Gruppenkohomologie

Votragsausarbeitung der Teilnehmer am Seminar

Kohomologie (pro-)endlicher Gruppen

von Prof. Dr. O. Venjakob, Dr. J. Stix

Bonn, im Wintersemester 2005/2006

Bonn, den 18.04.2006

universitätbonn

Vorwort

Der vorliegende Text enstand in Begleitung zum Seminar

Kohomologie (pro-)endlicher Gruppen

von Prof. O. Venjakob und Dr. J. Stix, welches in Bonn im Wintersemester 2005/2006 stattfand, und besteht aus Vortragsausarbeitungen der Seminarteilnehmer.

Sinn und Zweck dieser Textfassung des Seminars war zum einen, den Seminarteilnehmern zum Ende der Veranstaltung ein Skript an die Hand zu geben, welches den Verlauf des Seminars dokumentiert und in Teilen über die mündliche Darstellung hinausgeht. Dies betrifft Argumente und Details die während des Vortrags dem engen Zeitrahmen zum Opfer fielen; von den Vortragenden wurde verlangt, den zur Verfügung stehenden Zeitrahmen nicht zu überschreiten und so neben dem Verständnis der Mathematik auch ein Gefühl für Zeitmanagement zu entwickeln.

Zum andern übt das schriftliche Festhalten eines Vortrags die für die Diplomarbeit wichtige Fähigkeit, kompliziertere mathematische Zusammenhänge zu organisieren und zu verschriftlichen. Darüberhinaus erfordert es den Umgang mit dem Satzsystem LaTeX, das spätestens bei der Diplomarbeit unerläßlich ist.

Allerdings wäre dieses Skript nicht in der vorliegenden Form entstanden, wenn nicht zwei der Seminarteilnehmer den zugehörigen Rahmen entworfen hätten und damit ihre schon weit entwickelte LaTeX-Professionalität unter Beweis gestellt hätten. Sebastian Hensel und Franz-Benjamin Mocnik gebührt dafür ein großer Dank.

Jakob Stix

Bonn, im Februar 2006

Einleitung

Kohomologie liefert eine Familie von Invarianten für ein Paar bestehend aus einer Gruppe (bzw. einem topologischen Raum) und gewissen Koeffizienten. Je nach Perspektive kann man damit die Gruppe (bzw. den Raum) oder die Koeffizienten studieren. Die Invarianten der Kohomologie sind ihrerseits abelsche Gruppen oder Vektorräume und tragen reichhaltige zusätzliche Struktur, die sie als Invarianten wertvoll machen, zumal man sie Dank der gut geölten Maschine der homologischen Algebra in der Regel gut berechnen kann.

In sämtlichen Bereichen der modernen reinen Mathematik (algebraische Topologie, Differentialgeometrie, algebraische Geometrie, algebraische Zahlentheorie, mathematische Physik, ...) treten Kohomologietheorien unvermeidbar auf und sind sowohl als konzeptionelles Hilfsmittel als auch als Kalkül nicht mehr wegzudenken. Die Kohomologie von Gruppen eignet sich hervorragend dazu, exemplarisch den Mechanismus einer Kohomologietheorie zu erlernen und dabei die algebraische Komponente einer solchen Theorie zu betonen. Die hierbei erworbenen Kenntnisse sollten das Erlernen jeglicher Kohomologietheorie und insbesondere das der wichtigen Kohomologie von Garben erlauben. Letztendlich ist Gruppenkohomologie ja auch nichts anderes als Garbenkohomologie auf einem geeigneten Situs. Doch davon ein anderes mal.

Das Folgende gibt einen Abriß des Seminars und beleuchtet den gewählten Zugang zur Gruppenkohomologie.

In Vortrag 1 treffen wir auf Probleme der Gruppentheorie, die historisch ursächlich daran beteiligt waren, das Konzept der Gruppenkohomologie zu entwickeln. Hierbei wirken die beschriebenen Probleme, das Studium von Gruppenextensionen und Spaltungen, natürlich, aber ihre Lösungen, Faktorsysteme und verschränkte Homomorphismen, erscheinen unsystematisch. Wir kommen hierauf in Vortrag 4 zurück.

Die Vorträge 2 und 3 stellen die benötigte Theorie der Moduln über einem Ring zur Verfügung. Insbesondere wird bewiesen, daß es genügend viele injektive Moduln gibt. Dabei muß darauf Wert gelegt werden, daß auch nichtkommutative Ringe behandelt werden, da der für uns relevante Fall des Gruppenrings für nichtkommutative Gruppen ebenso nichtkommutativ ist.

Die Gruppenkohomolgie in allen Graden betritt in Vortrag 4 die Bühne. Allerdings werden sie zunächst ad hoc über eine projektive Auflösung von $\mathbb{Z}$ definiert. Der funktorielle Charakter wird zunächst unterdrückt, wohl aber der Bezug zu den Lösungen aus Vortrag 1 hergestellt und in Beispielen berechnet.

Vortrag 5 bringt uns das Sprechen bei: Kohomologie ist ein Funktor, und so lernen wir, was eine Kategorie, ein Funktor, etc. ..., kurz alles was wir aus der Kategorientheorie für die Belange des Seminars brauchen. Dieser Vortrag hätte auch früher platziert werden können um den Preis, mit weniger und dann hauptsächlich dumpfen Beispielen auskommen zu müssen.

Nach diesen Vorarbeiten wenden wir uns der konzeptionellen Struktur von Kohomologietheorien zu. In Vortrag 6 wird, das in der homologischen Algebra allgegenwärtige Schlangenlemma nutzend, aus einer kurzen exakten Sequenz von Komplexen eine lange exakte Sequenz. Dies wenden wir auf die in Vortrag 4 über eine projektive Auflösung von $\mathbb{Z}$ definierte Gruppenkohomologie an und formalisieren das Erhaltene als *kohomologischen δ-Funktor*.

Letztere sind Gegenstand der Untersuchung in Vortrag 7, der die Definition eines (rechts-)derivierten Funktors und Grothendiecks Satz enthält, daß auslöschbar universell impliziert. Es mag die Konstruktion der derivierten Funktoren willkürlich erscheinen, aber daß man ein gutes Objekt in Händen hält, weiß man spätestens, wenn man eine solche universelle Eigenschaft beweisen kann.

Jetzt sind wir soweit, daß in Vortrag 8 die Handlungsstränge zusammen geführt werden können. Gruppenkohomologie bekommt man jetzt umsonst als $\mathrm{Ext}^*_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, und dies ist auch leicht mit der vorher definierten Gruppenkohomologie zu identifizieren. Mit Shapiro's Lemma und der Methode des Dimensionsshifts beginnt das feinere Studium der Gruppenkohomologie, welche Vortrag 9 mit der Behandlung von Restriktion, Inflation und Corestriktion weiterführt.

Ab Vortrag 10 werden wir dem Titel des Seminars gerecht und studieren detaillierter die Kohomologie endlicher und proendlicher Gruppen. Gerade die Kohomologie proendlicher Gruppen ist das unverzichtbare Hilfsmittel zum Verständnis von Klassenkörpertheorie und damit den weiterführenden Veranstaltungungen in der algebraischen Zahlentheorie. Vortrag 10 führt die Kohomologie proendlicher Gruppen ein und bemüht sich, die ad hoc Definitionen als derivierten Funktor zu erkennen.

Vortrag 11 studiert den speziellen aber wichtigen Fall der Kohomologie der absoluten Galoisgruppe eines Körpers. Vortrag 12 studiert den Begriff der Kohomologischen Dimension, während Vortrag 13 sich auf pro-p-Gruppen konzentriert und mit dem Satz von Golod–Shafarevich einen würdigen Schlußpunkt setzt.

Zusammenfassend läßt sich also sagen, daß Vortrag 1 zur Motivation, die Vorträge 2 bis 7/8 der Definition der Gruppenkohomologie, die Vorträge 8 und 9 der Entwicklung der Eigenschaften der Gruppenkohomologie und die Vorträge 10 bis 13 dem speziellen Studium der Kohomologie proendlicher Gruppen dient.

Vortragsübersicht

Inhaltsverzeichnis

Vortrag 1

Gruppenkohomologie in Graden 0, 1 und 2

Matthias Klotz
18.10.2005

Ziel des Vortrages ist es, uns auf einem ersten Weg mit dem Begriff der Gruppenkohomologie in den Graden 0, 1 *und* 2 *vertraut zu machen. In den späteren Vorträgen werden wir zwar einen systematischen Aufbau der Thematik kennen lernen, aber jetzt stehen wir erst einmal vor dem Problem, dass uns die Definition der Gruppenkohomologie auf den ersten Blick etwas merkwürdig und künstlich erscheinen mag. Daher wollen wir uns dem Begriff auf eine etwas ungewöhnliche Weise nähern.*

Wir werden uns nämlich zunächst mit einem völlig anderem Begriff näher befassen, dem der Extension von Gruppen. Hier führen wir verschiedene Mengen von Äquivalenzklassen ein, die wir durch dazu bijektive Mengen darstellen möchten. Auf der Suche nach solchen darstellenden Mengen werden wir fast wie von selbst auf die Kohomologiegruppe in den Graden 1 *und* 2 *stoßen. Dass wir bei der Suche nach diesen Mengen sogar auf Gruppenstrukturen treffen, ist quasi eine Sache des Zufalls.*

Nach einer kurzen Ergänzung der Definition der nullten Kohomologiegruppe stellt sich natürlich berechtigterweise die Frage nach einem Gesamtzusammenhang, in dem unsere drei Gruppen stehen. Schließlich verbindet sie ja auch ihre gemeinsame Bezeichnung, die sich nur im Grad unterscheidet. Auch wenn sich diese Fragestellung natürlich eigentlich an den systematischen Aufbau der Thematik wendet, werden wir trotzdem schon einen erstaunlichen Zusammenhang feststellen: Die lange exakte Sequenz der Kohomologiegruppen in den Graden $0, 1$ *und* 2.

In einem letzten Abschnitt entnehmen wir der langen exakten Sequenz noch eine Deutung für die erste Kohomologiegruppe. Wir können sie nämlich als ein Maß für die Nichtexaktheit des Invariantennehmens auffassen. Aber später mehr dazu!

1.1 Der Begriff der Gruppen-Extension

Bevor wir uns dem eigentlichen Ziel widmen können, die Gruppenkohomologie in den Graden 1 und 2 zu definieren, müssen wir uns mit dem Begriff der Extension vertraut machen. Dieser Abschnitt ist jedoch sehr knapp gehalten ist und führt nur *diejenigen* Begriffe ein, die wir wirklich benötigen. Für eine tiefergehende Beschäftigung mit Extensionen muss ich auf zusätzliche Literatur verweisen. Zum besseren Leseverständnis werde ich im Folgenden – wie es auch sonst üblich ist – abelsche Gruppen stets *additiv* schreiben, beliebige Gruppen hingegen *multiplikativ*.

Definition 1.1 (Gruppenoperation)**.** Gegeben sei eine Gruppe G und eine Menge X. Eine ***G*-Operation** oder ***G*-Aktion** auf X (von links) ist eine Abbildung

$$G \times X \longrightarrow X, \quad (g, x) \longmapsto g.x,$$

welche folgenden Bedingungen genügt:

(i) $\mathbf{1}.x = x$ für das Einselement $\mathbf{1} \in G$ und für beliebiges $x \in X$.

(ii) $(gh).\, x = g.(h.x)$ für $g, h \in G, x \in X$.

Definition 1.2 (G-Modul)**.** Gegeben sei eine Gruppe G. Ein ***G*-Modul** ist eine abelsche Gruppe A zusammen mit einer G-Operation von links auf A, so dass die Gruppenstruktur von A mit der Gruppenoperation von G verträglich ist, d. h. für alle $g \in G$ und $a_1, a_2 \in A$ gilt

$$g.(a_1 + a_2) = g.a_1 + g.a_2 \ .$$

Bemerkung 1.3. Insbesondere gilt $g.0 = 0$ für alle $g \in G$, denn es gilt $g.(0+0) = g.0 + g.0$.

Definition 1.4 (Exakte Sequenz von Gruppenhomomorphismen)**.** Eine Sequenz von Gruppenhomomorphismen der Form

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} G_2 \xrightarrow{f_3} \cdots \xrightarrow{f_n} G_n$$

heißt **exakt**, wenn sie an jeder Stelle G_i (mit $i \in \{1, \ldots, n-1\}$) exakt ist. Dabei bedeutegt Exaktheit bei G_i, dass $\mathrm{im}(f_i) = \ker(f_{i+1})$ gilt.

Bemerkung 1.5. Wegen $\mathrm{im}(f_i) = \ker(f_{i+1})$ ist die Verkettung zweier aufeinanderfolgender Homomorphismen einer exakten Sequenz stets der triviale Gruppenhomomorphismus.

Definition 1.6 (Kurze exakte Sequenz von Gruppenhomomorphismen)**.** Eine exakte Sequenz von Gruppenhomomorphismen der Form

$$1 \longrightarrow G_1 \xrightarrow{i} G_2 \xrightarrow{\pi} G_3 \longrightarrow 1$$

heißt **kurze exakte Sequenz**. Es muss also $\mathrm{im}(i) = \ker(\pi)$ gelten, außerdem i injektiv und π surjektiv sein.

Definition 1.7 (Extension mit einer abelschen Gruppe)**.** Eine **Extension einer Gruppe *G* mit einer abelschen Gruppe** A sei eine kurze exakte Sequenz von Gruppenhomomorphismen der Form

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1 \ ,$$

wobei E eine beliebige Gruppe sei. Wegen der Injektivität von i kann man A dabei insbesondere als abelsche Untergruppe von E auffassen. Wird im Folgenden eine Injektion mit $i, i', \tilde{i} \ldots$ bezeichnet, so werden wir die entsprechende Identifikation der Quelle mit dem Bild stillschweigend vornehmen.

Lemma 1.8 (Induktion einer natürlichen G-Modul-Struktur)**.** *Gegeben sei eine Extension einer Gruppe G mit einer abelschen Gruppe A mit den Bezeichnungen aus Definition 1.7. Dann induziert die Extension eine natürliche G-Modul-Struktur auf A, wobei die dazugehörige Gruppenoperation durch Konjugation gegeben ist. Genauer gilt*

$$g.a := \tilde{g}a\tilde{g}^{-1} = i^{-1}\left(\tilde{g}\; i(a)\,\tilde{g}^{-1}\right),$$

wobei $\tilde{g}$ ein beliebiges Urbild von g unter π ist. Die Konjugation passiert in der Gruppe E.

Beweis. Zur Wohldefiniertheit: Da π surjektiv ist (vgl. Definition 1.6), hat g also mindestens ein Urbild $\tilde{g}$. Weiterhin gilt $\tilde{g}a\tilde{g}^{-1} \in \ker(\pi) = \mathrm{im}(i) = A$, da

$$\pi\left(\tilde{g}a\tilde{g}^{-1}\right) = \pi(\tilde{g})\;\pi(a)\;\pi\left(\tilde{g}^{-1}\right) = \pi(\tilde{g}) \cdot \mathbf{1} \cdot \pi(\tilde{g})^{-1} = \mathbf{1}$$

(vgl. Bemerkung 1.5). Somit hat $\tilde{g}a\tilde{g}^{-1}$ ein Urbild unter i, welches wegen der Injektivität von i sogar eindeutig bestimmt ist. Zu zeigen bleibt die Unabhängigkeit von der Wahl des Urbildes $\tilde{g}$ von g. Seien hierfür $\tilde{g}_1$ und $\tilde{g}_2$ beide Urbilder von g unter π. Dann ist $\left(\tilde{g}_2^{-1}\,\tilde{g}_1\right) \in \ker(\pi) = \mathrm{im}(i)$, gehört also zur abelschen Untergruppe $A \subset E$. Folglich kommutieren $\tilde{g}_2^{-1}\,\tilde{g}_1$ und a, und wegen $\left(\tilde{g}_2^{-1}\,\tilde{g}_1\right)\,a = a\,\left(\tilde{g}_2^{-1}\,\tilde{g}_1\right)$ gilt dann auch $\tilde{g}_1 a\tilde{g}_1^{-1} = \tilde{g}_2 a\tilde{g}_2^{-1}$, womit die Wohldefiniertheit nachgewiesen ist.

Zur G-Modul-Eigenschaft: Die Forderungen $1.a = a$, $(gh).\,a = g.(h.a)$ und die Verträglichkeitsgleichung $g.(a_1 + a_2) = g.a_1 + g.a_2$ lassen sich relativ leicht nachweisen und werden dem Leser als Übung überlassen. □

Bemerkung 1.9 (Vertauschungsregel)*.* Eine kleine Umformung der definierenden Gleichung für die Gruppenoperation in Lemma 1.8 ergibt unmittelbar die Vertauschungsregel

$$ea = (\pi(e).a)e$$

mit $e \in E$ und $a \in A$. Diese werden wir noch verwenden.

Definition 1.10 (Extension mit einem G-Modul)**.** Eine **Extension einer Gruppe G mit einem G-Modul A** ist eine Extension

$$0 \longrightarrow A \xrightarrow{\;i\;} E \xrightarrow{\;\pi\;} G \longrightarrow 1$$

von G mit dem als abelsche Gruppe aufgefassten G-Modul A, sodass die auf natürliche Weise induzierte G-Modul-Struktur auf A (vgl. Lemma 1.8) mit der gegebenen übereinstimmt.

Definition 1.11 (Äquivalenz von Extensionen mit G-Moduln)**.** Gegeben seien zwei Extensionen E_ν für $\nu = 1, 2$

$$0 \longrightarrow A \xrightarrow{\;i_\nu\;} E_\nu \xrightarrow{\;\pi_\nu\;} G \longrightarrow 1$$

einer Gruppe G mit einem G-Modul A. Wir nennen die beiden Extensionen **äquivalent**, wenn es einen Isomorphismus $\varphi : E_1 \to E_2$ gibt, sodass das Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{i_1} & E_1 & \xrightarrow{\pi_1} & G & \longrightarrow & 1 \\
 & & \Vert{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle \varphi} & & \Vert{\scriptstyle \mathrm{id}_G} & & \\
0 & \longrightarrow & A & \xrightarrow{i_2} & E_2 & \xrightarrow{\pi_2} & G & \longrightarrow & 1
\end{array}$$

kommutiert.

Bemerkung 1.12. Dass es sich bei dem soeben eingeführten Äquivalenzbegriff um eine Äquivalenzrelation handelt, ist klar.

1.2 Gruppenkohomologie im Grad 1 im Zusammenhang mit spaltenden Extensionen

Nun sind wir endlich soweit, den Begriff der Gruppenkohomologie im Grad 1 einzuführen. Hierfür werden wir eine besondere Klasse von Extensionen mit G-Moduln untersuchen, nämlich die der *spaltenden* Extensionen:

Definition 1.13 (Spaltende Extensionen)**.** Eine Extension einer Gruppe G mit einem G-Modul A (mit den Bezeichnungen aus Definition 1.10) heißt **spaltend**, wenn es einen Gruppenhomomorphismus $s : G \to E$ gibt mit $\pi \circ s = \mathrm{id}_G$. Wir nennen s dann auch **Schnitt von π**:

$$0 \longrightarrow A \xrightarrow{i} E \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 1 \,.$$

Man kann nun zeigen, dass zu gegebener Gruppe G und gegebenem G-Modul A bis auf Äquivalenz genau eine spaltende Extension von G mit A existiert. Die Menge der Äquivalenzklassen von spaltenden Extensionen ist also nicht weiter interessant. Zu einer spaltenden Extension können wir uns jedoch die Menge der möglichen Schnitte genauer anschauen. Auch auf dieser Menge können wir eine Äquivalenzrelation einführen.

Unser Ziel ist es dann, die Menge dieser Äquivalenzklassen durch eine dazu bijektive Menge darzustellen. Bei diesem Versuch erhält man auf eine unglaublich natürliche Weise die Definition der 1. Kohomologie-Gruppe von G mit Koeffizienten in A, die wir formal mit $H^1(G, A)$ bezeichnen werden.

Werden wir also konkret: Gesucht ist die spaltende Extension von G mit A. Bei der Suche danach stoßen wir auf das *semidirekte Produkt* der Gruppe G mit dem G-Modul A. Auch wenn die Definition dieses Begriffes etwas künstlich erscheinen mag, möchte ich sie zur Übersichtlichkeit jetzt direkt bringen. Wir werden dann im Beweis des darauffolgenden Satzes sehen, dass sie sich von ganz alleine ergibt.

Lemma–Definition 1.14 (Semidirektes Produkt)**.** *Das* **semidirekte Produkt** *einer Gruppe G mit einem G-Modul A ist die Gruppe $A \rtimes G$ auf der Menge $A \times G$ gegeben durch die Verknüpfung*

$$(a_1, g_1) \cdot (a_2, g_2) := (a_1 + g_1.a_2, g_1 g_2).$$

Beweis. Dass es sich bei der angegebenen Verknüpfung tatsächlich um ein Gruppengesetz handelt, weist man durch einfaches Nachrechnen nach. Das neutrale Element ist $(0, 1)$, während $(-g^{-1}.a, g^{-1})$ das Inverse zu (a, g) ist. □

Bemerkung 1.15. Die Konstruktion kann auch in der nicht-abelschen Situation durchgeführt werden:operiert die Gruppe G auf einer nicht notwendig abelschen Gruppe A, so ist $A \times G$ mit obiger Verknüpfung auch eine Gruppe, das semidirekte Produkt $A \rtimes G$.

Satz 1.16 (Existenz und Eindeutigkeit der spaltenden Extension)**.** *Gegeben sei eine Gruppe G und ein G-Modul A. Dann gibt es bis auf Äquivalenz genau eine Extension von G mit A, die spaltend ist. Diese ist gegeben durch*

$$0 \longrightarrow A \xrightarrow{\tilde{i}} A \rtimes G \xrightarrow{\tilde{\pi}} G \longrightarrow 1\,, \tag{1.1}$$

wobei $\tilde{i}$ die natürliche Inklusion $a \mapsto (a,1)$ und $\tilde{\pi}$ die natürliche Projektion $(a,g) \mapsto g$ ist.

Beweis. Man zeigt leicht, dass $\tilde{i}$ und $\tilde{\pi}$ Homomorphismen sind. Die im Satz angegebene Sequenz (1.1) ist daher eine kurze exakte Sequenz von Gruppenhomomorphismen (denn $\tilde{i}$ ist injektiv, $\tilde{\pi}$ ist surjektiv und $\mathrm{im}(\tilde{i}) = \ker(\tilde{\pi})$) und somit eine Extension von G mit (als abelsche Gruppe aufgefasstem) A. Wir zeigen nun, dass die von der Extension auf natürliche Weise induzierte G-Modul-Struktur auf A (vgl. Lemma 1.8) mit der gegebenen übereinstimmt, sodass (1.1) sogar eine Extension von G mit dem G-Modul A ist (vgl. Definition 1.10). Dies ist in der Tat der Fall, denn wählen wir zum Beispiel $(0,g)$ als Urbild von g, so ist die zu zeigende Gleichung

$$g.a = (0,g)(a,1)(0,g)^{-1}$$

und ergibt sich durch direktes Nachrechnen:

$$(0,g)(a,1)(0,g)^{-1} = (g.a,g)\left(0,g^{-1}\right) = (g.a,1) = \tilde{i}(g.a) = g.a.$$

Ein möglicher Schnitt ist zum Beispiel durch den Homomorphismus

$$\tilde{s} : G \to A \rtimes G, \quad g \mapsto (0,g)$$

gegeben. Zu zeigen bleibt, dass jede spaltende Extension von G mit A äquivalent zu (1.1) ist. Dabei wollen wir – wie versprochen – die Konstruktion des semidirekten Produktes auf natürlicher Weise herleiten. Gegeben sei also eine beliebige spaltende Extension

$$0 \longrightarrow A \xrightarrow{i} E \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 1$$

mit Schnitt s. Auf die Vermutung hin, dass es eine mengentheoretische Bijektion zwischen der Gruppe E und der Menge $A \times G$ gibt, definieren wir die Abbildung $\varphi : A \times G \to E$ mittels der natürlichsten Vorschrift, die uns überhaupt einzufallen vermag:

$$\varphi : A \times G \longrightarrow E, \quad (a,g) \longmapsto i(a)s(g) = as(g). \tag{1.2}$$

Suchen wir doch jetzt noch eine möglichst natürliche Abbildung $\psi : E \to A \times G$ in der Hoffnung, dass φ und ψ zueinander inverse Abbildungen sind. Also $e \mapsto (?, \pi(e))$ liegt auf der Hand, aber $? = i^{-1}(e)$ muss nicht unbedingt existieren. Hierfür benötigen wir dann schon ein Element aus $\mathrm{im}(i) = \ker(\pi)$. Unter Ausnutzung der Schnitt-Eigenschaft $\pi \circ s = \mathrm{id}_G$ stellen wir fest, dass $e \cdot s(\pi(e))^{-1}$ im Kern von π liegt, und wir definieren daher:

$$\psi : E \longrightarrow A \times G, \quad e \longmapsto \left(e \cdot s(\pi(e))^{-1}, \pi(e)\right).$$

Einfaches Nachrechnen ergibt sofort $\psi \circ \varphi = \mathrm{id}_{A\times G}$ und $\varphi \circ \psi = \mathrm{id}_E$, womit die mengentheoretische Äquivalenz von E und $A \times G$ nachgewiesen ist. Es sei angemerkt, dass wir

für diesen Nachweis die Homomorphismus-Eigenschaft von s *nicht* benötigt haben. Darauf werden wir in einem späteren Abschnitt noch einmal zurückgreifen. Wir können nun die Gruppenstruktur von E mittels φ und ψ auf $A \times G$ übertragen. Möchten wir zwei Elemente (a_1, g_1) und (a_2, g_2) multiplizieren, so multiplizieren wir einfach die enstprechenden Elemente $a_1\, s(g_1)$ und $a_2\, s(g_2)$ in E, und mit Hilfe der Vertauschungsregel (vgl. Bemerkung 1.9) erhalten wir

$$a_1\,[s(g_1)a_2]\,s(g_2) = a_1\,[(g_1.a_2)s(g_1)]\,s(g_2) = (a_1 + g_1.a_2)s(g_1g_2),$$

also

$$(a_1, g_1) \cdot (a_2, g_2) = (a_1 + g_1.a_2, g_1g_2),$$

was dem Gruppengesetz des semidirekten Produktes $A \rtimes G$ entspricht (vgl. Defintion 1.14). Nach Definition 1.11 über die Äquivalenz von Extensionen mit G-Moduln bleibt also zu zeigen, dass das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\tilde{i}} & A \rtimes G & \xrightarrow{\tilde{\pi}} & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

kommutiert, d. h. $\varphi \circ \tilde{i} = i$ und $\pi \circ \varphi = \tilde{\pi}$. Dies ist der Fall, denn

$$\varphi(\tilde{i}(a)) = \varphi(a, 1) = i(a)s(1) = i(a)$$

und

$$\pi(\varphi(a, g)) = \pi(i(a)s(g)) = \pi(i(a))\pi(s(g)) = 1 \cdot g = \tilde{\pi}(a, g).$$

□

Wir haben nun unsere bis auf Äquivalenz einzige spaltende Extension von G mit A konstruiert. Erinnern wir uns an die Worte zu Beginn dieses Abschnittes, so ist es jetzt an der Zeit, die Menge aller möglichen Schnitte zu betrachten. Auch hier führen wir wieder einen Äquivalenzbegriff ein:

Definition 1.17 (A-Konjugiertheit)**.** Zwei Schnitte s_1 und s_2 einer spaltenden Extension

$$0 \longrightarrow A \xrightarrow{\tilde{i}} A \rtimes G \xrightarrow{\tilde{\pi}} G \longrightarrow 1$$

nennt man ***A*-konjugiert**, wenn es ein $a \in A$ gibt, sodass die folgende Gleichung gilt:

$$s_1(\cdot) = a\, s_2(\cdot)\, a^{-1}\ .$$

Bemerkung 1.18. Es ist sofort einsichtig, dass es sich bei der Relation der A-Konjugiertheit um eine Äquivalenzrelation handelt.

Ziel ist es nun, die Menge aller A-Konjugationsklassen mit Hilfe einer dazu bijektiven Menge darzustellen. Bei der Suche nach einer dafür geeigneten Menge stoßen wir auf die Definition der 1. Kohomologiegruppe, die auf die Definition von 1-Kozyklen und 1-Korändern aufbaut. Zur Übersichtlichkeit vorab die Definitionen, die jetzt noch künstlich scheinen mögen:

Definition 1.19 (1-Kozykel)**.** Gegeben sei eine Gruppe G und ein G-Modul A. Ein **1-Kozykel von G mit Koeffizienten in A** ist eine Abbildung $f : G \to A$ mit

$$f(g_1g_2) = f(g_1) + g_1.f(g_2)$$

für alle $g_1, g_2 \in G$. Die Menge $\mathrm{Z}^1(G, A)$ aller 1-Kozykel bildet mit werteweiser Addition eine abelsche Gruppe.

Bemerkung 1.20. Die Gruppeneigenschaften von $\mathrm{Z}^1(G, A)$ müssen natürlich nachgewiesen werden, liegen aber auf der Hand.

Definition 1.21 (1-Korand)**.** Gegeben sei eine Gruppe G und ein G-Modul A. Ein **1-Korand von G mit Koeffizienten in A** ist eine Abbildung

$$f_a : G \longrightarrow A, \quad g \longmapsto g.a - a$$

für ein $a \in A$. Die 1-Koränder bilden eine Untergruppe von $\mathrm{Z}^1(G, A)$, die mit $\mathrm{B}^1(G, A)$ bezeichnet wird.

Bemerkung 1.22. Dass $\mathrm{B}^1(G, A)$ tatsächlich eine Untergruppe von $\mathrm{Z}^1(G, A)$ ist, muss natürlich nachgewiesen werden. Der Beweis erfordert jedoch bloßes Nachrechnen und sei daher dem Leser überlassen.

Definition 1.23 (Erste Kohomologiegruppe)**.** Zwei 1-Kozyklen heißen **kohomolog**, wenn sie sich um einen 1-Korand unterscheiden. Die Faktorgruppe

$$\mathrm{H}^1(G, A) := \mathrm{Z}^1(G, A)/\,\mathrm{B}^1(G, A)$$

der Kohomologieklassen von 1-Kozyklen heißt **erste Kohomologiegruppe von G mit Koeffizienten in A**. Die Kohomologieklasse eines Kozykels f bezeichnen wir im Folgenden stets mit $[f]$.

Satz 1.24. *Gegeben sei die spaltende Extension*

$$0 \longrightarrow A \xrightarrow{\tilde{i}} A \rtimes G \xrightarrow{\tilde{\pi}} G \longrightarrow 1.$$

Dann gibt es eine natürliche Bijektion zwischen der Menge aller A-Konjugationsklassen von Schnitten (vgl. Definition 1.17) und $\mathrm{H}^1(G, A)$.

Beweis. Zuerst zeigen wir, dass es eine natürliche Bijektion zwischen der Menge aller möglichen Schnitte und der Gruppe $\mathrm{Z}^1(G, A)$ aller 1-Kozyklen gibt, danach dann, dass die Einteilung in A-Konjugationsklassen der Einteilung in Kohomologieklassen entspricht.

Betrachten wir eine Abbildung $s : G \to A \rtimes G$ mit $\tilde{\pi} \circ s = \mathrm{id}_G$, so stellen wir fest, dass sie die Form

$$s : G \longrightarrow A \rtimes G, \quad g \longmapsto (f(g), g)$$

hat, wobei f eine Abbildung $G \to A$ ist. Wegen

$$s(g_1)s(g_2) = (f(g_1), g_1) \cdot (f(g_2), g_2) = (f(g_1) + g_1.f(g_2), g_1g_2)$$

und

$$s(g_1g_2) = (f(g_1g_2), g_1g_2)$$

ist s genau dann ein Homomorphismus, also ein Schnitt, wenn f ein 1-Kozykel ist. Damit haben wir unsere Bijektion zwischen der Menge der Schnitte und $Z^1(G, A)$ gefunden. Zu zeigen bleibt, dass zwei Schnitte s_1 und s_2 genau dann A-konjugiert sind, wenn sich die dazu entsprechenden 1-Kozykel f_1 und f_2 um einen 1-Korand unterscheiden. Dies ergibt sich aber unmittelbar aus

$$\begin{aligned} & s_1(g) && = a \cdot s_2(g) \cdot \tilde{a}^{-1} \\ \iff & (f_1(g), g) && = (a, 1) \cdot (f_2(g), g) \cdot (a, 1)^{-1} \\ \iff & (f_1(g), g) && = (a + f_2(g), g) \cdot (-a, 1) \\ \iff & (f_1(g), g) && = (a + f_2(g) - g.a, g) \\ \iff & f_2(g) - f_1(g) && = g.a - a, \end{aligned}$$

für alle $a \in A$ und $g \in G$. □

1.3 Gruppenkohomologie im Grad 2 im Zusammenhang mit beliebigen Extensionen

Nachdem wir die erste Kohomologiegruppe kennen gelernt haben, wollen wir uns nun der zweiten widmen. Dieses Mal werden wir hierfür jedoch nicht nur die *spaltenden* Extensionen betrachten, sondern *beliebige* Extensionen einer Gruppe G mit einem G-Modul A. Im einleitenden Abschnitt über Extensionen haben wir bereits in Definition 1.11 den Begriff der Äquivalenz von Extensionen eingeführt. Ziel ist es nun, die Menge aller Äquivalenzklassen von Extensionen zu gegebenem G und A durch eine dazu bijektive Menge darzustellen. Hierbei werden wir auf natürliche Weise auf die Definition der 2. Kohomologie-Gruppe von G mit Koeffizienten in A stoßen, die wir formal mit $\mathrm{H}^2(G, A)$ bezeichnen werden.

Da wir es dieses Mal mit beliebigen Extensionen zu tun haben, die also nicht unbedingt spaltend sein müssen, gibt es im Allgemeinen auch keinen Schnitt. Geben wir aber die Forderung der Homomorphismus-Eigenschaft eines Schnittes auf – wir werden daher von einem *mengentheoretischen Schnitt* sprechen – so finden wir für eine Extension stets eine solche Abbildung:

Definition 1.25 (Extension mit mengentheoretischen Schnitt)**.** Gegeben sei eine Gruppe G und ein G-Modul A. Eine **mit einem mengentheoretischen Schnitt versehene Extension von G mit A** ist eine mit einer Abbildung $s : G \to A$ versehene Extension

$$0 \longrightarrow A \xrightarrow{i} E \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 1$$

von G mit A, sodass $\pi \circ s = \mathrm{id}_G$ gilt.

Bemerkung 1.26. Ein derartiges s existiert immer, da π surjektiv ist. Wir werden zur Vereinfachung im Folgenden nur von einem *Schnitt* reden und betonen besonders, falls dieser Schnitt auch ein Homomorphismus von Gruppen ist.

Definition 1.27 (Äquivalenz von Extensionen mit Schnitt)**.** Gegeben seien zwei mit Schnitten versehene Extensionen E_ν für $\nu = 1, 2$

$$0 \longrightarrow A \xrightarrow{i_\nu} E_\nu \underset{s_\nu}{\overset{\pi_\nu}{\rightleftarrows}} G \longrightarrow 1$$

einer Gruppe G mit einem G-Modul A. Wir nennen die beiden Extensionen **äquivalent**, wenn es einen Isomorphismus $\varphi : E_1 \to E_2$ gibt, sodass das Diagramm

$$\begin{array}{ccccccccc}
 & & & & \overset{s_1}{\curvearrowleft} & & & & \\
0 & \longrightarrow & A & \xrightarrow{i_1} & E_1 & \underset{\pi_1}{\rightarrow} & G & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \| & & \\
0 & \longrightarrow & A & \xrightarrow{i_2} & E_2 & \underset{s_2}{\overset{\pi_2}{\rightleftarrows}} & G & \longrightarrow & 1
\end{array}$$

kommutiert, d. h. $i_2 = \varphi \circ i_1$, $\pi_1 = \pi_2 \circ \varphi$ und $s_2 = \varphi \circ s_1$.

Bemerkung 1.28. Zwei äquivalente mit Schnitten versehene Extensionen sind natürlich erst recht äquivalent im Sinne von Definition 1.11.

Wozu jedoch nun diese neuen Begriffe? Wollten wir nicht einfach die Menge der Äquivalenzklassen von beliebigen Extensionen betrachten (vgl. Definition 1.11)? Um diese Menge zu erhalten, können wir anstatt einer direkten Einteilung in Äquivalenzklassen aber auch in folgenden zwei Schritten vorgehen: Zuerst betrachten wir die Menge aller mit einem Schnitt versehenen Extensionen von G mit A, teilen diese Menge dann enstprechend der Definition 1.27 in Äquivalenzklassen ein und identifizieren dann in einem zweiten Schritt Äquivalenzklassen, deren Repräsentanten sich bis auf Extensions-Äquivalenz (vgl. Definition 1.11) nur noch im Schnitt unterscheiden.

Diese auf Anhieb etwas kompliziert klingende Vorgehensweise hat einen ganz einfachen Grund. Betrachten wir nämlich zuerst einmal die Menge der Äquivalenzklasen von Extensionen mit Schnitt, so können wir mit Hilfe der Schnitte für jede Klasse einen Standard-Repräsentanten konstruieren, wodurch wir unsere etwas abstrakten Äquivalenzklassen besser in den Begriff bekommen. Dies haben wir ja bei den spaltenden Extensionen auch tun können, wo wir das semidirekte Produkt von A und G erhalten haben.

Der Konstruktion eines derartigen Standard-Repräsentanten wollen wir uns nun genauer widmen. Hierfür führen wir zuvor den Begriff des „Faktorsystems“ ein, der auch in anderen Gebieten der Mathematik von Bedeutung ist und sich für uns noch als äußerst nützlich erweisen wird. Unter der Fragestellung, für welche $g_1, g_2 \in G$ (im Kontext der Definition 1.25) der Schnitt s die Homomorphismus-Eigenschaft $s(g_1 g_2) = s(g_1)s(g_2)$ erfüllt, möchten wir eine Abbildung f auf der Menge $G \times G$ definieren, die auf genau solchen Paaren (g_1, g_2) verschwindet. Dies ist der Fall für das Produkt

$$s(g_1)s(g_2)s(g_1 g_2)^{-1},$$

welches Werte sogar in $\ker(\pi) = \mathrm{im}(i) = A$ annimmt:

$$\pi\left(s(g_1)s(g_2)s(g_1 g_2)^{-1}\right) = g_1 g_2 (g_1 g_2)^{-1} = 1 \ .$$

Definition 1.29 (Faktorsystem)**.** Gegeben sei eine mit einem Schnitt s versehene Extension

$$0 \longrightarrow A \xrightarrow{i} E \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 1 \tag{1.3}$$

einer Gruppe G mit einem G-Modul A. Unter dem **Faktorsystem** der Extension mit Schnitt (1.3) verstehen wir die Abbildung

$$f : G \times G \longrightarrow A, \quad (g_1, g_2) \longmapsto s(g_1)s(g_2)s(g_1g_2)^{-1}.$$

Das ist diejenige Abbildung f, die der folgenden Bedingung genügt:

$$s(g_1)s(g_2) = f(g_1, g_2)s(g_1g_2)\ . \tag{1.4}$$

Da wir das Faktorsystem einer Extension wie (1.3) als Abbildung nach A und nicht nach E definiert haben, ist es prinzipiell möglich, dass die Faktorsysteme für alle Repräsentanten einer Äquivalenzklasse identisch sind:

Lemma 1.30. *Sind zwei mit normalisiertem Schnitt versehene Extensionen äquivalent, so haben sie auch dasselbe Faktorsystem.*

Beweis. Man betrachte zwei solche Extensionen mit den Bezeichnungen aus Defintion 1.27. Dann gilt:

$$\begin{aligned} f'(g_1, g_2) &= s'(g_1)s'(g_2)s'(g_1g_2)^{-1} \\ &= \varphi(s(g_1)) \cdot \varphi(s(g_2)) \cdot \varphi(s(g_1g_2))^{-1} \\ &= \varphi\left(s(g_1)s(g_2)s(g_1g_2)^{-1}\right) = s(g_1)s(g_2)s(g_1g_2)^{-1} \\ &= f(g_1, g_2). \end{aligned}$$

□

Nun haben wir alles zusammen, um einen Standardrepräsentanten für jede Äquivalenzklasse von Extensionen mit Schnitten zu konstruieren. Dieser mag auf Anhieb gekünstelt scheinen, wir werden aber beim Beweis sehen, dass er sich genauso natürlich ergibt wie die Konstruktion des semidirekten Produktes im Falle der spaltenden Extensionen.

Lemma–Definition 1.31 (Standardrepraesentant@Standardrepräsentant)**.** *Gegeben sei eine mit einem Schnitt s versehende Extension*

$$0 \longrightarrow A \xrightarrow{i} E \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 1 \tag{1.5}$$

einer Gruppe G mit einem G-Modul A und dazugehörigen Faktorsystem f. Die Extension (1.5) ist äquivalent zur Extension

$$0 \longrightarrow A \xrightarrow{\tilde{i}} \tilde{E}_f \underset{\tilde{s}}{\overset{\tilde{\pi}}{\rightleftarrows}} G \longrightarrow 1\ , \tag{1.6}$$

wobei $\tilde{E}_f$ die aus der Menge $A \times G$ bestehende Gruppe mit dem Gruppengesetz

$$(a_1, g_1) \cdot (a_2, g_2) := (a_1 + g_1.a_2 + f(g_1, g_2), g_1g_2) \tag{1.7}$$

und $\tilde{i}$, $\tilde{\pi}$ und $\tilde{s}$ die Abbildungen $a \mapsto (a - a_1, 1)$, $(a, g) \mapsto g$ bzw. $g \mapsto (0, g)$ sind, und $a_1 = s(1) \in A$ bezeichnet. Da die Extension (1.6) eindeutig durch A, G und f bestimmt ist, können wir sie wegen Lemma 1.30 im Folgenden **Standardrepräsentant** *der Äquivalenzklasse von (1.5) nennen.*

Beweis. Wie bei den spaltenden Extensionen zeigt man, dass die Abbildung

$$\varphi : A \times G \longrightarrow E, \quad (a, g) \longmapsto i(a)s(g).$$

eine Bijektion ist, vgl. Beweis zu Satz 1.16 mit (1.2). Denn wir haben damals für den Nachweis die Homomorphismuseigenschaft von s nicht benötigt. Mittels φ übertragen wir die Gruppenstruktur von E auf $A \times G$ übertragen. Wir wollen nun zeigen, dass das sich daraus ergebende Gruppengesetz gerade mit (1.7) übereinstimmt, also bereits durch das Faktorsystem f eindeutig bestimmt ist. Dies rechtfertigt die Bezeichnung $\tilde{E}_f$. Möchten wir zwei Elemente (a_1, g_1) und (a_2, g_2) multiplizieren, so multiplizieren wir wieder einfach die entsprechenden Elemente $a_1 s(g_1)$ und $a_2 s(g_2)$ in E, und mit Hilfe der Vertauschungsregel (vgl. Bemerkung 1.9) und (1.4) erhalten wir

$$\begin{aligned} a_1 \left[s(g_1)i(a_2)\right] s(g_2) &= a_1 \left[i(g_1.a_2)s(g_1)\right] s(g_2) \\ &= (a_1 + g_1.a_2) \left[s(g_1)s(g_2)\right] \\ &= (a_1 + g_1.a_2)\, f(g_1, g_2)\, s(g_1 g_2) \\ &= (a_1 + g_1.a_2 + f(g_1, g_2))\, s(g_1 g_2), \end{aligned}$$

also

$$(a_1, g_1) \cdot (a_2, g_2) = (a + g_1.a_2 + f(g_1, g_2), g_1 g_2).$$

Wir haben nun mittels φ eine zu E isomorphe Gruppe $\tilde{E}_f$ konstruiert, die nur von A, G und f abhängt, also die beste Voraussetzung dafür, einen Standardrepräsentanten für die Äquivalenzklasse von (1.5) zu erhalten. Als nächstes übertragen wir nun mit Hilfe des Isomorphismus φ auch die Abbildungen i, π und s, d. h. wir konstruieren die Abbildungen $\tilde{i}$, $\tilde{\pi}$ und $\tilde{s}$, sodass das das Diagramm

$$\begin{array}{ccccccccc} & & & & \overset{\tilde{s}}{\curvearrowleft} & & & & \\ 0 & \longrightarrow & A & \xrightarrow{\tilde{i}} & \tilde{E}_f & \xrightarrow[\tilde{\pi}]{} & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow[s]{\pi} & G & \longrightarrow & 1 \end{array}$$

kommutiert (d. h. $i = \varphi \circ \tilde{i}$, $\tilde{\pi} = \pi \circ \varphi$ und $s = \varphi \circ \tilde{s}$). Dabei erhalten wir die im Satz beschriebenen natürlichen Abbildungen:

$$\tilde{i}(a) := \varphi^{-1}(i(a)) = \varphi^{-1}(i(a - a_1)s(1)) = (a - a_1, 1))$$

und

$$\tilde{\pi}(a, g) := \pi(\varphi(a, g)) = \pi(i(a)s(g)) = \pi(i(a)) \cdot \pi(s(g)) = g$$

und

$$\tilde{s}(g) := \varphi^{-1}(s(g)) = \varphi^{-1}(i(0)s(g)) = (0, g).$$

Da alle diese drei Abbildungen natürlich sind, also nur von A, G und $\tilde{E}_f$ abhängen, haben wir einen Standardrepräsentanten konstruiert. □

Wir haben es also nun geschafft, für jede Äquivalenzklasse von mit einem Schnitt versehenen Extensionen von G mit A einen Standardrepräsentanten zu konstruieren. Dieser ist schon eindeutig durch das Faktorsystem einer Klasse gegeben. Zwei verschiedene Äquivalenzklassen haben logischerweise auch verschiedene Faktorsysteme, denn sonst hätten sie ja denselben Standardrepräsentanten. Wir stellen also fest, dass die Menge aller Äquivalenzklassen bijektiv zu der Menge aller möglichen Faktorsysteme ist.

