Algebraische Zahlentheorie 2
Prof. Dr. Werner Bley
Sommersemester 2017

Pascal Stucky

22. Juli 2017

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

Inhaltsverzeichnis

Literatur

- Grundlage für die Vorlesung: [NS11]
- Grundlage für das Vorwissen (Dedekindringe, Ganzheitsringe, Zerlegungsgesetze, Dirichletscher Einheitensatz, 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 (idealtheoretisch)

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 τ (bzw. durch $\sigma, \overline{\sigma}$) einen Betrag

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

bzw.

$$|\alpha|_\sigma := |\sigma(\alpha)| = |\overline{\sigma}(\alpha)| \qquad \forall \alpha \in k\,.$$

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

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

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 ∞ 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 ∞_1 und ∞_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

$$\alpha \equiv 1 \mod {}^*\mathfrak{m}$$

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 σ in $\mathfrak{m}_\infty$.

(2) Die Gruppe

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

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

$$\varepsilon\alpha \equiv 1 \mod {}^*\mathfrak{m}$$

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 $\pi : ({}^{\mathbb{Z}}/_{n\mathbb{Z}})^\times \longrightarrow cl_{\mathbb{Q}}((n))$ induziert von

$$\overline{a} \longmapsto a\mathbb{Z} = (a)\,.$$

Diese ist wohldefiniert:

Angenommen $a \equiv b \mod n$. Es gilt

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

Man rechnet

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

und erhält Wohldefiniertheit. Weiter ist π 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 $\pi(\overline{a}_1 \overline{a}_2^{-1}) = \left(\frac{a_1}{a_2}\right) \mathcal{P}_{\mathbb{Q}}((n))$ und somit ist π surjektiv.

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

$$0 \longrightarrow \{\pm\overline{1}\} \hookrightarrow ({}^{\mathbb{Z}}/_{n\mathbb{Z}})^\times \overset{\pi}{\twoheadrightarrow} cl_{\mathbb{Q}}((n)) \longrightarrow 0$$

exakt.

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

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

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

Notation.
- Wir schreiben

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

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

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

Dies ist unabhängig von der Wahl von β und γ.

Betrachte nun die Abbildung

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

Mithilfe des starken Approximationssatzes, lässt sich die Surjektivität von ρ zeigen.

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

$$\begin{array}{ccccccccccccc} 0 \longrightarrow \mathcal{O}_k^\times \cap k_\mathfrak{m}^\times \longrightarrow \mathcal{O}_k^\times & \xrightarrow{\quad\rho\quad} & (\mathcal{O}_k/\mathfrak{m})^\times & \longrightarrow & cl_k(\mathfrak{m}) & \longrightarrow & cl_k \longrightarrow 0 \\ u & \longmapsto & (\overline{u}, (\operatorname{sgn}(\sigma(u)))_{\sigma\in\mathfrak{m}_\infty}) & & \mathfrak{a}\mathcal{P}_k(\mathfrak{m}) & \longmapsto & \mathfrak{a}\mathcal{P}_k \\ & & \rho(\alpha) & \longmapsto & (\alpha)\mathcal{P}_k(\mathfrak{m}) & & \end{array}$$

Tipp: [Coh12, Prop.3.2.3].

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

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

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 $\overline{K} := \kappa(\mathfrak{P}) := \mathcal{O}_K/\mathfrak{P}$ ist eine endliche Erweiterung von $\overline{k} := \kappa(\mathfrak{p}) := \mathcal{O}_k/\mathfrak{p}$ mit Restklassengrad $f(\mathfrak{P}|\mathfrak{p}) := [\overline{K} : \overline{k}]$. Die Galoisgruppe $G := \operatorname{Gal}(\overline{K}|\overline{k})$ ist zyklisch und wird erzeugt vom *Frobenius*

$$x \longmapsto x^q \qquad \forall x \in \overline{K} ,$$

wobei $q = \left|\overline{k}\right| = N_{k/\mathbb{Q}}(\mathfrak{p})$.
Sei

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

die *Zerlegungsgruppe* und

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

die *Verzweigungsgruppe* oder *Trägheitsgruppe.*
Es gilt: Die Sequenz

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

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

$$\sigma_{\mathfrak{P}}(\alpha) \equiv \alpha^{N_{k/\mathbb{Q}}(\mathfrak{p})} \mod \mathfrak{P} \qquad \forall \alpha \in \mathcal{O}_K$$

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

$$\begin{aligned} & \sigma_{\mathfrak{P}}(\tau^{-1}(\alpha)) \equiv \tau^{-1}(\alpha)^{N\mathfrak{p}} \mod \mathfrak{P} && \forall \alpha \in \mathcal{O}_K \\ \Longrightarrow \quad & (\tau\sigma_{\mathfrak{P}}\tau^{-1})(\alpha) \equiv \alpha^{N\mathfrak{p}} \mod \mathfrak{P}' && \forall \alpha \in \mathcal{O}_K \\ \Longrightarrow \quad & \sigma_{\mathfrak{P}'} = \tau\sigma_{\mathfrak{P}}\tau^{-1} \end{aligned}$$

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 $\mathfrak{p} \longmapsto \sigma_{\mathfrak{p}}$ einen Homomorphismus

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

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

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

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 $\tau, \overline{\tau} : k \hookrightarrow \mathbb{C}$ wobei $\tau(k) \nsubseteq \mathbb{R}$.
Sei w eine Stelle über v, d.h. w entspricht entweder einer reellen Einbettung $\sigma : K \hookrightarrow \mathbb{R}$ oder einem Paar komplexer Einbettungen $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$ wobei $\sigma(K) \nsubseteq \mathbb{R}$ und $\sigma|_k = \tau$.

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

Dies ist wohldefiniert, denn:

(1) Falls σ reell ist, ist nichts zu zeigen.

(2) Falls σ komplex ist, so ist zu zeigen $\overline{\sigma} \circ g = \overline{\sigma \circ g}$. Dies gilt offensichtlich.

Betrachte nun eine Stelle $w|v$ mit korrespondierender Einbettung σ 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

$$\begin{tikzcd} k(\alpha) = K \arrow[r, hook, "\sigma"] \arrow[d, dash, "n"] & \mathbb{C} \arrow[d, equal] \\ k \arrow[r, hook, "\tau"] & \mathbb{C} \end{tikzcd}$$

Aus der Algebra ist bekannt, dass es n verschiedene Fortsetzungen von τ gibt. Falls $\sigma_0 : K \longrightarrow \mathbb{C}$ 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* σ *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

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

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:*

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

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:

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

Erinnerung 1.19. Für zyklotomische Erweiterungen gilt

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) &\cong ({}^{\mathbb{Z}}\!/_{n\mathbb{Z}})^\times \\ (\zeta_n \overset{\sigma_a}{\mapsto} \zeta_n^a) &\leftarrow\!\shortmid \overline{a} \end{aligned}$$

Die Artinabbildung ist von der Form

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

<u>Ziel</u>: 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.

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

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

Beispiel 1.20. Betrachte

$$\begin{tikzcd} \mathbb{Q}(\zeta_n) \arrow[r, leftrightarrow] \arrow[d, dash] & \mathcal{P}_{\mathbb{Q}}(n\mathbb{Z}\infty) \arrow[d, dash] \\ \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n)^+ \arrow[r, leftrightarrow] \arrow[d, dash] & \mathcal{P}_{\mathbb{Q}}(n\mathbb{Z}) \\ \mathbb{Q} & \end{tikzcd}$$

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 $cl_k \cong \mathrm{Gal}(k(1)|k)$ *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. □

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:

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

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:*

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

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 $n \equiv 2 \mod 4$, d.h. $n = 2n_1$ mit n_1 ungerade. Dann ist $[k((n)\infty) : k] = \varphi(n)$ (φ bezeichnet die Eulersche φ-Funktion, d.h. $\varphi(n) = \left|({}^{\mathbb{Z}}/_{n\mathbb{Z}})^{\times}\right|$).

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 μ_k die Gruppe der Einheitswurzeln in k bezeichnet, und

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

Übung 1.28. *Es gilt*

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

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

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

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

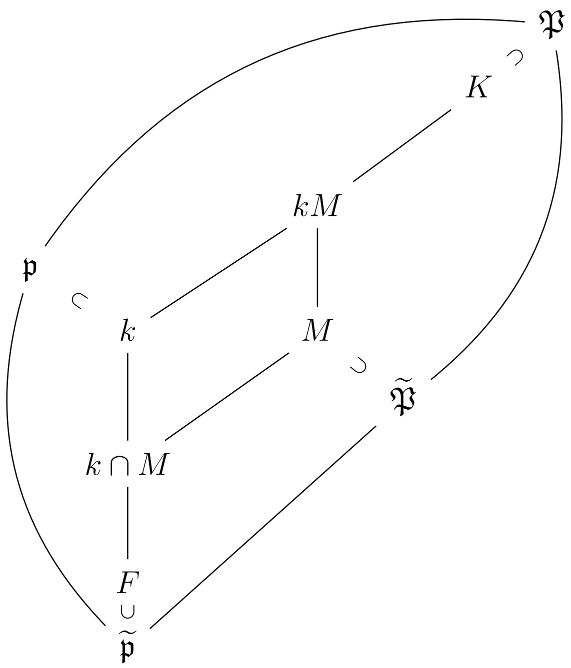
Also gilt $k(2) = k(1)$ falls 2 zerlegt ist in $k/\mathbb{Q}$.

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 $\widetilde{\mathfrak{p}}, \mathfrak{p}$ und $\widetilde{\mathfrak{P}}$ unter $\mathfrak{P}$ liegen. Es seien M/F und K/k abelsch, dann ist Abbildung

$$\mathrm{Gal}(K|k) \twoheadrightarrow \mathrm{Gal}(M|k \cap M) \subseteq \mathrm{Gal}(M|F)$$

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

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

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

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

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

und

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

Ferner gilt

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

Es folgt also

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

oder allgemeiner

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

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

Anwendung. Betrachte den Fall

$$\begin{tikzcd}
 & & k(1) = K \\
 & kM \arrow[ur, dash] \arrow[d, dash] & \\
k \arrow[ur, dash] & F(1) = M & \\
k \cap M \arrow[u, dash] \arrow[ur, dash] & & \\
F \arrow[u, equal] & &
\end{tikzcd}$$

Dann ist die Restriktionsabbildung

$$\mathrm{Gal}(K|k) \overset{\text{res}}{\twoheadrightarrow} \mathrm{Gal}(M|F)$$

surjektiv und das Diagramm

$$\begin{tikzcd}
cl_k = \mathcal{I}_k/\mathcal{P}_k \arrow[r, "(\,\text{—}\,{,}K/k)", "\cong"'] \arrow[d, two heads, "N_{k/F}"] & \mathrm{Gal}(K|k) \arrow[d, two heads, "\text{res}"] \\
cl_F = \mathcal{I}_F/\mathcal{P}_F \arrow[r, "(\,\text{—}\,{,}M/F)", "\cong"'] & \mathrm{Gal}(M|F)
\end{tikzcd}$$

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 $v_p : \mathbb{Q}_p^\times \longrightarrow \mathbb{Z}$ ($v_p(0) := \infty$) und Absolutbetrag $|\alpha|_p = p^{-v_p(\alpha)}$. Dann ist

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

und

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

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

k ist Quotientenkörper des diskreten Bewertungsrings $\mathcal{O}_k$ 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

$$v_k : k \longrightarrow \mathbb{Z} \cup \{\infty\}$$
$$v_k\big|_{\mathbb{Q}_p} = ev_p$$

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

Der zugehörige Absolutbetrag ist definiert als

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

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

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

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 $\overline{k} = \mathcal{O}_k/\mathfrak{p}_k$. 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,

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

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:

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

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

$$\begin{aligned} 0 \longrightarrow G_0 \hookrightarrow G &\twoheadrightarrow \mathrm{Gal}(\overline{K}|\overline{k}) \longrightarrow 0 \\ \sigma &\longmapsto (\overline{a} \mapsto \overline{\sigma(a)}) \end{aligned}$$

ist exakt, wobei

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

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

$$\begin{aligned} G &\xrightarrow{\cong} \mathrm{Gal}(\overline{K}|\overline{k}) \\ \sigma_{K/k} &\longmapsto (x \mapsto x^{|\overline{k}|}) \end{aligned}$$

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) $H_1 \cap H_2 \longleftrightarrow K_1 K_2$,

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

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 Komplettierung 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 α 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 $N_{K/k} : \mathcal{J}_K \longrightarrow \mathcal{J}_k$ 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 $N_{K/k} : \mathcal{C}_K \longrightarrow \mathcal{C}_k$.

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

$$\alpha \equiv 1 \mod {}^*\mathfrak{m}\,,$$

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

$$\mathcal{J}_k(\mathfrak{m}) := \{\alpha = (\alpha_v)_v \in \mathcal{J}_k \,|\, \alpha \equiv 1 \mod {}^*\mathfrak{m}\} \leq \mathcal{J}_k$$

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

$$\begin{tikzcd} \mathcal{J}_k(\mathfrak{m}) \arrow[r, "\subseteq"] \arrow[rr, bend right, "\psi"'] & \mathcal{J}_k \arrow[r] & \mathcal{J}_k/k^\times \end{tikzcd}$$

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* $|\cdot|_1, ..., |\cdot|_n$ *paarweise inäquivalente Beträge auf* k. *Seien* $a_1, ..., a_n \in k$. *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

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

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 $\mathrm{sgn}(\sigma(\beta)) = \mathrm{sgn}(\alpha_v)$. Wähle

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

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

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

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

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

für alle $v|\mathfrak{m}$. Dann folgt

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

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

Definition 1.44. Der Homomorphismus

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

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]. $\square$

Betrachte das kommutative Diagramm

$$\begin{tikzcd}
 & \mathcal{J}_k(\mathfrak{m}) / (k^\times N_{K/k}(\mathcal{J}_k))_{\mathfrak{m}} \arrow[r, "\cong"] \arrow[d, "\text{siehe Lemma 1.42}"', "\cong"] & \mathcal{I}_k(\mathfrak{m}) / \mathcal{P}_k(\mathfrak{m}) N_{K/k}(\mathcal{I}_K(\mathfrak{m}_0 \mathcal{O}_K)) \arrow[d, "\cong"', "(_\,{,}K/k)"] \\
 & \mathcal{J}_k / k^\times N_{K/k}(\mathcal{J}_K) \arrow[r, "\Theta"] & \mathrm{Gal}(K|k) \\
\mathcal{J}_k \arrow[ur, dashed] \arrow[urr, dashed, "(_\,{,}K/k)"'] & &
\end{tikzcd}$$

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

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

Bemerkung 1.48. Sei $\alpha = (\alpha_v)_v \in \mathcal{J}_k$ und K/k modulo $\mathfrak{m}$ definiert. Finde mit dem Approximationssatz $\beta \in k^\times$ 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 $(\_\,, K/k) : \mathcal{J}_k \longrightarrow \mathrm{Gal}(K|k)$ einen Isomorphismus*

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

(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

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

(2) Mittels der Zuordnung

$$\begin{tikzcd}
\mathcal{J}_k \arrow[r] \arrow[d, dash] & \mathcal{C}_k \arrow[d, dash] \\
H \arrow[r] \arrow[d, dash] & U \arrow[d, dash] \\
k^\times \arrow[r] & 1
\end{tikzcd}$$

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) $H_1 \leq H_2 \Longleftrightarrow K_1 \supseteq K_2$,

(ii) $H_1H_2 \longleftrightarrow K_1 \cap K_2$,

(iii) $H_1 \cap H_2 \longleftrightarrow K_1K_2$.

