Zur Fontaine-Mazur-Vermutung für Erweiterungen mit beschränkter Verzweigung von CM-Körpern [1]

19. Januar 2002

Gabor Wiese

[1]Dies ist eine leicht modifizierte Version meiner Diplomarbeit, die ich 2001 an der Uni Heidelberg unter der Betreuung von Prof. Kay Wingberg geschrieben habe. Kommentare, Hinweise auf Fehler etc. können gerne an mich gesendet werden: `gabor@maths.univ-rennes1.fr`

Einleitung

Die vorliegende Diplomarbeit basiert auf der Arbeit [W] und führt deren Hauptresultate aus. Insbesondere werden erwähnte Verallgemeinerungen im Detail durchgeführt.

Im Rahmen ihrer Vermutungen zu geometrischen Galois-Darstellungen haben Fontaine und Mazur in [FM] die folgende Vermutung aufgestellt (Conjecture 5a):

(1) Vermutung. *Sei k ein Zahlkörper, p eine Primzahl, S eine endliche Menge von Primstellen, welche keine über p liegende enthalte, und $G_{K,S}$ die Galois-Gruppe der maximalen außerhalb S unverzweigten Erweiterung von k in einem vorgegebenen algebraischen Abschluß $\overline{k}$ von k.*

Ist H ein Quotient von $G_{K,S}$, und ist H p-adisch analytisch, dann ist H endlich.

Es ist ein bemerkenswerter Umstand, daß sich p-adisch analytische Gruppen rein gruppentheoretisch charakterisieren lassen. Es gilt nämlich folgendes Resultat von Lazard (siehe [DDMS], Theorem 8.1).

(2) Theorem. *Eine topologische Gruppe G hat die Struktur einer p-adischen analytischen Gruppe genau dann, wenn sie eine offene, endlich erzeugte potenzreiche Untergruppe enthält.*

Eine Pro-p-Gruppe heißt im Fall $p \neq 2$ *potenzreich* (engl.: *powerful*), falls $G/\overline{G^p}$ abelsch ist, wobei $\overline{G^p}$ den Abschluß des Erzeugnisses der p-ten Potenzen von G bezeichnet. Eine weitere wichtige Klasse von Pro-p-Gruppen sind die *uniformen* Gruppen, welche als die endlich erzeugten torsionsfreien potenzreichen Gruppen definiert werden können. Ab einem gewissen Index sind die Gruppen der absteigenden p-Zentralreihe einer potenzreichen Gruppe stets uniform.

Eine natürliche Frage lautet daher:

> Gibt es unendliche unverzweigte p-Erweiterungen eines Zahlkörpers, deren Galois-Gruppe potenzreich bzw. uniform ist?

Man möchte, um sich dem Problem zu nähern, Zusatzstrukturen ausnutzen können. Daher ist in [W] der Ansatz gewählt, *CM-Körper* zu betrachten. Dies sind total imaginäre quadratische Erweiterungen total reeller Zahlkörper. Sie sind dadurch ausgezeichnet, daß auf ihnen eine Involution, die *komplexe Konjugation*, operiert. Diese liefert für bestimmte galoissche Erweiterungen $L|k^+$ des total reellen Teilkörpers k^+ eine Aktion auf $G(L|k)$, welche im Falle einer abelschen Erweiterung $L|k$ kanonisch ist. In jedem Fall erhält man jedoch eine kanonische Aktion auf den Kohomologiegruppen. Diese Aktion ist verträglich mit allen wichtigen Abbildungen von Kohomologiegruppen, insbesondere auch dem Reziprozitätshomomorphismus der globalen Klassenkörpertheorie. Daher kann z. B. die Aktion der Involution auf der Galois-Gruppe der maximalen unverzweigten abelschen Erweiterung auf der Idealklassengruppe mithilfe der vom CM-Körper bereitgestellten komplexen Konjugation studiert werden.

Die Ergebnisse dieser Arbeit entstehen dadurch, daß zunächst untersucht wird, welche Eigenschaften potenzreiche Gruppen haben, auf denen eine Involution operiert. Diese werden dann verglichen mit Resultaten der Analyse der körpertheoretischen Situation.

Ist A eine abelsche Gruppe, auf der eine Involution σ operiert, so zerfällt A in

$$A = A^+ \oplus A^-,$$

wobei σ auf A^+ trivial und auf A^- durch $\sigma a = -a$ operiert, vorausgesetzt, daß Multiplikation mit 2 in A ein Automorphismus ist.

Wir fixieren eine Primzahl $p \neq 2$. Ist G eine potenzreiche Pro-p-Gruppe, auf der eine Involution operiert, so haben wir die direkte Zerlegung

$$G/G^p = (G/G^p)^+ \oplus (G/G^p)^-.$$

So wie wir die $\mathbb{F}_p$-Dimension von G/G^p als *Erzeugendenrang* $d(G)$ von G auffassen können, kann die Dimension von $(G/G^p)^\pm$ als Erzeugendenrang von $(G^{ab})^\pm$, bezeichnet mit $d(G)^\pm$, interpretiert werden.

Diese Zahlen spielen eine zentrale Rolle in unseren Betrachtungen, denn es gilt nach Satz (2.2.21)

$$d(G)^+ \cdot d(G)^- \leq d(G)^- + dim_{\mathbb{F}_P}\ ({}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^-). \tag{1}$$

Wir haben sogar Gleichheit, falls G uniform mit endlicher Abelisierung ist.

Es ist ein bekannter Satz, daß

$$dim_{\mathbb{F}_P}\ H^2(G, \mathbb{Z}/p\mathbb{Z}) = r(G)$$

den *Relationenrang* von G angibt, falls G eine Pro-p-Gruppe ist. Im Fall uniformer Gruppen läßt sich dieser explizit aus dem Erzeugendenrang berechnen:

$$r(G) = \binom{d(G)}{2}. \tag{2}$$

Wir zeigen ein Resultat aus [W], welches besagt, daß sogar stärker gilt (Korollar (2.2.18)):

$$dim_{\mathbb{F}_P}\ H^2(G, \mathbb{Z}/p\mathbb{Z})^+ = \binom{d(G)^+}{2} + \binom{d(G)^-}{2} \quad \text{und} \tag{3}$$

$$dim_{\mathbb{F}_P}\ H^2(G, \mathbb{Z}/p\mathbb{Z})^- = d(G)^+ \cdot d(G)^-. \tag{4}$$

Daraus schließt man z. B., daß eine uniforme Gruppe mit endlicher Abelisierung und Erzeugendenrang $d(G) \leq 3$ nur die Möglichkeiten

$$(d(G)^+ = 1 \text{ und } d(G)^- = 2) \quad \text{oder} \quad (d(G)^+ = 3 \text{ und } d(G)^- = 0) \tag{5}$$

zuläßt (vgl. Satz (2.2.22)).

Es ist von entscheidender Wichtigkeit, $dim_{\mathbb{F}_p}\ ({}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^-)$ zu kennen, um aus (1) Schlüsse ziehen zu können. Wir werden sehen, daß diese Dimension in vielen Fällen kleiner gleich 1 ist, woraus sich für $d(G)^+ \neq 1$ sofort ergibt, daß nur $d(G) \leq 3$ auftreten kann.

Dieses Resultat erhält man aus dem Dualitätssatz

$$\hat{H}^i(G, E) \cong \hat{H}^{2-i}(G, \mathbb{Q}/\mathbb{Z})^\vee \quad \text{für alle } i \in \mathbb{Z}, \tag{6}$$

welcher in den beiden folgenden Fällen gilt (vgl. Theoreme (1.2.29) bzw. (1.2.30)):

(I)
- S sei eine (möglicherweise leere) Menge von Primstellen eines Zahlkörpers k.
- $L_S(p)|k$ sei die maximale unverzweigte galoissche p-Erweiterung von k, in welcher alle Stellen aus S voll zerlegt sind.
- $G := G(L_S(p)|k)$ sei die Galois-Gruppe dieser Erweiterung.
- $E := E_S(L_S(p)) = \varinjlim_{L_S(p)\supset K\supset k,\ K|k \text{ endlich}} E(K)$, wobei $E(K) := E_S(K)$ die Gruppe der S-Einheiten einer endlichen galoisschen Körpererweiterung $L_S(p) \supset K \supset k$ bezeichnet.

(II)

- S sei eine endliche Menge von Primstellen eines Zahlkörpers k.
- In S sei keine über p liegende Stelle (deren Menge wir mit S_p bezeichnen) enthalten: $S_p \cap S = \emptyset$.
- $k_S(p)|k$ sei die maximale außerhalb S unverzweigte galoissche p-Erweiterung von k.
- $G := G(k_S(p)|k)$ sei die Galois-Gruppe dieser Erweiterung.
- $E(K) := \mathcal{O}_{K,\mathfrak{m}}^{\times} := \{a \in \mathcal{O}_K \mid a \in \mathcal{U}_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \text{ für alle } \mathfrak{p}\}$, wobei $k_S(p) \supset K$ eine endliche galoissche Körpererweiterung von k sei. Dabei ist $\mathfrak{m}$ der Modul $\prod_{\mathfrak{p} \in S} \mathfrak{p}$, und $\mathcal{U}^{(n_{\mathfrak{p}})}$ bezeichnet die höheren Einseinheiten. Für deren Definition an unendlichen Stelle siehe S. 30.
- $E := \mathcal{O}_{k_S(p),\mathfrak{m}}^{\times} = \varinjlim_{K} E(K)$, wobei der direkte Limes über die in $k_S(p)$ enthaltenen endlichen galoisschen Erweiterungen von k läuft.

Liegt ein CM-Körper zugrunde, so ist diese Dualität kompatibel mit der Aktion der komplexen Konjugation. Im Fall (I) fordern wir zusätzlich, daß keine Primstelle aus S in der Erweiterung $k|k^+$ zerfalle.

Aus dem Dualitätssatz werden wir eine Surjektion

$$\mu(k)/p \supseteq (E(k)/p)^- \twoheadrightarrow ({}_p\hat{H}^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^-)^\vee \tag{7}$$

($\mu(k)$ sind die in k enthaltenen Einheitswurzeln) schließen können, welche sofort die behauptete Dimensionsbeschränkung liefert.

Die benutzte Kohomologie ist die *Tate-Kohomologie*, welche zunächst für endliche Gruppen definiert ist. Man definiert im Fall proendlicher Gruppen die $\hat{H}^i(G, A)$ als die gewöhnliche Kohomologie für $i > 0$. Für $i \leq 0$ setzt man

$$\hat{H}^i(G, A) = \varprojlim_{U \lhd G \text{ offen}} \hat{H}^i(G/U, A^U), \tag{8}$$

wobei der projektive Limes via den *Deflationen* zu bilden ist.

Auf diese Weise erhält man keinen kohomologischen Funktor. Man bekommt dennoch eine proendliche Version des Satzes von Nakayama-Tate und des Dualitätssatzes von Poitou, was in der Arbeit [S] studiert wurde. Wir benötigen jedoch nur die Verallgemeinerung des Satzes von Nakayama-Tate, denn dieser liefert im Zusammenspiel mit dem Reziprozitätshomomorphismus und dem Hauptidealsatz den Dualitätssatz (6).

Um die Gemeinsamkeiten der Fälle (I) und (II) herauszustellen, haben wir den Dualitätssatz zunächst in der Sprache der abstrakten Klassenkörpertheorie bewiesen und schließlich auf die konkreten Situationen angewendet.

Für die Idealklassengruppe von CM-Körpern gilt, falls $\mu_p \subset k$ gegeben ist, der Leopoldtsche Spiegelungssatz:

$$d(\mathcal{C}l_k)^+ \leq 1 + d(\mathcal{C}l_k)^-. \tag{9}$$

Dieses Ergebnis läßt sich einfach auf die Fälle (I) und (II) verallgemeinern. Wir werden den Satz benutzen, um zu schließen, daß $d(\mathcal{C}l_k)^-$ ungleich Null ist.

Die zusammengestellten Resultate führen auf folgendes Theorem, das Hauptergebnis dieser Arbeit. Es stellt eine Verallgemeinerung der Resultate der Arbeit [W] dar, in der nur unverzweigte Erweiterungen betrachtet werden.

(3) Theorem. *Sei p eine ungerade Primzahl, sei $k|k^+$ ein CM-Körper, der die p-ten Einheitswurzeln enthält, und sei $\mu(k)(p) = \mu_{p^s}(k)$ die Gruppe der Einheitswurzeln von p-Potenzordnung in k. In den Situationen*

(I) S sei eine beliebige Stellenmenge von k^+ mit der Eigenschaft, daß keine Primstelle in der Erweiterung $k|k^+$ zerfällt, und $G = G(L_S(p)|k)$ sei die Galois-Gruppe der maximalen galoisschen p-Erweiterung von k, in der alle Stellen von S voll zerlegt sind.

(II) S sei eine endliche Stellenmenge von k^+ mit $S_p \cap S = \emptyset$, und $G = G(k_S(p)|k)$ sei die Galois-Gruppe der maximalen außerhalb von S unverzweigten galoisschen p-Erweiterung von k.

gilt:

Ist G potenzreich, dann ist G endlich oder $d(G)^+ = 1$.
Ist $d(G)^+ = 1$ und gilt

im Fall (I): $k(\mu_{p^{s+1}})|k$ ist nicht unverzweigt und in S voll zerlegt,
im Fall (II): $k(\mu_{p^{s+1}})|k$ ist nicht unverzweigt außerhalb S und $\mu_p(k) \subseteq \mathcal{O}^\times_{K,\mathfrak{m}}$,

dann ist G nicht uniform.

Im Folgenden werden wir noch auf die Struktur der Arbeit näher eingehen.

Die Arbeit gliedert sich in zwei Kapitel. Im ersten werden wir die beiden benötigten Versionen des Dualitätssatzes beweisen. Dazu werden wir im ersten Abschnitt zunächst eine Version in der Sprache der abstrakten Klassenkörpertheorie herleiten, und diese dann im zweiten Abschnitt auf die konkreten Situationen anwenden.

Den ersten Abschnitt beginnen wir mit einer detaillierten Einführung der Tate-Kohomologie. Danach werden wir wichtige Begriffe der abstrakten Klassenkörpertheorie und die Pontrjaginsche Dualitätstheorie erwähnen. In einem längeren Teilabschnitt widmen wir uns dann diversen Dualitätssätzen. U. a. wird der Satz von Nakayama-Tate für endliche und proendliche Gruppen bewiesen. Die Ergebnisse dieses Teilabschnittes fließen danach ein in einen Kurzüberblick über die abstrakte Klassenkörpertheorie. Schließlich wird der für die Arbeit zentrale abstrakte Dualitätssatz formuliert und bewiesen.

Den zweiten Abschnitt beginnen wir mit einer Einführung der Sprache der globalen Klassenkörpertheorie, wie wir sie benötigen werden. Danach leiten wir zwei exakte Sequenzen her, auf denen die Dualitätssätze beruhen. Anschließend geben wir einen Überblick über die Hauptsätze der globalen Klassenkörpertheorie. Im darauf folgenden Teilabschnitt analysieren wir die Situationen (I) und (II) genauer. Daraufhin gehen wir auf Versionen des Hauptidealsatzes in beiden Fällen ein, denn dieser ist ein wichtiger Bestandteil des für die Arbeit zentralen Dualitätssatzes. Letzteren beweisen wir in beiden Fällen in den letzten beiden Teilabschnitten.

Das zweite Kapitel beschäftigt sich mit Galois-Gruppen von CM-Körpern. Im ersten Abschnitt werden wir Pro-p-Gruppen untersuchen, insbesondere potenzreiche Gruppen. Dazu werden wir zunächst Erzeuger und Relationen, sowie deren kohomologische Interpretation betrachten, dann auf Filtrierungen eingehen, welche für die danach zusammengefaßte Theorie der potenzreichen und uniformen Gruppen benötigt werden.

Daraufhin werden im zweiten Abschnitt gruppentheoretische Konsequenzen einer Aktion einer Involution auf einer potenzreichen Gruppe behandelt; und zwar zunächst im einfachen Fall abelscher Gruppen und, nach einem Studium der Aktion auf den Kohomologiegruppen, schließlich für Pro-p-Gruppen und potenzreiche Gruppen.

Im dritten Abschnitt werden wir auf die körpertheoretische Situation eingehen, indem wir CM-Körper, ihre Kohomologietheorie und ihre Ideal- und Strahlklassengruppen näher betrachten.

Schließlich werden wir im vierten Abschnitt die Hauptresultate herleiten.

Einen herzlichen Dank möchte ich Herrn Wingberg aussprechen, der für meine Fragen stets ein offenes Ohr und gute Antworten hatte.

Ich danke auch Otmar Venjakob, Denis Vogel und Markus Fenn für nützliche Diskussionen.

Inhaltsverzeichnis

I. Ein Dualitätssatz

1.1. Ein abstrakter Dualitätssatz

In [W] ist ein Dualitätssatz für Tate-Kohomologiegruppen von Galois-Gruppen bestimmter Erweiterungen der Ausgangspunkt für die Ergebnisse zur Fontaine-Mazur-Vermutung. In diesem Abschnitt werden wir uns von den konkreten Vorgaben lösen und eine abstrakte Version des Dualitätssatzes beweisen, die eine Übertragung auf eine leicht modifizierte Situation ermöglicht.

1.1.1. Tate-Kohomologie

Wir wollen kurz die grundlegenden Definitionen und Sätze über Homologie und Kohomologie von Gruppen zusammenfassen und die Tate-Kohomologie definieren, die im Zentrum unseres Interesses steht.

Vorbereitungen zur Homologie und Kohomologie

Sei G eine Gruppe (möglicherweise unendlich und ohne Topologie). Zunächst wenden wir unser Augenmerk den G-Moduln zu. Seien A, B zwei G-Moduln (wenn nichts anderes explizit gefordert ist, wollen wir darunter immer Linksmoduln verstehen). Dann sind $A \otimes_{\mathbb{Z}} B$ und $Hom(A, B)$ G-Moduln unter den Aktionen

$$g.(a \otimes b) := g.a \otimes g.b \quad \text{bzw.} \quad (g.\phi)(a) := g.(\phi(g^{-1}.a)).$$

$\mathbb{Z}$ wollen wir stets mit der trivialen G-Aktion von rechts und von links versehen. Wir wollen ferner $A \otimes_{\mathbb{Z}[G]} B$ erklären, wofür wir auch $A \otimes_G B$ schreiben werden. Dazu fassen wir A auf als Rechtsmodul mit $a.g := g^{-1}.a$. Per Definition gilt also $a.g \otimes_G b = a \otimes_G g.b$ bzw. $g.a \otimes_G g.b = a.g^{-1} \otimes_G g.b = a \otimes_G b$. In Verallgemeinerung der oben erklärten Aktion erhalten wir daher einen trivialen G-Modul.

Wir definieren als $I_G = (s - 1 | s \in G)$ den Kern der *Augmentation* $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}, g \mapsto 1$. Die Abbildung

$$\mathbb{Z} \otimes_G A \to A/I_G A =: A_G, \quad n \otimes_G a \mapsto na + I_G A$$

ist ein Isomorphismus. Damit ist A_G der größte Faktormodul von A, auf dem G trivial operiert. Ein weiterer Isomorphismus ist gegeben durch

$$A \otimes_G B \to (A \otimes_{\mathbb{Z}} B)_G, \quad a \otimes_G b \mapsto (a \otimes_{\mathbb{Z}} b) + I_G(A \otimes_{\mathbb{Z}} B).$$

Ferner bemerken wir, daß

$$Hom_G(A, B) := \{f \in Hom(A, B) \mid g.f(a) = f(g.a)\ \forall a \in A\} = (Hom(A, B))^G$$

und speziell $A^G = Hom_G(\mathbb{Z}, A)$ gilt.

Wir betrachten die *Standardauflösung* $F(G)_\bullet$ von $\mathbb{Z}$ über $\mathbb{Z}[G]$

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\epsilon} F(G)_0 := \mathbb{Z}[G] \xleftarrow{\partial_1} F(G)_1 := \mathbb{Z}[G^2] \xleftarrow{\partial_2} \ldots,$$

wobei wir definieren:

$$\partial_n := \sum_{i=0}^{n} (-1)^i d_i \quad \text{und} \quad d_i(g_0, \ldots, g_n) := (g_0, \ldots, \hat{g}_i, \ldots, g_n).$$

Setzen wir $h_r := g_{r-1}^{-1} g_r$, so erhalten wir die Identität

$$(g_0, g_1, g_2, \ldots, g_n) = g_0.(1, h_1, h_1 h_2, \ldots, h_1 h_2 \ldots h_n) =: g_0.[h_1|h_2|\ldots h_n].$$

Die Symbole $[h_1|h_2|\ldots|h_n]$ mit beliebigen $h_i \in G$ bilden somit eine $\mathbb{Z}[G]$-Basis von $F(G)_n$, bzw. $F(G)_n = \mathbb{Z}[G] \otimes_{\mathbb{Z}}$ (freie abelsche Gruppe auf $[h_1|h_2|\ldots|h_n]$). Man berechnet die Wirkung von d_i auf dieser Basis zu

$$d_i[h_1|\ldots|h_n] = \begin{cases} h_1[h_2|\ldots|h_n] & i = 0 \\ [h_1|\ldots|h_i h_{i+1}|\ldots|h_n] & 0 < i < n \\ [h_1|\ldots|h_{n-1}] & i = n. \end{cases}$$

Homologie

Tensorieren wir die Standardauflösung über $\mathbb{Z}[G]$ mit dem G-Modul A, bzw. tensorieren wir über $\mathbb{Z}$ mit A und nehmen den größten G-invarianten Faktormodul, so erhalten wir den Komplex (nach Komposition der ersten beiden Abbildungen)

$$0 \leftarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \leftarrow \mathbb{Z}[G^2] \otimes_{\mathbb{Z}[G]} A \leftarrow \mathbb{Z}[G^3] \otimes_{\mathbb{Z}[G]} A \leftarrow \ldots,$$

dessen Homologie wir mit $H_n(G, A)$ bezeichnen wollen. Die Elemente von $\mathbb{Z}[G^{n+1}] \otimes_{\mathbb{Z}[G]} A$ nennen wir *n-Ketten*.

$H_*(G, \cdot)$ bildet einen *positiven homologischen Funktor* bzgl. der G-Moduln, d.h. für jede kurze exakte Sequenz $0 \to A \to B \to C \to 0$ von G-Moduln gibt es für jedes n einen Verbindungshomomorphismus (der nicht eindeutig sein muß, aber natürlich gewählt werden kann) $\delta_n : H_{n+1}(G, C) \to H_n(G, A)$, so daß gelten:

(i) Für jedes kommutative Diagramm

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

mit exakten Zeilen kommutiert das folgende Diagramm:

$$\begin{array}{ccc} H_{n+1}(G, C) & \xrightarrow{\delta_n} & H_n(G, A) \\ {\scriptstyle H_{n+1}(h)}\downarrow & & {\scriptstyle H_n(f)}\downarrow \\ H_{n+1}(G, C') & \xrightarrow{\delta_n} & H_n(G, A') \end{array}$$

(ii) Für jede kurze exakte Sequenz $0 \to A \to B \to C \to 0$ ist die folgende Sequenz (die *lange exakte Sequenz*) für alle n exakt:

$$H_n(G, B) \leftarrow H_n(G, A) \xleftarrow{\delta_n} H_{n+1}(G, C) \leftarrow H_{n+1}(G, B) \leftarrow H_{n+1}(G, A)$$

Die *Positivität* bedeutet, daß $H_n(G, A)$ für alle $n < 0$ trivial ist.

(1.1.1) Lemma. *Sei A ein projektiver G-Modul. Dann gelten:*

(a) A ist homologisch trivial, d.h. $H_n(G, A) = 0$ für alle $n > 0$.

(b) A_U ist ebenfalls projektiv als G/U-Modul für einen Normalteiler $U \lhd G$.

Beweis. Für (a) siehe z.B. [Br]. Zu (b) sei $M \twoheadrightarrow N$ eine Surjektion zweier G/U-Moduln, und $\phi : A_U \to N$ ein Homomorphismus. Durch $G \twoheadrightarrow G/U$ werden M und N auch zu G-Moduln, weshalb ein G-Modulhomomorphismus $\psi : A \to M$ existiert. Dieser faktorisiert aber über A_U. □

Wir bemerken noch, daß zu jedem G-Modul A ein freier (und damit projektiver) G-Modul F existiert zusammen mit einer Surjektion $F \twoheadrightarrow A$. Diese Eigenschaft bedeutet, daß $H(G, \cdot)$ ein (bzgl. der projektiven G-Moduln) *effaçabler* homologischer Funktor ist.

Wir wollen kurz den Verbindungshomomorphismus $\delta_0 : H_1(G, C = B/A) \to H_0(G, A)$ explizit beschreiben (vgl. [AW]). Ein 1-Zyklus in $H_1(G, B/A)$ hat die Form $f = \sum_g [g] \otimes_G (b_g + A)$, wobei die b_g fast alle Null sind. Unter der Randabbildung gilt: $df = \sum_g (1 - g^{-1})(b_g + A) = 0$. Setzen wir $\overline{f} := \sum_g [g] \otimes_G b_g \in H_1(G, B)$, so gilt folglich $d\overline{f} \in A_G$. Damit erhalten wir die explizite Beschreibung:

$$\delta_0(\sum_g [g] \otimes_G (b_g + A)) = \sum_g (1 - g^{-1}) b_g + I_G A$$

Man überzeugt sich leicht, daß dies unabhängig ist von der Auswahl der b_g.

Sei $H < G$ eine Untergruppe. Wir definieren für einen H-Modul

$$Ind_H^G A := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A.$$

Ist $H = 1$ und X eine abelsche Gruppe, so nennen wir $Ind_1^G X$ einen *induzierten* Modul. Es gilt das *Lemma von Shapiro*:

$$H_n(G, Ind_H^G A) \cong H_n(H, A) \text{ für alle } n \geq 0.$$

Speziell folgt, daß die Homologiegruppen $H_n(G, Ind_1^G X)$ für alle $n \geq 1$ trivial sind.

Seien $\phi : G \to H$ und $\theta : A \to B$ Gruppenhomomorphismen für einen G-Modul A und einen H-Modul B. Das Paar (ϕ, θ) heißt *verträglich*, wenn gilt

$$\theta(g.a) = \phi(g).\theta(a),$$

oder äquivalent dazu, wenn θ ein G-Modulhomorphismus ist, wobei B via ϕ als G-Modul aufgefaßt wird.

(1.1.2) Bemerkung. *Ein verträgliches Paar (ϕ, θ) wie oben induziert eine eindeutige Familie von Homomorphismen*

$$(\phi, \theta)_n : H_n(G, A) \to H_n(H, B)$$

durch Festlegung auf den Ketten

$$\sum_{\underline{g}} [g_1 | \ldots | g_n] \otimes_G a_{\underline{g}} \mapsto \sum_{\underline{g}} [\phi(g_1) | \ldots | \phi(g_n)] \otimes_H \theta(a_{\underline{g}}),$$

wobei $\underline{g}$ das n-Tupel $g_1, \ldots, g_n$ bezeichne.

Beweis. Die Verträglichkeit impliziert $\delta \circ (\phi, \theta) = (\phi, \theta) \circ \delta$, weshalb Zykeln in Zykeln und Ränder in Ränder überführt werden. □

Wir wollen dies zur Definition einiger wichtiger Abbildungen verwenden:

- Für eine Untergruppe $H < G$ und einen G-Modul A erhalten wir aus der Einbettung $H \hookrightarrow G$ und der Identität auf A die *Korestriktion*

$$\text{cor} : H_n(H, A) \to H_n(G, A).$$

- Für einen Normalteiler $U \lhd G$ haben wir die natürlichen Projektionen $\phi : G \to G/U$ und $\theta : A \to A/I_U A = A_U$, welche ein verträgliches Paar bilden. Dieses liefert die *Koinflation*

$$\mathrm{coinf} : H_n(G, A) \to H_n(G/U, A_U).$$

- Sei wiederum $H < G$ eine Untergruppe, A ein G-Modul und $g \in G$. Wir erhalten ein verträgliches Paar durch $\phi_g : H \to gHg^{-1}, h \mapsto ghg^{-1}$ und $\theta_g : A \to A, a \mapsto g.a$. Dies liefert Homomorphismen

$$H_n(H, A) \to H_n(gHg^{-1}, A).$$

  Für einen Normalteiler $H \lhd G$ erhält man so eine G-Aktion auf den Homologiegruppen.

Der folgende Satz liefert u.a. eine natürliche Verträglichkeit der so definierten Abbildungen mit Verbindungshomomorphismen.

(1.1.3) Satz. *Sei $\phi : G \to H$ ein Gruppenhomomorphismus und Θ ein Funktor der G-Moduln in die H-Moduln, so daß es zu jedem G-Modul A einen G-Modulhomomorphismus $\theta_A : A \to \Theta A$ gibt (d.h. ϕ und θ_A sind verträglich), so daß das folgende Diagramm von G-Moduln kommutiert:*

$$\begin{tikzcd} A \arrow[r, "\theta_A"] \arrow[d, "f"'] & \Theta A \arrow[d, "\Theta(f)"] \\ A' \arrow[r, "\theta_{A'}"] & \Theta A' \end{tikzcd}$$

Außerdem sei das Bild eines projektiven Moduls unter Θ projektiv. Dann gelten:

(a) Für eine gegebene kurze exakte Sequenz $0 \to A \to B \to C \to 0$ von G-Moduln sei außerdem $0 \to \Theta(A) \to \Theta(B) \to \Theta(C) \to 0$ exakt. Dann ist das folgende Diagramm abelscher Gruppen für alle $n \geq 0$ kommutativ, wobei die $(\phi, \Theta)_n$ die Homomorphismen $(\phi, \theta_C)_n$ bzw. $(\phi, \theta_A)_n$ aus Bemerkung (1.1.2) sind:

$$\begin{tikzcd} H_{n+1}(G, C) \arrow[r, "\delta_n"] \arrow[d, "(\phi,\Theta)_{n+1}"'] & H_n(G, A) \arrow[d, "(\phi,\Theta)_n"] \\ H_{n+1}(H, \Theta C) \arrow[r, "\delta_n"] & H_n(H, \Theta A) \end{tikzcd}$$

(b) Sei der Funktor Θ nun zusätzlich exakt. Dann gibt es zu jedem G-Modul A eine eindeutig bestimmte Familie $(\phi, \Theta)_*$ von Homomorphismen

$$(\phi, \Theta)_n : H_n(G, A) \to H_n(H, \Theta A),$$

so daß

(i) $(\phi, \Theta)_0$ der Homomorphismus $(\phi, \theta_A)_0$ aus Bemerkung (1.1.2) ist, und

(ii) für jede kurze exakte Sequenz $0 \to A \to B \to C \to 0$ von G-Moduln das Diagramm aus (a) kommutiert.

Eine Familie von Homomorphismen, die die Eigenschaft (ii) des Satzes erfüllt, heißt *Morphismus homologischer Funktoren.*

Beweis. (a) kann man unter Benutzung der expliziten Beschreibung des Verbindungshomomorphismus nachrechnen. Wir konzentrieren hier unser Augenmerk auf (b).

Sei $0 \to A \to B \to C \to 0$ eine exakte Sequenz von G-Moduln, so daß nach Voraussetzung $0 \to \Theta(A) \xrightarrow{\alpha} \Theta(B) \xrightarrow{\beta} \Theta(C) \to 0$ eine exakte Sequenz von H-Moduln ist.

Im folgenden bedienen wir uns einer Variante der Methode der *Dimensionsverschiebung.*

Seien $\{a_i \mid i \in I\}$ und $\{b_j \mid j \in J\}$ Erzeugendensysteme von A bzw. B. Wir bezeichnen mit F_A, F_B und F_C die freien H-Moduln auf den Symbolen I, $I \cup J$ bzw. J.

Wir betrachten das exakte kommutative Diagramm

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & K_A \arrow[r] \arrow[d] & F_A \arrow[r, "\rho"] \arrow[d] & A \arrow[r] \arrow[d, "\alpha"'] & 0 \\
0 \arrow[r] & K_B \arrow[r] \arrow[d] & F_B \arrow[r, "\sigma"] \arrow[d] & B \arrow[r] \arrow[d, "\beta"'] & 0, \\
0 \arrow[r] & K_C \arrow[r] \arrow[d] & F_C \arrow[r, "\tau"] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

wobei ρ, σ und τ auf den Symbolen definiert sind durch $\rho : i \mapsto a_i$ bzw. $\sigma : i \mapsto \alpha(a_i), j \mapsto b_i$ und $\tau : j \mapsto \beta(b_i)$. K_A, K_B und K_C bezeichnen die Kerne dieser Homomorphismen.

Hieraus erhalten wir folgenden Würfel ($n \geq 0$):

$$\begin{tikzcd}
 & & H_{n+1}(G,K_C) \arrow[rrr, "\delta"] \arrow[dd, "(\phi,\Theta)_{n+1}"'] & & & H_n(G,K_A) \arrow[dd, "(\phi,\Theta)_n"] \\
H_{n+2}(G,C) \arrow[urr, Rightarrow, "\delta"] \arrow[rrrr, "-\delta"] \arrow[dd, "(\phi,\Theta)_{n+2}"'] & & & & H_{n+1}(G,A) \arrow[ur, "\delta"] \arrow[dd, "(\phi,\Theta)_{n+1}"] & \\
 & & H_{n+1}(H,\Theta(K_C)) \arrow[rrr, "\delta"] & & & H_n(H,\Theta(K_A)) \\
H_{n+2}(H,\Theta(C)) \arrow[urr, Rightarrow, "\delta"] \arrow[rrrr, "-\delta"] & & & & H_{n+1}(H,\Theta(A)) \arrow[ur, "\delta"] &
\end{tikzcd}$$

Die linken Verbindungshomomorphismen sind bijektiv, die rechten injektiv und für $n \geq 1$ sogar auch bijektiv, da projektive Moduln homologisch trivial sind. Der Deckel und der Boden sind kommutativ, was eine allgemeine Eigenschaften homologischer Funktoren ist. Die Kommutativität der rechten Seitenwand ist als eindeutige Definition von $(\phi, \Theta)_n$ für $n \geq 1$ unter Vorgabe von (i) und (ii) zu verstehen.

Nun benutzt man, daß $(\phi, \Theta)_1 : H_1(G, C) \to H_1(H, \Theta(C))$ wegen der Injektivität von $\delta_0 : H_1(G, C) \hookrightarrow H_0(G, K_C)$ die Einschränkung von $(\phi, \Theta)_0 : H_1(G, K_C) \to H_1(H, \Theta(K_C))$ ist. Damit kann man die Kommutativität von

$$\begin{tikzcd}
H_1(G,C) \arrow[r, "\delta_0"] \arrow[d, "(\phi,\Theta)_1"'] & H_0(G,A) \arrow[d, "(\phi,\Theta)_0"] \\
H_1(H,\Theta C) \arrow[r, "\delta_0"] & H_0(H,\Theta A).
\end{tikzcd}$$

unter Verwendung der expliziten Beschreibung des Verbindungshomomorphismus nachrechnen.

Daher überträgt sich die Kommutativität der Rückwand auf die Vorderwand, weswegen (ii) allgemein erfüllt ist. □

Wir können Teil (b) des Satzes auch wie folgt auffassen. Daß projektive Moduln unter Θ auf projektive Moduln abgebildet werden, hat zur Folge, daß der Funktor $H_n(H, \Theta(\cdot))$ effaçable bzgl. der projektiven G-Moduln ist. Der Satz besagt dann, daß ein Morphismus von einem homologischen Funktor in einen effaçablen homologischen Funktor (beide bzgl. derselben abelschen Kategorie) bereits durch Festlegung in Dimension 0 eindeutig bestimmt ist.

Kohomologie

Nun wenden wir uns der Kohomologie zu. Aus der Standardauflösung erhalten wir durch Anwendung des Funktors $Hom_G(\cdot, A)$ einen Kokomplex (nach Komposition der ersten beiden Abbildungen)

$$0 \to Hom_G(\mathbb{Z}[G], A) \to Hom_G(\mathbb{Z}[G^2], A) \to Hom_G(\mathbb{Z}[G^3], A) \to \dots,$$

dessen Kohomologiegruppen wir mit $H^n(G, A)$ bezeichnen wollen. Die Elemente aus

$$C^n(G, A) := Hom_G(\mathbb{Z}[G^{n+1}], A)$$

heißen *homogene n-Koketten*. In natürlicher Weise ergibt sich die G-Isomorphie

$$C^n(G, A) \cong \{f : G^{n+1} \to A \text{ Abbildung } \mid f(gg_0, \dots, gg_n) = gf(g_0, \dots, g_n) \text{ für alle } g \in G\}.$$

Benutzen wir die Beschreibung der $\mathbb{Z}[G]$-Basis der Standardauflösung von S. 4, so erhalten wir eine natürliche G-Isomorphie

$$C^n(G, A) \cong \{f : G^n \to A \text{ Abbildung }\} =: \mathcal{C}^n(G, A)$$

zwischen $C^n(G, A)$ und der Gruppe der *inhomogenen n-Koketten*. Die Randabbildungen erscheinen in beiden Fällen natürlich in anderer Gestalt.

$H^n(G, \cdot)$ ist ein *positiver kohomologischer Funktor* bzgl. der G-Moduln, worunter wir ("dual" zum homologischen Funktor) das Folgende verstehen wollen: Für jede kurze exakte Sequenz $0 \to A \to B \to C \to 0$ von G-Moduln gibt es für jedes n einen Verbindungshomomorphismus $\delta^n : H^n(G, C) \to H^{n+1}(G, A)$, so daß gelten:

(i) Für jedes kommutative Diagramm

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "f"'] & B \arrow[r] \arrow[d, "g"'] & C \arrow[r] \arrow[d, "h"'] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

mit exakten Zeilen kommutiert das folgende Diagramm:

$$\begin{tikzcd}
H^n(G, C) \arrow[r, "\delta^n"] \arrow[d, "H^n(h)"'] & H^{n+1}(G, A) \arrow[d, "H^{n+1}(f)"'] \\
H^n(G, C') \arrow[r, "\delta^n"] & H^{n+1}(G, A')
\end{tikzcd}$$

(ii) Für jede kurze exakte Sequenz $0 \to A \to B \to C \to 0$ ist die folgende Sequenz (die *lange exakte Sequenz*) für alle n exakt:

$$H^n(G, A) \to H^n(G, B) \to H^n(G, C) \xrightarrow{\delta^n} H^{n+1}(G, A) \to H^{n+1}(G, B).$$

Die *Positivität* bedeutet wiederum, daß die Gruppen $H^n(G, A)$ für alle $n < 0$ trivial sind.