Diese Menge aller möglichen Faktorsysteme möchten wir daher jetzt bestimmen. Nach Definition eines Faktorsystems und Lemma–Definition 1.31 erfüllt die Verknüpfung 1.7 das Assoziativgesetz:

$$[(a_1, g_1)\,(a_2, g_2)]\,(a_3, g_3) = (a_1, g_1)\,[(a_2, g_2)\,(a_3, g_3)]$$

für alle $a_1, a_2, a_3 \in A$ und $g_1, g_2, g_3 \in G$. Ausmultiplizieren beider Seiten ergibt

$$(a_1 + g_1.a_2 + f(g_1g_2) + (g_1g_2).a_3 + f(g_1g_2, g_3), g_1g_2g_3)$$

für die linke und

$$(a_1 + g_1.a_2 + g_1.(g_2.a_3) + g_1.f(g_2, g_3) + f(g_1, g_2g_3), g_1g_2g_3)$$

für die rechte Seite. Das Assoziativgesetz ist also genau dann stets erfüllt, wenn die Abbildung f für alle $g_1, g_2, g_3 \in G$ der Gleichung

$$f(g_1, g_2) + f(g_1g_2, g_3) = g_1.f(g_2, g_3) + f(g_1, g_2g_3)$$

bzw. der Gleichung

$$g_1.f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3) - f(g_1, g_2) = 0 \tag{1.8}$$

genügt. Wir zeigen in Satz 1.34, dass (1.8) die entscheidende Eigenschaft der Abbildung f ist. Vorher wollen wir solchen f jedoch noch einen Namen geben:

Definition 1.32 (2-Kozykel)**.** Gegeben sei eine Gruppe G und ein G-Modul A. Ein **2-Kozykel von G mit Koeffizienten in A** ist eine Abbildung $f : G \times G \to A$ mit

$$g_1.f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3) - f(g_1, g_2) = 0$$

für alle $g_1, g_2, g_3 \in G$. Die Menge $\mathrm{Z}^2(G, A)$ aller 2-Kozykel bildet mit werteweiser Addition eine abelsche Gruppe.

Bemerkung 1.33. Die Gruppeneigenschaften von $\mathrm{Z}^2(G, A)$ müssen natürlich nachgewiesen werden, was jedoch durch einfaches Nachrechnen geschieht.

Satz 1.34. *Gegeben sei eine Gruppe G und ein G-Modul A. Dann gibt es eine natürliche Bijektion zwischen $\mathrm{Z}^2(G, A)$ und der Menge aller Äquivalenzklassen von mit einem Schnitt versehenen Extensionen von G mit A.*

Beweis. Wir haben bereits gesehen, dass wir jeder Äquivalenzklasse eindeutig ein Faktorsystem zuordnen können, dass dieses in $\mathrm{Z}^2(G, A)$ enthalten ist und dass diese Zuordnung

injektiv ist, d. h. zwei verschiedenen Äquivalenzklassen werden auch verschiedene 2-Kozykel zugeordnet. Zu zeigen bleibt die Surjektivität dieser Zuordnung!

Hierfür sei ein beliebiger 2-Kozykel f gegeben. Wir zeigen, dass $\tilde{E}_f = A \times G$ mit der Multiplikation (1.7)

$$(a_1, g_1) \cdot (a_2, g_2) := (a_1 + g_1.a_2 + f(g_1, g_2), g_1 g_2)$$

eine Gruppe ist, und dass die natürlichen Abbildungen $\tilde{i} : A \to \tilde{E}_f, a \mapsto (a - a_1, 1)$ mit $a_1 = f(1,1)$ und $\tilde{\pi} : \tilde{E}_f \to G, (a, g) \mapsto g$ in der Tat Gruppenhomomorphismen sind, dass die natürliche Abbildung $\tilde{s} : G \to \tilde{E}_f, g \mapsto (0, g)$ ein mengentheoretischer Schnitt ist, dass die Sequenz

$$0 \longrightarrow A \xrightarrow{\tilde{i}} \tilde{E}_f \underset{\tilde{s}}{\overset{\tilde{\pi}}{\rightleftarrows}} G \longrightarrow 1 \tag{1.9}$$

dann eine mit einem Schnitt versehene Extension von G mit A ist und dass der dieser Extension zugeordnete 2-Kozykel gerade f ist.

Das alles müssen wir jetzt zeigen: Die Assoziativität der Multiplikation von $\tilde{E}_f$ gilt wegen der 2-Kozykel-Bedingung. Das haben wir bereits gesehen. Das neutrale Element ist durch $(-a_1, 1)$ gegeben: setzt man in die 2-Kozykelgleichung (1.8) die Elemente $g_1 = g_2 = 1$ und $g_3 = g$, so folgt

$$f(1, g) = f(1, 1) = a_1,$$

und setzt man $g_1 = g$ und $g_2 = g_3 = 1$, so folgt

$$g.f(1, 1) = f(g, 1).$$

Daher gilt

$$(-a_1, 1)(a, g) = (-a_1 + a + f(1, g), g) = (a, g),$$

und

$$(a, g)(-a_1, 1) = (a - g.a_1 + f(g, 1), g) = (a, g).$$

Das Linksinverse von (a, g) ist $(-a_1 - g^{-1}.a - f\left(g^{-1}, g\right), g^{-1})$, das Rechtsinverse ist durch $(g^{-1}.(-a - a_1 - f\left(g, g^{-1}\right)), g^{-1})$ gegeben:

$$\left(-a_1 - g^{-1}.a - f\left(g^{-1}, g\right), g^{-1}\right)(a, g) = (-a_1, 1),$$
$$(a, g)\left(g^{-1}.\left(-a - a_1 - f\left(g, g^{-1}\right)\right), g^{-1}\right) = (-a_1, 1).$$

Links- und Rechtsinverses sind wegen der Assoziativität der Multiplikation identisch. Der Nachweis der notwendigen Eigenschaften von $\tilde{i}$, $\tilde{\pi}$ und $\tilde{s}$ erfordert einfaches Nachrechnen und sei an dieser Stelle dem Leser überlassen.

Die Sequenz (1.9) ist exakt, da $\tilde{i}$ injektiv und $\tilde{\pi}$ surjektiv sind und da $\mathrm{im}(\tilde{i}) = \ker(\tilde{\pi})$ gilt. Die durch (1.9) induzierte G-Modulstruktur auf A (vgl. Lemma 1.8) entspricht der gegebenen, denn für beliebiges $g \in G$ und $a \in A$ gilt:

$$\begin{aligned}
& \tilde{i}^{-1}\left((0, g) \cdot \tilde{i}(a) \cdot (0, g)^{-1}\right) \\
= \; & \tilde{i}^{-1}\left((0, g) \cdot (a - a_1, 1) \cdot (0, g)^{-1}\right) \\
= \; & \tilde{i}^{-1}\left(g.a - g.a_1 + f(g, 1), g) \cdot \left(-g^{-1}.\left(a_1 + f\left(g, g^{-1}\right)\right), g^{-1}\right)\right) \\
= \; & \tilde{i}^{-1}\left(g.a - g.a_1 + f(g, 1) - a_1 - f\left(g, g^{-1}\right) + f\left(g, g^{-1}\right), 1\right) \\
= \; & \tilde{i}^{-1}\left(g.a - a_1, 1\right) \\
= \; & g.a,
\end{aligned}$$

denn $g.a_1 = g.f(1,1) = f(g,1)$ (siehe oben). Damit ist (1.9) in der Tat eine mit einem Schnitt versehene Extension von G mit dem G-Modul A ist. Weiter ist das zugeordnete Faktorsystem wirklich f, denn nach Definition 1.29 ist das Faktorsystem von (1.9) gerade *die* Abbildung $G \times G \to A$, die einem Paar (g_1, g_2) mit $g_1, g_2 \in G$ das Element

$$\begin{aligned}
& \tilde{i}^{-1}\left(\tilde{s}(g_1)\cdot\tilde{s}(g_2)\cdot\tilde{s}(g_1g_2)^{-1}\right)\\
= \;& \tilde{i}^{-1}\left((0,g_1)\cdot(0,g_2)\cdot(0,g_1g_2)^{-1}\right)\\
= \;& \tilde{i}^{-1}\left((f(g_1,g_2),g_1g_2)\cdot\left(-\left(g_2^{-1}g_1^{-1}\right).\left(a_1+f\left(g_1g_2,g_2^{-1}g_1^{-1}\right)\right),g_2^{-1}g_1^{-1}\right)\right)\\
= \;& \tilde{i}^{-1}\left(f(g_1,g_2)-a_1-f\left(g_1g_2,g_2^{-1}g_1^{-1}\right)+f\left(g_1g_2,g_2^{-1}g_1^{-1}\right),1\right)\\
= \;& f(g_1,g_2)
\end{aligned}$$

zuordnet. □

Erinnern wir uns nun zurück an die Worte relativ zu Anfang dieses Abschnittes: Wir haben jetzt die Menge aller mit einem Schnitt versehenen Extensionen von G mit A in Äquivalenzklassen eingeteilt und bereits durch die dazu bijektive Menge $\mathrm{Z}^2(G,A)$ beschrieben. In einem zweiten Schritt wollen wir nun *diejenigen* Äquivalenzklassen identifizieren, deren Repräsentanten sich bis auf Extensions-Äquivalenz (vgl. Definition 1.11) nur noch durch den gewählten Schnitt unterscheiden, sodass wir also die eigentliche Menge erhalten, um die es geht, nämlich die Menge aller Äquivalenzklassen von beliebigen Extensionen von G mit A. Gehen wir bei der Menge $\mathrm{Z}^2(G,A)$ parallel dazu vor, so erhalten wir auch wieder unsere entsprechende Darstellungsmenge.

Zuerst machen wir uns mit dem Begriff des 2-Korandes vertraut, auch wenn sich dieser danach noch auf ganz natürliche Weise ergeben wird:

Definition 1.35 (2-Korand)**.** Gegeben sei eine Gruppe G und ein G-Modul A. Ein **2-Korand von G mit Koeffizienten in A** ist eine Abbildung

$$f_\eta : G \times G \longrightarrow A, \quad (g_1,g_2) \longmapsto g_1.\eta(g_2) - \eta(g_1g_2) + \eta(g_1)$$

mit einer beliebigen Abbildung $\eta : G \to A$. Die 2-Koränder bilden eine Untergruppe von $\mathrm{Z}^2(G,A)$, die wir fortan mit $\mathrm{B}^2(G,A)$ bezeichnen werden.

Bemerkung 1.36. Dass $\mathrm{B}^2(G,A)$ tatsächlich eine Untergruppe von $\mathrm{Z}^2(G,A)$ ist, muss natürlich nachgewiesen werden. Der Beweis erfordert jedoch bloßes Nachrechnen und sei daher dem Leser überlassen.

Lemma 1.37. *Gegeben sei eine Gruppe G, ein G-Modul A und zwei beliebige mit Schnitten versehene Extensionen von G mit A. Dann sind die beiden Extensionen (unter Nichtbeachtung ihrer Schnitte) genau dann äquivalent im Sinne von Definition 1.11, wenn die Differenz ihrer Faktorsysteme ein 2-Korand ist.*

Beweis. Unsere zwei mit Schnitten versehenen Extensionen seien durch

$$0 \longrightarrow A \xrightarrow{i} E \underset{s}{\overset{\pi}{\rightleftarrows}} G \longrightarrow 1 \tag{1.10}$$

und

$$0 \longrightarrow A \xrightarrow{i'} E' \underset{s'}{\overset{\pi'}{\rightleftarrows}} G \longrightarrow 1 \tag{1.11}$$

gegeben. Sind (1.10) und (1.11) äquivalent im Sinne der Definition 1.11, so gibt es einen Isomorphismus $\varphi : E \to E'$, sodass das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{i'} & E' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \end{array}$$

kommutiert. Aus $\pi' \circ s' = \mathrm{id}_G = \pi \circ s$ folgt daher $\pi' \circ s' = \pi' \circ \varphi \circ s$, also

$$\pi' \left(s'(g) \cdot \varphi(s(g))^{-1} \right) = 1$$

für alle $g \in G$. Wegen $\ker(\pi') = \mathrm{im}(i')$ gibt es daher eine Abbildung $\eta : G \to A$ mit $s'(g) \cdot \varphi(s(g))^{-1} = i'(\eta(g))$, also

$$s'(g) = i'(\eta(g)) \cdot \varphi(s(g)) \tag{1.12}$$

für alle $g \in G$. Wir haben nun den Schnitt s' in Abhängigkeit von s dargestellt. Damit wollen wir nun auch die zu zeigende Beziehung zwischen f' und f herleiten, dass nämlich die Differenz ein 2-Korand ist. Nach Gleichung (1.4) aus der Definition eines Faktorsystemes (vgl. Definition 1.29), gilt $s(g_1)s(g_2) = i(f(g_1, g_2))s(g_1g_2)$ und $s'(g_1)s'(g_2) = i'(f'(g_1, g_2))s'(g_1g_2)$ für alle $g_1, g_2 \in G$. Damit erhalten wir unter anderem mit Hilfe der Vertauschungsregel (1.9)

$$\begin{aligned} & i'(f'(g_1, g_2)) \cdot s'(g_1g_2) \\ = \; & s'(g_1) \cdot s'(g_2) \\ = \; & i'(\eta(g_1)) \cdot [\varphi(s(g_1)) \cdot i'(\eta(g_2))] \cdot \varphi(s(g_2)) \\ = \; & i'(\eta(g_1)) \cdot i'[g_1.\eta(g_2)] \cdot \varphi(s(g_1))) \cdot \varphi(s(g_2)) \\ = \; & i'(\eta(g_1) + g_1.\eta(g_2)) \cdot \varphi(s(g_1)s(g_2)) \\ = \; & i'(\eta(g_1) + g_1.\eta(g_2)) \cdot \varphi\big(i(f(g_1, g_2))s(g_1g_2)\big) \\ = \; & i'(\eta(g_1) + g_1.\eta(g_2)) \cdot i'(f(g_1, g_2)) \cdot \varphi(s(g_1g_2)) \\ = \; & i'(\eta(g_1) + g_1.\eta(g_2) + f(g_1, g_2)) \cdot i'(\eta(g_1g_2))^{-1} \cdot i'(\eta(g_1g_2)) \cdot \varphi(s(g_1g_2)) \\ = \; & i'(\eta(g_1) + g_1.\eta(g_2) + f(g_1, g_2) - \eta(g_1g_2)) \cdot s'(g_1g_2) \end{aligned}$$

für alle $g_1, g_2 \in G$, also

$$f'(g_1, g_2) - f(g_1, g_2) = g_1.\eta(g_2) - \eta(g_1g_2) + \eta(g_1), \tag{1.13}$$

d. h. $f' - f$ ist ein 2-Korand.

Sei nun umgekehrt bei gegebenem (1.10) und (1.11) die Differenz der zugehörigen Faktorsysteme f und f' ein 2-Korand, d. h. es gebe eine Abbildung $\eta : G \to A$, die der Bedingung (1.13) genügt. Unsere Idee ist es nun, zu (1.10) einen (mengentheoretischen)

normalisierten Schnitt s^* zu konstruieren, sodass die Extension das Faktorsystem f' bekommt. Die neu erhaltene Extension ist natürlich noch weiterhin äquivalent zu (1.10) im Sinne von Definition 1.11. Sie ist jedoch auch äquivalent zu (1.11) (da hier wegen der gleichen Faktorsysteme sogar Äquivalenz im Sinne von Definition 1.27 gelten muß und da diese Eigenschaft nach Bemerkung 1.28 die stärkere ist). Gelingt uns also die Konstruktion von s^*, so haben wir die Rückrichtung des Satzes bewiesen.

Der Beweis der Hinrichtung gibt uns die richtige Idee für die Konstruktion von s^*. Schauen wir uns nämlich Gleichung (1.12) noch einmal an, so haben wir bereits die gesuchte Beziehung, wenn wir statt φ die Identität und statt i' einfach i nehmen (das macht insofern Sinn, da wir ja die Extension in ihren Abbildungen beibehalten und nur s verändern). Wir definieren also

$$s^*(g) := i(\eta(g)) \cdot s(g)$$

für alle $g \in G$. Dies ist tatsächlich ein Schnitt, da $\pi(s^*(g)) = \pi(i(\eta(g))) \cdot \pi(s(g)) = 1 \cdot g$ gilt. Dieselben Umformungen wie oben zeigen uns dann, dass

$$f^*(g_1, g_2) - f(g_1, g_2) = g_1.\eta(g_2) - \eta(g_1 g_2) + \eta(g_1)$$

für alle $g_1, g_2 \in G$ gilt, d. h. $f^* = f'$. □

Definition 1.38 (Zweite Kohomologiegruppe)**.** Im Kontext der Definitionen 1.32 und 1.35 nennt man zwei 2-Kozyklen **kohomolog**, wenn sie sich um einen 2-Korand unterscheiden. Die Faktorgruppe

$$\mathrm{H}^2(G, A) := \mathrm{Z}^2(G, A) / \mathrm{B}^2(G, A)$$

der Kohomologieklassen von 2-Kozyklen heißt **zweite Kohomologiegruppe von G mit Koeffizienten in A**. Die Kohomologieklasse eines Kozykels f bezeichnen wir im Folgenden stets mit $[f]$.

Wir haben nun den folgenden wichtigen Satz, der uns eine Interpretation für die Kohomologieklassen von 2-Kozyklen liefert.

Satz 1.39. *Gegeben sei eine Gruppe G und ein G-Modul A. Dann gibt es eine natürliche Bijektion zwischen der Menge aller Äquivalenzklassen von Extensionen von G mit A und der zweiten Kohomologiegruppe* $\mathrm{H}^2(G, A)$.

Beweis. Lemma 1.37 gilt natürlich nicht nur für einzelne Repräsentanten, sondern wegen Lemma 1.30 für die ganzen Äquivalenzklassen, genauer: Die Repräsentanten zweier Äquivalenzklassen von mit einem Schnitt versehenen Extensionen sind genau dann paarweise äquivalent im Sinne von Definition 1.11, d. h. unter Nichtbeachtung ihrer Schnitte, wenn die Differenz der Faktorsysteme der Äquivalenzklassen ein 2-Korand ist. Zusammen mit Satz 1.34 ergibt das sofort die zu zeigende Aussage. □

1.4 Die lange exakte Sequenz der Kohomologiegruppen in den Graden 0, 1 und 2

Schauen wir zurück, so können wir festhalten, dass wir uns ausgehend von Betrachtungen über Gruppen-Extensionen mit dem Begriff der Kohomologiegruppe in den Graden 1 und

2 näher auseinandergesetzt haben. Die Definition des Begriffs für den Grad 0 werden wir jetzt noch direkt nachholen:

Definition 1.40 (Nullte Kohomologie-Gruppe)**.** Gegeben sei eine Gruppe G und ein G-Modul A. Dann heißt die abelsche Untergruppe

$$A^G := \{a \in A \mid g.a = a \text{ für alle } g \in G\}$$

der G-invarianten Elemente von A die **nullte Kohomologiegruppe von G mit Koeffizienten in A**. Wir bezeichnen diese Gruppe formal auch mit $H^0(G, A)$.

Bemerkung 1.41. Dass es sich bei A^G tatsächlich um eine Untergruppe von A handelt, muss natürlich noch nachgewiesen werden. Der Nachweis erfordert jedoch nur einfaches Nachrechnen. A^G ist insbesondere nicht nur abelsche Untergruppe, sondern G-Untermodul. Allerdings operiert G nur trivial auf A, d.h. $g.a = a$ für alle $g \in G$ und $a \in A$, sodass die G-Modulstruktur nicht weiter von Interesse ist.

Zwar haben wir jetzt die Gruppenkohomologie in drei Graden definiert, aber bei solch verschiedenartigen Definitionen mag der eine oder andere Zweifel daran hegen, ob denn hier überhaupt ein Zusammenhang besteht, der es erlaubt, unsere Gruppen alle mit derselben Bezeichnung zu versehen. Wir werden zwar später im Seminar die gesamte Thematik systematisch angehen, wollen uns aber natürlich auch an dieser Stelle nicht einen ersten wichtigen und verblüffenden Zusammenhang entgehen lassen, der sich hinter dem Begriff der *langen exakten Sequenz* verbirgt.

Erinnern wir uns an die Definition einer exakten Sequenz von Gruppenhomomorphismen zurück! Diesen Begriff können wir auch ohne Weiteres auf G-Moduln ausdehnen, wenn wir noch kurz die Definition eines G-Modulhomomorphismus zur Kenntnis nehmen. Außerdem werden wir feststellen, dass ein solcher G-Modulhomomorphismus stets natürliche Abbildungen zwischen den jeweiligen nullten, ersten bzw. zweiten Kohomolgiegruppen induziert:

Definition 1.42 (G-Modulhomomorphismus)**.** Eine Abbildung $\varphi : A \to B$ zwischen G-Moduln A und B heiße **G-Modulhomomorphismus**, wenn sie ein Gruppenhomomorphismus ist, der zusätzlich **G-äquivariant** ist, d. h. der

$$\varphi(g.a) = g.\varphi(a)$$

für alle $g \in G$ und $a \in A$ erfüllt.

Definition 1.43 (Kurze exakte Sequenz von G-Modulhomomorphismen)**.** Gegeben sei eine Gruppe G. Eine Sequenz von G-Modulhomomorphismen der Form

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

heiße **kurze exakte Sequenz von G-Modulhomomorphismen**, wenn i injektiv und π surjektiv ist und wenn $\mathrm{im}(i) = \ker(\pi)$ gilt.

Lemma 1.44. *Gegeben sei eine Gruppe G und ein G-Modulhomomorphismus $\varphi : A \to B$. Dann sind die von φ auf natürliche Weise induzierten Abbildungen*

$$\varphi_0 : \mathrm{H}^0(G, A) \longrightarrow \mathrm{H}^0(G, B), \qquad a \longmapsto \varphi(a) \tag{1.14}$$
$$\varphi_1 : \mathrm{H}^1(G, A) \longrightarrow \mathrm{H}^1(G, B), \qquad [f] \longmapsto [\varphi \circ f] \tag{1.15}$$
$$\varphi_2 : \mathrm{H}^2(G, A) \longrightarrow \mathrm{H}^2(G, B), \qquad [f] \longmapsto [\varphi \circ f] \tag{1.16}$$

wohldefinierte Gruppenhomomorphismen.

Beweis. Wir zeigen die Wohldefiniertheit der drei Abbildungen. Die Homomorphismuseigenschaft ist dann trivial.

Zu (1.14): Sei $a \in \mathrm{H}^0(G, A)$, d. h. a ist G-invariant. Dann ist auch $\varphi(a)$ ein G-invariantes Element aus B, liegt also in $\mathrm{H}^0(G, B)$, denn

$$g.\varphi(a) = \varphi(g.a) = \varphi(a)$$

für alle $g \in G$.

Zu (1.15): Sei $f : G \to A$ ein Kozykel von G mit Koeffizienten in A, d. h. $f(g_1 g_2) = f(g_1) + g_1.f(g_2)$ für alle $g_1, g_2 \in G$. Dann ist $(\varphi \circ f) : G \to B$ wegen der G-Modul-Homomorphismuseigenschaft von φ ein Kozykel von G mit Koeffizienten in B, denn

$$(\varphi \circ f)(g_1 g_2) = \varphi(f(g_1) + g_1.f(g_2)) = (\varphi \circ f)(g_1) + g_1.(\varphi \circ f)(g_2)$$

für alle $g_1, g_2 \in G$. Die Zuordnung $[f] \mapsto [\varphi \circ f]$ ist unabhängig von der Wahl des Repräsentanten f, da zu einem zu f kohomologen f' auch die Kozykel $\varphi \circ f$ und $\varphi \circ f'$ kohomolog sind, denn wenn $f_a : G \to A, g \mapsto g.a - a$ für geeignet gewähltes $a \in A$ der Korand $(f - f')$ ist, so ist $(\varphi \circ f - \varphi \circ f')$ der Korand $f_b : G \to B, g \mapsto g.b - b$ mit $b := \varphi(a)$:

$$(\varphi \circ f - \varphi \circ f')(g) = \varphi \circ (f - f')(g) = \varphi(g.a - a) = g.\varphi(a) - \varphi(a).$$

Zu (1.16): Auch hier ist der Nachweis der Wohldefiniertheit stupides Nachrechnen und sei daher dem eifrigen Leser überlassen. □

Satz 1.45 (Lange exakte Sequenz in den Kohomologiegruppen)**.** *Gegeben sei eine Gruppe G und eine kurze exakte Sequenz*

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

von G-Modulhomomorphismen. Dann gibt es Gruppenhomomorphismen $\delta^1 : \mathrm{H}^0(G, C) \to \mathrm{H}^1(G, A)$ und $\delta^2 : \mathrm{H}^1(G, C) \to \mathrm{H}^2(G, A)$, sodass die Sequenz

$$\begin{array}{l} 0 \longrightarrow H^0(G, A) \xrightarrow{i_0} \mathrm{H}^0(G, B) \xrightarrow{\pi_0} \mathrm{H}^0(G, C) \overset{\delta^1}{\frown} \\ \longrightarrow H^1(G, A) \xrightarrow{i_1} \mathrm{H}^1(G, B) \xrightarrow{\pi_1} \mathrm{H}^1(G, C) \overset{\delta^2}{\frown} \\ \longrightarrow H^2(G, A) \xrightarrow{i_2} \mathrm{H}^2(G, B) \xrightarrow{\pi_2} \mathrm{H}^2(G; C) \end{array}$$

von Gruppenhomomorphismen exakt ist. Genauer: Wir wählen

$$\delta^1 : \mathrm{H}^0(G, C) \longrightarrow \mathrm{H}^1(G, A), \quad c \longmapsto \left[g \mapsto i^{-1}(g.b - b) \right], \tag{1.17}$$

wobei b ein beliebiges Urbild von c unter π sei, und wir wählen

$$\delta^2 : \mathrm{H}^1(G, C) \longrightarrow \mathrm{H}^2(G, A), \quad [f] \longmapsto \left[(g_1, g_2) \mapsto i^{-1}(g_1.b_f(g_2) - b_f(g_1 g_2) + b_f(g_1)) \right], \tag{1.18}$$

wobei b_f eine beliebige Abbildung $G \to B$ von Mengen sei, die $\pi \circ b_f = f$ erfüllt (solche existieren wegen der Surjektivität von π). Die Abbildungen δ^1 und δ^2 nennen wir auch **Verbindungshomomorphismen**.

Beweis. Ziel ist es, auf möglichst natürliche Weise die im Satz angegebenen Definitionen der Verbindungshomomorphismen zu erhalten und dann die Exaktheit der gesamten Sequenz nachzuweisen.

Zur Definition von δ^1: Gegeben sei ein Element $c \in \mathrm{H}^0(G, C)$, d. h. also ein G-in-variantes Element aus C. Wir müssen nun diesem c die Kohomologieklasse eines 1-Kozykels $f : G \to A$ zuordnen, müssen also eine Abbildung definieren, die jedem $g \in G$ ein Element aus A zuordnet. Hierfür sei also auch ein beliebiges $g \in G$ gegeben. Um nun ein Element aus A zu erhalten, müssen wir uns aber irgendwie in $\mathrm{im}(i)$ bewegen, d. h. in $\ker(\pi)$. Das bekommen wir wie folgt hin: Man wähle zu unserem c ein beliebiges Urbild b unter der surjektiven Abbildung π. Wegen der G-Invarianz von c ist aber auch $g.b$ ein Urbild von c, denn $\pi(g.b) = g.\pi(b) = g.c = c$. Folglich gilt $(g.b - b) \in \ker(\pi) = \mathrm{im}(i)$, und wir können wegen der Injektivität von i die Abbildung δ^1 wie in (1.17) definieren. Die Abbildung $f : g \mapsto i^{-1}(g.b - b)$ ist in der Tat ein 1-Kozykel, da sie die Bedingung $f(g_1 g_2) = f(g_1) + g_1.f(g_2)$ erfüllt, wie man durch einfache Rechnung kontrolliert. Unser δ^1 ist wohldefiniert, da wir bei Wahl eines anderen Urbildes b' von c zwar den Kozykel $f' : g \mapsto i^{-1}(g.b' - b')$ erhalten würden, dieser aber in derselben Kohomologieklasse wie f liegt, da die Differenz ein 1-Korand ist:

$$(f - f')(g) = i^{-1}(g.(b - b') - (b - b')) = i^{-1}(g.i(a) - i(a)) = i^{-1}(i(g.a - a)) = g.a - a$$

mit $i(a) = b - b'$ (denn $(b - b') \in \ker(\pi) = \mathrm{im}(i)$). Der Nachweis der Homomorphismuseigenschaft von δ^1 erfolgt wieder durch einfaches Rechnen.

Zur Definition von δ^2: Gegeben sei eine beliebige Kohomologieklasse $[f]$ aus $\mathrm{H}^1(G, C)$, repräsentiert durch den 1-Kozykel $f : G \to C$. Mit Hilfe von f wollen wir nun einen 2-Kozykel $h : G \times G \to A$ konstruieren, der dann Repräsentant der zu $[f]$ zuzuordnenden Kohomologieklasse sein wird. Gegeben sei also auch ein beliebiges Paar $(g_1, g_2) \in G \times G$, mit dem wir ein Element aus A herleiten wollen. Wieder benötigen wir dafür ein Element aus $\mathrm{im}(i) = \ker(\pi)$. Dieses erhalten wir durch Umformen der 1-Kozykel-Bedingung von f:

$$\begin{aligned}
& f(g_1 g_2) = f(g_1) + g_1.f(g_2) \\
\Longrightarrow \quad & g_1.f(g_2) - f(g_1 g_2) + f(g_1) = 0 \\
\Longrightarrow \quad & g_1.(\pi(b_f(g_2))) - \pi(b_f(g_1 g_2)) + \pi(b_f(g_1)) = 0 \\
\Longrightarrow \quad & \pi(g_1.(b_f(g_2)) - b_f(g_1 g_2) + b_f(g_1)) = 0.
\end{aligned}$$

Damit lässt sich h wegen der Injektivität von i wie in (1.18) definieren, d. h. $h(g_1, g_2) := i^{-1}(g_1.(b_f(g_2)) - b_f(g_1g_2) + b_f(g_1))$. Bloßes Nachrechnen zeigt, dass es sich bei h tatsächlich um einen 2-Kozykel handelt. Zu zeigen bleibt, dass die Kohomologieklasse $[h]$ unabhängig von der Wahl der Abbildung b_f und sogar unabhängig vom Repräsentanten f von $[f]$ ist. Der Nachweis der Homomorphismuseigenschaft von δ^2 sei wieder dem Leser überlassen. Für den Beweis der Unabhängigkeit von der Wahl von b_f sei ein weiteres mögliches b'_f gegeben. Der entsprechende 2-Kozykel h' liegt dann aber in derselben Kohomologieklasse wie h, da die Differenz ein 2-Korand ist:

$$\begin{aligned}(h - h')(g_1, g_2) &= i^{-1}(g_1.(b_f - b'_f)(g_2) - (b_f - b'_f)(g_1g_2) + (b_f - b'_f)(g_1)) \\ &= i^{-1}(g_1.(i \circ a_f)(g_2) - (i \circ a_f)(g_1g_2) + (i \circ a_f)(g_1)) \\ &= i^{-1}(i(g_1.a_f(g_2) - a_f(g_1g_2) + a_f(g_1)) \\ &= g_1.a_f(g_2) - a_f(g_1g_2) + a_f(g_1) \\ &= \text{2-Korand}(g_1, g_2)\end{aligned}$$

mit $a_f : G \to A$ und $i \circ a_f = (b_f - b'_f)$ (denn $(b_f - b'_f)(g) \in \ker(\pi) = \mathrm{im}(i)$ für alle $g \in G$). Für den Beweis der Unabhängigkeit von der Wahl des 1-Kozykels f sei ein zu f kohomologer 1-Kozykel f' gegeben. Wieder liegt der entsprechende 2-Kozykel h' in derselben Kohomologieklasse wie h, da die Differenz ein 2-Korand ist. Dies zu zeigen, ist jedoch etwas schwieriger als es gerade beim Beweis für die Unabhängigkeit der Wahl von b_f der Fall war. Derselbe Ansatz

$$(h - h')(g_1, g_2) = i^{-1}(g_1.(b_f - b_{f'})(g_2) - (b_f - b_{f'})(g_1g_2) + (b_f - b_{f'})(g_1)) \quad (1.19)$$

führt nämlich zu dem Problem, dass dieses Mal $(b_f - b_{f'})(g)$ nicht grundsätzlich für alle $g \in G$ in $\mathrm{im}(i) = \ker(\pi)$ liegen muss, da $\pi((b_f - b_{f'})(g)) = (f - f')(g) = g.c - c$ gilt für ein fest gewähltes $c \in C$ (denn $f - f'$ ist ein 1-Korand). Wir verhelfen uns mit einem ganz einfachen Trick, indem wir für unser c ein beliebiges Urbild b (unter π) wählen. Wegen $g.c - c = g.\pi(b) - \pi(b) = \pi(g.b - b)$ gilt dann also:

$$((b_f - b_{f'})(g) - (g.b - b)) \in \ker(\pi) = \mathrm{im}(i),$$

und wir können $b_f - b_{f'}$ in der Form

$$(b_f - b_{f'})(g) = (g.b - b) + i(a_f(g)) \quad (1.20)$$

schreiben, wobei a_f die entsprechende (mengentheoretische) Abbildung $G \to A$ sei. Setzen wir nun (1.20) für die Werte g_2, g_1g_2 und g_1 in (1.19) ein, so erhalten wir nach einigen Umformungen:

$$\begin{aligned}(h - h')(g_1, g_2) &= g_1.a_f(g_2) - a_f(g_1g_2) + a_f(g_1) \\ &= \text{2-Korand}(g_1, g_2),\end{aligned}$$

was wir zeigen wollten.

Zur Exaktheit bei $\mathrm{H}^0(G, A)$*:* Die Abbildung i_0 ist als Einschränkung von i auf $\mathrm{H}^0(G; A)$ natürlich auch injektiv.

Zur Exaktheit bei $\mathrm{H}^0(G,B)$*:* Zu zeigen ist $\mathrm{im}(i_0) = \ker(\pi_0)$. Sei hierfür $i_0(a)$ gegeben mit $a \in \mathrm{H}^0(G;A)$. Dann ist $i_0(a) \in \ker(\pi_0)$, da $\pi_0(i_0(a)) = \pi(i(a)) = 0$ gilt, also $\mathrm{im}(i_0) \subseteq \ker(\pi_0)$. Sei umgekehrt $b \in \ker(\pi_0)$, also erst recht $b \in \ker(\pi) = \mathrm{im}(i)$, und somit gibt es ein $a \in A$ mit $i(a) = b$. Dieses a liegt sogar in $\mathrm{H}^0(G,A)$ (womit dann $b \in \mathrm{im}(i_0)$ gezeigt ist), denn a ist G-invariant:

$$i(a) = b$$

und

$$i(g.a) = g.i(a) = g.b = b$$

ergeben

$$g.a = a$$

für alle $g \in G$ wegen der Injektivität von i.

Zur Exaktheit bei $\mathrm{H}^0(G,C)$*:* Zu zeigen ist $\mathrm{im}(\pi_0) = \ker(\delta^1)$. Sei hierfür $\pi_0(b)$ gegeben mit $b \in \mathrm{H}^0(G,B)$. Dann ist $\pi_0(b) \in \ker(\delta^1)$, da

$$\begin{aligned}
\delta^1(\pi_0(b)) &= \delta^1(\pi(b)) \\
&= \left[g \longmapsto i^{-1}(g.b - b)\right] \\
&= \left[g \longmapsto i^{-1}(b - b)\right] \\
&= 0
\end{aligned}$$

gilt, also $\mathrm{im}(\pi_0) \subseteq \ker(\delta^1)$. Sei umgekehrt $c \in \ker(\delta^1)$ und sei b ein beliebiges Urbild von c unter π. Es ist leider nicht so, dass b dann automatisch bereits in $\mathrm{H}^0(G,B)$ liegt, d. h G-invariant ist. Dafür müssen wir es noch leicht verändern. Wegen $0 = \delta^1(c) = [g \mapsto i^{-1}(g.b - b)]$ ist der 1-Koyzkel $g \mapsto i^{-1}(g.b - b)$ ein 1-Korand. Es gibt also ein $a \in A$, sodass für alle $g \in G$ gilt:

$$\begin{aligned}
& i^{-1}(g.b - b) &&= g.a - a \\
\Longrightarrow \quad & g.b - b &&= i(g.a - a) \\
\Longrightarrow \quad & g.b - b &&= g.i(a) - i(a) \\
\Longrightarrow \quad & g.(b - i(a)) &&= b - i(a).
\end{aligned}$$

Somit ist $b - i(a)$ ein G-invariantes Element von B, d. h. aus $\mathrm{H}^0(G,B)$, insbesondere natürlich ein Urbild von c unter π (da wir b ja bloß durch Subtraktion eines Elementes aus $\ker(\pi)$ modifiziert haben). Folglich gilt $c \in \mathrm{im}(\pi_0)$.

Zur Exaktheit bei $\mathrm{H}^1(G,A)$*:* Zu zeigen ist $\mathrm{im}(\delta^1) = \ker(i_1)$. Sei hierfür $\delta^1(c)$ gegeben mit $c \in \mathrm{H}^0(G,C)$. Wählen wir für c ein beliebiges Urbild b unter π, so können wir zeigen, dass $\delta^1(c)$ in $\ker(i_1)$ liegt:

$$\begin{aligned}
i_1(\delta^1(c)) &= i_1\left(\left[g \longmapsto i^{-1}(g.b - b)\right]\right) \\
&= \left[i \circ \left(g \longmapsto i^{-1}(g.b - b)\right)\right] \\
&= [g \longmapsto g.b - b] \\
&= [\text{1-Korand}] \\
&= 0,
\end{aligned}$$

also $\mathrm{im}(\delta^1) \subseteq \ker(i_1)$. Sei umgekehrt $[f] \in \mathrm{H}^1(G,A)$ und $[f] \in \ker(i_1)$, also $0 = i_1([f]) = [i \circ f]$, und daher ist $i \circ f$ ein 1-Korand mit Koeffizienten in B. Es gibt also ein $b \in B$ mit $i \circ f = (g \mapsto g.b - b)$, und wegen der Injektivität von i erhalten wir

$$f = \big(g \longmapsto i^{-1}(g.b - b)\big)\,.$$

Das erinnert uns sofort an die Definition von δ^1. Wir brauchen nur zeigen, dass $\pi(b)$ in $\mathrm{H}^0(G,C)$ liegt, d. h. G-invariant ist, denn dann ist $[f] = \delta^1(\pi(b))$, also $[f] \in \mathrm{im}(\delta^1)$:

$$g.\pi(b) - \pi(b) = \pi(g.b - b) = \pi(i(f(g))) = 0.$$

Zur Exaktheit bei $\mathrm{H}^1(G,B)$*:* Zu zeigen ist $\mathrm{im}(i_1) = \ker(\pi_1)$. Sei hierfür $i_1([f])$ gegeben mit $[f] \in \mathrm{H}^1(G,A)$, d. h. $f : G \to A$ sei ein 1−Kozykel. Dann ist $i_1([f]) \in \ker(\pi_1)$, da

$$\pi_1(i_1([f])) = [\pi \circ i \circ f] = 0$$

gilt, also $\mathrm{im}(i_1) \subseteq \ker(\pi_1)$. Sei umgekehrt $[f] \in \mathrm{H}^1(G,B)$ und $[f] \in \ker(\pi_1)$, also $0 = \pi_1([f]) = [\pi \circ f]$, und daher ist $\pi \circ f$ ein 1-Korand mit Koeffizienten in C. Es gibt also ein $c \in C$ mit $\pi \circ f = (g \mapsto g.c - c)$. Nun wird es etwas trickreich. Wählen wir für c ein beliebiges Urbild b unter π, so erhalten wir durch Einsetzen von $\pi(b)$ für c und durch ein paar Umformungen

$$\pi(f(g)) = \pi(g.b - b)$$

für alle $g \in G$. Somit liegt die Differenz $f(g) - (g.b - b)$ in $\ker(\pi) = \mathrm{im}(i)$ für alle $g \in G$. Da

$$[f] = [f - (g \longmapsto g.b - b)]$$

gilt (denn die Repräsentanten unterscheiden sich nur um einen 1-Korand), können wir auch für die rechte Seite ein Urbild unter i_1 suchen. Der klare Vorteil hier ist nämlich, dass unser Repräsentant (auf alle $g \in G$ angewendet) immer in $\mathrm{im}(i)$ liegt. Es gibt also eine (wegen der Injektivität von i eindeutige) Abbildung $a_f : G \to A$ mit

$$f - (g \longmapsto g.b - b) = i \circ a_f.$$

Wir müssen nur noch zeigen, dass die Abbildung a_f ein 1-Kozykel mit Koeffizienten in A ist, denn dann gilt

$$i_1([a_f]) = [f - (g \longmapsto g.b - b)] = [f],$$

also $[f] \in \mathrm{im}(i_1)$. Da $i \circ a_f$ (als Differenz zweier 1-Kozykel) ein 1-Kozykel ist, gilt:

$$\begin{array}{rcl} (i \circ a_f)(g_1 g_2) & = & (i \circ a_f)(g_1) + g_1.(i \circ a_f)(g_2) \\ \Longrightarrow \quad i(a_f(g_1 g_2)) & = & i(a_f(g_1) + g_1.a_f(g_2)) \\ \Longrightarrow \quad a_f(g_1 g_2)) & = & a_f(g_1) + g_1.a_f(g_2) \\ \Longrightarrow \quad a_f & = & \text{1-Kozykel.} \end{array}$$

Zur Exaktheit bei $\mathrm{H}^1(G,C)$*:* Zu zeigen ist $\mathrm{im}(\pi_1) = \ker(\delta^2)$. Sei hierfür $\pi_1([f])$ gegeben mit $[f] \in \mathrm{H}^1(G,B)$, d. h. $f : G \to B$ sei ein 1-Kozykel. Dann ist $\pi_1([f]) \in \ker(\delta^2)$, da

$$\begin{array}{rcl} \delta^2(\pi_1([f])) & = & \delta^2([\pi \circ f]) \\ & = & \big[(g_1, g_2) \longmapsto i^{-1}(g_1.f(g_2) - f(g_1 g_2) + f(g_1))\big] \\ & = & \big[(g_1, g_2) \longmapsto i^{-1}(0)\big] \\ & = & 0 \end{array}$$

gilt, also $\mathrm{im}(\pi_1) \subseteq \ker(\delta^2)$. Sei umgekehrt $[f] \in \ker(\delta^2)$ und sei b_f eine beliebige (mengentheoretische) Abbildung $G \to B$, die $\pi \circ b_f = f$ erfüllt (existiert wegen der Surjektivität von π). Es muss natürlich nicht so sein, dass b_f dann automatisch bereits ein 1-Kozykel ist und quasi $[b_f]$ in $\mathrm{H}^1(G, B)$ liegt. Dafür müssen wir es noch leicht verändern. Wegen $0 = \delta^2([f]) = [(g_1, g_2) \mapsto i^{-1}(g_1.b_f(g_2) - b_f(g_1g_2) + b_f(g_1))]$ ist der 2-Koyzkel $(g_1, g_2) \mapsto i^{-1}(g_1.b_f(g_2) - b_f(g_1g_2) + b_f(g_1))$ ein 2-Korand. Es gibt also ein $\eta : G \to A$, sodass für alle $g_1, g_2 \in G$ gilt:

$$\begin{aligned} & i^{-1}(g_1.b_f(g_2) - b_f(g_1g_2) + b_f(g_1)) &&= g_1.\eta(g_2) - \eta(g_1g_2) + \eta(g_1) \\ \Longrightarrow \quad & g_1.b_f(g_2) - b_f(g_1g_2) + b_f(g_1) &&= i(g_1.\eta(g_2) - \eta(g_1g_2) + \eta(g_1)) \end{aligned}$$

$$\Longrightarrow g_1.(b_f - i \circ \eta)(g_2) - (b_f - i \circ \eta)(g_1g_2) + (b_f - i \circ \eta)(g_1) = 0$$

Somit ist $b_f - i \circ \eta$ ein 1-Kozykel von G mit Werten in B, d. h. $[b_f - i \circ \eta] \in \mathrm{H}^1(GB)$, insbesondere natürlich ein Urbild von $[f]$ unter π_1 (denn $\pi_1([b_f - i \circ \eta]) = [\pi \circ b_f - \pi \circ i \circ \eta] = [\pi \circ b_f]$). Folglich gilt $[f] \in \mathrm{im}(\pi_1)$.