(4) Betrachte die Situation

$$\begin{tikzcd}
 & & K \arrow[dl, dash] \\
 & kM \arrow[dl, dash] \arrow[d, dash] & \\
k \arrow[d, dash] & M \arrow[dl, dash] & \\
k \cap M \arrow[d, dash] & & \\
F & &
\end{tikzcd}$$

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

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

Zusammenhang zum Lokalen

Sei K/k eine Galoiserweiterung von Zahlkörpern. Betrachte

$$\begin{tikzcd}
 & & K_{\mathfrak{P}} \arrow[d, dash, "\text{galoissch}"] \\
\mathfrak{P} \arrow[d, dash] & K \arrow[ur, dash] \arrow[d, dash, "Z"] \arrow[dd, dash, bend right, "G"'] & k_{\mathfrak{p}} \arrow[dl, dash] \\
\widetilde{\mathfrak{P}} \arrow[d, dash] & K^Z \arrow[d, dash] & \\
\mathfrak{p} & k &
\end{tikzcd}$$

wobei

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

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

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

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

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

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". $\Longrightarrow$: $\mathfrak{p}$ 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 $\iota_{\mathfrak{p}}(\mathcal{U}_{\mathfrak{p}}) \subseteq N_{K/k}(\mathcal{J}_K)$.
$\Longleftarrow$: 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

<u>Literatur</u>: Dieses Kapitel folgt [NS11].
G sei stets eine endliche Gruppe. Der *ganzzahlige Gruppenring* ist definiert als

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

$\mathbb{Z}[G]$ 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 μ_L ein $\mathbb{Z}[G]$-Modul.

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

$$1 \longrightarrow A \hookrightarrow E \overset{\pi}{\twoheadrightarrow} G \longrightarrow 1\,.$$

sei exakt. Dann können wir A als G-Modul betrachten mittels:
Wähle eine mengentheoretische Abbildung σ 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 σ.*

Definition 2.3. (1) Die Abbildung

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

heißt *Augmentation*. Der Kern von ε 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 $J_G := \operatorname{coker}(\mu) = {}^{\mathbb{Z}[G]}/_{\mathbb{Z} \cdot N_G}$.

Wir haben also die exakten Sequenzen

$$0 \longrightarrow I_G \hookrightarrow \mathbb{Z}[G] \overset{\varepsilon}{\twoheadrightarrow} \mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow \mathbb{Z} \overset{\mu}{\hookrightarrow} \mathbb{Z}[G] \twoheadrightarrow J_G \longrightarrow 0$$

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

$$\{g - 1 \,|\, g \in G \setminus \{1\}\}\,.$$

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

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

(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* $I_G = \mathrm{Ann}_{\mathbb{Z}[G]}(\mathbb{Z} \cdot N_G)$ *und* $\mathbb{Z} \cdot N_G = \mathrm{Ann}_{\mathbb{Z}[G]}(I_G)$.

Sei nun A ein G-Modul.

Definition 2.6. Die Menge

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

heißt der *Fixmodul* und die Teilmenge

$$N_G A := \{N_G a \,|\, a \in A\}$$

heißt die *Normengruppe* von A. Weiter ist

$${}_{N_G}A := \{a \in A \,|\, N_G a = 0\}$$

der Kern der Norm und wir definieren den Teilmodul

$$I_G A := \Big\{ \sum_{g \neq 1} a_g(ga - a) \,|\, a \in A,\, a_g \in \mathbb{Z} \Big\} \subseteq {}_{N_G}A$$

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

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

und falls L/K abelsch ist folgt

$$H^{-2}(G, \mathbb{Z}) \cong \mathrm{Gal}(L|K) \overset{Artin}{\cong} {}^{K^\times}\!/_{N_{L/K}(L^\times)} \cong H^0(G, L^\times)\,.$$

Etwas ausführlicher: $\mathrm{Gal}(L/K)$ 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

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

definieren.

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

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

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

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

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 $\omega_1, ..., \omega_n$ mit $n = [K : Q]$ 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*

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

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

$$0 \longrightarrow \mathrm{Hom}_G(X, A) \hookrightarrow \mathrm{Hom}_G(X, B) \twoheadrightarrow \mathrm{Hom}_G(X, C) \longrightarrow 0$$

exakt.

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

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_G(\mathbb{Z}[G], A) \arrow[r, hook, "h^*"] \arrow[d, "f\mapsto f(1)", "\cong"'] & \mathrm{Hom}_G(\mathbb{Z}[G], B) \arrow[r, two heads, "g^*"] \arrow[d, "h\circ f\mapsto h(f(1))"', "\cong"] & \mathrm{Hom}_G(\mathbb{Z}[G], C) \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & A \arrow[r, hook] & B \arrow[r, two heads] & C \arrow[r] & 0
\end{tikzcd}$$

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 $\mathrm{Hom}_G(X, \_)$.
Genauer sei $X = \bigoplus_{j\in J} X_j$ für G-Moduln X_j. Dann ist

$$\begin{aligned}
\mathrm{Hom}_G\Big(\bigoplus_{j\in J} X_j, A\Big) &\longrightarrow \prod_{j\in J} \mathrm{Hom}_G(X_j, A) \\
f &\longmapsto (f|_{X_j})_{j\in J} \\
\Big(\sum_{j\in J} x_j \mapsto \sum_{j\in J} f_j(x_j)\Big) &\longleftarrow (f_j)_{j\in J}
\end{aligned}$$

ein Isomorphismus. □

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

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

ist exakt.

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

Beweis zu (1). Sei $f \in \mathrm{Hom}_G(X, A)$, dann ist $(g^* \circ h^*)(f) = g \circ h \circ f = 0$, d.h. $\mathrm{im}(h^*) \subseteq \ker(g^*)$.
Sei nun $f_2 \in \mathrm{Hom}_G(X, B)$ und es gelte $g \circ f_2 = 0$, d.h. $\mathrm{im}(f_2) \subseteq \ker(g) = \mathrm{im}(h)$. Wir suchen f_1, sodass

$$\begin{tikzcd}
X \arrow[r, "f_2"] \arrow[dr, dashed, "f_1"'] & B \\
& A \arrow[u, "h"']
\end{tikzcd}$$

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

$$\begin{tikzcd}
& X \arrow[d] \arrow[dl, dashed, "\exists"'] & \\
V \arrow[r] & W \arrow[r] & 0
\end{tikzcd}$$

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

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

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

$$\begin{tikzcd} & X \arrow[dl, dashed, "f_2"'] \arrow[d, "f_3"] & \\ V \arrow[r, "h"] & W \arrow[r] & 0 \end{tikzcd}$$

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) $\mathrm{Hom}_G(X, \_)$ 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

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, hook] & B \arrow[r, two heads, "\pi"] & X \arrow[r] \arrow[l, dashed, bend left, "\sigma"] & 0 \end{tikzcd}$$

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

Drei Lemmata (ohne Beweis)

Lemma 2.14. *Ist*

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

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

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

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

$$\begin{aligned} 0 \longrightarrow \mathbb{Z} \xhookrightarrow{n} \mathbb{Z} &\twoheadrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \\ a \longmapsto na & \end{aligned}$$

für ein $n \in \mathbb{N}$.

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

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \arrow[r, "n"] \arrow[d, phantom, "\cong"] & \mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[d, phantom, "\cong"] & \mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \arrow[r] \arrow[d, phantom, "="] & 0 \\ 0 \arrow[r] & \mathbb{Z}/n\mathbb{Z} \arrow[r, "n"] & \mathbb{Z}/n\mathbb{Z} \arrow[r] & \mathbb{Z}/n\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

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

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

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

$$\ldots \longrightarrow 0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \longrightarrow 0 \longrightarrow \ldots$$

also

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

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

$$\begin{tikzcd} \ldots & X_{-2} \arrow[l] & X_{-1} \arrow[l, "d_{-1}"'] & & X_0 \arrow[ll, "d_0"'] \arrow[dl, "\varepsilon"] & X_1 \arrow[l, "d_1"'] & X_2 \arrow[l, "d_2"'] & \ldots \arrow[l] \\ & & & \mathbb{Z} \arrow[ul, "\mu"] \arrow[dl] & & & & \\ & & 0 & & 0 \arrow[ul] & & & \end{tikzcd}$$

sodass

(1) die X_q sind freie $\mathbb{Z}[G]$-Moduln,

(2) $\mu\varepsilon = d_0$,

(3) μ, ε, 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

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

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

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

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

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\varepsilon} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \longleftarrow ... \tag{2.1}$$

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

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(X_0, \mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(X_1, \mathbb{Z}) \longrightarrow ... \tag{2.2}$$

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

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

Die Abbildung

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

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

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

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

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

Somit wird aus (2.2) durch diese Dualisierung

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

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

Die expliziten Formeln ergeben sich ebenfalls aus (2.1) durch dualisieren. □

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

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

ist eine Sequenz von G-Moduln mit

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

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

Notation. Definiere

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

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

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

mittels $f \longmapsto f(1)$. Die Formeln für die d_q liefern nun für die ∂_q die Formeln

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

(siehe [NS11, S. 17] für die restlichen Formeln).
Beispielsweise hat man für $q = 0$

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

und die Formel für ∂_0 folgt aus

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

Ebenso hat man für $q = 1$

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

und die Formel für ∂_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 $q = -1$:

$$\begin{aligned} Z_{-1} &= \ker(N_G) = {}_{N_G}A\,, \\ B_{-1} &= \operatorname{im}(\partial_{-1}) = I_G A = \Big\{ \sum_{\sigma \neq 1} n_\sigma(\sigma(a) - a) \,|\, a \in A, n_\sigma \in \mathbb{Z} \Big\}\,, \\ H^{-1}(G, A) &= {}_{N_G}A / I_G A\,. \end{aligned}$$

Für $q = 0$ ergibt sich

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

Für $q = 1$ erhalten wir

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

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

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

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

$$\begin{tikzcd} ... \arrow[r] & A_{q-1} \arrow[r, "\partial_q"] \arrow[d, "f_{q-1}"] & A_q \arrow[r, "\partial_{q+1}"] \arrow[d, "f_q"] & A_{q+1} \arrow[r] \arrow[d, "f_{q+1}"] & ... \\ ... \arrow[r] & B_{q-1} \arrow[r, "\partial_q"] & B_q \arrow[r, "\partial_{q+1}"] & B_{q+1} \arrow[r] & ... \end{tikzcd}$$

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

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

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

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

exakt ist.

Definition 2.23. Die Abbildung δ_q heißt *Verbindungshomomorphismus*, die Sequenz 2.3 heißt *lange exakte Kohomologiesequenz.*

Beweis. Betrachte

$$\begin{tikzcd} 0 \arrow[r] & A_{q-1} \arrow[r, "i_{q-1}"] \arrow[d, "\partial_q"] & B_{q-1} \arrow[r, "j_{q-1}"] \arrow[d, "\partial_q"] & C_{q-1} \arrow[r] \arrow[d, "\partial_q"] & 0 \\ 0 \arrow[r] & A_q \arrow[r, "i_q"] \arrow[d, "\partial_{q+1}"] & B_q \arrow[r, "j_q"] \arrow[d, "\partial_{q+1}"] & C_q \arrow[r] \arrow[d, "\partial_{q+1}"] & 0 \\ 0 \arrow[r] & A_{q+1} \arrow[r, "i_{q+1}"] & B_{q+1} \arrow[r, "j_{q+1}"] & C_{q+1} \arrow[r] & 0 \end{tikzcd}$$

Die Zeilen sind exakt, da sie aus

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

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

Sei $\overline{c}_q \in H^q(G, C) = {}^{Z_q(C)}/_{B_q(C)} \subseteq {}^{C_q}/_{B_q(C)}$. Es gilt $\partial_{q+1}(c_q) = 0$. Sei $b_q \in B_q$ mit $j_q(b_q) = c_q$. Dann ist $\partial_{q+1}(b_q) \in \ker(j_{q+1}) = \mathrm{im}(i_{q+1})$ 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

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

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

Wohldefiniertheit: Folgt ebenfalls mittels Diagrammjagd:

Sei $\overline{c}_q = \overline{c'}_q$, 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 $b_q - b'_q \in \ker(j_q) = \mathrm{im}(i_q)$ 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

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

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

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

Es gilt nun $\overline{a}_{q+1} = 0$, 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

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

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*

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

bzw.

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

bzw.