$H^n(G, \cdot)$ ist *coeffaçable* bzgl. der injektiven G-Moduln, d.h. zu jedem G-Modul A gibt es einen injektiven Modul I zusammen mit einem Monomorphismus $A \hookrightarrow I$.

Wir wollen auch hier den Verbindungshomomorphismus $\delta^0 : H^0(G, C) \to H^1(G, A)$ für $0 \to A \to B \to C \to 0$ explizit beschreiben (vgl. [AW]). Sei $b + A \in (B/A)^G = C^G$. Wir bilden den 1-Kozyklus $[g] \mapsto g.b - b$ in $H^1(G, B)$. Nun ist $g.(b + A) - (b + A) = 0$ nach Voraussetzung und daher ist $g.b - b \in A$. Man kann leicht die Unabhängigkeit von der Auswahl von b nachprüfen und erhält die explizite Beschreibung

$$\delta^0(b + A) := (g \mapsto g.b - b).$$

Wir definieren für eine Untergruppe $H < G$ und einen H-Modul A den G-Modul

$$Coind_H^G(A) := Hom_H(\mathbb{Z}[G], A)$$

und nennen im Spezialfall von $H = 1$ und einer abelschen Gruppe X den Modul $Coind_1^G(X)$ *koinduziert*. Auch in dieser Situation gibt es das *Lemma von Shapiro*, welches die Isomorphie

$$H^n(G, Coind_H^G(A)) \cong H^n(H, A) \text{ für alle } n \geq 0$$

besagt. Insbesondere sind die Gruppen $H^n(G, Coind_1^G(X)$ für alle $n \geq 1$ trivial.

Analog zum homologischen Fall heiße für einen G-Modul A und einen H-Modul B ein Paar von Gruppenhomomorphismen $\phi : G \to H$ und $\theta : B \to A$ *verträglich*, wenn gilt

$$\theta(\phi(g).b) = g.\theta(b),$$

bzw. äquivalent dazu, wenn θ ein G-Modulhomomorphismus ist.

Wir erhalten wie im homologischen Fall die

(1.1.4) Bemerkung. *Ein verträgliches Paar (ϕ, θ) wie oben induziert eine eindeutige Familie von Homomorphismen*

$$(\phi, \theta)^n : H^n(H, B) \to H^n(G, A)$$

durch Festlegung auf den inhomogenen Koketten

$$f \mapsto ([g_1| \ldots |g_n] \mapsto \theta(f([\phi(g_1)| \ldots |\phi(g_n)]))).$$

Wir wollen auch dies zur Definition einiger wichtiger Abbildungen verwenden:

- Für eine Untergruppe $H < G$ und einen G-Modul A erhalten wir aus der Einbettung $H \hookrightarrow G$ und der Identität auf A die *Restriktion*

$$\text{res} : H^n(G, A) \to H^n(H, A).$$

- Für einen Normalteiler $U \lhd G$ haben wir die natürliche Projektion $\phi : G \to G/U$ und die Einbettung $\Theta : A^U \hookrightarrow A$, welche ein verträgliches Paar bilden. Dieses liefert die *Inflation*

$$\inf : H^n(G/U, A^U) \to H^n(G, A).$$

- Sei wiederum $H < G$ eine Untergruppe, A ein G-Modul und $g \in G$. Wir erhalten ein verträgliches Paar durch $\phi_g : gHg^{-1} \to H, ghg^{-1} \mapsto h$ und $\theta_g : A \to A, a \mapsto g.a$. Dieses liefert Homomorphismen

$$H^n(gHg^{-1}, A) \to H^n(H, A).$$

  Für einen Normalteiler $H \lhd G$ erhält man so eine G-Aktion auf den Kohomologiegruppen.

Der folgende Satz liefert u.a. eine natürliche Verträglichkeit der so definierten Abbildungen mit Verbindungshomomorphismen. Er ist das kohomologische Analogon des Satzes (1.1.3).

(1.1.5) Satz. *Sei $\phi : G \to H$ ein Gruppenhomomorphismus und Θ ein Funktor der G-Moduln in die H-Moduln, so daß es zu jedem G-Modul A einen G-Modulhomomorphismus $\theta_A : \Theta A \to A$ gibt (d.h. ϕ und θ_A sind verträglich), so daß das folgende Diagramm von G-Moduln kommutiert:*

$$\begin{array}{ccc} \Theta A & \xrightarrow{\theta_A} & A \\ {\scriptstyle \Theta f}\downarrow & & \downarrow{\scriptstyle f} \\ \Theta A' & \xrightarrow{\theta_{A'}} & A' \end{array}$$

Außerdem bilde Θ injektive Objekte auf injektive ab. Dann gelten:

(a) *Für eine gegebene kurze exakte Sequenz $0 \to A \to B \to C \to 0$ von G-Moduln sei außerdem $0 \to \Theta(A) \to \Theta(B) \to \Theta(C) \to 0$ exakt. Dann ist das folgende Diagramm abelscher Gruppen für alle $n \geq 0$ kommutativ, wobei die $(\phi, \Theta)^n$ die Homomorphismen $(\phi, \theta_C)^n$ bzw. $(\phi, \theta_A)^n$ aus Bemerkung (1.1.4) sind:*

$$\begin{array}{ccc} H^n(H, \Theta C) & \xrightarrow{\delta^n} & H^{n+1}(H, \Theta A) \\ {\scriptstyle (\phi,\Theta)^n}\downarrow & & \downarrow{\scriptstyle (\phi,\Theta)^{n+1}} \\ H^n(G, C) & \xrightarrow{\delta^n} & H^{n+1}(G, A) \end{array}$$

(b) *Sei der Funktor Θ nun zusätzlich exakt. Dann gibt es zu jedem G-Modul A eine eindeutig bestimmte Familie $(\phi, \Theta)^*$ von Homomorphismen*

$$(\phi, \Theta)^n : H^n(H, \Theta A) \to H^n(G, A),$$

so daß

(i) *$(\phi, \Theta)^0$ der Homomorphismus $(\phi, \theta_A)^0$ aus Bemerkung (1.1.4) ist, und*

(ii) *für jede kurze exakte Sequenz $0 \to A \to B \to C \to 0$ von G-Moduln das Diagramm aus (a) kommutiert.*

Eine Familie von Homomorphismen, die (ii) erfüllt, nennen wir einen *Morphismus kohomologischer Funktoren.*

Homologie und Kohomologie proendlicher Gruppen

Sei G in diesem Abschnitt eine proendliche Gruppe. Seien $V \leq U$ offene Normalteiler von G. Wir definieren die *Norm* durch

$$N_{U/V} := \sum_{g \in U/V} g \in \mathbb{Z}[U/V].$$

Wir erhalten durch Anwendung von $N_{U/V}$ einen Homomorphismus $A^V \xrightarrow{N_{U/V}} A^U$, welcher einen Homomorphismus $(A^V)_U \longrightarrow A^U$ induziert. Dieser ist mit der Identität auf G/U verträglich.

In Verallgemeinerung dieser Situation betrachten wir eine Familie $A(U)$ von abelschen Gruppen für offene Normalteiler $U \lhd G$. Jedes $A(U)$ sei mit einer G/U-Modulstruktur versehen, die mit der Norm verträglich sei, d. h. die Homomorphismen $G/V \twoheadrightarrow G/U$ und $A(V) \xrightarrow{N_{U/V}} A(U)$ bilden ein verträgliches Paar. Mittels Definition auf den Ketten (vgl. Bemerkung (1.1.2)) erhalten wir einen Homomorphismus

$$N_n : H_n(G/U, A(V)_U) \longrightarrow H_n(G/U, A(U))$$

für alle $n \in \mathbb{N}$.

Dies wollen wir benutzen, um die *Deflation* wie folgt zu erklären:

$$\mathrm{def} : H_n(G/V, A(V)) \xrightarrow{\text{coinf}} H_n(G/U, A(V)_U) \xrightarrow{N_n} H_n(G/U, A(U))$$

Via der Deflation bilden die Gruppen $H_n(G/U, A(U))$ ein projektives System, was man in Dimension 0 nachrechnet und per Dimensionsverschiebung ausdehnt.

Man stellt fest, daß die Gruppen $H^n(G/U, A^U)$ für einen G-Modul A via der Inflation ein direktes System bilden, was wiederum auf Dimension 0 klar ist und durch Dimensionsverschiebung ausgedehnt werden kann. Wir setzen

$$H^n(G, A) := \varinjlim H^n(G/U, A^U).$$

(Dies sind nicht die vorne definierten $H^n(G, A)$.) Alternativ ergeben sich die neu definierten $H^n(G, A)$ als Kohomologie des Komplexes der $C^n(G, A)$ bzw. $\mathcal{C}^n(G, A)$, indem man den G-Modul

A mit der diskreten Topologie versieht und zusätzlich die Stetigkeit aller Abbildungen fordert. Auf diese Weise verallgemeinert sich auch der Begriff des koinduzierten Moduls zu

$$Coind_H^G(A) := \{f : G \to A \mid f(h.g) = h.f(g)\ \forall h \in H, f \text{ stetig}\}.$$

Die Definition des verträglichen Paares und der mit seiner Hilfe erhaltenen Abbildungen überträgt sich direkt.

Tate-Kohomologie endlicher Gruppen

In diesem Abschnitt sei die Gruppe G stets endlich. Wir erinnern an bzw. treffen folgende Definitionen:

- $N_G := \sum_{g\in G} g \in \mathbb{Z}[G]$,
- $I_G := ker(\epsilon : \mathbb{Z}[G] \to \mathbb{Z}) = (g-1|g \in G) \lhd \mathbb{Z}[G]$,
- ${}_{N_G}A = ker(A \xrightarrow{N_G} A)$ für einen G-Modul A.

(1.1.6) Lemma. *(a) Sei X eine abelsche Gruppe. Dann ist*

$$Hom(\mathbb{Z}[G], X) \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} X, \quad \phi \mapsto \sum_{g\in G} g \otimes_{\mathbb{Z}} \phi(g)$$

ein G-Isomorphismus, dessen Umkehrabbildung durch $h \otimes_{\mathbb{Z}} x \mapsto (g \mapsto x\delta_{g,h})$ definiert ist, wobei $\delta_{g,h}$ das Kronecker-Delta sei. Damit fallen die Begriffe des induzierten und koinduzierten Moduls zusammen.

(b) Sei $A = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$ ein induzierter bzw. koinduzierter G-Modul. Dann gelten $A^G = N_G A$, ${}_{N_G}A = I_G A$, und $A_G = A/I_G A \xrightarrow{N_G} A^G$ ist ein G-Isomorphismus (G operiert trivial).

(c) Sei C ein endlich erzeugter freier G-Modul. Mit C^* bezeichnen wir seinen dualen Modul $Hom(C, \mathbb{Z})$. Die Abbildung

$$C \otimes_{\mathbb{Z}} A \to Hom(C^*, A), \quad c \otimes a \mapsto \big((f : C \to \mathbb{Z}) \mapsto f(c) \cdot a\big)$$

ist ein G-Isomorphismus.

(d) Für zwei $\mathbb{Z}[G]$-Moduln A und C, wobei C endlich erzeugt und $\mathbb{Z}[G]$-frei sei, erhalten wir die G-Isomorphie

$$C \otimes_{\mathbb{Z}[G]} A = (C \otimes_{\mathbb{Z}} A)_G \xrightarrow{N_G} (C \otimes_{\mathbb{Z}} A)^G \xrightarrow{(c)} Hom(C^*, A)^G = Hom_G(C^*, A).$$

Beweis. Für (a) und (c) überzeugt man sich leicht, daß es sich tatsächlich um G-Homomorphismen handelt, und rechnet die Bijektivität nach. (d) folgt sofort aus (a)-(c).

Zu (b) sei zunächst $a \in A^G$. Da A $\mathbb{Z}$-frei ist, können wir eindeutig

$$a = \sum_{s\in G} s \otimes x_s$$

schreiben mit $x_s \in X$. Wegen der G-Invarianz gilt

$$a = \sum_{s\in G} gs \otimes x_s = \sum_{s\in G} s \otimes x_{g^{-1}s},$$

weshalb die x_s alle gleich sind. Somit ist $a = N_G(1 \otimes x_{id})$ ein Element von $N_G A$.

Desweiteren sei nun $a \in {}_{N_G}A$ gegeben, d.h.

$$0 = N_G\, a = N_G \sum_{s\in G} s \otimes x_s = \sum_{g\in G} g \otimes \sum_{s\in G} x_s,$$

so daß $\sum_{s\in G} x_s = 0$ folgt. Somit ergibt sich

$$a = \sum_{s\in G} s \otimes x_s = \sum_{s\in G} s \otimes x_s - \sum_{s\in G} 1 \otimes x_s = \sum_{s\in G} (s-1)(1 \otimes x_s) \in I_G A.$$

Die Isomorphie zwischen A_G und A^G folgt aus

$$A_G = A/I_G A = A/{}_{N_G}A \xrightarrow{N_G} N_G A = A^G.$$

□

Bezeichne $F_\bullet$ die freie Standardauflösung von $\mathbb{Z}$, also

$$0 \to \mathbb{Z} \xleftarrow{\epsilon} F_0 \to F_1 \to F_2 \to \dots .$$

Wir setzen $F_{-n} := F_{n-1}^*$ für $n \geq 1$ und erhalten dadurch die Sequenz

$$\dots \leftarrow F_{-3} \leftarrow F_{-2} \leftarrow F_{-1} \xleftarrow{\epsilon^*} \mathbb{Z} \leftarrow 0,$$

welche exakt ist, da die F_{-n} endlich erzeugte freie $\mathbb{Z}[G]$-Moduln sind. Wir verschmelzen beide Sequenzen und erhalten folgendes Diagramm, das an jeder Stelle exakt ist

$$\begin{tikzcd}
{} & F_{-3} \arrow[l] & F_{-2} \arrow[l] & F_{-1} \arrow[l] & F_0 \arrow[l, "\alpha"'] \arrow[d, "\epsilon"] & F_1 \arrow[l] & F_2 \arrow[l] & {} \arrow[l] \\
 & & & \mathbb{Z} \arrow[u, "\epsilon^*"] \arrow[r, equal] & \mathbb{Z} \arrow[d] & & & \\
 & & & 0 \arrow[u] & 0, & & &
\end{tikzcd}$$

wobei α die Komposition $\epsilon^* \circ \epsilon$ sei. Aus Teil (d) des Lemmas (1.1.6) lesen wir ab, daß für $n \geq 1$

$$Hom_G(F_{-n}, A) = Hom_G(F_{n-1}^*, A) \cong F_{n-1} \otimes_{\mathbb{Z}[G]} A$$

gilt. Außerdem haben wir die Isomorphie

$$\mathbb{Z} \otimes_{\mathbb{Z}[G]} A = A_G \xrightarrow{N_G} A^G = Hom_G(\mathbb{Z}, A).$$

Anwendung des Funktors $Hom_G(\cdot, A)$ ergibt nun das folgende kommutative Diagramm, dessen oberste Zeile ein Kokomplex ist:

$$\begin{tikzcd}
{} \arrow[r] & F_1 \otimes_{\mathbb{Z}[G]} A \arrow[r] & F_0 \otimes_{\mathbb{Z}[G]} A \arrow[r] \arrow[d] & Hom_G(F_0, A) \arrow[r] & Hom_G(F_1, A) \arrow[r] & {} \\
 & & A_G \arrow[r, "N_G"] \arrow[d] & A^G \arrow[u] & & \\
 & & 0 & 0. \arrow[u] & &
\end{tikzcd}$$

Wir definieren die *Tate-Kohomologiegruppen* $\hat{H}^n$ für $n \in \mathbb{Z}$ als die Kohomologie der obersten Zeile. Die Tate-Kohomologie $\hat{H}^n(G, \cdot)$ bildet einen kohomologischen Funktor. Es gilt der

(1.1.7) Satz.

$$\hat{H}^n(G,A) = \begin{cases} H^n(G,A) & n \geq 1 \\ A^G/N_G A & n = 0 \\ {}_{N_G}A/I_G A & n = -1 \\ H_{-n-1}(G,A) & n \leq -2 \end{cases}$$

Beweis. Den ersten und letzten Fall liest man direkt aus dem Diagramm ab. Für $n = 0, -1$ ergibt sich das Ergebnis daraus, daß die Pfeile nach unten surjektiv und die nach oben injektiv sind. □

Es ist üblich, die Bezeichnung $\hat{H}_0(G,A) := \hat{H}^{-1}(G,A) = {}_{N_G}A/I_G A$ zu wählen. Trivialerweise erhalten wir dann die folgende exakte Sequenz abelscher Gruppen:

$$0 \to \hat{H}_0(G,A) \to H_0(G,A) \xrightarrow{\cdot N_G} H^0(G,A) \to \hat{H}^0(G,A) \to 0.$$

Mittels der expliziten Beschreibung der Verbindungshomomorphismen stellt man fest, daß $N_G \cdot im(\delta_0) = 0$ gilt, und daß δ^0 über $N_G A$ faktorisiert. Für die Tate-Kohomologie ergeben sich daraus die Verbindungshomomorphismen

$$\delta^{-2} : \hat{H}^{-2}(G,A) \to \hat{H}^{-1}(G,A) \quad \text{und} \quad \delta^0 : \hat{H}^0(G,A) \to \hat{H}^1(G,A)$$

auf natürliche Weise. Die Abbildung

$$\delta^{-1} : {}_{N_G}C/I_G C \to A^G/N_G A$$

wird (vgl. [AW]) durch Multiplikation mit N_G induziert ($C = B/A$):

$$\delta^{-1} : (b + A) + I_G C \mapsto N_G \cdot b + N_G A.$$

Man überzeugt sich wiederum leicht von der Wohldefiniertheit.

Teil (b) des Lemmas (1.1.6) besagt nun, daß für einen induzierten bzw. koinduzierten G-Modul A gilt: $\hat{H}^{-1}(G,A) = \hat{H}^0(G,A) = 0$. Aus unserem Wissen über Homologie und Kohomologie schließen wir $\hat{H}^n(G,A) = 0$ für alle $n \in \mathbb{Z}$.

Aufgrund der natürlichen Homomorphismen $Hom_G(\mathbb{Z}[G], A) \twoheadrightarrow A$ und $A \hookrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ ist jeder G-Modul sowohl Faktor- als auch Untermodul eines induzierten bzw. koinduzierten Moduls, und wir dürfen die Methode der Dimensionsverschiebung in beiden Richtungen benutzen.

Auf diese Weise können wir u. a. die Restriktion und die Korestriktion auf alle Dimensionen $n \in \mathbb{Z}$ ausdehnen.

Für die Homologie hatten wir die Deflation bereits vorne definiert. Es stellt sich heraus, daß

$$\mathrm{def}_0 : H_0(G,A) = A_G \to H_0(G/U, A^U) = (A^U)_{G/U}$$

gerade die Multiplikation mit N_U ist. Wir schließen daher die Existenz der induzierten Abbildung

$$\mathrm{def}^{-1} : \hat{H}^{-1}(G,A) \to \hat{H}^{-1}(G/U, A^U).$$

Wir setzen $\mathrm{def}^{-n-1} := \mathrm{def}_n$ für $n > 0$. Es ergibt sich die gewünschte Verträglichkeit mit Verbindungshomomorphismen.

Als nächstes möchten wir auch eine Deflation auf Dimension 0 für die Tate-Kohomologie definieren. Dazu erinnern wir uns daran, daß die Verbindungshomomorphismen auf Dimension -1 im Wesentlichen durch die Norm gegeben sind. Wir betrachten für eine exakte Sequenz $0 \to A \to B \to C \to 0$ das Diagramm

$$\begin{array}{ccc} {}_{N_G}C/I_G C & \xrightarrow[\cdot N_G]{\delta_{-1}} & A^G/N_G A \\ {\scriptstyle \mathrm{def}_{-1}}\big\downarrow{\scriptstyle \cdot N_U} & & \big\downarrow \\ {}_{N_{G/U}}C^U/I_{G/U}C^U & \xrightarrow[\cdot N_{G/U}]{\delta_{-1}} & A^G/N_{G/U}A^U \end{array} .$$

Wenn die rechte Abbildung durch die Identität induziert ist, wird das Diagramm offensichtlich kommutativ. Daher definieren wir def^0 als diesen Homorphismus.

Wir stellen einige Eigenschaften zusammen. Aus [N-KKT], Satz 7.1, zitieren wir folgenden

(1.1.8) Satz. *Ein G-Modul A ist bereits kohomologisch trivial, wenn es eine Dimension n gibt, derart daß*

$$\hat{H}^n(H,A) = \hat{H}^{n+1}(H,A) = 0$$

für alle Untergruppen $H \leq G$ gilt.

Aus [NSW], Proposition 1.7.6, entnehmen wir folgenden

(1.1.9) Satz. *Seien A und B G-Moduln. Wenn A kohomologisch trivial und B divisibel ist, oder wenn A $\mathbb{Z}$-frei und B kohomologisch trivial ist, dann ist auch $Hom(A,B)$ kohomologisch trivial.*

Der Beweis des folgenden Satzes befindet sich in [AW].

(1.1.10) Satz. *(a) Für jede Untergruppe $H \leq G$ vom Index n gilt: $cor \circ res = n$.*

(b) Sei $|G| = n$, dann gilt $n\hat{H}^q(G,A) = 0$ für alle $q \in \mathbb{Z}$.

(c) A sei ein endlich erzeugter $\mathbb{Z}[G]$-Modul. Dann sind die Gruppen $\hat{H}^q(G,A)$ für alle $q \in \mathbb{Z}$ endlich.

(d) Sei $H \lhd G$ ein Normalteiler. Die Inflation-Restriktion-Sequenz

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

ist exakt. Falls $\hat{H}^i(H,A) = 0$ für alle $i = 1, \ldots, n-1$ gilt, dann ist auch die Sequenz

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

exakt.

Von besonderer Wichtigkeit für uns ist die Existenz des *Cupproduktes*, da wir an Dualitätsaussagen interessiert sind. Dafür zitieren wir den folgenden Satz aus [N-KKT], I.5.1:

(1.1.11) Satz. *Seien A und B G-Moduln. Es gibt eine eindeutig bestimmte Familie bilinearer Abbildungen, das* Cupprodukt,

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

für $p, q \in \mathbb{Z}$ mit den folgenden Eigenschaften:

(i) Für $p = q = 0$ ist das Cupprodukt durch die Zuordnung

$$(\overline{a}, \overline{b}) \mapsto \overline{a} \cup \overline{b} := \overline{a \otimes b}, \quad \overline{a} \in \hat{H}^0(G,A), \quad \overline{b} \in \hat{H}^0(G,B)$$

gegeben.

(ii) Sind die G-Modulsequenzen $0 \to A \to A' \to A'' \to 0$ und $0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$ beide exakt, so ist das Diagramm

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

kommutativ.

(iii) Sind die G-Modulsequenzen $0 \to B \to B' \to B'' \to 0$ *und* $0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$ *beide exakt, so ist das Diagramm*

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

kommutativ.

Weiter gilt (vgl. [NSW], Proposition 1.4.5 zusammen mit Remark auf S. 42) der folgende

(1.1.12) Satz. *Sei* $0 \to A \to B \to C \to 0$ *eine exakte Sequenz von G-Moduln und M ein weiterer G-Modul, derart daß auch die induzierte Sequenz* $0 \to Hom(C,M) \to Hom(B,M) \to Hom(A,M) \to 0$ *exakt ist. Dann ist für alle* $p, q \in \mathbb{Z}$ *das Diagramm*

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

kommutativ, d.h. es gilt

$$(\delta\alpha) \cup \beta + (-1)^p(\alpha \cup \delta\beta) = 0$$

für $\alpha \in \hat{H}^p(G,Hom(A,M))$ *und* $\beta \in \hat{H}^{q-1}(G,C)$.

Das im Satz verwendete Cupprodukt ergibt sich aus dem normalen durch folgende Hintereinanderschaltung

$$\hat{H}^i(G,Hom(A,M)) \times \hat{H}^{n-i}(G,A) \xrightarrow{\cup} \hat{H}^n(G,Hom(A,M)\otimes A) \xrightarrow{ev} \hat{H}^n(G,M).$$

Dabei bezeichne ev die Auswertungsabbildung $ev(f \otimes a) := f(a)$.

Wir würden gerne auch ein Cupprodukt, zumindest für bestimmte Dimensionen, für die noch zu definierenden Tate-Kohomologiegruppen von proendlichen Gruppen erhalten. Der folgende Satz aus [S] (Proposition 3) liefert den Schlüssel dazu.

(1.1.13) Satz. *Sei G endlich,* $U \lhd G$ *ein Normalteiler und A, B G-Moduln. Für* $i \leq 0$ *und* $q \geq 1$ *ist das Diagramm*

$$\begin{array}{ccccc} \hat{H}^i(G,A) & \times & \hat{H}^{q-i}(G,B) & \xrightarrow{\cup} & \hat{H}^q(G,A\otimes B) \\ {\scriptstyle def}\downarrow & & {\scriptstyle inf}\uparrow & & {\scriptstyle inf}\uparrow \\ \hat{H}^i(G/U,A^U) & \times & \hat{H}^{q-i}(G/U,B^U) & \xrightarrow{\cup} & \hat{H}^q(G/U,(A\otimes B)^U) \end{array}$$

kommutativ, d.h. es gilt

$$inf(def(x) \cup y) = x \cup inf(y)$$

für $x \in \hat{H}^i(G,A)$ *und* $y \in \hat{H}^{q-i}(G/U,B^U)$.

Tate-Kohomologie proendlicher Gruppen

In der Definition der Tate-Kohomologie ging an entscheidender Stelle die Endlichkeit der Gruppe G ein. Wir wollen nun unter stärkeren Voraussetzungen eine Ausdehnung auf den Fall einer proendlichen Gruppe vornehmen. Man vergleiche dazu die Arbeit [S].

Wie schon vorne benutzt, wollen wir unter einem *diskreten* G-Modul A einen G-Modul verstehen, der eine der beiden äquivalenten Bedingungen erfüllt:

(i) Die Operation $G \times A \to A$ ist stetig, wenn wir A mit der diskreten Topologie versehen.

(ii)
$$A = \bigcup_{U \lhd G \text{ offen}} A^U$$

Wie schon für $i < -1$ vorne bemerkt, bilden die $\hat{H}^i(G/U, A^U)$ auch für $i = -1, 0$ via der Deflation ein projektives System.

(1.1.14) Definition. *Sei G proendlich und A ein diskreter G-Modul. Wir definieren die* Tate-Kohomologiegruppen *für $i \leq 0$ durch*

$$\hat{H}^i(G, A) = \varprojlim_{U \lhd G \text{ offen}} \hat{H}^i(G/U, A^U),$$

wobei der projektive Limes via der Deflation genommen wird, und für $i > 0$ durch

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

wobei rechts die gewöhnliche Kohomologie steht (vgl. vorheriger Abschnitt).

(1.1.15) Definition. *Sei G eine proendliche Gruppe und A ein diskreter G-Modul. Dieser heißt* level-kompakt, *falls er mit einer zusätzlichen Topologie versehen ist, so daß A^U kompakt und Hausdorffsch ist für alle offenen Untergruppen $U \leq G$.*

Mithilfe dieser Zusatzforderung an die G-Moduln wollen wir die Exaktheit des projektiven Limes erreichen.

(1.1.16) Lemma. *Sei G proendlich und A ein level-kompakter G-Modul. Dann ist für $i \leq 0$ die Tate-Kohomologiegruppe $\hat{H}^i(G, A)$ eine proendliche Gruppe.*

Beweis. Für jedes G/U tragen die Ketten $F_n \otimes_{G/U} A^U$ bzw. $Hom_{G/U}(F_0, A)$ in natürlicher Weise eine von A^U kommende kompakte und Hausdorffsche Topologie. Die Zykel bilden darin als Kern eines stetigen Homomorphismus eine abgeschlossene Untergruppe, sind damit also kompakt und Hausdorffsch. Ferner bleiben diese Eigenschaften auch unter der offenen Projektion $Zykel \twoheadrightarrow Zykel/Ränder$ erhalten, woraus die Kompaktheit von $\hat{H}^i(G/U, A^U)$ für alle offenen Normalteiler $U \lhd G$ folgt.

Ferner wissen wir, daß $(G : U)\hat{H}^i(G/U, A^U) = 0$ gilt. Damit ist $\hat{H}^i(G/U, A^U)$ eine kompakte, Hausdorffsche, abelsche Torsionsgruppe. Wir zeigen gleich, daß sie dann proendlich ist. Da projektive Limites von proendlichen Gruppen proendlich sind, folgt die Aussage.

Sei H eine kompakte, Hausdorffsche, abelsche Torsionsgruppe, die sich als abstrakte Gruppe schreiben läßt als $H = \bigoplus_{i \in I} < h_i >$. Für jede endliche Teilmenge $J \subseteq I$ ist die Untergruppe $\bigoplus_{i \in I \setminus J} < h_i >$ offen, da ihr Komplement eine endliche, also wegen der Hausdorffeigenschaft abgeschlossene, Menge ist. Diese Mengen bilden eine Umgebungsbasis der 0 bestehend aus Normalteilern, weshalb H proendlich ist. $\square$

Im Folgenden sei $\hat{H}^i(G, A)$ für $i \leq 0$ stets mit dieser kompakten und für $i > 0$ mit der diskreten Topologie ausgestattet.

Da im allgemeinen zu einer exakten Sequenz $0 \to A \to B \to C \to 0$ nicht auch $0 \to A^U \to B^U \to C^U \to 0$ exakt ist (für offene Normalteiler $U \lhd G$), erhalten wir in negativen Dimensionen nicht ohne Zusatzvoraussetzungen lange exakte Sequenzen. Daher ist $\hat{H}(G, \cdot)$ kein kohomologischer Funktor.

Wir haben jedoch das folgende

(1.1.17) Lemma. *Sei A ein level-kompakter G-Modul. Dann gilt:*

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

Dabei bezeichne

$$N_G A = \bigcap_{U \lhd G \text{ offen}} N_{G/U} A^U$$

die Gruppe der universellen Normen.

Beweis. Dies ist eine unmittelbare Konsequenz der Anwendung des projektiven Limes auf die exakte Sequenz kompakter Gruppen $0 \to N_{G/U} A^U \to A^G \to \hat{H}^0(G/U, A^U) \to 0$. □

Wenden wir uns nun dem Cupprodukt zu. Wir definieren

$$\hat{H}^i(G, A) \ \times \ \hat{H}^{q-i}(G, B) \ \xrightarrow{\cup} \ \hat{H}^q(G, A \otimes B)$$

für $i \leq 0$ und $q \geq 1$ wie folgt: Seien $x \in \hat{H}^i(G, A)$ und $y \in \hat{H}^{q-i}(G, B)$. Dann gibt es einen offenen Normalteiler $U \lhd G$, so daß $y = \inf(z)$ für ein $z \in \hat{H}^{q-i}(G/U, B^U)$ gilt. Wir setzen:

$$x \cup y := \inf(\operatorname{def}(x) \cup z).$$

Dieses ist wegen Satz (1.1.13) wohldefiniert.

Ist zusätzlich A als $\mathbb{Z}$-Modul endlich erzeugt, so bildet das Cupprodukt einen stetigen Homomorphismus. Dafür genügt es zu zeigen, daß für alle $e \in \hat{H}^q(G, A \otimes B)$ und alle (x, y) im Urbild von $\{e\}$, etwa mit $\inf_U(z) = y$ und $\inf_U(f) = e$, eine offene Umgebung V von x in $\hat{H}^i(G, A)$ existiert mit $\operatorname{def}(V) \cup z = f$. Wegen der endlichen Erzeugtheit von A ist die Gruppe $\hat{H}^i(G/U, A^U)$ als endlich erzeugte Torsionsgruppe endlich. Somit ist der Kern K der Deflation $\hat{H}^i(G, A) \to \hat{H}^i(G/U, A^U)$ offen. Daher ist $x + K$ (additiv geschrieben) eine solche gesuchte Umgebung.

1.1.2. Begriffe der abstrakten Klassenkörpertheorie

Wir stellen kurz wichtige Begriffe der abstrakten Klassenkörpertheorie zusammen.

(1.1.18) Definition. *Sei G eine proendliche Gruppe und A ein diskreter G-Modul.*

(a) Ist G endlich, so nennen wir A einen Klassenmodul*, falls für jede Untergruppe $H \leq G$ gilt:*

- *(i) $H^1(H, A) = 0$.*
- *(ii) Die Gruppe $H^2(H, A)$ ist zyklisch von der Ordnung $|H|$.*

(b) Wir nennen A einen Formationsmodul *und das Paar (G, A) eine* Klassenformation*, falls für jedes Paar $V \lhd U$ offener Untergruppen von G*

- *(i) die Gruppe $H^1(U/V, A^V)$ trivial ist,*
- *(ii) und ein Isomorphismus*

$$\mathit{inv}_{U/V} : H^2(U/V, A^V) \to \frac{1}{(U:V)}\mathbb{Z}/\mathbb{Z}$$

gegeben ist, so daß für jede offene Untergruppe $W \lhd U$ von G mit $W \leq V$ das Diagramm

$$\begin{array}{ccccc} H^2(U/V, A^V) & \xrightarrow{\mathit{inf}} & H^2(U/W, A^W) & \xrightarrow{\mathit{res}} & H^2(V/W, A^W) \\ \Big\downarrow{\scriptstyle \mathit{inv}} & & \Big\downarrow{\scriptstyle \mathit{inv}} & & \Big\downarrow{\scriptstyle \mathit{inv}} \\ \frac{1}{(U:V)}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\mathit{Inklusion}} & \frac{1}{(U:W)}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\cdot (U:V)} & \frac{1}{(V:W)}\mathbb{Z}/\mathbb{Z} \end{array}$$

kommutativ ist.

Das durch $\mathit{inv}_{U/V}(u_{U/V}) = \frac{1}{(U:V)} + \mathbb{Z}$ eindeutig bestimmte Element $u_{U/V} \in H^2(U/V, A^V)$ heißt Fundamentalklasse.

1.1.3. Pontrjaginsche Dualitätstheorie

Sei G eine abelsche topologische Gruppe.

(1.1.19) Definition. *Die abelsche Gruppe*

$$G^\vee := Hom_{stetig}(G, \mathbb{R}/\mathbb{Z})$$

versehen mit der kompakt-offenen Topologie heißt die Charaktergruppe *bzw. das* Pontrjagin-Dual *von G.*

Ist G eine diskrete Torsionsgruppe, so gilt offensichtlich $G^\vee = Hom(G, \mathbb{Q}/\mathbb{Z})$. Wir setzen

$$G^* := Hom(G, \mathbb{Q}/\mathbb{Z}).$$

Statt einer abelschen Gruppe können wir natürlich auch einen G-Modul A betrachten. Dann ist auch A^* mit einer G-Modulstruktur ausgestattet, via $(g.f)(a) := f(g^{-1}.a)$.

Der Hauptsatz der Pontrjaginschen Dualitätstheorie besagt die Existenz eines kanonischen Isomorphismus

$$G \to (G^\vee)^\vee,\ g \mapsto \big(f : Hom_{\text{stetig}}(G, \mathbb{R}/\mathbb{Z}) \to \mathbb{R}/\mathbb{Z},\ f(\phi) := \phi(g)\big).$$

Die Zuordnung $G \mapsto G^\vee$ hat folgende Eigenschaften:

- diskrete abelsche Gruppen $\mapsto$ kompakte abelsche Gruppen,
- diskrete abelsche Torsionsgruppen $\mapsto$ proendliche abelsche Gruppen,
- proendliche abelsche Gruppen $\mapsto$ diskrete abelsche Torsionsgruppen,
- kompakte abelsche Gruppen $\mapsto$ diskrete abelsche Gruppen.

1.1.4. Dualitätssätze

Vorbereitungen

Zunächst wollen wir einige Vorbereitungen treffen.

(1.1.20) Bemerkung. *Sei G eine proendliche Gruppe.*

(a) Sei A ein diskreter G-Modul, der als $\mathbb{Z}$-Modul endlich erzeugt ist. Dann gibt es eine offene Untergruppe $V \leq G$, so daß für alle in V enthaltenen offenen Untergruppen $U \leq G$ gilt: $A^U = A$.

(b) Sei $U \leq G$ eine offene Untergruppe, und A und B seien G-Moduln, wobei $A^U = A$ angenommen werde. Dann gilt: $Hom(A, B)^U = Hom_U(A, B) = Hom(A, B^U)$.

Beweis. Zu (a) betrachten wir die Untergruppe

$$V = \{g \in G \mid ga = a\ \forall a \in A\ \} = \bigcap_{a \in A} G_a = \bigcap_{a\ \mathbb{Z}-\text{Generator}} G_a.$$

Die G_a seien dabei die Stabilisatoren von a, die wegen der Diskretheit von A offen sind. V ist als endlicher Durchschnitt aus ihnen somit auch offen. V erfüllt offensichtlich die Forderungen.

(b) Die erste Gleichheit ist klar und wurde schon gezeigt. Weiter haben wir

$$\begin{aligned} Hom_U(A, B) &= \{f : A \to B \text{ Homomorphismus} \mid u.f(a) = f(a)\ \forall a \in A\} \\ &= \{f : A \to B \text{ Homomorphismus} \mid f(A) \subseteq B^U\} \qquad = Hom(A, B^U). \end{aligned}$$

□

(1.1.21) Lemma. *Sei G eine proendliche Gruppe, A ein als $\mathbb{Z}$-Modul endlich erzeugter diskreter G-Modul, und B ein level-kompakter G-Modul. Dann ist auch $Hom(A, B)$ versehen mit der kompakt-offenen Topologie level-kompakt.*

Beweis. Sei $U \leq G$ eine offene Untergruppe. Diese enthält nach Bemerkung (1.1.20) eine offene Untergruppe $V \leq G$, für die $Hom(A, B)^V = Hom(A, B^V)$ ist. Letzterer Raum ist aber kompakt, da für B die Level-Kompaktheit vorausgesetzt wurde. Nun ist $Hom(A, B)^U$ eine abgeschlossene Untergruppe von $Hom(A, B)^V$ und somit selbst kompakt. □

(1.1.22) Lemma. *Seien A, B topologische abelsche Gruppen, und es sei ein stetiger Homomorphismus*

$$A \times B \xrightarrow{\cup} \mathbb{R}/\mathbb{Z}$$

gegeben. Dann ist die induzierte Abbildung

$$\psi : A \to B^\vee, \ a \mapsto (b \mapsto a \cup b)$$

ein stetiger Homomorphismus.