Zur Exaktheit bei $\mathrm{H}^2(G, A)$ *und* $\mathrm{H}^2(G, B)$*:* Da hier nicht wirklich etwas wesentlich Neues passiert, außer dass die Beweise immer unübersichtlicher werden, sei dies dem interessierten Leser zur Übung gelassen. □

1.5 H^1 als Maß für die Nichtexaktheit der Invariantenbildung

Schauen wir auf die lange exakte Sequenz aus dem letzten Abschnitt zurück, so können wir der ersten Kohomologiegruppe noch eine interessante Deutungsmöglichkeit zuordnen. Betrachten wir hierfür noch einmal eine kurze exakte Sequenz

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

von G-Modulhomomorphismen. Durch das Bilden der nullten Kohomologiegruppen, die ja nichts anderes als jeweils die Untergruppe der G-invarianten Element sind, erhalten wir (mit den auf natürliche Weise induzierten Gruppenhomomorphismen zusammen) die Sequenz

$$0 \longrightarrow A^G \xrightarrow{i^G} B^G \xrightarrow{\pi^G} C^G \longrightarrow 0\,.$$

Um den Vorgang der Invariantenbildung zu betonen, verwenden wir hier die Bezeichnung A^G statt $\mathrm{H}^0(G, A)$. Unsere neue Sequenz ist bei A^G und B^G exakt, das wissen wir bereits aus der langen exakten Sequenz aus dem letzten Abschnitt. Bei C^G würde Exaktheit nichts anderes als Surjektivität bedeuten. Dies muss jedoch nicht unbedingt der Fall sein, was folgendes Beispiel zeigt:

Beispiel 1.46. Betrachten wir die Galoisgruppe von $\mathbb{C}$ über $\mathbb{R}$, also $G := \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Dann enthält G also alle Automorphismen von $\mathbb{C}$, die $\mathbb{R}$ punktweise festlassen, d. h. $G := \{\mathrm{id}, \tau\}$, wobei τ die Konjugatiosabbildung ist. Die natürliche Operation von G auf $\mathbb{C}^*$ und auf

$\{-1;1\}$ macht die beiden multiplikativen Gruppen zu G-Moduln (zu zeigen ist die Verträglichkeit von Gruppenoperation und Gruppenmultiplikation). Damit ist die Sequenz

$$0 \longrightarrow \{-1;1\} \xhookrightarrow{\text{inkl.}} \mathbb{C}^* \xrightarrow{()^2} \mathbb{C}^* \longrightarrow 0$$

eine kurze exakte Sequenz von G-Modulhomomorphismen (zu zeigen ist natürlich die G-Äquivarianz der Abbildungen). Invariantenbildung liefert die Sequenz

$$0 \longrightarrow \{-1;1\} \xhookrightarrow{\text{inkl.}} \mathbb{R}^* \xrightarrow{(\ )^2} \mathbb{R}^* \longrightarrow 0 \ ,$$

welche aber nicht exakt ist, denn $\mathbb{R}^* \xrightarrow{(\ )^2} \mathbb{R}^*$ ist nicht surjektiv.

Wäre unsere durch Invariantenbildung erhaltene Sequenz stets exakt, so würde man auch sagen, dass der Vorgang der Invariantenbildung *exakt* ist. Die Exaktheit scheitert nun aber an der fehlenden Surjektivität von π^G. Ein natürliches Hindernis für die Surjektivität von π^G liegt nun gerade in *denjenigen* Elementen $c \in C^G$, die kein Urbild haben. Der Verbindungshomomorphismus $\delta : C^G \to \mathrm{H}^1(G, A)$ aus der langen exakten Sequenz in den Kohomologiegruppen hat nun die ganz tolle Eigenschaft, dass er jedem $c \in C^G$ ein Element zuordnet, das genau dann 0 ist, wenn c die Surjektivität von π^G nicht obstruiert (denn $\mathrm{im}(\pi^G) = \ker(\delta)$). Man kann etwas gestelzt davon sprechen, dass $\delta(c)$ die Obstruktion gegen das finden eines Urbilds von c unter π^G darstellt: das Problem hat genau dann eine Lösung, wenn die Obstruktion verschwindet.

Die erste Kohomologiegruppe $\mathrm{H}^1(G, A)$ ist nun der natürliche Aufenthaltsort, in dem sich die den Elementen aus C^G zugeordneten Obstruktionsklassen tummeln. Ist $\mathrm{H}^1(G, A)$ trivial, so ist π^G surjektiv. Man kann daher $\mathrm{H}^1(G; A)$ auch als ein Maß für die Nichtexaktheit des Invariantenbildens bezeichnen. Allerdings kann π^G durchaus auch surjektiv sein, wenn $\mathrm{H}^1(G, A)$ nicht trivial ist. Dies ist genau dann der Fall, wenn $\mathrm{H}^1(G, A)$ nicht-trivial ist und die Abbildung $\mathrm{H}^1(G, A) \to \mathrm{H}^1(G, B)$ injektiv ist.

Vortrag 2

Homologische Algebra I: Projektive und injektive Moduln

Nicolas Poettering
25.10.2005

2.1 Einführung

Definition 2.1. Sei R ein Ring. Ein **linksseitiger Modul M** ist eine abelsche Gruppe (normalerweise additiv geschrieben) mit einer Skalarmultiplikation $R \times M \to M$, so dass für alle $a, b \in R$ und $x, y \in M$ gilt:

(i) $\mathbf{1}x = x$,

(ii) $a(bx) = (ab)x$,

(iii) $(a+b)x = ax + bx$ und $a(x+y) = ax + ay$.

Analog zum linksseitigen Modul lässt sich ein rechtsseitiger Modul definieren. Ich werde nur mit linksseitigen Moduln arbeiten und spreche kurz nur über Moduln.

Beispiel 2.2. (1) In jedem Modul M gilt $0x = 0$ für alle $x \in M$.

(2) Vektorräume sind nichts anderes als Moduln über einem Körper.

(3) Sei R ein Ring. Jedes Ideal ist ein R-Modul, somit auch R selber.

(4) Jede kommutative Gruppe ist kanonisch ein $\mathbb{Z}$-Modul.

(5) Über jedem Ring gibt es einen Modul, den **Nullmodul**, dessen additive Gruppe nur aus der Null besteht.

Definition 2.3. Seien M und M' Moduln über dem Ring R. So ist die Abbildung $f : M \to M'$ ein **Modul-Homomorphismus** (kurz: Homomorphismus), falls f ein Gruppen-Homomorphismus ist und für alle $a \in R$ und $x \in M$ gilt: $f(ax) = af(x)$.

Definition 2.4. Seien M, M' und M'' Moduln über dem Ring R. So wird die Folge von Homomorphismen

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

als **exakte Sequenz** (oder kurze exakte Sequenz) bezeichnet, falls $\operatorname{im} f = \ker g$ gilt.

Definition 2.5. Seien M und M' Moduln über dem Ring R. So wird die Menge aller R-Homomorphismen von M' nach M mit $\mathrm{Hom}_R(M', M)$ bezeichnet.

Es ist $\mathrm{Hom}_R(M', M)$ eine abelsche Gruppe mit der werteweisen Addition von Abbildungen als Verknüpfung. Falls R *kommutativ* ist, wird $\mathrm{Hom}_R(M', M)$ zu einem R-Modul, indem wir für alle $a \in R$ und $f \in \mathrm{Hom}_R(M', M)$ definieren: $(af)(x) = af(x)$.

Jedem Homomorphismus von Moduln $f : M \to M'$ können mit einem weiteren Modul T zwei Homomorphismen zugeordnet werden:

$$\circ f : \mathrm{Hom}_R(T, M) \longrightarrow \mathrm{Hom}_R(T, M'), \quad \alpha \longmapsto f \circ \alpha,$$

$$f\circ : \mathrm{Hom}_R(M', T) \longrightarrow \mathrm{Hom}_R(M, T), \quad \beta \longmapsto \beta \circ f.$$

Dies sind Homomorphismen abelscher Gruppen oder sogar von R-Moduln, sofern R kommutativ ist.

Lemma 2.6. *Eine Sequenz $0 \to M' \to M \to M''$ ist genau dann exakt, wenn die folgende Sequenz für alle Moduln T exakt ist:*

$$0 \longrightarrow \mathrm{Hom}_R(T, M') \longrightarrow \mathrm{Hom}_R(T, M) \longrightarrow \mathrm{Hom}_R(T, M''). \tag{2.1}$$

Es reicht sogar, dass (2.1) nur für $T = R$ exakt ist.

Beweis. Als erstes nehmen wir an: Die Sequenz $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ ist exakt, was insbesondere bedeutet, dass M' isomorph zu einem Untermodul von M ist. Der Einfachheit halber identifizieren wir M' mit dem Bild $\alpha(M') \subseteq M$.

Sei T nun ein beliebiger Modul. Somit ist klar, dass $0 \to \mathrm{Hom}_R(T, M') \to \mathrm{Hom}_R(T, M)$ exakt ist. Ein $f \in \mathrm{Hom}_R(T, M')$ wird auf $\beta \circ \alpha \circ f$ abgebildet, den Nullhomomorphismus in $\mathrm{Hom}_R(T, M'')$, da gilt: $(\beta \circ \alpha)(M') = 0 \subset M''$.

Sei $g \in \mathrm{Hom}_R(T, M)$ im Kern von $\beta\circ$, also $0 = \beta \circ g$, in $\mathrm{Hom}_R(T, M'')$. Das heißt $\mathrm{im}\, g \subset \ker \beta = \mathrm{im}\, \alpha = M'$ und g kann als Homomorphismus $g' : T \to M'$ betrachtet werden. Damit gilt $g = \alpha \circ g'$ und die Sequenz $\mathrm{Hom}_R(T, M') \to \mathrm{Hom}_R(T, M) \to \mathrm{Hom}_R(T, M'')$ ist exakt.

Andersherum nehmen wir an, die Sequenz (2.1) ist für alle $T = R$. Es gilt für alle Moduln M:

$$\mathrm{Hom}_R(R, M) \cong M,$$

da jeder Homomorphismus $f \in \mathrm{Hom}_R(R, M)$ vollständig durch $f(1)$ beschrieben wird und jedes Element aus M als $f(1)$ in Frage kommt: der Homomorphismus $\mathrm{Hom}_R(R, M) \to M$ mit $f \mapsto f(1)$ ist bijektiv mit Inversem $a \mapsto (r \mapsto ra)$.

Wir erhalten das folgende Diagramm mit vertikalen Isomorphimen

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_R(R, M') & \longrightarrow & \mathrm{Hom}_R(R, M) & \longrightarrow & \mathrm{Hom}_R(R, M'') \\
 & & \cong\downarrow & & \cong\downarrow & & \cong\downarrow \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'',
\end{array}$$

welches kommutativ ist: etwa $(\beta \circ f)(1) = \beta(f(1))$. Dies zeigt die Behauptung. □

Lemma 2.7. *Eine Sequenz $M' \to M \to M'' \to 0$ ist genau dann exakt, wenn die folgende Sequenz für alle Moduln T exakt ist:*

$$0 \longrightarrow \mathrm{Hom}_R(M'', T) \longrightarrow \mathrm{Hom}_R(M, T) \longrightarrow \mathrm{Hom}_R(M', T).$$

Auf den Beweis wird hier verzichtet, er sei dem interessierten Leser zur Übung überlassen.

Definition 2.8. Die **direkte Summe** einer Familie $\{M_i\}_{i \in I}$ von Moduln unter dem Ring R ist der R-Modul

$$\bigoplus_{i \in I} M_i = \{(x_i) \mid x_i \in M_i, x_i = 0 \text{ für fast alle } i \in I\}$$

mit der komponentenweise Multiplikation und Addition als Verknüpfungen.

2.2 Gespaltene exakte Sequenzen

Satz 2.9. *Sei $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ eine exakte Sequenz von Moduln. Dann sind die folgenden Bedingungen äquivalent:*

(a) Es existiert ein Homomorphismus φ: $M'' \to M$, so dass $g \circ \varphi = \mathrm{id}_{M''}$.

(b) Es existiert ein Homomorphismus ψ: $M \to M'$, so dass $\psi \circ f = \mathrm{id}_{M'}$.

Falls diese Bedingungen zutreffen, so gilt

$$M = \mathrm{im}\, f \oplus \ker \psi, \quad M = \ker g \oplus \mathrm{im}\, \varphi \quad \textit{und} \quad M \cong M' \oplus M''.$$

Beispiel 2.10. Es folgen zwei Beispiele, die insbesondere zeigen, dass es nicht immer solche Abbildungen φ, ψ geben muss.

(1) Seien M und M' zwei Moduln über dem Ring R, so gibt es für die Sequenz

$$0 \longrightarrow M \longrightarrow M \oplus M' \longrightarrow M' \longrightarrow 0$$

mit der kanonischen Inklusion und Projektion solche Abbildungen nämlich die Projektion und Inklusion in die andere Richtung.

(2) Sei $n \in \mathbb{N}_{\geq 2}$ und $g : \mathbb{Z}/(n^2) \to \mathbb{Z}/(n)$ mit $g(x + (n^2)) = x + (n)$, wobei diese Gruppen als $\mathbb{Z}$-Moduln betrachtet werden sollen. Somit ist g ein surjektiver Homomorphismus und die Sequenz

$$\mathbb{Z}/(n^2) \xrightarrow{g} \mathbb{Z}/(n) \longrightarrow 0$$

ist exakt. Gesucht ist ein Homomorphismus $\varphi : \mathbb{Z}/(n) \to \mathbb{Z}/(n^2)$ für den gilt $g \circ \varphi = \mathrm{id}_{\mathbb{Z}/(n)}$, dass heißt es muss gelten: $\varphi(1 + (n)) = r \cdot n + 1 + (n^2)$ mit geeignetem $r \in \mathbb{Z}$. Daraus folgt:

$$0 + \left(n^2\right) = \varphi(0 + (n)) = \varphi(n \cdot (1 + (n)))$$

$$= n \cdot \varphi(1 + (n)) = n \cdot \left(r \cdot n + 1 + \left(n^2\right)\right) = r \cdot n^2 + n + \left(n^2\right) = n + \left(n^2\right),$$

was ein Widerspruch ist, so dass es keinen solchen Homomorphismus gibt.

Beweis von Satz 2.9. Als erstes werde ich die Äquivalenz der beiden Bedingungen beweisen.

Um aus (a) folgt (b) zu zeigen, betrachtet man den Homomorphismus

$$\alpha := (\mathrm{id}_M - \varphi \circ g) : M \longrightarrow \mathrm{im}\, f.$$

Die Abbildung α nimmt tatsächlich Werte in $\mathrm{im}\, f$ an, da

$$g \circ (\mathrm{id}_M - \varphi \circ g) = g - g \circ \varphi \circ g = g - g = 0.$$

Da f injektiv ist, existiert also eine eindeutige Abbildung $\psi : M \to M'$ mit $f \circ \psi = \alpha$. Es gelten weiter die Äquivalenzen

$$\psi(ax) = a\psi(x) \iff f(\psi(ax)) = f(a\psi(x)) = af(\psi(x)) \iff \alpha(ax) = a\alpha(x),$$

$$\psi(x+y) = \psi(x)+\psi(y) \iff f(\psi(x+y)) = f(\psi(x))+f(\psi(y)) \iff \alpha(x+y) = \alpha(x)+\alpha(y).$$

Daher ist ψ ein Homomorphismus. Für alle $x \in M'$ gilt

$$f(\psi(f(x))) = (f \circ \psi)(f(x)) = (\mathrm{id}_M - \varphi \circ g)(f(x)) = f(x) - \varphi(g(f(x))) = f(x),$$

somit folgt wegen der Injektivität von f die Gleichung $(\psi \circ f)(x) = x$ für alle $x \in M'$. Damit erfüllt ψ die erwünschten Bedingungen.

Für die andere Richtung startet man mit dem Homomorphismus

$$\beta := (\mathrm{id}_M - f \circ \psi) : M \longrightarrow M,$$

welcher auf $\mathrm{im}\, f$ verschwindet. Denn ist $x \in \mathrm{im}\, f$, so gibt es ein $y \in M'$ mit $f(y) = x$, und es gilt:

$$\beta(x) = (\mathrm{id}_M - f \circ \psi)(x) = x - f(\psi(f(y))) = x - f(y) = 0.$$

Somit kann β wegen der Surjektivität von g eindeutig als $\varphi \circ g$ mit einer Abbildung $\varphi : M'' \to M$ geschrieben werden. Bei der Abbildung φ handelt es sich um einen Modulhomomorphismus: sind $x', y' \in M''$ und $r \in R$, so gibt es wegen der Surjektivität von g Elemente $x, y \in M$, so dass $g(x) = x'$ und $g(y) = y'$ gilt. Damit folgt

$$\varphi(r \cdot x') = \varphi(r \cdot g(x)) = \varphi(g(r \cdot x)) = \beta(r \cdot x) = r \cdot \beta(x) = r \cdot \varphi(g(x)) = r \cdot \varphi(x'),$$

$$\varphi(x' + y') = \varphi(g(x) + g(y) = \varphi(g(x + y) = \beta(x + y) = \beta(x) + \beta(y) = \varphi(x') + \varphi(y').$$

Der Homomorphismus φ erfüllt nun die geforderte Bedingung:

$$(g \circ \varphi)(x') = g\left((\varphi \circ g)(x)\right) = g\left((\mathrm{id}_M - f \circ \psi)(x)\right) = g(x) - (g \circ f)(\psi(x)) = g(x) = x'.$$

Um die Gleichung $M = \mathrm{im}\, f \oplus \ker \psi$ zu zeigen, betrachten wir den vorderen Teil der exakten Sequenz:

$$0 \longrightarrow M' \underset{\psi}{\overset{f}{\rightleftarrows}} M$$

Für $x \in M$ gilt: $\beta(x) = x - f\left(\psi(x)\right) \in \ker \psi$, da $\psi(\beta(x)) = \psi(x) - \psi(f(\psi(x))) = 0$. Also $x = f\left(\psi(x)\right) + \beta(x) \in \mathrm{im}\, f + \ker \psi$ und somit $M = \mathrm{im}\, f + \ker \psi$. Nun ist zu zeigen,

dass die Summe direkt ist. Sei $x \in \operatorname{im} f \cap \ker \psi$, so gibt es ein $y \in M'$ mit dem $f(y) = x$. Somit ist $y = \psi(f(y)) = \psi(x) = 0$ und $x = f(0) = 0$. Die Gleichung $M = M = \ker g \oplus \operatorname{im} \varphi$ lässt sich völlig analog beweisen.

Für die dritte Gleichung geben wir zueinander inverse Isomorphismen an:

$$(\psi, g) : M \longrightarrow M' \oplus M'', \quad x \longmapsto (\psi(x), g(x)),$$

$$(f + \varphi) : M' \oplus M'' \longrightarrow M, \quad (x', x'') \longmapsto f(x') + \varphi(x'').$$

In der Tat gelten mit der naheliegenden Matrixschreibweise für die Komponenten der Abbildungen die Gleichungen

$$(f + \varphi) \circ (\psi, g) = f \circ \psi + \varphi \circ g = \mathrm{id}_M,$$

$$(\psi, g) \circ (f + \varphi) = \begin{pmatrix} \psi \circ f & g \circ f \\ \psi \circ \varphi & g \circ \varphi \end{pmatrix} = \begin{pmatrix} \mathrm{id}_{M'} & 0 \\ 0 & \mathrm{id}_{M''} \end{pmatrix} = \mathrm{id}_{M' \oplus M''}.$$

In der Tat gilt $\psi \circ \varphi = 0$, da

$$\psi(\varphi(g(y))) = \psi(y - (f \circ \psi)(y)) = \psi(y) - \psi(y) = 0.$$

□

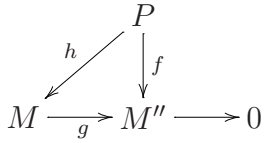
Definition 2.11. Ist die in Satz 2.9 beschriebene Bedingung erfüllt, so bezeichnet man die Sequenz als **gespaltene exakte Sequenz**. Ein Morphismus φ wie in Satz 2.9 heißt **Schnitt**, ein Morphismus ψ eine **Retraktion** der Extension.

2.3 Freie und projektive Moduln

Definition 2.12. Unter einem **freien Modul** versteht man einen Modul, zu dem eine Basis existiert. Eine **Basis** ist ein linear unabhängiges Erzeugendensystem. Wir betonen, dass auch der Nullmodul frei ist, denn er hat das freie lehre Erzeugendensystem.

Satz–Definition 2.13. *Sei R ein Ring und P ein Modul. P ist ein* **projektiver Modul**, *falls er eine der nachfolgenden äquivalenten Bedingungen erfüllt:*

(a) Zu jedem Homomorphismus $f : P \to M''$ und jedem surjektiven Homomorphismus $g : M \to M''$ gibt es einen Homomorphismus $h : P \to M$, so dass das folgende Diagramm kommutiert:



(b) Jede exakte Sequenz $0 \to M' \to M \to P \to 0$ ist gespalten.

(c) Es existiert ein Modul M, so dass $P \oplus M$ frei ist: P ist direkter Summand eines freien Moduls.

(d) Die Zuordnung $M \mapsto \mathrm{Hom}_R(P, M)$ *ist exakt: für jede exakte Sequenz*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

folgt die Exaktheit der Sequenz der Gruppen der Homomorphismen von P *in die entsprechenden Moduln:*

$$0 \to \mathrm{Hom}_R(P, M') \longrightarrow \mathrm{Hom}_R(P, M) \longrightarrow \mathrm{Hom}_R(P, M'') \longrightarrow 0.$$

Beispiel 2.14. (1) Jeder freie Modul ist wegen Bedingung (c) ein projektiver Modul.

(2) Für jedes $n \in \mathbb{N}_{\geq 2}$ ist der $\mathbb{Z}$-Modul $\mathbb{Z}/(n)$ kein projektiver Modul, da die dazugehörige in den Beipielen 2.10 beschriebene exakte Sequenz nicht gespalten ist und somit Bedingung (b) widerspricht.

(3) Sei $R = \mathbb{Z}/(6)$, $P = \{0, 3\} \subset R$ und $M = \{0, 2, 4\} \subset R$, so sind P und M R-Module, wobei P keine Basis hat, da in R gilt: $2 \cdot 3 = 0$. Aber $B = \{(3, 2)\}$ ist eine Basis von, dem Modul $P \oplus M$, da B diesen Modul erzeugt und $r \cdot (3, 2) \neq 0$ für alle $r \in R\backslash\{0\}$ gilt. Somit ist P nach Bedingung (c) ein projektiver Modul der überdies nicht frei ist.

Beweis des Satzes 2.13. Wir zeigen die Äquivalenzen durch einen Ringschluss der Bedingungen (a) bis (c) und dann die Äquvalenz zur (d) extra.

Angenommen, die Bedingung (a) gilt und es sei

$$0 \longrightarrow M' \longrightarrow M \xrightarrow{g} P \longrightarrow 0$$

eine Extension. Für $f = \mathrm{id}_P$ und die Surjektion g finden wir nach (a) einen Homomorphismus h, der ein Schnitt der Extension ist und diese damit spaltet, somit gilt (b).

Angenommen, die Bedingung (b) gilt: Zu jedem Modul, somit auch zu P, gibt es einen freien Modul, zum Beispiel $F = \bigoplus_{x \in P} R$, und eine Surjektion

$$F \xrightarrow{g} P \longrightarrow 0.$$

Im Fall $F = \bigoplus_{x \in P} R$ bilden wir das $x$ten Basiselement auf $x \in P$ ab, so dass die Abbildung tautologisch surjektiv ist. Wegen (b) ist die zugehörige Extension

$$0 \longrightarrow \ker g \longrightarrow F \longrightarrow P \longrightarrow 0$$

gespalten und nach Satz 2.9 gilt $F \cong P \oplus \ker g$. Somit folgt (c).

Nehmen wir nun an, dass Bedingung (c) gilt. Sei F ein freier Modul, so dass $F = P \oplus M'$ gilt und $\{w_i\}_{i \in I}$ die zugehörige Basis von F. Betrachte folgendes Diagramm:

$$\begin{array}{ccccc} P \oplus M' & \underset{\varphi}{\overset{\pi}{\rightleftarrows}} & P & \longrightarrow & 0 \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow[g]{} & M'' & \longrightarrow & 0. \end{array}$$

Wobei in der oberen Zeile mit π die Projektion und φ die Inklusion gemeint ist, für diese gilt somit: $\pi \circ \varphi = \mathrm{id}_P$. Da g surjektiv ist, gibt es zu jedem $x'' \in M''$ ein $\overline{x''} \in M$, so dass $g\left(\overline{x''}\right) = x''$. Wir definieren

$$\psi : F = P \oplus M' \longrightarrow M, \quad w_i \longmapsto \overline{f(\pi(w_i))} \quad \forall\, i \in I.$$

Dieses beschreibt einen Homomorphismus, da man bei freien Moduln einen Homomorphismus eindeutig dadurch beschreibt, indem man den Basiselementen Bilder zuordnet.

Es gilt $g \circ \psi = f \circ \pi$, da für alle $i \in I$

$$g(\psi(w_i)) = g\left(\overline{f(\pi(w_i))}\right) = f(\pi(w_i)).$$

Nun betrachte man den Homomorphismus $h : P \to M$, mit $h := \psi \circ \varphi$. Da

$$g \circ h = g \circ (\psi \circ \varphi) = (f \circ \pi) \circ \varphi = f,$$

erfüllt der Homomorphismus h die gewünschten Bedingungen, und bringt das Diagramm zum Kommutieren.

Nun wird gezeigt, dass die Bedingung (a) äquivalent zur Bedingung (d) ist. Nach Lemma 2.6 ist bei (d) nur fraglich, ob $\mathrm{Hom}_R(P, -)$ surjektive Morphismen in Surjektionen überführt. Dies ist aber nichts anderes als die Bedingung (a). □

Satz 2.15. *Jeder Untermodul M eines freien Moduls F über einem Hauptidealring R ist ein freier Modul. Hat F eine Basis der Länge $n < \infty$, so hat M eine Basis der Länge $m \leq n$.*

Beweis. Hier sollen zwei Fälle unterschieden werden. Zuerst gehe man davon aus, dass F eine endliche Basis hat. Sei $\{x_i\}_{i=1,\ldots,n}$ eine Basis von F und M_r der Schnitt des Moduls M mit dem von den Elementen $x_1, x_2, \ldots, x_r$ erzeugten Modul F_r. So ist $M_1 = M \cap (x_1)$ ein Untermodul von $(x_1) \cong R$, der sich mit einem geeigneten $a_1 \in R$ als $(a_1 x_1) \cong a_1 R$ darstellen lässt, da R ein Hauptidealring ist. Somit ist M_1 der Nullmodul oder frei und hat Rang 1.

Wir nehmen per Induktion an, dass M_r ein freier Modul des Rangs $\leq r$ ist. Sei I die Menge aller $a \in R$, so dass es ein $x \in M$ und $b_i \in R$ gibt, mit denen folgendes gilt:

$$x = b_1 x_1 + \ldots + b_r x_r + a x_{r+1}.$$

Diese x liegen alle in M_{r+1} und I ist ein Ideal, nämlich das Annullatorideal des Bildes des Elements x_{r+1} im Quotienten $F_{r+1}/(F_r + M_{r+1})$.

Somit gibt es ein $a_{r+1} \in I$, welches I erzeugt. Falls $a_{r+1} = 0$ gilt, sind wir fertig, da dann $M_r = M_{r+1}$. Also ist nun $a_{r+1} \neq 0$. Sei $w \in M_{r+1}$ nun so gewählt, dass der Koeffizient vor x_{r+1} genau a_{r+1} ist. Sei nun $x \in M_{r+1}$ beliebig, so gibt es eine Darstellung wie oben und der Koeffizient vor x_{r+1} ist durch a_{r+1} teilbar, das heißt es existiert ein $c \in R$, so dass $x - cw$ in M_r liegt. Also gilt:

$$M_{r+1} = M_r + wR.$$

Diese Summe ist direkt, da für w der Koeffizient a_{r+1} vor x_{r+1} ungleich Null ist und somit $M_r \cap wR = \{0\}$ gilt (gerechnet im freien F).

Nun habe F eine unendliche Basis $\{x_i\}_{i\in I}$, so muss nur noch gezeigt werden, dass M auch eine Basis besitzt. Man kann sogar zeigen, dass sich diese Basis im nicht trivialen Fall mit einer Teilmenge von I indizieren lässt.

Für alle $J \subset I$ sei F_J der freie Untermodul von F der von allen $x_i,\ i \in J$ erzeugt wird und M_J der Schnitt von F_J und M. Weiter sei nun $\mathcal{N}$ die Menge aller Paare (M_J, α), bei denen $J \subset I$ und das Bild der Abbildung $\alpha : J' \to F_J$ eine Basis von M_J ist, wobei J' eine geeignete Teilmenge von J ist. Der Einfachheit halber schreibe man α_i statt $\alpha(i)$ für alle $i \in J'$.

Die Menge $\mathcal{N}$ ist wie folgt induktiv geordnet. Seien $(M_J, \alpha), (M_K, \beta) \in \mathcal{N}$, so gilt $(M_J, \alpha) \leq (M_K, \beta)$, falls $J \subset K$, $J' \subset K'$ und $\beta\,|_{J'} = \alpha$, das heißt die durch β beschriebene Basis ist eine Erweiterung der durch α beschriebenen Basis.

Nun ist zu zeigen, dass jede Kette von geordneten Elementen aus $\mathcal{N}$, etwa $(M_{J_1}, \alpha_1) \leq (M_{J_2}, \alpha_2) \leq \ldots$, eine obere Schranke in $\mathcal{N}$ besitzt. Sei $J := \bigcup_{i\in\mathbb{N}} J_i$ und $J' := \bigcup_{i\in\mathbb{N}} J_i'$. M_J ist ein freier Modul für den ein Homomorphismus α existiert, so dass $\alpha|_{J_i'} = \alpha_i$ gilt. Das dies ein Modul und ein wohldefinierter Homomorphismus ist, wird klar, wenn man für jedes $x \in M_J$ im M_{J_i} mit einem genügend großen $i \in \mathbb{N}$ rechnet. Die Menge $\alpha(J')$ ist eine Basis, da sie M_J erzeugt und für jede endliche Menge von Elementen gilt, dass diese in einem System $\alpha(J_i')$ mit großem i liegt und somit linear unabhängig ist. Damit ist $(M_J, \alpha) \in \mathcal{N}$ eine obere Schranke unserer Kette.

Nach dem ersten Teil ist $\mathcal{N}$ nicht leer. somit liefert uns das Lemma von Zorn die Existenz maximaler Elemente in $\mathcal{N}$, etwa (M_J, α).

Falls nun $M_J = M$ gilt, haben wir gewonnen. Angenommen $M_J \neq M$, dann existiert ein $j \in I\backslash J$ mit $M_{J\cup\{j\}}$ echt größer als M_J. Andernfalls ist $(M_{J\cup\{j\}}, \alpha) \in \mathcal{N}$ ein größeres Paar im Widerspruch zur Maximalität von (M_J, α).

Somit gibt es ein Element in $M_{J\cup\{j\}}$, welches sich wie folgt darstellen lässt: $cx_j + y$ mit $c \in R\backslash\{0\}$ und $y \in F_J$. Die Menge aller dieser $c \in R$, so dass es ein $y \in F_J$ gibt und $cx_j + y \in M$, ist ein Ideal, welches von einem $a \in R\backslash\{0\}$ erzeugt wird. Setze $\alpha_j := ax_j + y$ mit einem geeigneten Element $y \in F_J$, so dass $\alpha_j \in M$. Zu zeigen bleibt nun, dass $\{\alpha_i\}_{i\in J\cup\{j\}}$ eine Basis von $M_{J\cup\{j\}}$ ist, da dann $(M_{J\cup\{j\}}, \tilde{\alpha}) \in \mathcal{N}$, wobei $\tilde{\alpha}$ die Erweiterung um $j \mapsto \alpha_j$ von α ist, ein größeres Paar als (M_J, α) ist. Dies folgt mit der selben Überlegung wie zum Schluß des Induktionsschritts im Fall endlichen Rangs. □

2.4 Injektive Moduln

Analog zu projektiven Moduln definiert man durch umdrehen der Pfeile injektive Moduln.

Satz–Definition 2.16. *Ein* **injektiver Modul** *ist ein Modul Q, der die folgenden äquivalenten Bedingungen erfüllt:*

(a) Jeder Homomorphismus $f : M' \to Q$ auf einem Untermodul M' eines Moduls M lässt sich auf M fortsetzen, d. h. es existiert ein Homomorphismus $h : M \to Q$, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \hookrightarrow & M \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle h} & \\ & & Q & & \end{array}$$

(b) Die Zuordnung $M \longmapsto \mathrm{Hom}_R(M, Q)$ *ist exakt.*

(c) Jede exakte Sequenz $0 \longrightarrow Q \longrightarrow M \longrightarrow M'' \longrightarrow 0$ *ist gespalten.*

Beweis. Man starte mit der exakten Sequenz $0 \to M' \to M \to M'' \to 0$. Wegen Lemma 2.7 ist für die Exaktheit der Zuordnung aus Bedingung (b) nur die Surjektivität der $\mathrm{Hom}_r(-, Q)$-Sequenz zu betrachten, was genau Bedingung (a) entspricht. Somit sind Bedingung (a) und (b) zueinander äquivalent.

Nehmen wir nun an, dass Bedingung (a). Mit dem folgenden Diagramm, dem Fall $f = \mathrm{id}_Q$ der Bedingung (a),

$$\begin{array}{ccccc} 0 & \longrightarrow & Q & \longrightarrow & M \\ & & \Big\downarrow{\scriptstyle \mathrm{id}} & \swarrow{\scriptstyle h} & \\ & & Q & & \end{array}$$

konstruiert man eine Retraktion für jede Extension wie in (c). Gemäß Satz 2.9 spaltet jede solche Extension, und dies beweist (c).

Als letztes nehmen wir an, dass die Bedingung (c) erfüllt ist und zeigen die Bedingung (a). Wir setzten

$$N = (Q \oplus M)/\{(f(x), -\varphi(x)); x \in M'\},$$

und betrachten die Homomorphismen $\alpha : Q \to N$ mit $q \mapsto (q, 0)$ und $\beta : M \to N$ mit $m \mapsto (0, m)$ in folgendem kommutativen Diagramm:

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \overset{\varphi}{\hookrightarrow} & M \\ & & \Big\downarrow{\scriptstyle f} & & \Big\downarrow{\scriptstyle \beta} \\ & & Q & \xrightarrow{\alpha} & N, \end{array}$$

das kommutativ ist wegen:

$$\alpha(f(x)) = (f(x), 0) = (0, \varphi(x)) = \beta(\varphi(x)).$$

Sei $x \in \ker \alpha$, so gilt $0 = \alpha(x) = (x, 0)$ in N, das heißt es gibt ein $y \in M'$, so dass $(x, 0) = (f(y), -\varphi(y))$ in $Q \oplus M$. Da φ injektiv ist, folgt $y = 0$ und $x = f(y) = 0$. Also ist auch α injektiv.

Wegen Bedingung (c) ist die Sequenz

$$0 \longrightarrow Q \xrightarrow{\alpha} N \longrightarrow \mathrm{coker}\, \alpha \longrightarrow 0$$

gespalten, und esexistiert ein Homomorphismus $\psi : N \to Q$ mit $\psi \circ \alpha = \mathrm{id}_Q$. Der Homomorphismus $h := \psi \circ \beta : M \to Q$ setzt f auf M fort:

$$h|_{M'} = h \circ \varphi = (\psi \circ \beta) \circ \varphi = \psi \circ (\alpha \circ f) = f,$$

und Bedingung (a) gilt. □

Ab jetzt konzentrieren wir uns auf den Fall von Moduln über Hauptidealringen R. Dies schließt den Fall abelscher Gruppen als Moduln über dem Hauptidealring $\mathbb{Z}$ ein.

Definition 2.17. Sei R ein Hauptidealring. Ein Modul M heißt **divisibel**, falls für alle $r \neq 0$ aus R der Homomorphismus „Multiplikation mit r“ $\lambda_r : M \to M, x \mapsto rx$ surjektiv ist.

Beispiel 2.18. Die Moduln $\mathbb{Q}$ und $\mathbb{Q}/\mathbb{Z}$ sind divisibele $\mathbb{Z}$-Moduln.

Satz 2.19. *Über einem Hauptidealring R sind die injektiven Moduln genau die divisiblen Moduln.*

Beweis. Wir zeigen zunächst, dass injektive Moduln divisibel sind. Dazu bemerken wir, dass die Mulitplikation λ_r mit einem von 0 verschiedenen Element $r \in R$ injektiv ist. Daher setzt sich die Identität des injektiven Moduls I entlang der Injektion $\lambda_r : I \hookrightarrow I$ zu einem Homomorphismus μ_r fort, so dass $\mu_r \circ \lambda_r = \mathrm{id}_I$ und damit

$$x = \mu_r(\lambda_r(x)) = \mu_r(rx) = r\mu_r(x) = \lambda_r(\mu_r(x)$$

gilt. Demnach ist λ_r surjektiv und I ist divisibler R-Modul.

Sei T ein divisibler R-Modul, M' ein Untermodul des Moduls M und $f : M' \to T$ ein Homomorphismus. Wir müssen zeigen, dass sich f zu $\tilde{f} : M \to T$ fortsetzen lässt. Sei $x \in M \backslash M'$. Als erstes bilden wir eine Fortsetzung auf $(M', x) \subset M$, den von allen Elementen von M' und x erzeugten Modul. Wenn x frei über M' ist, was heißt, dass die Gleichung $m = a \cdot x$ für alle $m \in M'$ und $a \in R$ nur mit $a = 0$ lösbar ist, so ist $M' \oplus R \cong (M', x)$ vermöge $(m, a) \mapsto m + ax$ Die Fortsetzung läßt sich also durch die Wahl eines beliebigen Elements $t \in T$ durch $\tilde{f}|_{M'} = f$ und $\tilde{f}(x) = t$ wohl definieren.

Ist x nicht frei über M', so ist $\mathfrak{a} = \{a \in R \mid \ ax \in M'\} \subset R$ ein echtes Ideal. Da R ein Hauptidealring ist, gibt es ein Element $0 \neq d \in R$ mit $\mathfrak{a} = (d)$. Da T divisibel ist, finden wir ein $u \in T$ mit $du = f(dx)$, wobei wir verwenden, dass f auf $dx \in M'$ definiert ist. Nun setze wir

$$\tilde{f} : (M', x) \longrightarrow T, \quad m + ax \longmapsto f(m) + au \quad \forall\, m \in M',\ a \in R.$$

Diese Vorschrift ist wohldefiniert: aus $m_1 + a_1 x = m_2 + a_2 x$ mit $m_i \in M'$ und $a_i \in R$ folgt $m_1 - m_2 = (a_2 - a_1)x$, also gibt es ein $b \in R$ mit $bd = a_1 - a_2$ und somit

$$\big(f(m_1)+a_1u\big)-\big(f(m_2)+a_2u\big) = f(m_1-m_2)+(a_1-a_2)u = f(bdx)-bdu = b(f(dx)-du) = 0$$

nach Definition von u. Des weiteren ist $\tilde{f}$ ein Homomorphismus:

$$\tilde{f}(r(m + ax)) = \tilde{f}(rm + rax) = f(rm) + rau = r(f(m) + ax) = r\tilde{f}(m + ax),$$

$$\tilde{f}((m+ax)+(n+bx)) = \tilde{f}((m+n)+(a+b)x) = f(m+n)+(a+b)u = f(m+ax)+f(n+bx).$$

Wir betrachten nun die Menge $\mathscr{N}$ aller Paare (N, g), so dass $M' \subset N \subset M$ ein Modul und g eine Fortsetzung von $g|_{M'} = f$ ist. Wir definieren die folgende partielle Ordnung auf $\mathscr{N}$: man sagt $(N, g) \leq (N', g')$, falls $N \subset N'$ und $g'|_N = g$. Diese Menge ist nicht leer, da $(M', f) \in \mathscr{N}$, und jede Kette $(N_1, g_1) \leq (N_2, g_2) \leq \ldots$ hat eine obere Schranke nämlich: $\big(\bigcup_{i\in\mathbb{N}} N_i, g\big)$, wobei für alle $x \in \bigcup_{i\in\mathbb{N}} N_i$ gilt: $g(x) := g_i(x)$ mit einem genügend großen $i \in \mathbb{N}$, so dass $x \in N_i$.

Nach dem Lemma von Zorn gibt es maximale Elemente in $\mathscr{N}$. Sei das Paar (N, g) maximal. Angenommen $N \neq M$, so gibt es ein $x \in M \backslash N$ und der erste Teil des Beweises angewandt auf N und x zeigt, dass (N, g) nicht maximal gewesen sein kann. Somit ist $N = M$ und g setzt f auf M fort. □

Vortrag 3

Homologische Algebra II: Auflösungen

Tobias Leßmeister
8.11.2005

3.1 Komplexe und Homologie

Definition 3.1. Ein **(offener) Komplex** von Moduln über einem Ring R ist gegeben durch ein Diagramm von R-Moduln E^i, $i \in \mathbb{Z}$ der folgenden Form:

$$\dots \xrightarrow{d^{i-2}} E^{i-1} \xrightarrow{d^{i-1}} E^i \xrightarrow{d^i} E^{i+1} \xrightarrow{d^{i+1}} \dots,$$

wobei die folgenden Gleichungen erfüllt sind:

$$d^i \circ d^{i-1} = 0. \tag{3.1}$$

Im Folgenden wird ein solcher Komplex mit $(E^\bullet, d)$ bzw. $E^\bullet$ bezeichnet.