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

Satz 2.25. *Falls*

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

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

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

Beweis. Das folgt direkt aus der Konstruktion von δ. □

Satz 2.26. *Sei*

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

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

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

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

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

- 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. $\mathrm{im}(I) \subseteq \ker(J)$. 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

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

$\square$

Behauptung 2. *Das folgende Diagramm ist kommutativ:*

$$\begin{tikzcd}
A' \arrow[r, "f_1"] & A \arrow[r, "f_2"] & A'' \arrow[r, "i''"] & B'' \arrow[r, "j''"] & C'' \\
A' \arrow[u, "\mathrm{id}"] \arrow[r, "I"] \arrow[d, "-\mathrm{id}"'] & A \oplus B' \arrow[u, "{(\mathrm{id},0)}"] \arrow[r, "J"] \arrow[d, "{(0,-\mathrm{id})}"'] & D \arrow[u, dashed] \arrow[r, "\subseteq"] \arrow[d, dashed] & B \arrow[u, "g_2"] \arrow[r, "j''\circ g_2"] \arrow[d, "j"'] & C'' \arrow[u, "\mathrm{id}"] \arrow[d, "\mathrm{id}"'] \\
A' \arrow[r, "i'"] & B' \arrow[r, "j'"] & C' \arrow[r, "h_1"] & C \arrow[r, "h_2"] & C''
\end{tikzcd}$$

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

$$\begin{tikzcd}
B'' \arrow[r, "j''"] & C'' \\
B \arrow[u, "g_2"] \arrow[r, "j''\circ g_2"] & C'' \arrow[u, "\mathrm{id}"]
\end{tikzcd}$$

  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:

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

Die Kommutativität der restlichen Rechtecke folgt analog. $\square$

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 $\ker(J) = \mathrm{im}(I)$ 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

$$\begin{tikzcd}
H^{q-1}(G, C'') \arrow[r] & H^q(G, A'') \arrow[r] & H^{q+1}(G, A') \\
H^{q-1}(G, C'') \arrow[r] \arrow[u, equal] \arrow[d, equal] & H^q(G, D) \arrow[r] \arrow[u] \arrow[d] & H^{q+1}(G, A') \arrow[u, "\mathrm{id}"'] \arrow[d, "-\mathrm{id}"'] \\
H^{q-1}(G, C'') \arrow[r] & H^q(G, C') \arrow[r] & H^{q+1}(G, A')
\end{tikzcd}$$

kommutiert wegen der Funktorialität des Verbindungshomomorphismus δ. Das ist die Aussage des Satzes. □

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

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

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

$$A_q = \mathrm{Hom}_G(X_q, A) \cong \bigoplus_{i\in I} \mathrm{Hom}_G(X_q, A_i) = \bigoplus_{i\in I} (A_i)_q$$
$$f \mapsto (\pi_i \circ f)_{i\in I}$$
$$(x \mapsto \sum_{i\in I} f_i(x)) \leftarrow\!\shortmid (f_i)_{i\in I}$$

(wohldefiniert, da die X_q endlich erzeugt sind).
Damit erhalten wir das unendliche kommutative Diagramm

$$\begin{tikzcd}
\ldots \arrow[r] & A_{q-1} \arrow[r] \arrow[d, "\cong"] & A_q \arrow[r] \arrow[d, "\cong"] & A_{q+1} \arrow[r] \arrow[d, "\cong"] & \ldots \\
\ldots \arrow[r] & \bigoplus_{i\in I}(A_i)_{q-1} \arrow[r] & \bigoplus_{i\in I}(A_i)_q \arrow[r] & \bigoplus_{i\in I}(A_i)_{q+1} \arrow[r] & \ldots
\end{tikzcd}$$

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

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

□

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

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

exakt ist.

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

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

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)

$$\ldots \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(X_q, D) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(X_{q+1}, D) \longrightarrow \ldots \tag{2.6}$$

Da die Sequenz

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

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

Betrachte

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

und

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

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

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

Für $m \geq 0$ erhält man

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

und für $m \leq 0$

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

Bemerkungen 2.37. (1) δ^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 $A_q = \mathrm{Hom}_G(X_q, A)$ 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

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

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

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

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

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0\,. \tag{2.7}$$

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

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

Wir können nun zeigen

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

denn wir erhalten aus (2.7)

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

und die Abbildung

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

ist ein Isomorphismus.

Definition 2.45. Die Gruppe

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

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

$$x : {}^{G}\!/\!_{U} \times \cdots {}^{G}\!/\!_{U} \longrightarrow A^U$$

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

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

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

Das Diagramm

$$\begin{tikzcd} (A^U)_q \arrow[r, "\partial_{q+1}"] \arrow[d, "\inf"] & (A^U)_{q+1} \arrow[d, "\inf"] \\ A_q \arrow[r, "\partial_{q+1}"] & A_{q+1} \end{tikzcd}$$

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

Definition 2.47. Die induzierte Abbildung

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

heißt *Inflation*.

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

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

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

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

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

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

Beweis.

- Exaktheit bei $H^1({}^{G}\!/\!_{U}, A^U)$:

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

  $$\inf(x)(\sigma) = x(\sigma U) = \sigma a - a$$

  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

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

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

- <u>Exaktheit bei $H^1(G, A)$</u>:

  Sei $x : {}^{G}\!/_{U} \longrightarrow A^U$ ein 1-Kozyklus. Dann gilt

  $$\mathrm{res}(\inf(x))(\tau) = \inf(x)(\tau) = x(\tau U) = x(\overline{1}) = 0\,,$$

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

  Sei umgekehrt $x : G \longrightarrow A$ ein 1-Kozyklus mit $\mathrm{Res}(\overline{x}) = 0$. Dann ist $\mathrm{res}(x)$ 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

  $$\begin{aligned} \rho : G &\longrightarrow A \\ \sigma &\longmapsto \sigma a - a \end{aligned}$$

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

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

  für alle $\tau \in U$ und $\overline{x'} = \overline{x}$ 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

  $$\begin{aligned} y : {}^{G}\!/_{U} &\longrightarrow A^U \\ \sigma U &\longmapsto x'(\sigma) \end{aligned}$$

  Wegen (2.8) ist dies wohldefiniert und wegen

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

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

□

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 $i = 1, ..., q-1$. Dann ist die Sequenz*

$$0 \longrightarrow H^q({}^{G}\!/_{U}, A^U) \xrightarrow{\mathrm{Inf}} H^q(G, A) \xrightarrow{\mathrm{Res}} H^q(U, A)$$

exakt.

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

Die Restriktion für $q = 0$

Betrachte

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

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

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

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

<u>Ziel</u>: 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

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

Dies ist wohldefiniert, da

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

$q = 0$ Definiere

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

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

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

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

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

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

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

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

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

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

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

Also ist

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

(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

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

mit:

(1) $\mathrm{Kor}_0(a + N_U A) = N_{G/U} a + N_G A$,

(2) Für jede exakte Sequenz von G-Moduln

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

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

$$\begin{tikzcd} H^q(U,C) \arrow[r, "\delta"] \arrow[d, "\mathrm{Kor}_q"] & H^{q+1}(U,A) \arrow[d, "\mathrm{Kor}_{q+1}"] \\ H^q(G,C) \arrow[r, "\delta"] & H^{q+1}(G,A) \end{tikzcd}$$

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

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

Kor_q wird definiert durch

$$\begin{tikzcd} H^0(U,A^q) \arrow[r, "\delta_U^q", "\cong"'] \arrow[d, "\mathrm{Kor}_0"] & H^q(U,A) \arrow[d, dashed, "\mathrm{Kor}_q"] \\ H^0(G,A^q) \arrow[r, "\delta_G^q", "\cong"'] & H^q(G,A) \end{tikzcd}$$

□

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*

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

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

Satz 2.56. *Es gilt*

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

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

$$\begin{aligned}\mathrm{Kor}_0(\mathrm{Res}_0(\overline{a})) = \mathrm{Kor}_0(a + N_U A) &= N_{G/U}a + N_G A\\ &\overset{a\in A^G}{=} (G:U)(a + N_G A)\,.\end{aligned}$$

Der allgemeine Fall folgt mittels Dimensionsverschiebung:
Betrachte

$$\begin{tikzcd} H^0(G,A^q) \arrow[r, "\mathrm{Kor}_0 \circ \mathrm{Res}_0"] \arrow[d, "\delta^q"', "\cong"] & H^0(G,A^q) \arrow[d, "\delta^q"', "\cong"] \\ H^q(G,A) \arrow[r, "\mathrm{Kor}_q \circ \mathrm{Res}_q"] & H^q(G,A) \end{tikzcd}$$

Dann gilt

$$(\mathrm{Kor}_q \circ Res_q)(\overline{x}) = \delta^q((G:U)(\delta^q)^{-1}(\overline{x})) = (G:U)(\overline{x})\,.$$

□

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

$$\begin{tikzcd} H^q(G,A) \arrow[r, "\bar{f}"] \arrow[d, shift left, "\mathrm{Res}"] & H^q(G,B) \arrow[d, shift left, "\mathrm{Res}"] \\ H^q(U,A) \arrow[r, "\bar{f}"] \arrow[u, shift left, "\mathrm{Kor}"] & H^q(G,B) \arrow[u, shift left, "\mathrm{Kor}"] \end{tikzcd}$$

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:

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

- $H^q(G,A)_p = \{\overline{x} \in H^q(G,A) \mid \operatorname{ord}(\overline{x}) = p^n \text{ für ein } n \in \mathbb{N}\}$,
- $H^q(G,A)_p = H^q(G,A) \otimes \mathbb{Z}_p = H^q(G, A \otimes \mathbb{Z}_p)$. 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*

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

Beweis. Betrachte

$$\begin{tikzcd} H^q(G,A)_p \arrow[rr, "(G:G_p)", "\cong"'] \arrow[dr, "\mathrm{Res}"'] & & H^q(G,A)_p \\ & H^q(G_p,A) \arrow[ur, "\mathrm{Kor}"'] & \end{tikzcd}$$

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

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

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

wobei $\pi : A \longrightarrow D$ 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.

<u>Ziel</u>: Berechne $H^q(G, I_L)$ für $g = -1, 0, 1$.

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
$$\begin{aligned} I_L(\mathfrak{p}) &\cong \mathbb{Z}[{}^{G}/{}_{G_{\mathfrak{P}}}] \\ \prod_\sigma \sigma(\mathfrak{P})^{a_\sigma} &\leftarrow\!\shortmid \sum_{\sigma \in {}^{G}/{}_{G_{\mathfrak{P}}}} a_\sigma \sigma \end{aligned}$$
  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:

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

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

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

Diese Abbildung

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

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 $\overline{a} \cup \overline{b} = \overline{a \otimes b}$,

(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

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

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

(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

$$\begin{tikzcd} H^p(G,A) \times H^q(G,B'') \arrow[r, "\cup"] \arrow[d, "(\mathrm{id},\delta)"] & H^{p+q}(G, A \otimes B'') \arrow[d, "(-1)^p\delta"] \\ H^p(G,A) \times H^{q+1}(G,B) \arrow[r, "\cup"] & H^{p+q+1}(G, A \otimes B) \end{tikzcd}$$

Zur Konstruktion:

$$\begin{tikzcd} H^0(G,A^p) \times H^0(G,B^q) \arrow[r, "\cup"] \arrow[d, "(\delta^p,\mathrm{id})"] & H^0(G, A^p \otimes B^q) = H^0(G, (A \otimes B^q)^p) \arrow[d, "\delta^p"] \\ H^p(G,A) \times H^0(G,B^q) \arrow[r, dashed, "\cup"] \arrow[d, "(\mathrm{id},\delta^q)"] & H^p(G, A \otimes B^q) = H^p(G, (A \otimes B)^q) \arrow[d, "(-1)^{pq}\delta^q"] \\ H^p(G,A) \times H^q(G,B) \arrow[r, dashed, "\cup"] & H^{p+q}(G, A \otimes B) \end{tikzcd}$$

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

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

für $a_0 \in A^G$ ein q-Kozyklus.

Satz 2.68. *Es gilt*

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

Eigenschaften des Cupprodukts

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

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

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

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

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

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

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

$$\mathrm{Kor}(\mathrm{Res}(\overline{a}) \cup \overline{b}) = \overline{a} \cup \mathrm{Kor}(\overline{b}) \, .$$

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

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

(5) Das Cupprodukt ist assoziativ.

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

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

mit

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

Beweis. Aus

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

folgt

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

und

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

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

$$a_1(\tau) = \tau a_0' - a_0' \tag{2.12}$$

für alle $\tau \in G$. Sei $a_0'' \in (A'')^G$ das Bild von a_0' in A''. Betrachte dazu

$$\begin{tikzcd}
0 \arrow[r] & A_0 \arrow[r] \arrow[d, "\partial"] & A_0' \arrow[r, "a_0' \mapsto a_0''"] \arrow[d, "\partial"] & A_0'' \arrow[r] \arrow[d, "\partial"] & 0 \\
0 \arrow[r] & A_1 \arrow[r] & A_1' \arrow[r] & A_1'' \arrow[r] & 0
\end{tikzcd}$$

Es gilt $\partial(a_0'')(\sigma) = \sigma a_0'' - a_0''$ und $\overline{a}_1 = \delta(\overline{a_0''})$. Damit folgt

$$\begin{aligned}
\overline{a}_1 \cup \overline{b}_{-1} &= \delta(\overline{a_0''}) \cup \overline{b}_{-1} = \delta(\overline{a_0''} \cup \overline{b}_{-1}) \\
&= \delta(\overline{a_0'' \otimes b_{-1}}) = \partial(\underbrace{\overline{a_0' \otimes b_{-1}}}_{\in H^{-1}(G, A \otimes B)}) \\
&\overset{\partial = N_G}{=} \overline{N_G(a_0' \otimes b_{-1})} = \overline{\sum_{\tau \in G} \tau a_0' \otimes \tau b_{-1}} \\
&\overset{(2.12)}{=} \overline{\sum_{\tau \in G} (a_1(\tau) + a_0') \otimes \tau b_{-1}} \\
&= \overline{\sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1}} + \overline{a_0' \otimes \underbrace{N_G b_{-1}}_{=0}}
\end{aligned}$$

□

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

Erinnerung 2.70. Es gilt

$$\begin{aligned}
H^{-2}(G, \mathbb{Z}) &\cong G^{ab} \\
\overline{\sigma} &\leftarrow\!\shortmid \sigma G'
\end{aligned}$$

Der Isomorphismus folgt aus der Sequenz

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

und ist gegeben durch

$$\begin{array}{ccccccc}
H^{-2}(G, \mathbb{Z}) & \xrightarrow{\cong} & H^{-1}(G, I_G) & = & I_G/I_G^2 & \longrightarrow & G^{ab} \\
\overline{\sigma} & \longmapsto & & & (\sigma - 1) + I_G^2 & \longmapsto & \sigma G'
\end{array} \tag{2.13}$$

Lemma 2.71. *Es gilt*

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

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:

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

Zur rechten Seite betrachte

$$a_1(\sigma) \otimes 1 \longmapsto a_1(\sigma)$$

$$\begin{tikzcd}
0 \arrow[r] & A \otimes I_G \arrow[r] \arrow[d, "\partial"] & A \otimes \mathbb{Z}[G] \arrow[r] \arrow[d, "\partial"] & A \arrow[r] \arrow[d, "\partial"] & 0 & q = -1 \\
0 \arrow[r] & A \otimes I_G \arrow[r] & A \otimes \mathbb{Z}[G] \arrow[r] & A \arrow[r] & 0 & q = 0
\end{tikzcd}$$

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

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

Für die linke Seite gilt

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

wobei das erste δ den Verbindungshomomorphismus zur Sequenz

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

bezeichnet, während das zweite δ 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 $\overline{y}_0 = \overline{x}_0 \in H^0(G, A \otimes I_G)$.

$\square$

Anwendung. Sei $\overline{a}_2 \in H^2(G, A)$. Dann ist

$$\overline{a}_2 \cup \_ \; : H^{-2}(G, \mathbb{Z}) \longrightarrow H^0(G, A)$$

ein Gruppenhomomorphismus.

