatorname{Inf}_{G_{L'/K}}^{G_{N/K}} H^2(L'|K)$$

in  $H^2(N|K)$ .

*Beweis.* Es genügt zu zeigen, dass  $H^2(L'|K) \subseteq H^2(L|K)$ , denn:

Es gilt  $|H^2(L'|K)| = [L' : K] = [L : K]$  und  $|H^2(L|K)|$  teilt  $[L : K]$ . Zusammengekommen folgt, dass die Inklusion schon eine Gleichheit ist.

$N/L$  ist unverzweigt, da  $G_0(N|L) \hookrightarrow G_0(L'|E) = 1$ . Sei  $c \in H^2(L'|K)$ . Aus

$$0 \longrightarrow H^2(L|K) \xrightarrow{\operatorname{Inf}} H^2(N|K) \xrightarrow{\operatorname{Res}_L} H^2(N|L)$$

folgt:

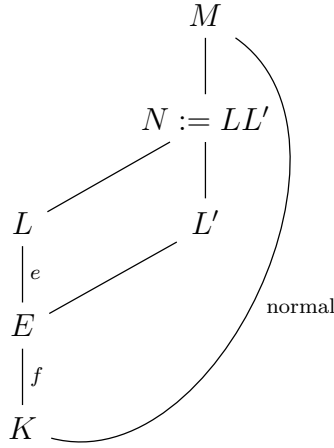
$$\begin{aligned} c \in H^2(L|K) &\iff \operatorname{Res}_L(c) = 1 \in H^2(N|L) \\ &\iff \operatorname{inv}_{N/L}(\operatorname{Res}_L(c)) = 0 \in \frac{1}{[N:L]} \mathbb{Z}/\mathbb{Z} \end{aligned}$$

Also reicht es zu zeigen:

$$\text{inv}_{N/L}(\text{Res}_L(c)) = [L : K] \underbrace{\text{inv}_{L'/K}(c)}_{\in \frac{1}{[L':K]} \mathbb{Z}/\mathbb{Z}}.$$

Dazu folgendes

**Lemma 3.60.** *Sei  $M/K$  normal und  $L'/K$  unverzweigt. Seien  $L, L' \subseteq M$ , sodass der maximal unverzweigte Teilkörper  $E$  von  $L/K$  in  $L'$  enthalten ist. Es ergibt sich die folgende Situation:*



Dann ist  $N/L$  unverzweigt. Sei  $c \in H^2(L'|K)$ . Dann ist  $\text{Res}_L(c) \in H^2(N|L)$  und es gilt

$$\text{inv}_{N/L}(\text{Res}_L(c)) = [L : K] \text{inv}_{L'/K}(c).$$

*Beweis von Lemma 3.60.* An den 2-Kozyklen liest man ab

$$\text{Res}_{G_{M/L}}^{G_{M/K}} \text{Inf}_{G_{L'/K}}^{G_{M/K}} = \text{Inf}_{G_{N/L}}^{G_{M/L}} \underbrace{\text{Res}_{G_{L'/E}}^{G_{L'/K}}}_{\substack{\text{betrachte dies als} \\ \text{2-Kozykel auf} \\ G_{L'/E} \cong G_{N/L}}} \quad (3.4)$$

Damit ist

$$\text{Res}_L(c) \in H^2(N|L).$$

Seien  $e$  und  $f$  der Verzweigungsindex und Restklassenkörpergrad von  $L/K$ . Also gilt  $[L : K] = ef$  und  $v_K = ev_L$ . Es ist die Kommutativität von folgendem Diagramm zu zeigen:

$$\begin{array}{ccccccc} H^2(L'|K) & \xrightarrow{\overline{v_K}} & H^2(G_{L'/K}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{L'/K}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[L':K]} \mathbb{Z}/\mathbb{Z} \\ \downarrow \subseteq = \text{Inf} & & \downarrow \text{Inf} & & \downarrow \text{Inf} & & \downarrow \subseteq \\ H^2(M|K) & & H^2(G_{M/K}, \mathbb{Z}) & & H^1(G_{M/K}, \mathbb{Q}/\mathbb{Z}) & & \frac{1}{[M:K]} \mathbb{Z}/\mathbb{Z} \\ \downarrow \text{Res}_L & & \downarrow e \text{Res}_L & & \downarrow e \text{Res}_L & & \downarrow [L:K] \\ H^2(N|L) & \xrightarrow{\overline{v_L}} & H^2(G_{N/L}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{N/L}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N:L]} \mathbb{Z}/\mathbb{Z} \end{array}$$

Die unteren vertikalen Abbildungen sind eigentlich die Restriktionen auf die Bilder der oberen vertikalen Abbildungen.