Bemerkung 3.2. Die Bedingung (3.1) kann „auf zwei Arten“ erfüllt werden:

(1) Ist $\ker d^i = \operatorname{im} d^{i-1}$, dann heißt der Komplex *exakt* bei i.

(2) Ist allerdings nur $\ker d^i \subset \operatorname{im} d^{i-1}$, so möchte man die Abweichung von der Exaktheit messen. Dies führt zur folgenden

Definition 3.3. (1) Die ***i*-te Homologie-Gruppe** eines Komplexes $(E^\bullet, d)$ ist gegeben durch

$$\mathrm{H}^i(E^\bullet) = \frac{\ker d^i}{\operatorname{im} d^{i-1}} = \frac{\mathrm{Z}^i(E^\bullet)}{\mathrm{B}^i(E^\bullet)}$$

wobei $\mathrm{Z}^i = \mathrm{Z}^i(E^\bullet) = \ker d^i$ der Modul der ***i*-Zykel** und $\mathrm{B}^i = \mathrm{B}^i(E^\bullet) = \operatorname{im} d^{i-1}$ für den Modul der ***i*-Ränder** (engl. boundary) steht.

(2) Die **Homologie** eines Komplexes $E^\bullet$ ist gegeben durch den $\mathbb{Z}$- graduierten Modul

$$\mathrm{H}(E^\bullet) = \bigoplus_{i \in \mathbb{Z}} \mathrm{H}^i(E^\bullet),$$

bzw. die Familie der Homologiemoduln $\mathrm{H}^i(E^\bullet)$, $i \in \mathbb{Z}$.

Definition 3.4. Ein **Morphismus von Komplexen** $f : (E^\bullet, d) \to (E'^\bullet, d')$ vom **Grad** $n \in \mathbb{Z}$. ist gegeben durch eine Sequenz von Modulhomomorphismen $f_i : E^i \to E'^{(i+n)}$, $i \in \mathbb{Z}$ so dass das Diagramm

$$\begin{array}{ccc} E^{(i-1)} & \xrightarrow{d} & E^i \\ \downarrow{\scriptstyle f_{i-1}} & & \downarrow{\scriptstyle f_i} \\ E'^{(i+n-1)} & \xrightarrow{d'} & E'^{(i+n)} \end{array}$$

für alle $i \in \mathbb{Z}$ kommutiert.

Bemerkung 3.5. Während des gesamten Vortrages werden nur Morphismen von Komplexen vom Grad $n = 0$ betrachtet.

Lemma–Definition 3.6. *Ein Morphismus f von Komplexen induziert einen kanonischen Homomorphismus auf jeder Homologiegruppe:*

$$\mathrm{H}^i(f) : \mathrm{H}^i(E^\bullet) \longrightarrow \mathrm{H}^i(E'^\bullet), \quad \mathrm{H}^i(f)\left(a + \mathrm{B}^i(E^\bullet)\right) := f^i(a) + \mathrm{B}^i(E'^\bullet).$$

Wir fassen die Abbildungen $\mathrm{H}^i(f)$ *zur Abbildung*

$$\mathrm{H}(f) := \bigoplus_{i\in\mathbb{Z}} \mathrm{H}^i(f) : \mathrm{H}(E^\bullet) \longrightarrow \mathrm{H}(E'^\bullet),$$

der **von f auf der Homologie induzierten Abbildung**, *zusammen.*

Beweis. Es muss gezeigt werden, dass unter der Abbildung f die Zykel bzw. Ränder von $E^\bullet$ auf die Zykel bzw. Ränder von $E'^\bullet$ abgebildet werden. Nach Definition eines Morphismus von Komplexen gilt

$$d'^i f^i\left(\mathrm{Z}^i\right) = f^{i+1} d^i\left(\mathrm{Z}^i\right) = 0$$

Es folgt $f^i\left(Z^i\right) \subseteq Z^i$. Die Rechnung für Ränder geht analog:

$$f^i\left(\mathrm{B}^i\right) = f^i d^{i-1}\left(E^{i-1}\right) = d'^{i-1} f^{i-1}\left(E^{i-1}\right) \subset d'^{i-1}\left(E'^{i-1}\right) = \mathrm{B}^i\left(E'^\bullet\right).$$

□

Lemma 3.7. *Seien $f : E^\bullet \to E'^\bullet$ und $g : E'^\bullet \to E'^\bullet$ Morphismen von Komplexen. Dann ist*

$$\mathrm{H}(g) \circ \mathrm{H}(f) = \mathrm{H}(g \circ f)$$

und $\mathrm{H}(\mathrm{id}) = \mathrm{id}$. *Es ist also* H *ist also ein Funktor von der Kategorie der Komplexe in die Kategorie der graduierten Moduln.*

Beweis. Dies ist aus der Definition der Abbildungen auf der Homologie aus Lemma 3.6 unmittelbar klar. □

3.2 Auflösungen

Definition 3.8. (1) Eine **Auflösung (nach links bzw. nach rechts)** des R-Moduls M ist gegeben durch eine exakte Sequenz von Moduln

$$\cdots \longrightarrow E^i \longrightarrow E^{i-1} \longrightarrow \cdots \longrightarrow E^0 \longrightarrow M \longrightarrow 0$$

bzw.

$$0 \longrightarrow M \longrightarrow E^0 \longrightarrow \cdots \longrightarrow E^{i-1} \longrightarrow E^i \longrightarrow \cdots$$

Eine Auflösung von M ist also eine exakte Sequenz, deren letzter Term auf der rechten bzw. linken Seite vor der Null M ist.

(2) Eine Auflösung nach links heißt **freie (bzw. projektive) Auflösung**, wenn die E^i frei (bzw. projektiv) sind für alle $i \leq 0$.

(3) Eine Auflösung nach rechts heißt **injektive Auflösung**, wenn die E^i injektiv sind für alle $i \geq 0$.

(4) Eine Auflösung heißt **endlich**, falls $E^i = 0$ für alle i bis auf endlich viele Ausnahmen.

Satz 3.9. *Für jeden Modul M gibt es eine injektive Auflösung*

$$0 \longrightarrow M \longrightarrow I^0 \longrightarrow I^1 \longrightarrow I^2 \longrightarrow \cdots.$$

Für den Beweis benötigen wir folgenden

Satz 3.10. *Es gibt genügend viele injektive Moduln. Das heißt, für jeden R-Modul M gibt es einen injektiven Modul I und einen injektiven Modulhomomorphismus $M \to I$.*

Beweis von Satz 3.9. Nach Satz 3.10 existiert ein I^0, so dass $0 \to M \xrightarrow{d^{-1}} I^0$ exakt ist. Sei die Auflösung bis zur Stelle $n \geq 0$ bereits konstruiert. Wir wählen nach Satz 3.10 einen injektiven Modul I^{n+1} mit einer injektiven Abbildung

$$\iota : \operatorname{coker}\left(d^{n-1} : I^{n-1} \longrightarrow I^n\right) \hookrightarrow I^{n+1}.$$

Mit

$$d^n = \iota \circ \left(I^n \twoheadrightarrow \operatorname{coker}\left(d^{n-1} : I^{n-1} \longrightarrow I^n\right)\right) : I^n \longrightarrow I^{n+1}$$

ist $I^{n-1} \xrightarrow{d^{n-1}} I^n \xrightarrow{d^{n+1}} I^{n+1}$ exakt, wobei wir vereinbaren, dass in Mißbrauch der Notation $I^{-1} = M$ sein soll. Auf diese Art wird induktiv eine injektive Auflösung von M konstruiert. □

Für den Beweis von Satz 3.10 benutzen wir folgendes

Lemma 3.11. *Sei I ein injektiver $\mathbb{Z}$-Modul, also eine injektive abelsche Gruppe. Dann ist $\operatorname{Hom}_{\mathbb{Z}}(R, I)$ mit der Multiplikation*

$$r \cdot \varphi : \; x \longmapsto \varphi(xr) \;\; \textit{mit } x, r \in R; \varphi \in \operatorname{Hom}_{\mathbb{Z}}(R, I)$$

ein injektiver R-Modul.

Beweis. Der Beweis erfolgt in zwei Schritten. Zuerst zeigen wir, dass $\mathrm{Hom}_{\mathbb{Z}}(R, I)$ mit der oben definierten Multiplikation ein R-Modul ist. Sei $\varphi, \varphi' \in \mathrm{Hom}_{\mathbb{Z}}(R, I)$ und seien $s, r, x \in R$. Es gilt

$$\mathbf{1} \cdot \varphi(x) = \varphi(x\mathbf{1}) = \varphi(x),$$
$$(r \cdot (\varphi + \varphi'))(x) = (\varphi + \varphi')(xr) = \varphi(xr) + \varphi'(xr) = (r \cdot \varphi)(x) + (r \cdot \varphi')(x),$$

und

$$r(s\varphi)(x) = (s \cdot \varphi)(xr) = \varphi((xs)r) = \varphi(x(rs)) = ((rs) \cdot \varphi)(x).$$

Als nächstes zeigen wir, dass $\mathrm{Hom}_{\mathbb{Z}}(R, I)$ ein injektiver R-Modul ist. Hierzu benutzen wir folgendes

Lemma 3.12. *Sei M ein R-Modul und I eine abelsche Gruppe. Dann gibt es einen natürlichen Isomorphismus von abelschen Gruppen*

$$\mathrm{Hom}_{\mathbb{Z}}(M, I) \cong \mathrm{Hom}_R\left(M, \mathrm{Hom}_{\mathbb{Z}}(R, I)\right)$$

Beweis. Wir definieren

$$F : \mathrm{Hom}_{\mathbb{Z}}(M, I) \longrightarrow \mathrm{Hom}_R\left(M, \mathrm{Hom}_{\mathbb{Z}}(R, I)\right),\ (\psi : M \longrightarrow I) \longmapsto f_\psi : M \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, I)$$

für $m \in M$ und $x \in R$ durch $f_\psi(m) = (x \mapsto \psi(xm))$. Das muss man überprüfen:

Es ist offenbar f_ψ linear, also ein $\mathbb{Z}$-Modulhomomorphismus $\in \mathrm{Hom}_{\mathbb{Z}}(R, I)$. Des weiteren ist f_ψ ein R-Modulhomomorphismus, denn es gilt

$$f_\psi(rm) = (x \longmapsto \psi(xrm)) = r \cdot f_\psi(m).$$

Daher ist F eine wohldefinierte Abbildung, die Homomorphieeigenschaften von F sind klar. Das Inverse zu F ist die Abbildung

$$\Psi : \mathrm{Hom}_R\left(M, \mathrm{Hom}_{\mathbb{Z}}(R, I)\right) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(M, I), \quad f \longmapsto \psi_f := \big(m \longmapsto f(m)(1)\big).$$

Es gilt

$$\psi_f(m_1 + m_2) = f(m_1 + m_2)(1) = (f(m_1) + f(m_2))(1)$$
$$= f(m_1)(1) + f(m_2)(1) = \psi_f(m_1) + \psi_f(m_2),$$

daher ist Ψ wohldefiniert. Es ist Ψ ein Gruppenhomomorphismus, da

$$\psi_{f+g} = (m \longmapsto (f + g)(m)(1)) = (m \longmapsto \big(f(m) + g(m)\big)(1))$$
$$= (m \longmapsto f(m)(1) + g(m)(1)) = \psi_f + \psi_g.$$

Die Abbildungen F und Ψ sind zueinander invers:

$$F(\Psi(f)) = F(\psi_f) = \big(m \longmapsto (x \longmapsto \psi_f(xm))\big) = \big(m, x \longmapsto f(xm)(1)\big)$$
$$= (m, x \longmapsto (x \cdot f(m))(1)) = (m, x \longmapsto f(m)(x)) = f,$$

und

$$\Psi(F(\psi)) = \Psi(f_\psi) = (m \longmapsto f_\psi(m)(1)) = (m \longmapsto \psi(m)) = \psi.$$

□

Wir kommen zurück zum Beweis von Lemma 3.11. Sei M ein R-Modul und M' ein Untermodul von M. Wir müssen zeigen, dass die Abbildung

$$\mathrm{Hom}_R\left(M, \mathrm{Hom}_{\mathbb{Z}}(R, I)\right) \longrightarrow \mathrm{Hom}_R\left(M', \mathrm{Hom}_{\mathbb{Z}}(R, I)\right)$$

surjektiv ist. Wir wissen allerdings, dass

$$\mathrm{Hom}_{\mathbb{Z}}(M, I) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(M', I)$$

surjektiv ist, da hier M und M' als abelsche Gruppen aufgefasst werden und I eine injektive abelsche Gruppe ist. Durch den natürlichen Isomorphismus aus Lemma 3.12 erhalten wir folgendes kommutative Diagramm, welches den Beweis vollendet.

$$\begin{array}{ccc} \mathrm{Hom}_R\left(M, \mathrm{Hom}_{\mathbb{Z}}(R, I)\right) & \longrightarrow & \mathrm{Hom}_R\left(M', \mathrm{Hom}_{\mathbb{Z}}(R, I)\right) \\ \cong\uparrow & & \cong\uparrow \\ \mathrm{Hom}_{\mathbb{Z}}(M, I) & \twoheadrightarrow & \mathrm{Hom}_{\mathbb{Z}}(M', I) \end{array}$$

□

Beweis von Satz 3.10. Der Beweis erfolgt in zwei Schritten. Sei zunächst $R = \mathbb{Z}$. Wir wählen eine surjektive Abbildung $\pi : \bigoplus_{\lambda\in\Lambda} \mathbb{Z} \twoheadrightarrow M$ und setzen $K = \ker(\pi)$. Wir haben dann das folgende folgendes Diagramm

$$\begin{array}{ccccccc} K & \longrightarrow & \bigoplus_{\lambda\in\Lambda} \mathbb{Z} & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow\iota & & \\ K & \longrightarrow & \bigoplus_{\lambda\in\Lambda} \mathbb{Q} & \longrightarrow & \bigoplus_{\lambda\in\Lambda} \mathbb{Q}/K & \longrightarrow & 0 \end{array}$$

Wir setzen $I := \left(\bigoplus_{\lambda\in\Lambda} \mathbb{Q}\right)/K$ und behaupten, dass I eine injektive abelsche Gruppe ist. Damit haben wir $\iota : M \hookrightarrow I$ gefunden, dessen Injektivität durch Diagrammjagd (oder dem Schlangenlemma) aus dem Diagramm hervorgeht. Es bleibt zu zeigen, dass I injektiv ist. Dazu genügt es nach Vortrag 2 Satz 2.19 zu zeigen, dass I divisibel ist. Die Gruppe $\bigoplus_{\lambda\in\Lambda} \mathbb{Q}$ ist sogar ein $\mathbb{Q}$-Vektorraum und daher divisibel. Da der Quotient einer divisiblen Gruppe wiederum divisibel ist, ist auch I divisibel.

Sei nun R beliebig und sei M ein beliebiger R-Modul. Aus dem Vorangehenden wissen wir, dass es eine injektive abelsche Gruppe I und einen injektiven Gruppenhomomorphismus $\iota : M \hookrightarrow I$ gibt. Wir wollen zeigen, dass man M in $\mathrm{Hom}_{\mathbb{Z}}(R, I)$ als R-Modul einbetten kann. Dazu betrachten wir

$$\eta : M \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, M) \xrightarrow{\iota\circ} \mathrm{Hom}_{\mathbb{Z}}(R, I), \quad m \longmapsto (x \mapsto \iota(xm)).$$

Da $\eta(m)(1) = \iota(m)$ gilt, ist η ein injektiver Gruppenhomomorphismus, denn ι ist injektiv. Es muss noch gezeigt werden, dass die Abbildung ein R-Modulhomomorphismen ist:

$$\eta(rm) = (x \longmapsto \iota(xrm)) = r \cdot (x \longmapsto \iota(xm)) = r\eta(m).$$

□

3.3 Homotopie

Definition 3.13. Eine **Homotopie** zwischen Morphismen $f, g : E^\bullet \to E'^\bullet$ von Komplexen ist eine Sequenz von Homomorphismen

$$h_i : E^i \longrightarrow E'^{(i-1)},$$

so dass die Gleichungen

$$f_i - g_i = d'^{(i-1)} \circ h_i + h_{n+1} \circ d^i$$

gelten. Die Morphismen f und g heißen dann **homotop**. Wir wollen betonen, dass das Diagramm

$$\begin{array}{ccccc} E^{i-1} & \xrightarrow{d^{i-1}} & E^i & \xrightarrow{d^i} & E^{i+1} \\ {\scriptstyle f-g}\downarrow & \swarrow{\scriptstyle h_i} & {\scriptstyle f-g}\downarrow & \swarrow{\scriptstyle h_{i+1}} & \downarrow{\scriptstyle f-g} \\ E'^{(i-1)} & \xrightarrow[d'^{(i-1)}]{} & E'^i & \xrightarrow[d'^i]{} & E'^{i+1} \end{array}$$

nicht kommutativ ist.

Lemma 3.14. *Sind f und g homotop, dann induzieren sie denselben Homomorphismus auf der Homologie* $\mathrm{H}(E^\bullet)$*, also*

$$\mathrm{H}^i(f) = \mathrm{H}^i(g) : \mathrm{H}^i(E) \longrightarrow \mathrm{H}^i(E').$$

Beweis. Sei h eine Homotopie zwischen f und g, also $f - g = d'h + hd$. Wir müssen zeigen, dass $f_i - g_i$ die Gruppe der Zykeln $\mathrm{Z}^i(E^\bullet)$ in die Gruppe der Ränder $\mathrm{B}^i(E'^\bullet)$ abbildet. Sei $x \in \mathrm{Z}^i(E^\bullet)$. Dann gilt

$$(f_i - g_i)(x) = d'^{i-1}h_i(x) + h_{i+1}d^i(x) = d'^{i-1}h_i(x) \in \mathrm{B}^i(E'^\bullet).$$

□

Jetzt beweisen wir noch einen fundamentalen Baustein für den Formalismus des derivierten Funktors.

Satz 3.15. *(1) Betrachte zwei Komplexe*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{d^{-1}} & E^0 & \longrightarrow & E^1 & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \varphi} & & & & & & \\ 0 & \longrightarrow & N & \xrightarrow{d'^{-1}} & I^0 & \longrightarrow & I^1 & \longrightarrow & \cdots \end{array}$$

wobei $E^\bullet$ eine Auflösung von M ist, die Moduln I^n injektiv sind und $\varphi : M \to N$ ein Modulhomomorphismus ist. Dann existiert ein Morphismus f von Komplexen, der φ fortsetz: $f_{-1} = \varphi$, und je zwei solcher Fortsetzungen sind homotop.

(2) Die Zuordnung $f \mapsto \mathrm{H}^0(f)$ definiert einen Isomorphismus

$$\mathrm{Hom}(E^\bullet, I^\bullet)/(\textit{Homotopie}) \xrightarrow{\cong} \mathrm{Hom}(M, N).$$

Beweis. Die Aussage (2) faßt nur die Aussage (1) zusammen. Konstruieren wir also eine fortsetzung f zu φ. Die Konstruktion erfolgt induktiv. Da I^0 injektiv ist, existiert ein $f_0 : E^0 \to I^0$, so dass $f_0 \circ d^{-1} = d'^{-1} \circ \varphi$:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M & \xrightarrow{d^{-1}} & E^0 & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \varphi} & & \vdots{\scriptstyle f_0} & & \\ & & N & \xrightarrow{d'^{-1}} & I^0 & \longrightarrow & \cdots \end{array}$$

Wir teilen nun die Bilder von M und N heraus, setzen $M_1 = E^0/M$ und $N_1 = I^0/N$, und erhalten für f_1 das Liftungsproblem

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_1 & \xrightarrow{d^0} & E^1 & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f_0} & & \vdots{\scriptstyle f_1} & & \\ & & N_1 & \xrightarrow{d'^0} & I^1 & \longrightarrow & \cdots \end{array}$$

Mit dem gleichen Argument wie oben existiert auch f_1, und alle weitern f_i erhält man offensichtlich induktiv.

Sein nun f und g zwei Fortsetzungen von φ. Wenn wir eine Homotopie zwischen f und g finden wollen, interessiert uns nur die Differenz $f - g$. Wir nehmen daher o.E. an, dass $\varphi = 0$ und $g = 0$ ist. Die Homotopie h konstruieren wir nun per Induktion nach dem Grad.

Wir setzen $h_0 : E^0 \to N$ als Nullabbildung. Dann muss h_1 das Liftungsproblem im folgenden Diagramm für $i = 0$ lösen.

$$\begin{array}{ccc} E^i & \xrightarrow{d^i} & E^{i+1} \\ {\scriptstyle f_i - d'^{i-1} h_i}\downarrow & \swarrow{\scriptstyle h_{i+1}} & \\ I^i & & \end{array}$$

Dies gelingt wegen der Injektivität von I^i genau falls $f_i - d'^{i-1} h_i$ auf $\ker d^i = \operatorname{im} d^{i-1}$ verschwindet:

$$\begin{aligned} \left(f_i - d'^{i-1} h_i\right) \circ d^{i-1} &= f_{\mathrm{id}}^{i-1} - d'^{i-1} h_{\mathrm{id}}^{i-1} = d'^{i-1} f_{i-1} - d'^{i-1} h_{\mathrm{id}}^{i-1} \\ &= d'^{i-1} \left(f_{i-1} - h_{\mathrm{id}}^{i-1}\right) = d'^{i-1} d'^{i-2} h_{i-1} = 0. \end{aligned}$$

In diese Rechnung sind alle bisher nicht definierten Abbildungen mit negativem Index die Nullabbildung. Die präsentierte Form zeigt aber gleichzeitig den Induktionsschritt von i auf $i + 1$. □

Vortrag 4

Gruppenkohomologie I: Die Standardauflösung

Boryana Dimitrova
15.11.2005

4.1 Der Gruppenring

Definition 4.1. Sei S eine Menge. Die **freie abelsche Gruppe erzeugt von S** ist

$$\mathbb{Z}\langle S\rangle := \{\varphi : S \longrightarrow \mathbb{Z} \mid \varphi(s) = 0 \text{ für alle bis auf endlich viele } s \in S\}$$

mit komponentenweise Addition als Verknüpfung.

Bemerkung 4.2. Sei $\varphi \in \mathbb{Z}\langle S\rangle$. Dann gibt es eindeutige Darstellung

$$\varphi = \sum_{s\in S} m_s.s, \quad m_s \in \mathbb{Z}, \quad \text{mit } m_s = 0 \text{ für fast alle } s \in S,$$

wobei $s \in \mathbb{Z}\langle S\rangle$ definiert ist durch $s(s) = 1$ und $s(s') = 0$ für alle $s' \neq s$.

Definition 4.3. Sei G eine beliebige Gruppe. Der **Gruppenring $\mathbb{Z}[G]$** ist die freie abelsche Gruppe $\mathbb{Z}\langle G\rangle$ ausgestattet mit der Multiplikation gegeben durch:

$$\sum_{g\in G} m_g.g \cdot \sum_{g'\in G} m'_{g'}.g' = \sum_{h\in G} \sum_{h=gg'} m_g m'_{g'}.h$$

Bemerkung 4.4. Einfaches Nachrechnen ergibt:

(1) $\mathbb{Z}[G]$ ist ein Ring, sogar eine $\mathbb{Z}$-Algebra.

(2) $\mathbb{Z}$ ist kommutativ $\iff$ G ist kommutativ.

(3) Eine analoge Konstruktion liefert $A[P]$ für ein beliebigen kommutativen Ring A und ein multiplikatives Monoid P.

Bemerkung 4.5. (1) Es gibt eine natürliche Bijektion zwischen:

$$\begin{array}{ccc}
G\text{-Mod} & \longleftrightarrow & \mathbb{Z}[G]\text{-Mod} \\
G \times M \to M & \longleftrightarrow & \mathbb{Z}[G] \times M \to M \\
(g, m) \to g \cdot m & \longmapsto & \left(\left(\sum_{g\in G} m_g.g\right), m\right) \to \sum_{g\in G} m_g.(g \cdot m) \\
(g, m) \to g \cdot m & \longleftarrow & \left(\left(\sum_{g\in G} m_g.g\right), m\right) \to \left(\sum_{g\in G} m_g.g\right) \cdot m
\end{array}$$

(2) Seien A, A' G-Module bzw. $\mathbb{Z}[G]$-Module, dann gilt:

$$\mathrm{Hom}_G(A, A') \cong \mathrm{Hom}_{\mathbb{Z}[G]}(A, A').$$

(3) Die **Augmentation** von $\mathbb{Z}[G]$ ist der Ringhomomorphismus

$$\begin{array}{rcl} \varepsilon : \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} \\ \sum_{g\in G} m_g.g & \longmapsto & \sum_{g\in G} m_g. \end{array}$$

Den Kern $IG = \ker \varepsilon$ nennt man das **Augmentationsideal** von G.

Lemma 4.6. *(1) IG hat als abelsche Gruppe die Basis $\{g-1 \in \mathbb{Z}\langle G\rangle \mid 1 \neq g \in G\}$.*

(2) Falls $G = \langle S\rangle$, dann ist $S-1 = \{s-1 \in \mathbb{Z}\langle G\rangle \mid s \in S\}$ ein Erzeugendensystem von IG als G-Modul.

Beweis. (1) *Lineare Unabhängigkeit* ist klar: Eine Relation $\sum_{g\in G, g\neq 1} m_g.(g-1) = 0$ impliziert

$$\sum_{g\in G, g\neq 1} m_g.g - \left(\sum_{g\in G, g\neq 1} m_g\right)\cdot 1 = 0$$

und da die $g \in G$ eine Basis von $\mathbb{Z}[G]$ bilden, folgt $m_g = 0$.

Erzeugendensystem: Die Koeffizienten eines Elements $\left(\sum_{g\in G} m_g.g\right) \in IG$ erfüllen

$$\sum_{g\in G} m_g = 0.$$

Damit gilt

$$\sum_{g\in G} m_g.g = \sum_{g\in G} m_g.g - 0 = \sum_{g\in G} m_g.g - \sum_{g\in G} m_g = \sum_{g\in G, g\neq 1} m_g.(g-1)\ .$$

(2) Nach $\imath$ genügt es zu zeigen, dass $\forall\ g \in G$ das Element $(g-1)$ in dem von $S-1$ erzeugten G-Modul liegt. Wir wissen:

$$\forall\ g \in G : \exists k \in \mathbb{N}, g_1, \ldots g_k \in S : g = g_1^{\pm 1} g_2^{\pm 1} \ldots g_k^{\pm 1}.$$

Also genügt zu zeigen:

$$g_1 - 1, g_2 - 1 \in \langle S-1\rangle \Longrightarrow g_1 g_2 - 1, g_1^{-1} - 1 \in \langle S-1\rangle,$$

aber $g_1 g_2 - 1 = g_1(g_2-1) + (g_1-1)$ und $g_1^{-1} - 1 = -g_1^{-1}(g_1-1)$, und damit folgt die Behauptung.

□

4.2 Die Kohomologiegruppen

Definition 4.7. Ein **trivialer *G*-Modul** ist ein G-Modul A mit $g.a = a, \forall\, g \in G, \forall\, a \in A$.

Im folgenden ist $\mathbb{Z}$ stets mit der trivialen G-Modulstruktur versehen.

Definition 4.8. Sei M ein G-Modul. Sei

$$P_\bullet \longrightarrow \mathbb{Z} \longrightarrow 0$$

eine projektive Auflösung von $\mathbb{Z}$ mit G-Modulen (bzw. $\mathbb{Z}[G]$-Modulen). Sei

$$C^i := \mathrm{Hom}_G(P_i, M)$$

und C der Komplex

$$0 \longrightarrow C^0 \longrightarrow C^1 \longrightarrow \cdots$$

mit induzierten Differentialen $f \mapsto f \circ d$. Wir nennen $\mathrm{H}^i(G, M) := \mathrm{H}^i(C)$ **die *i*-te Kohomologiegruppe von *G* mit Koeffizienten in *M***.

Bemerkung 4.9. Es existiert mindestens eine projektive Auflösung von $\mathbb{Z}$. (vgl. Vortrag 2)

$$P_1 = \bigoplus_{m_j \in M} R_{m_j}, \qquad P_i = \bigoplus_{m_j \in M_{i-1}} R_{m_j}$$

$$f_i : P_i \longrightarrow P_{i-1}, \quad 1_{m_j} \longrightarrow m_j, \qquad M_i = \mathrm{im}\, f_{i+1}$$

$$\cdots \xrightarrow{f_4} P_3 \xrightarrow{f_3} P_2 \xrightarrow{f_2} P_1 \xrightarrow{f_1} M \to 0.$$

Wohldefiniertheit der Gruppen $\mathrm{H}^i(G, A)$: Wir definieren vorübergehend zur besseren Unterscheidung der Abhängigkeit von der gewählten Auflösung

$$\mathrm{H}^i_{P^\bullet}(G, M) := \mathrm{H}^i(\mathrm{Hom}_G(P_\bullet, M)).$$

Sei $Q_\bullet$ eine weitere projektive Auflösung von $\mathbb{Z}$. In Vortrag 3 Satz 3.15 wurde gezeigt, dass ein Morphismus von Komplexen $f : P_\bullet \longrightarrow Q_\bullet$ mit $f_{-1} = \mathrm{id}$ existiert, d.h. ein Morphismus von Komplexen, der die Identität fortsetzt. Darüberhinaus sind je zwei solche Morphismen homotop.

$$\begin{array}{ccccccccc}
\cdots & \xrightarrow{d} & P_1 & \longrightarrow & P_0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & \swarrow^{h} & \downarrow{\scriptstyle f_1 - g_1} & \swarrow^{h} & \downarrow{\scriptstyle f_0 - g_0} & & \downarrow{\scriptstyle Id} & & \\
\cdots & \xrightarrow{d'} & Q_1 & \longrightarrow & Q_0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

Seien $f, g : P_\bullet \longrightarrow Q_\bullet$ zwei solche und h die entsprechende Homotopie. Dann sind $\circ f$ und $\circ g$ Morphismen von $\mathrm{Hom}_G(Q_*, M)$ nach $\mathrm{Hom}_G(P_*, M)$ und $\circ h$ ist eine Homotopie zwischen diesen: $\circ f - \circ g = \circ(f - g) = \circ(d'h + hd) = (\circ d')(\circ h) + (\circ h)(\circ d)$:

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & \mathrm{Hom}_G(Q_0, M) & \longrightarrow & \mathrm{Hom}_G(Q_1, M) & \longrightarrow & \mathrm{Hom}_G(Q_2, M) & \xrightarrow{\circ h} & \cdots. \\
 & & \downarrow{\scriptstyle \circ f}\ \downarrow{\scriptstyle \circ g} & \swarrow^{\circ h} & \downarrow{\scriptstyle \circ f}\ \downarrow{\scriptstyle \circ g} & \swarrow^{\circ h} & \downarrow{\scriptstyle \circ f}\ \downarrow{\scriptstyle \circ g} & & \\
0 & \longrightarrow & \mathrm{Hom}_G(P_0, M) & \longrightarrow & \mathrm{Hom}_G(P_1, M) & \longrightarrow & \mathrm{Hom}_G(P_2, M) & \longrightarrow & \cdots
\end{array}$$

Insbesondere induzieren $(\circ f)$ und $(\circ g)$ denselben Morphismus auf der Homologie, den wir wie folgt bezeichnen

$$\Phi^i_{P^\bullet,Q^\bullet} = \mathrm{H}^i(\circ f) = \mathrm{H}^i(\circ g) : \mathrm{H}^i_{Q^\bullet}(G,M) \to \mathrm{H}^i_{P^\bullet}(G,M).$$

Hat man eine dritte projektive Auflösung $R^\bullet \to \mathbb{Z}$. Dann folgt aus der Eindeutigkeit der Fortsetzung bis auf Homotopie aus Vortrag 3, Satz 3.15

$$\Phi^i_{P^\bullet,P^\bullet} = \mathrm{id} \qquad \text{und} \qquad \Phi^i_{P^\bullet,R^\bullet} = \Phi^i_{P^\bullet,Q^\bullet}\Phi^i_{Q^\bullet,R^\bullet}$$

Daher ist $\Phi^i_{Q^\bullet,P^\bullet}$ ein Isomorphismus mit Inversem $\Phi^i_{P^\bullet,Q^\bullet}$ und die Kohomologiegruppen hängen also nur bis auf einen kanonischen eindeutigen Isomorphismus von der Wahl der projektiven Auflösung ab.

4.3 Die Standardauflösung

Wir wollen jetzt eine projektive Auflösung von $\mathbb{Z}$ konstruieren, die sogenannte Standardauflösung. Wir setzen $P_r = \mathbb{Z}\left\langle \prod_{i=0}^r G \right\rangle$ als abelsche Gruppe. Die Operaton von G auf P_r definieren wir mittels

$$g \cdot \left(\sum_{\overline{g} \in G^{r+1}} m_{\overline{g}}.\overline{g} \right) = \sum_{\overline{g} \in G^{r+1}} m_{\overline{g}}.(g\overline{g})$$

$$\overline{g} = (g_0, g_1, \cdots, g_r), g\overline{g} = (gg_0, gg_1, \cdots, gg_r).$$

Die Differentiale $d_r : P_{r+1} \longrightarrow P_r$ seien

$$d_r(\overline{g}) = \sum_{i=0}^{r+1} (-1)^i \overline{g}_i$$

$$\overline{g} = (g_0, g_1, \cdots, g_{r+1}), \quad \overline{g}_i = (g_0, \cdots, \hat{g}_i, g_{i+1}, \cdots, g_{r+1}).$$

Wir erhalten somit die **Standardauflösung** von $\mathbb{Z}$

$$\cdots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

wobei ε die Augmentation $P_0 = \mathbb{Z}[G] \to \mathbb{Z}$ ist.

Lemma 4.10. *Mit den Bezeichnungen von oben ist*

$$P_\bullet \longrightarrow \mathbb{Z} \longrightarrow 0$$

eine projektive Auflösung von $\mathbb{Z}$.

Beweis. Wir zeigen zunächst, dass $P_\bullet \to \mathbb{Z}$ ein Komplex ist:

$$d_{r-1} \circ d_r(\overline{g}) = d_{r-1}\left(\sum_{i=0}^{r+1} (-1)^i \overline{g}_i \right) = \sum_{i=0}^{r+1} (-1)^i \left(\sum_{j<i} (-1)^j \overline{g}_{ji} + \sum_{j>i} (-1)^{j+1} \overline{g}_{ij} \right)$$

$$= \sum_{i=0}^{r+1} \sum_{j<i} (-1)^{i+j} \overline{g}_{ji} + \sum_{i=0}^{r+1} \sum_{j>i} (-1)^{i+j+1} \overline{g}_{ij} = 0,$$

und

$$\varepsilon \circ d_0(\overline{g}) = \varepsilon(\overline{g}_2 - \overline{g}_1) = 1 - 1 = 0.$$

Dieser Komplex ist exakt: wähle $h \in G$ und definiere $k_r : P_r \to P_{r+1}$ durch $\overline{g} \to (h, \overline{g})$. Wir betonen, dass die k_r keine G-Homomorphismen sind. Es gilt

$$d_r \circ k_r + k_{r-1} \circ d_{r-1} = \mathrm{id}\,. \tag{4.1}$$

und es folgt: $\forall\, x \in \ker d_{r-1} : d_r(k_r(x)) = x \Rightarrow x \in \mathrm{im}\, d_r$.

Alternativ kann man wie folgt argumentieren. Zwar sind die k_r keine G-Homomorphismen, aber um Exaktheit zu prüfen, kann man die G-Modulstruktur vergessen und nur mit den zugrundeliegenden abelschen Gruppen arbeiten. Als Komplex von Abelschen Gruppen ist die Identität homotop zur Nullabbildung vermöge der Homotopie $k_\bullet$. Daher ist die Identität auf der Homologie von $P_\bullet \to \mathbb{Z}$ gleich der Nullabbildung: die Homologie verschwindet also.

Die Gleichung (4.1) sieht man wie folgt:

$$d_r \circ k_r(\overline{g}) + k_{r-1} \circ d_{r-1}(\overline{g}) = d_r(h, \overline{g}) + k_{r-1} \left(\sum_{i=0}^{r} (-1)^i \overline{g}_i \right)$$

$$= \sum_{i=0}^{r} (-1)^{i+1} (h, \overline{g}_i) + \overline{g} + \sum_{i=0}^{r} (-1)^i (h, \overline{g}_i) = \overline{g}.$$

Für die Exaktheit bei P_0 beachte, daß $d_0(1, \overline{g}) = g - 1$. Mit Lemma 4.6 folgt:

$$\langle d_0(1, g_i) | g_i \in G \rangle = IG = \ker \varepsilon.$$

Die G-Moduln P_r sind projektive G-Moduln: P_r sind sogar freie $\mathbb{Z}[G]$-Module: Eine Basis ist gegeben durch $B_r = \{(1, \overline{g}) \mid \overline{g} \in G^r\}$. Klar ist $\langle B_r \rangle = P_r$, denn

$$(g_0, g_1, \ldots, g_r) = g_0(1, g_0^{-1} g_1, \ldots, g_0^{-1} g_r).$$

Die lineare Unabhängigkeit über $\mathbb{Z}[G]$ ergibt sich wie folgt. Eine Relation

$$\sum_{\overline{g} \in G^r} \left(\left(\sum_{g \in G} m_g^{\overline{g}} \right) g \cdot (1, \overline{g}) \right) = \sum_{g \in G} \sum_{\overline{g} \in G^r} m_g^{\overline{g}} \cdot (g, g\overline{g}) = 0$$

erzwingt $m_g^{\overline{g}} = 0, \forall\, g \in G, \forall\, \overline{g} \in G^r$, da die $(g, g\overline{g})$ eine $\mathbb{Z}$-Basis von P_r sind. □

Definition 4.11. Die **Gruppe der homogenen r-Koketten von G mit Werten in M** ist

$$\tilde{\mathscr{C}}^r(G, M) = \{\varphi \in \mathrm{Abb}(G^{r+1}, M) \mid \varphi(g\overline{g}) = g\varphi(\overline{g}), \forall\, g \in G, \forall\, \overline{g} \in G^r\}.$$

Wir identifizieren $\tilde{\mathscr{C}}^r$ kanonisch mit $\mathrm{Hom}_G(P_r, M)$ vermöge der kanonischen $\mathbb{Z}$-Basen der P_r und berechnen die induzierten Differentiale:

$$\overline{d}^r : \tilde{\mathscr{C}}^r(G,M) \longrightarrow \tilde{\mathscr{C}}^{r+1}(G,M), \quad \varphi \longmapsto \left(\left(\overline{d}^r \varphi\right)(\overline{g}) = \sum_{i=0}^{r+1} (-1)^i \varphi(\overline{g}_i) \right).$$

Nach Lemma 4.10 folgt $\mathrm{H}^r(G,M) \cong \ker \overline{d}^r / \operatorname{im} \overline{d}^{r-1}$.

Definition 4.12. Die **Gruppe der inhomogenen r-Koketten von G mit Werten in M** ist

$$\mathscr{C}^r(G,M) = \{\varphi \in \mathrm{Abb}(G^r, M)\}, \mathscr{C}^0(G,M) := M.$$

Wir identifiziere $\mathscr{C}^r$ kanonisch mit $\mathrm{Hom}_G(P_r, M)$ vermöge der $\mathbb{Z}[G]$-Basen $\{1\} \times G^r$ von P^r und berechnen die induzierten Differentiale:

$$\begin{aligned} d^r : \mathscr{C}^r(G,M) &\longrightarrow \mathscr{C}^{r+1}(G,M) \\ \varphi &\longrightarrow (d^r\varphi)(g_1, \dots g_{r+1}) = g_1\varphi(g_2, \dots, g_{r+1}) \\ &\quad + \sum_{j=1}^{r} (-1)^j \varphi(g_1, \dots, g_j g_{j+1}, \dots, g_{r+1}) + (-1)^{r+1}\varphi(g_1, \dots, g_r). \end{aligned}$$

Lemma 4.13. $0 \longrightarrow \mathscr{C}^0(G,M) \xrightarrow{d^0} \mathscr{C}^1(G,M) \xrightarrow{d^1} \mathscr{C}^2(G,M) \longrightarrow \cdots$
ist ein Komplex und es gilt $\mathrm{H}^i(G,M) \cong \mathrm{H}^i(\mathscr{C})$.

Beweis. Wir haben ein kommutatives Diagramm

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \tilde{\mathscr{C}}^r(G,M) & \xrightarrow{\overline{d}^r} & \tilde{\mathscr{C}}^{r+1}(G,M) & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f^r} & & \downarrow{\scriptstyle f^{r+1}} & & \\ \cdots & \longrightarrow & \mathscr{C}^r(G,M) & \xrightarrow{d^r} & \mathscr{C}^{r+1}(G,M) & \longrightarrow & \cdots \end{array}$$

mit den bijektiven Abbildungen $f^r : \tilde{\mathscr{C}}^r(G,M) \longrightarrow \mathscr{C}^r(G,M)$ definiert durch

$$f^r(\varphi)(g_1, \dots, g_r) = \varphi(1, g_1, g_1g_2, \dots, g_1g_2 \cdots g_r).$$

Die f^r definieren eine Abbildung von Komplexen: $f^{r+1} \circ \overline{d^r} = d^r \circ f^r$, denn

$$\begin{aligned} & \left(\left(f^{r+1} \circ \overline{d^r}\right)(\varphi)\right)(g_1, g_2, \dots, g_{r+1}) = \left(f^{r+1} \circ \overline{d^r}\varphi\right)(g_1, g_2, \dots, g_{r+1}) \\ = \; & \overline{d^r}(\varphi)(1, g_1, g_1g_2, \dots, g_1g_2 \dots g_{r+1}) \\ = \; & \sum_{i=0}^{r+1} (-1)^i \varphi\left(1, g_1, \dots, \widehat{g_1 g_2 \cdots} g_i, \dots, g_1 \dots, g_{r+1}\right) \\ = \; & g_1 f^r(\varphi)(g_2, \dots, g_{r+1}) + \sum_{i=1}^{r} (-1)^i f^r(\varphi)(g_1, \dots, g_i g_{i+1}, \dots g_{r+1}) \\ & + (-1)^{r+1} f^r(\varphi)(g_1, \dots, g_r) \\ = \; & d^r\left(f^r(\varphi)\right)(g_1, \dots, g_{r+1}) = ((d^r \circ f)(\varphi))(g_1, \dots, g_{r+1}). \end{aligned}$$

Somit ist $\mathscr{C}^\bullet(G,M)$ ein Komplex und $f^\bullet$ ein Isomorphismus von Komplexen und damit ein Homologieisomorphismus, d.h. $\mathrm{H}(f)$ ist ein Isomorphismus auf den Homologiegruppen. $\square$

Vergleich mit $\mathbf{H^0, H^1, H^2}$ aus Vortrag 1:

(1) $\mathrm{H}^0(G,M) = \ker d^0$:
$\mathscr{C}^0(G,M) = M, d^0(m) = (g \mapsto gm - m)$,
$\ker d^0 = \{m \in M \mid gm = m, \forall\, g \in G\}$, d.h. $\mathrm{H}^0(G,M) = M^G$.

(2) $\mathrm{H}^1(G,M) = \ker d^1 / \operatorname{im} d^0$:
$\ker d^1 = \{\varphi \in \mathscr{C}^1(G,M) \mid g_1\varphi(g_2) - \varphi(g_1g_2) + \varphi(g_1) = 0\}$,
$\operatorname{im} d^0 = \{\varphi \in \mathscr{C}^1(G,M) \mid \varphi(g) = gm - m, \text{ für ein } m \in M\}$.