Beweis. Die Homomorphieeigenschaft ist klar. Sei $a \in \psi^{-1}([K, U])$, wobei $[K, U]$ mit $K \subseteq B$ kompakt und $U \subseteq \mathbb{R}/\mathbb{Z}$ offen die Menge aller stetigen Homomorphismen $B \to \mathbb{R}/\mathbb{Z}$ sei, die K in U abbilden. Die Menge $V := \{b \in B \mid a \cup b \in U\}$ ist offen in B und umfaßt K. Es gilt: $a \in \psi^{-1}([V, U]) \subseteq \psi^{-1}([K, U])$. Nun ist aber $\psi^{-1}([V, U])$ gleich der Projektion auf A von $(\cup^{-1}(U)) \cap (A \times V)$, also eine offene Umgebung von a, die ganz in $\psi^{-1}([K, U])$ liegt, woraus die Stetigkeit folgt. □

(1.1.23) Lemma. *Seien A, A', B, B' abelsche topologische Gruppen. Ferner sei folgendes Diagramm kommutativ, und alle Abbildungen seien stetig:*

$$\begin{array}{ccccc} A' & \times & B' & \xrightarrow{\cup} & \mathbb{R}/\mathbb{Z} \\ \phi\downarrow & & \psi\uparrow & & \downarrow\delta \\ A & \times & B & \xrightarrow{\cup} & \mathbb{R}/\mathbb{Z} \end{array}$$

Dann erhalten wir die Kommutativität von:

$$\begin{array}{ccc} A' & \longrightarrow & B'^\vee \\ \phi\downarrow & & \downarrow f\mapsto\delta\circ f\circ\psi \\ A & \longrightarrow & B^\vee \end{array}$$

Beweis. Das läßt sich direkt nachrechnen. □

Der Dualitätssatz von Nakayama-Tate

Der zentrale Dualitätssatz für endliche Gruppen ist der folgende Satz von *Nakayama-Tate* (vgl. [NSW], Theorem 3.1.5).

(1.1.24) Satz. *Sei G eine endliche Gruppe und C ein Klassenmodul. Weiter bezeichne $\gamma \in H^2(G, C)$ eine Fundamentalklasse. Dann liefert für einen als $\mathbb{Z}$-Modul endlich erzeugten und $\mathbb{Z}$-freien G-Modul A das Cupprodukt*

$$\hat{H}^i(G, Hom(A, C)) \times \hat{H}^{2-i}(G, A) \xrightarrow{\cup} \hat{H}^2(G, C) \xrightarrow[\gamma\mapsto\frac{1}{|G|}+\mathbb{Z}]{inv} \tfrac{1}{|G|}\mathbb{Z}/\mathbb{Z}$$

für alle $i \in \mathbb{Z}$ einen Isomorphismus

$$\hat{H}^i(G, Hom(A, C)) \cong \hat{H}^{2-i}(G, A)^\vee$$

endlicher abelscher Gruppen.

Hier wurde wieder das mit der Auswertungsabbildung verknüpfte Cupprodukt verwendet (vgl. dazu die Diskussion im Anschluß an Satz (1.1.12)).

Bevor wir uns den Beweis des Satzes von Nakayama-Tate anschauen, wollen wir den Satz kurz einordnen.

Die abstrakte Klassenkörpertheorie baut auf der Isomorphie

$$(\mathrm{res}_H^G \gamma) \cup : \hat{H}^q(H, \mathbb{Z}) \cong \hat{H}^{q+2}(H, C)$$

(für Untergruppen H von G) auf, die für einen Klassenmodul C mit Fundamentalklsse γ gilt, wie wir in diesem Abschnitt sehen werden. Es geht hier darum, diese Abbildung genauer zu kennen und zu untersuchen, welche Bedingungen an C zu stellen sind, damit Isomorphie vorliegt.

Eine elegante Methode wird durch den *Zerfällungsmodul* geliefert, den wir im folgenden definieren und untersuchen werden.

Ausgangspunkt der Betrachtungen ist die Suche eines Moduls $C(\gamma)$, der einen vorgegebenen G-Modul C mit $\gamma \in \hat{H}^2(G, C)$ umfasse, so daß γ unter der natürlichen Abbildung in $\hat{H}^2(G, C(\gamma))$ auf die Null geht.

2-Kozykeln in $\hat{H}^2(G, C)$ erfüllen

$$\rho c(\sigma, \tau) - c(\rho\sigma, \tau) + c(\rho, \sigma\tau) - c(\rho, \sigma) = 0,$$

während ein 2-Korand $c(\sigma, \tau)$ zu einem geeigneten Modul durch eine Gleichung des Typs

$$c(\sigma, \tau) = \sigma b(\tau) - b(\sigma\tau) + b(\sigma)$$

gegeben ist. Wir sehen für einen 2-Kozykel durch Setzen von $\rho = \sigma = 1$, daß $c(1, \tau) = c(1, 1)$ ist, und für einen 2-Korand, daß $c(1, \tau) = 1.b(\tau) - b(\tau) + b(1) = b(1)$ gilt.

Im Folgenden sei $c(\sigma, \tau)$ ein Vertreter von γ. Wir werden nun den *Zerfällungsmodul* $C(\gamma)$ so definieren, daß das Bild von $c(\sigma, \tau)$ in $\hat{H}^2(G, C(\gamma))$ Null ist:

$$C(\gamma) := C \oplus B := C \oplus \bigoplus_{1 \neq \sigma \in G} b_\sigma$$

B ist also die freie abelsche Gruppe auf Symbolen b_σ für $\sigma \neq 1$. Die G-Aktion auf $C(\gamma)$ definieren wir unserem Ziel entsprechend durch

$$\sigma b_\tau := b_{\sigma\tau} - b_\sigma + c(\sigma, \tau),$$

wobei $b_1 = c(1, 1)$ sei.

Es ist natürlich zu überprüfen, daß es sich um eine G-Aktion handelt. Das sieht man wie folgt:

$$\begin{aligned}
1.b_\tau &= b_\tau - b_1 + c(1, \tau) = b_\tau \\
\rho(\sigma b_\tau) &= \rho(b_{\sigma\tau} - b_\sigma + c(\sigma, \tau)) \\
&= b_{\rho\sigma\tau} - b_\rho + b_{\rho\sigma} + b_\rho + c(\rho, \sigma\tau) - c(\rho, \sigma) + \rho c(\sigma, \tau) \\
&= b_{\rho\sigma\tau} - b_{\rho\sigma} + c(\rho\sigma, \tau) = (\rho\sigma) b_\tau
\end{aligned}$$

Dabei wurde die Kozykelrelation von oben benutzt.

Es ist klar, daß der Modul $C(\gamma)$ wohldefiniert ist, da er bis auf Isomorphie nicht von der Auswahl des Vertreters $c(\sigma, \tau)$ von γ abhängt. Denn sei $d(\sigma, \tau) = \sigma c(\tau) - c(\sigma\tau) + c(\sigma)$ ein 2-Korand von C und sei $\widetilde{C(\gamma)}$ der zu $c(\sigma, \tau) + d(\sigma, \tau)$ gebildete Zerfällungsmodul auf Symbolen $\tilde{b}_\sigma$, dann wird die Isomorphie durch $b_\sigma \mapsto \tilde{b}_\sigma - c(\sigma)$ gegeben.

Es ergibt sich sofort der folgende G-Epimorphismus

$$\phi : C(\gamma) = C \oplus B \to I_G,\ c \mapsto 0,\ b_\sigma \mapsto \sigma - 1.$$

Hieraus erhalten wir die exakte Sequenz

$$0 \longrightarrow C \longrightarrow C(\gamma) \xrightarrow{\phi} I_G \longrightarrow 0,$$

wobei die erste Abbildung die natürliche Einbettung $C \hookrightarrow C \oplus B$ ist. Weiter haben wir die exakte Sequenz

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

Dies gibt den folgenden Homomorphismus für jede Untergruppe $H \leq G$ und jedes $n \in \mathbb{Z}$:

$$\delta^2 : \hat{H}^n(H,\mathbb{Z}) \xrightarrow{\delta_1} \hat{H}^{n+1}(H, I_G) \xrightarrow{\delta_2} \hat{H}^{n+2}(H,C).$$

Er ist der Homomorphismus, den wir suchen:

(1.1.25) Satz. *Der obige Homomorphismus*

$$\delta^2 : \hat{H}^n(H,\mathbb{Z}) \to \hat{H}^{n+2}(H,C)$$

für einen G-Modul C und ein $\gamma \in \hat{H}^2(G,C)$ ist gegeben durch

$$\beta \mapsto res_H^G(\gamma) \cup \beta =: \gamma_H \cup \beta.$$

Ferner sind äquivalent:

(i) *$C(\gamma)$ ist kohomologisch trivial.*

(ii) *C ist ein Klassenmodul.*

(iii) *δ^2 ist ein Isomorphismus.*

Beweis. Zunächst rechnen wir unter Verwendung der expliziten Beschreibung der Verbindungshomomorphismen nach, daß $\delta^2(\overline{1}) = \gamma_H$ ist für $\overline{1} = 1 + |H|\mathbb{Z} \in \hat{H}^0(H,\mathbb{Z})$: Ein Urbild der $\overline{1}$ in den 0-Zykeln bzgl. $\mathbb{Z}[G]$ ist gegeben durch die 1; dessen Bild unter dem Randhomomorphismus ergibt den 1-Kozykel bzgl. I_G als $\delta_1(\overline{1})(\sigma) = \sigma - 1$. Ein Urbild davon in den 1-Zykeln bzgl. $C(\gamma)$ ist $x(\sigma) = b_\sigma$. Dessen Bild unter dem Randhomorphismus ist $\delta_2 \circ \delta_1(\overline{1})(\sigma,\tau) = \sigma b_\tau - b_{\sigma,\tau} + b_\sigma = c(\sigma,\tau)$.

Die Aussage $\delta^2 = \gamma_H \cup$ folgt nun aus Satz (1.1.12).

Es gilt $\hat{H}^{-1}(H,\mathbb{Z}) = \hat{H}^1(H,\mathbb{Z}) = 0$, da es aufgrund der Endlichkeit von H keine nichttrivialen Homomorphismen $H \to \mathbb{Z}$ gibt, und außerdem ${}_{N_H}\mathbb{Z} = 0$ ist wegen der Injektivität der Multiplikation mit $|H|$. Da $\mathbb{Z}[G]$ kohomologisch trivial ist, folgt $\hat{H}^n(H,\mathbb{Z}) \cong \hat{H}^{n+1}(H, I_G)$ und hieraus $\hat{H}^0(H, I_G) = \hat{H}^2(H, I_G) = 0$. Somit erhalten wir den folgenden Teil einer langen exakten Sequenz

$$0 \to \hat{H}^1(H,C) \to \hat{H}^1(H,C(\gamma)) \to \hat{H}^1(H,I_G) \to \hat{H}^2(H,C) \to \hat{H}^2(H,C(\gamma)) \to 0, \qquad (*)$$

den wir zum Beweis der Äquivalenzen heranziehen.

(i) $\Rightarrow$ *(ii)*: Ist $C(\gamma)$ kohomologisch trivial, so folgt aus $(*)$, daß $\hat{H}^1(H,C) = 0$ ist, und daß δ_2 und somit auch $\delta^2 : \hat{H}^0(H,\mathbb{Z}) \to \hat{H}^2(H,C)$ ein Isomorphismus ist. Daher ist C ein Klassenmodul.

(ii) $\Rightarrow$ *(i)*: Ist C ein Klassenmodul, dann ist notwendig $\delta_2 : \hat{H}^1(H,I_G) \to \hat{H}^2(H,C)$ ein Isomorphismus, weshalb wegen $(*)$ $\hat{H}^1(H,C(\gamma)) = \hat{H}^2(H,C(\gamma)) = 0$ ist. Hieraus schließen wir mittels Satz (1.1.8) die kohomologische Trivialität von $C(\gamma)$.

Die Äquivalenz von *(ii)* und *(iii)* ergibt sich sofort aus Betrachtung der zu $0 \to C \to C(\gamma) \to I_G \to 0$ gehörigen langen exakten Sequenz. □

Einen ersten Schritt auf dem Weg zum Satz von Nakayama-Tate bildet das folgende Lemma (vgl. [NSW], Proposition 3.1.1):

(1.1.26) Lemma. *Sei G eine endliche Gruppe und A ein G-Modul. Dann liefert für alle $i \in \mathbb{Z}$ das Cupprodukt*

$$\hat{H}^i(G, A^*) \times \hat{H}^{-i-1}(G, A) \xrightarrow{\cup} \hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) = \tfrac{1}{|G|}\mathbb{Z}/\mathbb{Z}$$

einen Isomorphismus

$$\hat{H}^i(G, A^*) \cong \hat{H}^{-i-1}(G, A)^*.$$

Beweis. Zunächst beschreibt man für $i = 0$ den Isomorphismus $\hat{H}^0(G, A^*) \cong \hat{H}^{-1}(G, A)^*$ direkt. Dann verwendet man Dimensionsverschiebung und den Satz (1.1.12), um das Resultat für alle $i \in \mathbb{Z}$ zu erhalten. Die Details des Beweises sind in [NSW], S. 113, nachzulesen. □

Der nächste Schritt wird geliefert durch folgendes Lemma ([NSW], Proposition 3.1.2).

(1.1.27) Lemma. *Sei G eine endliche Gruppe und A ein $\mathbb{Z}$-freier G-Modul. Dann liefert für alle $i \in \mathbb{Z}$ das Cupprodukt*

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

einen Isomorphismus

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

Beweis. A ist ein $\mathbb{Z}$-freier Modul, weshalb die induzierte Sequenz

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

exakt ist. Nun ist $Hom(A, \mathbb{Q})$ aber kohomologisch trivial, denn Multiplikation mit $|G|$ ist auf $\mathbb{Q}$ und somit auch auf $Hom(A, \mathbb{Q})$ bijektiv, weshalb $|G| \cdot \hat{H}^n(G, Hom(A, \mathbb{Q})) = 0$ nur gelten kann, wenn bereits $\hat{H}^n(G, Hom(A, \mathbb{Q})) = 0$ ist.

Aus Satz (1.1.11) erhalten wir das kommutative Diagramm

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

in dem die senkrechten Abbildungen Isomorphismen sind. Mittels der expliziten Beschreibung des rechten Verbindungshomomorphismus weiß man weiter, daß dieser die Identität ist. Somit folgt die Aussage vermöge Lemma (1.1.23) aus Lemma (1.1.26). □

Beweis des Satzes von Nakayama-Tate (1.1.24). Aus den exakten Sequenzen $0 \to C \to C(\gamma) \to I_G \to 0$ und $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ erhalten wir, da A $\mathbb{Z}$-frei ist, die exakten Sequenzen

$$0 \to Hom(A, C) \to Hom(A, C(\gamma)) \to Hom(A, I_G) \to 0$$

und

$$0 \to Hom(A, I_G) \to Hom(A, \mathbb{Z}[G]) \to Hom(A, \mathbb{Z}) \to 0.$$

Hieraus schließen wir nun unter Verwendung von Satz (1.1.11) die Kommutativität folgenden Diagramms:

$$\begin{array}{ccccc}
\hat{H}^{i-2}(G, Hom(A, \mathbb{Z})) & \times & \hat{H}^{2-i}(G, A) & \xrightarrow{\cup} & \hat{H}^0(G, \mathbb{Z}) \\
\delta\downarrow & & \mathrm{id}\uparrow & & \delta\downarrow \\
\hat{H}^{i-1}(G, Hom(A, I_G)) & \times & \hat{H}^{2-i}(G, A) & \xrightarrow{\cup} & \hat{H}^1(G, I_G) \\
\delta\downarrow & & \mathrm{id}\uparrow & & \delta\downarrow \\
\hat{H}^i(G, Hom(A, C)) & \times & \hat{H}^{2-i}(G, A) & \xrightarrow{\cup} & \hat{H}^2(G, C).
\end{array}$$

Da C ein Klassenmodul ist, folgt nach Satz (1.1.25) die kohomologische Trivialität von $C(\gamma)$. Nun schließt man mittels Satz (1.1.9) auf die kohomologische Trivialtität von $Hom(A,\mathbb{Z}[G])$ und $Hom(A, C(\gamma))$. Folglich sind die vertikalen Abbildungen im Diagramm Isomorphismen.

Der Satz folgt daher aus Lemma (1.1.27) unter Verwendung von Lemma (1.1.23). □

Proendliche Version des Satzes von Nakayama-Tate

Aus dem Dualitätssatz von Nakayama-Tate schließen wir folgende proendliche Version (vgl. [S], Proposition 4).

(1.1.28) Satz. *Sei G eine proendliche Gruppe und C ein Formationsmodul, der level-kompakt sei. Dann liefert für einen als $\mathbb{Z}$-Modul endlich erzeugten, diskreten und $\mathbb{Z}$-freien G-Modul A das Cupprodukt*

$$\hat{H}^i(G, Hom(A,C)) \times \hat{H}^{2-i}(G,A) \xrightarrow{\ \cup\ } \hat{H}^2(G,C) \subseteq \mathbb{Q}/\mathbb{Z}$$

für alle $i \in \mathbb{Z}$ einen topologischen Isomorphismus (d.h. insbesondere einen Homöomorphismus)

$$\hat{H}^i(G, Hom(A,C)) \cong \hat{H}^{2-i}(G,A)^\vee.$$

Im Fall $i=1$ sind die Gruppen endlich.

Beweis. Für den Verlauf des Beweises fixieren wir einen offenen Normalteiler $U \lhd G$ mit der Eigenschaft, daß $A = A^U$ ist, was wegen Bemerkung (1.1.20) erlaubt ist. Wir müssen drei Fälle unterscheiden.

(I) $\underline{i < 1}$: Dann ist $2 - i > 1$. Sei $V \lhd G$ ein offener Normalteiler mit $V \leq U$. Aus dem kommutativen Diagramm aus Satz (1.1.13)

$$\begin{array}{ccccc} \hat{H}^i(G/U, Hom(A,C^U)) & \times & \hat{H}^{2-i}(G/U,A) & \xrightarrow{\ \cup\ } & \hat{H}^2(G/U,C^U) \subseteq \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle\mathrm{def}}\big\uparrow & & {\scriptstyle\mathrm{inf}}\big\downarrow & & {\scriptstyle\mathrm{inf}}\big\downarrow \\ \hat{H}^i(G/V, Hom(A,C^V)) & \times & \hat{H}^{2-i}(G/V,A) & \xrightarrow{\ \cup\ } & \hat{H}^2(G/V,C^V) \subseteq \mathbb{Q}/\mathbb{Z} \end{array}$$

erhalten wir mittels Lemma (1.1.23) das kommutative Diagramm,

$$\begin{array}{ccc} \hat{H}^i(G/U, Hom(A,C^U)) & \longrightarrow & \hat{H}^{2-i}(G/U,A)^\vee \\ {\scriptstyle\mathrm{def}}\big\uparrow & & {\scriptstyle\mathrm{inf}^\vee}\big\uparrow \\ \hat{H}^i(G/V, Hom(A,C^V)) & \longrightarrow & \hat{H}^{2-i}(G/V,A)^\vee \end{array},$$

dessen horizontale Abbildungen nach dem Satz von Nakayama-Tate (1.1.24) Isomorphismen sind. Anwendung des projektiven Limes liefert nun die Behauptung in diesem Fall.

(II) $\underline{i > 1}$: Dann ist $2-i < 1$. Zunächst haben wir das kommutative Diagramm aus Satz (1.1.13)

$$\begin{array}{ccccc} \hat{H}^{2-i}(G/U,A) & \times & \hat{H}^i(G/U, Hom(A,C^U)) & \xrightarrow{\ \cup\ } & \hat{H}^2(G/U,C^U) \subseteq \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle\mathrm{def}}\big\uparrow & & {\scriptstyle\mathrm{inf}}\big\downarrow & & {\scriptstyle\mathrm{inf}}\big\downarrow \\ \hat{H}^{2-i}(G/V,A) & \times & \hat{H}^i(G/V, Hom(A,C^V)) & \xrightarrow{\ \cup\ } & \hat{H}^2(G/V,C^V) \subseteq \mathbb{Q}/\mathbb{Z} \end{array}.$$

Indem wir in der oberen und in der unteren Zeile die Argumente formal vertauschen (dabei werde beachtet, daß $a \cup b = (-1)^{i(i-2)} b \cup a$ gilt), erhalten wir mittels Lemma (1.1.23) das kommutative Diagramm

$$\begin{array}{ccc} \hat{H}^i(G/U, Hom(A,C^U)) & \longrightarrow & \hat{H}^{2-i}(G/U,A)^\vee \\ {\scriptstyle\mathrm{inf}}\big\downarrow & & {\scriptstyle\mathrm{def}^\vee}\big\downarrow \\ \hat{H}^i(G/V, Hom(A,C^V)) & \longrightarrow & \hat{H}^{2-i}(G/V,A)^\vee \end{array}$$

mit horizontalen Isomorphismen, aus dem durch Anwendung des induktiven Limes die Behauptung folgt.

(III) $\underline{i=1:}$ Wir haben $\hat{H}^1(U/V,A^V)=\hat{H}^1(U/V,A)=Hom(U/V,A)=0$, denn A ist $\mathbb{Z}$-frei. Aus der Inflation-Restriktion-Sequenz

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

erhalten wir folglich die Isomorphie $\hat{H}^1(G/U,A)\cong\hat{H}^1(G/V,A)$. Das heißt, daß der induktive Limes über diese Objekte stationär wird. Damit ist insbesondere $\hat{H}^1(G,A)$ endlich.

Ferner haben wir

$$\hat{H}^1(U/V,Hom(A,C)^V)=\hat{H}^1(U/V,Hom(A,C^V))=\bigoplus_{rk_{\mathbb{Z}}(A)}\hat{H}^1(U/V,C^V)=0,$$

denn C ist eine Klassenformation.

Hieraus schließen wir wieder mittels der Inflation-Restriktion-Sequenz

$$\begin{aligned} 0 &\longrightarrow \hat{H}^1(G/U,Hom(A,C)^U) \xrightarrow{\text{inf}} \hat{H}^1(G/V,Hom(A,C)^V) \\ &\xrightarrow{\text{res}} \hat{H}^1(U/V,Hom(A,C)^V) \end{aligned}$$

auf die Isomorphie $\hat{H}^1(G/U,Hom(A,C^U))\cong\hat{H}^1(G/V,Hom(A,C^V))$, weshalb wiederum der induktive Limes hierüber stationär wird.

Damit folgt das Resultat aus dem endlichen Fall (Satz (1.1.24)). □

1.1.5. Abstrakte Klassenkörpertheorie

Aus Satz (1.1.25) erhalten wir sofort den *Hauptsatz über Klassenformationen*:

(1.1.29) Satz. *Sei (G,C) eine Klassenformation. Dann ist die Abbildung*

$$u_{U/V}\cup:\hat{H}^q(U/V,\mathbb{Z})\to\hat{H}^{q+2}(U/V,C^V)$$

für offene Untergruppen $V\lhd U$ von G ein Isomorphismus.

Insbesondere gilt das *allgemeine Reziprozitätsgesetz*:

(1.1.30) Satz. *Für offene Untergruppen $V\lhd U$ von G liefert*

$$u_{U/V}\cup:\hat{H}^{-2}(U/V,\mathbb{Z})\to\hat{H}^0(U/V,C^V)$$

den Isomorphismus

$$\Theta_{U/V}:(U/V)^{ab}\to C^U/N_{U/V}C^V.$$

Den von seiner Umkehrabbildung erzeugten Homomorphismus

$$(\cdot,U/V):C^U\to(U/V)^{ab}$$

nennen wir den Reziprozitätshomomorphismus.

Der Reziprozitätshomomorphismus hat folgende Eigenschaften (vgl. [N-KKT], Satz II.1.11).

(1.1.31) Satz. *Sei (G,C) eine Klassenformation und seien $W\lhd V\lhd U$, $W\lhd U$ offene Untergruppen von G. Dann sind die folgenden Diagramme kommutativ.*

(a)

$$\begin{array}{ccc} C^U & \xrightarrow{(\cdot,U/W)} & (U/W)^{ab} \\ {\scriptstyle Identität}\big\downarrow & & \big\downarrow{\scriptstyle kanonisch} \\ C^U & \xrightarrow{(\cdot,U/V)} & (U/V)^{ab} \end{array}$$

(b)

$$\begin{array}{ccc} C^U & \xrightarrow{(\cdot,U/W)} & (U/W)^{ab} \\ {\scriptstyle Inklusion}\big\downarrow & & \big\downarrow{\scriptstyle Verlagerung} \\ C^V & \xrightarrow{(\cdot,V/W)} & (V/W)^{ab} \end{array}$$

Dabei wird die Verlagerung *von der Restriktion* $\hat{H}^{-2}(U/W,\mathbb{Z}) \to \hat{H}^{-2}(V/W,\mathbb{Z})$ *induziert.*

(c)

$$\begin{array}{ccc} C^V & \xrightarrow{(\cdot,V/W)} & (V/W)^{ab} \\ {\scriptstyle N_{U/V}}\big\downarrow & & \big\downarrow{\scriptstyle kanonisch} \\ C^U & \xrightarrow{(\cdot,U/W)} & (U/W)^{ab} \end{array}$$

Die Klassenkörpertheorie beinhaltet die Klassifikation der abelschen Oberkörper eines Körpers. Der folgende Satz (vgl. [N-KKT], Satz II.1.14) stellt die abstrakte Version dessen dar.

(1.1.32) Satz. *Sei (G,C) eine Klassenformation und sei $U \leq G$ eine offene Untergruppe. Eine* Normengruppe *(bzgl. U) ist eine Untergruppe I von C^U, so daß eine offene Untergruppe $V \leq G$ mit $V \lhd U$ existiert, für die $I = N_{U/V}C^V$ gilt.*

Die Normengruppen bilden einen Verband. Die Zuordnung

$$V \mapsto N_{U/V}C^V$$

bildet einen inklusionsumkehrenden Verbandsisomorphismus zwischen dem Verband der in G offenen Normalteiler von U, für die U/V abelsch ist, und dem Verband der Normengruppen bzgl. U.

Außerdem ist jede in C^U enthaltene Obergruppe einer Normengruppe selbst eine Normengruppe.

1.1.6. Ein abstrakter Dualitätssatz

Sei G_k eine proendliche Gruppe. Wir indizieren die abgeschlossenen Normalteiler von G_k mit formalen Körpern $G_K \lhd G_k$ und schreiben für eine zwei formale Körper $L|k$ und $K|k$ mit $G_L \subseteq G_K$ für den Quotienten $G(L|K) := G_K/G_L$. Wir nennen die formale (galoissche) Erweiterung $L|K$ abelsch bzw. eine p-Erweiterung, falls $G(L|K)$ eine abelsche bzw. eine Pro-p-Gruppe ist.

Wir betrachten die folgende Situation:

- $(G_k,\mathcal{C})$ sei eine Klassenformation.
- Es existiere ein level-kompakter G_k-Modul $\mathcal{C}^0$ und ein kohomologisch trivialer G_k-Modul X, so daß die Sequenz
$$1 \to \mathcal{C}^0 \to \mathcal{C} \to X \to 1$$
mit stetigen Homomorphismen exakt ist.

- Für jede endliche formale Körpererweiterung $K|k$ seien die $G(K|k)$-Moduln

$$\mathcal{C}_K := \mathcal{C}^{G_K},\ \ \mathcal{I}_K,\ \ E_K,\ \ \mathcal{C}l_K$$

gegeben, welche eine exakte Sequenz bilden:

$$1 \to E_K \to \mathcal{I}_K \to \mathcal{C}_K \to \mathcal{C}l_K \to 1. \tag{1}$$

- Für endliche formale Körpererweiterungen $K'|K$ seien Abbildungen ι gegeben, wobei $\iota : \mathcal{C}_K \hookrightarrow \mathcal{C}_{K'}$ die Einbettung sei, so daß das Diagramm **(1.1.33)**

$$\begin{array}{ccccccccc}
1 & \longrightarrow & E_{K'} & \longrightarrow & \mathcal{I}_{K'} & \longrightarrow & \mathcal{C}_{K'} & \longrightarrow & \mathcal{C}l_{K'} & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle\iota} & & \uparrow{\scriptstyle\iota} & & \uparrow{\scriptstyle\iota} & & \uparrow{\scriptstyle\iota} & & \\
1 & \longrightarrow & E_K & \longrightarrow & \mathcal{I}_K & \longrightarrow & \mathcal{C}_K & \longrightarrow & \mathcal{C}l_K & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle N_{K'|K}} & & \uparrow{\scriptstyle N_{K'|K}} & & \uparrow{\scriptstyle N_{K'|K}} & & \uparrow{\scriptstyle N_{K'|K}} & & \\
1 & \longrightarrow & E_{K'} & \longrightarrow & \mathcal{I}_{K'} & \longrightarrow & \mathcal{C}_{K'} & \longrightarrow & \mathcal{C}l_{K'} & \longrightarrow & 1
\end{array}$$

kommutativ ist. Außerdem bilden die Moduln via ι direkte Systeme. Wir setzen:

$$\mathcal{I} = \varinjlim_{K|k \text{ endl.}} \mathcal{I}_K,\ E = \varinjlim_{K|k \text{ endl.}} E_K,\ E(p) = \varinjlim_{K|k \text{ endl. } p\text{-Erw.}} E_K,\ \mathcal{C}(p) = \varinjlim_{K|k \text{ endl. } p\text{-Erw.}} \mathcal{C}_K.$$

- $\mathcal{I}_K$ hat guten Galois-Abstieg, d. h. $\mathcal{I}_{K'}^{G(K'|K)} = \mathcal{I}_K$.
  Außerdem gilt $H^1(G(K'|K), \mathcal{I}_{K'}) = 1$ für jede endliche formale Erweiterung $K'|K$.

- Für jede endliche formale Körpererweiterung $K|k$ ist $\mathcal{C}l_K$ endlich, und der Reziprozitätshomomorphismus induziert einen Isomorphismus

$$\mathcal{C}l_K \cong \mathcal{C}_K / N_{L|K}\mathcal{C}_L \cong G(L|K) = G_K^{ab},$$

wobei der formale Körper L durch $G_L = \overline{[G_K, G_K]}$ festgelegt ist.

- (a) $\hat{H}^i(G(K|k), \mathcal{I}_K) = 1$ für alle endlichen $K|k$ und alle $i \in \mathbb{Z}$.
  (b) $\hat{H}^i(G(K|k), \mathcal{I}_K) = 1$ für alle endlichen p-Erweiterungen $K|k$ und alle $i \in \mathbb{Z}$.

- (a) Via ι gilt: $\varinjlim_{K|k \text{ endl.}} \mathcal{C}l_K = 1.$
  (b) Via ι gilt: $\varinjlim_{K|k \text{ endl.}} \mathcal{C}l_K = 1$ und $\varinjlim_{K|k \text{ endl. } p\text{-Erw.}} \mathcal{C}l_K(p) = 1.$

(1.1.34) Theorem. *Für jedes $i \in \mathbb{Z}$ gibt es in Situation (a) einen kanonischen topologischen Isomorphismus*

$$\hat{H}^i(G_k, E) \cong \hat{H}^{2-i}(G_k, \mathbb{Q}/\mathbb{Z})^\vee$$

und in Situation (b) einen kanonischen topologischen Isomorphismus

$$\hat{H}^i(G_k(p), E(p)) \cong \hat{H}^{2-i}(G_k(p), \mathbb{Q}_p/\mathbb{Z}_p)^\vee.$$

Für eine proendliche Gruppe G bezeichnen wir dabei mit $G(p)$ ihren maximalen Pro-p-Quotienten. Für ihn gilt $G(p) = G/R$, wobei R für den Durchschnitt aller offenen Normalteiler $H \lhd G$ steht, für die G/H eine p-Gruppe ist.

(1.1.35) Lemma. *$(G(p))^{ab}$ ist der maximale Pro-p-Quotient von G^{ab}, d.h.*

$$(G(p))^{ab} = (G^{ab})(p).$$

Beweis. Es gilt: $(G/R)^{ab} \cong (G/R)/\overline{[G/R, G/R]} \cong G/\overline{[G,G]}R$. Da, falls $H \lhd G$ ein offener Normalteiler ist, auch $H\overline{[G,G]}/\overline{[G,G]} \lhd G/\overline{[G,G]}$ ein offener Normalteiler ist, und es umgekehrt zu jedem offenen Normalteiler $N \lhd G/\overline{[G,G]}$ einen offenen Normalteiler $H \lhd G$ mit $\overline{[G,G]} \subseteq H$ und $N = H/\overline{[G,G]}$ gibt, ergibt sich die Gleichheit von $(G/R)^{ab}$ und $(G^{ab})(p)$. □

Bevor wir zum Beweis des Theorems kommen, beweisen wir zunächst ein

(1.1.36) Lemma. *E hat guten Galois-Abstieg und es gilt für alle $K|k$*

$$H^1(G_K, E) \cong \mathcal{C}l_K$$

und im Fall (b) zusätzlich

$$H^1(G_K(p), E(p)) \cong \mathcal{C}l_K(p).$$

Beweis. Wegen $\varinjlim_{K|k} \mathcal{C}l_K = 1$ ist die Sequenz $1 \to E \to \mathcal{I} \to \mathcal{C} \to 1$ exakt. Zu ihr betrachten wir die lange exakte Sequenz $1 \to E^{G_K} \to \mathcal{I}_K \to \mathcal{C}_K \to H^1(G_K, E) \to H^1(G_K, \mathcal{I}) = 1$. Vergleichen wir diese mit der exakten Sequenz $1 \to E_K \to \mathcal{I}_K \to \mathcal{C}_K \to \mathcal{C}l_K \to 1$, so folgt der erste Teil der Aussage.

Sind wir in der Situation (b), so betrachten wir

$$G_K(p) = G_K/\Big(\bigcap_{L|K \text{ endl. } p\text{-Erw.}} G_L\Big) = G_K/\Big(\varprojlim_{L|K \text{ endl. } p\text{-Erw.}} G_L\Big).$$

Daher ist aufgrund des ersten Teils

$$H^1\Big(\varprojlim_{L|K \text{ endl. } p\text{-Erw.}} G_L, E\Big)(p) = \varinjlim_{L|K \text{ endl. } p\text{-Erw.}} H^1(G_L, E)(p) = \varinjlim_{L|K \text{ endl. } p\text{-Erw.}} \mathcal{C}l_L(p) = 1.$$

Folglich schließen wir aus der Inflation-Restriktion-Sequenz

$$1 \to H^1(G_K(p), E(p)) \xrightarrow{\text{inf}} H^1(G_K, E)(p) \xrightarrow{\text{res}} H^1\Big(\varprojlim_{L|K \text{ endl. } p\text{-Erw.}} G_L, E\Big)(p) = 1$$

die Isomorphie $H^1(G_K(p), E(p)) \cong \mathcal{C}l_K(p)$. □

Beweis von (1.1.34). Zunächst erhalten wir wegen der kohomologischen Trivialität von X die Homöomorphie

$$\hat{H}^i(G_k, \mathcal{C}) \cong \hat{H}^i(G_k, \mathcal{C}^0)$$

für alle $i \in \mathbb{Z}$. Dies hat zur Folge, daß sich die proendliche Version des Satzes von Nakayama-Tate (1.1.28) auch auf $\mathcal{C}$ anwenden läßt, und wir für alle $i \in \mathbb{Z}$ einen Homöomorphismus

$$\hat{H}^i(G_k, \mathcal{C}) \cong \hat{H}^{2-i}(G_k, \mathbb{Z})^\vee$$

erhalten. Die gleichen Überlegungen ergeben im Falle (b) eine Homöomorphie

$$\hat{H}^i(G_k(p), \mathcal{C}(p)) \cong \hat{H}^{2-i}(G_k(p), \mathbb{Z})^\vee.$$

Ebenso erhalten wir für eine endliche Erweiterung $K|k$ Isomorphismen

$$\hat{H}^i(G(K|k), \mathcal{C}_K) \cong \hat{H}^{2-i}(G(K|k), \mathbb{Z})^\vee,$$

aus denen wir auf die Endlichkeit der linken Gruppe schließen, da die rechte als $\mathbb{Z}$-Modul endlich erzeugt ist und von $|G(K|k)|$ annulliert wird.

Wir teilen die 4-Terme-Sequenz (1) auf in

$$1 \to E_K \to \mathcal{I}_K \to M_K \to 1$$

und

$$1 \to M_K \to \mathcal{C}_K \to \mathcal{C}l_K \to 1.$$

Wegen der kohomologischen Trivialität von $\mathcal{I}_K$ erhalten wir hieraus für $i \in \mathbb{Z}$ Isomorphismen

$$\hat{H}^{i+1}(G(K|k), E_K) \xrightarrow{\sim} \hat{H}^i(G(K|k), M_K) \tag{2}$$

für alle endlichen Erweiterungen $K|k$ im Fall (a) bzw. für alle endlichen p-Erweiterungen $K|k$ im Fall (b). Ferner bekommen wir die exakte Sequenz

$$\hat{H}^i(G(K|k), M_K) \to \hat{H}^i(G(K|k), \mathcal{C}_K) \to \hat{H}^i(G(K|k), \mathcal{C}l_K) \to \hat{H}^{i+1}(G(K|k), M_K). \tag{3}$$

Wir wollen im folgenden für alle $i \in \mathbb{Z}$ die Existenz eines Homöomorphismus

$$\hat{H}^i(G_k, \mathcal{C}) \cong \hat{H}^{i+1}(G_k, E)$$

im Fall (a) bzw. im Fall (b)

$$\hat{H}^i(G_k(p), \mathcal{C}(p)) \cong \hat{H}^{i+1}(G_k(p), E(p))$$

zeigen, denn dann folgt der Satz im Fall (a) wegen

$$\hat{H}^i(G_k, E) \cong \hat{H}^{i-1}(G_k, \mathcal{C}) \cong \hat{H}^{3-i}(G_k, \mathbb{Z})^\vee \cong \hat{H}^{2-i}(G_k, \mathbb{Q}/\mathbb{Z})^\vee$$

bzw. der analogen Rechnung im Fall (b).