Zum linken Teildiagramm:

$$\begin{array}{ccc}
H^2(L'|K) \ni c & \xrightarrow{\quad} & \left( G_{L'/K}^2 \ni \sigma \mapsto v_{L'}(\underbrace{c(\sigma)}_{\in L'^{\times}}) \right) \\
\downarrow & & \downarrow \\
\text{Inf}_{G_{L'/K}}^{G_{M/K}} c & & \left( G_{M/K}^2 \ni \tau \mapsto v_{L'}(c(\bar{\tau})) \right) \\
\downarrow & & \downarrow \\
\text{Res}_{G_{M/L}}^{G_{M/K}} \text{Inf}_{G_{L'/K}}^{G_{M/K}} c & & \left( G_{M/L}^2 \ni \tau \mapsto ev_K(c(\bar{\tau})) \right) \\
\parallel (3.4) & & \parallel \\
\text{Inf}_{G_{N/L}}^{G_{M/L}} \text{Res}_{G_{L'/E}}^{G_{L'/K}} c & \xrightarrow{\quad} & \left( G_{M/L}^2 \ni \tau \mapsto v_L(c(\bar{\tau})) \right)
\end{array}$$

Zum mittleren Teildiagramm: Dies folgt wie bisher üblich.

Zum rechten Teildiagramm: Es ist

$$\varphi_{N/L}|_{L'} = \varphi_{L'/K}^{[E:K]} = \varphi_{L'/K}^f, \quad (3.5)$$

denn für  $a \in L'$  gilt:

$$\begin{aligned}
\varphi_{N/L}(a) &\equiv a^{q_L} \pmod{\mathfrak{p}_N \cap L'} \\
&\equiv a^{q_K} \pmod{\mathfrak{p}_{L'}} \\
&\equiv \varphi_{L'/K}^f(a) \pmod{\mathfrak{p}_{L'}}
\end{aligned}$$

Damit erhalten wir

$$\begin{array}{ccc}
\chi & \xrightarrow{\quad} & \chi(\varphi_{L'/K}) \\
\downarrow & & \downarrow \\
\text{Inf}_{G_{L'/K}}^{G_{M/K}} \chi & & \chi(\varphi_{L'/K}) \\
\downarrow & & \downarrow \\
e \text{Res}_{G_{M/L}}^{G_{M/K}} \text{Inf}_{G_{L'/K}}^{G_{M/K}} \chi & & [L : K] \chi(\varphi_{L'/K}) \\
\downarrow & & \parallel \\
e\chi(\varphi_{N/L}) & \xlongequal{(3.5)} & e\chi(\varphi_{L'/K}^f)
\end{array}$$

□

Damit folgt die Aussage des Satzes.  $\square$

**Definition 3.61.** Sei  $K_0/\mathbb{Q}_p$  ein  $\mathfrak{p}$ -adischer Körper und  $\Omega = K_0^c$ . Sei  $L/K$  eine normale Teilerweiterung von  $\Omega/K_0$ . Dann sei

$$\text{inv}_{L/K} : H^2(L|K) \xrightarrow{\cong} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

definiert durch

$$\text{inv}_{L/K}(c) := \text{inv}_{L'/K}(c)$$

für alle  $c \in H^2(L|K) = H^2(L'|K)$ , wobei  $L'/K$  die unverzweigte Erweiterung mit  $[L' : K] = [L : K]$  ist.

**Satz 3.62.**  $(G_{K_0}, \Omega^\times)$  ist eine Klassenformation.

*Beweis.* Axiom 3.24.I. ist erfüllt nach Hilberts Satz 90.