Satz 2.73. *Es gilt*

$$\overline{a}_2 \cup \overline{\sigma} = \overline{\sum_{\tau \in G} a_2(\tau, \sigma)}$$

Bemerkung 2.74. Es gilt $\sum_{\tau \in G} a_2(\tau, \sigma) \in A^G$ (leichte Übung).

Beweis. Betrachte

$$\begin{aligned} &0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G] \longrightarrow J_G \longrightarrow 0 \\ &0 \longrightarrow A \longrightarrow \underbrace{A \otimes \mathbb{Z}[G]}_{=:A'} \longrightarrow \underbrace{A \otimes J_G}_{=:A''} \longrightarrow 0 \end{aligned}$$

Wegen $H^2(G, A') = 0$ gibt es eine 1-Kokette $a_1' \in A_1'$ mit $a_2 = \partial a_1'$, d.h.

$$a_2(\tau, \sigma) = \tau a_1'(\sigma) - a_1'(\tau\sigma) + a_1'(\tau) \tag{2.14}$$

für alle $\tau, \sigma \in G$. Betrachte

$$\begin{tikzcd} & & a_1' \arrow[r, mapsto] & a_1'' & \\ 0 \arrow[r] & A_1 \arrow[r] \arrow[d, "\partial"] & A_1' \arrow[r] \arrow[d, "\partial"] & A_1'' \arrow[r] \arrow[d, "\partial"] & 0 \\ 0 \arrow[r] & A_2 \arrow[r] & A_2' \arrow[r] & A_2'' \arrow[r] & 0 \end{tikzcd}$$

Dann ist a_1' ein 1-Kozyklus, da a_2 eine 2-Kokette mit Werten in A ist.
Es gilt $\delta\overline{a_1''} = \overline{a}_2$ und man berechnet

$$\begin{aligned} \overline{a}_2 \cup \overline{\sigma} &= \delta\overline{a_1''} \cup \overline{\sigma} = \delta(\overline{a_1''} \cup \overline{\sigma}) \\ &\overset{2.71}{=} \delta(\overline{a_1''(\sigma)}) = \overline{\partial(a_1'(\sigma))} \\ &= \overline{\sum_{\tau \in G} \tau a_1(\sigma)} \overset{(2.14)}{=} \overline{\sum_{\tau \in G} a_2(\tau, \sigma) + a_1'(\tau\sigma) - a_1'(\tau)} \\ &= \overline{\sum_{\tau \in G} a_2(\tau, \sigma)} \end{aligned}$$

$\square$

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

$$\begin{tikzcd}
H^2(G,A) \arrow[r, "\cong"] & H^0(G,A) \arrow[r] & H^0(G,B) \arrow[dr] & \\
H^1(G,C) \arrow[u] \arrow[ur] \arrow[r, "\cong"] & H^{-1}(G,C) \arrow[u] & & H^0(G,C) \arrow[dl] \\
& H^1(G,B) \arrow[ul] & H^1(G,A) \arrow[l] &
\end{tikzcd}$$

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. $\square$

Satz 2.80. *Sei $|A| < \infty$. Dann gilt $h(A) = 1$.*

Beweis. Die Sequenz

$$\begin{gathered} 0 \longrightarrow A^G \longrightarrow A \xrightarrow{\sigma - 1} A \longrightarrow {}^{A}/_{I_G A} \longrightarrow 0 \\ a \longmapsto \sigma a - a \end{gathered}$$

ist exakt. Also folgt $\left|A^G\right| = |{}^{A}/_{I_G A}|$. Aus

$$\begin{gathered} 0 \longrightarrow H^{-1}(G,A) \longrightarrow {}^{A}/_{I_G A} \xrightarrow{N_G} A^G \longrightarrow H^0(G,A) \longrightarrow 0 \\ a + I_G A \longmapsto N_G a \end{gathered}$$

folgt nun $|H^1(G,A)| = |H^{-1}(G,A)| = |H^0(G,A)|$. $\square$

Korollar 2.81. *Sei $f : A \longrightarrow B$ 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

$$\begin{tikzcd} 0 \arrow[r] & \ker(f) \arrow[r] & A \arrow[rr, "f"] \arrow[dr, two heads, "f"'] & & B \arrow[r] & \operatorname{coker}(f) \arrow[r] & 0 \\ & & & W \arrow[ur, hook] & & & \end{tikzcd}$$

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

$$\varphi(A) := \frac{|{}^{A}/_{pA}|}{\left|\ker(A \xrightarrow{p} A)\right|}\,,$$

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

$$A \cong A_{tor} \oplus \mathbb{Z}^r$$

mit A_{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* $\operatorname{coker}(p), \ker(p)$ *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 α und β die Ränge von A und A^G, d.h. $A \cong A_{tor} \oplus \mathbb{Z}^\alpha$ und $A^G \cong (A^G)_{tor} \oplus \mathbb{Z}^\beta$. Dann gilt*

$$h(A) = p^{(p\beta-\alpha)/(p-1)}$$

Beweis. Betrachte

$$0 \longrightarrow A_{tor} \longrightarrow A \longrightarrow A_{tf} \longrightarrow 0$$

mit $A_{tf} := {}^{A}\!/_{A_{tor}}$. Daraus erhalten wir die exakte Sequenz

$$0 \longrightarrow (A_{tor})^G \longrightarrow A^G \longrightarrow (A_{tf})^G \longrightarrow H^1(G, A_{tor})\,.$$

Damit folgt $\operatorname{rg}(A^G) = \operatorname{rg}((A_{tf})^G)$ und ferner gilt

$$h(A) = h(A_{tor}\cdot)h(A_{tf}) = h(A_{tf})\,.$$

Es folgt

$$h(A)^{p-1} = h(A_{tf})^{p-1} \overset{2.86}{=} \frac{\varphi((A_{tf})^G)^p}{\varphi(A_{tf})}\,.$$

Nach Definition erhalten wir

$$\varphi(A_{tf}) = \frac{\left|{}^{A_{tf}}\!/_{pA_{tf}}\right|}{\left|\ker(A_{tf} \xrightarrow{p} A_{tf})\right|} = \left|{}^{A_{tf}}\!/_{pA_{tf}}\right| = p^\alpha$$

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) $\Longrightarrow$ (2) ist offensichtlich. Für (2) $\Longrightarrow$ (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:

$$\left.\begin{array}{r} 0 = H^{q_0}(U,A) \cong H^1(U,A^{q_0-1}) \\ 0 = H^{q_0+1}(U,A) \cong H^2(U,A^{q_0-1}) \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} 0 = H^0(U,A^{q_0-1}) \cong H^{q_0-1}(U,A) \\ 0 = H^3(U,A^{q_0-1}) \cong H^{q_0+2}(U,A) \end{array}\right.$$

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 $U \lneq G$.
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

   $$H^q(G,A)_p \overset{\mathrm{Res}}{\hookrightarrow} H^q(G_p,A) = 0$$

   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

   $$H^q(G/H, A^H) \overset{\mathrm{Inf}}{\cong} H^q(G,A)$$

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) $H^0(U, A)$ 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 $\bar{f} : H^q(U, \mathbb{Z}) \longrightarrow H^q(U, B)$. Dann kommutiert

$$\begin{tikzcd} H^q(U,\mathbb{Z}) \arrow[r, "a\cup -"] \arrow[dr, "\bar{f}"'] & H^q(U,A) \arrow[d, "\bar{i}"] \\ & H^q(U,B) \end{tikzcd}$$

denn: Sei

$$\begin{aligned} b_q : G \times \cdots \times G &\longrightarrow \mathbb{Z} \\ \sigma = (\sigma_1, ..., \sigma_q) &\longmapsto b_q(\sigma) \end{aligned}$$

ein q-Kozyklus. Es gilt

$$\begin{tikzcd} H^q(U,\mathbb{Z}) \ni \bar{b}_q \arrow[rr, mapsto, "a\cup -"] \arrow[dr, mapsto] & & \overline{a_0 \otimes b_q} \in H^q(U,A) \arrow[d, mapsto, "\bar{i}"] \\ & \overline{(\sigma \mapsto (b_q(\sigma)a_0, b_q(\sigma)N_G))} = & \overline{(\sigma \mapsto (b_q(\sigma)a_0, 0))} \end{tikzcd}$$

Es ist noch zu zeigen, dass $\bar{f}$ ein Isomorphismus ist. Betrachte dazu

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} B \longrightarrow C \longrightarrow 0\,, \tag{2.16}$$

mit $C = \operatorname{coker}(f)$. Dann folgt

$$0 \longrightarrow H^{-1}(U,C) \longrightarrow H^0(U,\mathbb{Z}) \xrightarrow{\bar{f}} H^0(U,B) \longrightarrow H^0(U,C) \longrightarrow 0\,,$$

da $H^1(U, \mathbb{Z}) = \operatorname{Hom}_{\mathbb{Z}}(U, \mathbb{Z}) = 0$.

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

$$\begin{tikzcd} H^0(G,A) \arrow[r, "\mathrm{Res}"] \arrow[rr, bend right, "|G/U|\cdot \mathrm{id}"'] & H^0(U,A) \arrow[r, "\mathrm{Kor}"] & H^0(G,A) \end{tikzcd}$$

Sei $m := \operatorname{ord}(\operatorname{Res}^G_U(a))$ ($\operatorname{Res}^G_U(a) \in H^0(U, A)$). Dann gilt

$$0 = \operatorname{Kor}(\operatorname{Res}(ma)) = m \cdot \frac{|G|}{|U|} a\,.$$

Es folgt $|U|$ teilt m und $\operatorname{Res}^G_U(a)$ ist somit ein Erzeuger von $H^0(U, A)$.
Wegen $\bar{f}(1 + |U|\,\mathbb{Z}) = a_0 + N_U A = \operatorname{Res}^G_U(a)$ ist $\bar{f} : H^0(U, \mathbb{Z}) \longrightarrow H^0(U, B)$ surjektiv.
Wegen

$$\left|H^0(U,\mathbb{Z})\right| = |U| = \left|H^0(U,A)\right| = \left|H^0(U,B)\right|$$

ist $\bar{f}$ ein Isomorphismus.

$\square$

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) $H^2(U, A)$ *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: $\mathrm{Res}_U^G(a)$ *erzeugt $H^2(U, A)$ für alle Untergruppen $U \leq G$ und man erhält Isomorphismen*

$$\mathrm{Res}_U^G(a) \cup \_ : H^q(U, \mathbb{Z}) \longrightarrow H^{q+2}(U, A)\,.$$

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

$$\begin{tikzcd} H^q(U, \mathbb{Z}) \arrow[r, "\delta^{-1}a\cup\_"] \arrow[d, "\mathrm{id}"] & H^q(U, A^2) \arrow[d, "\delta"] \\ H^q(U, \mathbb{Z}) \arrow[r, "a\cup\_"] & H^{q+2}(U, A) \end{tikzcd}$$

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 $\mathrm{Kor} \circ \mathrm{Res} = |G/U| \cdot \mathrm{id}$.

$\square$

3 Lokale Klassenkörpertheorie

3.1 Abstrakte Klassenkörpertheorie

Einschub: Unendliche Galoistheorie

Literatur: [NS11, Kapitel IV, §1]

Sei k ein Körper und $\overline{k}$ der separable Abschluss. Sei $G_k := \mathrm{Gal}(\overline{k}|k)$ die absolute Galoisgruppe.

Definition 3.1. Sei Ω/k eine Galoiserweiterung mit Galoisgruppe G. Dann wird für jedes $\sigma \in G$ durch die Nebenklassen

$$\sigma \,\mathrm{Gal}(\Omega|K)$$

für endliche, galoissche Erweiterungen K/k eine Umgebungsbasis von σ definiert. Die so erzeugte Topologie auf G heißt *Krulltopologie.*

Die Situation wird in folgendem Bild veranschaulicht:

$$\begin{tikzcd} \Omega \arrow[d, dash, "\mathrm{Gal}(\Omega|K)"] \arrow[dd, dash, bend right=60, "G"'] \\ K \arrow[d, dash, "{<\infty,\ \text{gal.}}"] \\ k \end{tikzcd}$$

Bemerkung 3.2. Eine Teilmenge $U \subseteq G$ ist offen, wenn es zu jedem $\sigma \in U$ eine endliche Galoiserweiterung K/k gibt mit $\sigma \,\mathrm{Gal}(\Omega|K) \subseteq U$.

Satz 3.3. *Für jede Galoiserweiterung Ω/k ist $G = \mathrm{Gal}(\Omega|k)$ hausdorffsch und kompakt.*

Beweisskizze. Zu „hausdorffsch“:
Sei $\sigma \neq \tau$, $\sigma, \tau \in G$. Dann gibt es eine endliche Galoiserweiterung K/k mit $\sigma\big|_K \neq \tau\big|_K$. Dies gilt genau dann, wenn $\sigma \,\mathrm{Gal}(\Omega|K) \neq \tau \,\mathrm{Gal}(\Omega|K)$ und ist somit äquivalent zu

$$\sigma \,\mathrm{Gal}(\Omega|K) \cap \tau \,\mathrm{Gal}(\Omega|K) = \emptyset\,.$$

Zu „kompakt“:
Betrachte

$$\begin{aligned} h : G &\longrightarrow \prod_{\substack{K/k \\ \text{endl., gal.}}} \mathrm{Gal}(K|k) \\ \sigma &\longmapsto \left(\sigma\big|_K\right)_K \end{aligned}$$

Es gilt:

- h ist injektiv,
- h ist ein Homöomorphismus auf $h(G)$,
- $h(G) \subseteq \prod_K \mathrm{Gal}(K|k)$ ist abgeschlossen, wobei jede der endlichen Gruppen $\mathrm{Gal}(K|k)$ mit der diskreten Topologie versehen wird und das Produkt die Produkttopologie trägt.
- $\prod_K \mathrm{Gal}(K|k)$ ist kompakt nach dem Satz von Tychonoff.

Damit folgt $h(G) \cong G$ ist kompakt. $\square$

Bemerkung 3.4. Es ist

$$h(G) = \varprojlim_{\substack{K/k \\ \text{endl., gal.}}} \mathrm{Gal}(K|k)$$

mit Elementen der Form

$$\left\{ (\sigma_K)_K \in \prod_K \mathrm{Gal}(K|k) \;\middle|\; \sigma_L\big|_K = \sigma_K \text{ für alle } L/K/k \right\}.$$

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 $\Omega = \overline{k}$. Betrachte

$$\begin{tikzcd}
N \arrow[d, dash] \arrow[dd, dash, bend left, "m"] \\
K \arrow[d, dash] \arrow[d, dash, bend right, "n"'] \\
k
\end{tikzcd}$$

mit $n|m$. Dann gilt

$$\mathbb{Z}/m\mathbb{Z} \cong \mathrm{Gal}(N|k) \xrightarrow{\text{res}} \mathrm{Gal}(K|k) \cong \mathbb{Z}/n\mathbb{Z}$$
$$\varphi \longmapsto \varphi$$

wobei φ den Frobenius bezeichnet. Dann gilt

$$\mathrm{Gal}(\overline{k}|k) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}}\,.$$

$\widehat{\mathbb{Z}}$ wird als der *Prüferring* bezeichnet.