Wir behandeln drei Fälle getrennt.

(I) $\underline{i = 0}$: In diesem Fall haben wir für (a) folgende Isomorphismen:

$$\begin{aligned} \mathcal{C}l_k &\xrightarrow{\text{Reziprozität}} G_k^{ab} \xrightarrow{\text{Bidual}} H^1(G_k, \mathbb{R}/\mathbb{Z})^\vee \\ &\xrightarrow{\delta} H^2(G_k, \mathbb{Z})^\vee \xrightarrow{\text{proendlicher Nakayama-Tate}} \hat{H}^0(G_k, \mathcal{C}). \end{aligned}$$

Im Fall (b) ergibt sich:

$$\mathcal{C}l_k(p) \to G_k^{ab}(p) \to H^1(G_k(p), \mathbb{R}/\mathbb{Z})^\vee \to H^2(G_k(p), \mathbb{Z})^\vee \to \hat{H}^0(G_k(p), \mathcal{C}(p)).$$

Dabei haben wir Lemma (1.1.35) benutzt.

Mittels Lemma (1.1.36) erhalten wir die Aussage.

(II) $\underline{i > 0}$: Entscheidend ist, daß

$$\varinjlim_{K|k \text{ endl.}} H^i\big(G(K|k), \mathcal{C}l_K\big) = H^i\big(G_k, \varinjlim_{K|k \text{ endl.}} \mathcal{C}l_K\big) = H^i\big(G_k, 1\big) = 1$$

für (a) und im Fall (b) zusätzlich

$$\varinjlim_{K|k \text{ endl. } p\text{-Erw.}} H^i\big(G(K|k), \mathcal{C}l_K\big) = H^i\big(G_k(p), \varinjlim_{K|k \text{ endl. } p\text{-Erw.}} \mathcal{C}l_K(p)\big) = H^i\big(G_k(p), 1\big) = 1$$

gilt. Bildung des direkten Limes von (2) und (3) über alle endlichen Erweiterungen $K|k$ im Fall (a) und im Fall (b) über die endlichen p-Erweiterungen ergibt dann topologische Isomorphismen

$$H^{i+1}\big(G_k, E\big) \cong H^i\big(G_k, \varinjlim M_K\big) \quad \text{bzw.} \quad H^{i+1}\big(G_k(p), E(p)\big) \cong H^i\big(G_k(p), \varinjlim M_K\big)$$

und

$$H^i\big(G_k, \varinjlim M_K\big) \cong H^i\big(G_k, \mathcal{C}\big) \quad \text{bzw.} \quad H^i\big(G_k(p), \varinjlim M_K\big) \cong H^i\big(G_k(p), \mathcal{C}(p)\big).$$

(III) $\underline{i < 0:}$ Entscheidend ist, daß im Fall (a)

$$\varprojlim_{K|k \text{ endl.}} \hat{H}^i\big(G(K|k), \mathcal{C}l_K\big) = 1$$

bzw. im Fall (b)

$$\varprojlim_{K|k \text{ endl. } p\text{-Erw.}} \hat{H}^i\big(G(K|k), \mathcal{C}l_K\big) = 1$$

gilt. Das sieht man wie folgt: Aus Satz (1.1.31) schließen wir auf die Kommutativität der Diagramme

$$\begin{array}{ccc} \mathcal{C}l_{K'} & \xrightarrow{N_{K'|K}} & \mathcal{C}l_K \\ {\scriptstyle \text{Rezipr}}\big\downarrow & & {\scriptstyle \text{Rezipr}}\big\downarrow \\ G_{K'}^{ab} & \xrightarrow{\text{kanonisch}} & G_K^{ab} \end{array} \quad \text{und} \quad \begin{array}{ccc} \mathcal{C}l_{K'}(p) & \xrightarrow{N_{K'|K}} & \mathcal{C}l_K(p) \\ {\scriptstyle \text{Rezipr}}\big\downarrow & & {\scriptstyle \text{Rezipr}}\big\downarrow \\ G_{K'}^{ab}(p) & \xrightarrow{\text{kanonisch}} & G_K^{ab}(p) \end{array}$$

mit senkrechten Isomorphismen. Wählen wir $K'|K$ so, daß $G(K'|K) = G_K^{ab}$ gilt, d.h. $G_{K'} = \overline{[G_K, G_K]}$, dann ist die kanonische Abbildung oben, die induziert wird von

$$G_{K'} = \overline{[G_K, G_K]} \to G_K^{ab} = G_K/\overline{[G_K, G_K]},$$

die Nullabbildung. Dies hat zur Folge, daß in diesem Fall auch $\mathcal{C}l_{K'} \xrightarrow{N_{K'|K}} \mathcal{C}l_K$ und $\mathcal{C}l_{K'}(p) \xrightarrow{N_{K'|K}} \mathcal{C}l_K(p)$ die Nullabbildungen sind, woraus sich die Behauptung ergibt.

Wir wollen nun wie im Fall (II) durch Übergang in (2) und (3) zum projektiven Limes via den Deflationen über die endlichen Erweiterungen $K|k$ im Fall (a) bzw. über die endlichen p-Erweiterungen im Fall (b) den Beweis abschließen. Dazu beachten wir, daß aus der Endlichkeit von $\mathcal{C}l_K$ die Endlichkeit von $\hat{H}^i(G(K|k), \mathcal{C}l_K)$ folgt, und wie oben gesehen auch die Gruppe $\hat{H}^i(G(K|k), \mathcal{C}_K)$ endlich ist. Daher schließen wir aus (3) auf die Endlichkeit von $\hat{H}^i(G(K|k), M_K)$. Also bleibt die Exaktheit beim Übergang zum projektiven Limes erhalten.

Somit ergibt sich

$$\hat{H}^{i+1}\big(G_k, E\big) \cong \varprojlim_{K|k \text{ endl.}} \hat{H}^i\big(G(K|k), M_K\big) \qquad \text{bzw.}$$

$$\hat{H}^{i+1}\big(G_k(p), E(p)\big) \cong \varprojlim_{K|k \text{ endl. } p\text{-Erw.}} \hat{H}^i\big(G_k(p), M_K\big) \qquad \text{und}$$

$$\varprojlim_{K|k \text{ endl.}} \hat{H}^i\big(G(K|k), M_K\big) \cong \hat{H}^i\big(G_k, \mathcal{C}\big) \qquad \text{bzw.}$$

$$\varprojlim_{K|k \text{ endl. } p\text{-Erw.}} \hat{H}^i\big(G(K|k), M_K\big) \cong \hat{H}^i\big(G_k(p), \mathcal{C}(p)\big).$$

□

1.2. Dualitätssätze in globaler Klassenkörpertheorie

1.2.1. Grundlagen

In diesem Abschnitt wollen wir kurz die wichtigsten im folgenden auftretenden Definitionen und einige ihrer elementarsten Eigenschaften auflisten, die in der globalen Klassenkörpertheorie Verwendung finden.

Eingeschränkte Produkte

(1.2.1) Definition. *Seien I eine Indexmenge und X_i und Y_i für $i \in I$ topologische Gruppen, so daß $Y_i \le X_i$ offene Untergruppen sind. Dann ist das* eingeschränkte Produkt *definiert als*

$$\prod_{\underline{i\in I}}(X_i, Y_i) := \{(x_i) \in \prod_{i\in I} X_i \mid x_i \in Y_i \text{ für fast alle } i \in I\ \}.$$

Dieses wird zur topologischen Gruppe durch Wahl einer Umgebungsbasis der 1 bestehend aus den Mengen

$$\prod_{j\in J} U_j \times \prod_{i\in I\setminus J} Y_j,$$

wobei U_j für festes $j \in J$ eine Umgebungsbasis der 1 von X_j, und J die endlichen Teilmengen von I durchläuft.

Das eingeschränkte Produkt hat die folgenden Eigenschaften (siehe [NSW], I.1):

(1.2.2) Satz. *Die X_i seien Hausdorffsch. Dann gilt:*

(a) $\prod_{\underline{i\in I}}(X_i, Y_i)$ ist Hausdorffsch.

(b) Sind die X_i lokal kompakt und die Y_i kompakt, so ist $\prod_{\underline{i\in I}}(X_i, Y_i)$ lokal kompakt.

Idel- und Idealgruppen

Sei k ein algebraischer Zahlkörper, von dem wir einen algebraischen Abschluß $\overline{k}$ fixiert halten wollen. Zu jeder Primstelle $\mathfrak{p}$ von k wählen wir eine Einbettung $i_\mathfrak{p} : \overline{k} \hookrightarrow \overline{k}_\mathfrak{p}$. Via dieser Einbettung entspricht einer endlichen Erweiterung $K|k$ mit $K \subset \overline{k}$ eine eindeutige vollständige Erweiterung $\overline{k}_\mathfrak{p}|K_{\mathfrak{P}^\bullet}|k_\mathfrak{p}$. Somit haben wir eine verträgliche Auswahl von Primstellen $\mathfrak{P}^\bullet|\mathfrak{p}$ für jede endliche Erweiterung getroffen.

Wir wollen schreiben: $G_\mathfrak{p}(K|k) = G(K_{\mathfrak{P}^\bullet}|k_\mathfrak{p})$, $G_K := G(\overline{k}|K)$ und $K_\mathfrak{p} := K_{\mathfrak{P}^\bullet}$.

Ferner wollen wir uns darauf einigen, was wir unter den Einseinheitengruppen eines Zahlkörpers K auch für unendliche Stellen verstehen möchten und setzen für $n \ge 0$:

$$\mathcal{U}_\mathfrak{p}^{(n)} := \begin{cases} \mathcal{U}_\mathfrak{p} & \text{für } n = 0,\ \mathfrak{p} \nmid \infty, \\ n-\text{te Einseinheitengruppe von } K_\mathfrak{p} & \text{für } n > 0,\ \mathfrak{p} \nmid \infty, \\ \mathbb{R}^\times & \text{für } n = 0,\ \mathfrak{p} \text{ reell}, \\ \mathbb{R}_+ & \text{für } n \ge 1,\ \mathfrak{p} \text{ reell}, \\ \mathbb{C}^\times & \text{für } \mathfrak{p} \text{ komplex}. \end{cases}$$

Wir definieren nun die *Idelgruppe* als das eingeschränkte Produkt

$$\mathcal{I}_K := \prod_{\underline{\mathfrak{p}}}(K_\mathfrak{p}^\times, \mathcal{U}_\mathfrak{p}^{(0)}).$$

Nach Satz (1.2.2) ist die Idelgruppe lokal kompakt und Hausdorffsch.

Unter einem *Modul* wollen wir ein formales Produkt

$$\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$$

verstehen, wobei $n_\mathfrak{p} \ge 0$ für alle und $n_\mathfrak{p} = 0$ für fast alle $\mathfrak{p}$ vorausgesetzt sei.

Für einen Modul $\mathfrak{m}$ definieren wir die *Idelgruppe modulo* $\mathfrak{m}$ als

$$\mathcal{I}_K^{\mathfrak{m}} := \prod_{\mathfrak{p}|\mathfrak{m}} \mathcal{U}_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \times \prod_{\mathfrak{p}\nmid\mathfrak{m}} \mathcal{U}_{\mathfrak{p}}^{(0)},$$

die als abgeschlossene Untergruppe von $\mathcal{I}_K$ auch lokal kompakt ist.

Sei S eine Primstellenmenge von K. Für sie definieren wir die S-*Idelgruppe*

$$\mathcal{I}_S(K) := \underline{\prod_{\mathfrak{p}\in S}} (K_{\mathfrak{p}}^{\times}, \mathcal{U}_{\mathfrak{p}}^{(0)}) \times \prod_{\mathfrak{p}\notin S} \mathcal{U}_{\mathfrak{p}}^{(0)},$$

die ebenfalls abgeschlossen in $\mathcal{I}_K$ und lokal kompakt ist. Weiter halten wir fest, daß aufgrund unserer Definition von $\mathcal{U}_{\mathfrak{p}}^{(0)}$ an reellen Stellen $\mathcal{I}_S(K)$ gleich $\mathcal{I}_T(K)$ ist, falls sich die Primstellenmengen S und T nur an unendlichen Stellen unterscheiden.

Mit $\mathcal{O}_K$ wollen wir wie gewöhnlich den Ring der ganzen Zahlen von K bezeichnen. Ferner setzen wir für eine Primstellenmenge S

$$\mathcal{O}_{K,S} := \{a \in K \mid v_{\mathfrak{p}}(a) \geq 0 \text{ für alle } \mathfrak{p} \notin S, \mathfrak{p} \nmid \infty\},$$

d. h. daß gilt

$$\mathcal{O}_{K,S}^{\times} = \{a \in K \mid v_{\mathfrak{p}}(a) = 0 \text{ für alle } \mathfrak{p} \notin S, \mathfrak{p} \nmid \infty\} = \mathcal{I}_S(K) \cap K^{\times}.$$

Wir definieren für einen Modul $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$

$$\mathcal{O}_{K,\mathfrak{m}}^{\times} := \{a \in \mathcal{O}_K \mid a \in \mathcal{U}_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \text{ für alle } \mathfrak{p}\} = \mathcal{I}_K^{\mathfrak{m}} \cap K^{\times}.$$

Weiter bezeichne $\mathcal{J}_K$ die *Idealgruppe* von $\mathcal{O}_K$. Sie ist die freie abelsche Gruppe mit den Primidealen als Erzeugenden. Unter $\mathcal{J}_K^S$ wollen wir die Idealgruppe von $\mathcal{O}_{K,S}$ verstehen, welche isomorph ist zur freien abelschen Gruppe erzeugt von den Primidealen außerhalb von S. Ebenso sei $\mathcal{J}_K^{\mathfrak{m}}$ die Untergruppe von $\mathcal{J}_K$ der zu $\mathfrak{m}$ teilerfremden Ideale, welche somit isomorph zu $\mathcal{J}_K^S$ ist, wobei S hier die Menge aller $\mathfrak{m}$ teilenden Primideale bezeichnet.

Galois-Aktion

Im folgenden wollen wir eine Galois-Aktion auf den Idelen definieren. Sei dazu $K|k$ eine endliche galoissche Erweiterung mit Galois-Gruppe $G(K|k)$. Ein $\sigma \in G(K|k)$ operiere nun auf einem Idel $\mathfrak{a} = (\mathfrak{a}_{\mathfrak{P}})_{\mathfrak{P}}$ durch

$$(\sigma\mathfrak{a})_{\mathfrak{P}} := \sigma\mathfrak{a}_{\sigma^{-1}\mathfrak{P}}.$$

Für eine Menge S von Primstellen von k werde die Menge aller Primstellen von K, die über denen von S liegen, ebenfalls mit S bezeichnet. Ist $\mathfrak{m} = \prod_i \mathfrak{p}_i^{n_i}$ ein Modul von k, so bezeichnen wir ebenfalls mit $\mathfrak{m}$ den Modul $\prod_i (\mathfrak{P}_{i,1} \cdots \mathfrak{P}_{i,r_i})^{e_i n_i}$ von K, wobei die $\mathfrak{P}_{i,j}$ die über $\mathfrak{p}_i$ liegenden Primstellen von K sind, und e_i der Verzweigungsindex von $\mathfrak{P}_{i,j}$ über $\mathfrak{p}_i$ ist.

Es ist klar, daß die Untergruppen $\mathcal{I}_S(K)$ und $\mathcal{I}_K^{\mathfrak{m}}$ unter dieser Aktion abgeschlossen sind. Die Idealgruppe $\mathcal{J}_K$ versehen wir mit der gewöhnlichen Galois-Aktion, also der Anwendung von $\sigma \in G(K|k)$ auf das Ideal. Der Homomorphismus

$$\chi : \mathcal{I}_K \to \mathcal{J}_K,\ \mathfrak{a} \mapsto \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}})}$$

ist ein G-Homomorphismus: $\sigma.\chi(\mathfrak{a}) = \sigma \prod \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}})} = \prod (\sigma\mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}})} = \prod \mathfrak{p}^{v_{\mathfrak{p}}(\sigma\mathfrak{a}_{\sigma^{-1}\mathfrak{p}})} = \chi(\sigma\mathfrak{a})$.

Ferner gilt nach Satz III.2.5 aus [N-KKT], daß $\mathcal{I}(K)$ guten Galois-Abstieg hat, daß also

$$\mathcal{I}_k = \mathcal{I}_K^{G(K|k)}$$

ist, was sich natürlich auch auf $\mathcal{I}_K^{\mathfrak{m}}$ und $\mathcal{I}_S(K)$ überträgt. Damit erhalten wir für eine Galois-Erweiterung $M|K$ diskrete $G(M|K)$-Moduln wie folgt:

$$\mathcal{I}_M = \varinjlim_{L|K,\, L\subseteq M} \mathcal{I}_L = \bigcup_{L|K,\, L\subseteq M} \mathcal{I}_M^{G(M|L)}$$

(bzw. Gleiches für $\mathcal{I}_S(K)$ und $\mathcal{I}_K^{\mathfrak{m}}$).

Wir können nun auch die Tate-Kohomologie der Idelgruppe betrachten. Diese hat folgende fundamentale Eigenschaft, die uns erlauben wird, Resultate aus dem Lokalen ins Globale zu übertragen.

(1.2.3) Satz. *Sei $K|k$ eine endliche Galois-Erweiterung. Dann gilt für alle $i \in \mathbb{Z}$*

$$\hat{H}^i(G(K|k), I_K) \cong \bigoplus_{\mathfrak{p}} \hat{H}^i(G_{\mathfrak{p}}(K|k), K_{\mathfrak{p}}^\times).$$

Dabei beachte man die Konvention der Primstellenauswahl bei Erweiterungen.

Beweis. Der Beweis beruht auf dem Lemma von Shapiro und ist z. B. in [NSW], Proposition 8.1.2, nachzulesen. □

Als Konsequenz von Hilberts Satz 90 erhalten wir das

(1.2.4) Korollar. *Für endliche Galois-Erweiterungen $K|k$ gilt: $H^1(G(K|k), \mathcal{I}_K) = 1$.*

(1.2.5) Korollar. *Sei $K|k$ eine unverzweigte endliche Galois-Erweiterung, die in einer Primstellenmenge S voll zerlegt ist, dann gilt für alle $i \in \mathbb{Z}$: $\hat{H}^i(G(K|k), \mathcal{I}_S(K)) = 1$.*

Beweis. Ist $\mathfrak{p} \in S$, so ist die Zerlegungsgruppe gleich $G(K_{\mathfrak{p}}|k_{\mathfrak{p}}) = 1$. Außerdem gilt für unverzweigte Stellen $\mathfrak{p}$ nach [N-KKT], II.4.3, daß $\hat{H}^i(G(K_{\mathfrak{p}}|k_{\mathfrak{p}}), \mathcal{U}_{\mathfrak{p}}) = 1$ ist. □

Idel-, Ideal- und Strahlklassengruppen

Aus [N-ZT] zitieren wir den wichtigen Satz VI.1.5:

(1.2.6) Satz. *$k^\times$ ist eine diskrete und abgeschlossene Untergruppe von $\mathcal{I}_k$ unter der diagonalen Einbettung $a \mapsto (a)_{\mathfrak{p}}$.*

Somit ist die durch

$$\mathcal{C}_K = \mathcal{I}_K / K^\times$$

definierte *Idelklassengruppe* eine lokal kompakte Hausdorffsche abelsche Gruppe. Da die diagonale Einbettung $K^\times \hookrightarrow \mathcal{I}_K$ für eine endliche galoissche Erweiterung $K|k$ ein $G(K|k)$-Homomorphismus ist, erhalten wir auch auf $\mathcal{C}_K$ eine $G(K|k)$-Modulstruktur, die wie die Idelgruppe einen guten Galois-Abstieg hat, d.h.

$$\mathcal{C}_k = \mathcal{C}_K^{G(K|k)},$$

was aus der exakten Sequenz $0 \to k^\times \to \mathcal{I}_k \to \mathcal{C}_K^{G(K|k)} \to H^1(G(K|k), K^\times)$ zusammen mit Hilberts Satz 90 folgt.

Wir definieren die *Absolutnorm* eines Idels $\mathfrak{a} \in \mathcal{I}_k$ durch

$$\mathcal{N}(\mathfrak{a}) := \prod_{\mathfrak{p}} |\mathfrak{a}_{\mathfrak{p}}|_{\mathfrak{p}}.$$

Wegen der Geschlossenheitsrelation ist $\mathcal{N}(a) = 1$ für $a \in k^\times$. Somit wird auch eine Absolutnorm auf der Idelklassengruppe $\mathcal{C}_k$ induziert. Mit $\mathcal{C}_k^0$ bezeichnen wir den Kern der Absolutnorm auf $\mathcal{C}_k$. Als fundamental wird sich die Kompaktheit der Gruppe $\mathcal{C}_k^0$ erweisen ([N-ZT], Theorem VI.1.6).

Den lokal kompakten, Hausdorffschen $G(K|k)$-Modul

$$\mathcal{C}_S(K) = \mathcal{I}_K / K^\times \mathcal{U}_{K,S},$$

wobei die kompakte Gruppe $\mathcal{U}_{K,S}$ durch $\prod_{p\in S}\{1\} \times \prod_{p\notin S} \mathcal{U}_{\mathfrak{p}}^{(0)}$ gegeben sei, nennen wir die S-*Idelklassengruppe.* Falls $K|k$ außerhalb von S unverzweigt ist, ist der Modul $U_{K,S}$ kohomologisch trivial, was aus dem lokalen Resultat für unverzweigte Primstellen $\mathfrak{p}$ von k folgt (vgl. [N-KKT], Satz II.4.3), und daraus, daß wir die Erweiterung $\mathbb{C}|\mathbb{R}$ als verzweigt ansehen. In dieser Situation hat der Modul $\mathcal{C}_S(K)$ guten Galois-Abstieg, da die Sequenz $0 \to \mathcal{U}_{k,S} \to \mathcal{I}_k \to (\mathcal{C}_S(K))^{G(K|k)} \to 0$ exakt ist.

Unter der *Idelklassengruppe modulo* $\mathfrak{m}$ wollen wir den ebenfalls lokal kompakten und Hausdorffschen $G(K|k)$-Modul

$$\mathcal{C}_K^{\mathfrak{m}} = \mathcal{I}_K^{\mathfrak{m}} K^\times / K^\times = \mathcal{I}_K^{\mathfrak{m}} / \mathcal{O}_{K,\mathfrak{m}}^\times$$

verstehen.

Es sei $\mathcal{P}_K$ die Gruppe der Hauptideale von $\mathcal{O}_K$ und weiter

$$\mathcal{P}_K^{\mathfrak{m}} := \{(a) \in \mathcal{J}_K^{\mathfrak{m}} \mid a \in \mathcal{O}_K^\times \text{ und } a \in \mathcal{U}_{\mathfrak{p}}^{(n_\mathfrak{p})} \text{ für } \mathfrak{p} \mid \mathfrak{m}\}$$

und

$$\mathcal{P}_K^S := \{(a) \in \mathcal{J}_K^S \mid a \in K^\times\}.$$

Von Interesse für uns sind neben der gewöhnlichen *Idealklassengruppe*

$$\mathcal{C}l_K = \mathcal{J}_K / \mathcal{P}_K$$

auch die durch

$$\mathcal{C}l_K^{\mathfrak{m}} = \mathcal{J}_K^{\mathfrak{m}} / \mathcal{P}_K^{\mathfrak{m}} \quad \text{bzw.} \quad \mathcal{C}l_S(K) = \mathcal{J}_K^S / \mathcal{P}_K^S$$

definierte *Idealklassengruppe modulo* $\mathfrak{m}$ bzw. die *S-Idealklassengruppe.*

Wir betrachten den Epimorphismus $\mathcal{J}_K \twoheadrightarrow \mathcal{J}_K^S$, $\mathfrak{a} \mapsto \mathcal{O}_{K,S}\mathfrak{a}$, welcher den Epimorphismus $\mathcal{J}_K \twoheadrightarrow \mathcal{J}_K^S/\mathcal{P}_K^S = \mathcal{C}l_S(K)$ induziert. $\mathcal{P}_K$ liegt im Kern dieses Homomorphismus, so daß $\mathcal{C}l_S(K)$ ein Faktor von $\mathcal{C}l_K$ und somit endlich ist.

Die Gruppe $\mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}}$ heißt *Strahlklassengruppe modulo* $\mathfrak{m}$. Im folgenden wollen wir sie idealtheoretisch beschreiben und ihre Endlichkeit ableiten. Dazu betrachten wir die Gruppe

$$\mathcal{I}_K^{(\mathfrak{m})} = \{\mathfrak{a} \in \mathcal{I}_K \mid \mathfrak{a}_\mathfrak{p} \in \mathcal{U}_\mathfrak{p}^{(n_\mathfrak{p})} \text{ für } \mathfrak{p} \mid \mathfrak{m}\}.$$

Aus dem Approximationssatz folgt, daß $\mathcal{I}_K = \mathcal{I}_K^{(\mathfrak{m})} K^\times$ ist. Der Homomorphismus

$$\chi : \mathcal{I}_K^{(\mathfrak{m})} \to \mathcal{J}_K^{\mathfrak{m}},\ \mathfrak{a} \mapsto \prod_{\mathfrak{p}\nmid\infty,\, \mathfrak{p}\nmid\mathfrak{m}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})}$$

ist mit dem vorher definierten χ verträglich in dem Sinne, daß dieser sich aus $a \mapsto (a)$ für $a \in K^\times$ und obigem χ zusammensetzt.

Wir betrachten die Surjektion

$$\overline{\chi} : \mathcal{I}_K^{(\mathfrak{m})} \twoheadrightarrow \mathcal{J}_K^{\mathfrak{m}} / \mathcal{P}_K^{\mathfrak{m}}.$$

Sei $\mathfrak{a} \in \mathcal{I}_K^{(\mathfrak{m})}$ im Kern von $\overline{\chi}$. Dann gibt es ein $(x) \in \mathcal{P}_K^{\mathfrak{m}}$, d.h. $x \in \mathcal{U}_\mathfrak{p}^{(n_\mathfrak{p})}$ für $\mathfrak{p} \mid \mathfrak{m}$, mit $(x) = \chi(\mathfrak{a})$. Dann ist $\mathfrak{a}_\mathfrak{p} x^{-1}$ ein Element von $\mathcal{U}_\mathfrak{p}^{(0)}$ für $\mathfrak{p} \nmid \mathfrak{m}$ und von $\mathcal{U}_\mathfrak{p}^{(n_\mathfrak{p})}$, falls $\mathfrak{p}$ den Modul $\mathfrak{m}$ teilt. Daher gilt

$$ker(\overline{\chi}) = \mathcal{I}_K^{(\mathfrak{m})} \cap \mathcal{I}_K^{\mathfrak{m}} K^\times.$$

Also erhalten wir

$$\mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}} \cong \mathcal{I}_K/\mathcal{I}_K^{\mathfrak{m}} K^\times \cong \mathcal{I}_K^{(\mathfrak{m})} K^\times / \mathcal{I}_K^{\mathfrak{m}} K^\times \cong \mathcal{I}_K^{(\mathfrak{m})} / (\mathcal{I}_K^{(\mathfrak{m})} \cap \mathcal{I}_K^{\mathfrak{m}} K^\times) \cong \mathcal{J}_K^{\mathfrak{m}} / \mathcal{P}_K^{\mathfrak{m}}.$$

Es sei $\mathfrak{m}_f$ der endliche Anteil des Moduls $\mathfrak{m}$ aufgefaßt als Ideal von $\mathcal{O}_K$. Nach dem chinesischen Restsatz gilt die Isomorphie

$$\mathcal{O}_K/\mathfrak{m}_f \cong \prod_{\mathfrak{p}|\mathfrak{m}_f} \mathcal{O}_K/\mathfrak{p}^{v_\mathfrak{p}(n_\mathfrak{p})}.$$

Aus dem Isomorphismus $(\mathcal{O}_K/\mathfrak{p}^s)^\times \cong \mathcal{U}_\mathfrak{p}/\mathcal{U}_\mathfrak{p}^{(s)}$, $a + \mathfrak{p}^s \mapsto a\mathcal{U}_\mathfrak{p}^{(s)}$ erhalten wir $(\mathcal{O}_K/\mathfrak{m}_f)^\times \cong \prod_{\mathfrak{p}|\mathfrak{m}_f} \mathcal{U}_\mathfrak{p}/\mathcal{U}_\mathfrak{p}^{(n_\mathfrak{p})} \cong \mathcal{I}_{S_\infty}(K)/\mathcal{I}_K^{\mathfrak{m}_f}$. Hieraus leiten wir die Isomorphie

$$\mathcal{I}_{S_\infty}(K)/\mathcal{I}_K^{\mathfrak{m}} \cong \prod_{\mathfrak{p}|\mathfrak{m}_f} \mathcal{U}_\mathfrak{p}/\mathcal{U}_\mathfrak{p}^{(n_\mathfrak{p})} \times \prod_{\mathfrak{p}|\mathfrak{m},\ \mathfrak{p} \text{ reell},\ n_\mathfrak{p}=1} \mathbb{R}^\times/\mathbb{R}_+^\times$$

ab, aus der wir die Endlichkeit von $\mathcal{I}_{S_\infty}(K)/\mathcal{I}_K^{\mathfrak{m}}$ unter Benutzung der Endlichkeit von $\mathcal{O}_K/\mathfrak{p}^{v_\mathfrak{p}(n_\mathfrak{p})}$ erhalten. Betrachten wir nun die exakte Sequenz

$$\mathcal{I}_{S_\infty}(K)K^\times/\mathcal{I}_K^{\mathfrak{m}}K^\times \to \mathcal{I}_K/\mathcal{I}_K^{\mathfrak{m}}K^\times \to \mathcal{I}_K/\mathcal{I}_{S_\infty}(K)K^\times \to 0,$$

so erhalten wir die Endlichkeit von $\mathcal{I}_K/\mathcal{I}_K^{\mathfrak{m}}K^\times \cong \mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}}$, denn $\mathcal{I}_K/\mathcal{I}_{S_\infty}(K)K^\times$ ist isomorph zur Idealklassengruppe Cl_K, und $\mathcal{I}_{S_\infty}(K)K^\times/\mathcal{I}_K^{\mathfrak{m}}K^\times = \mathcal{I}_{S_\infty}(K)/\mathcal{I}_K^{\mathfrak{m}}(K^\times \cap \mathcal{I}_{S_\infty}(K))$ ist ein Faktor von $\mathcal{I}_{S_\infty}(K)/\mathcal{I}_K^{\mathfrak{m}}$. Wir halten fest:

(1.2.7) Satz. *Die Strahlklassengruppe modulo* $\mathfrak{m}$ *ist endlich, und wir haben via* χ *die Isomorphie*

$$\mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}} \cong \mathcal{J}_K^{\mathfrak{m}}/\mathcal{P}_K^{\mathfrak{m}}.$$

1.2.2. Zwei exakte Sequenzen

In diesem Kapitel werden wir zwei exakte Sequenzen herleiten, auf denen die folgenden Dualitätssätze beruhen.

Wir starten zunächst mit einem

(1.2.8) Lemma. *Sei* $0 \to A \to B \xrightarrow{\phi} C \to 0$ *eine exakte Sequenz von abelschen topologischen Gruppen (bzw. G-Moduln), in der alle Homomorphismen stetig sind. Es seien ferner zwei abgeschlossene Untergruppen (bzw. -moduln)* $M \subseteq B$ *und* $D \subseteq C$ *gegeben, so daß* $\phi(M) \subseteq D$ *ist. Dann gilt:*

(a) Die Sequenz

$$0 \to \phi^{-1}(D)/M \to B/M \xrightarrow{\phi} C/D \to 0$$

ist exakt mit stetigen Homomorphismen.

(b) Ist zusätzlich $\phi(M) = D$*, so ist die Sequenz*

$$0 \to A/A \cap M \to B/M \xrightarrow{\phi} C/D \to 0$$

exakt mit stetigen Homomorphismen.

Beweis. $\phi^{-1}(D) \leq B$ ist ein abgeschlossener Untermodul. Die Stetigkeit der Abbildungen in (a) und (b) ist klar. Wegen $C \cong B/A$ gilt $D \cong \phi^{-1}(D)/A$. Daher folgt

$$C/D \cong (B/A)/(\phi^{-1}(D)/A) \cong B/\phi^{-1}(D),$$

weshalb die Sequenz in (a) exakt ist.

Zu (b) genügt es zu zeigen, daß $\phi^{-1}(D) = AM$ (multiplikativ geschrieben) gilt. Dies überprüft man sofort. □

Als erstes wenden wir uns der *S-Theorie* zu. Sei S also eine Menge von Primstellen des Zahlkörpers K. Wir halten zunächst fest:

(1.2.9) Lemma. *Die Sequenz* $0 \to \mathcal{I}_S(K) \to \mathcal{I}_K \xrightarrow{\chi} \mathcal{J}_K^S \to 0$ *ist exakt, und die Homomorphismen sind stetig, wobei* $\mathcal{J}_K^S$ *mit der Quotiententopologie versehen sei.*

Wir definieren

$$\mathcal{I}_{K,S} := \prod_{\mathfrak{p}\in S}(K_\mathfrak{p}^\times, \mathcal{U}_\mathfrak{p}^{(0)}).$$

Dies hat umittelbar die Exaktheit der Sequenz

$$0 \to \mathcal{U}_{K,S} \to \mathcal{I}_S(K) \xrightarrow{\text{proj}} \mathcal{I}_{K,S} \to 0 \tag{4}$$

zur Folge. Weiter definieren wir $\mathcal{C}_{K,S}$ durch die exakte Sequenz

$$0 \to \mathcal{O}_{K,S}^\times \to \mathcal{I}_{K,S} \to \mathcal{C}_{K,S} \to 0. \tag{5}$$

Als Anwendung von Lemma (1.2.8) erhalten wir zunächst das

(1.2.10) Lemma. *Folgende Sequenzen sind exakt, und die Homomorphismen sind stetige Abbildungen:*

(a) $0 \to K^\times\mathcal{I}_S(K) \to \mathcal{I}_K \to \mathcal{C}l_S(K) \to 0$

(b) $0 \to \mathcal{I}_S(K)/\mathcal{O}_{K,S}^\times \to \mathcal{C}_K \to \mathcal{C}l_S(K) \to 0$

(c) $0 \to \mathcal{C}_{K,S} \to \mathcal{C}_S(K) \to \mathcal{C}l_S(K) \to 0$

Beweis. Wir gehen aus von der exakten Sequenz $0 \to \mathcal{I}_S(K) \to \mathcal{I}_K \xrightarrow{\chi} \mathcal{J}_K^S \to 0$ aus vorigem Lemma (1.2.9).

Für (a) wählen wir die Untergruppen $\mathcal{P}_K^S \leq \mathcal{J}_K^S$ und $K^\times\mathcal{I}_S(K) \leq \mathcal{I}_K$, für die $\chi(K^\times\mathcal{I}_S(K)) = \mathcal{P}_K^S$ gilt. Lemma (1.2.8) liefert nun die Aussage.

Für (b) wählen wir $\mathcal{P}_K^S \leq \mathcal{J}_K^S$ und $K^\times \leq \mathcal{I}_K$. Es gilt: $\chi(K^\times) = \mathcal{P}_K^S$, woraus die Aussage folgt.

Für (c) wählen wir wiederum $\mathcal{P}_K^S \leq \mathcal{J}_K^S$, aber nun $K^\times\mathcal{U}_{K,S} \leq \mathcal{I}_K$. Es gilt $\chi(K^\times\mathcal{U}_{K,S}) = \mathcal{P}_K^S$. Aus Lemma (1.2.8) erhalten wir die exakte Sequenz

$$0 \to \mathcal{I}_S(K)/(\mathcal{I}_S(K) \cap K^\times\mathcal{U}_{K,S}) \to \mathcal{C}_S(K) \to \mathcal{C}l_S(K) \to 0.$$

Mittels (4) sehen wir, daß der Kern von *proj* : $\mathcal{I}_S(K) \to \mathcal{C}_{K,S} \cong \mathcal{I}_{K,S}/\mathcal{O}_{K,S}^\times$ gegeben ist durch $\mathcal{U}_{K,S}\mathcal{O}_{K,S}^\times \cong \mathcal{U}_{K,S}(K^\times \cap \mathcal{I}_S(K)) \cong K^\times\mathcal{U}_{K,S} \cap \mathcal{I}_S(K)$. Also gilt $\mathcal{C}_{K,S} \cong \mathcal{I}_S(K)/(\mathcal{I}_S(K) \cap K^\times\mathcal{U}_{K,S})$, womit alles bewiesen ist. □

Aus (b) und durch Zusammensetzen von (5) mit Teil (c) erhalten wir den

(1.2.11) Satz. *Sei S eine Menge von Primstellen. Dann sind die Sequenzen*

$$0 \to \mathcal{O}_{K,S}^\times \to \mathcal{I}_S(K) \to \mathcal{C}_K \to \mathcal{C}l_S(K) \to 0$$

und

$$0 \to \mathcal{O}_{K,S}^\times \to \mathcal{I}_{K,S} \to \mathcal{C}_S(K) \to \mathcal{C}l_S(K) \to 0$$

exakt mit stetigen Homomorphismen.