Zu Axiom 3.24.II.(1): Sei  $N/L/K$  und  $N/K$  und  $L/K$  seien normal. Seien  $N'$  und  $L'$  die entsprechenden unverzweigten Erweiterungen, d.h.

$$[N' : K] = [N : K], \quad [L' : K] = [L : K].$$

Dann gilt für  $c \in H^2(L|K)$

$$\text{inv}_{N/K}(c) = \text{inv}_{N'/K}(c) = \text{inv}_{L'/K}(c) = \text{inv}_{L/K}(c).$$

Zu Axiom 3.24.II.(2): Wir haben jetzt eine injektive Abbildung

$$\text{Br}(K) = H^2(K) = \bigcup_{L/K \text{ normal}} H^2(L|K) \xrightarrow{\text{inv}_K} \mathbb{Q}/\mathbb{Z}$$

(diese Abbildung ist auch surjektiv).

Für 3.24.II.(2) ist folgendes nachzuweisen: Sei  $N/L/K$  mit  $N/K$  normal. Dann ist für  $c \in H^2(N|K)$  zu zeigen:

$$\text{inv}_{N/L}(\underbrace{\text{Res}_L(c)}_{\in H^2(N|L)}) = [L : K] \text{inv}_{N/K}(c)$$

Dazu zeigt man für beliebige  $L/K$

$$\text{inv}_L(\text{Res}_L(c)) = [L : K] \text{inv}_K(c)$$

für  $c \in H^2(K)$ . Dies folgt aus Lemma 3.60.  $\square$

**Satz 3.63.** Sei  $L/K$  eine abelsche Erweiterung von  $\mathfrak{p}$ -adischen Körpern. Sei

$$G_0 := \{\sigma \in G = \text{Gal}(L|K) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{p}_L} \forall \alpha \in \mathcal{O}_L\}$$

die Verzweigungsgruppe und

$$G_1 = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{p}_L^2} \forall \alpha \in \mathcal{O}_L\}$$

die wilde Verzweigungsgruppe. Dann gilt

$$(1) (-, L/K) : U_K \longrightarrow G_0,$$

$$(2) (-, L/K) : U_K^1 \longrightarrow G_1.$$

*Beweis.* Für (1) betrachte

$$G \left( \begin{array}{c} L \\ \left| \begin{array}{c} e \\ \end{array} \right. \\ T = L^{G_0} \\ \left| \begin{array}{c} f \\ \end{array} \right. \\ K \end{array} \right) \begin{array}{l} G_0 \\ \text{unverzweigt} \end{array}$$

Sei  $u \in U_K$ . Dann gilt

$$(u, L/K)|_T = (u, T/K) = \varphi_{T/K}^{v_K(u)} = 1$$

und somit  $(u, L/K) \in G_0$ .

Sei umgekehrt  $\tau \in G_0$ . Sei  $a \in K^\times$  mit  $(a, L/K) = \tau$ .

Ziel: Finde  $u \in U_K$  mit  $(a, L/K) = (u, L/K)$ . Dies gilt genau dann, wenn  $a = N_{L/K}(b)u$  für ein  $b \in L^\times$ .

Dazu: Da  $\tau \in G_0$  ist gilt

$$\tau|_T = 1 = (a, L/K)|_T = (a, T/K) = \varphi_{T/K}^{v_K(a)}$$

Damit folgt  $f$  teilt  $v_K(a)$ . Sei  $b \in L^\times$  mit  $v_L(b) = \frac{1}{f}v_K(a)$ . Dann leistet  $b$  das Gewünschte.

Zu (2):  $G_1$  ist die  $p$ -Sylowuntergruppe von  $G_0$ , denn:

$$G_0/G_1 \hookrightarrow U_L/U_L^1 \cong \overline{L}^\times \quad (3.6)$$

Für  $n$  groß genug ist  $U_K^n \subseteq \ker((-, L/K))$ .

*Beweis hierfür.* Es ist z.B. für große  $n'$   $U_K^{n'} \xrightarrow[\cong]{m} U_K^{n'+v_K(m)}$ . Sei  $m = [L : K]$ , so gilt  $(K^\times)^m \subseteq \ker((-, L/K))$ . Also gilt  $U_K^n \subseteq \ker((-, L/K))$  für  $n = n' + v_K(m)$   $\square$

Dann gilt nach (1)

$$U_K/U_K^n \xrightarrow{(-, L/K)} G_0.$$

Die  $p$ -Sylowuntergruppe von  $U_K/U_K^n$  ist gerade  $U_K^1/U_K^n$ , denn:

$$\begin{aligned} U_K^i/U_K^{i+1} &\cong \mathfrak{p}_K^i/\mathfrak{p}_K^{i+1} \cong \mathcal{O}_K/\mathfrak{p}_K = \overline{K} \\ (1+x)U_K^{i+1} &\leftarrow x + \mathfrak{p}_K^{i+1} \end{aligned}$$