(3) $\mathrm{H}^2(G,M) = \ker d^2 / \operatorname{im} d^1$:
$\ker d^2 = \{\varphi \in \mathscr{C}^2(G,M) \mid g_1\varphi(g_2,g_3) - \varphi(g_1g_2,g_3) + \varphi(g_1,g_2g_3) - \varphi(g_1g_2) = 0\}$,
$\operatorname{im} d^1 = \{\varphi \in \mathscr{C}^2(G,M) \mid \varphi(g_1,g_2) = g_1\varphi'(g_2) - \varphi'(g_1g_2) + \varphi'(g_1), \text{ für ein } \varphi' \in \mathscr{C}^1(G,M)\}$.

Bemerkung 4.14. Falls die Operation von G auf M trivial ist, dann gilt:

$$\begin{aligned} \mathrm{H}^0(G,M) &= M \\ \mathrm{H}^1(G,M) &= \mathrm{Hom}(G,M), \end{aligned}$$

denn

$$g_1\varphi(g_2) - \varphi(g_1g_2) + \varphi(g_1) = 0 \Leftrightarrow \varphi(g_1) + \varphi(g_2) = \varphi(g_1g_2) \Leftrightarrow \varphi \in \mathrm{Hom}(G,M),$$

also $\ker d_1 = \mathrm{Hom}(G,M)$ und $\operatorname{im} d^0 = 0$, weil $gm - m = 0$ für alle $m \in M$.

4.4 Beispiele

(1) $\boldsymbol{G \cong \mathbb{Z}}$: Sei $G = \langle g \rangle$ multiplikativ geschrieben. Betrachte den Komplex

$$0 \longrightarrow \mathbb{Z}[G] \xrightarrow{\cdot(g-1)} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Die Moduln $\mathbb{Z}[G]$ sind frei und $(\cdot(g-1))$ sowie ε sind G-Homomorphismen. Benutze nun die Isomorphie $\mathbb{Z}[G] \cong \mathbb{Z}[t,t^{-1}]$ mit dem Laurant-Polynomring. Wir erhalten

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}[t,t^{-1}] & \xrightarrow{f} & \mathbb{Z}[t,t^{-1}] & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0 \\ & & p & \longmapsto & p(t-1),\ t & \longmapsto & 1 & & \end{array}$$

$$IG = \ker \varepsilon = (t-1)\mathbb{Z}[t,t^{-1}] = \operatorname{im} f, \quad \ker f = \{0\}$$

also ist der Komplex eine projektive Auflösung von $\mathbb{Z}$ mit G-Modulen. diesen benutzen wir zum Berechnen der Kohomologie von $\mathbb{Z}$. Diese Präsentation der Kohomologiegruppen hängt ein wenig vom gewählten Erzeuger von G ab. Wir bekommen:

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}[G],M) \xrightarrow{\circ(\cdot(g-1))} \mathrm{Hom}_G(\mathbb{Z}[G],M) \longrightarrow 0$$

Mit $\mathrm{Hom}_G(\mathbb{Z}[G],M) \cong M$ erhalten wir:

$$\begin{aligned} \mathrm{H}^0(G,M) &= M^G, \\ \mathrm{H}^1(G,M) &= M/\{m' \in M \mid gm - m = m', \text{ für ein m} \in M\}, \\ \mathrm{H}^i(G,M) &= 0, \qquad \forall\, i > 1. \end{aligned}$$

Insbesondere gilt für $M = \mathbb{Z}$ das folgende:

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

(2) $\boldsymbol{G \cong \mathbb{Z}/m\mathbb{Z}}$: Sei $G = \langle g \rangle$, und sei $N \in \mathbb{Z}[G], N := 1 + g + g^2 + \cdots + g^{m-1}$ das Normelement in $\mathbb{Z}[G]$. Betrachte den Komplex:

$$\cdots \xrightarrow{(\cdot(g-1))} \mathbb{Z}[G] \xrightarrow{(\cdot N)} \mathbb{Z}[G] \xrightarrow{(\cdot(g-1))} \mathbb{Z}[G] \xrightarrow{(\cdot N)} \mathbb{Z}[G] \xrightarrow{(\cdot(g-1))} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

Dieser Komplex ist eine projektive Auflösung von $\mathbb{Z}$, denn $\mathbb{Z}[G]$ ist frei, sowie $(\cdot N)$ und $(\cdot(g-1)$ sind G-Homomorphismen. Wir haben tatsächlich einen Komplex, da $0 = g^m - 1 = (g-1)N$, sowie $IG = \ker \varepsilon = \mathrm{im}(\cdot(g-1))$ vgl. Lemma 4.6.

Die Exaktheit rechnet man nach: für $\sum_{i=0}^{m-1} m_{g^i} g^i \in \ker(\cdot N)$ ist ein Urbild unter $\cdot(g-1)$ durch $\sum_{i=0}^{m-1} \left(\sum_{j \leq i} -m_{g^j} \right) g^i$ gegeben, sowie für $\sum_{i=0}^{m-1} m_{g^i} g^i \in \ker(\cdot(g-1))$ ist ein Urbild unter $\cdot N$ durch $m_{g^i} g$ gegeben.

Also bekommen wir folgenden Komplexen:

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}[G], M) \xrightarrow{(\circ\cdot(g-1))} \mathrm{Hom}_G(\mathbb{Z}[G], M) \xrightarrow{\circ(\cdot N)} \mathrm{Hom}_G(\mathbb{Z}[G], M) \longrightarrow \cdots$$

und damit unter Berücksichtigung von $\mathrm{Hom}_G(\mathbb{Z}[G], M) \cong M$:

$$\begin{aligned}
&\mathrm{H}^0(G, M) = M^G, \\
&\mathrm{H}^i(G, M) = \{m \in M \mid Nm = 0\}/(g-1)M, && i = 1, 3, 5, 7, \ldots, \\
&\mathrm{H}^i(G, M) = M^G/N \cdot M, && i = 2, 4, 6, 8, \ldots
\end{aligned}$$

Für $M = \mathbb{Z}$ bekommen wir:

$$\begin{aligned}
&\mathrm{H}^0(G, \mathbb{Z}) = \mathbb{Z}, \\
&\mathrm{H}^i(G, \mathbb{Z}) = 0, && i = 1, 3, 5, 7, \ldots, \\
&\mathrm{H}^i(G, \mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}, && i = 2, 4, 6, 8, \ldots
\end{aligned}$$

Vortrag 5

Kategorielle Sprache

Sebastian Hensel
22.11.2005

In diesem Vortrag werden wir keine neuen Resultate beweisen, vielmehr lernen wir mit der Kategorientheorie eine Sprache kennen, die sehr gut geeignet ist, den Formalismus der Kohomologie zu beschreiben.

Dazu müssen wir zunächst die grundlegenden Begriffe der Kategorie, des Funktors und der natürlichen Transformation definieren und durch Beispiele erläutern. Daraufhin werden wir einige Eigenschaften der Modulkategorie abstrahieren und so den Begriff der abelschen Kategorie entwickeln.

Schließlich werden wir einige einfache, aber wichtige Resultate über abelsche Kategorien beweisen, die wir im Folgenden für Konstruktionen benötigen.

5.1 Der Begriff der Kategorie

Definition 5.1 (Kategorie)**.** Eine **Kategorie** $\mathscr{C}$ besteht aus

(i) einer Klasse $\mathrm{Ob}(\mathscr{C})$ der **Objekte von** $\mathscr{C}$,

(ii) zu je zwei Objekten $A, B \in \mathrm{Ob}(\mathscr{C})$ einer Menge $\mathrm{Mor}(A, B) = \mathscr{C}(A, B)$, der **Menge der Morphismen von** $\mathscr{C}$. Dabei vereinbaren wir, dass $\mathscr{C}(A, B)$ und $\mathscr{C}(A', B')$ disjunkt sind, außer $A = A', B = B'$.

(iii) für alle $A, B, C \in \mathrm{Ob}(\mathscr{C})$ einer Verknüpfung

$$\mathscr{C}(B, C) \times \mathscr{C}(A, B) \longrightarrow \mathscr{C}(A, C)$$

$$(f, g) \longmapsto f \circ g,$$

die assoziativ ist. Ferner gibt es in allen $A \in \mathrm{Ob}(\mathscr{C})$ einen Morphismus **Identität** $\mathrm{id}_A \in \mathscr{C}(A, A)$, welches Einselement bezüglich der Verknüpfung ist.

Um uns mit dem Begriff vertraut zu machen, werden wir nun einige Beispiele kennenlernen, von denen einige für unsere späteren Betrachtungen sehr wichtig sind.

Beispiel 5.2. (1) Die Kategorie Set der Mengen. Objekte sind Mengen, $\mathrm{Set}(M, N)$ ist die Menge der Abbildungen von M nach N, die Verknüpfung ist die übliche Verkettung von Funktionen. Man überprüft leicht, dass die Axiome einer Kategorie erfüllt sind. Dieses Beispiel trägt die Schuld daran, dass man die Morphismen einer jeden Kategorie auch unpräzise als Abbildungen bezeichnet.

(2) Ähnlich definiert man auf natürliche Weise die Kategorie Grp der Gruppen, Rng der Ringe oder R-Mod der Links-R-Moduln, wobei die Morphismenmengen die Mengen der Homomorphismen von Gruppen, von Ringen oder von Moduln sind.

(3) Unterkategorien: Ist $\mathscr{C}$ eine Kategorie, so nennt man eine Kategorie $\mathscr{D}$ Unterkategorie von $\mathscr{C}$, falls

$$\mathrm{Ob}(\mathscr{D}) \subset \mathrm{Ob}(\mathscr{C}), \qquad \mathscr{D}(A,B) \subset \mathscr{C}(A,B)$$

und die Verknüpfungsabbildung von $\mathscr{D}$ mit der von $\mathscr{C}$ übereinstimmt.

(4) Die Kategorie $\mathrm{Ch}^\bullet(R\text{-Mod})$ der Kokettenkomplexe von R-Moduln. Objekte sind Kokettenkomplexe $(E^\bullet, d)$, mit $d^n : E^n \to E^{n+1}$, Morphismen sind Abbildungen von Kokettenkomplexen.

Die opponierte Kategorie $\mathscr{C}^{\mathrm{opp}}$ entsteht aus $\mathscr{C}$ durch „Umdrehen der Pfeile“:

Definition 5.3 (opponierte Kategorie)**.** Sei $\mathscr{C}$ eine Kategorie. Wir definieren die **opponierte Kategorie** $\mathscr{C}^{\mathrm{opp}}$ durch

$$\mathrm{Ob}(\mathscr{C}^{\mathrm{opp}}) = \mathrm{Ob}(\mathscr{C}).$$

$$\mathscr{C}^{\mathrm{opp}}(A,B) = \mathscr{C}(B,A)$$

$$f \circ_{\mathscr{C}^{\mathrm{opp}}} g = g \circ_{\mathscr{C}} f.$$

Wir haben bei der opponierten Kategorie bereits gesehen, dass die Morphismen in beliebigen Kategorien keine Abbildungen sein müssen. Noch deutlicher wird dies, wenn wir erneut Kokettenkomplexe betrachten, als Morphismen zwischen $A^\bullet$ und $B^\bullet$ jedoch nicht die Menge der Komplexabbildungen zwischen $A^\bullet$ und $B^\bullet$ betrachten, sondern die Menge der Äquivalenzklassen solcher Abbildungen bezüglich Homotopie. Um dies überhaupt hinschreiben zu können, benötigen wir

Lemma 5.4. *Seien $A^\bullet, B^\bullet, C^\bullet$ Kokettenkomplexe und $g : A^\bullet \to B^\bullet, f : B^\bullet \to C^\bullet$ zwei Abbildungen. Die Homotopieklasse von $f \circ g$ hängt nur von den Klassen von f und g ab, genauer gilt*

$$f \sim f' \quad \Rightarrow \quad f \circ g \sim f' \circ g$$
$$g \sim g' \quad \Rightarrow \quad f \circ g \sim f \circ g',$$

wann immer definiert.

Beweis. Wir zeigen nur die erste Behauptung, die zweite folgt analog. Sei also h eine Homotopie mit

$$f - f' = dh + hd$$

Dann gilt

$$f \circ g - f' \circ g = (f - f')g = (dh + hd)g = dhg + hdg = d(hg) + (hg)d,$$

da g Abbildung von Kokettenkomplexen ist und somit mit d kommutiert. Also ist hg Homotopie zwischen $f \circ g$ und $f' \circ g$. □

Das Lemma erlaubt es uns, die Verknüpfung von Homotopieklassen repräsentantenweise zu definieren; die Axiome einer Kategorie werden somit von $\mathrm{Ch}^\bullet(R\text{-Mod})$ übernommen. Wir können also eine Kategorie definieren durch

$$\mathrm{Ob}(\mathscr{C}) = \mathrm{Ob}(\mathrm{Ch}^\bullet(R\text{-Mod}))$$

$$\mathscr{C}(A^\bullet, B^\bullet) = \mathrm{Ch}^\bullet(R\text{-Mod})(A^\bullet, B^\bullet)/(\text{Homotopie})$$

$$[f] \circ_{\mathscr{C}} [g] = [f \circ g]$$

Der Begriff der Kategorie erlaubt es uns, einige Eigenschaften von Abbildungen von Moduln zu abstrahieren, wenn wir sie nur in Termen von Abbildungen (also Pfeilen und Diagrammen) formulieren können. Insbesondere müssen wir dabei den Bezug auf Elemente vermeiden, da die Objekte in beliebigen Kategorien nicht unbedingt Mengen sind.

So ist ein Modulhomomorphismus $f : M \to M'$ beispielsweise genau dann injektiv, wenn für alle $g, g' : M'' \to M$ gilt

$$f \circ g = f \circ g' \qquad \Rightarrow \qquad g = g'$$

Diese Charakterisierung verwendet weder die besondere Struktur eines Moduls noch Elemente, und lässt sich somit auf beliebige Kategorien übertragen.

Definition 5.5. (1) Wir nennen einen Morphismus $f : A \to B$ einer Kategorie $\mathscr{C}$ **Monomorphismus**, falls

$$f \circ g = f \circ g' \qquad \Rightarrow \qquad g = g'$$

gilt, wann immer definiert.

(2) Wir nennen einen Morphismus $f : A \to B$ einer Kategorie $\mathscr{C}$ **Epimorphismus**, falls

$$g \circ f = g' \circ f \qquad \Rightarrow \qquad g = g'$$

gilt, wann immer definiert.

(3) Wir nennen einen Morphismus $f : A \to B$ einer Kategorie $\mathscr{C}$ **Isomorphismus**, falls es einen Morphismus $g : B \to A$ gibt, sodass

$$f \circ g = \mathrm{id}_B, \qquad g \circ f = \mathrm{id}_A$$

In diesem Fall nennen wir A und B **isomorph**.

5.2 Funktoren

Definition 5.6 (Funktor)**.** Seien $\mathscr{C}, \mathscr{D}$ Kategorien. Ein **(kovarianter) Funktor** $F : \mathscr{C} \to \mathscr{D}$ besteht aus Abbildungen

$$F : \mathrm{Ob}(\mathscr{C}) \longrightarrow \mathrm{Ob}(\mathscr{D})$$

und

$$F : \mathscr{C}(A, B) \longrightarrow \mathscr{D}(FA, FB)$$

für alle $A, B \in \mathrm{Ob}(\mathscr{C})$, sodass

$$F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$$

und

$$F(f \circ g) = F(f) \circ F(g)$$

gelten.

Auch für diesen Begriff werden wir uns zunächst eine Beispiele ansehen.

Beispiel 5.7. (1) „Vergiss-Funktoren“: Wir können einen einfachen und dennoch nützlichen und wichtigen Funktor dadurch definieren, dass Struktur „weggelassen“ wird, z.B.

$$\mathrm{Grp} \longrightarrow \mathrm{Set}$$

indem einer Gruppe die zugrundeliegende Menge und einem Gruppenhomomorphismus die zugrundeliegende Mengenabbildung zugeordnet wird.

(2) In einem gewissen Sinne adjungiert zu „Vergissfunktoren“ können wir auch Funktoren definieren, die zusätzliche Struktur erzeugen. Wir haben als Beispiel dafür bereits den Gruppenring $\mathbb{Z}[G]$ kennengelernt. Die Bildung

$$\mathbb{Z}[\ ] : \mathrm{Grp} \longrightarrow \mathrm{Rng}$$

$$G \longmapsto \mathbb{Z}[G]$$

ist ein Funktor. Um dies nachzuweisen, müssen wir zunächst definieren, worauf $\mathbb{Z}[\ ]$ einen Gruppenhomomorphismus $f : G \to G'$ abbildet:

$$\widetilde{f} = \mathbb{Z}[\ ]f : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G'], \qquad \widetilde{f}(h_g) = h_{f(g)}, \quad \widetilde{f}|_{\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}}$$

wobei h_g die Basis von $\mathbb{Z}[G]$ bezeichne und $\tilde{f}$ dann linear fortgesetzt wird.

Auf diese Weise wird $\tilde{f}$ offenbar zu einem Homomorphismus der *Gruppen* $\mathbb{Z}[G] \to \mathbb{Z}[H]$. Wir müssen noch nachrechnen, dass diese Bildung auch ein Ringhomomorphismus ist.

$$\widetilde{f}\left(\left(\sum_{g\in G} m_g \cdot h_g\right)\left(\sum_{g\in G} m_g \cdot h_g\right)\right) = \widetilde{f}\left(\sum_{g,g'\in G} m_g m_{g'} \cdot h_{gg'}\right)$$

$$= \sum_{g,g'\in G} m_g m_{g'} \cdot h_{f(gg')} = \sum_{g,g'\in G} m_g m_{g'} \cdot h_{f(g)f(g')}$$

$$= \left(\sum_{g\in G} m_g \cdot h_{f(g)}\right)\left(\sum_{g'\in G} m_{g'} \cdot h_{f(g')}\right) = \widetilde{f}\left(\sum_{g\in G} m_g \cdot h_g\right)\widetilde{f}\left(\sum_{g'\in G} m_{g'} \cdot h_{g'}\right)$$

Die restlichen Axiome eines Funktors prüft man leicht nach.

(3) Auch die Bildung der i-ten Homologiegruppe eines Komplexes kann man als Funktor ansehen:

$$\mathrm{H}^i : \mathrm{Ch}^\bullet(R\text{-Mod}) \longrightarrow R\text{-Mod}$$

$$C^\bullet \longmapsto \mathrm{H}^i(C^\bullet)$$

Wir wissen bereits, dass jede Abbildung f von Kokettenkomplexen auf natürliche Weise eine Abbildung f_i auf den i-ten Homologiegruppen induziert. Setzt man

$$\mathrm{H}^i f = f_i$$

so wird H^i zu einem Funktor.

(4) Sei nun $\mathscr{C}$ eine beliebige Kategorie und $M \in \mathrm{Ob}(\mathscr{C})$ ein fest gewähltes Objekt. Dann definieren wir einen Funktor durch

$$\mathscr{C}(M,-) : \mathscr{C} \longrightarrow \mathrm{Set}$$
$$\mathscr{C}(M,-)(A) = \mathscr{C}(M,A)$$
$$\mathscr{C}(M,-)(f) = f^*, \qquad f^*\varphi = f \circ \varphi$$

Die Axiome eines Funktors sind erfüllt, da die Identität auf die Identität abgebildet wird und

$$(fg)^*\varphi = fg\varphi = f^*(g\varphi) = f^*g^*\varphi.$$

Man könnte versuchen, analog zu Beispiel (4) einen Funktor durch

$$\mathscr{C}(-,M) : \mathscr{C} \longrightarrow \mathrm{Set}$$
$$\mathscr{C}(-,M)(A) = \mathscr{C}(A,M)$$

zu definieren. Jedoch tritt bei dieser Bildung das Problem auf, dass es keine kanonische Möglichkeit gibt, eine Abbildung $f : A \to B$ zu einer Abbildung

$$f_* : \mathscr{C}(A,M) \longrightarrow \mathscr{C}(B,M)$$

fortzusetzen. Allerdings lässt sich durch die Vorschrift $f_*(\varphi) = \varphi f$ eine Abbildung

$$f_* : \mathscr{C}(B,M) \longrightarrow \mathscr{C}(A,M)$$

definieren. Auf diese Weise erhält man fast einen Funktor

$$\mathscr{C}(-,M) : \mathscr{C} \longrightarrow \mathrm{Set}$$
$$\mathscr{C}(-,M)(A) = \mathscr{C}(A,M)$$
$$\mathscr{C}(-,M)(f) = f_* : \mathscr{C}(B,M) \longrightarrow \mathscr{C}(A,M),$$

so dass

$$\mathscr{C}(-,M)(fg)(\varphi) = (fg)_*(\varphi) = \varphi fg = g_*(\varphi f) = g_*f_*\varphi = \mathscr{C}(-,M)(g)\mathscr{C}(-,M)(f)(\varphi).$$

Eine andere Möglichkeit diese Abbildung zu charakterisieren liefert die opponierte Kategorie: wir können nämlich $\mathscr{C}(-,M)$ als kovarianten Funktor $F : \mathscr{C}^{\mathrm{opp}} \to \mathrm{Set}$ auffassen: für $f \in \mathscr{C}(A,B) = \mathscr{C}^{\mathrm{opp}}(B,A)$ gilt nämlich dann

$$F(f) \in \mathrm{Set}(\mathscr{C}(B,M), \mathscr{C}(A,M)) = \mathrm{Set}(FB, FA)$$

und es gilt

$$F(f \circ_{\mathscr{C}^{\mathrm{opp}}} g) = F(g \circ_{\mathscr{C}} f) = F(f) \circ F(g).$$

Diese Betrachtungen liefern

Definition 5.8 (kontravarianter Funktor)**.** Seien $\mathscr{C}, \mathscr{D}$ Kategorien. Ein (kovarianter) Funktor

$$F : \mathscr{C}^{\mathrm{opp}} \longrightarrow \mathscr{D}$$

wird **kontravarianter Funktor** von $\mathscr{C} \to \mathscr{D}$ genannt.

5.3 Natürliche Transformationen

Definition 5.9 (natürliche Transformation)**.** (1) Seien $F, G : \mathscr{C} \to \mathscr{D}$ kovariante Funktoren. Eine **natürliche Transformation** $\eta : F \to G$ ist eine Abbildung, die jedem $C \in \mathrm{Ob}(\mathscr{C})$ einen Morphismus $\eta_C : FC \to GC$ zuordnet, sodass das Diagramm

$$\begin{array}{ccc} FC & \xrightarrow{Ff} & FC' \\ {\scriptstyle \eta_C}\downarrow & & \downarrow{\scriptstyle \eta_{C'}} \\ GC & \xrightarrow{Gf} & GC' \end{array}$$

für alle $C, C' \in \mathrm{Ob}(\mathscr{C})$ und alle $f : C \to C'$ kommutiert.

(2) Sind alle Abbildungen η_C einer natürlichen Transformation Isomorphismen, so nennen wir η einen **natürlichen Isomorphismus** und schreiben

$$\eta : F \simeq G.$$

(3) Gibt es Funktoren $F : \mathscr{C} \to \mathscr{D}$ und $G : \mathscr{D} \to \mathscr{C}$ sodass

$$FG \simeq \mathrm{id}, \qquad GF \simeq \mathrm{id}$$

gilt, so nennt man $\mathscr{C}$ und $\mathscr{D}$ **äquivalent** und F und G heißen **Äquivalenzen von Kategorien**.

Beispiel 5.10. (1) Aus Linearer Algebra I wissen wir, dass ein endlich-dimensionaler Vektorraum isomorph zu seinem Dualraum und natürlich isomorph zu dem zweifach dualen Raum ist. Diese Aussage können wir nun präzisieren. Sei Vect_k die Kategorie der Vektorräume über dem Körper k.

Wir behaupten, dass der Funktor

$$** : \mathrm{Vect}_k \longrightarrow \mathrm{Vect}_k$$

$$(**)V = V^{**}$$

$$(**)f = f^{**}; \qquad f^{**}\varphi = (\psi \longmapsto \varphi(\psi \circ f))$$

natürlich isomorph zum Identitätsfunktor ist. Dazu müssen wir zunächst zeigen, dass das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \eta}\downarrow & & \downarrow{\scriptstyle \eta} \\ V^{**} & \xrightarrow{f^{**}} & W^{**} \end{array}$$

für

$$\eta_V(v) = (\varphi \longmapsto \varphi(v))$$

kommutiert.

Doch

$$(\eta f)(v) = \eta(f(v)) = (\varphi \longmapsto \varphi \circ f(v))$$

und

$$(f^{**}\eta)(v) = f^{**}((\varphi \longmapsto \varphi(v)) = (\psi \longmapsto \psi \circ f(v)).$$

Ferner ist η offenbar injektiv. Aus linearer Algebra wissen wir, dass $\dim V = \dim V^*$, also ist η sogar ein natürlicher Isomorphismus.

(2) Fixiert man eine projektive Auflösung, so kann man die Bildung der Kohomologiegruppen zu dieser Auflösung aus dem vorherigen Vortrag als Funktor interpretieren.

Es wurde gezeigt, ohne diese Sprache zu verwenden, dass zwei solche Funktoren für verschiedene projektive Auflösungen natürlich isomorph zueinander sind.

5.4 Nullobjekte, Kerne und Kokerne

Wir haben bisher beliebige, abstrakte Kategorien betrachtet, die keinerlei zusätzliche Struktur tragen. Nun wollen wir einige Eigenschaften und Konstruktionen, die wir von Moduln her kennen, in die Sprache der Kategorientheorie übertragen. Dazu benötigen wir zunächst

Definition 5.11. Sei $\mathscr{C}$ eine Kategorie.

(1) $A \in \mathrm{Ob}(\mathscr{C})$ heißt **Anfangsobjekt (initiales Objekt)**, falls $\mathscr{C}(A, M)$ für alle $M \in \mathrm{Ob}(\mathscr{C})$ aus genau einem Element besteht.

(2) $A \in \mathrm{Ob}(\mathscr{C})$ heißt **Endobjekt (finales Objekt)**, falls $\mathscr{C}(M, A)$ für alle $M \in \mathrm{Ob}(\mathscr{C})$ aus genau einem Element besteht.

(3) $\mathbf{0} \in \mathrm{Ob}(\mathscr{C})$ heißt **Nullobjekt**, falls $\mathbf{0}$ sowohl initial wie final ist.

Lemma 5.12. *Je zwei initiale (bzw. finale) Objekte sind eindeutig isomorph zueinander. Gibt es ein Nullobjekt, so ist jedes initale oder finale Objekt zu diesem Nullobjekt eindeutig isomorph. Insbesondere sind alle Nullobjekte eindeutig isomorph.*

Beweis. Wir zeigen nur die Isomorphie zweier Anfangsobjekte – die anderen Aussagen folgen analog. Seien also A, A' zwei Anfangsobjekte. Ferner seien f, g so, dass

$$\mathscr{C}(A, A') = \{f\}, \qquad \mathscr{C}(A', A) = \{g\}.$$

Dann gilt

$$gf \in \mathscr{C}(A, A) = \{\mathrm{id}_A\}, \qquad fg \in \mathscr{C}(A', A') = \{\mathrm{id}_{A'}\}$$

und somit $A \simeq A'$. □

Beispiel 5.13. (1) In R-Mod ist der Nullring das Nullobjekt.

(2) In der Kategorie der Mengen gibt es kein Nullobjekt, denn $\emptyset$ ist initial und jede einelementige Menge ist final. Aber eine einelementige Menge ist nicht isomorph zu der leeren Menge. Gäbe es ein Nullobjekt, so müsste es aber nach dem Lemma isomorph zu sowohl der leeren wie der einelementigen Menge sein.

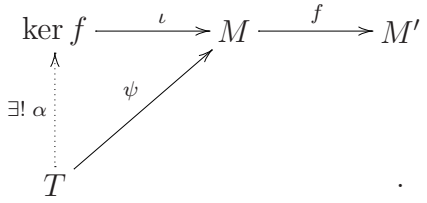
Besitzt eine Kategorie $\mathscr{C}$ ein Nullobjekt $\mathbf{0}$, so gibt es zu je zwei Objekten $A, B \in \mathrm{Ob}(\mathscr{C})$ einen ausgezeichneten Morphismus

$$A \longrightarrow \mathbf{0} \longrightarrow B$$

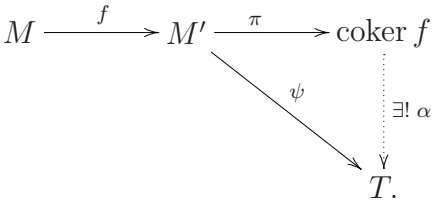
den wir den Nullmorphismus 0_{AB} oder einfach 0 nennen. Dies erlaubt es uns, den Begriff des Kerns und Kokerns elementfrei zu formulieren. Grundlage bildet dabei das folgende Lemma für Moduln

Lemma 5.14. *Sei $f : M \to M'$ ein Modulhomomorphismus. Dann gilt:*

(1) $\ker f$ *zusammen mit der natürlichen Inklusion $\iota : \ker f \to M$ hat die folgende universelle Eigenschaft: Es gilt $f \circ \iota = 0$, und ist T zusammen mit einem Modulhomomorphismus $\psi : T \to M$ ein weiteres Objekt mit $f\psi = 0$, so faktorisiert ψ eindeutig über* $\ker f$*:*



(2) $\operatorname{coker} f = M'/\operatorname{im}(f)$ *zusammen mit der natürlichen Projektion $\pi : M' \to \operatorname{coker} f$ hat die folgende universelle Eigenschaft: Es gilt $\pi \circ f = 0$, und ist T zusammen mit einem Modulhomomorphismus $\psi : M' \to T$ ein weiteres Objekt mit $\psi f = 0$, so faktorisiert ψ eindeutig über* $\operatorname{coker} f$*:*



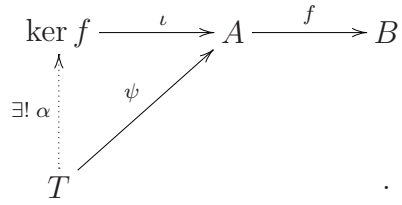
Beweis. (1) Nach Definition des Kerns gilt offenbar $f \circ \iota = 0$. Sei nun ein Testobjekt T zusammen mit $\psi : T \to M$ gegeben, sodass $f\psi = 0$. Dann gilt $\operatorname{im}\psi \subset \ker f$. Also lässt sich ψ als Abbildung $\psi : T \to \ker f$ auffassen. Doch dies heißt gerade, dass ψ über $\ker f$ faktorisiert. Die Eindeutigkeit ist offenbar.

(2) Nach Definition des Quotientenmoduls gilt $\pi \circ f = 0$. Ist ferner T Testobjekt mit $\psi : T \to M$, sodass $\psi f = 0$, so folgt $\operatorname{im} f \subset \ker \psi$. Doch dann faktorisiert ψ eindeutig über $\operatorname{coker} f$ nach der universellen Eigenschaft des Quotientenmoduls. □

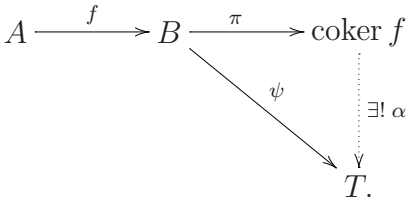
Das Lemma charakterisiert den Kern und Kokern einer Modulabbildung elementfrei. Da in Kategorien mit Nullobjekt die Nullabbildung definiert ist, können wir die Aussage des Lemmas nun als Definition verwenden:

Definition 5.15. Sei $\mathscr{C}$ Kategorie mit Nullobjekt und $f : A \to B$ Morphismus.

(1) Ein Objekt $\ker f$ zusammen mit einem Morphismus $\iota : \ker f \to A$ heißt **Kern von** f, falls $f \circ \iota = 0$ und ferner für jedes Objekt T zusammen mit einem Morphismus $\psi : T \to A$ mit $f \circ \psi = 0$ der Morphismus ψ eindeutig über $\ker f$ faktorisiert:



(2) Ein Objekt $\operatorname{coker} f$ zusammen mit einem Morphismus $\pi : B \to \operatorname{coker} f$ heißt **Kokern von** f, falls $\pi \circ f = 0$ und ferner für jedes Objekt T zusammen mit einem Morphismus $\psi : B \to T$ mit $\psi \circ f = 0$ der Morphismus ψ eindeutig über $\operatorname{coker} f$ faktorisiert:

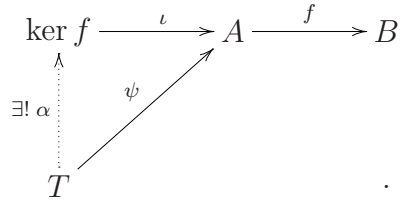


Das Lemma sagt nun nichts anderes, als dass Kerne und Kokerne von Modulhomomorphismen im üblichen Sinne auch Kerne bzw. Kokerne in der Kategorie der Moduln sind.

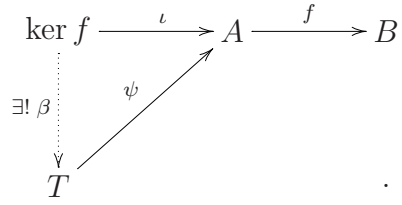
In beliebigen Kategorien müssen Kerne oder Kokerne von beliebigen Abbildungen nicht existieren. Ferner sind sie auf keinen Fall eindeutig, denn ein Objekt, welches isomorph zu einem Kern ist, ist sicherlich wieder ein Kern. Wir wollen aber zeigen, dass Kerne und Kokerne aber bis auf *eindeutige* Isomorphie eindeutig sind:

Lemma 5.16. *Je zwei Kerne (bzw. Kokerne) einer Abbildung $f : A \to B$ sind isomorph. Der Isomorphismus ist eindeutig, wenn man die Verträglichkeit mit der Kernabbildung $\ker f \to A$ (bzw. Kokernabbildung $B \to \operatorname{coker} f$) verlangt.*

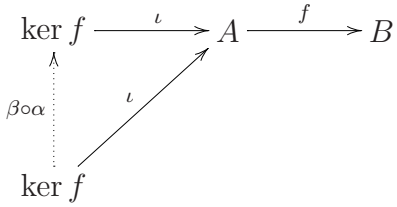
Beweis. Wir zeigen nur die Isomorphie zweier Kerne, der Fall für Kokerne folgt analog. Sei also $\ker f$ mit $\iota : \ker f \to A$ ein Kern von f und T mit $\psi : T \to A$ ein weiterer. Nach der universellen Eigenschaft von $\ker f$ faktorisiert ψ über $\ker f$ mittels einem α:



Analog folgt mit der universellen Eigenschaft von T die Existenz eines β mit



Somit ist $\beta \circ \alpha$ ein Morphismus, der das kommutative Diagramm



vervollständigt. Aber offensichtlich erfüllt auch id diese Eigenschaft. Wegen der Eindeutigkeit der Faktorisierung folgt $\beta\alpha = \mathrm{id}$. Analog folgt $\alpha\beta = \ \mathrm{id}$. Also ist α ein Isomorphismus. Die Eindeutigkeit von α ist klar. □

Im Folgenden werden wir oft etwas unpräzise von dem Kern oder Kokern einer Abbildung reden; streng genommen ist dieser natürlich nur bis auf Isomorphie bestimmt. Da unsere Argumente aber nur die universelle Eigenschaft und nicht die genaue Struktur des Objekts verwenden, ist diese Ungenauigkeit gerechtfertigt. Ferner werden wir oft von dem Kern $\ker f$ eines Morphismus $f : A \to B$ reden und dabei den Morphismus $\iota : \ker f \to A$ in unserer Notation weglassen, wenn der Kontext klar ist.

Definition 5.17 (Bild und Kobild)**.** Sei $f : A \to B$ Morphismus. Im Existenzfall nennen wir $\ker(\mathrm{coker}\, f)$ das **Bild** $\mathrm{im}\, f$ von f und $\mathrm{coker}(\ker f)$ das **Kobild** $\mathrm{coim}\, f$ von f.

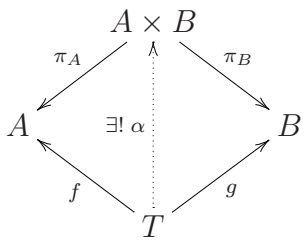
5.5 Additive und abelsche Kategorien

Definition 5.18 (Produkt und Koprodukt)**.** Sei $\mathscr{C}$ eine Kategorie und $A, B \in \mathrm{Ob}(\mathscr{C})$.

(1) Wir nennen ein Objekt $A \times B \in \mathrm{Ob}(\mathscr{C})$ zusammen mit Abbildungen

$$\pi_A : A \times B \longrightarrow A, \qquad \pi_B : A \times B \longrightarrow B$$

ein **(direktes) Produkt** von A in B, falls folgende universelle Eigenschaft erfüllt ist: Sei T ein beliebiges Objekt und $f : T \to A, g : T \to B$ Morphismen. Dann gibt es einen eindeutigen Morphismus $\alpha : T \to A \times B$, der das folgende Diagramm kommutieren lässt.

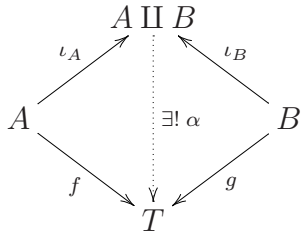


Die Abbildungen π_A, π_B heißen die **Projektionen** des Produkts. Der Morphismus α wird mit (f, g) bezeichnet.

(2) Wir nennen ein Objekt $A \amalg B \in \mathrm{Ob}(\mathscr{C})$ zusammen mit Abbildungen

$$\iota_A : A \longrightarrow A \amalg B, \qquad \iota_B : B \longrightarrow A \amalg B$$

ein **Koprodukt** (oder eine **Summe**) von A in B, falls folgende universelle Eigenschaft erfüllt ist: Sei T ein beliebiges Objekt und $f : A \to T, g : B \to T$ Morphismen. Dann gibt es einen eindeutigen Morphismus $\alpha : A \amalg B \to T$, der das folgende Diagramm kommutieren lässt.



Die Abbildungen ι_A, ι_B heißen die **Inklusionen** des Koprodukts. Der Morphismus α wird mit $f + g$ bezeichnet.

Produkte und Koprodukte sind ähnlich wie Kerne oder Kokerne nicht eindeutig bestimmt. Mit dem bei Kernen vorgeführten Standardargument zeigt man jedoch leicht

Lemma 5.19. *Je zwei Produkte (bzw. Koprodukte) von A und B sind isomorph. Der Isomorphismus ist eindeutig, wenn man die Verträglichkeit mit den zugehörigen Projektionen (bzw. Inklusionen) verlangt.*

Im Folgenden werden wir daher oft von dem Produkt (bzw. Koprodukt) reden, obwohl dieses nur bis auf Isomorphie bestimmt ist. Ferner werden wir oft davon reden, dass $A \times B$ das Produkt von A und B sei und dabei die Abbildungen weglassen, wenn dies im Kontext klar ist.

Definition 5.20 (additive Kategorie)**.** Eine **additive Kategorie** ist eine Kategorie $\mathscr{C}$, so dass

(i) $\mathscr{C}$ besitzt ein Nullobjekt,

(ii) für alle $A, B \in \mathrm{Ob}(\mathscr{C})$ besitzt $\mathscr{C}(A, B)$ die Struktur einer abelschen Gruppe,

(iii) die Kompositionsabbildung von $\mathscr{C}$ ist bilinear im Bezug auf diese Struktur,

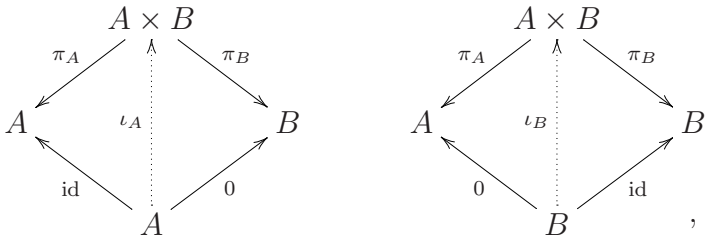
(iv) zu je zwei Objekten $A, B \in \mathrm{Ob}(\mathscr{C})$ existiert das direkte Produkt $A \times B$.

Beispiel 5.21. Die Kategorie der R-Moduln wird durch punktweise Addition von Homomorphismen zu einer additiven Kategorie. Direkte Produkte sind einfach die Produkte von Moduln, Koprodukte sind direkte Summen.

Im Falle der Kategorie von R-Moduln sind endliche direkte Summen isomorph zu endlichen direkten Produkten. Dies ist für alle additiven Kategorien wahr.

Lemma 5.22. *Sei $\mathscr{C}$ additive Kategorie und $A, B \in \mathrm{Ob}(\mathscr{C})$. Dann existiert $A \amalg B$ und ist natürlich isomorph zu $A \times B$.*

Beweis. Es reicht zu zeigen, dass $A \times B$ die universelle Eigenschaft eines Koproduktes erfüllt. Betrachten wir zunächst die Diagramme



wobei die ι_A, ι_B die eindeutigen, durch die universelle Eigenschaft induzierten Abbildungen sind. Diese haben die Eigenschaft, dass

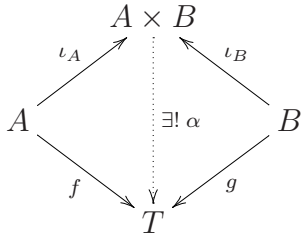
$$\pi_A \iota_A = \mathrm{id}_A, \qquad \pi_B \iota_B = \mathrm{id}_B$$

$$\pi_B \iota_A = 0, \qquad \pi_A \iota_B = 0.$$

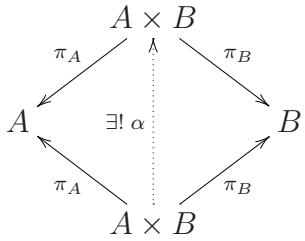
Wir behaupten, dass dies die Morphismen sind, die $A \times B$ zu einem Koprodukt machen. Sei dazu T beliebig und $f : A \to T, g : B \to T$ Morphismen. Definiere dann

$$\varphi = f\pi_A + g\pi_B$$

Dann gilt $\varphi\iota_A = f, \varphi\iota_B = g$, also kommutiert das Diagramm



Es bleibt zu zeigen, dass φ der einzige Morphismus mit dieser Eigenschaft ist. Es reicht dafür aber für einen Morphismus $\varphi : A \times B \to T$ zu zeigen, dass $\varphi\iota_A = 0$ und $\varphi\iota_B = 0$ gemeinsam $\varphi = 0$ implizieren. Dafür wiederum reicht es zu zeigen, dass $\iota_A\pi_A + \iota_B\pi_B = \mathrm{id}_{A\times B}$ ist. Doch dazu betrachte man das Diagramm



Sowohl $\alpha = \mathrm{id}$ wie auch $\alpha = \iota_A\pi_A + \iota_B\pi_B$ vervollständigen das kommutative Diagramm. Wegen der Eindeutigkeit der Faktorisierung folgt das Gewünschte. □

In additiven Kategorien können wir den Begriff des Mono- bzw. Epimorphismus etwas einfacher formulieren, es gilt die einfache

Bemerkung 5.23. Der Morphismus f ist genau dann Monomorphismus, wenn $f\varphi = 0$ bereits $\varphi = 0$ impliziert. Der Morphismus f ist genau dann Epimorphismus, wenn aus $\varphi f = 0$ bereits $\varphi = 0$ folgt.

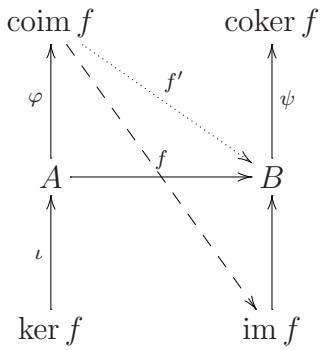
Lemma 5.24. *Sei $f : A \to B$ Morphismus einer Kategorie $\mathscr{C}$. Wenn* $\operatorname{im} f$ *und* $\operatorname{coim} f$ *existieren, so gibt es einen natürlichen Morphismus* $\operatorname{coim} f \to \operatorname{im} f$.