Nun wollen wir ein analoges Ergebnis für die $\mathfrak{m}$-*Theorie* entwickeln. Sei dazu $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}$ ein Modul. Ihm ordnen wir die endliche Menge S der Primstellen zu, die in $\mathfrak{m}$ aufgehen. Wir definieren die lokal kompakte, Hausdorffsche, abelsche Gruppe

$$\mathcal{I}_{K,\mathfrak{m}} := \prod_{\mathfrak{p}|\mathfrak{m}} \mathcal{U}_\mathfrak{p}^{(n_\mathfrak{p})}.$$

Es ergibt sich wieder die exakte Sequenz

$$0 \to \mathcal{U}_{K,S} \to \mathcal{I}_K^{\mathfrak{m}} \xrightarrow{proj} \mathcal{I}_{K,\mathfrak{m}} \to 0. \tag{6}$$

Weiterhin definieren wir analog zu Vorherigem die Gruppe $\mathcal{C}_{K,\mathfrak{m}}$ durch die Exaktheit der Sequenz

$$0 \to \mathcal{O}_{K,\mathfrak{m}}^\times \to \mathcal{I}_{K,\mathfrak{m}} \to \mathcal{C}_{K,\mathfrak{m}} \to 0. \tag{7}$$

(1.2.12) Lemma. *Die Sequenz*

$$0 \to \mathcal{I}_K^{\mathfrak{m}}/\mathcal{O}_{K,\mathfrak{m}}^\times \to \mathcal{C}_K \to \mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}} \to 0$$

ist exakt mit stetigen Homomorphismen.

Beweis. Per Definition haben wir die exakte Sequenz

$$0 \to K^\times \mathcal{I}_K^{\mathfrak{m}} \to \mathcal{I}_K \to \mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}} \to 0.$$

Faktorisieren wir aus den ersten beiden Gliedern $K^\times$ heraus, so erhalten wir das Ergebnis unter Beachtung von $K^\times \mathcal{I}_K^{\mathfrak{m}}/K^\times \cong \mathcal{I}_K^{\mathfrak{m}}/\mathcal{I}_K^{\mathfrak{m}} \cap K^\times \cong \mathcal{I}_K^{\mathfrak{m}}/\mathcal{O}_{K,\mathfrak{m}}^\times$. □

Die zu Satz (1.2.11) analogen exakten Sequenzen sind die folgenden:

(1.2.13) Satz. *Sei $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ ein Modul und S die endliche Menge der in $\mathfrak{m}$ aufgehenden Primstellen. Dann sind die Sequenzen*

$$0 \to \mathcal{O}_{K,\mathfrak{m}}^\times \to \mathcal{I}_K^{\mathfrak{m}} \to \mathcal{C}_K \to \mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}} \to 0$$

und

$$0 \to \mathcal{O}_{K,\mathfrak{m}}^\times \to \mathcal{I}_{K,\mathfrak{m}} \to \mathcal{C}_S(K) \to \mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}} \to 0$$

exakt mit stetigen Homomorphismen.

Beweis. Die Exaktheit der ersten Sequenz folgt unmittelbar aus Lemma (1.2.12).
Die Inklusion $K^\times \mathcal{U}_{K,S} \subseteq K^\times \mathcal{I}_K^{\mathfrak{m}}$ liefert die exakte Sequenz

$$0 \to K^\times \mathcal{I}_K^{\mathfrak{m}}/K^\times \mathcal{U}_{K,S} \to \mathcal{I}_K/K^\times \mathcal{U}_{K,S} = \mathcal{C}_S(K) \to \mathcal{I}_K/K^\times \mathcal{I}_K^{\mathfrak{m}} = \mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}} \to 0.$$

Analog wie in Lemma (1.2.10) betrachten wir die natürliche Abbildung $\mathcal{I}_K^{\mathfrak{m}} \xrightarrow{\text{proj}} \mathcal{I}_{K,\mathfrak{m}}/\mathcal{O}_{K,\mathfrak{m}}^\times$, die aufgrund von (6) den Kern $\mathcal{U}_{K,S}\mathcal{O}_{K,\mathfrak{m}}^\times = \mathcal{U}_{K,S}(\mathcal{I}_K^{\mathfrak{m}} \cap K^\times) = \mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{U}_{K,S}K^\times$ hat. Damit erhalten wir die Isomorphie $K^\times \mathcal{I}_K^{\mathfrak{m}}/K^\times \mathcal{U}_{K,S} \cong \mathcal{I}_K^{\mathfrak{m}}/(\mathcal{I}_K^{\mathfrak{m}} \cap \mathcal{U}_{K,S}K^\times) \cong \mathcal{I}_{K,\mathfrak{m}}/\mathcal{O}_{K,\mathfrak{m}}^\times \cong \mathcal{C}_{K,\mathfrak{m}}$. Die zweite Sequenz folgt nun mittels Zusammensetzen von (7) mit der gerade erhaltenen Sequenz. □

1.2.3. Allgemeine globale Klassenkörpertheorie

Sei k ein algebraischer Zahlkörper und $K|k$ eine endliche galoissche Erweiterung. Die lokale Klassenkörpertheorie (vgl. etwa [N-KKT], Kapitel II) liefert für endliche Primstellen $\mathfrak{p}$ von k *Invariantenabbildungen*

$$\mathrm{inv}_{K_{\mathfrak{p}}|k_{\mathfrak{p}}} : H^2(G(K_{\mathfrak{p}}|k_{\mathfrak{p}}), K_{\mathfrak{p}}^\times) \xrightarrow{\sim} \frac{1}{[K_{\mathfrak{p}} : k_{\mathfrak{p}}]}\mathbb{Z}/\mathbb{Z}.$$

Für unendliche Primstellen ist nur der Fall $K_{\mathfrak{p}} = \mathbb{C}$ und $k_{\mathfrak{p}} = \mathbb{R}$ von Relevanz. Für ihn definieren wir

$$\mathrm{inv}_{\mathbb{C}|\mathbb{R}} : H^2(G(\mathbb{C}|\mathbb{R}), \mathbb{C}^\times) \cong \hat{H}^0(G(\mathbb{C}|\mathbb{R}), \mathbb{C}^\times) \cong \mathbb{R}/\mathbb{R}_+ \xrightarrow{\sim} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$

durch das Vorzeichen. Aufgrund von Satz (1.2.3) können wir nun einen Homomorphismus

$$\mathrm{inv}_{K|k} : H^2(G(K|k), \mathcal{I}_K) \to \frac{1}{[K : k]}\mathbb{Z}/\mathbb{Z}$$

durch die (endliche) Summe der Invariantenabbildungen seiner Komponenten definieren. Ein fundamentales Ergebnis (vgl. [N-KKT], Satz III.5.5) besagt

$$c \in H^2(G(K|k), K^\times) \;\Rightarrow\; \mathrm{inv}_{K|k} c = 0,$$

womit der Homomorphismus

$$\mathrm{inv}_{K|k} : H^2(G(K|k), \mathcal{C}_K) \to \frac{1}{[K:k]}\mathbb{Z}/\mathbb{Z}$$

wohldefiniert ist. Auch diesen Homomorphismus nennen wir *Invariantenabbildung.*

Nun können wir das folgende Theorem formulieren, für dessen Beweis wir auf [NSW], Theorem 8.1.22, bzw. auf [N-KKT], Satz III.6.9, verweisen.

(1.2.14) Theorem. *Sei k ein algebraischer Zahlkörper und $\overline{k}$ ein algebraischer Abschluß. $\mathcal{C} = \varinjlim_{K|k} \mathcal{C}_K$ sei die Idelklassengruppe und $G = G(\overline{k}|k)$ die Galoisgruppe. Dann ist $(G, \mathcal{C})$ eine Klassenformation.*

Mittels der abstrakten Theorie erhalten wir aus Satz (1.1.30) den *Hauptsatz der globalen Klassenkörpertheorie.*

(1.2.15) Theorem. *Für endliche Erweiterungen $L|K|k$, wobei $L|K$ galoissch sei, gibt es einen* Reziprozitätshomomorphismus $(\cdot, L|K)$*, so daß die Sequenz*

$$0 \longrightarrow N_{L|K}\mathcal{C}_L \longrightarrow \mathcal{C}_K \xrightarrow{(\cdot,L|K)} G(L|K)^{ab} \longrightarrow 0$$

exakt ist. Ferner übertragen sich die kommutativen Diagramme aus Satz (1.1.31) sinngemäß.

Aus Satz (1.1.32) überträgt sich der Begriff der Normengruppe. Dies sind genau die Untergruppen von $\mathcal{C}_K$ der Form $N_{L|K}\mathcal{C}_L$. Ferner gibt es einen inklusionsumkehrenden Verbandsisomorphismus

$$L \mapsto N_{L|K}\mathcal{C}_L$$

zwischen den endlichen, galoisschen und abelschen Oberkörpern von K und den Normengruppen.

Für diese gilt der wichtige *Existenzsatz* (siehe [N-KKT], Satz III.7.8):

(1.2.16) Satz. *Die Normengruppen von $\mathcal{C}_K$ sind gerade die offenen Untergruppen von endlichem Index von $\mathcal{C}_K$.*

1.2.4. Beschränkte Verzweigung und volle Zerlegung

Allgemeines

Wir wollen nun einige Vorbereitungen zur genaueren Analyse von Körpererweiterungen mittels Idelklassen treffen. Dazu betrachten wir zunächst den Sachverhalt im Lokalen.

(1.2.17) Satz. *Sei $L|K$ eine endliche, galoissche und abelsche Erweiterung p-adischer Zahlkörper. Dann bildet das lokale Normrestsymbol $(\cdot, L|K)$*

(a) die Einheitengruppe $\mathcal{U}_K$ surjektiv auf die Trägheitsgruppe $G_0(L|K)$ ab,

(b) die Einseinheitengruppe $\mathcal{U}_K^{(1)}$ surjektiv auf die Verzweigungsgruppe $G_1(L|K)$ ab,

(c) die n-te Einseinheitengruppe $\mathcal{U}_K^{(n)}$ für $n > 0$ surjektiv auf die n-te Verzweigungsgruppe in oberer Numerierung $G^n(L|K)$ ab.

Beweis. Der Teil (c) wird für die Hauptsätze dieser Arbeit keine Anwendung finden, und sein Beweis ist nicht so elementar wie der der beiden anderen Fälle. Wir begnügen uns daher mit einem Verweis auf [Se-LF], chapter XV, Theorem 2. Der Beweis der anderen Fälle ist an [N-KKT] angelehnt.

(a) Sei T der Trägheitskörper der Erweiterung $L|K$, die vom Grad $n = e \cdot f$ mit Verzweigungindex e sei. Die Galois-Gruppe $G(L|T)$ ist gerade die Trägheitsgruppe $G_0(L|K)$, und die Erweiterung $T|K$ ist unverzweigt vom Grad f. In diesem Fall wird das lokale Normrestsymbol durch den Frobeniusautomorphismus beschrieben: $(a, T|K) = \varphi_{T|K}^{v_K(a)}$ (vgl. [N-KKT], Kapitel II.4). Sei $u \in \mathcal{U}_K$ und $\pi : G(L|K)^{ab} \to G(T|K)^{ab}$ die natürliche Abbildung. Dann ist $\pi((u, L|K)) = (u, L|K)G_0(L|K) = (u, T|K) = \varphi_{T|K}^{v_K(u)} = 1$, damit gilt also $(u, L|K) \in G_0(L|K)$.

Betrachten wir nun $\tau \in G_0(L|K)$ mit $(a, L|K) = \tau$ für ein $a \in K^\times$. Das impliziert $(a, T|K) = \varphi_{T|K}^{v_K(a)} = 1$, also ist $v_K(a)$ durch f teilbar, und wir können ein $b \in L^\times$ mit $v_K(a) = f v_L(b)$ wählen. Es ist $e \cdot v_K(N_{L|K} b) = v_L(N_{L|K} b) = n \cdot v_L(b) = e \cdot v_K(a)$ und somit $v_K(a) = v_K(N_{L|K} b)$. Daher finden wir ein $u \in U_K$ mit $a = u \cdot N_{L|K} b$. Somit ist $(a, L|K) = (u, L|K) = \tau$, und die gesamte Trägheitsgruppe wird getroffen.

(b) Da die Normengruppen aufgrund der Endlichkeit der Galois-Gruppe offene Untergruppen von $K^\times$ sind, und die $\mathcal{U}_K^{(n)}$ eine Umgebungsbasis der 1 bilden, muß es ein n geben, so daß $(\mathcal{U}_K^{(n)}, L|K) = 1$ ist. Die Verzweigungsgruppe $G_1(L|K)$ ist charakterisiert als die einzige p-Sylowgruppe von $G_0(L|K)$. Daher ist sie das Bild der p-Sylowgruppe $\mathcal{U}_K^{(1)}/\mathcal{U}_K^{(n)}$ von $\mathcal{U}_K/\mathcal{U}_K^{(n)}$ unter dem Normrestsymbol (man beachte, daß alle Faktorgruppen $\mathcal{U}_K^{(i)}/\mathcal{U}_K^{(i+1)}$ für $i \geq 1$ isomorph zur additiven und $\mathcal{U}_K/\mathcal{U}_K^{(1)}$ isomorph zur multiplikativen Gruppe des Restklassenkörpers von K sind). □

Wir verwenden den folgenden Satz (vgl. [N-KKT], Satz III.8.2) für den Übergang vom Lokalen zum Globalen:

(1.2.18) Satz. *Sei $K|k$ eine endliche, galoissche und abelsche Erweiterung von Zahlkörpern. Mittels der natürlichen Abbildung $k_\mathfrak{p} \to \mathcal{C}_k$ gilt:*

$$N_{K|k}\mathcal{C}_K \cap k_\mathfrak{p}^\times = N_{K_\mathfrak{P}|k_\mathfrak{p}} K_\mathfrak{P}^\times$$

Beweis. Die Inklusion $\supseteq$ ist klar. Für die andere betrachten wir eine Idelklasse

$$\bar{\mathfrak{a}} = \overline{(\dots, 1, x_\mathfrak{p}, 1, \dots)} \in \mathcal{C}_K$$

mit $x_\mathfrak{p} \in k_\mathfrak{p}^\times$. Diese kommt per Voraussetzung von einem Normidel her:

$$N_{K|k}\mathfrak{b} = (\dots, 1, x_\mathfrak{p}, 1, \dots)a,$$

wobei a in $k^\times$ liege. Damit ist a Normenelement für alle von $\mathfrak{p}$ verschiedenen Primstellen. Aus der Produktformel entnehmen wir, daß a auch für $\mathfrak{p}$ Normenelement sein muß, weshalb dies auch für $x_\mathfrak{p}$ gilt. □

Fundamental für das Folgende ist der

(1.2.19) Satz. *Sei $K|k$ eine endliche, galoissche und abelsche Erweiterung von Zahlkörpern, und sei $\mathfrak{p}$ eine (endliche oder unendliche) Primstelle von k. Dann gilt:*

(a) $\mathfrak{p}$ ist voll zerlegt in K $\Leftrightarrow$ $k_\mathfrak{p}^\times \subseteq N_{K|k}\mathcal{C}_K$.

(b) $\mathfrak{p}$ ist unverzweigt in K $\Leftrightarrow$ $\mathcal{U}_{k_\mathfrak{p}}^{(0)} \subseteq N_{K|k}\mathcal{C}_K$.

(c) $\mathfrak{p}$ ist zahm verzweigt in K $\Leftrightarrow$ $\mathcal{U}_{k_\mathfrak{p}}^{(1)} \subseteq N_{K|k}\mathcal{C}_K$.

(d) *Sei* $\mathfrak{p}$ *eine endliche Stelle und* $G^n(K_\mathfrak{p}|k_\mathfrak{p})$ *die* n*-te Verzweigungsgruppe in oberer Numerierung. Es ist dann:*

$$G^n(K_\mathfrak{p}|k_\mathfrak{p}) = 1 \quad \Leftrightarrow \quad \mathcal{U}_{k_\mathfrak{p}}^{(n)} \subseteq N_{K|k}\mathcal{C}_K.$$

Dabei heiße eine unendliche Stelle unverzweigt bzw. gleichbedeutend damit voll zerlegt genau dann, wenn $k_\mathfrak{p} = K_\mathfrak{p}$ *ist. Insbesondere fassen wir* $\mathbb{C}|\mathbb{R}$ *als verzweigt auf.*

Beweis. Dies überträgt sich mittels des Satzes (1.2.18) direkt aus dem Lokalen (Satz (1.2.17)). □

In S voll zerlegter Fall

Nun wenden wir uns dem Fall von Erweiterungen zu, die in einer Primstellenmenge S voll zerlegt sind.

(1.2.20) Lemma. *Sei* k *ein algebraischer Zahlkörper,* $K|k$ *eine endliche, galoissche und unverzweigte Erweiterung, die in der Primstellenmenge* S *von* k *voll zerlegt ist. Dann gilt:*

$$\mathcal{I}_S(k)/\mathcal{O}_{k,S}^\times = \mathcal{I}_S(k)k^\times/k^\times \subseteq N_{K|k}\mathcal{C}_K.$$

Beweis. Dies ist eine unmittelbare Konsequenz von Satz (1.2.19) (a). □

(1.2.21) Satz. *Sei* $L_S^{ab} \subseteq \overline{k}$ *die maximale abelsche unverzweigte und in* S *voll zerlegte Erweiterung des Zahlkörpers* k*. Dann gilt:*

$$G(L_S^{ab}|k) \cong \mathcal{C}l_S(k).$$

Beweis. Aufgrund von Lemma (1.2.10) (b) ist $\mathcal{I}_S(k)/\mathcal{O}_{k,S}^\times$ eine offene Untergruppe von $\mathcal{C}_k$ und somit eine Normengruppe, etwa zum Körper K. Dieser hat aber wegen des Lemmas (1.2.20) die gewünschten Eigenschaften, also ist K gleich L_S^{ab}. □

Wir wollen auch Aussagen über maximale galoissche p-Erweiterungen machen. Wir bemerken, daß Lemma (1.1.35) für eine beliebige galoissche Erweiterung $L|k$ bedeutet, daß die maximale galoissche p-Erweiterung innerhalb der maximalen abelschen Teilerweiterung von $L|k$ das gleiche ist, wie die maximale abelsche Erweiterung innerhalb der maximalen galoisschen p-Teilerweiterung von $L|k$.

Wir nennen $L_S^{ab}(p)$ die maximale abelsche unverzweigte p-Erweiterung von k, die in S voll zerlegt ist. Es folgt das

(1.2.22) Korollar. $G(L_S^{ab}(p)|k) \cong \mathcal{C}l_S(k)(p)$*.*

Beschränkte Verzweigung

Nun wenden wir uns der Theorie der beschränkten Verzweigung zu. Dafür haben wir zunächst den wichtigen

(1.2.23) Satz. *Sei* k *ein algebraischer Zahlkörper. Die Normengruppen von* $\mathcal{C}_k$ *sind gerade die Obergruppen der Kongruenzuntergruppen* $\mathcal{C}_k^\mathfrak{m}$*.*

Beweis. $\mathcal{C}_k^\mathfrak{m} \leq \mathcal{C}_k$ ist wegen Satz (1.2.7) offen, also eine Normengruppe. Damit sind auch alle Obergruppen Normengruppen.

Umgekehrt sei I eine Normengruppe, also eine offene Untergruppe von $\mathcal{C}_k$. Die höheren Einseinheiten definieren eine Umgebungsbasis der 1 in den lokalen Körpern $k_\mathfrak{p}$. Damit ist die Gruppe

$$(\prod_{p|\infty} k_\mathfrak{p}^\times \times \prod_{p\in S} \mathcal{U}_\mathfrak{p}^{(n_\mathfrak{p})} \times \prod_{p\notin S} \mathcal{U}_\mathfrak{p}^{(0)})k^\times/k^\times$$

für geeignetes endliches S, das die unendlichen Stellen nicht enthalte, eine Teilmenge von I. I ist also Obergruppe von $\mathcal{C}_K^{\mathfrak{m}}$ mit dem entsprechend definierten Modul $\mathfrak{m}$. $\square$

Der Satz besagt also, daß jede endliche galoissche und abelsche Erweiterung $K|k$ in einem *Strahlklassenkörper* $k^{\mathfrak{m}}$ enthalten ist. Dies seien die zu $\mathcal{C}_k^{\mathfrak{m}}$ gehörigen Körper. Damit sind die Galois-Gruppen dieser Erweiterungen gerade die Strahlklassengruppen:

$$G(k^{\mathfrak{m}}|k) \cong \mathcal{C}_k/\mathcal{C}_k^{\mathfrak{m}}$$

Als Konsequenz aus Satz (1.2.19) (c) erhalten wir den

(1.2.24) Satz. *Sei k ein Zahlkörper mit algebraischem Abschluß $\overline{k}$ und S eine endliche Menge von Primstellen von k. Setze $\mathfrak{m} = \prod_{\mathfrak{p}\in S} \mathfrak{p}$. Dann ist der Strahlklassenkörper $k^{\mathfrak{m}}$ die maximale abelsche, außerhalb S unverzweigte und innerhalb S zahm verzweigte galoissche Erweiterung von k mit endlicher abelscher Galois-Gruppe*

$$G(k^{\mathfrak{m}}|k) \cong \mathcal{C}_k/\mathcal{C}_k^{\mathfrak{m}}.$$

Mit $k^{\mathfrak{m}}(p)$ bezeichnen wir die maximale in $k^{\mathfrak{m}}$ enthaltene galoissche p-Erweiterung von k. Für sie gilt:

$$G(k^{\mathfrak{m}}(p)|k) \cong (\mathcal{C}_k/\mathcal{C}_k^{\mathfrak{m}})(p).$$

Wir wollen noch kurz auf eine alternative Formulierung des Reziprozitätsgesetzes für beschränkte Verzweigung eingehen. Sei S eine endliche Menge von Primstellen von k. Die Definition von $\mathcal{C}_S(K) = \mathcal{I}_K/K^\times \mathcal{U}_{K,S}$ ist dadurch motiviert, daß in den Stellen $\mathfrak{p} \notin S$ im Hinblick auf Satz (1.2.19) (b) die Gruppen $\mathcal{U}_{\mathfrak{p}}$ stets in den Normengruppen enthalten sind. Wegen $K^\times \cap \mathcal{U}_{K,S} = 1$ können wir $\mathcal{U}_{K,S}$ als Untergruppe von $\mathcal{C}_K$ auffassen. Aufgrund der kohomologischen Trivialität von $\mathcal{U}_{K,S}$ (siehe S. 33) folgt aus der exakten Sequenz $0 \to \mathcal{U}_{K,S} \to \mathcal{C}_K \to \mathcal{C}_S(K) \to 0$, daß für alle $i \in \mathbb{Z}$ gilt:

$$\hat{H}^i(G(K|k), \mathcal{C}_K) \cong \hat{H}^i(G(K|k), \mathcal{C}_S(K)).$$

Ruft man sich ferner den guten Galois-Abstieg von $\mathcal{C}_S(K)$ in Erinnerung, erhält man sofort, daß $(G_S, \mathcal{C}_S)$ eine Klassenformation bildet. Dabei sei G_S die Galois-Gruppe der maximalen außerhalb S unverzweigten Erweiterung k_S von k, und $\mathcal{C}_S = \varinjlim \mathcal{C}_S(K)$, wobei der Limes über die endlichen galoisschen Erweiterungen K von k laufe, die in k_S enthalten sind. Die Normengruppen ergeben sich aus den gewöhnlichen durch Faktorbildung nach $\mathcal{U}_{K,S}$. Damit sind es gerade wieder die offenen Untergruppen endlichen Indexes von $\mathcal{C}_S(k)$.

1.2.5. Der Hauptidealsatz

Abstrakte Fassung

Zunächst formulieren wir eine abstrakte Fassung des Hauptidealsatzes in der im Abschnitt 1.1.6 benutzten Notation.

Sei $G = G_k$ eine proendliche Gruppe und C eine Klassenformation zu G. Wir indizieren die abgeschlossenen Normalteiler von G_k mit formalen Körpern $K|k$ und schreiben wieder $G(L|K) = G_K/G_L$ für zwei formale Körper $L|k$ und $K|k$ mit $G_L \subseteq G_K$. Außerdem setzen wir $C_K = C^{G_K}$.

Wir setzen in diesem Abschnitt voraus, daß für alle endlichen formalen Körpererweiterungen $K|k$ die Abelisierung G_K^{ab} endlich ist.

Wir fixieren eine endliche formale Körpererweiterung $K|k$ und bezeichnen mit K_1 den Körper mit

$$G_K^{ab} = G(K_1|K)$$

und mit K_2 den Körper mit

$$G_{K_1}^{ab} = G(K_2|K_1).$$

Nach Definition erhalten wir, daß $G_{K_2} = G'_{K_1}$ eine Untergruppe von G'_K ist, und daß $G_{K_1} = G'_K$ gilt (dabei bezeiche jeweils G' die Kommutatorgruppe $\overline{[G,G]}$). Daraus schließen wir die Gleichheiten

$$G(K_2|K)^{ab} = G(K_1|K) \quad \text{und} \quad G(K_2|K)' = G(K_2|K_1).$$

Nach Satz (1.1.31) ist das Diagramm

$$\begin{array}{ccc} C_K/N_{K_1|K}C_{K_1} & \xrightarrow[\sim]{(\cdot,K_2|K)} & G(K_2|K)^{ab} \\ {\scriptstyle i}\downarrow & & {\scriptstyle \text{Ver}}\downarrow \\ C_{K_1}/N_{K_2|K_1}C_{K_2} & \xrightarrow[\sim]{(\cdot,K_2|K_1)} & G(K_2|K_1) \end{array}$$

kommutativ, wobei i der von der Inklusion $C_K \hookrightarrow C_{K_1}$ induzierte Homomorphismus ist.

Die berühmte gruppentheoretische Version des Hauptidealsatzes von Furtwängler (vgl. [N-ZT], Theorem VI.7.6) ist das folgende

(1.2.25) Theorem. *Sei G eine endlich erzeugte Gruppe, so ist die Verlagerung*

$$Ver : G^{ab} \to (G')^{ab}$$

die triviale Abbildung.

Daraus ziehen wir die für uns relevante Konsequenz:

(1.2.26) Korollar. *Der von der Inklusion induzierte Homomorphismus*

$$i : C_K/N_{K_1|K}C_{K_1} \to C_{K_1}/N_{K_2|K_1}C_{K_2}$$

ist trivial.

Der Hauptidealsatz in der globalen Klassenkörpertheorie

Sei k ein Zahlkörper mit fixiertem algebraischen Abschluß $\overline{k}|k$ und S eine Primstellenmenge von k. L_S sei die maximale unverzweigte Erweiterung von k, die in S voll zerlegt ist. Eine Verbindung zum abstrakten Fall erhalten wir durch die Definition

$$G_k := G(L_S|k) \text{ und } C := \mathcal{C}_{L_S}.$$

Mit k_1 bezeichnen wir die maximale abelsche unverzweigte und in S voll zerlegte Erweiterung von k und mit k_2 die entsprechende von k_1, welche galoissch über k ist. Weiter seien $k_1(p)$ und $k_2(p)$ die maximalen in k_1 bzw. k_2 enthaltenen galoisschen p-Erweiterungen. Dann kommutieren die Diagramme

$$\begin{array}{ccc} \mathcal{C}l_S(k) & \xleftarrow[\sim]{\chi} & \mathcal{C}_k/N_{k_1|k}\mathcal{C}_{k_1} \\ {\scriptstyle \text{nat}}\downarrow & & {\scriptstyle i}\downarrow \\ \mathcal{C}l_S(k_1) & \xleftarrow[\sim]{\chi} & \mathcal{C}_{k_1}/N_{k_2|k_1}\mathcal{C}_{k_2} \end{array} \quad \text{und} \quad \begin{array}{ccc} \mathcal{C}l_S(k)(p) & \xleftarrow[\sim]{\chi} & (\mathcal{C}_k/N_{k_1(p)|k}\mathcal{C}_{k_1(p)})(p) \\ {\scriptstyle \text{nat}}\downarrow & & {\scriptstyle i}\downarrow \\ \mathcal{C}l_S(k_1(p))(p) & \xleftarrow[\sim]{\chi} & (\mathcal{C}_{k_1(p)}/N_{k_2(p)|k_1(p)}\mathcal{C}_{k_2(p)})(p) \end{array} .$$

Damit ergibt sich das

(1.2.27) Korollar. *Die natürlichen Abbildungen*

$$\mathcal{C}l_S(k) \to \mathcal{C}l_S(k_1) \quad \textit{und} \quad \mathcal{C}l_S(k)(p) \to \mathcal{C}l_S(k_1(p))(p)$$

sind trivial.

Nun sei $\mathfrak{m}$ ein Modul und $L^{\mathfrak{m}}$ die maximale Erweiterung von k innerhalb von $\overline{k}$, so daß für $L^{\mathfrak{m}} \supset K \supset k$ stets $K^{ab} \subset k^{\mathfrak{m}}$ gilt. Die Verbindung zum abstrakten Fall wird gegeben durch

$$G_k := G(L^{\mathfrak{m}}|k) \quad \text{und} \quad C := \mathcal{C}_{L^{\mathfrak{m}}}.$$

Wir schreiben $k_1 := k^{\mathfrak{m}}$ und $k_2 := k_1^{\mathfrak{m}}$ für die Strahlklassenkörper modulo $\mathfrak{m}$ von k bzw. k_1 und wieder $k_1(p)$ bzw. $k_2(p)$ für die in k_1 bzw. k_2 enthaltenen maximalen galoisschen p-Erweiterungen. k_2 ist galoissch über k. Es kommutieren die Diagramme

$$\begin{tikzcd} \mathcal{J}_k^{\mathfrak{m}}/\mathcal{P}_k^{\mathfrak{m}} \arrow[d, "\text{nat}"'] & \mathcal{C}_k/\mathcal{C}_k^{\mathfrak{m}} \arrow[l, "\chi"', "\sim"] \arrow[d, "i"'] \\ \mathcal{J}_{k_1}^{\mathfrak{m}}/\mathcal{P}_{k_1}^{\mathfrak{m}} & \mathcal{C}_{k_1}/\mathcal{C}_{k_1}^{\mathfrak{m}} \arrow[l, "\chi"', "\sim"] \end{tikzcd} \quad \text{und} \quad \begin{tikzcd} (\mathcal{J}_k^{\mathfrak{m}}/\mathcal{P}_k^{\mathfrak{m}})(p) \arrow[d, "\text{nat}"'] & (\mathcal{C}_k/\mathcal{C}_k^{\mathfrak{m}})(p) \arrow[l, "\chi"', "\sim"] \arrow[d, "i"'] \\ (\mathcal{J}_{k_1(p)}^{\mathfrak{m}}/\mathcal{P}_{k_1(p)}^{\mathfrak{m}})(p) & (\mathcal{C}_{k_1(p)}/\mathcal{C}_{k_1(p)}^{\mathfrak{m}})(p) \arrow[l, "\chi"', "\sim"] \end{tikzcd}.$$

Somit ergibt sich das

(1.2.28) Korollar. *Die natürlichen Abbildungen*

$$\mathcal{J}_k^{\mathfrak{m}}/\mathcal{P}_k^{\mathfrak{m}} \to \mathcal{J}_{k^{\mathfrak{m}}}^{\mathfrak{m}}/\mathcal{P}_{k^{\mathfrak{m}}}^{\mathfrak{m}} \quad \textit{und} \quad (\mathcal{J}_k^{\mathfrak{m}}/\mathcal{P}_k^{\mathfrak{m}})(p) \to (\mathcal{J}_{k^{\mathfrak{m}}(p)}^{\mathfrak{m}}/\mathcal{P}_{k^{\mathfrak{m}}(p)}^{\mathfrak{m}})(p)$$

und die von der Inklusion induzierten Abbildungen

$$i : \mathcal{C}_k/\mathcal{C}_k^{\mathfrak{m}} \to \mathcal{C}_{k^{\mathfrak{m}}}/\mathcal{C}_{k^{\mathfrak{m}}}^{\mathfrak{m}} \qquad \textit{und} \qquad i : (\mathcal{C}_k/\mathcal{C}_k^{\mathfrak{m}})(p) \to (\mathcal{C}_{k^{\mathfrak{m}}(p)}/\mathcal{C}_{k^{\mathfrak{m}}(p)}^{\mathfrak{m}})(p)$$

sind trivial.

Speziell für $\mathfrak{m} = 1$ ist der Strahlklassenkörper gerade die maximale abelsche unverzweigte Erweiterung, *(kleiner) Hilbertscher Klassenkörper* genannt. Die Aussage des *klassischen Hauptidealsatzes* ist nun, daß jedes Ideal von k im Hilbertschen Klassenkörper k_1 ein Hauptideal wird.

1.2.6. Ein Dualitätssatz für in S voll zerlegte Erweiterungen

Wir nehmen nun die Voraussetzungen der Arbeit [W].

- Sei k ein algebraischer Zahlkörper und S eine Menge von Primstellen von k.
- L_S sei die maximale unverzweigte und in S voll zerlegte Erweiterung von k, und $L_S(p)$ die maximale in L_S enthaltene galoissche p-Erweiterung.
- Für eine endliche Galois-Erweiterung $K|k$ sei $E_S(K)$ die Gruppe der S-Einheiten $\mathcal{O}_{K,S}^{\times}$, und wir setzen

$$E_S(L_S) := \varinjlim_{K|k, K\subseteq L_S} E_S(K) \quad \text{bzw.} \quad E_S(L_S(p)) := \varinjlim_{K|k, K\subseteq L_S(p)} E_S(K).$$

Aus dem abstrakten Dualitätssatz (Theorem (1.1.34)) schließen wir Theorem 1.1 von [W].

(1.2.29) Theorem. *(a) Für alle $i \in \mathbb{Z}$ gibt es kanonische topologische Isomorphismen*

$$\hat{H}^i\big(G(L_S|k), E_S(L_S)\big) \cong \hat{H}^{2-i}\big(G(L_S|k), \mathbb{Q}/\mathbb{Z}\big)^{\vee}.$$

(b) Für alle $i \in \mathbb{Z}$ gibt es kanonische topologische Isomorphismen

$$\hat{H}^i\big(G(L_S(p)|k), E_S(L_S(p))\big) \cong \hat{H}^{2-i}\big(G(L_S(p)|k), \mathbb{Q}_p/\mathbb{Z}_p\big)^{\vee}.$$

Beweis. Wir müssen die Bedeutung der im abstrakten Dualitätssatz verwendeten Bezeichnungen festlegen.

Für eine endliche galoissche Erweiterung $K \subseteq L_S$ von k bezeichne $\mathcal{C}_K$ die Idelklassengruppe und $\mathcal{C}_K^0$ den kompakten Kern der Absolutnorm. Setzen wir

$$\mathcal{C} = \varinjlim_{L_S \supset K|k} \mathcal{C}_K \quad \text{und} \quad \mathcal{C}^0 = \varinjlim_{L_S \supset K|k} \mathcal{C}_K^0,$$

so ist $\mathcal{C}^0$ level-kompakt, und wir haben die exakte Sequenz

$$0 \to \mathcal{C}^0 \to \mathcal{C} \to \mathbb{R}_+ \to 0.$$

Die Rolle von E_K werde durch die S-Einheiten $E_S(K)$ übernommen und die von $\mathcal{I}_K$ durch $\mathcal{I}_S(K)$, welche für $K \subset L_S$ nach Korollar (1.2.5) kohomologisch trivial ist.

$\mathcal{C}l_K$ werde repräsentiert durch $\mathcal{C}l_S(K)$, welches nach Satz (1.2.21) isomorph zur Galois-Gruppe der maximalen unverzweigten abelschen und in S voll zerlegten Erweiterung von K ist.

Die Endlichkeit von $\mathcal{C}l_S(K)$ haben wir auf Seite 33 bewiesen.

Die Trivialität von $\varinjlim_{L_S \supset K|k} \mathcal{C}l_S(K)$ und $\varinjlim_{L_S(p) \supset K|k} \mathcal{C}l_S(K)(p)$ folgt aus dem Hauptidealsatz (Korollar (1.2.27)).

Die Exaktheit der Sequenzen in dem und die Kommutativität des Diagramms (1.1.33) folgen aus Satz (1.2.11) bzw. lassen sich sofort nachrechnen.

Das Theorem ergibt sich nun aus Theorem (1.1.34). □

1.2.7. Ein Dualitätssatz für beschränkte Verzweigung

Nun betrachten wir die folgende Situation:

- Sei p eine Primzahl und k ein algebraischer Zahlkörper, welchen wir im Falle $p = 2$ als total imaginär voraussetzen wollen, und sei $\overline{k}$ ein algebraischer Abschluß von k.

- Sei S eine endliche Menge von Primstellen von k mit

  $$S \cap S_p = \emptyset,$$

  wobei S_p die Menge der über p liegenden Primstellen von k sei.

- Mit k_S bezeichnen wir die maximale galoissche Erweiterung von k in $\overline{k}$, die außerhalb von S, also insbesondere über p, unverzweigt ist.

  Weiter sei $k_S(p)$ die maximale, darin enthaltene galoissche p-Erweiterung. Nach Voraussetzung ist $k_S(p)$ über k in allen Primstellen $\mathfrak{p} \in S$ zahm verzweigt.

- Für eine endliche galoissche Erweiterung $k_S \supset K|k$ schreiben wir $E^S(K) := \mathcal{O}_{k,\mathfrak{m}}^\times$ für den Modul $\mathfrak{m} := \prod_{\mathfrak{p} \in S} \mathfrak{p}$.

  Wir setzen $E^S(k_S) := \varinjlim_{k_S \supset K|k} E^S(K)$ und $E^S(k_S(p)) := \varinjlim_{k_S(p) \supset K|k} E^S(K)$.

(1.2.30) Theorem. *Für alle $i \in \mathbb{Z}$ gibt es kanonische topologische Isomorphismen*

$$\hat{H}^i\big(G(k_S(p)|k), E^S(k_S(p))\big) \cong \hat{H}^{2-i}\big(G(k_S(p)|k), \mathbb{Q}_p/\mathbb{Z}_p\big)^\vee.$$

Beweis. Wir müssen auch hier die Übersetzungen zum abstrakten Fall angeben.

Für eine endliche galoissche Erweiterung $K \subseteq k_S$ von k sei wieder $\mathcal{C}_K$ die Idelklassengruppe und $\mathcal{C}_K^0$ der kompakte Kern der Absolutnorm. Setzen wir auch hier

$$\mathcal{C} = \varinjlim_{k_S \supset K|k} \mathcal{C}_K \quad \text{und} \quad \mathcal{C}^0 = \varinjlim_{k_S \supset K|k} \mathcal{C}_K^0,$$

so ist $\mathcal{C}^0$ level-kompakt, und wir haben die exakte Sequenz

$$0 \to \mathcal{C}^0 \to \mathcal{C} \to \mathbb{R}_+ \to 0.$$

Die Rolle von E_K wird durch $E^S(K)$ übernommen und die von $\mathcal{I}_K$ durch die Gruppe $\mathcal{I}_K^{\mathfrak{m}}$, welche für $K \subset k_S(p)$ kohomologisch trivial ist, was aus dem folgenden Lemma (1.2.31) folgt. Denn es spielen nur die endlichen Stellen von S eine Rolle, da die Erweiterung außerhalb von S unverzweigt ist, und für $p \neq 2$ bei Vervollständigung nach archimedischen Stellen die Erweiterung $\mathbb{C}/\mathbb{R}$ nicht auftreten kann, und für $p = 2$ der Grundkörper k als total imaginär vorausgesetzt wurde.