$\square$

*Beweis von (3.6).* Definiere

$$\begin{aligned} \kappa_i : G_i &\longrightarrow U_L^i/U_L^{i+1} \\ \sigma &\longmapsto \frac{\sigma(\pi_L)}{\pi_L} \end{aligned}$$

für ein Primelement  $\pi_L$  von  $L$ .  $\kappa_i$  ist wohldefiniert, denn:

Sei  $\pi'_L = u\pi_L$  mit  $u \in U_L$ . Es ist zu zeigen, dass  $\frac{\sigma(u)}{u} \in U_L^{i+1}$ . Dies gilt, da

$$\begin{aligned} \sigma(u) &\equiv u \pmod{\mathfrak{p}_L^{i+1}} \\ \iff \frac{\sigma(u)}{u} &\equiv 1 \pmod{\mathfrak{p}_L^{i+1}} \end{aligned}$$

Weiter ist zu zeigen, dass  $\frac{\sigma(\pi_L)}{\pi_L} \in U_L^i$ . Dies gilt, da

$$\begin{aligned} \sigma(\pi_L) &\equiv \pi_L \pmod{\mathfrak{p}_L^{i+1}} \\ \iff \frac{\sigma(\pi_L)}{\pi_L} &\equiv 1 \pmod{\mathfrak{p}_L^i} \end{aligned}$$

$\kappa_i$  ist ein Homomorphismus, denn:

Seien  $\sigma, \tau \in G_i$ . Dann gilt wegen  $\tau(\pi_L) = u\pi_L$  für ein  $u \in U_L$ :

$$\begin{aligned} \frac{\sigma\tau(\pi_L)}{\pi_L} &= \frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)} \frac{\tau(\pi_L)}{\pi_L} \\ &= \frac{\sigma(\pi_L)}{\pi_L} \underbrace{\frac{\sigma(u)}{u}}_{\in U_L^{i+1}} \frac{\tau(\pi_L)}{\pi_L} \end{aligned}$$

□

**Bemerkung 3.64.** Die höheren Einseinheitengruppen werden nach Übergang zur oberen Nummerierung auf die entsprechenden Verzweigungsgruppen abgebildet.

Genauer:

$$\begin{array}{ccc} K^\times/N_{L/K}(L^\times) \geq U_K/N_{L/K}U_L \geq U_K^1/N_{L/K}U_L^{\psi(1)} \geq \dots \geq U_K^n/N_{L/K}U_L^{\psi(n)} \geq \dots \geq 1 \\ \parallel & & (*) \downarrow \cong \\ G & & G^n = G_{\psi(n)} \end{array}$$

Hierbei ist  $\psi$  die Herbrandfunktion (siehe [Ser13, Chapter IV, §3]). Die Isomorphie (\*) findet man in [Ser13, Chapter XV, §3, Cor.3].

### 3.7 Der Existenzsatz

Sei  $K$  ein  $\mathfrak{p}$ -adischer Körper. Wir wissen bereits, dass die Normengruppen  $N_{L/K}(L^\times)$  in 1 : 1-Korrespondenz zu den endlichen abelschen Erweiterungen von  $K$  stehen.



Jede Normengruppe ist offen in  $K^\times$  von endlichem Index, denn:

Sei

$$|K^\times / N_{L/K}(L^\times)| = [L : K] =: m$$

für eine endliche abelsche Erweiterung  $L/K$ . Damit folgt  $(K^\times)^m \leq N_{L/K}(L^\times)$ . In der Übung wurde gezeigt, dass  $(K^\times)^m \leq K^\times$  offen ist. Zusammengenommen erhalten wir, dass

$$N_{L/K}(L^\times) = \bigcup_{x \in N_{L/K}(L^\times) / (K^\times)^m} \underbrace{x(K^\times)^m}_{\text{offen}}$$

offen und von endlichem Index ist.

Die Umkehrung ist der

**Satz 3.65** (Existenzsatz). *Sei  $I \leq K^\times$  offen und  $[K^\times : I] =: m < \infty$ . Dann ist  $I$  eine Normengruppe.*

*Beweis.* Es ist  $(K^\times)^m \leq I \leq K$ , d.h. es genügt zu zeigen:  $(K^\times)^m$  ist Normengruppe.