Beweis. Zunächst bemerken wir, dass Kokernabbildungen stets Epimorphismen sind: Sei nämlich $f : A \to B$ ein Morphismus und $g : B \to \operatorname{coker} f$ der Kokernmorphismus. Gelte ferner

$$\varphi g = \psi g$$

Dann gilt insbesondere $\varphi g f = 0 = \psi g f$. Nach der universellen Eigenschaft faktorisieren also sowohl φg wie ψg eindeutig über g, und somit folgt $\varphi = \psi$.

Wir betrachten nun das Diagramm



Da $f\iota = 0$ faktorisiert f über $\operatorname{coim} f$ eindeutig, sei f' die entsprechende Abbildung. Nun gilt $\psi f' \varphi = \psi f = 0$, also folgt $\psi f' = 0$. Somit faktorisiert f' eindeutig über $\operatorname{im} f$. Dies ist der gesuchte Morphismus

$$\operatorname{coim} f \longrightarrow \operatorname{im} f.$$

□

Definition 5.25 (abelsche Kategorie)**.** Eine **abelsche Kategorie** ist eine additive Kategorie, in der gilt:

(i) jeder Morphismus hat einen Kern und einen Kokern,

(ii) die natürliche Abbildung $\operatorname{coim} f \to \operatorname{im} f$ ist für alle Morphismen f ein Isomorphismus.

Beispiel 5.26. Die Kategorie von R-Moduln ist offenbar eine abelsche Kategorie, da nach dem Homomorphiesatz für alle $F : M \to M'$ die induzierte Abbildung

$$\widetilde{f} : M/\ker f \longrightarrow \operatorname{im} f$$

ein Isomorphismus von Moduln ist.

In abelschen Kategorien gibt es den einfachen Zusammenhang zwischen Epi-, Mono- und Isomorphismen, den man von Moduln her kennt:

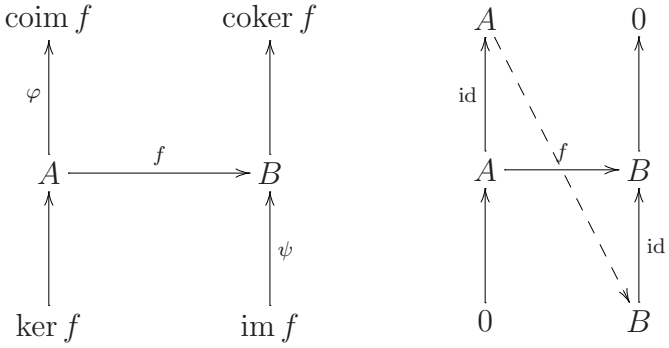
Lemma 5.27. *Sei $\mathscr{C}$ eine abelsche Kategorie. Ein Morphismus $f : A \to B$ ist genau dann ein Isomorphismus in $\mathscr{C}$, wenn f Epi- und Monomorphismus ist.*

Beweis. Ist f Isomorphismus, so ist f offenbar auch Epi- und Monomorphismus. Dies gilt in beliebigen Kategorien.

Sei nun f gleichzeitig Mono- und Epimorphismus. Wegen Bemerkung 5.23 gilt $\ker f = 0$ und $\operatorname{coker} f = 0$. Ferner bestimmt man leicht

$$\operatorname{coker}(0 \xrightarrow{0} A) = A \quad \text{und} \quad \ker(A \xrightarrow{0} 0) = A.$$

Also ergeben sich die Diagramme



und f ist Isomorphismus, da die natürliche Abbildung $\operatorname{coim} f \to \operatorname{im} f$ hier f selbst ist. □

Beispiel 5.28. Dass die Voraussetzung „abelsch“ in diesem Lemma tatsächlich gebraucht wird , genauer dass es nichtabelsche, additive Kategorien gibt, zeigt das folgende Beispiel.

Sei $\mathscr{C}$ die Kategorie der filtrierten Moduln mit Filtration der Länge 2, das heißt der Paare $(N \subseteq M)$ eines Moduls mit einem Untermodul. Morphismen $f : (N \subseteq M) \to (N' \subseteq M')$ sind Modulhomomorphismen $f : M \to M'$, sodass die Untermoduln ineinander überführt werden: $f(N) \subseteq N'$.

Dies ist eine additive Kategorie durch Addition von Modulhomomorphismen. Der Kern von f ist $(\ker f|_N \subseteq \ker f)$, der Kokern $(N'/(\operatorname{im} f \cap N') \subseteq M'/\operatorname{im} f)$ und die Produkte sind einfach die Produkte von Moduln. In dieser Kategorie betrachten wir nun den Morphismus

$$(0 \subset M) \xrightarrow{\mathrm{id}} (M \subset M)$$

für einen beliebigen Modul $M \neq 0$. Dieser ist Epi- und Monomorphismus, denn

$$\ker \mathrm{id} = (0 \subset 0) \quad \text{und} \quad \operatorname{coker} \mathrm{id} = (0 \subset 0)$$

Jedoch kann id in dieser Kategorie nicht Isomorphismus sein, da der Nullmorphismus die einzige Abbildung $(M \subset M) \to (0 \subset M)$ ist.

Da in abelschen Kategorien Kerne und Kokerne immer existieren, können wir auch den Begriff der exakten Sequenz übertragen:

Definition 5.29. Eine **exakte Sequenz** in einer abelsche Kategorie $\mathscr{C}$ ist ein Diagramm

$$A \xrightarrow{f} B \xrightarrow{g} C$$

in $\mathscr{C}$, so dass (bis auf kanonisch Isomorpie) $\ker g = \operatorname{im} f$ gilt.

Definition 5.30. (1) Ein **linksexakter Funktor** (bzw. **rechtsexakter Funktor**) ist ein Funktor $F : \mathscr{C} \to \mathscr{D}$ zwischen abelschen Kategorien $\mathscr{C}, \mathscr{D}$, so dass für jede kurze exakte Sequenz

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

in $\mathscr{C}$ die Sequenz

$$0 \longrightarrow FA \longrightarrow FB \longrightarrow FC \quad (\text{bzw. } FA \longrightarrow FB \longrightarrow FC \longrightarrow 0)$$

exakt in $\mathscr{D}$ ist.

(2) Ein **exakter Funktor** ist ein gleichzeitig rechts- und linksexakter Funktor.

Beispiel 5.31. Der Funktor $\mathscr{C}(M, -)$ ist linksexakt. Sei dazu

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

kurze exakte Sequenz. Wir betrachten die Sequenz

$$0 \longrightarrow \mathscr{C}(M, A) \xrightarrow{f^*} \mathscr{C}(M, B) \xrightarrow{g^*} \mathscr{C}(M, C)$$

Falls $\varphi \in \ker f^*$, also $f\varphi = 0$, so folgt $\varphi = 0$, da $\ker f = 0$. Ferner gilt $g^* f^* = 0$, da $gf = 0$. Sei nun

$$g^*\varphi = 0 \Leftrightarrow g\varphi = 0 \Leftrightarrow \varphi = \varphi_{\ker g}\psi = \varphi_{\operatorname{im} f}\psi$$

wobei $\varphi_{\ker g}, \varphi_{\operatorname{im} f}$ die Kern- bzw. Bildabbildung von f bezeichnen. Diese sind wegen der Exaktheit der Sequenz gleich. Doch f ist Monomorphismus, also folgt $\operatorname{coim} f = A$ und somit $\operatorname{im} f \simeq A$, also $\varphi_{\operatorname{im} f} = f$.

Wir haben die Modulkategorie als eine abelsche Kategorie kennengelernt. In einem gewissen Sinne gilt auch die Umkehrung. Wir brauchen dazu noch die Begriffe

Definition 5.32. Ein **kleine Kategorie** ist eine Kategorie $\mathscr{C}$, deren Klasse $\operatorname{Ob}(\mathscr{C})$ eine Menge ist.

Definition 5.33. (1) Ein **treuer Funktor** (bzw. ein **voller** Funktor) ist ein Funktor $F : \mathscr{A} \to \mathscr{B}$, so dass die Abbildungen

$$F : \mathscr{C}(A, B) \longrightarrow \mathscr{D}(FA, FB)$$

alle injektiv (bzw. surjektiv) sind.

(2) Ein **volltreuer Funktor** ist ein gleichzeitig treuer und voller Funktor.

Theorem 5.34 (Freyd-Mitchell Einbettungssatz)**.** *Sei $\mathscr{A}$ eine kleine abelsche Kategorie. Dann existiert ein Ring R und ein exakter, volltreuer Funktor $F : \mathscr{A} \to R$-Mod.*

Man kann also jede kleine abelsche Kategorie $\mathscr{A}$ als volle Unterkategorie einer Modulkategorie R-Mod interpretieren.

5.6 Dualtitätsprinzip

Abschließend wollen wir noch kurz ein allgemeines Prinzip für Kategorien vorstellen. Wir haben zu einer beliebigen Kategorie $\mathscr{C}$ die duale (oder opponierte) Kategorie $\mathscr{C}^{\mathrm{opp}}$ assoziiert, in der alle Morphismen „in die andere Richtung zeigen“.

Dies kann man sich zunutze machen, um bestimmte Aussagen in $\mathscr{C}$ zu dualisieren: hat man eine Aussage in einer Kategorie $\mathscr{C}$ so gezeigt, dass man den Beweis auch in der opponierten Kategorie führen könnte, so kann man direkt die duale Aussage folgern, also diejenige, die sich durch Interpretieren in der opponierten Kategorie ergibt.

So ist beispielsweise der Begriff des Produkts dual zu dem des Koprodukts (ist $A \times B$ das Produkt von A und B in $\mathscr{C}$, so hat dieses Produkt in der opponierten Kategorie gerade die Eigenschaften eines Koprodukts und umgekehrt). Zeigt man also (pfeiltheoretisch), dass Produkte in $\mathscr{C}$ bis auf Isomorphie eindeutig bestimmt sind, so kann man dieses Argument auch auf $\mathscr{C}^{\mathrm{opp}}$ anwenden. Doch die Aussage, dass Produkte in $\mathscr{C}^{\mathrm{opp}}$ bis auf Isomorphie eindeutig sind, bedeutet gerade, dass Koprodukte in $\mathscr{C}$ diese Eigenschaft haben.

Jedoch funktioniert dieses Verfahren nur dann, wenn der entsprechende Beweis auch wörtlich so in der opponierten Kategorie möglich wäre! Wir haben die beiden Aussagen

(a) *Die Modulkategorie enthält genügend viele injektive Objekte*, Vortrag 3, Satz 3.10.

(b) *Die Modulkategorie enthält genügend viele projektive Objekte*, Vortrag 2, im Beweis von Satz 2.13 (b) $\Longrightarrow$ (c).

bewiesen. Obwohl die beiden Aussagen dual zueinander sind, können wir keinen der Beweise wiederverwenden, da sie sich nicht in der dualen Modulkategorie durchführen lassen. Die Beweise der beiden Aussagen unterschieden sich deutlich: die Aussage über genügen viele injektive Moduln ist aufwendiger, während die Aussage über genügend viele projektive Moduln nahezu trivial ist.

Vortrag 6

Homologische Algebra III: δ-Funktoren

Frank Weilandt
29.11.2005

Es werden einige Eigenschaften des Homologie-Funktors auf kurzen exakten Sequenzen von Kettenkomplexen erarbeitet. Diese werden dann zum Konzept des δ-Funktors verallgemeinert und bei der Kohomologie von Gruppen wiedergefunden.

6.1 Vorüberlegungen

Gegeben sei ein kommutatives Diagramm von Moduln über einem Ring R und R-Modulhomomorphismen.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ X & \xrightarrow{g} & Y \end{array}$$

Nun induziert $f : A \to B$ mittels der Einschränkung einen Homomorphismus $f_K : \ker(\alpha) \to \ker(\beta)$. Klar, weil für ein $a \in \ker(\alpha)$ folgt: $\beta f(a) = g\alpha(a) = g(0) = 0$.

Der Morphismus g induziert auf naheliegende Art und Weise einen Homomorphismus

$$g_* : \operatorname{coker}(\alpha) \longrightarrow \operatorname{coker}(\beta), \quad g_* : [x] \longmapsto [gx].$$

Die Abbildung g_* ist wohldefiniert, denn wenn $\tilde{x} = x + \alpha(a)$ für ein $a \in A$, dann ist

$$g_*[\tilde{x}] = [gx + g\alpha(a)] = [gx + \beta f(a)] = [g(x)] = g_*[x].$$

Es ist ein Homomorphismus wegen

$$g_*[rx + sy] = [g(rx + sy)] = [rg(x) + sg(y)] = rg_*[x] + sg_*[y].$$

Nach diesen kurzen Vorarbeiten können wir nun ein nützliches Lemma formulieren.

Lemma 6.1 (Schlangenlemma)**.** *Sei folgendes Diagramm kommutativ mit exakten Zeilen.*

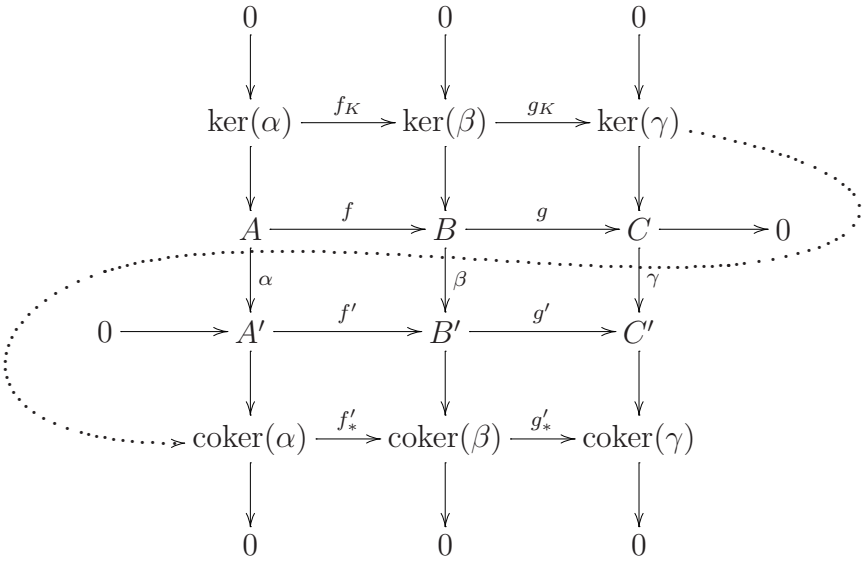
$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & {\scriptstyle\alpha}\downarrow & & {\scriptstyle\beta}\downarrow & & {\scriptstyle\gamma}\downarrow & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

Dann gibt es einen Homomorphismus $\delta : \ker(\gamma) \to \operatorname{coker}(\alpha)$*, so dass die folgende Sequenz exakt ist.*

$$\ker(\alpha) \xrightarrow{f_K} \ker(\beta) \xrightarrow{g_K} \ker(\gamma) \xrightarrow{\delta} \operatorname{coker}(\alpha) \xrightarrow{f'_*} \operatorname{coker}(\beta) \xrightarrow{g'_*} \operatorname{coker}(\gamma)$$

Wenn f *injektiv ist, so auch* f_K*. Und wenn* g' *surjektiv ist, dann auch* g'_**.*

Das folgende Diagramm mit den induzierten Abbildungen hat also exakte Zeilen und Spalten und die gepunktete Linie ist die „Schlange" δ.



Beweis. Definiere zunächst

$$\delta : c \longmapsto \left[f'^{-1}\beta g^{-1}\right].$$

Dabei bedeutet $g^{-1}(c)$, dass ein Urbild von c unter g gewählt wird. Dies ist möglich wegen der Surjektivität von g. Dass auch das Urbild von $\beta g^{-1}(c)$ unter f existiert, und zwar eindeutig, weil f injektiv ist, folgt wegen $g'\beta g^{-1}(c) = \gamma(c) = 0$ mit der Exaktheit der unteren Zeile.

Da wir bei der Wahl des Urbildes von c eventuell mehrere Möglichkeiten haben, bleibt die Wohldefiniertheit von δ zu zeigen, also die Unabhängigkeit von der Wahl der Repräsentanten in der Definition. Seien dazu b und $\tilde{b}$ Urbilder von c unter g, somit $g(b - \tilde{b}) = 0$. Dann existiert ein a mit $f(a) = b - \tilde{b}$. Also $f'\alpha(a) = \beta(b - \tilde{b})$, daher unterscheiden sich $f'^{-1}\beta b$ und $f'^{-1}\beta\tilde{b}$ um ein Element aus dem Bild von α, im Kokern ergeben also beide Terme das gleiche Bild δc.

Dass δ R-linear ist, sieht man schnell bei geschickter Urbildwahl. Für $s, t \in R$ gilt:

$$\delta(sc + t\tilde{c}) = \left[f'^{-1}\beta\left(sg^{-1}(c) + tg^{-1}(\tilde{c})\right)\right] = s\delta(c) + t\delta(\tilde{c}).$$

Nun bleibt die Exaktheit der Sequenz an vier Stellen zu prüfen. Die Aussagen zu den Implikationen der Injektivität von f und der Surjektivität von g' sind klar. Wir zeigen hier die Exaktheit an zwei Stellen. Der Rest des Beweises funktioniert ähnlich und wird nicht dadurch klarer, dass man ihn sich von jemand anders vormachen lässt.

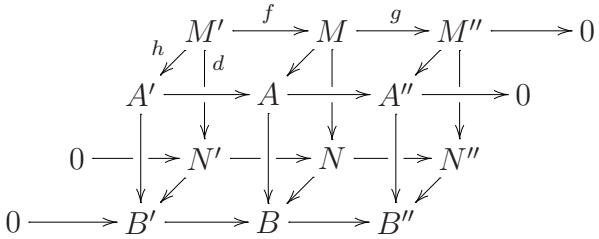
Exaktheit in $\ker(\beta)$: Es ist $g_K f_K = 0$ wegen $gf = 0$. Bleibt also $\ker(g_K) \subset \operatorname{im}(f_K)$: Sei $g(b) = 0, \beta(b) = 0$. Es gibt also $a \in A$ mit $f(a) = b$ wegen der Exaktheit der oberen

Zeile. Dieses a ist schon unser gesuchtes Urbild, da es wegen $f'\alpha(a) = \beta(b) = 0$ und der Injektivität von f' bereits im Kern von α liegt.

Exaktheit in $\ker(\gamma)$: Wir zeigen zunächst $\delta g_K = 0$. Sei $g(b) = c$ für $b \in \ker(\beta)$. Zur Berechnung von $\delta(c)$ kann man b als das Urbild von c unter g betrachten, mit dessen Hilfe δ bestimmt wird. Also gilt $\delta(c) = [f'^{-1}\beta b] = 0$.

Wir zeigen nun $\ker(\delta) \subset \mathrm{im}(g_K)$. Sei $\delta(c) = 0$ und b irgendein Urbild von c unter g. Wir wissen nicht, ob b in $\ker(\beta)$ liegt und suchen daher einen Korrekturterm. Es gibt wegen $\delta(c) = 0$ ein $a \in A$, so dass $f'^{-1}\beta(b) = \alpha(a)$. Setze $\tilde{b} = f(a)$. Dann folgt mit $f'\alpha(a) = \beta(b)$, dass $\beta(b - \tilde{b}) = \beta(b) - f'\alpha(a) = 0$ und $g(b - \tilde{b}) = g(b) - gf(a) = g(b)$. Dmit ist $b - \tilde{b}$ das gesuchte Urbild. □

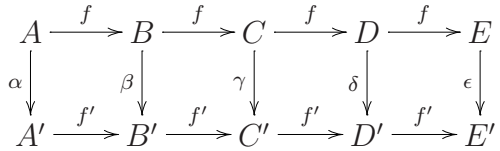
Lemma 6.2 (zwei Schlangendiagramme)**.** *Betrachte zwei Schlangendiagramme, die wie folgt in einer vorderen und hinteren Ebene angeordnet sind, so dass folgendes Diagramm kommutiert.*



Dabei leisten wir uns den Noationsmißbrauch und bezeichnen parallele Pfeile jeweils gleich, nur die waagerechten heißen links f und rechts g. Dann gilt $h_*\delta = \delta h_K$.

Beweis. Sei $m'' \in M''$, $d(m'') = 0$. Sei m ein Urbild von m'' unter g und $a = h(m)$. Nun ist $g(a) = hg(m) = h(m'')$. Also ist a ein Urbild von $h_K(m'')$, welches wir für die Bestimmung von $\delta h_K(m'')$ benutzen. Es ist $d(a) = hd(m) = fhf^{-1}d(m)$. Damit folgt $\delta h_K(m'') = [f^{-1}d(a)] = [hf^{-1}d(m)] = h_*\delta(m'')$. □

Lemma 6.3 (5er-Lemma)**.** *Das folgende kommutative Diagramm habe exakte Zeilen. Sind α, β, δ und ϵ Isomorphismen, so auch γ.*



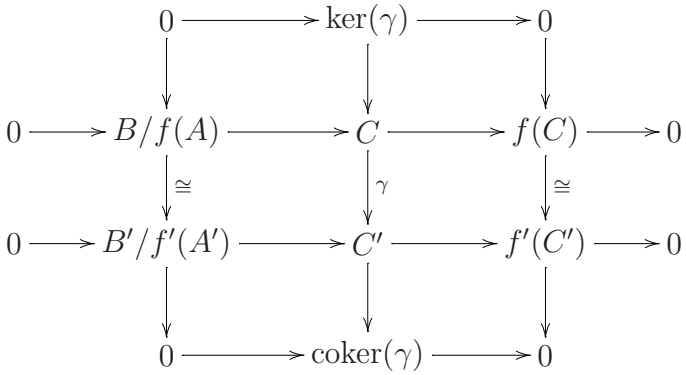
Genauer gilt:

(1) Ist α surjektiv und sind β und δ injektiv, so ist γ injektiv.

(2) Ist ϵ injektiv und sind β und δ surjektiv, so ist γ surjektiv.

Beweis. Die genaueren Behauptungen zeigt man am besten per Diagrammjagd. Den Fall, dass α, β, δ und ϵ Isomorphismen sind, beweist man mit folgendem Diagramm. In der linken bzw. rechten Spalte stehen jeweils die von β bzw. δ induzierten Abbildungen, welche Isomorphismen sind. In der oberen bzw. unteren Zeile stehen die Kerne bzw. Kokerne. Das

Diagramm ist kommutativ und da die beiden mittleren Zeilen exakt sind, folgt mit dem Schlangenlemma die Exaktheit der obersten und untersten Zeile, also die Behauptung.



□

6.2 Homologie

Satz–Definition 6.4 (δ-Morphismus der Homologie)**.** *Sei* $0 \to A^\bullet \xrightarrow{f} B^\bullet \xrightarrow{g} C^\bullet \to 0$ *eine kurze exakte Sequenz von Kokettenkomplexen. Dann gibt es natürliche Abbildungen, die* **Verbindungshomomorphismen**

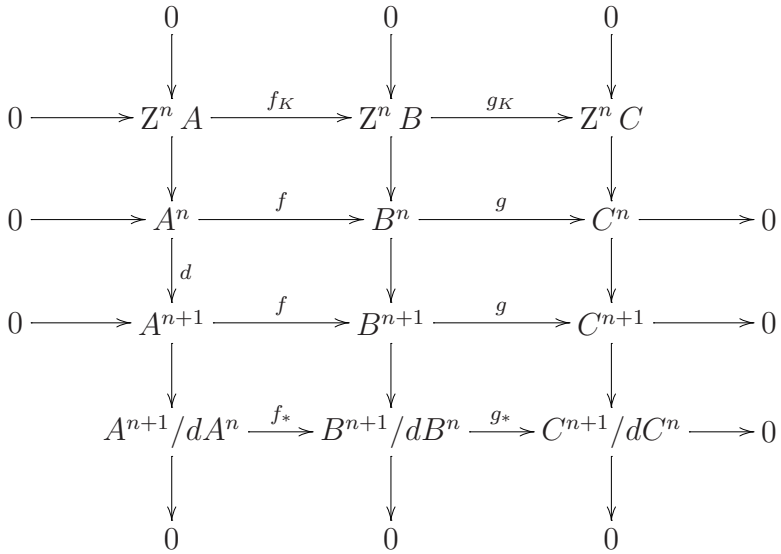
$$\delta^n : \mathrm{H}^n(C^\bullet) \to \mathrm{H}^{n+1}(A^\bullet),$$

so dass

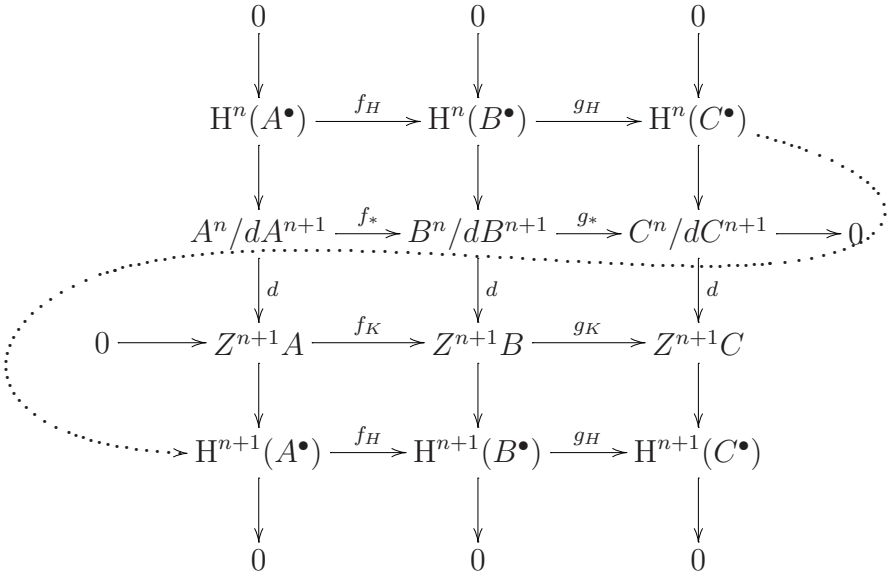
$$\cdots \xrightarrow{g} \mathrm{H}^{n-1}(C^\bullet) \xrightarrow{\delta} \mathrm{H}^n(A^\bullet) \xrightarrow{f} \mathrm{H}^n(B^\bullet) \xrightarrow{g} \mathrm{H}^n(C^\bullet) \xrightarrow{\delta} \mathrm{H}^{n+1}(A^\bullet) \xrightarrow{f} \cdots$$

eine exakte Sequenz von Moduln ist. Dies ist die zugehörige **lange exakte Sequenz***.*

Beweis. Betrachte zunächst folgendes Diagramm mit exakten Zeilen und Spalten, darin sind Z^n Zykel und d Differentiale.



Kombiniert man nun die untere Kokern-Zeile eines solchen Diagramms mit der oberen Kern-Zeile in passenden Graden, ergibt sich das folgende Diagramm. Die Abbildungen mit Index H sind die induzierten Abbildungen in der Homologie, die anderen die vom oberen Diagramm:



Das Schlangenlemma definiert $\delta^n : [c] \mapsto [f^{-1}dg^{-1}c]$ und liefert uns die exakte Sequenz

$$\mathrm{H}^n(A^\bullet) \longrightarrow \mathrm{H}^n(B^\bullet) \longrightarrow \mathrm{H}^n(C^\bullet) \xrightarrow{\delta^n} \mathrm{H}^{n+1}(A^\bullet) \longrightarrow \mathrm{H}^{n+1}(B^\bullet) \longrightarrow \mathrm{H}^{n+1}(C^\bullet).$$

Das Zusammensetzen dieser in den einzelnen Graden entstehenden exakten Sequenzen liefert die gewünschte lange exakte Sequenz. □

Sei $\mathscr{S}$ die Kategorie der kurzen exakte Sequenzen von Kokettenkomplexen von Moduln. Ein Morphismus sei ein Tripel von Kettenabbildungen, so dass folgendes Diagramm von Komplexen kommutiert.

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

Sei $\mathscr{L}$ die Kategorie der langen exakten Sequenzen von Moduln. Ein Morphismus sei eine Kettenabbildung zwischen zwei Sequenzen.

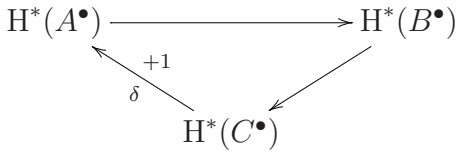
Proposition 6.5. *Die lange exakte Sequenz aus Satz 6.4 definiert einen Funktor $\mathscr{S} \to \mathscr{L}$.*

Beweis. Dass jedem Objekt aus $\mathscr{S}$ eines aus $\mathscr{L}$ zugeordnet wird, ist klar. Die Eigenschaft, dass ein Morphismus in einen Morphismus überführt wird, bedeutet die Kommutativität des folgenden Diagrammes.

$$\begin{array}{ccccccccccccc} \cdots & \longrightarrow & \mathrm{H}^{n-1}(C^\bullet) & \xrightarrow{\delta} & \mathrm{H}^n(A^\bullet) & \xrightarrow{f} & \mathrm{H}^n(B^\bullet) & \xrightarrow{g} & \mathrm{H}^n(C^\bullet) & \xrightarrow{\delta} & \mathrm{H}^{n+1}(A^\bullet) & \xrightarrow{f} & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & \mathrm{H}^{n-1}(C'^\bullet) & \xrightarrow{\delta} & \mathrm{H}^n(A'^\bullet) & \xrightarrow{f} & \mathrm{H}^n(B'^\bullet) & \xrightarrow{g} & \mathrm{H}^n(C'^\bullet) & \xrightarrow{\delta} & \mathrm{H}^{n+1}(A'^\bullet) & \xrightarrow{f} & \cdots \end{array}$$

Die Quadrate mit den δ's kommutieren wegen der Bermerkung zum Schlangenlemma. Die anderen kommutieren, weil H^n ein Funktor ist. Auch die Verträglichkeit von mit Verknüpfung und Identität folgt daraus. □

Bemerkung 6.6. Man prägt sich diese lange exakte Sequenz gern mit dem "exakten Dreieck" ein. Das Symbol +1 bedeutet, dass dort der Grad um 1 erhöht wird.



6.3 Der Begriff des δ-Funktors

Ab jetzt seien $\mathscr{A}$ und $\mathscr{B}$ abelsche Kategorien.

Definition 6.7. Ein Funktor $G : \mathscr{A} \to \mathscr{B}$ heiße **additiv**, wenn für Morphismen f, g in $\mathcal{A}$ die Gleichung $G(f+g) = G(f) + G(g)$ gilt.

Definition 6.8. Ein **kohomologischer** (bzw. **homologischer**) **δ-Funktor** zwischen $\mathscr{A}$ und $\mathscr{B}$ ist eine Kollektion additiver Funktoren $T^n : \mathscr{A} \to \mathscr{B}$ (bzw. $T_n n : \mathscr{A} \to \mathscr{B}$) für $n \geq 0$ und Homomorphismen für jede kurze exakte Sequenz $0 \to A \to B \to C \to 0$ in $\mathscr{A}$

$$\delta^n : T^n(C) \longrightarrow T^{n+1}(A) \quad \big(\text{bzw.} \quad \delta_n : T_n(C) \longrightarrow T_{n-1}(A)\big),$$

so dass folgendes Bedingungen gelten:

(i) Zu jeder kurzen exakten Sequenz wie oben gibt es eine lange exakte Sequenz

$$0 \longrightarrow T^0(A) \longrightarrow \cdots \longrightarrow T^{n-1}(C) \xrightarrow{\delta^{n-1}} T^n(A) \longrightarrow T^n(B) \longrightarrow \cdots$$

$$\big(\text{bzw.} \quad \cdots \longrightarrow T_n(B) \longrightarrow T_n(C) \xrightarrow{\delta_n} T_{n-1}(A) \longrightarrow \cdots \longrightarrow T_0(C) \longrightarrow 0\big).$$

(ii) Für jeden Morphismus von kurzen exakten Sequenzen

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

kommutiert das Diagramm

$$\begin{array}{ccc} T^n(C) & \xrightarrow{\delta} & T^{n+1}(A) \\ \downarrow & & \downarrow \\ T^n(C') & \xrightarrow{\delta} & T^{n+1}(A') \end{array} \quad \text{bzw.} \quad \begin{array}{ccc} T_n(C) & \xrightarrow{\delta} & T_{n-1}(A) \\ \downarrow & & \downarrow \\ T_n(C') & \xrightarrow{\delta} & T_{n-1}(A'). \end{array}$$

Eigenschaft (ii) besagt, dass δ eine natürliche Transformation ist zwischen dem Funktor, der aus der obigen exakten Sequenz $T^n(C)$ bildet, und dem, der $T^{n+1}(A)$ bildet (bzw. aus der obigen Sequenz $T_n(C)$ und $T_{n-1}(A)$).

Ein Beispiel für einen kohomologischen δ-Funktor von der Kategorie der Kokettenkomplexe von R-Moduln in nicht-negativem Grad in die Kategorie der R-Moduln ist das Bilden der Homologie, siehe Satz 6.4 und Proposition 6.5. Mit Hilfe dieses Beispiels reichern wir die Gruppenkohomologie aus Vortrag 4 zu einem kohomologischen δ-Funktor an.

6.4 Kohomologie von Gruppen

Sei $\cdots \longrightarrow P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$ eine projektive Auflösung des trivialen G-Moduls $\mathbb{Z}$. Ein G-Modulhomomorphismus $f : A \to B$ induziert einen Morphismus zwischen den Koketten

$$f\circ : \mathrm{Hom}_G(P_n, A) \longrightarrow \mathrm{Hom}_G(P_n, B), \quad \varphi \mapsto f \circ \varphi,$$

denn das Diagramm

$$\begin{array}{ccc} \mathrm{Hom}_G(P_n, A) & \xrightarrow{f\circ} & \mathrm{Hom}_G(P_n, B) \\ \downarrow{\scriptstyle d^n=(\circ d^n)} & & \downarrow{\scriptstyle d^n} \\ \mathrm{Hom}_G(P_{n+1}, A) & \xrightarrow{f\circ} & \mathrm{Hom}_G(P_{n+1}, B) \end{array}$$

kommutiert wegen $((f\circ)d^n)(\varphi) = f \circ \varphi \circ d^n = (d^n(f\circ))(\varphi)$.

Der Funktor $\mathrm{H}^n(G, -)$ ist additiver kovariant, weil er Komposition von zwei additiven kovarianten Funktoren ist: ein Morphismus $f : A \to B$ von G-Moduln wird mittels des Funktors $\mathrm{Hom}(P_*, -)$ abgebildet auf einen Morphismus $f\circ : \mathrm{Hom}(P_*, A) \to \mathrm{Hom}(P_*, B)$ in der Kategorie der Kokettenkomplexe über abelschen Gruppen und dieser dann mittels Homologie H^n auf einen Morphismus $\mathrm{H}^n(G, A) \to \mathrm{H}^n(G, B)$ in der Kategorie der abelschen Gruppen.

Sei $0 \to A \to B \to C \to 0$ eine kurze exakte Sequenz von G-Moduln. Dann ist

$$0 \longrightarrow \mathrm{Hom}(P_\bullet, A) \longrightarrow \mathrm{Hom}(P_\bullet, B) \longrightarrow \mathrm{Hom}(P_\bullet, C) \longrightarrow 0$$

eine kurze exakte Sequenz von Kokettenkomplexen, denn $\mathrm{Hom}(P^n, -)$ linksexakt, und speziell hier sogar exakt, weil alle P_n projektiv sind. Dies ist die entscheidende Stelle, wo eingeht, dass wir Gruppenkohomologie über eine projektive und nicht irgendeine Auflösung definiert haben.

Nach obiger Betrachtung zur langen exakten Sequenz der Homologie gibt es nun

$$\delta^n : \mathrm{H}^n(G, C) \longrightarrow \mathrm{H}^{n+1}(G, A),$$

so dass $(\mathrm{H}^*(G, -), \delta^*)$ ein kohomologischer δ-Funktor auf den G-Moduln mit Werten in den abelschen Gruppen ist. Die induzierte lange exakte Sequenz sieht wie folgt aus:

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} \mathrm{H}^1(G, A) \longrightarrow \mathrm{H}^1(G, B) \longrightarrow \mathrm{H}^1(G, C) \xrightarrow{\delta} \mathrm{H}^2(G, A) \longrightarrow \ldots$$

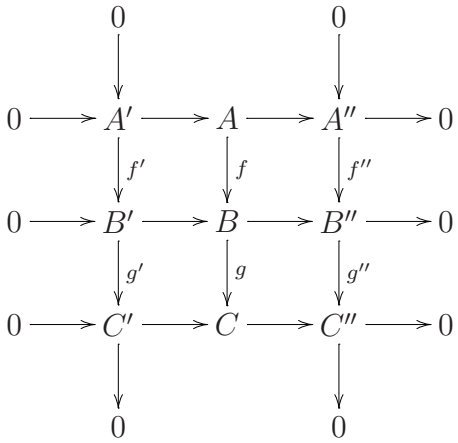
Vortrag 7

Homologische Algebra IV: Derivierte Funktoren

Katja Hutschenreuter, Michael Rieß
6.12.2005

7.1 Vorbereitung

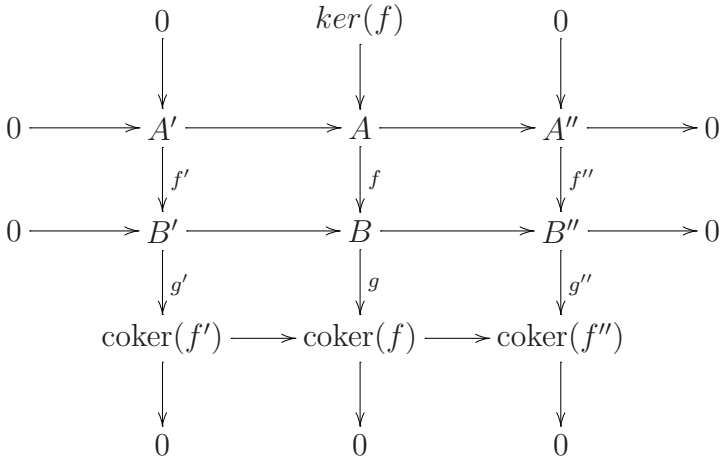
Lemma 7.1 (3×3-Lemma)**.** *Sei ein kommutatives Diagramm von R-Moduln gegeben, so dass alle Reihen und die mittlere Zeile exakt sind:*



Dann gilt: Die obere Zeile ist exakt und g ist surjektiv genau dann, wenn die untere Zeile exakt und f injektiv ist.

Bemerkung 7.2. Normalerweise wird beim 3×3-Lemma bereits vorausgesetzt, dass f injektiv und g surjektiv ist.

Beweis. Zum Beweis benutzen wir das Schlangenlemma aus Vortrag 6. Sei zunächst g surjektiv und die obere Zeile des Diagramms exakt. Dann erhalten wir das folgende Diagramm:



Da g', g und g'' surjektiv sind, gilt: $C' = \operatorname{coker}(f')$, $C = \operatorname{coker}(f)$ und $C'' = \operatorname{coker}(f'')$. Da die zwei oberen Zeilen exakt sind, gilt mit Hilfe des Schlangenlemmas, dass die Sequenz

$$0 \longrightarrow \ker(f) \longrightarrow 0 \xrightarrow{\delta} \operatorname{coker}(f') \longrightarrow \operatorname{coker}(f) \longrightarrow \operatorname{coker}(f'') \longrightarrow 0$$

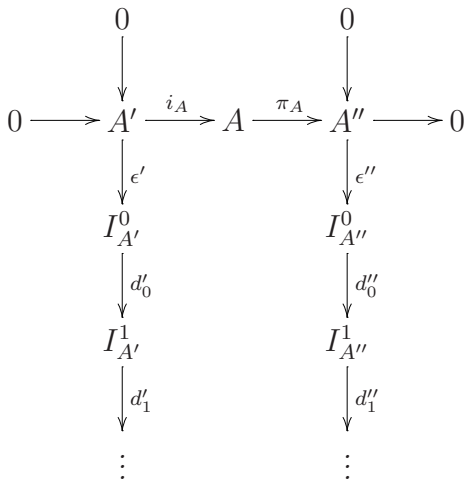
exakt ist. Deshalb ist f injektiv und die untere Zeile des Diagramms aus dem 3×3-Lemma ist exakt.

Die ander Richtung beweist man analog: Da f', f, und f'' injektiv sind, gilt mit Hilfe des Schlangenlemmas, dass die Sequenz

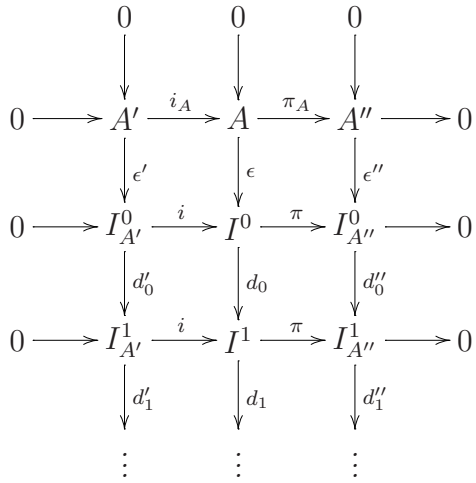
$$0 \longrightarrow \ker(f') \longrightarrow \ker(f) \longrightarrow \ker(f'') \xrightarrow{\delta} 0 \longrightarrow \operatorname{coker}(g) \longrightarrow 0$$

exakt ist. Daher ist g surjektiv und die obere Zeile des Diagramms exakt. □

Lemma 7.3 (Hufeisenlemma)**.** *Sei eine kurze exakte Sequenz zusammen mit injiektiven Auflösungen $A' \to I^\bullet_{A'}$ und $A'' \to I^\bullet_{A''}$ der äußeren Terme gegeben:*



Dann gibt es eine ijektive Auflösung $A \to I^\bullet_A$ mit $I^n := I^n_{A'} \oplus I^n_{A''}$, und das so aufgefüllte Diagramm kommutiert:



wobei i die jeweilige Inklusion und π die jeweilige Projektion ist.

Beweis. Es ist klar, dass die Sequenzen

$$0 \longrightarrow I^n_{A'} \xrightarrow{i} I^n_A = I^n_{A'} \oplus I^n_{A''} \xrightarrow{\pi} I^n_{A''} \longrightarrow 0$$

exakt sind und dass die I^n injektive Moduln sind, da eine direkte Summe von injektiven Moduln wieder injektiv ist. Damit das Diagramm kommutiert und

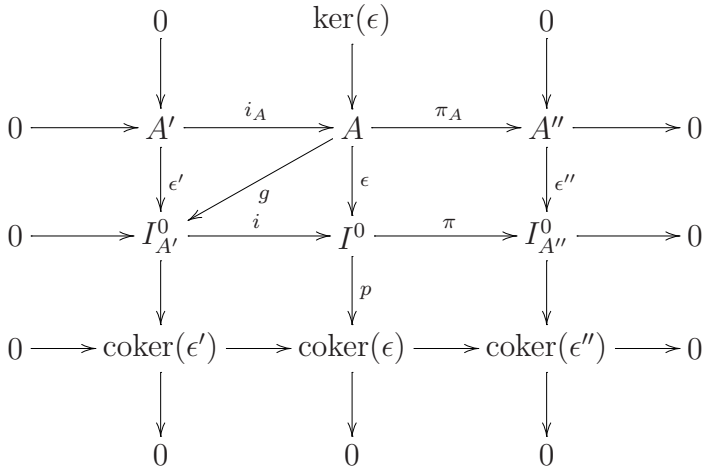
$$0 \longrightarrow A \xrightarrow{\epsilon} I^0 \xrightarrow{d_0} I^1 \xrightarrow{d_1} \dots$$

eine Auflösung ist, werden wir die Abbildungen ϵ, d_0, d_1, ... entsprechend konstruieren.