(2) Sei $k = \mathbb{Q}(\zeta_p)$ für eine Primzahl $p \neq 2$. Betrachte

$$\begin{tikzcd}[column sep=small]
 & & & \mathbb{Q}(\zeta_{p^\infty}) := \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{p^{n+1}}) =: \Omega \arrow[dl, dash] \\
 & & \mathbb{Q}(\zeta_{p^{n+1}}) \arrow[dl, dash] & \\
 & \mathbb{Q}(\zeta_{p^2}) \arrow[dl, dash] & & \\
\mathbb{Q}(\zeta_p) \arrow[d, dash] & & & \\
\mathbb{Q} & & &
\end{tikzcd}$$

Dann gilt

$$\varprojlim_n \underbrace{\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})|\mathbb{Q}(\zeta_p))}_{\cong \frac{1+p\mathbb{Z}}{1+p^{n+1}\mathbb{Z}} \hookrightarrow (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times} = \varprojlim_n \frac{1+p\mathbb{Z}}{1+p^{n+1}\mathbb{Z}} \overset{\log_p}{\cong} \varprojlim_n \frac{p\mathbb{Z}}{p^{n+1}\mathbb{Z}} \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p \,.$$

Satz 3.6 (Hauptsatz der Galoistheorie)**.** *Sei Ω/k eine Galoiserweiterung. Dann ist die Zuordnung $K \longmapsto \mathrm{Gal}(\Omega|K)$ eine $1:1$-Korrespondenz zwischen den Teilerweiterungen K/k von Ω/k und den abgeschlossenen Untergruppen von $\mathrm{Gal}(\Omega|k)$. 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

$$U \text{ offen} \quad \Longleftrightarrow \quad U \text{ abgeschlossen und } (G:U) < \infty \,.$$

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)**.** $G = \mathrm{Gal}(\Omega|k)$.

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

$$K = \bigcap_{i=1}^{n} K_i \iff G_K = \overline{\langle G_{K_i} \,:\, i = 1, ..., n \rangle}\,,$$
$$K = \prod_{i=1}^{n} K_i \iff G_K = \bigcap_{i=1}^{n} G_{K_i}\,.$$

- 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 Ω/k eine Galoiserweiterung, $G = \mathrm{Gal}(\Omega|k)$ und $A = \Omega^\times$.

Lemma 3.11. *Folgende Aussagen sind äquivalent:*

(1) $G \times A \longrightarrow A$ *ist stetig, wobei* A *mit der diskreten Topologie versehen ist.*

(2) Für jedes $a \in A$ *ist*

$$G_a := \{\sigma \in G \,|\, \sigma(a) = a\}$$

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 $G = \mathrm{Gal}(\Omega|k)$. Dann ist $(G, \Omega^\times)$ eine Formation.

Beweis. Sei $\alpha \in \Omega^\times$. Betrachte

$$\begin{tikzcd}
 & \Omega \\
K \arrow[ur, dash] \arrow[d, dash] \arrow[dd, dash, bend right, "\text{endl., gal.}"'] & \\
k(\alpha) \arrow[d, dash, "<\infty"] & \\
k &
\end{tikzcd}$$

Dann gilt

$$G_\alpha = \mathrm{Gal}(\Omega|k(\alpha)) = \bigcup_{\sigma \in \mathrm{Gal}(\Omega|k(\alpha))/\mathrm{Gal}(\Omega|K)} \sigma\, \mathrm{Gal}(\Omega|K)$$

ist offen. $\square$

Definition 3.15. Sei (G, A) eine Formation und $K \in X$. Dann setzt man

$$A_K := A^{G_K}\,.$$

<u>Im Standardbeispiel</u>: $A_K = K^\times$.

Bemerkungen 3.16. Sei (G, A) eine Formation.

(1) L/K ($\Longleftrightarrow G_L \leq G_K$) impliziert $A_K \subseteq A_L$.

(2) Ist L/K normal ($\Longleftrightarrow G_L \trianglelefteq G_K$), so ist $A_L = A^{G_L}$ ein ${}^{G_K}\!/_{G_L} = G_{L/K}$-Modul.

<u>Im Standardbeispiel</u>:

$$\begin{tikzcd}
\Omega \arrow[d, dash] \arrow[d, phantom, bend left, "G_L"] \arrow[dd, dash, bend left, "G_K"] \\
L \arrow[d, dash] \arrow[d, dash, bend right, "\text{gal.}"'] \\
K \arrow[d, dash] \\
k
\end{tikzcd}$$

$G_{L/K} = {}^{G_K}\!/_{G_L}$ 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

$$\begin{tikzcd}
H^q(L|K) \arrow[r, "\mathrm{Inf}_N"] \arrow[d, equal] & H^q(N|K) \arrow[d, equal] \\
H^q(G_{L/K}, A_L) \arrow[r, "\mathrm{Inf}"] & H^q(G_{N/K}, A_N)
\end{tikzcd}$$

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

$$\begin{tikzcd} H^q(N|K) \arrow[r, shift left, "\mathrm{Res}_L"] \arrow[d, equal] & H^q(N|L) \arrow[l, shift left, "\mathrm{Kor}_K"] \arrow[d, equal] \\ H^q(G_{N/K}, A_N) \arrow[r, shift left, "\mathrm{Res}"] & H^q(G_{N/L}, A_N) \arrow[l, shift left, "\mathrm{Kor}"] \end{tikzcd}$$

eine Restriktion und eine Korestriktion.
Falls N/K und L/K normal sind, so hat man exakte Inflations-Restriktions-Sequenzen

$$1 \longrightarrow H^q(L|K) \xrightarrow{\mathrm{Inf}_N} H^q(N|K) \xrightarrow{\mathrm{Res}_L} H^q(N|L)$$

falls $H^i(N|L) = 1$ für $1 \leq i \leq q-1$.
Im Standardbeispiel:

$$H^0(N|K) = {}^{K^\times}/_{N_{N/K}(N^\times)} \xrightarrow{\mathrm{Res}_L} H^0(N|L) = {}^{L^\times}/_{N_{N/L}(N^\times)}$$

ist induziert von der Inklusion $K^\times \subseteq L^\times$.

$${}^{L^\times}/_{N_{N/L}(N^\times)} = H^0(N|L) \xrightarrow{\mathrm{Kor}_K} H^0(N|K) = {}^{K^\times}/_{N_{N/K}(N^\times)}$$

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 Ω/k galoissch und $A = \Omega^\times$. Dann ist $(\mathrm{Gal}(\Omega|k), \Omega^\times)$ eine Körperformation.*

Beweis. $H^1(L|K) = H^1(\mathrm{Gal}(L|K), L^\times) = 1$ nach Hilberts Satz 90 (siehe Blatt 8, Aufgabe 1). □

Bemerkung 3.20. In einer Körperformation ist

$$1 \longrightarrow H^2(L|K) \xrightarrow{\mathrm{Inf}_N} H^2(N|K) \xrightarrow{\mathrm{Res}_L} H^2(N|L)$$

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 $\mathrm{Inf}_N(H^2(L|K)) \subseteq H^2(N|K)$.

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

$$x : G \times \cdots \times G \longrightarrow A\,, \qquad q \geq 1$$

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 $\mathrm{Res}_{K'}(c) = 0$ 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 $c \in \mathrm{im}(\mathrm{Inf}_L)$. □

Ziel: Finde $G^{\mathrm{ab}}_{L|K} \cong {}^{A_K}\!/\!_{N_{L/K}A_L}$. 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

$$a \cup \_ : G^{\mathrm{ab}}_{L/K} = H^{-2}(G_{L/K}, \mathbb{Z}) \xrightarrow{\cong} H^0(G_{L/K}, A_L) = {}^{A_K}\!/\!_{N_{L/K}A_L}$$

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*,

$$\mathrm{inv}_{L/K} : H^2(L|K) \xrightarrow{\cong} \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

mit folgenden Eigenschaften

(1) Falls $N/L/K$ mit N/K und L/K normal, so gilt:

$$\mathrm{inv}_{L/K} = \mathrm{inv}_{N/K}\big|_{H^2(L|K)}$$

bzw. das Diagramm

$$\begin{tikzcd} H^2(L|K) \arrow[r, "\mathrm{inv}_{L/K}"] \arrow[d, "\mathrm{Inf}"] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, "\subseteq"] \\ H^2(N|K) \arrow[r, "\mathrm{inv}_{N/K}"] & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} \end{tikzcd}$$

kommutiert.

(2) Falls $N/L/K$ mit N/K normal, so kommutiert das Diagramm

$$\begin{tikzcd} H^2(N|K) \arrow[r, "\mathrm{inv}_{N/K}"] \arrow[d, "\mathrm{Res}_L"] & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, "{[L:K]}"] \\ H^2(N|L) \arrow[r, "\mathrm{inv}_{N/L}"] & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z} \end{tikzcd}$$

Wegen 3.24.II.(1) erhält man einen injektiven Homomorphismus

$$\begin{aligned} \mathrm{inv}_K : H^2(K) &\hookrightarrow \mathbb{Q}/\mathbb{Z} \\ a &\longmapsto \mathrm{inv}_{L/K}(a)\,, \quad a \in H^2(L|K) \end{aligned}$$

Satz 3.25. *Sei $N/L/K$ und N/K normal. Dann gilt:*

(1) $\mathrm{inv}_{N/K}(c) = \mathrm{inv}_{L/K}(c)$ *falls L/K normal ist und $c \in H^2(L|K) \subseteq H^2(N|K)$.*

(2) $\mathrm{inv}_{N/L}(\mathrm{Res}_L(c)) = [L:K]\,\mathrm{inv}_{N/K}(c)$ *für $c \in H^2(N|K)$.*

(3) $\mathrm{inv}_{N/K}(\mathrm{Kor}_K(c)) = \mathrm{inv}_{N/L}(c)$ *für $c \in H^2(N|L)$.*

(4) $\mathrm{inv}_{\sigma L/\sigma K}(\sigma^* c) = \mathrm{inv}_{L/K}(c)$ *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

$$\begin{array}{l} x : G_{L/K} \times \cdots \times G_{L/K} \to A_L \\ \big\downarrow \\ \sigma^* x := m_\sigma \circ x \circ c_\sigma^{-1} \end{array}$$

Beweis von Satz 3.25. (1) und (2) sind Definition.

Zu (3): Wegen 3.24.II.(2) ist

$$\operatorname{Res}_L : H^2(N|K) \longrightarrow H^2(N|L)$$

surjektiv. Sei $\widetilde{c} \mapsto c$. Dann folgt

$$\operatorname{Kor}_K(c) = \operatorname{Kor}_K(\operatorname{Res}_L(\widetilde{c})) = \widetilde{c}^{[L:K]}$$

und somit

$$\operatorname{inv}_{N/K}(\operatorname{Kor}_K(c)) = \operatorname{inv}_{N/K}\left(\widetilde{c}^{[L:K]}\right) = [L:K] \operatorname{inv}_{N/K}(\widetilde{c}) = \operatorname{inv}_{N/L}(c)\,.$$

Für (4) siehe [NS11, Kapitel II, Satz (1.4)]. □

Definition 3.26. Das durch

$$\operatorname{inv}_{L/K}(u_{L/K}) = \frac{1}{[L:K]} + \mathbb{Z}$$

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) $\operatorname{Res}_L(u_{N/K}) = u_{N/L}$.

(3) $\operatorname{Kor}_K(u_{N/L}) = u_{N/K}^{[L:K]}$.

(4) $\sigma^*(u_{N/K}) = u_{\sigma N/\sigma K}$ *für $\sigma \in G$.*

Beweiskostprobe. Zu (1): Es gilt

$$\begin{aligned} \operatorname{inv}_{N/K}\left(u_{N/K}^{[N:L]}\right) &= [N:L] \operatorname{inv}_{N/K}(u_{N/K}) \\ &= \frac{[N:L]}{[N:K]} + \mathbb{Z} = \frac{1}{[L:K]} + \mathbb{Z} \\ &= \operatorname{inv}_{L/K}(u_{L/K}) \end{aligned}$$

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*

$$u_{L/K} \cup \_ : G_{L/K}^{\mathrm{ab}} \cong H^{-2}(G_{L/K}, \mathbb{Z}) \longrightarrow H^0(L|K) = {}^{A_K}\!/_{N_{L/K}A_L}$$

einen kanonischen Isomorphismus

$$\Theta_{L/K} : G_{L/K}^{\mathrm{ab}} \longrightarrow {}^{A_K}\!/_{N_{L/K}A_L}\,.$$

Definition 3.30.

- $\Theta_{L/K}$ heißt *Nakayamaabbildung.*
- Die zu $\Theta_{L/K}$ inverse Abbildung heißt *Reziprozitätsisomorphismus.*
- Das *Normrestsymbol* ist

$$\begin{tikzcd}
(_, L/K) : A_K \arrow[rr] \arrow[dr] & & G_{L/K}^{\mathrm{ab}} \\
& {}^{A_K}\!/_{N_{L/K}A_L} \arrow[ur, "\Theta_{L/K}^{-1}"'] &
\end{tikzcd}$$

In der lokalen Klassenkörpertheorie

Sei $k/\mathbb{Q}_p$ eine endliche Erweiterung und $G = G_k = \mathrm{Gal}(\overline{k}|k)$. Dann ist $(G, \overline{k}^{\times})$ eine Klassenformation (siehe [NS11, Kapitel II, Satz (5.6)]).