**Erinnerung 3.66.** Sei  $J \leq I \leq K^\times$  mit einer Normengruppe  $J$ . Dann ist auch  $I$  Normengruppe, denn:

Sei  $L/K$  eine endliche abelsche Erweiterung, sodass  $J = N_{L/K}(L^\times)$ . Dann erhalten wir

$$\begin{array}{ccc} K^\times/J & \xrightarrow[\cong]{(-, L/K)} & \text{Gal}(L|K) =: G \\ \text{IV} & & \text{IV} \\ I/J & \xrightarrow{\cong} & H \end{array}$$

Sei  $a \in I$ . Betrachte

$$G \left( \begin{array}{c} L \\ \left| \right)^H \\ M = L^H \\ \left| \right)^{G/H} \\ K \end{array} \right.$$

Dann ist

$$1 = (a, L/K) \Big|_M = (a, M/K) \iff a \in N_{M/K}(M^\times).$$

Also folgt  $I \leq N_{M/K}(M^\times)$ .

Andererseits gilt

$$J = N_{L/K}(L^\times) \overset{[L:K]}{\leq} N_{M/K}(M^\times) \underset{[M:K]}{\leq} K^\times .$$

Damit folgt

$$[N_{M/K}(M^\times) : J] = [L : M] = [I : J]$$

und somit  $I = N_{M/K}(M^\times)$ .

Zunächst sei  $\mu_m \subseteq K^\times$ . Für  $a \in K^\times$  sei  $L_a := K(\sqrt[m]{a}) = K(\sqrt[m]{ab^m})$ . Sei

$$L := \prod_{a \in K^\times / (K^\times)^m} L_a.$$

Dann ist  $L/K$  eine endliche, abelsche Erweiterung von Exponent  $m$ .

**Behauptung.**  $(K^\times)^m = N_{L/K}(L^\times) =: I_L$ .

*Beweis der Behauptung.* Wir wissen  $I_L = I_{\prod L_a} = \bigcap I_{L_a}$ . Es gilt:

$$[L_a : K] = [K(\sqrt[m]{a}) : K] = d|m$$

Daraus folgt  $(K^\times)^m \subseteq (K^\times)^d \subseteq I_{L_a}$  und somit insgesamt  $(K^\times)^m \subseteq I_L$ .

Aus der Kummertheorie erhalten wir

$$[K^\times : (K^\times)^m] = |\text{Gal}(L|K)| = [K^\times : I_L] \quad (3.7)$$

und somit  $(K^\times)^m = I_L$ . □

Zum allgemeinen Fall: Sei  $K_1 := K(\mu_m)$ . Sei  $L/K_1$  abelsch mit  $(K_1^\times)^m = N_{L/K_1}(L^\times)$ . Sei  $\tilde{L}/L$  endlich, sodass  $\tilde{L}/K$  galoissch ist:

$$\begin{array}{c} \tilde{L} \\ | \\ L \\ | \\ K_1 \\ | \\ K \end{array} \left. \begin{array}{l} \text{abelsch} \\ \text{galoissch} \end{array} \right\}$$

Es gilt:

$$\begin{aligned} N_{\tilde{L}/K}(\tilde{L}^\times) &= N_{K_1/K}(N_{\tilde{L}/K_1}(\tilde{L}^\times)) \\ &\subseteq N_{K_1/K}(N_{L/K_1}(L^\times)) \\ &= N_{K_1/K}((K_1^\times)^m) \\ &= (N_{K_1/K}(K_1^\times))^m \subseteq (K^\times)^m \end{aligned}$$

Also ist  $(K^\times)^m$  auch eine Normengruppe. □

**Satz 3.67.** Sei  $I \leq K^\times$ . Folgende Aussagen sind äquivalent:

- (1)  $I$  ist Normengruppe.
- (2)  $I$  ist offen von endlichem Index.
- (3)  $I$  ist abgeschlossen von endlichem Index.
- (4)  $[K^\times : I] < \infty$ .

*Beweis.* (1) $\iff$ (2) ist der Existenzsatz 3.65 zusammen mit der Vorbemerkung.

(2) $\iff$ (3) gilt nach Blatt 10, Aufgabe 1.

(2) $\implies$ (4) ist klar.