Da $I^0_{A'}$ ein injektives Modul ist, gibt es eine Abbildung $g : A \to I^0_{A''}$ mit $g \circ i_A = \epsilon'$. Wir betonen, dass diese Abbildung ist i.A. nicht eindeutig bestimmt ist. Mit Hilfe dieser Abbildung definieren wir

$$\epsilon := (g, \epsilon'' \circ \pi_A) : A \longrightarrow I^0 = I^0_{A'} \oplus I^0_{A''}.$$

Es gilt: $\pi \circ \epsilon = \epsilon'' \circ \pi_A$ und $\epsilon \circ i_A = (g \circ i_A, \epsilon'' \circ \pi_A \circ i_A) = (\epsilon', 0) = i \circ \epsilon'$. Man erhält also das folgende kummutierende Diagramm, in dem alle Spalten und die beiden oberen Zeilen exakt sind:



Also gilt nach dem 3×3-Lemma, dass die untere Zeile exakt ist, und dass die Abbildung ϵ injektiv ist. Wir erhalten danach das folgende Diagramm:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & \operatorname{coker}\epsilon' & \longrightarrow & \operatorname{coker}\epsilon & \longrightarrow & \operatorname{coker}\epsilon'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle D_0'} & & & & \downarrow{\scriptstyle D_0''} & & \\ & & I^1_{A'} & & & & I^1_{A''} & & \end{array}$$

Hier sind die Abbildungen D_0' und D_0'' von den Abbildungen $d_0' : I^0_{A'} \to I^1_{A'}$ und $d_0'' : I^0_{A''} \to I^1_{A''}$ induziert. Diese zwei Abbildungen sind wohldefiniert und injektiv, da $\operatorname{im}(\epsilon') = \ker(d_0')$ und $\operatorname{im}(\epsilon'') = \ker(d_0'')$ gilt. Dies ist genau die Situation, die wir anfangs hatten.

Man erhält also wieder eine injektive Abbildung $D_0 : \operatorname{coker}\epsilon \to I^1$. Die Abbildung $d_0 := D_0 \circ p : I^0 \to I^1$ hat den Kern $\ker(d_0) = \ker(p) = \operatorname{im}(\epsilon)$, da D_0 injektiv ist. Durch Induktion füllen wir nun das gesamte Hufeisen und erhalten, dass

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

exakt ist. □

7.2 Rechtsderivierte Funktoren

Es sei nun $F : \mathscr{A} \to \mathscr{B}$ ein linksexakter additiver Funktor auf und mit Werten in Kategorien von Moduln $\mathscr{A}, \mathscr{B}$. Die folgenden Ergebnisse gelten auch allgemein für abelsche Kategorien. Die Beweise sind jedoch manchmal anders.

Nun *fixieren* wir für jeden Modul $A \in \mathscr{A}$ eine injektive Auflösung $A \to I^\bullet_A$. Dies ist möglich, da die Kategorie der Moduln über einem Ring genügend viele Injektive hat. Wenn wir darauf den Funktor F anwenden, erhalten wir den Komplex

$$0 \longrightarrow F\left(I^0_A\right) \xrightarrow{F(d_0)} F\left(I^1_A\right) \xrightarrow{F(d_1)} F\left(I^2_A\right) \longrightarrow \dots$$

der im allgemeinen nicht exakt ist. Die „Abweichung“ von der Exaktheit wollen wir durch die Kohomolgiegruppen $\mathrm{H}^i(F(I^\bullet_A))$ messen. Wir definieren den **rechtsderivierten Funktor** von F durch:

$$\mathrm{R}^i F(A) := \mathrm{H}^i(F(I_A)).$$

Bemerkung 7.4. Es gilt natürlich $\mathrm{R}^0 F(A) \cong F(A)$, denn die Sequenz

$$0 \to F(A) \xrightarrow{F(\epsilon)} F\left(I^0_A\right) \longrightarrow F(d_0) \longrightarrow F\left(I^1_A\right)$$

ist exakt, da F linksexakt ist. Deshalb gilt

$$\mathrm{R}^0 F(A) = \mathrm{H}^0(F(I^\bullet_A)) = \ker(F(d_0)) \cong \operatorname{im}(F(\epsilon)) \cong F(A).$$

Nun haben wir zwar den rechtsderivierten Funktor $R^i F(A)$ definiert, aber wir wissen nicht, ob dieser überhaupt ein Funktor ist und ob er von der injektiven Auflösung $A \to I$ unabhängig ist, wie dies von der Schreibweise suggeriert wird. Die folgenden Lemmata werden diese Fragen beantworten.

Lemma 7.5. *Sei $g : A \to B$ ein Modulhomomorphismus. Dann existiert eine kanonische Abbildung $\mathrm{R}^i F(g) : \mathrm{R}^i F(A) \to \mathrm{R}^i F(B)$. Diese bezeichnen wir auch kurz mit $g_\star$.*

Beweis. Aus dem Vortrag 3 wissen wir, dass es eine Fortsetzung $\tilde{g} : I_A^\bullet \to I_B^\bullet$ der Abbildung $g : A \to B$ gibt und dass diese eindeutig bis auf Homotopie bestimmt ist. Also ist $F(g) : F(I_A^\bullet) \to F(I_B^\bullet)$ ein Morphismus von Kettenkomplexen, der ebenfalls bis auf Homotopie eindeutig bestimmt ist, da der Funktor F additiv ist:

$$F(g_1) - F(g_2) = F(g_1 - g_2) = F(dh + hd) = d(F(h)) + F(h)d.$$

Deshalb ist die Abbildung $\mathrm{R}^i F(g) := \mathrm{H}^i(F(g)) : \mathrm{R}^i F(A) \to \mathrm{R}^i F(B)$ unabhängig von der gewählten Fortsetzung. □

Lemma 7.6. *Falls $A \to J^\bullet$ eine weitere injektive Auflösung ist, dann existiert ein kanonischer Isomorphismus*

$$\varphi_A : \mathrm{R}^i F(A) = \mathrm{H}^i(F(I_A^\bullet)) \longrightarrow \mathrm{H}^i(F(J^\bullet)).$$

Mt andern Worten $\mathrm{R}^* F(A)$ ist unabhängig bis auf kanonischen Isomorphismus von der Wahl der injektiven Auflösung.

Beweis. Seien $\tilde{f}$ und $\tilde{g}$ Fortsetzungen von id_A:

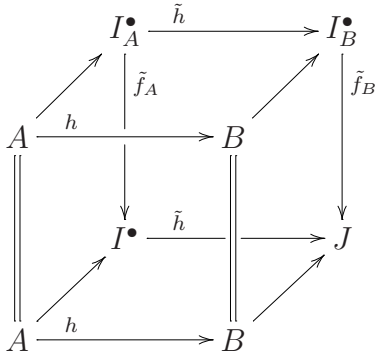
$$\begin{array}{ccccc} A & \xrightarrow{\mathrm{id}} & A & \xrightarrow{\mathrm{id}} & A \\ \downarrow & & \downarrow & & \downarrow \\ I_A^\bullet & \xrightarrow{\tilde{f}} & J^\bullet & \xrightarrow{\tilde{g}} & I_A^\bullet \end{array}$$

Also sind $\tilde{g} \circ \tilde{f}$ und $\mathrm{id}_{I_A^\bullet}$ Fortsetzung von id_A. Da H^i und F Funktoren sind, gilt also:

$$g_\star \circ f_\star = \mathrm{H}^i(F(\tilde{g})) \circ \mathrm{H}^i(F(\tilde{f})) = \mathrm{H}^i(F(\tilde{g} \circ \tilde{f})) = \mathrm{H}^i(F(\mathrm{id})) = \mathrm{id}\,.$$

Analog gilt: $f_\star \circ g_\star = \mathrm{id}$. Also ist $\varphi_A := f_\star : \mathrm{R}^i F(A) \to \mathrm{H}^i(F(J))$ ein Isomorphismus.

Die Abbildung φ_A ist natürlich: Sind $A \to I_A^\bullet$, $A \to I^\bullet$, $B \to I_B^\bullet$, $B \to J^\bullet$ injektive Auflösungen und $h : A \to B$ eine Abbildung mit Fortsetzungen $\tilde{h}$, $\tilde{f}_A$, $\tilde{f}_B$ von h, id_A und id_B, siehe folgendes nicht notwendig kommutative Diagramm



Es sind $\tilde{h} \circ \tilde{f}_A$ und $\tilde{f}_B \circ \tilde{h}$ Fortsetzungen von h und somit gilt

$$h_\star \circ \varphi_A = \mathrm{H}^i(F(\tilde{h})) \circ \mathrm{H}^i(F(\tilde{f}_A)) = \mathrm{H}^i(F(\tilde{h} \circ \tilde{f}_A)) = \mathrm{H}^i(F(\tilde{f}_B \circ \tilde{h})) = \varphi_B \circ h_\star.$$

□

Lemma 7.7. $\mathrm{R}^i F$ *ist ein additiver Funktor.*

Beweis. $\mathrm{R}^i F$ ist ein Funktor, da H^i und F Funktoren sind, und außerdem die Identität id fortsetzt und die Komposition von Fortsetzungen eine Fortsetzung der Komposition liefert. Der Funktor F ist additiv, da die Funktoren H^i und F additiv sind und für zwei Abbildungen $g,\ f : A \to B$ mit den Fortsetzungen $\tilde{g}$ und $\tilde{f}$ ist die Summe $\tilde{g} + \tilde{f}$ eine Fortsetzung von $g + f$ liefert. □

Theorem 7.8. *Die dervierten Funktoren* $\mathrm{R}^* F$ *tragen die Struktur eines kohomologischen* δ*-Funktors.*

Beweis. Teil 1: konstruktion von δ und der langen exakten Sequenz
Zuerst zeigen wir, dass es zu jeder kurzen exakten Sequenz $0 \to A' \to A \to A'' \to 0$ eine Abbildung $\delta : \mathrm{R}^\star F(A'') \to \mathrm{R}^{\star+1} F(A')$ gibt, so dass

$$\ldots \longrightarrow \mathrm{R}^n F(A') \longrightarrow \mathrm{R}^n F(A) \longrightarrow \mathrm{R}^n F(A'') \xrightarrow{\delta} \mathrm{R}^{n+1} F(A') \longrightarrow \ldots$$

eine lange exakte Sequenz ist. Durch das Hufeisenlemma wissen wir, dass wir die kurze exakte Sequenz $0 \to A' \to A \to A'' \to 0$ zu dem kommutierenden Diagramm

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A' & \xrightarrow{i_A} & A & \xrightarrow{\pi_A} & A'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \epsilon'} & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \epsilon''} & & \\
0 & \longrightarrow & I^0_{A'} & \xrightarrow{i} & I^0 & \xrightarrow{\pi} & I^0_{A''} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_0} & & \downarrow{\scriptstyle d_0} & & \downarrow{\scriptstyle d''_0} & & \\
0 & \longrightarrow & I^1_{A'} & \xrightarrow{i} & I^1 & \xrightarrow{\pi} & I^1_{A''} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'_1} & & \downarrow{\scriptstyle d_1} & & \downarrow{\scriptstyle d''_1} & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

fortsetzen können, wobei $I^n = I^n_{A'} \oplus I^n_{A''}$ ist und die i (bzw. π) die jeweiligen Inklusionen (bzw. Projektionen) sind. Wir wählen Spaltungen $s : I^n_{A''} \to I^n$ der kurzen exakten Zeilen. Da der Funktor F linksexakt ist, ist die Sequenz $0 \to F(I^n_{A'}) \to F(I^n) \overset{F(\pi)}{\to} F(I^n_{A''})$ exakt. Desweiteren ist $F(\pi)$ surjektiv, denn $F(\mathrm{id}) = F(\pi \circ s) = F(\pi) \circ F(s)$. Wir erhalten also eine kurzen exakte Sequenz von Kokettenkomplexen:

$$0 \longrightarrow F(I^\bullet_{A'}) \longrightarrow F(I^\bullet) \longrightarrow F(I^\bullet_{A''}) \longrightarrow 0.$$

Da H^i ein kohomologischer δ-Funktor ist erhalten wir die Abbildung δ und die folgende lange exakte Sequenz

$$\begin{array}{ccccccccccc}
\cdots \longrightarrow & \mathrm{H}^n(F(I^\bullet_{A''})) & \xrightarrow{\delta} & \mathrm{H}^{n+1}(F(I^\bullet_{A'})) & \xrightarrow{i_{A,*}} & \mathrm{H}^{n+1}(F(I^\bullet)) & \xrightarrow{\pi_{A,*}} & \mathrm{H}^{n+1}(F(I^\bullet_{A''})) & \longrightarrow \cdots \\
 & \| & & \| & \searrow^{i_{A,*}} & \uparrow{\scriptstyle \varphi_A}\ {\scriptstyle \simeq} & \nearrow_{\pi_{A,*}} & \| & \\
 & \mathrm{R}^n F(A'') & & \mathrm{R}^{n+1} F(A') & & \mathrm{R}^{n+1} F(A) & & \mathrm{R}^{n+1} F(A'') &
\end{array}$$

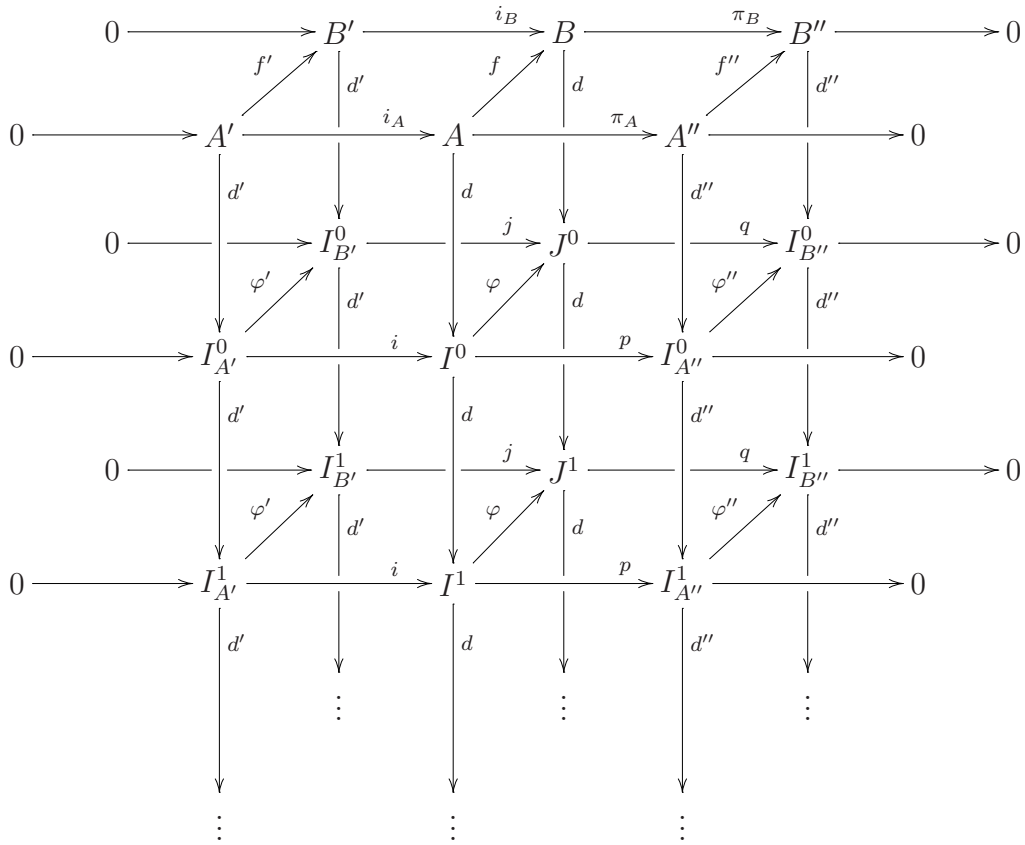
Nach dem Lemma 1.6. wissen wir, dass φ_A ein natürlicher Isomorphismus ist, d.h. dass das obige Diagramm kommutiert. Wir erhalten also die folgende lange exakte Sequenz

$$\ldots \longrightarrow \mathrm{R}^n F(A') \longrightarrow \mathrm{R}^n F(A) \longrightarrow \mathrm{R}^n F(A'') \xrightarrow{\delta} \mathrm{R}^{n+1} F(A') \longrightarrow \ldots$$

Teil 2: Jetzt werden wir zeigen, dass δ mit den Morphismen von kurzen exakten Sequenzen verträglich ist, d.h. dass für jeden Morphismus von kurzen exakten Sequenzen

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

die Gleichung $\delta \circ \mathrm{R}\,F(f'') = \mathrm{R}\,F(f') \circ \delta$ gilt. Um dies zu zeigen, konstruieren wir die Fortsetzungen φ', φ und φ'' der Abbildungen f', f und f'', so dass das folgende Diagramm kommutiert.



Hierbei sind $A' \to I^\bullet_{A'}$, $B' \to I^\bullet_{B'}$, $A'' \to I^\bullet_{A''}$ und $B'' \to I^\bullet_{B''}$ injektive Auflösungen und das Diagramm wird wie im Hufeisenlemma mit injektiven Auflösungen von A bzw. B "gefüllt": die vorderen und die hinteren Ebene des Diagramms kommutieren jeweils für sich.

Seien nun $\hat{\varphi}$ und φ'' beliebige Fortsetzungen von f und f''. Dann gilt aber leider im allgemeinen nicht, dass $q \circ \hat{\varphi} = \varphi'' \circ p$. Aber $q \circ \hat{\varphi}$ und $\varphi'' \circ p$ sind homotop, da sie Fortsetzungen von $f'' \circ \pi_A = \pi_B \circ f$ sind. Also existieren Abbildungen $h''_n : I^n \to I^{n-1}_{B''}$ so dass

$$\varphi'' \circ p - q \circ \hat{\varphi} = d'' \circ h''_n + h''_{n+1} \circ d$$

gilt. Wir werden nun eine neue Fortsetzung φ von f defnieren, indem wir den Fehlerterm $d'' \circ h'' + h'' \circ d$ verwenden. Da die kurzen exakten Sequenzen

$$0 \longrightarrow I_B^n \longrightarrow J^n \xrightarrow{q} I_{B''}^n \longrightarrow 0$$

spalten, existieren Abbildungen $s_n : I_{B''}^n \to J^n$ mit $q \circ s = id$. Wir definieren

$$h_n := s_{n-1} \circ h_n'' : I^n \longrightarrow J^{n-1}$$

und

$$\varphi_n := \hat{\varphi}_n + d \circ h_n + h_{n+1} \circ d.$$

Die Abbildung φ ist eine Fortsetzung von f da

$$d\hat{\varphi} = d\varphi + d(dh_n + h_{n+1}d) = d\varphi + dh_{n+1}d = \varphi d + (dh_{n+1} + h_{n+2}d)d = \hat{\varphi}d,$$

und $\hat{\varphi}|_A = \varphi|_A + (dh_{-1} + h_0 d)|_A = \varphi|_A = f$. Weiterhin gilt $q \circ \varphi = \varphi'' \circ p$, da:

$$\begin{aligned} q \circ \varphi - \varphi'' \circ p &= q \circ (d \circ h + h \circ d + \hat{\varphi}) - \varphi'' \circ p \\ &= d'' \circ q \circ h + q \circ s \circ h'' \circ d + (q \circ \hat{\varphi} - \varphi'' \circ p) \\ &= d'' \circ q \circ s \circ h'' + h'' \circ d - (d'' \circ h'' + h'' \circ d) \\ &= d'' \circ h'' + h'' \circ d - (d'' \circ h'' + h'' \circ d) = 0. \end{aligned}$$

Also gilt unter anderem, dass die Abbildungen φ_n Homomorphismen $\varphi_n' : I_{A'}^n \to I_{B'}^n$ induzieren, da die Etagen des großen Diagramms exakte Zeilen haben. Damit gilt per Definitionin $\varphi' \circ i = j \circ \varphi$.

Um zu zeigen, dass in dem oberen Diagramm alle Seiten kommutieren, bleibt also nur noch zeigen, dass die linken Seiten kommutieren, also φ' eine Kettenabbildung ist, die f' fortsetzt. Das ist aber klar nach Definition und der entsprechenden Eigenschaft von φ.

Wir haben nun also Fortsetzungen φ', φ und φ'' von f', f und f'' gefunden, so dass das grosse Diagramm kommutiert. Da F ein Funktor ist und aus der Defintion der Abbildung δ, folgt: $\delta \circ \mathrm{R}^n F(f'') = \delta \circ \mathrm{H}^n(F(\varphi'')) = \mathrm{H}^n(F(\varphi')) \circ \delta = \mathrm{R}^n F(f') \circ \delta$ für alle $n \in \mathbb{N}$.

3. Teil: Wohldefiniertheit von δ Nun bleibt nur noch das kleine Problem, dass die Abbildung δ abhängig von den Abbildungen der injektiven Auflösung

$$0 \longrightarrow A \xrightarrow{\epsilon} I^0 \xrightarrow{d_0} I^1 \xrightarrow{d_1} \dots$$

sein könnte, da wir bei der Konstruktion dieser Abbildungen eventuell Wahlmöglichkeiten haben (siehe Beweis vom Hufeisenlemma und Defintion der Abbildung δ). Dies ist jedoch nicht der Fall, da für den Morphismus

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \end{array}$$

mit den das Hufeisenfüllenden injektiven Auflösungen $A \xrightarrow{\epsilon} I^\bullet$ und $A \xrightarrow{\epsilon'} I'^\bullet$ nach Teil 2 dieses Beweises $\delta' = \delta' \circ \mathrm{R}\,F(\mathrm{id}) = \mathrm{R}\,F(\mathrm{id}) \circ \delta = \delta$ gilt, wobei δ bzw. δ' jeweils bezüglich der entsprechend gestrichenen Auflösung von A konstruiert sein soll. □

Beispiel 7.9 (Der Funktor Ext^*_R). Für jedes $A \in R\text{-Mod}$ ist, wie wir gesehen haben, der Funktor

$$\begin{array}{rccc} R\text{-Mod}(A,-): & R\text{-Mod} & \longrightarrow & R\text{-Mod} \\ & B & \longmapsto & R\text{-Mod}(A,B) \end{array}$$

linksexakt. Man bezeichnet seine rechtsderivierten Funktoren mit:

$$\mathrm{Ext}^i_R(A,B) := R^i R\text{-Mod}(A,-)(B)$$

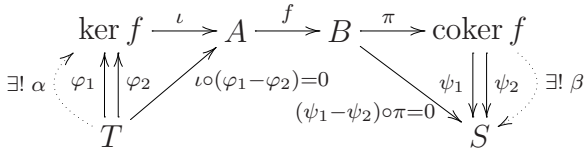
Also im Speziellen $\mathrm{Ext}^0_R(A,B) = R\text{-Mod}(A,B)$ in Grad 0.

7.3 Mehr über abelsche Kategorien

Die Ergebnisse des nächsten Abschnitts über Auslöschbarkeit und Universalität werden für allgemeine abelsche Kategorien behandelt, wofür es zunächst notwendig ist, einige allgemeine und elementfreie Fakten, die man für konkrete Fälle wie der Kategorie der Moduln schon kennt, zu formulieren. Ein nützliches Lemma ist das folgende.

Lemma 7.10. *Die Kernabbildung ist ein Monomorphismus und die Kokernabbildung ein Epimorphismus.*

Beweis. Betrachte das Diagramm:



Da $\iota \circ (\varphi_1 - \varphi_2) = 0$ gilt, folgt offensichtlich $f \circ \iota \circ (\varphi_1 - \varphi_2) = 0$. Also gibt es ein eindeutiges $\alpha : T \to \ker f$ mit $\iota \circ \alpha = \iota \circ (\varphi_1 - \varphi_2) = 0$. Wegen der Eindeutigkeit muss gelten $0 = \alpha = \varphi_1 - \varphi_2$.

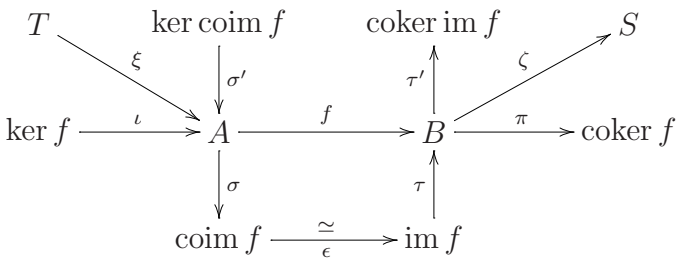
Da $(\psi_1 - \psi_2) \circ \pi = 0$ gilt, folgt offensichtlich $(\psi_1 - \psi_2) \circ \pi \circ f = 0$. Also gibt es ein eindeutiges $\beta : \mathrm{coker}\, f \to S$ mit $\beta \circ \pi = (\psi_1 - \psi_2) \circ \pi = 0$. Aus der Eindeutigkeit folgt dann $0 = \beta = \psi_1 - \psi_2$. □

Lemma 7.11. *Sei $f : A \to B$ ein Morphismus in $\mathscr{A}$. Dann gilt:*

(1) $\ker \mathrm{coim}\, f = \ker f$

(2) $\mathrm{coker}\, \mathrm{im}\, f = \mathrm{coker}\, f$

Beweis. Betrachten wir zunächst das Diagramm:



(1) Sei $\xi : T \to A$ mit $\sigma \circ \xi = 0$. Zu zeigen ist nun, dass es ein eindeutiges $\alpha : T \to \ker f$ mit $\iota \circ \alpha = \xi$ gibt, was die universelle Eigenschaft des Kerns beweist.

Nun ist aber $f \circ \xi = \tau \circ \epsilon \circ \sigma \circ \xi = \tau \circ \epsilon \circ 0 = 0$ und damit liefert die universelle Eigenschaft von $\ker f$ den gewünschten Morphismus.

(2) Sei $\zeta : B \to S$ mit $\zeta \circ \tau = 0$. Zu zeigen ist nun, dass es ein eindeutiges $\beta : \operatorname{coker} f \to S$ mit $\beta \circ \pi = \zeta$ gibt, was die universelle Eigenschaft des Kokerns beweist.

Es ist $\zeta \circ f = \zeta \circ \tau \circ \epsilon \circ \sigma = 0 \circ \epsilon \circ \sigma = 0$ und die universelle Eigenschaft von $\operatorname{coker} f$ garantiert den gesuchten Morphismus.

□

Definition 7.12. Seien $A, B, C \in \mathscr{A}$, $f \in \operatorname{Hom}_{\mathscr{A}}(A, B)$ und $g \in \operatorname{Hom}_{\mathscr{A}}(B, C)$. Die Sequenz

$$A \xrightarrow{f} B \xrightarrow{g} C$$

heißt **exakt** in B, wenn $\operatorname{im} f = \ker g$ gilt.

Lemma 7.13. *Sei $f : A \to B$ ein Morphismus in $\mathscr{A}$. Dann gilt:*

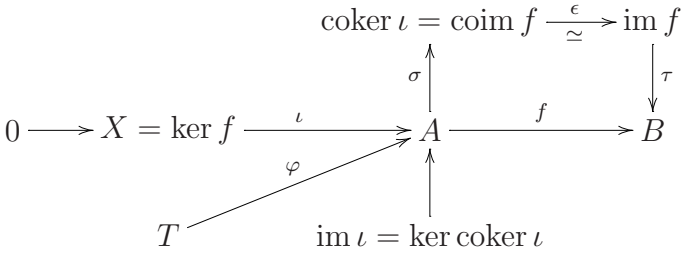
(1) $\iota : X \to A = \ker f \Leftrightarrow 0 \longrightarrow X \xrightarrow{\iota} A \xrightarrow{f} B$ *exakt in X und A.*

(2) $\pi : B \to X = \operatorname{coker} f \Leftrightarrow A \xrightarrow{f} B \xrightarrow{\pi} X \longrightarrow 0$ *exakt in B und X.*

Beweis. (1) Sei $\iota : X \to A = \ker f$, also nach dem vorangegangenen ein Monomorphismus. Zu zeigen ist nun:

(i) $\ker \iota = 0 \to X$
Es genügt zu zeigen, dass es für jedes $T \in \mathscr{A}$ nur einen eindeutigen Morphismus $\varphi : T \to X$ mit $\iota \circ \varphi = 0$. Dies wäre automatisch der Nullmorphismus.
Seien also $\varphi_1, \varphi_2 : T \to X$ mit $\iota \circ \varphi_1 = \iota \circ \varphi_2 = 0$. Dann folgt $\iota \circ (\varphi_1 - \varphi_2) = 0 \Rightarrow \varphi_1 - \varphi_2 = 0 \Rightarrow \varphi_1 = \varphi_2$.

(ii) $\ker f = \operatorname{im} \iota$
Zunächst wird festgestellt, dass $\operatorname{coim} f = \operatorname{coker} \ker f = \operatorname{coker} \iota$ gilt. Betrachte nun das folgende Diagramm:



Ist also $\varphi : T \to A$ mit $\sigma \circ \varphi = 0$, so ist auch $f \circ \varphi = \tau \circ \epsilon \circ \sigma \circ \varphi = \tau \circ \epsilon \circ 0 = 0$ und damit liefert die universelle Eigenschaft von $\ker f$ das gewünschte.

Sei nun andererseits $0 \longrightarrow X \xrightarrow{\iota} A \xrightarrow{f} B$ exakt. Es ist $\operatorname{coker}(0 \to X) = X \xrightarrow{\mathrm{id}} X$ und damit

$$\operatorname{im}(0 \to X) = \ker \operatorname{coker}(0 \to X) = \ker\left(X \xrightarrow{\mathrm{id}} X\right) = 0 \to X.$$

Wegen Exaktheit ist $\operatorname{im}(0 \to X) = \ker \iota$ und

$$\operatorname{coim} \iota = \operatorname{coker} \ker \iota = \operatorname{coker} \operatorname{im}(0 \to X) = \operatorname{coker}(0 \to X) = X \xrightarrow{\mathrm{id}} X.$$

Betrachte also das Diagramm:

$$\begin{array}{ccccccc} & & X = \operatorname{coim} \iota & \xrightarrow[\epsilon]{\simeq} & \operatorname{im} \iota = \ker f & & \\ & & \uparrow{\scriptstyle \mathrm{id}} & & \downarrow & & \\ 0 & \longrightarrow & X & \xrightarrow{\iota} & A & \xrightarrow{f} & B \end{array}$$

Ist jetzt $\varphi : T \to A$ ein Morphismus mit $f \circ \varphi = 0$, so gibt es ein eindeutiges $\alpha : T \to \ker f$ und damit ein eindeutiges $\epsilon^{-1} \circ \alpha : T \to X$, das wegen der Kommutativität des Diagramms die gewünschten Eigenschaften hat.

(2) Sei $\pi : B \to X = \operatorname{coker} f$, also ein Epimorphismus. Zu zeigen ist nun:

(i) $\operatorname{im} \pi = X \xrightarrow{\mathrm{id}} X$
Es genügt zu zeigen, dass $\operatorname{coker} \pi = X \to 0$. Also, dass für alle $T \in \mathscr{A}$ und $\varphi : X \to T$ mit $\varphi \circ \pi = 0$ folgt $\varphi = 0$.
Seien also $\varphi_1, \varphi_2 : X \to T$ mit $\varphi_1 \circ \pi = \varphi_2 \circ \pi = 0$. Da π ein Epimorphismus ist, folgt $\varphi_1 = \varphi_2$ und, da der Nullmorphismus sicherlich die Voraussetzung an φ erfüllt, auch $\varphi_1 = \varphi_2 = 0$.

(ii) $\operatorname{im} f = \ker \operatorname{coker} f = \ker \pi$

Sei andererseits $A \xrightarrow{f} B \xrightarrow{\pi} X \longrightarrow 0$ exakt. Dann ist $\ker(X \to 0) = X \xrightarrow{\mathrm{id}} X = \operatorname{im} \pi$ wegen Exaktheit. Dies und $\operatorname{coim} \pi = \operatorname{coker} \ker \pi = \operatorname{coker} \operatorname{im} f = \operatorname{coker} f$ liefert das Diagramm:

$$\begin{array}{ccccccc} & & \operatorname{coim} \pi = \operatorname{coker} f & \xrightarrow[\epsilon]{\simeq} & X = \operatorname{im} \pi & & \\ & & \uparrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ A & \xrightarrow{f} & B & \xrightarrow{\pi} & X & \longrightarrow & 0 \end{array}$$

Sei jetzt $\varphi : B \to T$ mit $\varphi \circ f = 0$, dann gibt es ein eindeutiges $\alpha : \operatorname{coker} f \to T$ und damit ein eindeutiges $\alpha \circ \epsilon^{-1} : X \to T$.

□

Korollar 7.14. *Es wurde sogar gezeigt:*

$$\begin{aligned} X \xrightarrow{\iota} Y \text{ ist Monomorphismus} &\Leftrightarrow 0 \longrightarrow X \xrightarrow{\iota} Y \text{ exakt} \\ &\Leftrightarrow \exists\, \varphi : Y \to V \text{ mit } \iota = \ker \varphi \\ \text{Und analog: } X \xrightarrow{\pi} Y \text{ ist Epimorphismus} &\Leftrightarrow X \xrightarrow{\pi} Y \longrightarrow 0 \text{ exakt} \\ &\Leftrightarrow \exists \psi : W \to X \text{ mit } \pi = \operatorname{coker} \psi \end{aligned}$$

Beweis. Folgt direkt unter zusätzlicher Verwendung der Existenz von Kernen und Kokernen. □

7.4 Auslöschbarkeit und Universalität

Definition 7.15 (Morphismus von kohomologischen δ-Funktoren)**.** Seien T^*, S^* kohomologische δ-Funktoren. Ein **Morphismus $f^* : T^* \to S^*$ von kohomologischen δ-Funktoren** ist eine Kollektion von natürlichen Transformationen $f^i : T^i \to S^i$, $i \geq 0$, die mit δ kommutieren: für alle kurzen exakten Sequenzen $0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$ ist das folgende Diagramm kommutativ:

$$\begin{array}{ccccccccccc}
\cdots \longrightarrow & T^{i-1}(A'') & \xrightarrow{\delta_T} & T^i(A') & \longrightarrow & T^i(A) & \longrightarrow & T^i(A'') & \xrightarrow{\delta_T} & T^{i+1}(A') & \longrightarrow \cdots \\
& \downarrow{\scriptstyle f^{i-1}_{A''}} & & \downarrow{\scriptstyle f^i_{A'}} & & \downarrow{\scriptstyle f^i_A} & & \downarrow{\scriptstyle f^i_{A''}} & & \downarrow{\scriptstyle f^{i+1}_{A'}} & \\
\cdots \longrightarrow & S^{i-1}(A'') & \xrightarrow{\delta_S} & S^i(A') & \longrightarrow & S^i(A) & \longrightarrow & S^i(A'') & \xrightarrow{\delta_S} & S^{i+1}(A') & \longrightarrow \cdots
\end{array}$$

Definition 7.16 (universeller kohomologischer δ-Funktor)**.** Ein kohomologischer δ-Funktor T^* heißt **universell**, wenn für alle kohomologischen δ-Funktoren S^* und natürlichen Transformationen $f^0 : T^0 \to S^0$ eine eindeutige Fortsetzung $f : T^* \to S^*$ als Morphismus von kohomologischen δ-Funktoren existiert.

Die Konstruktion der rechtsderivierten Funktoren zu linksexakten Funktoren $F : \mathscr{A} \to \mathscr{B}$ aus den ersten Abschnitten dieses Vortrags läßt sich unmittelbar von Kategorien von Moduln auf abelsche Kategorien ausdehnen, sofern nur die Ausgangskategorie $\mathscr{A}$ genügend viele Injektive Objekte besitzt. Um nachzuweisen, dass die rechtsderivierten Funktoren zu einem linksexakten Funktor einen universellen δ-Funktor bilden, benötigen wir noch folgende Eigenschaft:

Definition 7.17 (auslöschbare Funktoren)**.** (1) Ein additiver Funktor $F : \mathscr{A} \to \mathscr{B}$ heißt **auslöschbar**, wenn es für jedes $A \in \mathscr{A}$ ein $I \in \mathscr{A}$ und einen Monomorphismus $\varphi : A \hookrightarrow I$ mit $F(\varphi) = 0$ gibt.

(2) Ein kohomologischer δ-Funktor F^* heißt **auslöschbar**, falls alle F^i für $i > 0$ auslöschbar sind.

Lemma 7.18. *Ist $I \in \mathscr{A}$ injektiv, so verschwinden für jeden linksexakten, additiven Funktor F die Rechtsderivierten in höheren Graden, also*

$$\mathrm{R}^i F(I) = 0, \quad i > 0$$

Beweis. Wir berechnen $\mathrm{R}^i F(I)$ für ein injektives $I \in \mathscr{A}$ vermöge der injektiven Auflösung $\mathrm{id} : I \to I^\bullet$ mit

$$I^\bullet = [I \longrightarrow 0 \longrightarrow 0 \longrightarrow \ldots] .$$

Damit ist dann offenbar $\mathrm{R}^i F(I) = \mathrm{H}^i(F(I^\bullet)) = 0$ für $i > 0$. □

Theorem 7.19 (Auslöschbarkeit impliziert Universalität)**.** *Sei $F^* : \mathscr{A} \to \mathscr{B}$ ein auslöschbarer kohomologischer δ-Funktor zwischen abelschen Kategorien. Dann ist F^* ein universeller kohomologischer δ-Funktor.*

Bevor wir uns dem Beweis zuwenden, betrachten wir zunächst folgende wichtige Anwendung:

Korollar 7.20. *Die Rechtsderivierten eines linksexakten additiven Funktors von einer abelschen Kategorien mit genügend vielen Injektiven in eine beliebige abelsche Kategorie bilden einen universellen kohomologischen δ-Funktor.*

Beweis des Korollars. Sei $A \in \mathscr{A}$ mit $\mathscr{A}$ abelscher Kategorie mit genug Injektiven und sei F ein linksexakter Funktor. Dann gibt es einen Monomorphismus $\varphi : A \hookrightarrow I$ mit $I \in \mathscr{A}$ injektiv. Es verschwindet $\mathrm{R}^i F(\varphi)$ für $i > 0$, da sogar $\mathrm{R}^i F(I) = 0$ verschwindet nach Lemma 7.18. Also ist $\mathrm{R}^i F$ auslöschbar für alle $i > 0$ und mit dem Theorem $\mathrm{R}^* F$ ein universeller kohomologischer δ-Funktor. □

Beweis des Theorems. Es genügt zu zeigen, dass man für einen kohomologischen δ-Funktor G^* und eine natürliche Transformation $f^0 : F^0 \to G^0$ im Grad 0 eindeutig eine Fortsetzung $f^1 : F^1 \to G^1$ in Grad 1 erhält.

Sei $A \in \mathscr{A}$ und wähle $A \overset{\varphi}{\hookrightarrow} M$ mit $F^i(\varphi) = 0 \ \ \forall\, i > 0$. Wir ergänzen mit dem Kokern zu einer kurzen exakten Sequenz:

$$0 \longrightarrow A \xrightarrow{\varphi} M \xrightarrow{\pi} P \longrightarrow 0$$

Durch Anwendung der Funktoren erhält man folgendes kommutative Diagramm mit exakten Zeilen:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & F^0(A) & \xrightarrow{F^0(\varphi)} & F^0(M) & \xrightarrow{F^0(\pi)} & F^0(P) & \xrightarrow{\delta_F} & F^1(A) \longrightarrow 0 \\
 & & \downarrow{\scriptstyle f_A^0} & & \downarrow{\scriptstyle f_M^0} & & \downarrow{\scriptstyle f_P^0} & & \vdots{\scriptstyle \exists!\, f_A^1} \\
0 & \longrightarrow & G^0(A) & \xrightarrow{G^0(\varphi)} & G^0(M) & \xrightarrow{G^0(\pi)} & G^0(P) & \xrightarrow{\delta_G} & G^1(A) \xrightarrow{G^1(\varphi)} G^1(M)
\end{array}$$

Wegen Exaktheit der Zeilen ist

$$\operatorname{coker}\left(F^0(M) \xrightarrow{F^0(\pi)} F^0(P)\right) = F^0(P) \xrightarrow{\delta_F} F^1(A).$$

Der eindeutige Morphismus f_A^1 wird nun durch die universelle Eigenschaft des Kokerns gegeben, denn es gilt:

$$(\delta_G \circ f_P^0) \circ F^0(\pi) = \delta_G \circ (f_P^0 \circ F^0(\pi)) = (\delta_G \circ G^0(\pi)) \circ f_M^0 = 0 \circ f_M^0 = 0$$

Es bleibt jetzt noch zu zeigen, dass f^1 nicht von der Wahl von $A \overset{\varphi}{\hookrightarrow} M$ abhängt, eine natürliche Transformation ist und mit δ kommutiert.

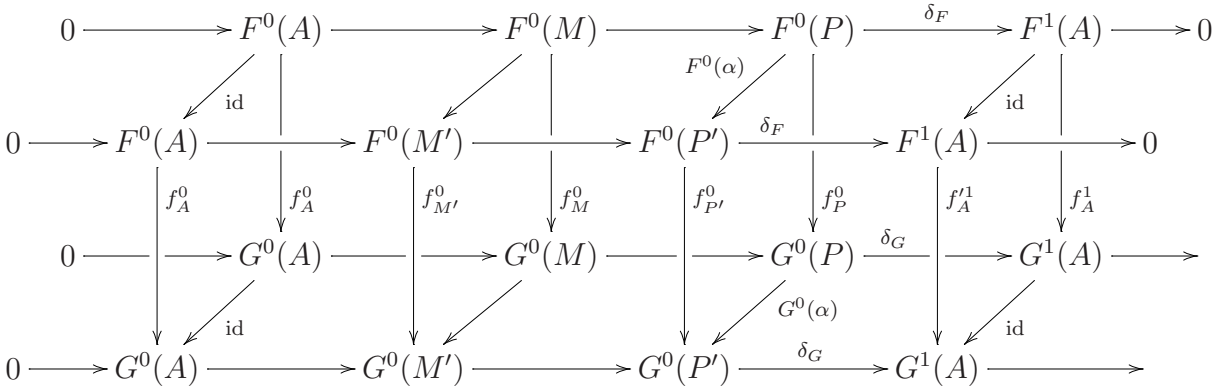
Sei also $A \overset{\varphi'}{\hookrightarrow} M'$ ein weiterer Monomorphismus mit $F^1(\varphi') = 0$. O.B.d.A. kann man annehmen, dass es einen Morphismus $M \to M'$ gibt, der mit φ, φ' kompatibel ist; Mittels des folgenden kommutativen Diagramms können wir dann auf alle Paare φ, φ' schließen.

$$\begin{array}{ccc}
A & \xrightarrow{\varphi} & M \\
\| & & \downarrow \\
A & \xrightarrow{(\varphi,\varphi')} & M \oplus M' \\
\| & & \uparrow \\
A & \xrightarrow{\varphi'} & M'
\end{array}$$

Auch hier erweitern wir zu einer kurzen exakten Sequenz und erhalten also:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\varphi} & M & \xrightarrow{\pi} & P & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & A & \xrightarrow{\varphi'} & M' & \xrightarrow{\pi'} & P' & \longrightarrow & 0 \end{array}$$

Anwendung der Funktoren führt zu:



Im rechten Würfel kommutieren a priori alle Seiten außer der rechten: Die obere und untere wegen der Definition eines δ-Funktors, die linke ,weil f^0 eine natürliche Transformation ist, und die vordere und hintere nach Konstruktion der f^1, f'^1. Wenn wir Kommutativität auf der rechten Seite zeigen können, so sind wir fertig. Dies gilt aber wegen

$$f'^1_A \circ \mathrm{id} \circ \delta_F = f'^1_A \circ \delta_F \circ F^0(\alpha) = \delta_G \circ f^0_{P'} \circ F^0(\alpha) = \delta_G \circ G^0(\alpha) \circ f^0_P = \mathrm{id} \circ \delta_G \circ f^0_P = \mathrm{id} \circ f^1_A \circ \delta_F.$$

Da δ_F ein Epimorphismus ist, können wir ihn von rechts kürzen und erhalten so die gewünschte Gleichung.