Im Globalen

Sei k ein Zahlkörper und $G = G_k = \mathrm{Gal}(\overline{k}|k)$. Dann ist $(G, \mathcal{C}_{\overline{k}})$ eine Klassenformation (siehe [NS11, Kapitel III, Satz (6.9)]). Hierbei ist

$$\mathcal{C}_{\overline{k}} := \varinjlim_{L} \mathcal{C}_L$$

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

$$0 \longrightarrow N_{L/K}A_L \longrightarrow A_K \xrightarrow{(\_\,,L/K)} G^{\mathrm{ab}}_{L/K} \longrightarrow 0$$

ist exakt, d.h.

$$(a, L/K) = 1 \qquad \Longleftrightarrow \qquad a \in N_{L/K}A_L\,.$$

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:*

$$\begin{tikzcd} A_K \arrow[r, "(\_\,,N/K)"] \arrow[d, equal] & G^{\mathrm{ab}}_{N/K} \arrow[d, "\pi"] \\ A_K \arrow[r, "(\_\,,L/K)"] & G^{\mathrm{ab}}_{L/K} \end{tikzcd}$$

wobei

$$\begin{aligned} \pi : {}^{G_{N/K}}\!/_{G'_{N/K}} = G^{\mathrm{ab}}_{N/K} &\longrightarrow G^{\mathrm{ab}}_{L/K} = \frac{\left({}^{G_{N/K}}\!/_{G_{N/L}}\right)}{\left({}^{G_{N/K}}\!/_{G_{N/L}}\right)'} \\ \tau G'_{N/K} &\longmapsto (\tau G_{N/L})\left({}^{G_{N/K}}\!/_{G_{N/L}}\right)' \end{aligned}$$

(2)

$$\begin{tikzcd} A_K \arrow[r, "(\_\,,N/K)"] \arrow[d, "\subseteq"] & G^{\mathrm{ab}}_{N/K} \arrow[d, "\mathrm{Ver}"] \\ A_L \arrow[r, "(\_\,,N/L)"] & G^{\mathrm{ab}}_{N/L} \end{tikzcd}$$

Hierbei ist Ver *induziert von*

$$H^{-2}(G_{N/K}, \mathbb{Z}) \xrightarrow{\mathrm{Res}} H^{-2}(G_{N/L}, \mathbb{Z})\,.$$

Bemerkung. Ver hat auch eine rein gruppentheoretische Definition, siehe [Neu06, Kapitel IV, §5] und [Ser13].

(3)

$$\begin{tikzcd} A_L \arrow[r, "(\_\,,N/L)"] \arrow[d, "N_{L/K}"] & G^{\mathrm{ab}}_{N/L} \arrow[d, "\kappa"] \\ A_K \arrow[r, "(\_\,,N/K)"] & G^{\mathrm{ab}}_{N/K} \end{tikzcd}$$

wobei

$$\begin{aligned} \kappa : {}^{G_{N/L}}\!/_{G'_{N/L}} = G^{\mathrm{ab}}_{N/L} &\longrightarrow G^{\mathrm{ab}}_{N/K} = {}^{G_{N/K}}\!/_{G'_{N/K}} \\ \tau G'_{N/L} &\longmapsto \tau G'_{N/K} \end{aligned}$$

(4)

$$\begin{tikzcd} A_K \arrow[r, "{(\_,N/K)}"] \arrow[d, "\sigma"] & G^{\mathrm{ab}}_{N/K} \arrow[d, "\sigma^*"] \\ A_{\sigma K} \arrow[r, "{(\_,\sigma N/\sigma K)}"] & G^{\mathrm{ab}}_{\sigma N/\sigma K} \end{tikzcd}$$

Hierbei ist σ^* induziert durch die Konjugation

$$\tau \longmapsto \sigma\tau\sigma^{-1}\,.$$

Beispiel 3.34. Sei $k/\mathbb{Q}_p$ endlich, $\overline{k}$ der algebraische Abschluss von k und $G_k = \mathrm{Gal}(\overline{k}|k)$. Dann folgt mit Hilberts Satz 90, dass $(G_k, \overline{k}^\times)$ eine Körperformation ist.

Bemerkung 3.35. Falls L/K normal, so ist $G^{\mathrm{ab}}_{L/K} = {}^{G_{L/K}}\!/\!_{G'_{L/K}}$ die Galoisgruppe der maximal abelschen Teilerweiterung L^{ab}/K von L/K, denn für $H \trianglelefteq G_{L/K}$ gilt:

$${}^{G_{L/K}}\!/\!_{H} \text{ abelsch} \quad\Longleftrightarrow\quad G'_{L/K} \subseteq H\,.$$

Das Reziprozitätsgesetz ist also ein Isomorphismus

$$G_{L^{\mathrm{ab}}/K} \cong {}^{A_K}\!/\!_{N_{L/K}A_L}\,.$$

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^{ab}/K die maximal abelsche Teilerweiterung. Dann gilt:*

$$N_{L/K}A_L = N_{L^{\mathrm{ab}}/K}A_{L^{\mathrm{ab}}}\,.$$

Beweis. Es gilt

$$N_{L/K}A_L = N_{L^{\mathrm{ab}}/K}\underbrace{N_{L/L^{\mathrm{ab}}}A_L}_{\subseteq A_{L^{\mathrm{ab}}}},$$

d.h. $N_{L/K}A_L \subseteq N_{L^{\mathrm{ab}}/K}A_{L^{\mathrm{ab}}} \subseteq A_K$. Aus dem Reziprozitätsgesetz erhalten wir

$${}^{A_K}\!/\!_{N_{L/K}A_L} \cong G^{\mathrm{ab}}_{L/K} \cong G_{L^{\mathrm{ab}}/K} \cong {}^{A_K}\!/\!_{N_{L^{\mathrm{ab}}/K}A_{L^{\mathrm{ab}}}}$$

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:

$$
\begin{tikzcd}[column sep=small]
 & L := L_1 L_2 \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 & & L_2 \\
 & L_1 \cap L_2 \arrow[ul, dash] \arrow[ur, dash] & \\
 & K \arrow[u, dash] &
\end{tikzcd}
$$

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

$$
\begin{tikzcd}
A_K \arrow[r, "{(\,\_\_\,, L/K)}"] \arrow[d, equal] & G^{\mathrm{ab}}_{L/K} \arrow[d, "\pi_i"] \\
A_K \arrow[r, "{(\,\_\_\,, L_i/K)}"] & G^{\mathrm{ab}}_{L_i/K}
\end{tikzcd}
$$

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 $L \longmapsto I_L$ folgt aus Satz 3.37, die Injektivität aus (1).

Zu (3): Es gilt

$$L_1 \cap L_2 \subseteq L_i \overset{(1)}{\Longrightarrow} I_{L_i} \subseteq I_{L_1 \cap L_2} \Longrightarrow I_{L_1} I_{L_2} \subseteq I_{L_1 \cap L_2} \, .$$

Betrachte

$$\begin{tikzcd}[column sep=small]
 & A_K \arrow[d, dash] & \\
 & I_{L_1 \cap L_2} \arrow[d, dash] & \\
 & I_{L_1} I_{L_2} \arrow[dl, dash] \arrow[dr, dash] & \\
I_{L_1} \arrow[dr, dash] & & I_{L_2} \arrow[dl, dash] \\
 & I_{L_1} \cap I_{L_2} = I_{L_1 L_2} &
\end{tikzcd}$$

Dann folgt

$$\begin{aligned}
\left| {}^{A_K}/_{I_{L_1 L_2}} \right| = [L_1 L_2 : K] = \frac{[L_1 : K][L_2 : K]}{[L_1 \cap L_2 : K]} \\
&= \frac{\left| {}^{A_K}/_{I_{L_1}} \right| \left| {}^{A_K}/_{I_{L_2}} \right|}{\left| {}^{A_K}/_{I_{L_1 \cap L_2}} \right|} \\
&= \frac{\left| {}^{A_K}/_{I_{L_1}} \right| \left| {}^{A_K}/_{I_{L_1} I_{L_2}} \right| \left| {}^{I_{L_1} I_{L_2}}/_{I_{L_2}} \right|}{\left| {}^{A_K}/_{I_{L_1 \cap L_2}} \right|} \\
&= \frac{\left| {}^{A_K}/_{I_{L_1}} \right| \left| {}^{I_{L_1}}/_{I_{L_1} \cap I_{L_2}} \right| \left| {}^{A_K}/_{I_{L_1} I_{L_2}} \right|}{\left| {}^{A_K}/_{I_{L_1 \cap L_2}} \right|} \\
&= \left| {}^{A_K}/_{I_{L_1} \cap I_{L_2}} \right| \frac{\left| {}^{A_K}/_{I_{L_1} I_{L_2}} \right|}{\left| {}^{A_K}/_{I_{L_1 \cap L_2}} \right|}
\end{aligned}$$

Damit folgt $\left| {}^{A_K}/_{I_{L_1} I_{L_2}} \right| = \left| {}^{A_K}/_{I_{L_1 \cap L_2}} \right|$ 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

$$\begin{tikzcd}
L \arrow[d, dash] \arrow[d, dash, bend right=40, "{}^{I}/_{N_{L/K} A_L}"'] \arrow[dd, dash, bend left=40, "{}^{A_K}/_{N_{L/K} A_L}"] \\
M \arrow[d, dash] \\
K
\end{tikzcd}$$

Dann gilt $I = N_{M/K} A_M$ (Übung). $\square$

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:

$$I \le K^\times \text{ ist Normengruppe} \quad \Longleftrightarrow \quad I \text{ ist abgeschlossen von endlichem Index.}$$

Die Richtung „$\Longrightarrow$“ ist relativ leicht. Die Richtung „$\Longleftarrow$“ 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. □

Satz 3.42. *Es gilt*

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

(2) Falls $G = \langle\tau\rangle$, so gilt für $\alpha \in L^\times$:

$$N_{L/K}(\alpha) = 1 \quad \Longleftrightarrow \quad \exists \beta \in L^\times : \ \alpha = \frac{\tau(\beta)}{\beta}\,.$$

Dabei ist β modulo $K^\times$ eindeutig bestimmt.

Beweis. (1) Dies ist Hilberts Satz 90 (siehe Blatt 8, Aufgabe 1).

(2) Dies folgt aus

$$1 = H^1(G, L^\times) \cong H^{-1}(G, L^\times) = {}_{N_G}L^\times / (\tau-1)L^\times\,.$$

□

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 $U \le G$.*

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. □

Definition 3.44. Die *Brauergruppe von K* ist definiert als

$$Br(K) := H^2(K) := \bigcup_L H^2(\mathrm{Gal}(L|K), L^\times)\,.$$

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 $H^2(\mathrm{Gal}(L|K), L^\times) \subseteq H^2(\mathrm{Gal}(N|K), N^\times)$.

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 $q = q_K = \left|\overline{K}\right| = p^f$, 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
$$\begin{aligned} U &\twoheadrightarrow \overline{K}^\times \\ u &\longmapsto \overline{u} \end{aligned}$$

hat den Kern U^1.

Die Abbildung
$$\begin{aligned} U^n &\twoheadrightarrow \overline{K} \\ 1 + a\pi_K^n &\longmapsto \overline{a}, \qquad a \in \mathcal{O}_K \end{aligned}$$

ist ein Homomorphismus, denn
$$(1 + a\pi_K^n)(1 + b\pi_K^n) = 1 + (a + b + ab\pi_K^n)\pi_K^n \longmapsto \overline{a+b} = \overline{a} + \overline{b}.$$

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

$$\begin{aligned} x^m &= 1 + ma\pi^n + \binom{m}{2} a^2 \pi^{2n} + \cdots \\ &\equiv 1 \mod \mathfrak{p}^{n+v(m)} \end{aligned}$$

falls $2n \geq n + v(m)$, also genau dann, wenn $n \geq v(m)$ (denn: $v(ma\pi^n) \geq v(m) + n$).

<u>Surjektivität</u>: Sei $1 + a\pi^{n+v(m)}$ mit $a \in \mathcal{O}_K$. Finde $x \in \mathcal{O}_K$ mit

$$1 + a\pi^{n+v(m)} = (1 + x\pi^n)^m = 1 + mx\pi^n + \pi^{2n} f(x) , \qquad f \in \mathcal{O}_K[X] .$$

Schreibe $m = u\pi^{v(m)}$ mit $u \in U$. Es ist zu lösen:

$$\begin{aligned} & 1 + ux\pi^{n+v(m)} + \pi^{2n} f(x) = 1 + a\pi^{n+v(m)} \\ \Longleftrightarrow \qquad & ux + \pi^{n-v(m)} f(x) - a = 0 \end{aligned}$$

Falls $n > v(m)$, so ist $\overline{x} := \overline{u}^{-1}\overline{a}$ eine Lösung modulo $\mathfrak{p}$. Diese kann man mit Hensels Lemma liften.

<u>Injektivität</u>: Es ist $|\mu_m(K)| < \infty$. Die U^n bilden eine Basis der offenen Umgebungen der 1. Da K hausdorffsch ist, folgt die Injektivität. □

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

$$\varphi_{L/K}(x) \equiv x^{q_K} \mod \mathfrak{p}_L$$

und es gilt

$$\langle \varphi_{L/K} \rangle = \mathrm{Gal}(L|K) .$$

Es gilt für unverzweigte $N/L/K$

$$\begin{aligned} \varphi_{N/K}^{[L:K]} &= \varphi_{N/L} , \\ \varphi_{L/K} &= \varphi_{N/K}\big|_L = \varphi_{N/K} \, \mathrm{Gal}(N|L) , \end{aligned}$$

wobei $\mathrm{Gal}(L|K) \cong {}^{\mathrm{Gal}(N|K)}/_{\mathrm{Gal}(N|L)}$.

Satz 3.47. *Sei L/K unverzweigt. Dann gilt*

$$H^q(\mathrm{Gal}(L|K), U_L) = 1$$

für alle $q \in \mathbb{Z}$, d.h. die U_L sind kohomologisch trivial.

Beweis. Wir identifizieren

$$G := \mathrm{Gal}(L|K) \cong \mathrm{Gal}(\overline{L}|\overline{K})$$
$$\sigma \mapsto \overline{\sigma}$$

mit

$$\overline{\sigma}(\overline{\alpha}) := \overline{\sigma(\alpha)}\,, \qquad \alpha \in \mathcal{O}_L\,.$$

Dann ist

$$0 \longrightarrow U_L^1 \longrightarrow U_L \longrightarrow \overline{L}^\times \longrightarrow 0$$

eine exakte Sequenz von G-Moduln. Da $\overline{L}^\times$ 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 $n \geq 2$

$$U_L^{n-1} \longrightarrow \overline{L}$$
$$1 + a\pi^{n-1} \longmapsto \overline{a}\,, \qquad a \in \mathcal{O}_L$$

Dies ist ein Homomorphismus von G-Moduln:

$$\sigma(1 + a\pi^{n-1}) = 1 + \sigma(a)\pi^{n-1} \longmapsto \overline{\sigma(a)} = \overline{\sigma}(\overline{a})\,.$$

Aus der exakten Sequenz

$$0 \longrightarrow U_L^n \longrightarrow U_L^{n-1} \longrightarrow \overline{L} \longrightarrow 0$$

und $H^q(G, \overline{L}) = 0$ folgt

$$H^q(G, U_L^n) \cong H^q(G, U_L^1) \cong H^q(G, U_L)\,.$$

Die Abbildung $x \longmapsto x^m$ 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

$$\begin{tikzcd}
H^q(G, U_L^n) \arrow[r, "\subseteq", "\cong"'] \arrow[d, "\cong"', "m"] & H^q(G, U_L) \arrow[d, "m"] \\
H^q(G, U_L^{n+v_L(m)}) \arrow[r, "\subseteq", "\cong"'] & H^q(G, U_L)
\end{tikzcd}$$

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 $H^q(G, U_L) = 1$.