$\mathcal{C}l_K$ werde repräsentiert durch die Gruppe $\mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}}$, welche nach Satz (1.2.24) isomorph zur Galois-Gruppe der maximalen außerhalb S unverzweigten (und innerhalb S zahm verzweigten) abelschen Erweiterung von K ist.

Die Endlichkeit von $\mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}}$ haben wir in Satz (1.2.7) bewiesen.

Die Trivialität von $\varinjlim_{k_S \supset K|k} \mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}}$ und $\varinjlim_{k_S(p) \supset K|k} \mathcal{C}_K/\mathcal{C}_K^{\mathfrak{m}}(p)$ folgt aus dem Hauptidealsatz (Korollar (1.2.28)).

Die Exaktheit der Sequenzen in dem und die Kommutativität des Diagramms (1.1.33) folgen aus Satz (1.2.13) bzw. lassen sich sofort nachrechnen.

Das Theorem ergibt sich nun aus dem Fall (b) von Theorem (1.1.34). □

(1.2.31) Lemma. *Sei p eine Primzahl, K ein q-adischer Zahlkörper mit $q \neq p$. Ist $L|K$ eine Galois-Erweiterung vom Grad p^s, so sind die höheren Einseinheitengruppen $\mathcal{U}_L^{(n)}$ für alle $n \geq 1$ kohomologisch trivial.*

Beweis. Die n-te Einseinheitengruppe ist projektiver Limes $\mathcal{U}_L^{(n)} = \varprojlim_m \mathcal{U}_L^{(n)}/\mathcal{U}_L^{(m)}$ für $n \geq 1$ von (multiplikativen) q-Gruppen, auf denen Potenzierung mit p^s bijektiv ist. Somit ist Potenzierung mit p^s auch auf $\mathcal{U}_L^{(n)}$ und daher auf $\hat{H}^i(G(L|K), \mathcal{U}_L^{(n)})$ bijektiv. Aufgrund von $f^{(p^s)} = 1$ für alle $f \in \hat{H}^i(G(L|K), \mathcal{U}_L^{(n)})$ ist $\hat{H}^i(G(L|K), \mathcal{U}_L^{(n)}) = 1$ für alle $i \in \mathbb{Z}$. □

II. Galois-Gruppen von CM-Körpern

2.1. Strukturen in Pro-p-Gruppen

2.1.1. Erzeuger und Relationen von Pro-p-Gruppen

Sei G eine Pro-p-Gruppe. Die *Frattini-Untergruppe* $\Phi(G)$ ist definiert als der Durchschnitt aller echten offenen Untergruppen von G. Es gilt (siehe [DDMS], Prop. 1.13)

$$\Phi(G) = \overline{G^p[G,G]},$$

wobei G^p das Erzeugnis der p-ten Potenzen von G bezeichnet. Daher ist $G/\Phi(G)$ die größte Faktorgruppe von G, die abelsch und vom Exponenten p ist. Da jeder Homomorphismus $G \to \mathbb{Z}/p\mathbb{Z}$ über $\Phi(G)$ faktorisiert, erhalten wir die Gleichheit

$$H^1(G) = Hom(G,\mathbb{Z}/p\mathbb{Z}) = Hom(G/\Phi(G),\mathbb{Z}/p\mathbb{Z}) = Hom(G/\Phi(G),\mathbb{R}/\mathbb{Z}) = (G/\Phi(G))^\vee.$$

Dabei haben wir $H^1(G)$ für $H^1(G,\mathbb{Z}/p\mathbb{Z})$ geschrieben.

Eine Teilmenge $S \subseteq G$ heißt *konvergent (gegen* 1*)*, falls in jeder offenen Untergruppe $U \leq G$ fast alle Elemente von S liegen.

Eine konvergente Teilmenge $S \subseteq G$ heißt *Erzeugendensystem* von G, falls $\overline{<S>}$ gleich G ist. Wir nennen die minimale Erzeugendenzahl den *Rang* von G und bezeichnen ihn mit $d(G)$.

Eine den Pro-p-Gruppen besondere Eigenschaft ist die folgende Charakterisierung des Ranges.

(2.1.1) Satz. *Eine konvergente Teilmenge S der Pro-p-Gruppe G erzeugt G genau dann, wenn $G/\Phi(G)$ durch die Restklassen $\overline{S}$ modulo $\Phi(G)$ von S erzeugt wird. Ferner gilt:*

$$d(G) = dim_{\mathbb{F}_p} H^1(G) = \frac{1}{p}|G/\Phi(G)|.$$

Beweis. Wir setzen $H := \overline{<S>}$. Falls nun $H/\Phi(H)$ gleich $G/\Phi(G)$ ist, dann gilt insbesondere $H^1(H/\Phi(H)) = H^1(G/\Phi(G))$ und somit $H^1(H) = H^1(G)$, weshalb aus der Inflation-Restriktion-Sequenz folgt, daß $H^1(G/H)$ trivial ist. Dann muß aber bereits G/H die Einsgruppe sein. Der Satz folgt nun sofort. $\square$

Eine Pro-p-Gruppe ist also genau dann endlich erzeugt, wenn $G/\Phi(G) = G/\overline{G^p[G,G]} = H^1(G)$ endlich ist. Dies wollen wir leicht verallgemeinern.

Unter Benutzung der exakten Sequenz

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^r\mathbb{Z} \to \mathbb{Z}/p^{r-1}\mathbb{Z} \to 0$$

für $r \in \mathbb{N}$ erhalten wir induktiv, daß $H^1(G,\mathbb{Z}/p^r\mathbb{Z})$ endlich ist, falls dies für $H^1(G,\mathbb{Z}/p\mathbb{Z})$ der Fall ist. Aus der Rechnung

$$H^1(G,\mathbb{Z}/p^r\mathbb{Z}) = Hom(G/\overline{G^{p^r}[G,G]},\mathbb{Z}/p^r\mathbb{Z}) = (G/\overline{G^{p^r}[G,G]})^\vee$$

schließen wir, daß in diesem Fall auch die Gruppe $G/\overline{G^{p^r}[G,G]}$ endlich ist. Wir erhalten:

(2.1.2) Lemma. *Sei G eine endlich erzeugte Pro-p-Gruppe.*

(a) $G/\overline{G^{p^r}[G,G]}$ ist endlich für alle $r \in \mathbb{N}$.

(b) Eine offene Untergruppe $H \leq G$ ist ebenfalls endlich erzeugt.

Beweis. (a) haben wir gerade gezeigt. (b) ist z. B. in [DDMS], Proposition 1.7, bewiesen. □

Sei $N \lhd G$ ein abgeschlossener Normalteiler von G. Ein *Erzeugendensystem als Normalteiler* von N ist eine konvergente Teilmenge $S \subseteq N$, so daß N der kleinste Normalteiler ist, der S enthält.

(2.1.3) Lemma. *Sei G eine Pro-p-Gruppe und N ein abgeschlossener Normalteiler, der als Normalteiler von der Menge $S \subseteq N$ erzeugt wird. Ferner sei $H \lhd G$ ein weiterer abgeschlossener Normalteiler. Dann wird NH/H als Normalteiler von G/H erzeugt von der Menge $\overline{S}$ der Restklassen modulo H der Elemente aus S.*

Beweis. Es gilt $N = \bigcap M$, wobei der Durchschnitt über alle abgeschlossenen Normalteiler $M \lhd G$ gebildet wird, die S umfassen. Dann ist

$$NH/H = \bigcap_{\overline{S} \subseteq MH/H,\, M \lhd G} MH/H = \bigcap_{\overline{S} \subseteq X,\, X \lhd G/H} X,$$

was die Behauptung impliziert. □

Aus [NSW] zitieren wir Corollary 3.9.3:

(2.1.4) Satz. *Sei $N \lhd G$ ein abgeschlossener Normalteiler der Pro-p-Gruppe G. Dann erzeugt die Menge $S \subseteq N$ den Normalteiler N als Normalteiler genau dann, wenn $\overline{S}$ (siehe Lemma (2.1.3)) $N/\overline{N^p[G,N]}$ als Normalteiler von $G/\Phi(G)$ erzeugt.*

Ist S minimal, so gilt

$$|S| = dim_{\mathbb{F}_p} H^1(N)^G.$$

Im folgenden wollen wir den Begriff der freien Pro-p-Gruppe einführen und ihn benutzen, um den Begriff der Relation zu definieren und zu charakterisieren.

(2.1.5) Definition. *Sei X eine Menge. Eine* freie Pro-p-Gruppe *auf X ist eine Pro-p-Gruppe F_X zusammen mit einer Abbildung $i : X \to F_X$, so daß gelten:*

(i) Jede offene Untergruppe $U \leq F_X$ enthält fast alle Elemente von $i(X)$.

(ii) Für jede Pro-p-Gruppe G mit Abbildung $j : X \to G$ gibt es genau einen Homomorphismus $f : F_X \to G$, so daß $f \circ i = j$ gilt.

Man erhält eine freie Pro-p-Gruppe durch Bildung des projektiven Limes über alle Quotienten $\mathcal{F}/U$, wobei $\mathcal{F}$ die gewöhnliche freie Gruppe bezeichnet, und U die Normalteiler von $\mathcal{F}$ von endlichem Index durchläuft, die fast alle Elemente $x \in X$ enthalten, und für die $\mathcal{F}/U$ eine p-Gruppe ist. Die Existenz und Eindeutigkeit des Homomorphismus $f : F_X \to G$ folgt dann im Wesentlichen aus der stetigen Fortsetzung auf F_X des eindeutigen Homomorphismus der gewöhnlichen freien Gruppe auf X nach G.

Aus der universellen Eigenschaft der freien Pro-p-Gruppen schließen wir, daß es zu vorgegebener Pro-p-Gruppe G mit Erzeugendensystem S eine exakte Sequenz

$$1 \to R \to F \to G \to 1$$

gibt, wobei F die freie Pro-p-Gruppe auf S ist.

Ein *Relationensystem* $\mathcal{R}$ von G bzgl. S ist ein Erzeugendensystem von R als Normalteiler von F. Auch für dieses haben wir eine kohomologische Charakterisierung.

(2.1.6) Satz. *Sei G eine endlich erzeugte Pro-p-Gruppe mit minimalem Erzeugendensystem S. Dann gilt für ein minimales Relationensystem $\mathcal{R}$ bzgl. S*

$$|\mathcal{R}| = dim_{\mathbb{F}_p} H^2(G).$$

Diese Zahl bezeichnen wir mit $r(G)$ und nennen sie den Relationenrang *von G.*

Beweis. Wir betrachten die Fünf-Terme-Sequenz aus Satz (2.2.7)

$$0 \to H^1(G) \to H^1(F) \to H^1(R)^G \to H^2(G) \to H^2(F).$$

Da nach [NSW], Proposition 3.5.8, $H^2(F) = 0$ gilt, erhalten wir zusammen mit Satz (2.1.4)

$$\begin{aligned} 0 &= dim_{\mathbb{F}_p} H^1(G) - dim_{\mathbb{F}_p} H^1(F) + dim_{\mathbb{F}_p} H^1(R)^G - dim_{\mathbb{F}_p} H^2(G) \\ &= d(G) - |S| + |\mathcal{R}| - dim_{\mathbb{F}_p} H^2(G). \end{aligned}$$

□

Wir werden später folgende Sätze benötigen.

(2.1.7) Satz. *Sei G eine endlich erzeugte Pro-p-Gruppe mit einer Relation, d.h. $r(G) = 1$. Dann ist $d(G) = 1$ oder G hat $\mathbb{Z}_p$ als Quotienten.*

Beweis. Ist $r(G) = 1$, so finden wir eine exakte Sequenz

$$1 \to R \to F \to G \to 1,$$

wobei R von einem Element als Normalteiler der freien Pro-p-Gruppe F (bzgl. einem minimalen Erzeugendensystem S von G) erzeugt wird. Nach Lemma (2.1.3) ist RF'/F' entweder trivial oder wird von einem Element als Untergruppe von $F/F' = F^{ab}$ erzeugt. Die Sequenz

$$1 \to RF'/F' \to F^{ab} \to G^{ab} \to 1$$

ist exakt, und alle vorkommenden Gruppen sind $\mathbb{Z}_p$-Moduln, wobei $rk_{\mathbb{Z}_p} F^{ab} = |S|$ ist. Daher gilt $rk_{\mathbb{Z}_p} G^{ab} \geq |S| - 1$, und die Behauptung folgt. □

(2.1.8) Satz. *Sei G eine endlich erzeugte Pro-p-Gruppe. Dann ist die Sequenz*

$$0 \to ({}_pG^{ab})^\vee \to H^2(G, \mathbb{Z}/p\mathbb{Z}) \to {}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p) \to 0$$

exakt. Insbesondere berechnet sich der Relationenrang von G zu

$$r(G) = dim_{\mathbb{F}_p}\, {}_pG^{ab} + dim_{\mathbb{F}_p}\, {}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p).$$

Beweis. Wir gehen aus von der exakten Sequenz

$$0 \to \frac{1}{p}\mathbb{Z}/\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p} \mathbb{Q}_p/\mathbb{Z}_p \to 0.$$

Dieser ordnen wir die lange exakte Sequenz

$$H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p} H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(G, \mathbb{Z}/p\mathbb{Z}) \to H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p} H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)$$

zu. Die Sequenz

$$0 \to {}_pG^{ab} \to G^{ab} \xrightarrow{p} G^{ab}$$

ist exakt, woraus wir durch Dualisierung die ebenfalls exakte Sequenz

$$H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p} H^1(G, \mathbb{Q}_p/\mathbb{Z}_p) \to H^1({}_pG^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) \to 0$$

erhalten. Deshalb können wir schließen, daß

$$0 \to H^1({}_pG^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(G, \mathbb{Z}/p\mathbb{Z}) \to {}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p) \to 0$$

exakt ist. Wegen

$$H^1({}_pG^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) = Hom({}_pG^{ab}, \mathbb{Q}_p/\mathbb{Z}_p) = ({}_pG^{ab})^\vee$$

ergibt sich der Satz. □

Der folgende Satz ist ein Analogon zur Zerlegung eines Moduls über einem Hauptidealring in einen freien und einen Torsionsteil.

(2.1.9) Satz. *Sei G eine endlich erzeugte Pro-p-Gruppe. Dann gilt:*

$$d(G) = dim_{\mathbb{F}_p}(G/\Phi(G)) = rk_{\mathbb{Z}_p}(G^{ab}) + dim_{\mathbb{F}_p}({}_pG^{ab}).$$

Beweis. Wegen $d(G^{ab}) = d(G)$ dürfen wir G als abelsch voraussetzen. Dann ist G direktes Produkt von r Kopien von $\mathbb{Z}_p$ und $s = d(G) - r$ Gruppen der Form $\mathbb{Z}/p^{e_i}\mathbb{Z}$. Dabei ist r der Rang von G als $\mathbb{Z}_p$-Modul. Aufgrund von ${}_p\mathbb{Z}_p = 0$ gilt ${}_pG = {}_p(\prod \mathbb{Z}/p^{e_i}\mathbb{Z})$. Für die $\mathbb{F}_p$-Dimension folgt nun $dim_{\mathbb{F}_p}({}_pG) = s$. □

2.1.2. Filtrierungen von Pro-p-Gruppen

Allgemeines

Eine *filtrierte Gruppe* ist eine Gruppe G zusammen mit einer Abbildung

$$\omega : G \to \mathbb{N} \cup \{\infty\},$$

so daß für alle $x, y \in G$

$$\omega(xy^{-1}) \geq min(\omega(x), \omega(y))$$

gilt. Definieren wir für jedes $n \in \mathbb{N}$ die Menge

$$G_n := \{x \in G |\ \omega(x) \geq n\},$$

so erhalten wir eine absteigende Kette von Untergruppen von G.

Umgekehrt definiert eine solche Kette auch eine Filtrierung via

$$\omega(x) := max\{n |\ x \in G_n\}.$$

In [Lz] wird von einer Filtrierung zusätzlich gefordert, daß

$$\omega([x, y]) \geq \omega(x) + \omega(y)$$

für alle $x, y \in G$ gilt, was gleichbedeutend ist mit

$$[G_n, G_m] \subseteq G_{n+m}.$$

Wir nennen eine solche Filtrierung *zentral*.

Wir halten noch fest, daß in diesem Falle G_n für alle n ein Normalteiler von G ist, und zusätzlich G_n/G_{n+1} im Zentrum von G/G_{n+1} liegt. Des weiteren sind sukzessive Quotienten zentraler Filtrierungen abelsch.

Zassenhaus-Filtrierung einer Pro-p-Gruppe

In diesem Abschnitt folgen wir weitgehend [K-G]. Sei G eine Pro-p-Gruppe. Wir möchten uns eine Filtrierung von G beschaffen. Dazu konstruieren wir zunächst eine Umgebungsbasis der 0 in der Gruppenalgebra. Viele Aussagen über Gruppenfiltrierungen können wir dann in der Gruppenalgebra behandeln.

Wir definieren die (vervollständigte) Gruppenalgebra durch

$$\mathbb{F}_p[[G]] = \varprojlim \mathbb{F}_p[G/N],$$

wobei der projektive Limes über die offenen Normalteiler von G gebildet wird. In ihr haben wir das Ideal

$$I(G) = \overline{(g-1|\ g \in G)}.$$

Ferner setzen wir

$$I^n(G) := \overline{(I(G))^n}.$$

Nun haben wir den folgenden Satz (vgl. [K-G], Satz 7.8).

(2.1.10) Satz. *Sei G eine endlich erzeugte Pro-p-Gruppe. Dann bilden die Ideale $I^n(G)$ eine Umgebungsbasis der 0 in $\mathbb{F}_p[[G]]$.*

Wir definieren die *Zassenhaus-Filtrierung* durch

$$G_{(n)} := \{g \in G|\ g-1 \in I^n(G)\}.$$

Für das Studium ihrer Eigenschaften beweisen wir zunächst das folgende Lemma.

(2.1.11) Lemma. *(a) Für alle $g, h \in G$ gilt:*

$$[g,h]-1 = (gh-1)(g^{-1}h^{-1}-1) + (gh-1) + (g^{-1}h^{-1}-1)$$

(b) Für alle $g \in G_{(n)}$ und alle $h \in G_{(m)}$ gilt:

$$gh-1 \equiv g-1+h-1 \ \ (\textit{modulo } I^{n+m}(G)).$$

(c) $[G_{(n)}, G_{(m)}] \subseteq G_{(n+m)}$.

(d) Für alle $g \in G_{(n)}$ gilt: $g^{p^k} \in G_{(p^k n)}$.

Beweis. (a) rechnet man unmittelbar aus. Für (b) berechnen wir

$$gh-1 = (g-1)(h-1) + g-1+h-1 \equiv g-1+h-1 \ \ (\text{modulo } I^{n+m}(G)).$$

Für (c) rechnen wir modulo $I^{n+m}(G)$:

$$\begin{aligned}
[g,h]-1 &= (gh-1)(g^{-1}h^{-1}-1) + (gh-1) + (g^{-1}h^{-1}-1) \\
&\equiv ((g-1)+(h-1))((g^{-1}-1)+(h^{-1}-1)) + g-1+h-1+g^{-1}-1+h^{-1}-1 \\
&\equiv (g-1)(g^{-1}-1) + (h-1)(h^{-1}-1) + g-1+h-1+g^{-1}-1+h^{-1}-1 \\
&= 0
\end{aligned}$$

$\mathbb{F}_p[[G]]$ hat Charakteristik p, daher ist

$$g^{p^k} - 1 = (g-1)^{p^k}$$

ein Element von $I^{p^k n}(G)$, weshalb (d) gilt. □

Wir erhalten nun den

(2.1.12) Satz. *Sei G eine endlich erzeugte Pro-p-Gruppe. Dann ist die Zassenhaus-Filtrierung eine zentrale Filtrierung, und die $G_{(n)}$ bilden eine Umgebungsbasis der 1 von G.*

Beweis. Die erste Behauptung folgt unmittelbar aus dem vorausgehenden Lemma. Zur zweiten betrachten wir die Abbildung

$$\phi : G_{(n)}/G_{(n+1)} \to I^n(G)/I^{n+1}(G), \ g \mapsto g-1.$$

Diese ist ein Homomorphismus nach Teil (b) des Lemmas. Ferner ist ϕ nach Definition von $G_{(n+1)}$ injektiv. Daher ist $G_{(n)}/G_{(n+1)}$ endlich, weshalb $G_{(n+1)}$ in G offen ist.

Sei ferner $U \lhd G$ ein offener Normalteiler und

$$\psi_U : \mathbb{F}_p[[G]] \to \mathbb{F}_p[G/U]$$

die natürliche Projektion. Da der Kern von ψ_U offen ist, gibt es einen Index n, so daß $I^n(G)$ im Kern enthalten ist. Für alle $g \in G_{(n)}$ haben wir also die Gleichheit

$$\psi_U(g-1) = 0 = \psi_U(g) - 1.$$

Daher ist $G_{(n)}$ in U enthalten, und die $G_{(n)}$ steigen zur 1 ab. □

Die absteigende q-Zentralreihe

Wir definieren im Folgenden für eine Pro-p-Gruppe G eine weitere zentrale Filtrierung, die ganz entscheidende Verwendung finden wird.

Sei zunächst allgemein q eine p-Potenz oder 0. Die *absteigende q-Zentralreihe* wird induktiv definiert durch

$$G^{(1,q)} := G \ \text{ und } \ G^{(n+1,q)} := \overline{(G^{(n,q)})^q[G^{(n,q)}, G]}.$$

(2.1.13) Satz. *Sei G eine endlich erzeugte Pro-p-Gruppe.*

(a) Sei $K \subseteq G$ eine abgeschlossene Untergruppe. Wir setzen induktiv

$$K^{(1)} := K \ \textit{ und } \ K^{(n+1)} := \overline{(K^{(n)})^q[K^{(n)}, G]}.$$

Dann gilt für alle $n \in \mathbb{N}$

$$K^{(n)} \subseteq G_{(n)},$$

wobei $G_{(n)}$ die n-te Gruppe in der Zassenhaus-Filtrierung ist. Insbesondere steigen die $K^{(n)}$ und damit auch die $G^{(n,q)}$ echt zur 1 ab.

(b) Sei $q = p^s$ eine p-Potenz. Dann ist

$$G^{(n,q)} \subseteq G$$

eine offene Untergruppe. Die $G^{(n,q)}$ bilden also eine Umgebungsbasis der 1.

Beweis. (a) Im Lemma (2.1.11) haben wir gesehen, daß

$$(G_{(n)})^q \subseteq G_{(nq)} \ \text{ und } \ [G_{(n)}, G] \subseteq G_{(n+1)}$$

gilt. Wir zeigen die Behauptung nun induktiv. Für $n = 1$ ist sie klar. Der Induktionsschritt folgt aus

$$K^{(n+1)} = \overline{(K^{(n)})^q[K^{(n)}, G]} \subseteq \overline{(G^{(n)})^q[G^{(n)}, G]} \subseteq G_{(nq)}G_{(n+1)} \subseteq G_{(n+1)}.$$

Dies gilt für $q = p^s$. Der Beweis für $q = 0$ ergibt sich aus gleicher Rechnung durch Weglassen aller Terme, in denen ein q auftritt.

(b) Wir benutzen wiederum Induktion nach n. Der Induktionsanfang ist klar. Für den Schritt setzen wir zunächst $H := G^{(n,q)}$. Dann ist H als offene Untergruppe nach Lemma (2.1.2) endlich erzeugt, und $H/\overline{H^q[H, H]}$ ist endlich. Daher ist aber auch $G^{(n,q)}/G^{(n+1,q)} = H/\overline{H^q[H, G]}$ endlich. □

Man kann weiterhin zeigen, daß die absteigende q-Zentralreihe tatsächlich eine zentrale Filtrierung darstellt. Für den Fall $q = p$ ist die Rechnung z.B. in [DDMS] durchgeführt.

Wir wollen im Folgenden schreiben: $G_n := G^{(n,p)}$.

2.1.3. Potenzreiche und uniforme Pro-p-Gruppen

In diesem Abschnitt präsentieren wir kurz die wichtigsten elementaren Resultate der Theorie der potenzreichen und uniformen Gruppen, wie sie in [DDMS] entwickelt wird.

Wir fixieren eine Primzahl p, welche wir der Einfachheit halber als ungerade annehmen wollen.

Sei G eine Pro-p-Gruppe. G heißt *potenzreich*, falls $G/\overline{G^p}$ abelsch ist.

Die wichtigsten aus der Definition folgenden Eigenschaften sind zusammengefaßt im folgenden Satz (vgl. [DDMS], Theorem 3.6, Proposition 3.7, Theorem 3.8).

(2.1.14) Satz. *Sei $G = \overline{< a_1, \ldots, a_d >}$ eine endlich erzeugte potenzreiche Gruppe, und bezeichne G_i die i-te Gruppe der absteigenden p-Zentralreihe.*

(a) Für alle $k \geq 0$ und alle $i \geq 1$ gilt $G_{i+k} = G_i^{p^k}$, insbesondere ist $G_{i+1} = \Phi(G_i)$ die Frattini-Untergruppe von G_i.

(b) $G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \overline{< a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} >}$.

(c) Die Abbildung $x \mapsto x^{p^k}$ induziert eine Surjektion von G_i/G_{i+1} auf G_{i+k}/G_{i+k+1} für alle $k \geq 0$ und alle $i \geq 1$.

(d) G ist das Produkt der prozyklischen Gruppen $\overline{< a_i >}$, d. h. $G = \overline{< a_1 >} \cdots \overline{< a_d >}$.

(e) Für eine abgeschlossene Untergruppe $H \leq G$ gilt: $d(H) \leq d(G)$.

Wir definieren den *Rang* einer proendlichen Gruppe durch

$$rk(G) = sup\{d(H) \mid H \leq G \text{ offene Untergruppe}\}.$$

Es gilt folgender fundamentaler Zusammenhang (vgl. [DDMS], Theorem 3.13).

(2.1.15) Satz. *Sei G eine Pro-p-Gruppe. Dann hat G endlichen Rang genau dann, wenn G endlich erzeugt ist und eine offene potenzreiche Untergruppe besitzt.*

Nach Satz (2.1.14) (c) ist für eine endlich erzeugte potenzreiche Gruppe G die Abbildung

$$G_i/G_{i+1} \twoheadrightarrow G_{i+1}/G_{i+2},\ x \mapsto x^p$$

ein surjektiver Homomorphismus, d. h. die Indizes $(G_i : G_{i+1})$ steigen ab. Also existiert ein k mit $(G_k : G_{k+1}) = (G_{k+i} : G_{k+i+1})$ für alle $i \geq 0$. Äquivalent dazu liefert Potenzierung mit x^{p^i} einen Isomorphismus zwischen G_k/G_{k+1} und G_{k+i}/G_{k+i+1}. Dieses erhebt man zur Definition:

Eine potenzreiche Gruppe heißt *uniform*, wenn sie endlich erzeugt ist, und Potenzierung mit p^i für alle $i \in \mathbb{N}$ einen Isomorphismus $G_1/G_2 \cong G_{i+1}/G_{i+2}$ induziert.

Wichtige Eigenschaften sind zusammengefaßt im folgenden Satz (vgl. [DDMS], Proposition 4.4, Theorem 4.5).

(2.1.16) Satz. *Sei G eine endlich erzeugte potenzreiche Pro-p-Gruppe. Dann sind äquivalent:*

(i) G ist uniform.

(ii) Es gilt $d(H) = d(G)$ für alle offenen und potenzreichen Untergruppen H von G.

(iii) G ist torsionsfrei.

Sind A und B offene uniforme Untergruppen einer endlich erzeugten Pro-p-Gruppe, dann gilt $d(A) = d(B)$. Dies erlaubt die Definition

$$dim(G) := d(H) \text{ für eine offene uniforme Untergruppe } H \text{ von } G.$$

Die Zahl $dim(G)$ nennen wir die *Dimension* von G.

Falls G von endlichem Rang, und $N \lhd G$ ein abgeschlossener Normalteiler ist, dann gilt (siehe [DDMS], Theorem 4.8):

$$dim(G) = dim(N) + dim(G/N).$$

Der Zusammenhang zu p-adischen analytischen Gruppen wird gegeben durch folgendes bereits in der Einleitung erwähntes Theorem (vgl. [DDMS], Theorem 8.1).

(2.1.17) Theorem. *Eine topologische Gruppe G hat die Struktur einer p-adischen analytischen Gruppe genau dann, wenn sie eine offene, endlich erzeugte potenzreiche Untergruppe enthält.*

Die oben eingeführte Dimension stimmt mit der Dimension als p-adische analytische Gruppe überein.

2.2. Pro-p-Gruppen mit Aktion einer Involution

2.2.1. Aktion einer Involution auf abelschen Gruppen

Wir wollen in diesem Abschnitt abelsche Gruppen untersuchen, auf denen eine Involution, die wir mit σ bezeichnen, operiert.

Zunächst setzen wir für eine (additiv geschriebene) abelsche Gruppe A

$$A^+ := \{a \in A \mid \sigma a = a\} \quad \text{und} \quad A^- := \{a \in A \mid \sigma a = -a\}.$$

(2.2.1) Lemma. *Seien A, B und C abelsche Gruppen, auf denen Multiplikation mit 2 ein Automorphismus ist. Die Involution σ operiere auf A, B und C. Dann gelten:*

(a) $A^+ = \{\frac{1}{2}(a + \sigma a) \mid a \in A\}$ *und* $A^- = \{\frac{1}{2}(a - \sigma a) \mid a \in A\}$.

(b) $A = A^+ \oplus A^-$.

(c) Ist $f : A \to B$ ein σ-invarianter Homomorphismus, so ist $f(A^\pm) \subseteq B^\pm$, und außerdem gelten $Ker(f)^\pm = Ker(f : A^\pm \to B^\pm)$ und $Im(f)^\pm = Im(f : A^\pm \to B^\pm)$.

(d) Ist $0 \to A \to B \to C \to 0$ eine exakte Sequenz mit σ-invarianten Homomorphismen, so sind auch die Sequenzen $0 \to A^\pm \to B^\pm \to C^\pm \to 0$ exakt.

(e) Die Gruppe $Hom(A, B)$ versehen wir mit der gewöhnlichen σ-Aktion (B sei hier ein trivialer σ-Modul), d.h. $(\sigma f)(a) := f(\sigma a)$. Dann gilt:

$$Hom(A, B)^\pm = Hom(A^\pm, B).$$

(f) $(A^\vee)^\pm = (A^\pm)^\vee$.

(g) $(A \otimes B)^+ = (A^+ \otimes B^+) \oplus (A^- \otimes B^-)$.

(h) $(A \otimes B)^- = (A^- \otimes B^+) \oplus (A^+ \otimes B^-)$.

Beweis. Das rechnet man unmittelbar nach. □

(2.2.2) Satz. *Sei C eine endliche abelsche Gruppe vom Exponenten $p \neq 2$, auf der die Involution σ operiert. Dann existiert eine σ-invariante Zerlegung*

$$C = A_1 \oplus \cdots \oplus A_{d^+} \oplus B_1 \oplus \cdots \oplus B_{d^-},$$

wobei $A_i = A_i^+$, $B_j = B_j^-$, $|A_i| = |B_j| = p$, $d^+ = dim_{\mathbb{F}_p} C^+$ und $d^- = dim_{\mathbb{F}_p} C^-$ gelten.

Beweis. Nach dem Satz von Maschke ist $\mathbb{F}_p[< \sigma >]$ halbeinfach, da $2 \neq p$ vorausgesetzt ist. Daher ist auch jeder $\mathbb{F}_p[< \sigma >]$-Modul halbeinfach, weshalb C in eine direkte Summe von irreduziblen Moduln zerfällt, auf denen σ entweder als Inversion oder als Identität operiert.

Wäre die Elementzahl eines irreduziblen $\mathbb{F}_p[< \sigma >]$-Moduls größer als p, so zerfiele er zunächst als abelsche Gruppe in die direkte Summe von zu $\mathbb{Z}/p\mathbb{Z}$ isomorphen Gruppen. Auf diesen kann man aber die σ-Aktion so einrichten, daß die direkte Summe σ-invariant ist. □

2.2.2. Aktion einer Involution auf den Kohomologiegruppen

Sei G eine proendliche Gruppe und A ein diskreter G-Modul. Weiter sei eine endliche Gruppe Δ gegeben, die auf G und auf A derart operiert, daß für alle $\sigma \in \Delta$ die Homomorphismen

$$\phi_\sigma : G \to G,\ g \mapsto \sigma^{-1}g \qquad \text{und} \qquad \theta_\sigma : A \to A,\ a \mapsto \sigma a$$

ein verträgliches Paar im Sinne der Bemerkung (1.1.4) bilden. Das heißt, daß

$$\theta_\sigma(\phi_\sigma(g).a) = g.\theta_\sigma(a) \qquad \text{bzw.} \qquad \sigma.\big((\sigma^{-1}g).a\big) = g.(\sigma.a) \tag{1}$$

für alle $a \in A$ und alle $g \in G$ gilt. Daher definiert die Festlegung auf den Koketten von G mit Werten in A

$$(\sigma f)(g_1|\dots|g_n) := \sigma f(\sigma^{-1}g_1|\dots|\sigma^{-1}g_n)$$

einen Homomorphismus $H^n(G,A) \to H^n(G,A)$. Insbesondere ist der Randoperator Δ-invariant, d. h. daß für alle n-Koketten $f : G^n \to A$ gilt

$$\partial(\sigma f) = \sigma(\partial f).$$

Aus Satz (1.1.5) erhalten wir, daß Verbindungshomomorphismen Δ-invariant sind, d.h.

$$\delta(\sigma f) = \sigma(\delta f).$$

Auf den Koketten sieht man sofort, daß wir auf diese Weise eine Δ-Aktion auf den Kohomologiegruppen $H^n(G,A)$ erhalten.

Wir werden uns im Folgenden in einer der beiden Situationen des nächsten Satzes befinden.

(2.2.3) Satz. *(a) Sei G eine proendliche Gruppe auf der die endliche Gruppe Δ operiert. A sei eine diskrete abelsche Gruppe mit trivialer Operation von G und Δ.*

Dann erhalten wir eine Δ-Aktion auf den Kohomologiegruppen $H^n(G,A)$.

(b) Sei F eine proendliche Gruppe mit offenem Normalteiler $G \lhd F$, und A sei ein diskreter F-Modul. Wir nehmen an, daß die resultierende exakte Sequenz

$$1 \to G \to F \xrightarrow{\pi} \Delta \to 1$$

zerfällt, d.h. daß es einen Homomorphismus $\varphi : \Delta \to F$ mit $\pi \circ \varphi = id$ gibt. Dies ist z.B. der Fall, wenn G eine Pro-p-Gruppe und Δ eine q-Gruppe mit $p \neq q$ ist.

Dann operiert $\sigma \in \Delta$ auf G durch Konjugation mit $\varphi(\sigma)$ und auf A durch $\sigma.a := \varphi(\sigma).a$.

Ferner erhalten wir eine von der Wahl des Schnittes unabhängige Operation von Δ auf den Kohomologiegruppen $H^n(G,A)$.

Beweis. (a) Die Gültigkeit von (1) folgt direkt.
(b) Die ersten Aussagen sind klar. Die Gültigkeit von (1) sieht man aus

$$g.(\sigma.a) = g.(\varphi(\sigma).a) = \varphi(\sigma).\big((\varphi(\sigma^{-1})\, g\, \varphi(\sigma)).a\big) = \sigma.\big((\sigma^{-1}.g).a\big).$$

Die letzte Aussage folgt daraus, daß $H^i(G,\cdot)$ invariant unter der Aktion von G ist (vgl. [NSW], Proposition 1.6.2), und je zwei Schnitte $\varphi, \psi : \Delta \to F$ stets konjugiert sind. □

Im Folgenden betrachten wir Konsequenzen für die Abbildungen zwischen den Kohomologiegruppen. Wir setzen stets voraus, daß eine Δ-Aktion auf den Kohomologiegruppen vorliegt.

(2.2.4) Lemma. *Ist $\phi : G \to H$ ein Δ-invarianter Homomorphismus, der mit einem Δ-invarianten Homomorphismus $\theta : B \to A$ vom H-Modul B in den G-Modul A verträglich ist im Sinne der Bemerkung (1.1.4), so sind die resultierenden Homomorphismen $(\phi, \theta) : H^n(H, B) \to H^n(G, A)$ ebenfalls Δ-invariant.*

Beweis. Sei $\sigma \in \Delta$. Wegen

$$\begin{aligned}\big(\psi(\sigma f)\big)(g_1|\ldots|g_r) &= \theta\Big(\sigma f\big(\sigma^{-1}(\phi(g_1))|\ldots|\sigma^{-1}(\phi(g_r))\big)\Big)\\ &= \sigma\theta\Big(f\big(\phi(\sigma^{-1}g_1)|\ldots|\phi(\sigma^{-1}g_r)\big)\Big) \qquad = \Big(\sigma\big(\psi(f)\big)\Big)(g_1|\ldots|g_n),\end{aligned}$$

wobei wir zur Abkürzung $\psi := (\phi, \theta)$ gesetzt haben, ergibt sich die Behauptung. □

Das Lemma können wir insbesondere auf die Inflation und die Restriktion anwenden. Eine analoge Aussage gilt für die Homologie, so daß auch die Korestriktion Δ-invariant ist.

Aus seiner expliziten Beschreibung (z.B. in [N-KKT], S. 48) ersehen wir, daß der kanonische Isomorphismus

$$G^{ab} \cong \hat{H}^{-2}(G, \mathbb{Z})$$

für eine endliche Gruppe G ebenfalls Δ-invariant ist. Gleiches gilt für die Isomorphie

$$A^G/N_G A \cong \hat{H}^0(G, A).$$

Aus der Beschreibung des Cup-Produktes auf den Koketten (z. B. in [NSW], p. 35) schließen wir seine Δ-Invarianz

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

Auf diese Situation wird das folgende Lemma, dessen Beweis sich sofort durch Nachrechnen ergibt, Anwendung finden.