Für (4) $\implies$ (2) sei  $m := [K^\times : I]$ , dann folgt  $(K^\times)^m \leq I$ . Mit  $a \in I$  ist auch  $a(K^\times)^m \subseteq I$  und wir erhalten

$$I = \bigcup_{a \in I} \underbrace{a(K^\times)^m}_{\text{offen}}$$

ist offen. □

**Satz 3.68.** Die Normengruppen sind genau die Obergruppen von

$$\langle \pi_K^f \rangle \times U_K^n$$

mit  $f \in \mathbb{N}$  und  $n \in \mathbb{N}_0$ .

*Beweis.* Wir zeigen, dass  $\langle \pi_K^f \rangle \times U_K^n \subseteq K^\times$  endlichen Index hat. Es gilt

$$[K^\times : \langle \pi_K^f \rangle \times U_K^n] = \begin{cases} f, & n = 0 \\ f(q_K - 1) \underbrace{[U_K^1 : U_K^n]}_{q_K^{n-1}}, & n > 0 \end{cases}$$

Also ist jede Obergruppe eine Normengruppe. Sei umgekehrt  $I$  eine Normengruppe. Dann existiert ein  $n$  mit  $U_K^n \subseteq I$  und  $\pi_K^f \in I$ , z.B. für  $f = [K^\times : I]$ . □

### Kummertheorie

Sei  $K$  ein Körper,  $m \in \mathbb{N}$  und  $\text{char}(K) = 0$ . Betrachte

$$0 \longrightarrow \mu_m \longrightarrow (K^c)^\times \xrightarrow{m} (K^c)^\times \longrightarrow 0.$$

Sei  $G = G_K = \text{Gal}(K^c|K)$ . Dann gilt

$$0 \longrightarrow \mu_m(K) \longrightarrow K^\times \xrightarrow{m} K^\times \longrightarrow H^1(G, \mu_m) \longrightarrow 0$$

wegen Hilberts Satz 90. Dann folgt

$$H^1(G, \mu_m) \cong K^\times / (K^\times)^m.$$

Dieser Isomorphismus heißt *Kummerisomorphismus*.

Falls der Körper  $K$  die  $m$ -ten Einheitswurzeln  $\mu_m$  enthält, kann man dieses Resultat verfeinern und erhält auch für nicht algebraisch abgeschlossene Körper sogenannte *Kummerisomorphismen*. Hierfür sei auf [NS11, S. 128/129] verwiesen, wo der Satz (1.3) die Lücke in (3.7) schließt.

## **Anmerkungen zur Klausur (vgl. Vorlesungshomepage)**

Die Klausur wird am 25.7. von 12:15 Uhr bis 13:45 Uhr anstelle des Tutoriums im Raum B252 stattfinden. Sie wird eine Kombination aus Übungsaufgaben und „wahr/falsch“-Fragen (ohne Begründungen) sein. Um pünktlich anfangen zu können, sollten alle Teilnehmer bereits um 12:00 Uhr anwesend sein.

## Literatur

- [CNT87] Cassou-Noguès, Philippe und Taylor, Martin J.: *Elliptic functions and rings of integers*, Band 66. Birkhäuser, 1987.
- [Coh12] Cohen, Henri: *Advanced topics in computational number theory*, Band 193. Springer Science & Business Media, 2012.
- [Lan13] Lang, Serge: *Algebraic number theory*, Band 110. Springer Science & Business Media, 2013.
- [Neu06] Neukirch, Jürgen: *Algebraische Zahlentheorie*. Springer-Verlag, Berlin Heidelberg New York, 2006, ISBN 978-3-540-37663-7.
- [NS11] Neukirch, Jürgen und Schmidt, Alexander: *Klassenkörpertheorie*. Neu herausgegeben von Alexander Schmidt, Springer-Verlag, Berlin Heidelberg New York, 1. Auflage, 2011, ISBN 978-3-642-17325-7.
- [NSW13] Neukirch, Jürgen, Schmidt, Alexander und Wingberg, Kay: *Cohomology of number fields*, Band 323. Springer Science & Business Media, 2013.
- [Ser13] Serre, Jean Pierre: *Local fields*, Band 67. Springer Science & Business Media, 2013.
- [Was97] Washington, Lawrence C.: *Introduction to cyclotomic fields*, Band 83. Springer Science & Business Media, 1997.