□

Korollar 3.48. *Sei L/K unverzweigt. Dann ist $N_{L/K}(U_L) = U_K$.*

Beweis. Dies folgt sofort aus $H^0(G, U_L) = {}^{U_K}/_{N_{L/K}(U_L)} = 0$. $\square$

<u>Ziel</u>: 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

$$(\mathrm{Gal}(T|K_0), T^\times)$$

eine Klassenformation ist.
Dazu ist

$$\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L|K), L^\times) \longrightarrow \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

für eine Erweiterung L/K in T/K_0 zu definieren.

Bemerkung 3.49. Es ist $\mathrm{Gal}(T|K_0) \cong \widehat{\mathbb{Z}}$.

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

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\cong]{\delta} H^2(G, \mathbb{Z})\,.$$

Betrachte noch

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\cong]{\varphi} \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

$$\chi \longmapsto \chi(\varphi_{L/K})$$

Zusammenfassend:

$$\begin{tikzcd}
H^2(G, L^\times) \arrow[r, "\mathrm{inv}_{L/K}"] \arrow[d, "\overline{v_L}"] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\
H^2(G, \mathbb{Z}) \arrow[r, "\delta^{-1}"] & H^1(G, \mathbb{Q}/\mathbb{Z}) \arrow[u, "\varphi"']
\end{tikzcd}$$

Setze wieder $H^q(L|K) := H^q(\mathrm{Gal}(L|K), L^\times)$.

Satz 3.50. $(\mathrm{Gal}(T|K_0), T^\times)$ *ist eine Klassenformation für $K_0/\mathbb{Q}_p$ endlich.*

Beweis. Es ist die Kommutativität von

$$
\begin{tikzcd}
H^2(L|K) \arrow[r, "\overline{v_L}"] \arrow[d, "\mathrm{Inf}=\subseteq"] & H^2(G_{L/K}, \mathbb{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "\mathrm{Inf}"] & H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\varphi"] \arrow[d, "\mathrm{Inf}"] & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, "\subseteq"] \\
H^2(N|K) \arrow[r, "\overline{v_N}"] & H^2(G_{N/K}, \mathbb{Z}) \arrow[r, "\delta^{-1}"] & H^1(G_{N/K}, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\varphi"] & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}
\tag{3.1}
$$

bzw.

$$
\begin{tikzcd}
H^2(N|K) \arrow[r, "\overline{v_N}"] \arrow[d, "\mathrm{Res}"] & H^2(G_{N/K}, \mathbb{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "\mathrm{Res}"] & H^1(G_{N/K}, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\varphi"] \arrow[d, "\mathrm{Res}"] & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, "{[L:K]}"] \\
H^2(N|L) \arrow[r, "\overline{v_N}"] & H^2(G_{N/L}, \mathbb{Z}) \arrow[r, "\delta^{-1}"] & H^1(G_{N/L}, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\varphi"] & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}
\tag{3.2}
$$

zu zeigen.

<u>Zum linken Rechteck in Diagramm 3.1</u>: Sei $\overline{x} \in H^2(G_{L/K}, L^\times)$. Dann gilt

$$
\begin{tikzcd}
\overline{x} \arrow[rr, mapsto, "\overline{v_L}"] \arrow[dd, mapsto] & & \overline{v_L \circ x} \arrow[d, mapsto] \\
& & ((\sigma_1, \sigma_2) \mapsto v_L(x(\overline{\sigma_1}, \overline{\sigma_2}))) \arrow[dl, equal] \\
\mathrm{Inf}\,\overline{x} \arrow[r, mapsto] & ((\sigma_1, \sigma_2) \mapsto v_N(x(\overline{\sigma_1}, \overline{\sigma_2}))) &
\end{tikzcd}
$$

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 δ mit Inf und Res.

<u>Zum rechten Rechteck in Diagramm 3.1</u>: Sei $\chi \in H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_{L/K}, \mathbb{Q}/\mathbb{Z})$. Dann gilt

$$
\begin{tikzcd}
\chi \arrow[rr, mapsto] \arrow[dd, mapsto] & & \chi(\varphi_{L/K}) \arrow[d, mapsto] \\
& & \chi(\varphi_{L/K}) \arrow[dl, equal] \\
\mathrm{Inf}\,\chi \arrow[r, mapsto] & (\mathrm{Inf}\,\chi)(\varphi_{N/K}) &
\end{tikzcd}
$$

Die Bilder sind gleich, da

$$(\mathrm{Inf}\,\chi)(\varphi_{N/K}) = \chi(\varphi_{N/K}\big|_L) = \chi(\varphi_{L/K})\,.$$

Das rechte Rechteck in Diagramm 3.2 folgt aus $\varphi_{N/K}^{[L:K]} = \varphi_{N/L}$. $\square$

Satz 3.51. *Die Abbildung*

$$H^2(T|K) = \bigcup_{L/K \text{unverzweigt}} H^2(L|K) \xrightarrow{\mathrm{inv}_{T/K}} \mathbb{Q}/\mathbb{Z}$$

ist ein Isomorphismus (hierbei ist $\mathrm{inv}_{T/K}\big|_L = \mathrm{inv}_{L/K}$*).*

Beweis. Injektivität ist eine allgemeine Tatsache aus der Theorie der Klassenformationen. Surjektivität folgt aus

$$\mathbb{Q}/\mathbb{Z} = \bigcup_{n \geq 1} \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}$$

und weil es zu jedem $n \geq 1$ eine unverzweigte Erweiterung L mit $[L : K] = n$ gibt. □

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* $\overline{a} \in H^0(L|K) = A_K/N_{L/K}A_L$*. Dann gilt für jedes* $\chi \in H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z})$

$$\chi((a, L/K)) = \mathrm{inv}_{L/K}(\overline{a} \cup \delta\chi)\,.$$

Hierbei ist δ *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

$$\begin{aligned}
\chi((a, L/K)) &= \mathrm{inv}_{L/K}(\overline{a} \cup \delta\chi) = (\varphi \circ \delta^{-1} \circ \overline{v_L})(\overline{a} \cup \delta\chi) \\
&\overset{(*)}{=} (\varphi \circ \delta^{-1})(v_L(a)\delta\chi) = \varphi(v_L(a)\chi) \\
&= \varphi(v_K(a)\chi) = v_K(a)\chi(\varphi_{L/K}) \\
&= \chi(\varphi_{L/K}^{v_K(a)})
\end{aligned}$$

Da dies für alle χ gilt, folgt $(a, L/K) = \varphi_{L/K}^{v_K(a)}$. Hierbei folgt $(*)$ aus Eigenschaften des Cupprodukts.

□

Beweis von Lemma 3.53. Setze $\sigma_a := (a, L/K) \in G_{L/K}^{\mathrm{ab}}$. Sei $\overline{\sigma_a}$ das Bild von σ_a unter

$$\begin{aligned}
G_{L/K}^{\mathrm{ab}} &\cong H^{-2}(G_{L/K}, \mathbb{Z}) \\
\sigma_a &\mapsto \overline{\sigma_a}
\end{aligned}$$

Wegen

$$\begin{tikzcd}
\overline{\sigma_a} & H^{-2}(G_{L/K},\mathbb{Z}) \arrow[r, "u_{L/K}\cup\, _"] & H^0(L|K) = A_K/N_{L/K}A_L & \overline{a} \\
\sigma_a \arrow[u, mapsto] & G_{L/K}^{\mathrm{ab}} \arrow[u, "\cong"] & A_K \arrow[l, "(_\,{,}L/K)"'] \arrow[u, two heads] & a \arrow[u, mapsto] \arrow[lll, bend left, mapsto]
\end{tikzcd}$$

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

$$\overline{\sigma_a} \cup \chi = \chi \cup \overline{\sigma_a} \overset{2.71}{=} \chi(\sigma_a) \overset{(*)}{=} \frac{r}{n} + \mathbb{Z}\,,$$

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

$$\mathrm{inv}_{L/K}(\overline{a} \cup \delta\chi) = r\,\mathrm{inv}_{L/K}(u_{L/K}) = \frac{r}{n} + \mathbb{Z} = \chi(\sigma_a)\,.$$

□

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

$$\begin{aligned} a \in N_{L/K}(L^\times) \quad &\Longleftrightarrow \quad (a, L/K) = 1\,, \\ &\Longleftrightarrow \quad \varphi_{L/K}^{v_K(a)} = 1\,, \\ &\Longleftrightarrow \quad f | v_K(a)\,, \\ &\Longleftrightarrow \quad a \in \langle \pi_K^f \rangle \times U_K\,. \end{aligned}$$

□

3.6 Das lokale Reziprozitätsgesetz

Sei $K_0/\mathbb{Q}_p$ endlich, $\Omega = K_0^c$ und $G_{K_0} = \mathrm{Gal}(\Omega|K_0)$.

Ziel: $(G_{K_0}, \Omega^\times)$ ist Klassenformation.

Dazu ist für L/K normal, K/K_0 endlich, ein Invariantenisomorphismus

$$\mathrm{inv}_{L/K} : H^2(\mathrm{Gal}(L|K), L^\times) \longrightarrow \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

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*

$$h(L^\times) = \frac{|H^2(L|K)|}{|H^1(L|K)|} = \left|H^2(L|K)\right| = l\,.$$

Beweis der Behauptung.

Erinnerung 3.56. Es ist

$$q_{f,g}(A) = \frac{(\ker(f) : \mathrm{im}(g))}{(\ker(g) : \mathrm{im}(f))}$$

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 $q_K = \left|\overline{K}\right|$.

Also erhalten wir

$$\begin{aligned} q_{0,l}(K^\times) &= l q_K^{v_K(l)}\,, \\ q_{0,l}(L^\times) &= l q_L^{v_L(l)}\,. \end{aligned}$$

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

$$h(L^\times)^{l-1} = \frac{l^l q_K^{lv_K(l)}}{l q_L^{v_L(l)}} = \frac{l^{l-1} q_K^{lv_K(l)}}{q_K^{fev_K(l)}} = l^{l-1}$$

und somit folgt $h(L^\times) = l$. ☐

Zum allgemeinen Fall: $G_{L/K}$ ist auflösbar, denn:

Definieren wir die *höheren Verzweigungsgruppen*

$$G_i = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \mod \mathfrak{p}_L^{i+1}\}$$

und betrachten $G \trianglerighteq G_0 \trianglerighteq G_1$, so folgt die Auflösbarkeit aus

$$\begin{tikzcd} L \arrow[d, dash, "G_1 \text{ ist } p\text{-Gruppe}"] \\ L^{G_1} \arrow[d, dash, "{\substack{G_0/G_1 \hookrightarrow \overline{L}^\times \\ \overline{\sigma} \mapsto \frac{\sigma(\pi_L)}{\pi_L}}}"] \\ L^{G_0} \arrow[d, dash, "\text{zyklisch von der Ordnung } f"] \\ K \end{tikzcd}$$

(siehe [Ser13, Chapter IV, §2, Prop. 7 bzw. Cor. 5]).

Also gilt $K \overset{l}{\subseteq} K' \subseteq L$. 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

$$\left|H^2(L|K)\right| \;\Big|\; \underbrace{\left|H^2(K'|K)\right|}_{=l=[K':K]} \left|H^2(L|K')\right|\,.$$

Mit Induktion folgt nun $|H^2(L|K')|$ teilt $[L : K']$ und insgesamt ergibt sich die Behauptung. ☐

Beweis von Satz 3.57. Es gilt

$$\begin{aligned} q_{0,m}(K^\times) &= \frac{(K^\times : (K^\times)^m)}{|\mu_m(K)|} \\ \Longleftrightarrow \qquad (K^\times : (K^\times)^m) &= |\mu_m(K)|\, q_{0,m}(K^\times) \end{aligned}$$

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

$$\begin{aligned} q_{0,m}(U_K) &= q_{0,m}(U_K^n)\, \underbrace{q_{0,m}({}^{U_K}/_{U_K^n})}_{\overset{3.58}{=}1} \\ &= \frac{(U_K^n : (U_K^n)^m)}{|\mu_m(K) \cap U_K^n|} \\ &= (U_K^n : U_K^{n+v_K(m)}) = q_K^{v_K(m)} \end{aligned}$$

da

$$\begin{aligned} {}^{U_K^i}/_{U_K^{i+1}} &\cong {}^{\mathfrak{p}_K^i}/_{\mathfrak{p}_K^{i+1}} \cong {}^{\mathcal{O}_K}/_{\mathfrak{p}_K} \\ (1+a)U_K^{i+1} &\leftarrow\!\shortmid a + \mathfrak{p}_K^{i+1} \end{aligned}$$

□

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

$$0 \longrightarrow \ker(f) \longrightarrow A \longrightarrow \operatorname{im}(f) \longrightarrow 0\,,$$
$$0 \longrightarrow \ker(g) \longrightarrow A \longrightarrow \operatorname{im}(g) \longrightarrow 0\,.$$

Dann folgt

$$|A| = |\ker(f)|\,|\operatorname{im}(f)| = |\ker(g)|\,|\operatorname{im}(g)|$$

und somit

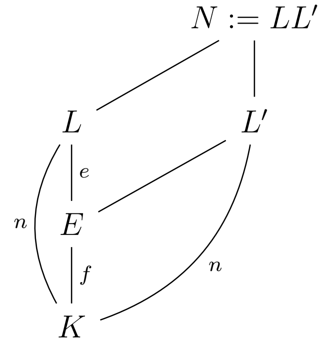
$$\frac{|\ker(f)|}{|\operatorname{im}(g)|} = \frac{|\ker(g)|}{|\operatorname{im}(f)|}\,.$$

□

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 $[L : K]$. Zusammengenommen 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:

$$\begin{aligned} c \in H^2(L|K) \quad &\Longleftrightarrow \quad \operatorname{Res}_L(c) = 1 \in H^2(N|L) \\ &\Longleftrightarrow \quad \operatorname{inv}_{N/L}(\operatorname{Res}_L(c)) = 0 \in \tfrac{1}{[N:L]}\mathbb{Z}/\mathbb{Z} \end{aligned}$$