(2.2.5) Lemma. *Sei $\cup : A \times B \to C$ eine $\mathbb{Z}$-bilineare Abbildung der abelschen Gruppen A, B, C, auf denen die Gruppe Δ operiert. Ist $\cup$ Δ-invariant, so sind die induzierten Homomorphismen*

$$A \to Hom(B, C),\ a \mapsto (b \mapsto a \cup b)$$

und

$$A \to C,\ a \mapsto a \cup b$$

für festes $b \in B$ mit $\sigma b = b$ auch Δ-invariant.

Wir wollen uns ab hier auf den Fall $\Delta \cong \mathbb{Z}/2\mathbb{Z}$ spezialisieren. Dabei werde Δ von der Involution σ erzeugt. Die resultierende Aktion auf den Kohomologiegruppen ist dann entweder trivial oder auch eine Involution.

Ein weiterer wichtiger Homomorphismus von Kohomologiegruppen ist die *Transgression.* Der Beweis ihrer Δ-Invarianz erfordert eine genaue Analyse der Definition. Wir werden ihn im Folgenden in einem Spezialfall durchführen.

(2.2.6) Lemma. *Sei $p \neq 2$ und G eine Pro-p-Gruppe auf der die Involution σ operiert, sei $H \lhd G$ ein offener Normalteiler, X ein trivialer G-Modul, auf dem σ trivial operiere, und auf dem Multiplikation mit 2 ein Automorphismus ist.*

Dann ist die Transgression

$$tg : H^1(H, X)^{G/H} \to H^2(G/H, X)$$

ein σ-invarianter Homomorphismus.

Beweis. Wir spezialisieren die in [K-G], Abschnitt 3.7, bzw. in [NSW], Prop. 1.6.5, gegebene explizite Beschreibung der Transgression auf unseren Fall und verfolgen die σ-Aktion.

Wir gehen aus von einem 1-Kozyklus $\overline{a} \in H^1(H,X)^{G/H}$ und einem Vertreter $a \in \overline{a}$, welcher im speziellen Fall des trivialen Moduls X ein Homomorphismus ist. a wird nach Voraussetzung unter der Konjugation mit Elementen aus G fixiert:

$$a(g^{-1}hg) = a(h) \quad \text{für alle } g \in G \text{ und alle } h \in H.$$

Daher gilt speziell:

$$a(g_1g_2) = a(g_2g_1) \quad \text{für alle } g_1, g_2 \in G \text{ mit } g_1g_2 \in H.$$

Wir wählen einen Schnitt $s : G/H \to G$ mit $s(0) = 0$. Dann schreibt sich $g \in G$ eindeutig als $g = s(\gamma) \cdot h$ mit $\gamma \in G/H$ und $h \in H$. Damit definieren wir eine 1-Kokette $b : G \to X$ durch

$$b(g) = b(s(\gamma) \cdot h) := a(h) + b(s(\gamma)).$$

Wir setzen dabei $b(s(0)) = b(0) = 0$. Daher ist die Einschränkung von b auf H gleich a. Für jede Auswahl der anderen Werte von $b(s(\gamma))$ gilt

$$b(g+h) = b(s(\gamma) \cdot h_1 \cdot h) = a(h_1 \cdot h) = a(h_1) + a(h) = b(g) + a(h)$$

für alle $g \in G$ und alle $h \in H$. Wir definieren die Funktion

$$\varphi_a : G/H \to X,\ \gamma \mapsto \frac{1}{2} a\big(s(\sigma\gamma)^{-1} \cdot \sigma s(\gamma)\big),$$

für die gilt

$$\begin{aligned} \varphi_a(\sigma\gamma) &= a\big(s(\gamma)^{-1} \cdot \sigma s(\sigma\gamma)\big) = (\sigma a)\big(\sigma s(\gamma)^{-1} \sigma s(\gamma)\big) \\ &= -(\sigma a)\big(s(\sigma\gamma)^{-1} \cdot \sigma s(\gamma)\big) \qquad\qquad = -\varphi_{\sigma a}(\gamma). \end{aligned}$$

Da die Transgression ein Homomorphismus ist und nach Voraussetzung die direkte Zerlegung

$$H^1(H,X)^{G/H} = (H^1(H,X)^{G/H})^+ \oplus (H^1(H,X)^{G/H})^-$$

existiert, können wir uns im Folgenden auf die Fälle $\sigma a = a$ oder $\sigma a = -a$ zurückziehen. Wir schreiben dann suggestiv $\frac{\sigma a}{a} = \pm 1$. Es gilt damit

$$\varphi_{\sigma a} = \frac{\sigma a}{a} \varphi_a.$$

Wir definieren nun

$$b(s(\gamma)) := \frac{\sigma a}{a} \varphi_a(\gamma).$$

Dann gilt

$$(\sigma b)(g) = \frac{\sigma a}{a} b(g) \quad \text{für alle } g \in G,$$

was man der Rechnung

$$\begin{aligned} (\sigma b)(g) &= b\big(\sigma s(\gamma)\big) + (\sigma a)(h) = b\big(s(\sigma\gamma) s(\sigma\gamma)^{-1} \sigma s(\gamma)\big) + (\sigma a)(h) \\ &= b\big(s(\sigma\gamma)\big) + a\big(s(\sigma\gamma)^{-1} \cdot \sigma s(\gamma)\big) + (\sigma a)(h) = b\big(s(\sigma\gamma)\big) + 2\varphi_a(\gamma) + (\sigma a)(h) \\ &= \frac{\sigma a}{a} \varphi_a(\sigma\gamma) + 2\varphi_a(\gamma) + (\sigma a)(h) = -\frac{\sigma a}{a} \varphi_{\sigma a}(\gamma) + 2\varphi_a(\gamma) + (\sigma a)(h) \\ &= \varphi_a(\gamma) + (\sigma a)(h) = \frac{\sigma a}{a} b(g). \end{aligned}$$

entnimmt. Damit ist gezeigt, daß die Zuordnung $a \mapsto b$ invariant unter σ ist.

Wir erhalten nun einen 2-Kozykel $f : G \times G \to X$ durch die Festlegung

$$f(g_1, g_2) := (\partial b)(g_1, g_2) = b(g_1) + b(g_2) - b(g_1 g_2).$$

Wir hatten bereits gesehen, daß der Randoperator σ-invariant ist, woraus sich ergibt, daß auch die Zuordnung $a \mapsto f$ unter σ invariant ist.

Der Kozykel f ist so konstruiert, daß er nur von den Nebenklassen $s(\gamma) + H$ abhängt, was man folgender Rechnung entnimmt:

$$\begin{aligned} f(g_1 \cdot h_1, g_2 \cdot h_2) &= b(g_1 \cdot h_1) + b(g_2 \cdot h_2) - b(g_1 \cdot h_1 \cdot g_2 \cdot h_2) \\ &= f(g_1, g_2) + a(h_1) + a(h_2) - a(h_1 \cdot h_2)) \qquad = f(g_1, g_2). \end{aligned}$$

Somit erhalten wir also einen 2-Kozykel $\overline{f} \in H^2(G/H, X)$. Nach [NSW], Prop. 1.6.5, wird die Transgression durch die Zuordnung $\overline{a} \mapsto \overline{f}$ gegeben, welche sich also als σ-invariant herausgestellt hat. □

Unsere bisherigen Überlegungen fließen ein in den

(2.2.7) Satz. *Sei G eine proendliche Gruppe, $H \lhd G$ ein abgeschlossener Normalteiler und X ein G-Modul. Dann gilt:*

(a) Die Fünf-Terme-Sequenz

$$0 \to H^1(G/H, X^H) \xrightarrow{inf} H^1(G, X) \xrightarrow{res} H^1(H, X)^{G/H} \xrightarrow{tg} H^2(G/H, X^H) \xrightarrow{inf} H^2(G, X)$$

ist exakt.

(b) Ist $H \lhd G$ offen, G eine Pro-p-Gruppe für $p \neq 2$, X ein trivialer G-Modul, auf dem Multiplikation mit 2 ein Isomorphismus ist, und operiert die Involution σ auf G (und trivial auf X), so ist die Sequenz aus (a) σ-invariant.

Beweis. Für (a) zitieren wir [NSW], Prop. 1.6.6. Die Aussage (b) folgt aus Lemma (2.2.4) angewendet auf die Inflation und die Restriktion und aus Lemma (2.2.6). □

Der folgende Satz faßt wichtige von uns benötigte Resultate zur σ-Aktion auf den Kohomologiegruppen zusammen.

(2.2.8) Satz. *Seien A und B abelsche proendliche Gruppen, versehen mit der Operation einer Involution σ, wobei wir $A = A^+$ und $B = B^-$ fordern.*

(a) Für alle trivialen diskreten B-Moduln X mit trivialer σ-Aktion und alle i gilt:

$$H^i(A, X) = H^i(A, X)^+.$$

(b) Für alle trivialen diskreten B-Moduln X mit trivialer σ-Aktion gilt:

$$H^1(B, X) = H^1(B, X)^-.$$

(c) Ist B eine zyklische Pro-p-Gruppe für $p \neq 2$, dann gelten

$$H^2(A, \mathbb{Z}/p\mathbb{Z}) = H^2(A, \mathbb{Z}/p\mathbb{Z})^+ \qquad \text{und} \qquad H^2(B, \mathbb{Z}/p\mathbb{Z}) = H^2(B, \mathbb{Z}/p\mathbb{Z})^-.$$

Beweis. (a) und (b) und die erste Aussage von (c) sind klar.

Für (c) betrachten wir das Ende der Fünf-Terme-Sequenz aus Satz (2.2.7) bzgl. der Darstellung $1 \to R \to \mathbb{Z}_p \to B \to 1$:

$$H^1(R, \mathbb{Z}/p\mathbb{Z})^B \xrightarrow{\text{tg}} H^2(B, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\text{inf}} H^2(\mathbb{Z}_p, \mathbb{Z}/p\mathbb{Z}).$$

Wir setzen die Aktion von σ auf $\mathbb{Z}_p$ fort, d.h. $\mathbb{Z}_p = (\mathbb{Z}_p)^-$. Dann gilt offensichtlich $R = R^-$. Da $\mathbb{Z}_p$ frei ist, gilt $H^2(\mathbb{Z}_p, \mathbb{Z}/p\mathbb{Z}) = 0$, und wir erhalten somit den σ-invarianten Isomorphismus

$$H^1(R, \mathbb{Z}/p\mathbb{Z})^B \to H^2(B, \mathbb{Z}/p\mathbb{Z}).$$

Da nach (b) aber $H^1(R, \mathbb{Z}/p\mathbb{Z}) = H^1(R, \mathbb{Z}/p\mathbb{Z})^-$ gilt, folgt die Aussage. □

2.2.3. Pro-p-Gruppen mit Aktion einer Involution

Wir stellen zunächst einige wichtige Kommutatorrelationen zusammen.

(2.2.9) Lemma. *Sei G eine Gruppe und bezeichne $G^{(n)}$ die von den n-fachen Kommutatoren erzeugte Untergruppe.*

(a) Für alle $x, y, z \in G$ gilt:

$$[x, yz] = [x, y][x, z][[x, y], z].$$

(b) Für alle $x, y \in G$ und alle $n \in \mathbb{N}$ gilt:

$$(xy)^n \equiv x^n y^n [x, y]^{\frac{n(n-1)}{2}} \ (modulo\ G^{(3)}).$$

(c) Für alle $x \in G^{(n)}$, alle $y \in G$ und alle $a, b \in \mathbb{N}$ gilt:

$$[x^a, y^b] \equiv [x, y]^{(ab)} \ (modulo\ G^{(n+2)}).$$

Sei p eine ungerade Primzahl. Wir haben gesehen, daß $dim_{\mathbb{F}_p} H^1(G)$ als minimale Erzeugerzahl von G interpretiert werden kann. Genauer gibt die Dimension des Plus- bzw. des Minusteils von $H^1(G)$ die minimale Erzeugerzahl des Plus- bzw. des Minusteils der Abelisierung von G an.

(2.2.10) Lemma. *Sei G eine endlich erzeugte Pro-p-Gruppe. Dann gilt:*

$$d(G)^{\pm} = dim_{\mathbb{F}_p} H^1(G)^{\pm} = d((G/G_2)^{\pm}) = d((G^{ab})^{\pm}).$$

Beweis. Die erste Gleichheit wollen wir als Definition von $d(G)^{\pm}$ verstehen. Es gilt nach Lemma (2.2.1)

$$Hom((G/G_2)^{\pm}, \mathbb{Z}/p\mathbb{Z}) = Hom(G/G_2, \mathbb{Z}/p\mathbb{Z})^{\pm},$$

woraus die zweite Gleichheit folgt. Wegen $Hom(G^{ab}, \mathbb{Z}/p\mathbb{Z}) = Hom(G/G_2, \mathbb{Z}/p\mathbb{Z})$ erhalten wir die dritte aus dem Diagramm

$$\begin{array}{ccccc}
G^{ab} & = & (G^{ab})^+ & \oplus & (G^{ab})^- \\
\downarrow & & \downarrow & & \downarrow \\
G/G_2 & = & (G/G_2)^+ & \oplus & (G/G_2)^-,
\end{array}$$

in dem alle Pfeile Surjektionen sind. □

(2.2.11) Lemma. *Sei G eine endlich erzeugte Pro-p-Gruppe, auf der eine Involution σ operiert, so daß $d(G)^+ = 0$ gilt. Dann operiert σ auf $G^{(n)}/G^{(n+1)}$ als Identität, falls n gerade ist, und als Inversion, falls n ungerade ist. Dabei bezeichne $G^{(n)}$ wiederum das Erzeugnis der n-fachen Kommutatoren.*

Beweis. Den Beweis führen wir per Induktion nach n. Nach Voraussetzung ist

$$G/\overline{G^p[G,G]} = (G/\overline{G^p[G,G]})^-.$$

Nun betrachten wir die natürliche Projektion

$$(G/\overline{[G,G]})^+ \twoheadrightarrow (G/\overline{G^p[G,G]})^+ = (G/\Phi(G))^+,$$

deren Bild trivial ist. Die Anzahl der Erzeugenden von $(G/\overline{[G,G]})^+$ ist somit 0, und $G/\overline{[G,G]}$ ist gleich $(G/\overline{[G,G]})^-$, was den Induktionsanfang darstellt.

Sei die Aussage nun für n bereits bewiesen. Wähle $x \in G^{(n)}$ und $y \in G$. Dann ist

$$\sigma[x, y] \equiv [\sigma x, y^{-1}] \text{ (modulo } G^{(3)}).$$

Modulo $G^{(n+1)}$ ist σx entweder x oder x^{-1} je nach dem, ob n gerade oder ungerade ist. Aus Lemma (2.2.9) (c) erhalten wir

$$[x, y^{-1}] \equiv [x, y]^{-1} \text{ (modulo } G^{(n+2)}) \text{ und } [x^{-1}, y^{-1}] \equiv [x, y] \text{ (modulo } G^{(n+2)}).$$

Daraus folgt der Induktionsschritt. □

(2.2.12) Bemerkung. *Sei G eine endlich erzeugte Pro-p-Gruppe, auf der eine Involution σ operiert. Dann ist die exakte Sequenz*

$$0 \to ({}_pG^{ab})^\vee \to H^2(G) \to {}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p) \to 0.$$

aus Satz (2.1.8) σ-invariant.

Beweis. Da diese Sequenz aus einer langen exakten Sequenz zu einer trivialerweise σ-invarianten kurzen exakten Sequenz gewonnen wurde, ist sie selbst σ-invariant. □

Es gilt der folgende Spezialfall der *Künneth-Formel.*

(2.2.13) Satz. *(a) Seien G, H endliche Gruppen und B ein bzgl. G und H trivialer Modul. Dann gilt:*

$$H^2(G \times H, B) = H^2(G, B) \oplus H^2(H, B) \oplus (H^1(G, B) \otimes H^1(H, B)).$$

(b) Seien G_i für $i = 1, \ldots, n$ endliche Gruppen und B ein bzgl. aller G_i trivialer Modul. Dann gilt:

$$H^2(\prod_{i=1}^n G_i, B) = \bigoplus_{i=1}^n H^2(G_i, B) \oplus \bigoplus_{i<j} (H^1(G_i, B) \otimes H^1(G_j, B)).$$

Sind die Gruppen G_i abelsch und operiert eine Involution σ auf ihnen, so ist die Zerlegung σ-invariant.

Beweis. (a) Dies folgt zum Beispiel aus [NSW], Ex. II.1.7. (b) folgt induktiv aus (a) unter Benutzung von

$$\begin{aligned} H^2((G_1 \times G_2) \times G_3, B) &= H^2(G_1 \times G_2, B) \oplus H^2(G_3, B) \oplus (H^1(G_1 \times G_2, B) \otimes H^1(G_3, B)) \\ &= \bigoplus_{i=1}^3 H^2(G_i, B) \oplus \bigoplus_{i<j} (H^1(G_i, B) \otimes H^1(G_j, B)) \end{aligned}$$

□

Die Künneth-Formel werden wir benutzen, um die Dimension von $H^2(G/G_2)^{\pm}$ zu bestimmen.

(2.2.14) Satz. *Sei G eine endlich erzeugte Pro-p-Gruppe.*

(a) Sei $d = d(G)$. Dann gilt:

$$dim_{\mathbb{F}_p} H^2(G/G_2) = \frac{d(d+1)}{2}.$$

(b) Operiert eine Involution σ auf G, so gilt genauer

$$\begin{aligned} dim_{\mathbb{F}_p} H^2(G/G_2)^+ &= d^+ + \binom{d^+}{2} + \binom{d^-}{2} \qquad \textit{und} \\ dim_{\mathbb{F}_p} H^2(G/G_2)^- &= d^- + d^+ \cdot d^-, \end{aligned}$$

wobei $d^+ = d(G)^+$ und $d^- = d(G)^-$ gesetzt wurde.

Beweis. (a) folgt aus (b), indem G mit der trivialen σ-Aktion versehen wird.

Aus Satz (2.2.2) erhalten wir eine σ-invariante Zerlegung

$$G/G_2 \cong A_1 \oplus \cdots \oplus A_{d^+} \oplus B_1 \oplus \cdots \oplus B_{d^-},$$

wobei die A_i und B_j Gruppen der Ordnung p sind, für die $A_i = A_i^+$ und $B_j = B_j^-$ gilt. Die Künneth-Zerlegung von $H^2(G/G_2)$ hat dann die Gestalt

$$\begin{aligned} H^2(G/G_2) \;\cong\; & \bigoplus_{i=1}^{d^+} H^2(A_i) \;\oplus \bigoplus_{i<j} H^1(A_i) \otimes H^1(A_j) \;\oplus \bigoplus_{i<j} H^1(B_i) \otimes H^1(B_j) \\ & \oplus \bigoplus_{i=1}^{d^+} \bigoplus_{j=1}^{d^-} (H^1(A_i) \otimes H^1(B_j)) \;\oplus \bigoplus_{j=1}^{d^-} H^2(B_j), \end{aligned}$$

wobei nach Satz (2.2.8) σ auf der ersten Zeile als Identität und auf der zweiten als Inversion operiert. Sowohl die Erzeugenden- als auch die Relationenzahl von $\mathbb{Z}/p\mathbb{Z}$ ist 1, weshalb sich die Behauptung durch Abzählen der Dimensionen ergibt. $\square$

2.2.4. Potenzreiche Pro-p-Gruppen mit Aktion einer Involution

Sei p eine ungerade Prizahl. Wir kommen nun zu einem Resultat, das für die Betrachtung der Galois-Gruppen von CM-Körpern von Nutzen sein wird (vgl. [W], Proposition 2.1).

(2.2.15) Satz. *Sei G eine endlich erzeugte potenzreiche Pro-p-Gruppe, auf welcher eine Involution σ operiert. Ist $d(G^+) = 0$, dann ist G abelsch.*

Beweis. Wegen $d(G^+) = 0$ erhalten wir aus Lemma (2.2.11), daß σ als Inversion auf $G/[G,G]$ und als Identität auf $[G,G]/[G,G,G]$ operiert. Letzteres impliziert insbesondere

$$[G,G]/H = ([G,G]/H)^+,$$

wobei $H = [G,G]^p[G,G,G]$ gesetzt wurde.

Sei $x \in G$. Dann gibt es ein $r \in [G,G]$ mit $\sigma x = x^{-1}r$. Wir berechnen nun die σ-Aktion auf auf G^pH/H:

$$\sigma x^p = (\sigma x)^p = (x^{-1}r)^p \equiv x^{-p} \text{ (modulo } H),$$

wobei die Rechenregel (b) von Lemma (2.2.9) benutzt wurde. Also gilt

$$G^pH/H = (G^pH/H)^-.$$

Da G potenzreich ist, erhalten wir die Inklusion

$$([G,G]/H)^+ = [G,G]/H \subseteq G^pH/H = (G^pH/H)^-,$$

woraus folgt, daß $[G,G]/H$ trivial ist.

Setzt man $K = K^{(1)} = [G,G]$ und $K^{(n+1)} = (K^{(n)})^p[K^n, G]$, d.h. $K^{(2)} = H$, so folgt aus Satz (2.1.13) (a), daß die $K^{(i)}$ echt zur 1 absteigen. Wegen $K^{(1)} = K^{(2)}$ muß daher $K^{(1)}$, also $[G,G]$, trivial sein. $\square$

Relationen in potenzreichen Pro-p-Gruppen

Aus der (σ-invarianten) exakten Sequenz

$$0 \to H^1(G/G_2) \xrightarrow{\sim} H^1(G) \xrightarrow{0} H^1(G_2)^G \xrightarrow{\text{tg}} H^2(G/G_2) \xrightarrow{\text{inf}} H^2(G)$$

(vgl. Satz (2.2.7)) und Satz (2.2.14) ersehen wir sofort, daß bei einer endlich erzeugten potenzreichen Pro-p-Gruppe G stets

$$r(G) \geq \binom{d(G)}{2}$$

gilt, da $d(G_2) \leq d(G)$ ist. Stärker noch gilt das

(2.2.16) Theorem. *Sei G eine endlich erzeugte potenzreiche Pro-p-Gruppe. Dann gilt:*

$$\binom{d(G)}{2} \leq r(G) \leq \binom{d(G)}{2} + d(G) - dim(G).$$

Insbesondere gilt daher

$$r(G) = \binom{d(G)}{2},$$

falls G uniform ist.

Beweis. Wir führen den gruppentheoretischen Beweis, wie er sich in [DDMS], Theorem 4.35, findet.

Wir setzen $d_i := (G_i : G_{i+1})$. Da G potenzreich ist, erhalten wir eine absteigende Kette

$$l := d(G) = d_1 \geq d_2 \geq \cdots \geq d_k = dim(G),$$

so daß G_k uniform ist.

Nach [DDMS], Theorem 3.6, gibt es ein Erzeugendensystem $\{x_1, \ldots, x_l\}$ von G, so daß die Menge $\{x_1^{p^{i-1}}, \ldots, x_{d_i}^{p^{i-1}}\}$ ein Erzeugendensystem von G_i bildet.

Wir wollen im Folgenden ein Relationensystem von G bzgl. $\{x_1, \ldots, x_l\}$ angeben. Sei dazu F die freie Pro-p-Gruppe auf der Menge $\{x_1, \ldots, x_l\}$, dann suchen wir also eine exakte Sequenz

$$0 \to R \to F \to H \to 0$$

mit $G \cong H$.

Zunächst nehmen wir in R Relationen auf, die garantieren, daß H eine potenzreiche Gruppe ist. In G gilt für $1 \leq i < j \leq l$

$$[x_i, x_j] x_1^{\lambda_1(i,j)} x_2^{\lambda_2(i,j)} \ldots x_l^{\lambda_l(i,j)} = 1$$

mit gewissen $\lambda_r(i,j) \in p\mathbb{Z}_p$, da die Kommutatoruntergruppe in den p-ten Potenzen enthalten ist.

Außerdem wollen wir erreichen, daß $|H/H_n| \leq |G/G_n|$ ist, das heißt, daß die Indizes in H mindestens so schnell absteigen wie die in G. Dieses ist dadurch charakterisiert, daß sich für $d_i \geq m > d_{i+1}$ das Element $x_m^{p^i}$ mit den d_{i+1} Erzeugern von G_{i+1} schreiben läßt, es also $\mu_r(m) \in p^i\mathbb{Z}_p$ gibt mit

$$x_m^{p^{-i}} x_1^{\mu_1(m)} x_2^{\mu_2(m)} \ldots x_{d_{i+1}}^{\mu_{d_{i+1}}(m)} = 1.$$

Definieren wir also nun R als den kleinsten abgeschlossenen Normalteiler von F, der die $\binom{l}{2} + l - dim(G)$ Elemente

$$[x_i, x_j] x_1^{\lambda_1(i,j)} x_2^{\lambda_2(i,j)} \ldots x_l^{\lambda_l(i,j)} \qquad \text{und} \qquad x_m^{p^{-i}} x_1^{\mu_1(m)} x_2^{\mu_2(m)} \ldots x_{d_{i+1}}^{\mu_{d_{i+1}}(m)}$$

enthält, so ist H eine potenzreiche Gruppe mit $|H/H_n| \leq |G/G_n|$.

Nun haben wir aber auch eine Projektion

$$\pi : H \twoheadrightarrow G,$$

da die Relationen von H auch in G erfüllt sind. Außerdem gilt $\pi(H_n) = G_n$. Deswegen erhalten wir via π Isomorphismen

$$H/H_n \cong G/G_n.$$

Ein Element aus dem Kern von π liegt daher im Durchschnitt aller H_n, welcher aber 1 ist. Daher ist H zu G isomorph, und die rechte Ungleichung ist bewiesen. □

Aus diesem mit gruppentheoretischen Mitteln erhaltenen Ergebnis ziehen wir Konsequenzen für die Kohomologiegruppen.

(2.2.17) Korollar. *Sei G eine endlich erzeugte uniforme Pro-p-Gruppe. Dann ist $H^1(G_2)^G = H^1(G_2)$ und die Sequenz*

$$0 \to H^1(G_2) \xrightarrow{tg} H^2(G/G_2) \xrightarrow{inf} H^2(G) \to 0$$

ist exakt.

Beweis. Wir müssen die Surjektivität der Inflation zeigen. Es ist (vgl. Satz (2.2.14))

$$dim_{\mathbb{F}_p}(im(\mathrm{inf})) = dim_{\mathbb{F}_p} H^2(G/G_2) - dim_{\mathbb{F}_p} H^1(G_2)^G \geq d(G) + \binom{d(G)}{2} - d(G_2) \geq \binom{d(G)}{2}.$$

Nach Theorem (2.2.16) gilt aber $dim_{\mathbb{F}_p} H^2(G) = \binom{d(G)}{2}$, weshalb die Behauptungen folgen. □

Hieraus können wir nun die Dimensionen des Plus- und des Minusteils von $H^2(G)$ berechnen.

(2.2.18) Korollar. *Sei G eine endlich erzeugte uniforme Pro-p-Gruppe, auf der eine Involution σ operiert. Dann gelten*

$$dim_{\mathbb{F}_p} H^2(G)^+ = \binom{d(G)^+}{2} + \binom{d(G)^-}{2} \qquad \textit{und}$$
$$dim_{\mathbb{F}_p} H^2(G)^- = d(G)^+ \cdot d(G)^-.$$

Beweis. Die exakte Sequenz aus Korollar (2.2.17) ist σ-invariant (vgl. Satz (2.2.7)). Das Ergebnis folgt deshalb sofort aus Satz (2.2.14). □

(2.2.19) Korollar. *Sei G eine endlich erzeugte uniforme Pro-p-Gruppe. Ist $d(G) = 1$ oder $d(G) = 2$, dann hat G^{ab} die Gruppe $\mathbb{Z}_p$ als Quotienten.*

Beweis. Ist $d(G) = 1$, so folgt nach Theorem (2.2.16), daß $r(G) = \binom{1}{2} = 0$ ist. Daher ist G eine freie Pro-p-Gruppe mit einem Erzeuger. Folglich ist $G = G^{ab}$ isomorph zu $\mathbb{Z}_p$.

Im Fall $d(G) = 2$ ist der Relationenrang $r(G) = \binom{2}{2} = 1$, und Satz (2.1.7) liefert das Ergebnis. □

Erzeugende in potenzreichen Pro-p-Gruppen

(2.2.20) Lemma. *Sei G eine endlich erzeugte potenzreiche Pro-p-Gruppe, auf der eine Involution σ operiert. Dann gilt für alle $i \in \mathbb{Z}$:*

$$d(G)^{\pm} \geq d(G_i)^{\pm}.$$

Beweis. Die Potenzierung mit p^i gibt eine σ-invariante Surjektion

$$G/G_2 \twoheadrightarrow G_i/G_{i+1} = G_i/(G_i)_2.$$

Lemma (2.2.10) liefert nun das Ergebnis. □

Nun kommen wir zu einem wichtigen Resultat aus [W] (Proposition 2.3) über die Beziehung der Plus- und Minusteile von $H^1(G)$, also von $d(G)^+$ zu $d(G)^-$.

(2.2.21) Satz. *Sei G eine potenzreiche Pro-p-Gruppe mit Aktion einer Involution σ. Dann gelten:*

(a) $\binom{d(G)^+}{2} + \binom{d(G)^-}{2} \leq d(G)^+ + dim_{\mathbb{F}_p}\, {}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^+$,

(b) $d(G)^+ \cdot d(G)^- \leq d(G)^- + dim_{\mathbb{F}_p}\, {}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^-$.

Ist G uniform mit endlicher Abelisierung, dann gilt in beiden Fällen Gleichheit.

Beweis. Aus dem Endstück der σ-invarianten exakten Sequenz (vgl. Satz (2.2.7))

$$0 \to H^1(G_2)^G \xrightarrow{\text{tg}} H^2(G/G_2) \xrightarrow{\text{inf}} H^2(G)$$

und Bemerkung (2.2.12) erhalten wir die Ungleichung

$$dim_{\mathbb{F}_p} H^2(G/G_2)^{\pm} \leq d(G_2)^{\pm} + dim_{\mathbb{F}_p} ({}_pG^{ab})^{\pm} + dim_{\mathbb{F}_p} {}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^{\pm}.$$

Da G potenzreich ist, gilt nach Lemma (2.2.20) $d(G_2)^{\pm} \leq d(G)^{\pm}$. Aus Satz (2.1.9) schließen wir weiter die Ungleichung

$$dim_{\mathbb{F}_p} ({}_pG^{ab})^{\pm} = d(G)^{\pm} - rk_{\mathbb{Z}_p}(G^{ab})^{\pm} \leq d(G)^{\pm},$$

so daß wir

$$dim_{\mathbb{F}_p} H^2(G/G_2)^{\pm} \leq 2d(G)^{\pm} + dim_{\mathbb{F}_p} {}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^{\pm}$$

bekommen. Setzen wir nun die Dimension von $H^2(G/G_2)^{\pm}$ ein, die in Satz (2.2.14) berechnet wurde, so folgt das Resultat.

Benutzen wir Korollar (2.2.17) und $d(G_i)^{\pm} = d(G)^{\pm}$, so erhalten wir im Falle einer uniformen Gruppe mit endlicher Abelisierung Gleichheiten. □

Es ist von Interesse, Fälle zu kennen, in denen ${}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^-$ trivial ist. Dies trifft zumindest für $d(G)^+ = 1$ und für $d(G)^- = 0$ zu, falls G uniform mit endlicher Abelisierung ist.

Wegen $\binom{3}{2} = 3$ und Theorem (2.2.16) stellt der Fall uniformer Gruppen mit $d(G) = 3$ eine Besonderheit dar, denn der Erzeugendenrang ist gleich dem Relationenrang. Daraus erhält man Einschränkungen für die Plus- und Minusteile. Das wird von großem Interesse für uns sein, da die potenzreichen Galois-Gruppen von CM-Körpern, die wir betrachten werden, Erzeugendenrang kleiner oder gleich 3 besitzen.

(2.2.22) Satz. *Sei G eine uniforme Pro-p-Gruppe, auf der eine Involution σ operiert. Es sei $d(G) \leq 3$, und die Abelisierung von G sei endlich. Dann gilt*

$$d(G)^+ = 1 \quad \textit{und} \quad d(G)^- = 2$$

oder

$$d(G)^+ = 3 \quad \textit{und} \quad d(G)^- = 0.$$

Beweis. Wegen Korollar (2.2.19) kann nur der Fall $d(G) = 3$ auftreten. Da $3 = r(G) = d(G) = dim_{\mathbb{F}_p} {}_pG^{ab} = dim_{\mathbb{F}_p} H^2(G)$ aus den Voraussetzungen folgt, erhalten wir aus Bemerkung (2.2.12) die σ-invariante Isomorphie

$$({}_pG^{ab})^{\vee} \cong H^2(G)$$

und daher aus Korollar (2.2.18)

$$d(G)^- = dim_{\mathbb{F}_p} H^2(G)^- = d(G)^+ \cdot d(G)^-,$$

woraus sich die Behauptung ergibt. □

2.3. Zu CM-Körpern

2.3.1. CM-Körper

In diesem Abschnitt wollen wir grundlegende Eigenschaften von CM-Körpern zusammenstellen.

(2.3.1) Definition. *Sei k ein Zahlkörper.*

- *k heißt* total reell*, falls das Bild aller Einbettungen $k \hookrightarrow \mathbb{C}$ in $\mathbb{R}$ enthalten ist.*

  Zu jedem Zahlkörper K gibt es einen maximalen total reellen Teilkörper, den wir stets mit K^+ bezeichnen wollen.

- *k heißt* total imaginär*, falls das Bild keiner Einbettung $k \hookrightarrow \mathbb{C}$ in $\mathbb{R}$ enthalten ist.*

- *k heißt* CM-Körper*, falls k total imaginär und eine quadratische Erweiterung seines maximalen total reellen Teilkörpers k^+ ist.*

Wir betrachten zunächst das wichtige

(2.3.2) Beispiel. *Sei $n > 2$. $\mathbb{Q}(\zeta_n)$ ist ein CM-Körper mit maximalem total reellem Teilkörper $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.*

Sei k ein CM-Körper und $\alpha : k \hookrightarrow \mathbb{C}$ eine Einbettung. Die Galois-Gruppe $G(k|k^+)$ wird erzeugt von dem Element

$$\sigma : x \mapsto \alpha^{-1}(\overline{\alpha(x)}) =: \overline{x},$$

welches nicht von der Auswahl der Einbettung abhängt. Wir nennen den Erzeuger von $G(k|k^+)$ auch *komplexe Konjugation.*

Sei $K^+|k^+$ eine galoissche Erweiterung total reeller Zahlkörper. Dann folgt aus dem Translationssatz der Galois-Theorie, daß $K := K^+k|K^+$ ein CM-Körper ist, und die Einschränkung einen Isomorphismus $G(K|k) \cong G(K^+|k^+)$ ergibt.

(2.3.3) Lemma. *Sei k ein CM-Körper, $\sigma \in G(k|k^+)$ die komplexe Konjugation, und sei $K|k^+$ eine galoissche Erweiterung, die k enthält. Der Grad $[K : k]$ werde nicht von 2 geteilt. Durch Auswahl von $\tilde{\sigma} \in G(K|k^+)$ mit $\tilde{\sigma}|_k = \sigma$ definieren wir eine Aktion von σ auf $G(K|k)$ durch Konjugation mit $\tilde{\sigma}$.*

Die Aktion auf den Kohomologiegruppen $H^i(G(K|k), A)$ für einen $G(K|k^+)$-Modul A ist unabhängig von der Auswahl von $\tilde{\sigma}$. Dabei operiere σ auf A durch $\sigma.a := \tilde{\sigma}.a$.

Außerdem ist die induzierte Aktion von σ auf $G(K^{ab}|k)$ unabhängig von der Auswahl von $\tilde{\sigma}$, wobei K^{ab} die maximale abelsche Teilerweiterung von K über k bezeichne.

Beweis. Die Forderung an den Grad stellt sicher, daß die Gruppenerweiterung $1 \to G(K|k) \to G(K|k^+) \to G(k|k^+) \to 1$ zerfällt. Dann folgt die erste Aussage aus Satz (2.2.3) (b).

Seien $\tilde{\sigma}$ und $\tilde{\tau}$ zwei Elemente aus $G(K^{ab}|k^+)$ mit $\tilde{\sigma}|_k = \sigma = \tilde{\tau}|_k$. Dann ist $\tilde{\sigma}\tilde{\tau}^{-1}$ ein Element der abelschen Gruppe $G(K^{ab}|k)$, mit dem Konjugation trivial ist. □

(2.3.4) Korollar. *Ist $K|k$ eine galoissche Erweiterung, wobei K und k CM-Körper seien. Dann liefert die Einschränkung der k-Automorphismen von K auf K^+ eine Isomorphie*

$$G(K|k) \cong G(K^+|k^+).$$

Falls ferner $K|k$ abelsch, $K|k^+$ galoissch ist, und der Grad $[K : k]$ nicht von 2 geteilt wird, dann operiert die komlexe Konjugation trivial auf $G(K|k)$.

Beweis. Die erste Aussage folgt, da $K = kK^+$ ist. σ operiert auf $G(K^+|k^+)$ als Konjugation mit $\tilde{\sigma}|_{K^+}$ für eine beliebige Fortsetzung $\tilde{\sigma}$ von σ auf $G(K|k^+)$. Wenn $G(K^+|k^+)$ abelsch ist, ist die Operation trivial, welche aufgrund der Voraussetzung an den Grad definiert ist. □

2.3.2. Zur Kohomologie- und Klassenkörpertheorie von CM-Körpern

Das zentrale Resultat in diesem Abschnitt ist die Kompatibilität der Invariantenabbildung eines CM-Körpers mit der Aktion der komplexen Konjugation. Daraus können wir die Kompatibilität des Reziprozitätshomomorphismus und des Isomorphismus aus dem Satz von Nakayama-Tate mit der komplexen Konjugation schließen.

(2.3.5) Satz. *Sei k ein CM-Körper mit maximalem total reellem Teilkörper k^+, und bezeichne σ die komplexe Konjugation. Sei $L|k^+$ eine galoissche Erweiterung, derart daß k in L enthalten ist, und der Grad $[L:k]$ nicht von 2 geteilt wird.*

Dann ist die Invariantenabbildung

$$inv : H^2(G(L|k), \mathcal{C}_L) \xrightarrow{\sim} \frac{1}{[L:k]}\mathbb{Z}/\mathbb{Z}$$

ein σ-invarianter Isomorphismus, wobei die Aktion von σ auf $\frac{1}{[L:k]}\mathbb{Z}/\mathbb{Z}$ die triviale sei.

Beweis. Es ist ein fundamentales Resultat der globalen Klassenkörpertheorie, daß die Invariantenabbildung stets ein Isomorphismus ist. Sei $\tilde{\sigma} \in G(L|k^+)$ eine Fortsetzung von σ, es gelte also $\tilde{\sigma}|_k = \sigma$. Dann ist nach [NSW], Proposition 1.6.2, die Gruppe $H^2(G(L|k^+), \mathcal{C}_L)$ invariant unter Konjugation mit $\tilde{\sigma}$, welches gerade die Aktion von σ ist. Nun liefert die Korestriktion aufgrund des kommutativen Diagrammes (vgl. [N-KKT], Satz II.1.4 (c))

$$\begin{array}{ccc} H^2(G(L|k), \mathcal{C}_L) & \xrightarrow{\text{cor}} & H^2(G(L|k^+), \mathcal{C}_L) \\ {\scriptstyle \text{inv}}\downarrow & & {\scriptstyle \text{inv}}\downarrow \\ \frac{1}{[L:k]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\text{Einbettung}} & \frac{1}{[L:k^+]}\mathbb{Z}/\mathbb{Z}, \end{array}$$

daß die Korestriktion injektiv ist, woraus sich die Behauptung unmittelbar ergibt. □

Wir kommen nun zu den bereits erwähnten Anwendungen.

(2.3.6) Korollar. *Sei k ein CM-Körper mit maximalem total reellem Teilkörper k^+, und bezeichne σ die komplexe Konjugation. Sei $L|k^+$ eine galoissche Erweiterung, derart daß k in L enthalten ist, und der Grad $[L:k]$ nicht von 2 geteilt wird.*

Dann bildet der Reziprozitätshomomorphismus die exakte Sequenz

$$1 \to N_{G(L|k)}\mathcal{C}_L \to \mathcal{C}_k \xrightarrow{\textit{Reziprozität}} G(L|k)^{ab} \to 1$$

mit σ-invarianten Homomorphismen.

Beweis. Setze $G := G(L|k)$. Der Reziprozitätshomomorphismus ergibt sich aus den Isomorphien

$$G^{ab} \to \hat{H}^{-2}(G, \mathbb{Z}) \xrightarrow{\cup\gamma} \hat{H}^0(G, \mathcal{C}_L) \to \mathcal{C}_k/N_G\mathcal{C}_L,$$

wobei $\gamma \in H^2(G, \mathcal{C}_L)$ eine Fundamentalklasse sei. Da σ auf dieser nach Satz (2.3.5) trivial operiert, ist der mittlere Isomorphismus nach Satz (2.2.5) σ-invariant. Diese Eigenschaft hatten wir von den anderen beiden Isomorphismen bereits nachgeprüft. □

(2.3.7) Korollar. *Sei k ein CM-Körper mit maximalem total reellem Teilkörper k^+, und bezeichne σ die komplexe Konjugation. Sei $L|k^+$ eine galoissche Erweiterung, derart daß k in L enthalten ist, und der Grad $[L:k]$ nicht von 2 geteilt wird.*

Dann liefert der Satz von Nakayama-Tate (1.1.24) einen σ-invarianten Isomorphismus

$$\hat{H}^i(G(L|k), \mathcal{C}_L) \cong \hat{H}^{2-i}(G(L|k), \mathbb{Z})^\vee$$

für alle $i \in \mathbb{Z}$.

Beweis. Der Homomorphismus entsteht aus dem Cupprodukt

$$\hat{H}^i(G(L|k), \mathcal{C}_L) \times \hat{H}^{2-i}(G(L|K), \mathbb{Z}) \xrightarrow{\cup} H^2(G(L|k), \mathcal{C}_L) \xrightarrow{\text{inv}} \frac{1}{[L:k]}\mathbb{Z}/\mathbb{Z}.$$

Die Behauptung folgt nun aus Satz (2.3.5) und Lemma (2.2.5). □

Wir wollen nun zu den im 1. Kapitel behandelten Dualitätssätzen kommen.

(2.3.8) Korollar. *Sei k ein CM-Körper und sei $p \neq 2$. Die komplexe Konjugation in $k|k^+$ bezeichnen wir wieder mit σ. Dann gilt:*

(a) Für alle $i \in \mathbb{Z}$ ist der Isomorphismus

$$\hat{H}^i(G(L_S(p)|k), E_S(L_S(p))) \cong \hat{H}^{2-i}(G(L_S(p)|k), \mathbb{Q}_p/\mathbb{Z}_p)^\vee.$$

aus Theorem (1.2.29) (b) σ-invariant.

(b) Für alle $i \in \mathbb{Z}$ ist der Isomorphismus

$$\hat{H}^i(G(k_S(p)|k), E^S(k_S(p))) \cong \hat{H}^{2-i}(G(k_S(p)|k), \mathbb{Q}_p/\mathbb{Z}_p)^\vee.$$

aus Theorem (1.2.30) σ-invariant.

Beweis. Einer Analyse des Beweises von Theorem (1.1.34) entnimmt man, daß sich beide Isomorphismen zusammensetzen aus Verbindungshomomorphismen, dem Bilden von Pontrjagin-Dualen, dem Reziprozitätshomomorphismus und dem Homomorphismus aus dem Satz von Nakayama-Tate. Von all diesen haben wir die σ-Invarianz bewiesen. □

2.3.3. Zur Ideal- und Strahlklassengruppe von CM-Körpern

In diesem Abschnitt stellen wir Resultate über die S-Idealklassengruppe und die Idealklassengruppe modulo einem Modul $\mathfrak{m}$ zusammen. Dabei orientieren wir uns weitestgehend an [Wa]. Das Hauptresultat ist eine Version des Leopoldtschen Spiegelungssatzes.

(2.3.9) Satz. *Sei k ein CM-Körper, der die p-ten Einheitswurzeln $\mu_p(k)$ enthalte. Wir betrachten eine galoissche Erweiterung $L|k^+$, von der wir fordern, daß die Galoisgruppe $H := G(L|k)$ abelsch und vom Exponenten $p \neq 2$ sei. Sei ferner*

$$B \subseteq k^\times/(k^\times)^p \text{ eine Untergruppe mit } L = k(B^{\frac{1}{p}}),$$

welche nach der Theorie Kummerscher Körper (vgl. z.B. [N-KKT], Satz III.1.4) existiert.

Dann definiert

$$H \times B \to \mu_p(k), \quad < h, b > := \frac{h(b^{1/p})}{b^{1/p}}$$

eine nicht-ausgeartete Paarung, die Kummer-Paarung, *welche σ-invariant ist, d. h.*

$$< h^\sigma, b^\sigma > = (< h, b >)^\sigma,$$

wobei σ wiederum die komplexe Konjugation in $k|k^+$ bezeichne.

Beweis. Zunächst seien $h \in H$ und $b_1, b_2 \in B$. Dann ist

$$< h, b_1 b_2 > = \frac{h(b_1^{1/p} b_2^{1/p})}{b_1^{1/p} b_2^{1/p}} = \frac{h(b_1^{1/p})}{b_1^{1/p}} \frac{h(b_2^{1/p})}{b_2^{1/p}} = < h, b_1 >< h, b_2 > .$$

Seien weiter $h_1, h_2 \in H$ und $b \in B$. Wenn i so gewählt ist, daß $h_2(b^{1/p}) = \zeta_p^i b^{1/p}$ gilt, wobei $\zeta_p \in \mu_p(k)$ eine primitive p-te Einheitswurzel sei, dann erhalten wir die Gleichheit

$$\frac{h_1 \circ h_2(b^{1/p})}{h_2(b^{1/p})} = \frac{h_1(\zeta_p^i b^{1/p})}{\zeta_p^i b^{1/p}} = \frac{h_1(b^{1/p})}{b^{1/p}}.$$

Damit errechnen wir

$$< h_1 h_2, b > = \frac{h_1 \circ h_2(b^{1/p})}{b^{1/p}} = \frac{h_1 \circ h_2(b^{1/p})}{h_2(b^{1/p})} \frac{h_2(b^{1/p})}{b^{1/p}} = < h_1, b >< h_2, b > .$$

Wenn i so gewählt ist, daß $\sigma(b^{1/p}) = \zeta_p^i b^{1/p}$ gilt, bekommen wir die σ-Invarianz

$$< h^\sigma, b^\sigma >= \frac{\tilde{\sigma}^{-1} \circ h \circ \tilde{\sigma}(\sigma(b^{1/p}))}{\sigma(b^{1/p})} = \tilde{\sigma} \frac{h(\zeta_p^i b^{1/p})}{\zeta_p^i b^{1/p}} = (< h, b >)^\sigma,$$

wobei $\tilde{\sigma} \in G(L|k^+)$ eine Fortsetzung von σ bezeichnet.

Weiter zeigen wir, daß die Paarung nicht-ausgeartet ist. Gilt für ein $h \in H$

$$< h, b^{1/p} >= \zeta_p^i = 1 \text{ für alle } b \in B,$$

dann operiert h trivial auf B und damit auf $L|k$. Folglich ist $h = id_k$. Ist umgekehrt für ein $b \in B$

$$< h, b^{1/p} >= \frac{h(b^{1/p})}{b^{1/p}} = 1 \text{ für alle } h \in H,$$

dann ist $b^{1/p} \in L$ und somit $b \in L^p$. □

(2.3.10) Lemma. *Sei S eine (möglicherweise leere) Menge von Primstellen eines Zahlkörpers k. Sei ferner $a \in k^\times$ derart, daß $K := k(a^{1/n})$ eine außerhalb von S unverzweigte Erweiterung von k ist. Dann existiert ein Ideal $\mathfrak{a} \in \mathcal{J}_k^S$ mit $\mathfrak{a}^n = (a)$.*

Beweis. Die Primzerlegung von $(a) \in \mathcal{J}_K^S$ laute

$$a\mathcal{O}_{k,S} \;=\; \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_s^{\alpha_s}$$

mit $\mathfrak{p}_i \notin S$. Wegen der Unverzweigtheit außerhalb von S ergibt sich die Zerlegung in $\mathcal{J}_L^S$

$$a\mathcal{O}_{L,S} \;=\; (\mathfrak{P}_{1,1} \cdots \mathfrak{P}_{1,r_1})^{\alpha_1} \cdots (\mathfrak{P}_{s,1} \cdots \mathfrak{P}_{s,r_s})^{\alpha_s},$$

wobei die Primideale $\mathfrak{P}_{i,j}$ über $\mathfrak{p}_i$ liegen. Nun ist $a^{1/n} \in L$, weshalb n die Zahlen α_i für $i = 1, \ldots, s$ teilt.

$$\mathfrak{a} := \mathfrak{p}_1^{\alpha_1/n} \cdots \mathfrak{p}_s^{\alpha_s/n}$$

ist somit ein Ideal mit den gewünschten Eigenschaften. □

(2.3.11) Satz. *Sei k ein CM-Körper.*

(a) Sei S eine (möglicherweise leere) Menge von Primstellen von k^+. In der Erweiterung $k|k^+$ zerfalle keine in S gelegene Primstelle. Dann gilt:

$$(E_S(k))^- = \mu(k),$$

wobei $\mu(k)$ die Menge der in k gelegenen Einheitswurzeln bezeichne.

(b) Sei $\mathfrak{m}$ ein Modul von k^+. Dann gilt:

$$(\mathcal{O}_{k,\mathfrak{m}}^\times)^- \subseteq \mu(k).$$

Beweis. (b) folgt aus (a) mit $S = \emptyset$, denn wir haben eine σ-invariante Einbettung (σ bezeichne wiederum die komplexe Konjugation; wir schreiben aber auch $\sigma x = \overline{x}$)

$$\mathcal{O}_{k,\mathfrak{m}}^\times \hookrightarrow E(k).$$

Zu (a) stellen wir zunächst fest, daß $\mu(k)$ in $(E_S(k))^-$ enthalten ist. Sei $x \in (E_S(k))^-$. Da keine Primstelle $\mathfrak{p} \in S$ zerfällt, gilt für diese

$$v_\mathfrak{p}(x^{-1}) = v_\mathfrak{p}(\overline{x}) = v_{\overline{\mathfrak{p}}}(x) = v_\mathfrak{p}(x),$$

also $v_{\mathfrak{p}}(x) = 0$, weshalb x bereits in $E(k)^-$ liegt. Es ist nach Voraussetzung $x\overline{x} = 1$.

Eine ganze Zahl $x \in E(k)$, deren Absolutbetrag 1 ist, ist eine Einheitswurzel. Ist nämlich $f \in \mathbb{Z}[X]$ das Minimalpolynom von x, welches den Grad n habe, so haben alle Minimalpolynome der Potenzen von x einen Grad kleiner gleich n. Die Koeffizienten dieser Polynome sind ganze Zahlen, die aber durch n betragsmäßig beschränkt sind. Da es nur endlich viele solcher Polynome gibt, gibt es auch nur endlich viele Potenzen von x, welches somit wie behauptet eine Einheitswurzel ist. □

(2.3.12) Satz. *Sei k ein CM-Körper.*

(a) Sei S eine (möglicherweise leere) Menge von Primstellen von k^+. In der Erweiterung $k|k^+$ zerfalle keine in S gelegene Primstelle. Dann hat der natürliche Homomorphismus

$$\phi : \mathcal{C}l_S(k^+) \to (\mathcal{C}l_S(k))^+, \ \mathfrak{a}\mathcal{P}^S_{k^+} \mapsto (\mathfrak{a}\mathcal{O}_{k,S})(\mathcal{P}^S_k)^+$$

einen Kern der Ordnung 1 oder 2 und einen Kokern vom Exponenten 2.

(b) Sei $\mathfrak{m}$ ein Modul von k^+. Dann hat der natürliche Homomorphismus

$$\psi : \mathcal{C}l^{\mathfrak{m}}_{k^+} \to (\mathcal{C}l^{\mathfrak{m}}_k)^+$$

einen Kern der Ordnung 1 oder 2 und einen Kokern vom Exponenten 2.

Beweis. (a) Wir betrachten den Homomorphismus

$$\varphi : \mathcal{J}^S_{k^+} \to (\mathcal{J}^S_k)^+, \quad \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{k,S}.$$

Ein Ideal $\mathfrak{a} \in (\mathcal{J}^S_k)^+$ hat eine Primzerlegung

$$\mathfrak{a} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \cdot \mathfrak{Q}_1^{f_1}\overline{\mathfrak{Q}_1}^{f_1} \cdots \mathfrak{Q}_s^{f_s}\overline{\mathfrak{Q}_s}^{f_s} \quad \text{mit } e_i, f_j \in \mathbb{Z},$$

wobei $\mathfrak{P}_i = \overline{\mathfrak{P}_i}$ für $i = 1, \ldots, r$ gilt, und keines der $\mathfrak{P}_i$ oder $\mathfrak{Q}_j$ bzw. $\overline{\mathfrak{Q}_j}$ in S liegt. Ist $\mathfrak{p}$ ein in $k|k^+$ unverzweigtes Primideal von k^+, so ist entweder $\varphi(\mathfrak{p}) = \mathfrak{P}$ mit $\mathfrak{P} = \overline{\mathfrak{P}}$ oder $\varphi(\mathfrak{p}) = \mathfrak{Q}\overline{\mathfrak{Q}}$ mit einem Primideal $\mathfrak{P}$ bzw. $\mathfrak{Q}$ von k. Ist hingegen $\mathfrak{p}$ eines der endlich vielen in $k|k^+$ verzweigten Primideale von k^+, dann erhalten wir $\varphi(\mathfrak{p}) = \mathfrak{P}^2$ mit einem Primideal $\mathfrak{P}$ von k, welches $\mathfrak{P} = \overline{\mathfrak{P}}$ erfüllt. Daraus schließen wir, daß der Kokern von φ den Exponenten 2 und so viele Erzeuger hat, wie es in $k|k^+$ verzweigte Primideale außerhalb von S gibt.

Direkt der Definition entnehmen wir, daß $(\mathcal{P}^S_k)^+ = \mathcal{P}^S_{k^+}$ gilt. Durch Übergang zu den Quotienten modulo $\mathcal{P}^S_{k^+}$ erhalten wir aus φ den Homomorphismus

$$\phi : \mathcal{C}l_S(k^+) = \mathcal{J}^S_{k^+}/\mathcal{P}^S_{k^+} \to (\mathcal{J}^S_k)^+/\mathcal{P}^S_{k^+} = (\mathcal{C}l_S(k))^+,$$

welcher daher auch einen Kokern vom Exponenten 2 besitzt.

Sei $\mathfrak{a}$ ein Element des Kernes von ϕ. Dann ist $\mathfrak{a}\mathcal{O}_{k,S} = \alpha\mathcal{O}_{k,S}$ mit einem $\alpha \in \mathcal{P}^S_k$. Daher gilt

$$(1) = \mathcal{O}_{k,S} = \frac{\mathfrak{a}\mathcal{O}_{k,S}}{\overline{\mathfrak{a}\mathcal{O}_{k,S}}} = \frac{\alpha}{\overline{\alpha}}\mathcal{O}_{k,S}.$$

$\frac{\alpha}{\overline{\alpha}}$ ist ein Element von $(E_S(k))^-$ und somit nach Satz (2.3.11) eine Einheitswurzel. Gibt es eine Einheitswurzel $\zeta \in \mu(k)$ derart, daß $\frac{\alpha}{\overline{\alpha}} = \zeta^2$ gilt, dann folgt $\alpha\zeta^{-1} = \overline{\alpha\zeta^{-1}}$ und $\mathfrak{a} = \alpha\mathcal{O}_{k,S}$. Deshalb ist der Kern von ϕ in $\mu(k)/(\mu(k))^2$ enthalten, welches isomorph zu $\mathbb{Z}/2\mathbb{Z}$ ist.

(b) Der Beweis verläuft vollkommen analog. □

(2.3.13) Korollar. *Sei k ein CM-Körper und p eine ungerade Primzahl.*

(a) *Sei S eine (möglicherweise leere) Menge von Primstellen von k^+. In der Erweiterung $k|k^+$ zerfalle keine in S gelegene Primstelle. Dann sind die Gruppen*

$$\mathcal{C}l_S(k^+)(p) \cong (\mathcal{C}l_S(k)(p))^+$$

isomorph.

(b) *Sei $\mathfrak{m}$ ein Modul von k^+. Dann sind die Gruppen*

$$\mathcal{C}l_{k^+}^{\mathfrak{m}}(p) \cong (\mathcal{C}l_k^{\mathfrak{m}}(p))^+$$

isomorph.

Beweis. Nach Satz (2.3.12) haben beide dort betrachteten Homomorphismen 2-Gruppen als Kern und Kokern. Da diese gleichzeitig auch p-Gruppen sind, müssen sie trivial sein. □

(2.3.14) Satz. *Sei k ein CM-Körper. Wir betrachten zwei Fälle.*

(a) *Sei S eine (möglicherweise leere) Menge von Primstellen von k^+. In der Erweiterung $k|k^+$ zerfalle keine in S gelegene Primstelle. Für $E := E_S(k)$ gelten dann $E^- = \mu_k$ und $(E : E^+E^-) \leq 2$.*

(b) *Sei $\mathfrak{m}$ ein Modul von k^+. Für $E := \mathcal{O}_{k,\mathfrak{m}}^\times$ gelten dann $E^- \subseteq \mu_k$ und $(E : E^+E^-) \leq 2$.*

Beweis. Die erste Behauptung ist die Aussage von Satz (2.3.11). Wir betrachten die exakte Sequenz

$$1 \to E^+E^- \to E \xrightarrow{\phi} E^-/(E^-)^2,$$

mit $\phi(x) := \frac{x}{\overline{x}}(E^-)^2$. Man beachte, daß $\phi(x) = \frac{x}{\overline{x}} \in (E^-)^2$, also $x = \overline{x}\zeta^2$, impliziert, daß $x\zeta^{-1}$ ein Element von E^+ ist. Daher existiert eine Zerlegung $x = (x\zeta^{-1})\zeta$ in einen E^+- und einen E^--Anteil. Wegen $|\mu(k)/\mu(k)^2| \leq 2$ folgt die zweite Behauptung. □

Nun haben wir alle Vorbereitungen beendet, und können die von uns benötigte Version des Leopoldtschen Spiegelungssatzes beweisen.

(2.3.15) Satz. *Sei $p \neq 2$, und sei k ein CM-Körper, der die Gruppe $\mu_p(k)$ der p-ten Einheitswurzeln enthalte. Wir betrachten zwei Fälle.*

(a) *Sei S eine (möglicherweise leere) Menge von Primstellen von k^+. In der Erweiterung $k|k^+$ zerfalle keine in S gelegene Primstelle. Sei $L|k$ die maximale unverzweigte elementar abelsche p-Erweiterung von k, in der alle Primstellen aus S voll zerlegt sind. Wir setzen*

$$A := \mathcal{C}l_S(k)(p), \text{ so daß } A^+ = \mathcal{C}l_S(k^+)(p)$$

gilt (vgl. Korollar (2.3.13)).

(b) *Sei S eine endliche Primstellenmenge von k^+, welche keine Stelle über p enthalte, und sei $L|k$ die maximale außerhalb S unverzweigte elementar abelsche p-Erweiterung von k. Setze $\mathfrak{m} = \prod_{\mathfrak{p}\in S}\mathfrak{p}$ und*

$$A := \mathcal{C}l_k^{\mathfrak{m}}(p), \text{ so daß } A^+ = \mathcal{C}l_{k^+}^{\mathfrak{m}}(p)$$

gilt (vgl. Korollar (2.3.13)).

Dann liefert der Reziprozitätshomomorphismus eine mit der komplexen Konjugation kompatible Isomorphie

$$A/A^p \cong G(L|k),$$

und es gilt

$$d(A)^+ \leq 1 + d(A)^-.$$

Beweis. Wegen der Maximalität ist die Erweiterung $L|k^+$ in beiden Fällen galoissch. Mit σ bezeichnen wir wiederum die komplexe Konjugation in $k|k^+$. Wir setzen $H := G(L|k)$. Die σ-invariante Isomorphie $A/A^p \cong G(L|k)$ folgt aus Korollar (2.3.6) und den Sätzen (1.2.21) bzw. (1.2.24).

Aus Satz (2.3.9) erhalten wir eine Untergruppe $B \subseteq k^\times/(k^\times)^p$ mit $L = k(B^{1/p})$ und die Kummer-Paarung $H \times B \to \mu_p(k)$. Die σ-Invarianz impliziert sofort, daß

$$< H^+, B^+ >= 1 =< H^-, B^- >$$

gilt, denn $(\mu_p(k))^+$ enthält nur die 1. Somit ist die Paarung

$$H^+ \times B^- \to \mu_p(k)$$

nicht-ausgeartet, und daher gilt

$$d(A)^+ = d(A^+) = d(H^+) = d(B^-).$$

Aus Lemma (2.3.10) lesen wir ab, daß es zu jedem $b \in B$, welches modulo $(k^\times)^p$ bestimmt ist, ein Ideal $\mathfrak{a} \in \mathcal{J}_k^S$ im Fall (a) und im Fall (b) $\mathfrak{a} \in \mathcal{J}_k^{\mathfrak{m}}$ (wir nehmen das Bild unter der Projektion $\mathcal{J}_k \twoheadrightarrow \mathcal{J}_k^{\mathfrak{m}}$) gibt mit $(b) = \mathfrak{a}^p$. Somit erhalten wir einen Homomorphismus

$$\phi : B \to {}_pA,\ b \mapsto \mathfrak{a}.$$

Es ist klar, daß ϕ wohldefiniert und σ-invariant ist, so daß sich ein Homomorphismus

$$\psi : B^- \to ({}_pA)^-$$

ergibt.

Im Fall (a) ist ein Element $b \in B$ im Kern von ϕ, falls $(b) = (a)^p$ für ein $a \in E_S(k)$ gilt. Daher ist

$$ker(\psi) \leq (E_S(k)/(E_S(k))^p)^-.$$

Im Fall (b) ergeben analoge Überlegungen

$$ker(\psi) \leq (\mathcal{O}_{k,\mathfrak{m}}^\times/(\mathcal{O}_{k,\mathfrak{m}}^\times)^p)^-.$$

Dabei wurde Satz (2.3.11) benutzt.

Nun folgt aus Satz (2.3.14) mittels Indexbetrachtungen, daß

$$(E_S(k)/(E_S(k))^p)^- = \mu(k)/(\mu(k))^p \text{ bzw. } (\mathcal{O}_{k,\mathfrak{m}}^\times/(\mathcal{O}_{k,\mathfrak{m}}^\times)^p)^- \subseteq \mu(k)/(\mu(k))^p$$

gilt. Wir haben also insgesamt die exakte Sequenz

$$1 \to ker(\psi) \to B^- \xrightarrow{\psi} ({}_pA)^-,$$

und daher erhalten wir

$$d(B^-) \leq d(ker(\psi)) + d({}_pA)^- \leq d(\mathbb{Z}/p\mathbb{Z}) + d(A^-) = 1 + d(A)^-.$$

Wegen der oben gezeigten Gleichheit $d(B^-) = d(A)^+$ ist der Satz bewiesen. $\square$

2.4. Potenzreiche Galois-Gruppen von CM-Körpern

Dieser Abschnitt enthält die zentralen Resultate zu potenzreichen Galois-Gruppen bestimmter p-Erweiterungen von CM-Körpern, wie sie in [W] zu finden sind und eine Verallgemeinerung auf außerhalb einer Primstellenmenge S unverzweigte Erweiterungen.

Sei $k|k^+$ ein CM-Körper und $p \neq 2$ eine Primzahl.

Wir betrachten die beiden folgenden Situationen:

(I)
- S sei eine (möglicherweise leere) Menge von Primstellen von k^+.
- In $k|k^+$ zerfalle keine in S gelegene Primstelle.
- $L_S(p)|k$ sei die maximale unverzweigte galoissche p-Erweiterung von k, in welcher alle Stellen aus S voll zerlegt sind.
- $G := G(L_S(p)|k)$ sei die Galois-Gruppe dieser Erweiterung.
- $E := E_S(L_S(p)) = \varinjlim_{L_S(p)\supset K\supset k,\ K|k \text{ endlich}} E(K)$, wobei $E(K) := E_S(K)$ die Gruppe der S-Einheiten einer endlichen galoisschen Körpererweiterung $L_S(p) \supset K \supset k$ bezeichnet.

(II)
- S sei eine endliche Menge von Primstellen von k^+.
- In S sei keine über p liegende Stelle (deren Menge wir mit S_p bezeichnen) enthalten: $S_p \cap S = \emptyset$.
- $k_S(p)|k$ sei die maximale außerhalb von S unverzweigte galoissche p-Erweiterung von k.
- $G := G(k_S(p)|k)$ sei die Galois-Gruppe dieser Erweiterung.
- $E(K) := \mathcal{O}_{K,\mathfrak{m}}^\times$, wobei $k_S(p) \supset K$ eine endliche galoissche Körpererweiterungen von k sei. Dabei ist $\mathfrak{m}$ der Modul $\prod_{\mathfrak{p}\in S} \mathfrak{p}$.
- $E := \mathcal{O}_{k_S(p),\mathfrak{m}}^\times = \varinjlim_K E(K)$, wobei der direkte Limes über die in $k_S(p)$ enthaltenen endlichen galoisschen Erweiterungen von k läuft.

Wir halten fest, daß in beiden Fällen die Abelisierung von G endlich ist (Abschnitt 1.2.1 bzw. Satz (1.2.7)). Die Erweiterungen $L_S(p)|k^+$ und $k_S(p)|k^+$ sind beide galoissch, so daß wir eine Aktion der komplexen Konjugation auf G bekommen, welche wir mit σ bezeichnen.

Wir wollen nun voraussetzen, daß G potenzreich ist und Konsequenzen betrachten.

Mithilfe von Satz (2.2.21) wollen wir die Möglichkeiten für $d^+ := d(G)^+$ und $d^- := d(G)^-$ einschränken. Dazu werden wir eine obere Schranke für

$$dim_{\mathbb{F}_p}\ ({}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^-)$$

suchen. Auf diese Weise werden wir auf den Fall $d(G) \leq 3$ geführt werden. An dieser Stelle gehen entscheidend die im Kapitel I bewiesenen Dualitätssätze ein.

In der Tat liefert Korollar (2.3.8) angewendet im Fall $i = 0$ eine σ-invariante Surjektion

$$E(k) \twoheadrightarrow \hat{H}^0(G, E) = E(k)/N_G E \cong H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^\vee$$

und daher insbesondere nach Satz (2.3.11) eine Surjektion

$$\mu_p(k) \supseteq (E(k)/p)^- \twoheadrightarrow ({}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^-)^\vee.$$

Dies impliziert also

$$dim_{\mathbb{F}_p}\ ({}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^-) \leq \begin{cases} 0 & \text{falls } \mu_p(k) \not\subseteq k \\ 1 & \text{falls } \mu_p(k) \subseteq k. \end{cases}$$

Aus Satz (2.2.21) ersehen wir nun die Ungleichung

$$d^+ \cdot d^- \leq d^- + 1.$$

Daher können nur die folgenden Fälle auftreten:

$$d^- = 0 \text{ oder } d^+ = 0 \text{ oder } d^+ = 1 \text{ oder } (d^+ = 2 \text{ und } d^- = 1 \text{ und } \mu_p(k) \subseteq k).$$

Wir wollen $d^+ \neq 1$ annehmen. Somit erhalten wir dann außer in den Sonderfällen $d^+ = 0$ und $d^- = 0$ die Ungleichung $d(G) \leq 3$.

Im Fall $d(G)^+ = 0$ ist G nach Satz (2.2.15) abelsch, in unserem Fall also endlich.

Sind die p-ten Einheitswurzeln in k enthalten, so liefert der Leopoldtsche Spiegelungssatz (Satz (2.3.15)) die Ungleichung

$$d^+ \leq 1 + d^-,$$

welche den Fall $d^- = 0$ ausschließt.

Nun gibt es einen Index i, so daß $G_i =: P$ eine uniforme Gruppe ist. Nach Lemma (2.2.20) gilt

$$d(P)^+ \leq d^+ \quad \text{und} \quad d(P)^- \leq d^-.$$

Wir wollen annehmen, daß $d^+ \neq 0$ und $d^- \neq 0$ und somit $d(P) \leq d(G) \leq 3$ gilt. Wäre $d(P) < 3$, so hätte P nach Korollar (2.2.19) eine unendliche Abelisierung, was aber den Voraussetzungen widerspricht. Deshalb können wir uns auf den Fall

$$d(G) = d(P) = 3, \quad d^+ = d(P)^+ \ \text{ und } \ d^- = d(P)^-$$

beschränken.

Das gruppentheoretische Resultat des Satzes (2.2.22) liefert nun einen Widerspruch.

Wir fassen die Diskussion zusammen im folgenden Theorem, welches Theorem 3.1 aus [W] verallgemeinert.

(2.4.1) Theorem. *Die Voraussetzungen seien die in (I) oder (II) am Beginn des Abschnitts gegebenen. Falls die p-ten Einheitswurzeln nicht in k enthalten sind, wollen wir zusätzlich $d(G)^- \neq 0$ fordern.*

Ist G potenzreich, dann ist G endlich oder $d(G)^+ = 1$.

Für den Fall $\mu_p(k) \not\subseteq k$ und $d(G)^+ = 1$ oder $d(G)^- = 0$ werden wir keine Aussage machen können. Beschränken wir uns jedoch auf uniforme Gruppen, so läßt sich noch mehr sagen.

$d(G)^+ = 1$ bedeutet nach Korollar (2.3.13) im Fall (I), daß die Galois-Gruppe H der maximalen unverzweigten abelschen p-Erweiterung von k^+, welche in S voll zerlegt ist, den Rang 1 hat, und im Fall (II), daß die Galois-Gruppe H der maximalen außerhalb S unverzweigten abelschen p-Erweiterung von k^+ ebenfalls $d(H) = 1$ erfüllt. In beiden Fällen existiert somit eine echte abelsche p-Erweiterung K^+ von k^+ innerhalb von $L_S(p)$ bzw. $k_S(p)$, welche total reell ist, da unendliche Stellen in p-Erweiterungen nicht verzweigen. Setzen wir $K := kK^+$, so erhalten wir also eine echte endliche Erweiterung von CM-Körpern.

Investieren wir ein weiteres Mal den Dualitätssatz aus Korollar (2.3.8), so erhalten wir eine σ-invariante Surjektion:

$$H^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong \hat{H}^0(G, E) \twoheadrightarrow \hat{H}^0(G(K|k), E(K)).$$

Da $K|k$ CM-Körper sind, gilt nach Korollar (2.3.4) $G(K|k) \cong G(K^+|k^+) \cong G(K|k)^+$ und daher

$$\hat{H}^0((G(K|k), E(K))/p)^- = \hat{H}^0(G(K|k), \mu(K)(p))/p,$$

vorausgesetzt $\mu_p(k) \subseteq \mathcal{O}_{K,\mathfrak{m}}^\times = E(K)$ im Fall (II). Wir haben somit insgesamt die Surjektion

$$({}_pH^2(G, \mathbb{Q}_p/\mathbb{Z}_p)^-)^\vee \twoheadrightarrow \hat{H}^0(G(K|k), \mu(K)(p))/p.$$

Ist G uniform mit endlicher Abelisierung, so folgt aus Satz (2.2.21), daß ${}_pH^2(G,\mathbb{Q}_p/\mathbb{Z}_p)^-$ trivial ist. Wir erhalten also einen Widerspruch, falls die Gruppe $\hat{H}^0(G(K|k),\mu(K)(p))/p$ nicht trivial ist. Nehmen wir z. B. an, daß $\mu(K)(p) = \mu(k)(p)$ gilt, und daß k die p-ten Einheitswurzeln enthält, dann erhalten wir

$$\hat{H}^0(G(K|k),\mu(K)(p))/p = \mu(k)(p)/p \cong \mathbb{Z}/p\mathbb{Z}.$$

Diesen Fall erreichen wir offenbar durch die Forderung, daß Adjunktion von $\mu_{p^{s+1}}$ im Fall (I) nicht unverzweigt und in S voll zerlegt und im Fall (II) außerhalb S nicht unverzweigt ist, falls $\mu_{p^s}(k)$ die Gruppe der in k enthaltenen Einheitswurzeln von p-Potenzordnung ist.

Als Resultat erhalten wir folgendes Theorem in Verallgemeinerung von [W], Theorem 3.2.

(2.4.2) Theorem. *Die Voraussetzungen seien die in (I) oder (II) am Beginn des Abschnitts gegebenen. Der CM-Körper $k|k^+$ enthalte die p-ten Einheitswurzeln. Im Fall (II) gelte außerdem $\mu_p(k) \subseteq \mathcal{O}_{K,\mathfrak{m}}^\times = E(K)$. Es sei $\mu(k)(p) = \mu_{p^s}(k)$ die Gruppe der Einheitswurzeln von p-Potenzordnung in k. Ist $d(G)^+ = 1$, so fordern wir zusätzlich*

im Fall (I): $k(\mu_{p^{s+1}})|k$ ist nicht unverzweigt und in S voll zerlegt,
im Fall (II): $k(\mu_{p^{s+1}})|k$ ist nicht unverzweigt außerhalb S.

Dann ist G nicht uniform.

Literaturverzeichnis

[AW] Atiyah, M. F., Wall, C. T. C.: *Cohomology of Groups,* in Cassels, J. W. S., Fröhlich, A.: *Algebraic Number Theory,* Academic Press, 1967

[Br] Brown, K. S.: *Cohomology of Groups,* GTM 87, Springer-Verlag, 1982

[DDMS] Dixon, J. D., Du Sautoy, M.P.F., Mann, A., Segal, D.: *Analytic Pro-p Groups,* 2nd Edition, Cambridge studies in advanced mathematics 61, Cambridge University Press, 1999

[FM] Fontaine, J.-M., Mazur, B.: *Geometric Galois Representations,* in *Elliptic Curves, Modular Forms, & Fermat's Last Theorem* edited by Coates, J., and Yau, S. T., International Press, 1995

[K-G] Koch, H.: *Galoissche Theorie der p-Erweiterungen,* VEB Deutscher Verlag der Wissenschaften, Berlin 1970

[K-ZT] Koch, H.: *Zahlentheorie,* Vieweg Studium, 1997

[La] Lang, S.: *Algebra,* 3rd Edition, Addison-Wesley, 1993

[Lz] Lazard, M.: *Groupes analytiques p-adiques,* Publ. Math. IHES 26, 1965

[N-ZT] Neukirch, J.: *Algebraische Zahlentheorie,* Springer-Verlag, 1992

[N-KKT] Neukirch, J.: *Klassenkörpertheorie,* Bibliographisches Institut, Mannheim, 1969

[NSW] Neukirch, J., Schmidt, A., Wingberg, K.: *Cohomology of Number Fields,* Springer-Verlag, 1999

[Ri] Ribes, L.: *Introduction to Profinite Groups and Galois Cohomology,* Queen's Papers in Pure and Applied Mathematics - No. 24, 1970

[S] Schmidt, A.: *On Poitou's Duality Theorem,* in *Journal für die reine und angewandte Mathematik* **517**, pp. 145-160, 1999

[Se-GC] Serre, J.-P.: *Galois Cohomology,* Springer-Verlag, 1997

[Se-LF] Serre, J.-P.: *Local Fields,* GTM 67, Springer-Verlag, 1979

[Wil] Wilson, J.: *Profinite Groups,* London Mathematical Society Monographs, New Series 19, Oxford University Press, 1998

[W] Wingberg, K.: *On the Fontaine-Mazur Conjecture for CM-fields,* Compositio Mathematica, 2001

[Wa] Washington, L. C.: *Introduction to Cyclotomic Fields,* GTM 83, Springer-Verlag, 1982