Also reicht es zu zeigen:

$$\operatorname{inv}_{N/L}(\operatorname{Res}_L(c)) = [L : K] \underbrace{\operatorname{inv}_{L'/K}(c)}_{\in \frac{1}{[L':K]}\mathbb{Z}/\mathbb{Z}} .$$

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:*

$$\begin{tikzcd}
 & M \arrow[d, dash] \arrow[ddddl, dash, bend left=60, "\text{normal}"] \\
 & N := LL' \arrow[dl, dash] \arrow[d, dash] \\
L \arrow[d, dash, "e"] & L' \arrow[dl, dash] \\
E \arrow[d, dash, "f"] & \\
K &
\end{tikzcd}$$

Dann ist N/L unverzweigt. Sei $c \in H^2(L'|K)$. Dann ist $\operatorname{Res}_L(c) \in H^2(N|L)$ und es gilt

$$\operatorname{inv}_{N/L}(\operatorname{Res}_L(c)) = [L : K] \operatorname{inv}_{L'/K}(c) .$$

Beweis von Lemma 3.60. An den 2-Kozyklen liest man ab

$$\operatorname{Res}^{G_{M/K}}_{G_{M/L}} \operatorname{Inf}^{G_{M/K}}_{G_{L'/K}} = \operatorname{Inf}^{G_{M/L}}_{G_{N/L}} \underbrace{\operatorname{Res}^{G_{L'/K}}_{G_{L'/E}}}_{\substack{\text{betrachte dies als} \\ \text{2-Kozykel auf} \\ G_{L'/E} \cong G_{N/L}}} \tag{3.4}$$

Damit ist

$$\operatorname{Res}_L(c) \in H^2(N|L) .$$

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:

$$\begin{tikzcd}
H^2(L'|K) \arrow[r, "\overline{v_K}"] \arrow[d, "\subseteq = \operatorname{Inf}"] & H^2(G_{L'/K}, \mathbb{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "\operatorname{Inf}"] & H^1(G_{L'/K}, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\varphi"] \arrow[d, "\operatorname{Inf}"] & \frac{1}{[L':K]}\mathbb{Z}/\mathbb{Z} \arrow[d, "\subseteq"] \\
H^2(M|K) \arrow[d, "\operatorname{Res}_L"] & H^2(G_{M/K}, \mathbb{Z}) \arrow[d, "e \operatorname{Res}_L"] & H^1(G_{M/K}, \mathbb{Q}/\mathbb{Z}) \arrow[d, "e \operatorname{Res}_L"] & \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z} \arrow[d, "{[L:K]}"] \\
H^2(N|L) \arrow[r, "\overline{v_L}"] & H^2(G_{N/L}, \mathbb{Z}) \arrow[r, "\delta^{-1}"] & H^1(G_{N/L}, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\varphi"] & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}$$

Die unteren vertikalen Abbildungen sind eigentlich die Restriktionen auf die Bilder der oberen vertikalen Abbildungen.

<u>Zum linken Teildiagramm</u>:

$$
\begin{tikzcd}
H^2(L'|K) \ni c \arrow[r, mapsto] \arrow[d, mapsto] & \Big(G^2_{L'/K} \ni \sigma \mapsto v_{L'}(\underbrace{c(\sigma)}_{\in L'^{\times}})\Big) \arrow[d, mapsto] \\
\mathrm{Inf}^{G_{M/K}}_{G_{L'/K}} c \arrow[d, mapsto] & \Big(G^2_{M/K} \ni \tau \mapsto v_{L'}(c(\overline{\tau}))\Big) \arrow[d, mapsto] \\
\mathrm{Res}^{G_{M/K}}_{G_{M/L}} \mathrm{Inf}^{G_{M/K}}_{G_{L'/K}} c \arrow[d, equal, "(3.4)"] & \Big(G^2_{M/L} \ni \tau \mapsto e v_K(c(\overline{\tau}))\Big) \arrow[d, equal] \\
\mathrm{Inf}^{G_{M/L}}_{G_{N/L}} \mathrm{Res}^{G_{L'/K}}_{G_{L'/E}} c \arrow[r, mapsto] & \Big(G^2_{M/L} \ni \tau \mapsto v_L(c(\overline{\tau}))\Big)
\end{tikzcd}
$$

<u>Zum mittleren Teildiagramm</u>: Dies folgt wie bisher üblich.

<u>Zum rechten Teildiagramm</u>: Es ist

$$\varphi_{N/L}\big|_{L'} = \varphi_{L'/K}^{[E:K]} = \varphi^f_{L'/K}\,, \tag{3.5}$$

denn für $a \in L'$ gilt:

$$
\begin{aligned}
\varphi_{N/L}(a) &\equiv a^{q_L} \mod (\mathfrak{p}_N \cap L') \\
&\equiv a^{q_K^f} \mod \mathfrak{p}_{L'} \\
&\equiv \varphi^f_{L'/K}(a) \mod \mathfrak{p}_{L'}
\end{aligned}
$$

Damit erhalten wir

$$
\begin{tikzcd}
\chi \arrow[r, mapsto] \arrow[d, mapsto] & \chi(\varphi_{L'/K}) \arrow[d, mapsto] \\
\mathrm{Inf}^{G_{M/K}}_{G_{L'/K}} \chi \arrow[d, mapsto] & \chi(\varphi_{L'/K}) \arrow[d, mapsto] \\
e\,\mathrm{Res}^{G_{M/K}}_{G_{M/L}} \mathrm{Inf}^{G_{M/K}}_{G_{L'/K}} \chi \arrow[d, mapsto] & [L:K]\chi(\varphi_{L'/K}) \arrow[d, equal] \\
e\chi(\varphi_{N/L}) \arrow[r, equal, "(3.5)"] & e\chi(\varphi^f_{L'/K})
\end{tikzcd}
$$

□

Damit folgt die Aussage des Satzes. □

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 Ω/K_0. Dann sei

$$\mathrm{inv}_{L/K} : H^2(L|K) \xrightarrow{\cong} {}^{\frac{1}{[L:K]}\mathbb{Z}}\!/\!_{\mathbb{Z}}$$

definiert durch

$$\mathrm{inv}_{L/K}(c) := \mathrm{inv}_{L'/K}(c)$$

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.

$$[N' : K] = [N : K]\,, \qquad [L' : K] = [L : K]\,.$$

Dann gilt für $c \in H^2(L|K)$

$$\mathrm{inv}_{N/K}(c) = \mathrm{inv}_{N'/K}(c) = \mathrm{inv}_{L'/K}(c) = \mathrm{inv}_{L/K}(c)\,.$$

Zu Axiom 3.24.II.(2): Wir haben jetzt eine injektive Abbildung

$$Br(K) = H^2(K) = \bigcup_{L/K \text{ normal}} H^2(L|K) \overset{\mathrm{inv}_K}{\hookrightarrow} {}^{\mathbb{Q}}\!/\!_{\mathbb{Z}}$$

(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:

$$\mathrm{inv}_{N/L}(\underbrace{\mathrm{Res}_L(c)}_{\in H^2(N|L)}) = [L : K]\,\mathrm{inv}_{N/K}(c)$$

Dazu zeigt man für beliebige L/K

$$\mathrm{inv}_L(\mathrm{Res}_L(c)) = [L : K]\,\mathrm{inv}_K(c)$$

für $c \in H^2(K)$. Dies folgt aus Lemma 3.60. □

Satz 3.63. *Sei L/K eine abelsche Erweiterung von $\mathfrak{p}$-adischen Körpern. Sei*

$$G_0 := \{\sigma \in G = \mathrm{Gal}(L|K) \,|\, \sigma(\alpha) \equiv \alpha \mod \mathfrak{p}_L \ \forall \alpha \in \mathcal{O}_L\}$$

die Verzweigungsgruppe *und*

$$G_1 = \{\sigma \in G \,|\, \sigma(\alpha) \equiv \alpha \mod \mathfrak{p}_L^2 \ \forall \alpha \in \mathcal{O}_L\}$$

die wilde Verzweigungsgruppe. *Dann gilt*

(1) $(\_\,, L/K) : U_K \twoheadrightarrow G_0$,

(2) $(\_\,, L/K) : U_K^1 \twoheadrightarrow G_1$.

Beweis. Für (1) betrachte

$$\begin{tikzcd}
L \arrow[d, dash, "e"] \arrow[d, phantom, bend left, "G_0"'] \\
T = L^{G_0} \arrow[d, dash, "f"] \arrow[d, phantom, bend left, "\text{unverzweigt}"'] \\
K \arrow[uu, dash, bend left=60, "G"]
\end{tikzcd}$$

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 $(a, L/K) = \tau$.

<u>Ziel</u>: 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.

<u>Zu (2)</u>: G_1 ist die p-Sylowuntergruppe von G_0, denn:

$$G_0/G_1 \hookrightarrow U_L/U_L^1 \cong \overline{L}^\times \tag{3.6}$$

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)

$$U_K/U_K^n \xrightarrow{(\_\,, L/K)} \!\!\!\!\rightarrow G_0 \quad .$$

Die p-Sylowuntergruppe von U_K/U_K^n ist gerade U_K^1/U_K^n, denn:

$$\begin{aligned} U_K^i/U_K^{i+1} &\cong \mathfrak{p}_K^i/\mathfrak{p}_K^{i+1} \cong \mathcal{O}_K/\mathfrak{p}_K = \overline{K} \\ (1+x)U_K^{i+1} &\leftarrow\!\shortmid x + \mathfrak{p}_K^{i+1} \end{aligned}$$

$\square$

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 π_L von L. κ_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

$$\begin{aligned}&\sigma(u) \equiv u \mod \mathfrak{p}_L^{i+1}\\ \iff\quad &\frac{\sigma(u)}{u} \equiv 1 \mod \mathfrak{p}_L^{i+1}\end{aligned}$$

Weiter ist zu zeigen, dass $\frac{\sigma(\pi_L)}{\pi_L} \in U_L^i$. Dies gilt, da

$$\begin{aligned}&\sigma(\pi_L) \equiv \pi_L \mod \mathfrak{p}_L^{i+1}\\ \iff\quad &\frac{\sigma(\pi_L)}{\pi_L} \equiv 1 \mod \mathfrak{p}_L^{i}\end{aligned}$$

κ_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:

$$\begin{array}{ccccccccccccc} {}^{K^\times}\!/\!{}_{N_{L/K}(L^\times)} & \geq & {}^{U_K}\!/\!{}_{N_{L/K}U_L} & \geq & {}^{U_K^1}\!/\!{}_{N_{L/K}U_L^{\psi(1)}} & \geq & \cdots & \geq & {}^{U_K^n}\!/\!{}_{N_{L/K}U_L^{\psi(n)}} & \geq & \cdots & \geq & 1\\ \wr\wr & & & & & & & & (*)\big\downarrow\cong & & & & \\ G & & & & & & & & G^n = G_{\psi(n)} & & & & \end{array}$$

Hierbei ist ψ 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

$$\left| {}^{K^\times}\!/_{N_{L/K}(L^\times)} \right| = [L:K] =: m$$

für eine endliche abelsche Erweiterung L/K. Damit folgt $(K^\times)^m \le N_{L/K}(\text{Ł}^\times)$. In der Übung wurde gezeigt, dass $(K^\times)^m \le K^\times$ 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 $I \le K^\times$ offen und $[K^\times : I] =: m < \infty$. Dann ist I eine Normengruppe.*

Beweis. Es ist $(K^\times)^m \le I \le K$, d.h. es genügt zu zeigen: $(K^\times)^m$ ist Normengruppe.

Erinnerung 3.66. Sei $J \le I \le K^\times$ 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

$$\begin{tikzcd} {}^{K^\times}\!/_J \arrow[r, "(\,\text{—}\,{,}L/K)", "\cong"'] & \mathrm{Gal}(L|K) =: G \\ {}^{I}\!/_J \arrow[u, phantom, "\rotatebox{90}{$\le$}"] \arrow[r, "\cong"] & H \arrow[u, phantom, "\rotatebox{90}{$\le$}"] \end{tikzcd}$$

Sei $a \in I$. Betrachte

$$\begin{tikzcd} L \arrow[d, dash, "H"] \arrow[dd, dash, bend right=60, "G"'] \\ M = L^H \arrow[d, dash, "G/H"] \\ K \end{tikzcd}$$

Dann ist

$$1 = (a, L/K)\big|_M = (a, M/K) \quad \Longleftrightarrow \quad a \in N_{M/K}(M^\times)\,.$$

Also folgt $I \le N_{M/K}(M^\times)$.

Andererseits gilt

$$J = \overbrace{N_{L/K}(L^\times) \le \underbrace{N_{M/K}(M^\times) \le K^\times}_{[M:K]}}^{[L:K]} \quad .$$

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

$$[K^\times : (K^\times)^m] = |\mathrm{Gal}(L|K)| = [K^\times : I_L] \tag{3.7}$$

und somit $(K^\times)^m = I_L$.

$\square$

<u>Zum allgemeinen Fall</u>: Sei $K_1 := K(\mu_m)$. Sei L/K_1 abelsch mit $(K_1^\times)^m = N_{L/K_1}(L^\times)$. Sei $\widetilde{L}/L$ endlich, sodass $\widetilde{L}/K$ galoissch ist:

$$\begin{tikzcd}
\widetilde{L} \arrow[d, dash] \arrow[ddd, dash, bend left, "\text{galoissch}"] \\
L \arrow[d, dash] \arrow[d, dash, bend right, "\text{abelsch}"'] \\
K_1 \arrow[d, dash] \\
K
\end{tikzcd}$$

Es gilt:

$$\begin{aligned}
N_{\widetilde{L}/K}(\widetilde{L}^\times) &= N_{K_1/K}(N_{\widetilde{L}/K_1}(\widetilde{L}^\times)) \\
&\subseteq N_{K_1/K}(N_{L/K_1}(L^\times)) \\
&= N_{K_1/K}((K_1^\times)^m) \\
&= (N_{K_1/K}(K_1^\times))^m \subseteq (K^\times)^m
\end{aligned}$$

Also ist $(K^\times)^m$ auch eine Normengruppe. $\square$

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)$\Longleftrightarrow$(2) ist der Existenzsatz 3.65 zusammen mit der Vorbemerkung.

(2)$\Longleftrightarrow$(3) gilt nach Blatt 10, Aufgabe 1.

(2)$\Longrightarrow$(4) ist klar.

Für (4)$\Longrightarrow$(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 $\operatorname{char}(K) = 0$. Betrachte

$$0 \longrightarrow \mu_m \longrightarrow (K^c)^\times \xrightarrow{m} (K^c)^\times \longrightarrow 0\,.$$

Sei $G = G_K = \operatorname{Gal}(K^c|K)$. 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 μ_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.