Als Nächstes werden wir zeigen, dass f^1 eine natürliche Transformation ist. Sei dazu $A \xrightarrow{u} B$ ein Morphismus und $A \overset{\varphi}{\hookrightarrow} M$ ein Morphismus mit $F^1(\varphi) = 0$. Wir konstruieren nun ein Objekt $B \overset{\varphi'}{\hookrightarrow} M'$ mit $F^1(\varphi') = 0$, so dass folgendes Diagramm kommutiert (und mit Kokernen ergänzt werden kann):

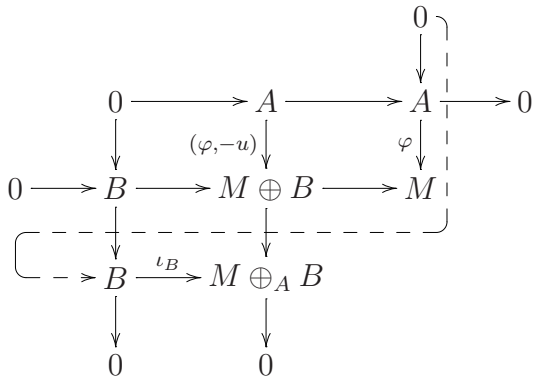
$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\varphi} & M & \cdots\!\!\rightarrow & P & \cdots\!\!\rightarrow & 0 \\ & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \vdots{\scriptstyle w} & & \\ 0 & \longrightarrow & B & \xrightarrow{\varphi'} & M' & \cdots\!\!\rightarrow & P' & \cdots\!\!\rightarrow & 0 \end{array}$$

Betrachte dazu die exakte Sequenz

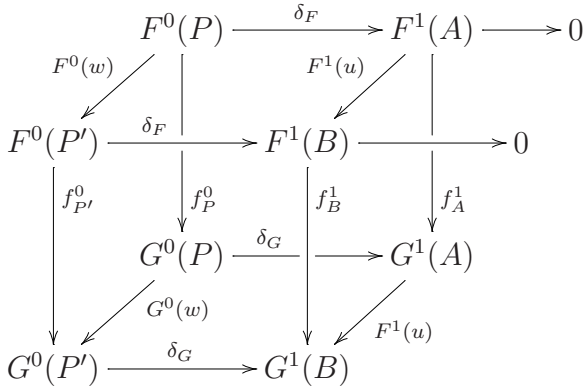
$$A \xrightarrow{(\varphi,-u)} M \oplus B \longrightarrow M \oplus_A B \longrightarrow 0$$

Mit $M \oplus B \to M \oplus_A B := \mathrm{coker}(A \to M \oplus B)$. Dann ist $0 \longrightarrow B \longrightarrow M \oplus_A B$ exakt,

denn



erfüllt die Bedingungen des Schlangenlemmas und dieses liefert das Gewünschte. Nun wähle $M \oplus_A B \overset{\alpha}{\hookrightarrow} M'$, so dass $F^1(\alpha) = 0$, und setze $\varphi' := \alpha \circ \iota_B : B \hookrightarrow M'$ bzw. $v := \alpha \circ \iota_M : M \to M'$. Da $F^1(\varphi') = F^1(\alpha) \circ F^1(\iota) = 0$ gilt, können wir φ' zur Definition von f^1 heranziehen. Wie im vorherigen Schritt erhalten wir ein Quadrat, in dem a priori alle Seiten außer der rechten kommutieren.



Komplett analog zeigen wir, dass dann auch diese kommutiert:

$$f_B^1 \circ F^1(u) \circ \delta_F = f_B^1 \circ \delta_F \circ F^0(w) = \delta_G \circ f_{P'}^0 \circ F^0(w)$$

$$= \delta_G \circ G^0(w) \circ f_P^0 = F^1(u) \circ \delta_G \circ f_P^0 = F^1(u) \circ f_A^1 \circ \delta_F$$

Bleibt also noch zu zeigen, dass f^1 mit δ kommutiert.

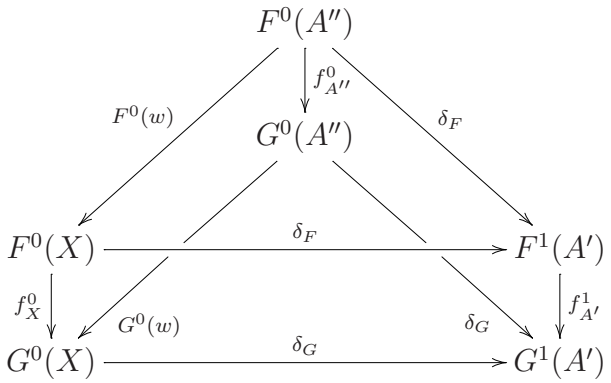
Dazu sei

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

eine kurze exakte Sequenz und wir konstruieren wie im vorherigen Schritt einen Monomorphismus $\alpha : A' \hookrightarrow M'$ mit $F^1(\alpha) = 0$, so dass das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \| \mathrm{id} & & \downarrow v & & \downarrow w & & \\ 0 & \longrightarrow & A' & \longrightarrow & M' & \longrightarrow & X & \longrightarrow & 0 \end{array}$$

kommutiert. Hier ist X der passende Kokern. Dies führt auf ein Diagramm der Form



in dem die Dreiecke oben und unten wegen der Eigenschaft von δ-Funktoren, die linke Seite wegen der Eigenschaft von f^0 als natürliche Transformation von Funktoren und die vordere Seite wegen der Konstruktion von f^1 kommutieren. Dann kommutiert wegen

$$f^1_{A'} \circ \delta_F = f^1_{A'} \circ \delta_F \circ F^0(w) = \delta_G \circ f^0_X \circ F^0(w) = \delta_G \circ G^0(w) \circ f^0_{A''} = \delta_G \circ f^0_{A''}$$

auch die rechte Seite. □

Beispiel 7.21 (Kategorie der Pfeile). Sei $\mathscr{A}$ eine abelsche Kategorie. Dann definiere eine neue Kategorie $\mathscr{AR}_{\mathscr{A}}$, die Kategorie der Pfeile in $\mathscr{A}$, durch

$$\mathrm{Ob}(\mathscr{AR}_{\mathscr{A}}) := \{f \in \mathrm{Hom}_{\mathscr{A}}(A, B) \mid A, B \in \mathscr{A}\}$$

und

$$\mathrm{Hom}_{\mathscr{AR}_{\mathscr{A}}}(f : A \to B, g : C \to D\} := \{(\varphi, \psi) \in \mathrm{Hom}_{\mathscr{A}}(A, C) \times \mathrm{Hom}_{\mathscr{A}}(B, D) \mid \psi \circ f = g \circ \varphi\},$$

also kommutative Diagramme der Form:

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & C \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ B & \xrightarrow{\psi} & D \end{array}$$

Man weist leicht nach, dass $\mathscr{AR}_{\mathscr{A}}$ eine abelsche Kategorie ist. Kurze exakte Sequenzen von Pfeilen sind dann Morphismen von kurzen exakten Sequenzen in $\mathscr{A}$:

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

Definiere nun Funktoren $F^0 := \ker$, $F^1 := \mathrm{coker}$ und $F^i := 0 \ \forall \ i > 1$. Dies ist ein kohomologischer δ-Funktor von $\mathscr{AR}_{\mathscr{A}}$ nach $\mathscr{A}$. Die lange exakte Sequenz, die man einer kurzen exakten Sequenz zuordnet, wird durch das Schlangenlemma geliefert und die Verträglichkeit mit Morphismen von kurzen exakten Sequenzen liefert die Bemerkung zum Schlangenlemma.

Dieser kohomologische δ-Funktor ist sogar universell, da man $F^1 = \operatorname{coker}$ auslöschen kann, denn betrachte zu $f \in \operatorname{Hom}_{\mathscr{A}}(A, B)$ den Morphismus von Pfeilen:

$$\begin{array}{ccc} A & \xrightarrow{(\mathrm{id}_A, f)} & A \oplus B \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \pi} \\ B & \xrightarrow{\mathrm{id}_B} & B \end{array}$$

so gilt $\operatorname{coker} \pi_B = 0$ und daher wird coker ausgelöscht. Man weist außerdem leicht nach, dass der angegebene Morphismus von Pfeilen ein Monomorphismus ist, da sowohl id_A als auch id_B vorkommt.

Vortrag 8

Gruppenkohomologie II: Dimensionsshift

Tobias Polley
13.12.2005

8.1 Kohomologie als derivierter Funktor

Sei M^G die Untergruppe der Elemente des G-Moduls M, die invariant unter G sind, d.h.

$$M^G := \{m \in M \mid \text{für alle } \ g \in G \text{ gilt } g.m = m\}.$$

Ist nun $f : M \to M'$ ein G-Homomorphismus, so wird M^G von f auf M'^G abgebildet, denn für $m \in M^G$ gilt $g.f(m) = f(g.m) = f(m)$. Also ist $(\ )^G$ ein Funktor von Mod_G nach Ab, der Funktor der G-Invarianten.

Der Funktor der G-Invarianten ist additiv, da die Addition der Gruppe der Invarianten die eingeschränkte Addition des Moduls ist und die Addition von Morphismen über die werteweise Addition definiert ist: $(f +_M f')^G = f^G +_{M^G} f'^G$.

Lemma 8.1. *Der Funktor $(\ )^G$ ist linksexakt.*

Beweis. Zu zeigen ist, daß für eine beliebige exakte Sequenz $0 \to M' \xrightarrow{f'} M \xrightarrow{f} M''$ die Sequenz

$$0 \longrightarrow M'^G \xrightarrow{f'^G} M^G \xrightarrow{f^G} M''^G$$

wieder exakt ist. Nun gilt $M^G \subset M$, etc. ... und f^G ist eine Einschränkung von f, somit folgt die Exaktheit bei M'^G. Außerdem gilt:

$$\ker f^G = \ker f \cap M^G = \mathrm{im}\, f' \cap M^G = \mathrm{im}\, f'^G.$$

□

Definition 8.2. Die **Kohomologie $\mathrm{H}^*(G, M)$ von G mit Koeffizienten im G-Modul M** ist der Wert $\mathrm{R}^*(\ )^G(M)$ der rechtsderivierten Funktoren des Funktors der G-Invarianten.

Bemerkung 8.3. Die Notation H^* statt H^q bedeutet, daß hier nicht nur die Gruppen in den einzelnen Graden q definiert werden, sondern daß es sich bei $\mathrm{R}^*(\ )^G$ um einen kohomologischen δ-Funktor handelt, dessen Verbindungshomomorphismen hier ebenfalls für H^* mit übernommen werden.

Sei nun $\mathbb{Z}$ der triviale G-Modul, d.h. $g.z = z$ für alle $z \in \mathbb{Z}$ und $g \in G$. Es gilt nun der folgende Satz, der Gruppenkohomologie mit einer **Ext**-Gruppe identifiziert.

Satz 8.4. $\mathrm{H}^*(G, M) = \mathrm{Ext}^*_G(\mathbb{Z}, M)$.

Beweis. In Vortrag 7 sahen wir, daß die Derivierten von linksexakten additiven Funktoren zwischen abelschen Kategorien mit genügend vielen Injektiven bereits universelle kohomologische δ-Funktoren sind. Nun folgt aus der Definition von universell, daß es bis auf eindeutige Isomorphie höchstens einen universellen kohomologischen δ-Funktor geben kann, wenn man den Funktor im Grad 0 vorgibt. Sowohl $\mathrm{H}^*(G, -)$ als auch $\mathrm{Ext}^*_G(\mathbb{Z}, -)$ sind derivierte, also universelle kohomologische δ-Funktoren, die im Grad 0 übereinstimmen:

$$\mathrm{H}^0(G, M) = M^G = \mathrm{Hom}_G(\mathbb{Z}, M) = \mathrm{Ext}^0_G(\mathbb{Z}, M).$$

□

Zum Schluß vergleichen wir die Definition von Gruppenkohomologie als deriviertem Funktor mit der ad-hoc Definition mittels einer projektiven Auflösung aus Vortrag 4.

Satz 8.5. *Die oben definierten Kohomologiegruppen sind genau die aus Vortrag 4 bekannten, d.h. für eine projektive Auflösung $P_\bullet \to \mathbb{Z}$ des trivialen G-Moduls $\mathbb{Z}$ gibt es einen kanonischen Isomorphismus*

$$\mathrm{H}^q(G, M) = \mathrm{H}^q(\mathrm{Hom}_G(P_\bullet, M)).$$

Beweis. Sei $P_\bullet \to \mathbb{Z}$ eine projektive Auflösung des trivialen G-Moduls $\mathbb{Z}$. In Vortrag 6 haben wir gesehen, daß $\mathrm{H}^q_{P_\bullet}(G, M) := \mathrm{H}^q(\mathrm{Hom}_G(P_\bullet, M))$ einen kohomologischen δ-Funktor auf der Kategorie der G-Moduln mit Werten in den abelschen Gruppen definiert. Im Grad 0 erhalten wir in natürlicher Weise $\mathrm{H}^0(G, M) = M^G = \mathrm{H}^0_{P_\bullet}(G, M)$ und damit eine natürliche Transformation von δ-Funktoren

$$\mathrm{H}^*(G, M) \longrightarrow \mathrm{H}^*_{P_\bullet}(G, M).$$

Diese ist im Grad 0 ein Isomorphismus und damit auch insgesamt, sofern $\mathrm{H}^*_{P_\bullet}(G, -)$ auslöschbar ist. Aber für einen injektiven G-Modul I ist

$$0 \longrightarrow I^G \longrightarrow \mathrm{Hom}_G(P_\bullet, I)$$

immer noch exakt, also verschwindet $\mathrm{H}^q_{P_\bullet}(G, I)$ für $q \geq 1$ wie gewünscht. □

8.2 Induzierte Moduln

Definition 8.6. Sei G eine Gruppe und $H \subset G$ eine Untergruppe. Für einen H-Modul M definieren wir **den von H nach G induzierten Modul $\mathrm{Ind}_H^G(M)$** als

$$\mathrm{Ind}_H^G(M) = \{\phi : G \to M \mid \text{für alle } h \in H \text{ gilt } \phi(hg) = h.\phi(g)\},$$

mit der G-Modulstruktur auf $\mathrm{Ind}_H^G(M)$, welche gegeben ist durch

$$(\phi + \phi')(x) = \phi(x) + \phi'(x)$$

$$(g.\phi)(x) = \phi(xg).$$

Ein Homomorphismus $\alpha : M \to M'$ von H-Moduln definiert einen Homomorphismus von G-Moduln

$$\mathrm{Ind}_H^G(\alpha) : \mathrm{Ind}_H^G(M) \longrightarrow \mathrm{Ind}_H^G(M'), \quad \phi \longmapsto \alpha \circ \phi.$$

Lemma 8.7. *Für jeden G-Modul M und H-Modul N ist in natürlicher Weise*

$$\mathrm{Hom}_H(M, N) = \mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)).$$

Beweis. Für einen G-Homomorphismus $\alpha : M \to \mathrm{Ind}_H^G(N)$ definieren wir

$$\beta : M \to N, \quad \beta(m) := \alpha(m)(1_G).$$

Nun gilt für $h \in H$

$$\beta(h.m) = (\alpha(h.m))(1_G) = (h.\alpha(m))(1_G) = \alpha(m)(1_G h)$$

$$= \alpha(m)(h) = h.(\alpha(m)(1_G)) = h.\beta(m).$$

Somit ist β ein H-Homomorphismus.

Umgekehrt definieren wir für $\beta : M \to N$ die Abbildung $\alpha : M \to \mathrm{Ind}_H^G(M)$, so daß $\alpha(m)(g) = \beta(g.m)$. Dann ist α ein G-Homomorphismus, denn

$$\alpha(g.m)(g') = \beta(g'g.m) = \alpha(m)(g'g) = (g.\alpha(m))(g').$$

Man sieht leicht, dass die Abbildungen $\alpha \mapsto \beta$ und $\beta \mapsto \alpha$ invers zueinander sind. □

Lemma 8.8. *Der Funktor $\mathrm{Ind}_H^G : \mathrm{Mod}_H \to \mathrm{Mod}_G$ ist exakt.*

Beweis. Für eine exakte Sequenz

$$0 \longrightarrow M' \longrightarrow M \xrightarrow{f} M'' \longrightarrow 0$$

müssen wir zeigen, daß

$$0 \longrightarrow \mathrm{Ind}_H^G(M') \longrightarrow \mathrm{Ind}_H^G(M) \xrightarrow{\mathrm{Ind}_H^G(f)} \mathrm{Ind}_H^G(M'') \longrightarrow 0$$

exakt ist. Die Exaktheit bei $\mathrm{Ind}_H^G(M')$ und $\mathrm{Ind}_H^G(M)$ folgt mit den gleichen Argumenten wie im Beweis der Exaktheit des Invariantenfunktors $(\ )^G$-Funktors in Lemma 8.1.

Nun zeigen wir, daß $\mathrm{Ind}_H^G(f)$ surjektiv ist, d.h. daß für alle $\phi \in \mathrm{Ind}_H^G(M'')$ ein Urbild existiert. Dazu sei S eine Menge von Repräsentanten von G/H, also $G = \cup_{s \in S} Hs$. Für jedes $s \in S$ wählen wir ein $m_s \in M$, so daß $f(m_s) = \phi(s)$ gilt, und definieren $\phi'(hs) := h.m_s$. Dann ist $\phi' \in \mathrm{Ind}_H^G(N)$ und $\mathrm{Ind}_H^G(f)(\phi') = \phi$. □

Ist $H = \{1\}$, so ist ein H-Modul lediglich eine abelsche Gruppe. In diesem Fall schreibt man für den von H nach G induzierten Modul $\mathrm{Ind}^G(A)$ und es gilt

$$\mathrm{Ind}^G(A) = \{\phi : G \longrightarrow A\} = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A).$$

Definition 8.9. Ein G-Modul M heißt **induziert**, wenn er es eine abelsche Gruppe A gibt, so dass M isomorph zu $\mathrm{Ind}^G(A)$ ist.

Definition 8.10. Funktoren $L : \mathscr{A} \to \mathscr{B}$ und $R : \mathscr{B} \to \mathscr{A}$ heißen **adjungiert**, falls es eine natürliche Bijektion

$$\tau = \tau_{AB} : \mathrm{Hom}_{\mathscr{B}}(L(A), B) \xrightarrow{\cong} \mathrm{Hom}_{\mathscr{A}}(A, R(B))$$

für alle A in $\mathscr{A}$ und B in $\mathscr{B}$ gibt. Natürlich bedeutet hierbei, dass für alle $f : A \to A'$ in $\mathscr{A}$ und $g : B \to B'$ in $\mathscr{B}$ das folgende Diagramm kommutiert:

$$\begin{array}{ccccc}
\mathrm{Hom}_{\mathscr{B}}(L(A'), B) & \xrightarrow{\circ Lf} & \mathrm{Hom}_{\mathscr{B}}(L(A), B) & \xrightarrow{g\circ} & \mathrm{Hom}_{\mathscr{B}}(L(A), B') \\
\downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\
\mathrm{Hom}_{\mathscr{A}}(A', R(B)) & \xrightarrow{\circ f} & \mathrm{Hom}_{\mathscr{A}}(A, R(B)) & \xrightarrow{Rg\circ} & \mathrm{Hom}_{\mathscr{A}}(A, R(B')).
\end{array}$$

L heißt **linksadjungiert** zu R und R heißt **rechtsadjungiert** zu L.

Lemma 8.11. *Der Funktor* Ind_H^G *erhält injektive Moduln.*

Beweis. In Lemma 8.7 haben wir gesehen, dass der Vergiß-Funktor $V : \mathrm{Mod}_G \to \mathrm{Mod}_H$ der linksadjungierte Funktor zu Ind_H^G ist. Darüberhinaus ist $V(-)$ offensichtlich exakt.

Für einen injektiven H-Modul I ist nun nach der Funktor $\mathrm{Hom}_{\mathrm{Mod}_H}(-, \mathrm{Ind}_H^G(I))$ isomorph zu $\mathrm{Hom}_{\mathrm{Mod}_G}(V(-), I)$, welcher exakt ist, da er die Komposition zweier exakten Funktoren ist, nämlich V und $\mathrm{Hom}_{\mathrm{Mod}_G}(-, I)$. Also ist $\mathrm{Ind}_H^G(I)$ ein injektiver G-Modul. □

Satz 8.12 (Shapiros Lemma)**.** *Sei H eine Untergruppe von G. Für jeden H-Modul N und $q \geq 0$ gibt es einen kanonischen Isomorphismus*

$$\mathrm{H}^q(G, \mathrm{Ind}_H^G(N)) \cong \mathrm{H}^q(H, N).$$

Beweis. Wir wählen eine injektive Auflösung $N \to I^\bullet$ von N. Nun wenden wir den Funktor Ind_H^G and und bekommen dadurch die injektive Auflösung $\mathrm{Ind}_H^G(N) \to \mathrm{Ind}_H^G(I^\bullet)$ des G-Moduls $\mathrm{Ind}_H^G(N)$, denn $\mathrm{Ind}_H^G(-)$ ist exakt nach Lemma 8.8 und erhält Injektive nach Lemma 8.11. Somit gilt:

$$\mathrm{H}^q(G, \mathrm{Ind}_H^G(N)) = \mathrm{H}^q((\mathrm{Ind}_H^G(I^\bullet))^G) = \mathrm{H}^q(I^{\bullet,H}) = \mathrm{H}^q(H, N),$$

denn

$$(\mathrm{Ind}_H^G(M))^G = \{\varphi \in \mathrm{Ind}_H^G(M) \mid g.\varphi = \varphi\} = \{\varphi \in \mathrm{Ind}_H^G(M) \mid \varphi(g'g) = \varphi(g')\}$$

$$= \{\varphi \in \mathrm{Ind}_H^G(M) \mid \varphi = \text{ konstant}\} = M^H.$$

□

Korollar 8.13. *Ist M ein induzierter G-Modul, so ist* $\mathrm{H}^q(G, M) = 0$ *für* $q > 0$.

Beweis. Ist $M = \mathrm{Ind}^G(A)$, so gilt $\mathrm{H}^q(G, M) = \mathrm{H}^q(1, A) = 0$ für $q > 0$. □

8.3 Dimensionsshift

Korollar 8.14. *Ist* $0 \to M' \to M \to M'' \to 0$ *eine exakte Sequenz von* G*-Moduln mit* $\mathrm{H}^q(G, M) = 0$ *für* $q > 0$*, so gilt*

$$\mathrm{H}^q(G, M'') = \mathrm{H}^{q+1}(G, M')$$

für $q > 0$.

Bemerkung 8.15. Dies ist zum Beispiel der Fall, wenn M ein induzierter G-Modul ist.

Beweis. Die exakte Kohomologiesequenz wird zu

$$0 \longrightarrow M'^G \longrightarrow M^G \longrightarrow M''^G \longrightarrow H^1(G, M) \longrightarrow 0$$

und

$$\mathrm{H}^q(G, N) \xrightarrow{\cong} \mathrm{H}^{q+1}(G, M), \qquad q > 1.$$

□

Allgemeiner läßt sich formulieren:

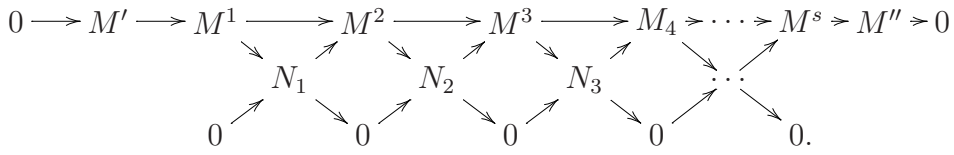
Korollar 8.16. *Ist*

$$0 \longrightarrow M' \to M^1 \longrightarrow \ldots \longrightarrow M^s \longrightarrow M'' \longrightarrow 0$$

exakt und $\mathrm{H}^q(G, M^i) = 0$ *für* $q, i > 0$*, so gilt für* $q > 0$

$$\mathrm{H}^q(G, M'') = \mathrm{H}^{q+s}(G, M').$$

Beweis. Per Induktion mit Korollar 8.14 in folgendem Diagramm:



□

Vortrag 9

Gruppenkohomologie III: Funktorialität in der Gruppe

Jonathan Pfaff, Cornelius Probst
20.12.2005

9.1 Gruppenwechsel

9.1.1 Abstrakte Beschreibung

Definition 9.1. Sei $f : G' \to G$ ein Gruppenhomomorphismus und A ein G'-Modul. Dann lässt sich auf A mittels f eine G'-Modul-Struktur erklären:

$$s'.a := f(s').a \qquad \forall\, s' \in G', \forall\, a \in A$$

Den so erhalten G'-Modul bezeichnet man mit f^*A.

Satz–Definition 9.2. *(1) Der Funktor $f^* : G\text{-Mod} \to G'\text{-Mod},\ A \mapsto f^*A$ ist additiv und exakt.*

(2) Die Komposition $(\mathrm{H}^q(G', f^*(-)), \delta)$ definiert einen kohomologischer δ-Funktor auf der Kategorie der G-Moduln mit Werten in der Kategorie der abelschen Gruppen.

Beweis. Klar. □

Die Inklusion definiert eine natürliche Transformation von $\mathrm{H}^0(G, -) \to \mathrm{H}^0(G, f^*(-))$: es kommutiert offenbar für jeden G-Modulhomomorphismus $A \to B$ das Diagramm

$$\begin{array}{ccc} A^G & \hookrightarrow & A^{G'} \\ \downarrow & & \downarrow \\ B^G & \hookrightarrow & B^{G'} \end{array}$$

Da derivierte Funktoren universell sind, existiert deshalb ein eindeutig bestimmter Morphismus kohomologischer δ-Funktoren

$$(\mathrm{H}^q(G, -), \delta) \longrightarrow (\mathrm{H}^q(G, f^*(-)), \delta),$$

welcher die Inklusion fortsetzt. Insbesondere existiert also für jedes $q \geq 0$ und für jeden G-Modul A ein Homomorphismus abelscher Gruppen

$$\mathrm{H}^q(G, A) \longrightarrow \mathrm{H}^q(G', f^*A).$$

Definition 9.3. Sei $f : G' \to G$ ein Gruppenhomomorphismus, A ein G-Modul, A' ein G'-Modul und $g : A \to A'$ ein Gruppenhomomorphismus. Es heißen f und g **kompatibel**, wenn g sogar einen G'-Homomorphismus $f^*A \to A'$ ist.

Komponiert man den von einer kompatiblen Abbildung $A \to A'$ wie in der Definition auf der G'-Kohomologie induzierten Abbildung $\mathrm{H}^q(G', f^*A) \to \mathrm{H}^q(G', A')$ mit der natürlichen Transformation $\mathrm{H}^q(G', A) \to \mathrm{H}^q(G', f^*A)$, so erhält man also für jedes $q \geq 0$ einen zum Paar (f, g) assoziierten Morphismus

$$(f, g)^q : \mathrm{H}^q(G, A) \longrightarrow \mathrm{H}^q(G', A').$$

Beispiel 9.4. Sei $G = G'$, $A = A'$ und $t \in G$. Sei $\varphi_t : G \to G$ der innere Automorphismus: $g \mapsto tgt^{-1}$, und sei $\lambda_{t^{-1}} : A \to A$ der Gruppenhomomorphismus $a \mapsto t^{-1}a$ Translation mit t^{-1}. Dann sind φ_t und $\lambda_{t^{-1}}$ kompatibel. Also haben wir für jedes $t \in G$ einen Automorphismus $(\varphi_t, \lambda_{t^{-1}})^q : \mathrm{H}^q(G, A) \to \mathrm{H}^q(G, A)$.

So interessant das Beispiel scheint, so enttäuschend aber dann auch wieder hilfreich ist das folgende Ergebnis.

Proposition 9.5. *Der zu einem Element $t \in G$ assoziierte Automorphismus $(\varphi_t, \lambda_{t^{-1}})^*$ der Kohomologie ist die Identität.*

Beweis. Die Automorphismen $(\varphi_t, \lambda_{t^{-1}})^*$ definieren einen natürlichen Automorphismus von des kohomologische δ-Funktors $\mathrm{H}^*(G, -)$ und sind daher durch $(\varphi_t, \lambda_{t^{-1}})^0$ eindeutig bestimmt: $(\varphi_t, \lambda_{t^{-1}})^0(a) = t^{-1}.a = a$, denn a gehört zu $A^G = \mathrm{H}^0(G, A)$. □

9.1.2 Explizite Beschreibung auf dem inhomogenen Koketten

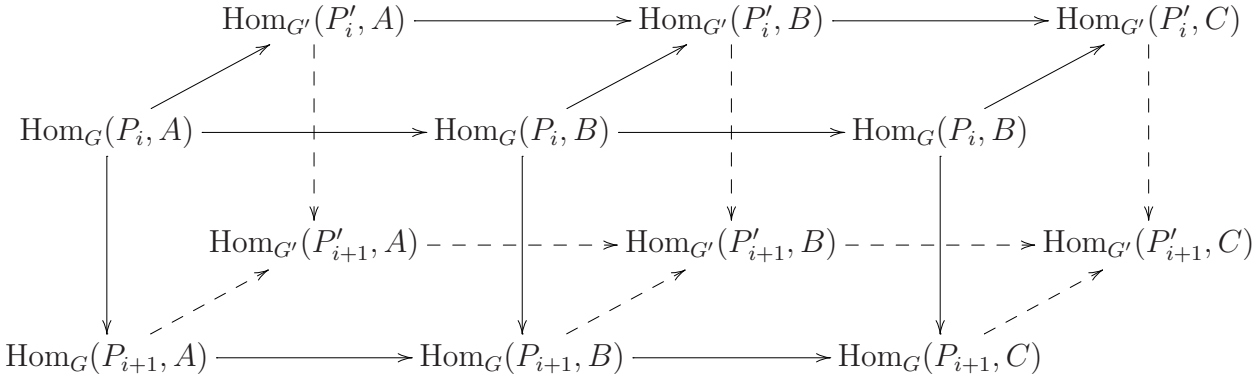
Seien $P_\bullet \to \mathbb{Z}$ (bzw. $P'_\bullet \to \mathbb{Z}$) die projektive Standardauflösung in G-Moduln (bzw. G'-Moduln). Ein Gruppenhomomorphismus $f : G' \to G$ definiert durch komponentenweise Anwendung G'-Homomorphismen $\circ f^{\times r+1} : P'_i \to f^*P_i$, die zu einem Morphismus $P'_\bullet \to f^*P_\bullet$ von Komplexen von G'-Moduln. Dieser induziert über den Funktor $\mathrm{Hom}_{G'}(-, f^*A)$, also durch Vorschalten von f, einen Homomorphismus von Kokettenkomplexen

$$\tau_A : \mathrm{Hom}_G(P_\bullet, A) \longrightarrow \mathrm{Hom}_{G'}(f^*P_\bullet, f^*A) \longrightarrow \mathrm{Hom}_{G'}(P'_\bullet, f^*A).$$

Diese Homomorphismen „rechnen" die Transformation $\mathrm{H}^q(G, -) \to \mathrm{H}^q(G', f^*(-))$ auf dem Niveau der Standardauflösung aus. In der Tat, für ein $g : A \to B$ kommutiert $(g\circ)\tau_A = \tau_B(f^*g\circ)$, und auch mit δ ist τ_- verträglich: für eine kurze exakte Sequenz

$$\mathbf{0} \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow \mathbf{0}$$

in G-Mod hat das folgende kommutative Diagramm



exakte Zeilen, wobei die Nullen aus Platzgründen fehlen. Die Natürlichkeit des Schlangenlemmas liefert nun $\delta \circ \mathrm{H}^q(\tau_C) = \mathrm{H}^q(\tau_A) \circ \delta$.

Nun prüft man leicht, die Behauptung, dass $\mathrm{H}^*(\tau_A)$ mit der natürlichen Transformation $\mathrm{H}^q(G, -) \to \mathrm{H}^q(G', f^*(-))$ übereistimmt, denn man muss dies nur noch im Grad 0 prüfen, un dort ist es klar.

Definition 9.6. (1) Sei H eine Untergruppe von G. Die oben konstruierte natürliche Transformation von kohomologischen δ-Funktoren

$$\mathrm{res}^q : \mathrm{H}^q(G, A) \longrightarrow \mathrm{H}^q(H, A)$$

heißt **Restriktion**.

(2) Sei H eine normale Untergruppe von G. Dann ist die Gruppe A^H ein G/H-Modul und die Homomorphismen $G \twoheadrightarrow G/H$ und $A^H \hookrightarrow A$ sind kompatibel. Die oben konstruierte natürliche Transformation von kohomologischen δ-Funktoren

$$\mathrm{inf} : \mathrm{H}^q(G/H, A^H) \longrightarrow \mathrm{H}^q(H, A)$$

heißt **Inflation**.

Theorem 9.7. *Sei A ein G-Modul und $H \subseteq G$ ein Normalteiler. Die Sequenz*

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

ist exakt.

Beweis. Es gilt $\mathrm{res} \circ \mathrm{inf} = 0$, da etwa auf Ketten die Abbildung durch Komposition mittels $H \to G \to G/H$ induziert wird.

Exaktheit an der Stelle. $\mathrm{H}^1\left(G/\mathrm{H}, A^{\mathrm{H}}\right)$: Sei $f : G/H \to A^H$ ein 1-Kozykel mit $\mathrm{inf}(f) = 0$. Dann gibt es ein $a \in A$ mit $f(s) = s.a - a$ für alle $s \in G$, außerdem gilt $f(st) = f(s)$ für alle $t \in H$. Damit gilt $0 = 1.a - a = (1.t).a - a = t.a - a$, daher liegt $a \in A^H$ und f ist auch ein 1-Rand als Kette mit Werten in A^H.

Exaktheit an der Stelle. $\mathrm{H}^1(G, A)$: Sei $f : G \to A$ ein 1-Kozykel mit $\mathrm{res}(f) = 0$. Dies bedeutet, dass es ein $a \in A$ gibt mit $f(t) = t.a - a$ für alle $t \in H$. Modifizieren wir f um den 1-Rand $s.a - a$, so darf angenommen werden, dass $f \mid H = 0$ gilt.

Da f ein Kozykel ist, gilt $f(st) = s.f(t) + f(s) = f(s)$ für alle $t \in H$. Also ist f auf den Rechtsnebenklassen von H konstant und definiert daher eine Abbildung $f : G/H \to A$, deren Bilder in A^H liegen wegen $t.f(s) = f(ts) - f(t) = f(s)$. Der so konstruierte $G/H \to A^H$ ist ein 1-Kozykel auf G/H mit Werten in A^H, der ein Urbild von f ist. □

9.2 Vorbereitungen zur Definition der Corestriktion

Ziel des zweiten Teils des Vortrages ist es, dem zu Beginn konstruierten Restriktionsmorphismus $\mathrm{res} : \mathrm{H}^n(G, A) \longrightarrow \mathrm{H}^n(H, A)$ für eine Untergruppe $H \subseteq G$ eine Ziel- und Ausgangsbereich vertauschende Abbildung zur Seite zu stellen: die **Corestriktion**. Während

das grobe Vorgehensmuster – die Definition der Abbildung als ein Morphismus von universellen kohomologischen δ-Funktoren im Grad 0, Ausdehnung auf alle Dimensionen mittels Universalität – auch weiterhin anwendbar bleibt, muß jedoch im Detail auf eine subtilere Weise argumentiert werden. Die im Grad 0 zu definierende Abbildung

$$A^H = \mathrm{H}^0(H, A) \longrightarrow \mathrm{H}^0(G, A) = A^G$$

ist beispielsweise weniger augenfällig als die zuvor benutzte Inklusion der Fixgruppen; größere Schwierigkeiten wird jedoch der Nachweis der Universalität des noch zu definierenden Funktors bereiten, den wir mit $\mathrm{H}^*(G, -)$ werden vergleichen wollen. Anders als bei der Restriktion wird man nicht mit der Deriviertheit des letztgenannten Funktors argumentieren können, stattdessen werden wir zeigen müssen, daß der erste Funktor auslöschbar ist. Der Vorbereitung dieser Tatsache dient dieser Abschnitt.

9.2.1 Wiederholung: induzierte Moduln und Shapiros Lemma

Wie üblich bezeichne G eine Gruppe und A einen G-Modul. In Übereinstimmung mit der allgemeinen Einführung des zueinander kompatiblen Paars eines Gruppen- und Modulmorphismus bezeichne $f\colon H \hookrightarrow G$ die Inklusion der Gruppen und f^*A die kanonische Einschränkung des G-Moduls A zu einem H-Modul.

Definition 9.8 (Induzierte Moduln)**.** (1) Ist X ein H-Modul, so wird die Menge

$$\mathrm{Ind}_H^G(X) = \{\text{Abbildungen } \varphi : G \longrightarrow X : \varphi(hg) = h\varphi(g)\}$$

mittels der durch $(g' \cdot \varphi)(g) := \varphi(gg')$ erklärten Operation zu einem G-Modul, dem **von H nach G induzierten Modul**.

(2) Ist $H = 1$ die triviale Gruppe, so schreibt man einfach $\mathrm{Ind}^G X := \mathrm{Ind}_H^G(X)$ und bezeichnet dies als **G-induzierten Modul.** Man sieht leicht, daß

$$\mathrm{Ind}^G X \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X).$$

Satz 9.9. $\mathrm{Ind}_H^G(-) : G\text{-Mod} \to H\text{-Mod}$ *ist ein exakter Funktor.*

Beweis. Siehe Vortrag 8. □

Satz 9.10 (Shapiros Lemma)**.** *Es gibt eine natürliche Isomorphie*

$$\mathrm{sh}^n : \mathrm{H}^n\left(G, \mathit{Ind}_H^G X\right) \xrightarrow{\sim} \mathrm{H}^n(H, X),$$

den **Shapiro-Isomorphismus**. *Insbesondere ist* $\mathrm{H}^n(G, M) = 0$ *für* $n > 0$*, falls* M *ein* G*-induzierter Modul ist.*

Beweis. Siehe Vortrag 8. □

Bemerkung 9.11. Ist A ein G-Modul und A_0 die zugrundeliegende abelsche Gruppe, so läßt sich A auf natürliche Weise in einen induzierten G-Modul einbetten. Hierfür definiere man einfach $A \hookrightarrow \mathrm{Ind}^G A_0$, $a \mapsto \varphi_a := (g \mapsto ga)$. Zu überprüfen ist allein die Verträglichkeit mit der auf $\mathrm{Ind}^G(A_0)$ zu Beginn definierten G-Modulstruktur, also die Gleichheit

$$\varphi_{ha} = (g \longmapsto g(ha)) = (g \longmapsto (gh)a) = h \cdot (g \longmapsto ga) = h \cdot \varphi_a.$$

9.2.2 G-induzierte Moduln sind H-induziert

Für die Konstruktion der Corestriktion ist das folgende Resultat entscheidend:

Satz 9.12. *Ist A ein G-induzierter Modul, also $A \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X)$ mit einer abelschen Gruppe X, so ist A auch H-induziert, also $f^*A \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], Y)$, für eine geeignete abelsche Gruppe Y.*

Der Beweis gründet sich auf die folgenden Hilfssätze:

Lemma 9.13. *$\mathbb{Z}[G]$ ist frei über $\mathbb{Z}[H]$ als links- (bzw. rechts-) $\mathbb{Z}[H]$-Modul.*

Beweis. Man wähle ein Repräsentantensystem $S \subset G$ für die Rechtsnebenklassen von H in G. Zu $s \in G$ ist $\mathbb{Z}[H] \cdot s$ ein zu $\mathbb{Z}[H]$ isomorpher $\mathbb{Z}[H]$-Untermodul von $\mathbb{Z}[G]$. Zusammengenommen ergibt sich $f^*\mathbb{Z}[G] \cong \bigoplus_{s\in S} \mathbb{Z}[H] \cdot s$ □

Lemma 9.14. *Als $\mathbb{Z}[H]$-Modul ist $f^*\mathbb{Z}[G] \cong \mathbb{Z}[H] \otimes_{\mathbb{Z}} M$ für eine abelsche Gruppe M.*

Beweis. Man schließe das Repräsentantensystem S zu einer abelschen Gruppe $M \subseteq \mathbb{Z}[G]$ ab. Dann erhält man eine $\mathbb{Z}$-bilineare Abbildung $\mathbb{Z}[H] \times M \twoheadrightarrow f^*\mathbb{Z}[G]$ mittels $(h, m) \mapsto hm$ und somit eine Abbildung $\mathbb{Z}[H] \otimes_{\mathbb{Z}} M \to f^*\mathbb{Z}[G]$, welcher die behauptete Isomorphie induziert. □

Lemma 9.15. $\mathrm{Hom}_{\mathbb{Z}}(f^*\mathbb{Z}[G], X) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H] \otimes_{\mathbb{Z}} M, X) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], \mathrm{Hom}(M, X))$

Beweis. Nur die zweite Isomorphie ist zu zeigen, und diese folgt da Gruppe der $\mathbb{Z}$-bilinearen Abbildungen $\mathbb{Z}[H] \times M \to X$ kanonisch isomorph ist zu $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H] \otimes_{\mathbb{Z}} M, X)$. □

9.3 Die Corestriktion

Von nun an nehmen wir an, H habe endlichen Index in G. Wir wählen wieder ein Repräsentantensystem $S = \{s_i \in G\}_{i=1\ldots n}$ mit $n = (G : H)$ und definieren die **Normabbildung**

$$\mathrm{N}_{G/H} : A^H \longrightarrow A, \quad a \longmapsto \sum_{i=1}^{n} s_i a$$

Man stellt leicht fest, daß $\mathrm{N}_{G/H}(a) \in A^G$. Mit Hilfe von Shapiros Lemma gelingt es uns, diesen Sachverhalt zu formalisieren und als Morphismus zweier kohomologischer δ-Funktoren in Grad 0 auszudrücken:

$$A^H = \mathrm{H}^0(H, f^*A) \xrightarrow{\mathrm{sh}} \mathrm{H}^0\left(G, \mathrm{Ind}_H^G f^*A\right) \xrightarrow{\mathrm{N}_{G/H}} \mathrm{H}^0(G, A) = A^G.$$

Nun greifen wir die Ergebnisse des vorangegangenen Abschnittes auf und bemerken, daß $\mathrm{H}^*\left(G, \mathrm{Ind}_H^G f^*-\right)$ ein auslöschbarer kohomologischer δ-Funktor ist. Die Aussage über die Funktorialität ist klar, denn Ind_H^G ist ein exakter Funktor; also kann man die Argumentation zur Einführung der Restriktion Wort für Wort wiederholen. Die Auslöschbarkeit wiederum ergibt sich mit Shapiros Lemma aus der Tatsache, daß man jeden G-Modul A einbetten kann in den G-induzierten Modul $\mathrm{Ind}^G A_0$, der dann wiederum auch H-induziert ist:

$$\mathrm{H}^n\left(G, \mathrm{Ind}_H^G f^*\mathrm{Ind}^G A_0\right) \xrightarrow{\mathrm{sh}} \mathrm{H}^n\left(H, f^*\mathrm{Ind}^G A_0\right) = 0 \quad \text{für } n > 0.$$

Nach Vortrag 7 ist $\mathrm{H}^*\left(G, \mathrm{Ind}_H^G f^* -\right)$ also ein universeller kohomolgischer δ-Funktor, und der in nullter Dimension definierte Morphismus besitzt eine eindeutige Fortsetzung in alle Dimensionen. Wir erhalten so die **Corestriktion** als einen Morphismus der Kohomologiegruppen:

$$\mathrm{cor}\colon \mathrm{H}^q(H, f^*A) \longrightarrow \mathrm{H}^q(G, A).$$

9.4 Eigenschaften und Anwendungen der (Co-)Restriktion

Die Zusammenführung von Restriktion und Corestriktion liefert uns nun ein überraschendes und nützliches Resultat:

Satz 9.16. $\mathrm{cor} \circ \mathrm{res} = n \cdot \mathrm{id}$ *als Endomorphismus von* $\mathrm{H}^n(G, A)$.

Beweis. Wir benutzen die Methode des Dimensionsshiftes. Im Grad 0 ist die Behauptung leicht direkt zu verifizieren. Den Induktionsschritt von q nach $(q+1)$ erhält man wie folgt: Die exakte Sequenz

$$0 \longrightarrow A \longrightarrow \mathrm{Ind}^G A_0 \longrightarrow B \longrightarrow 0$$

liefert nach Anwendung von $\mathrm{H}^*(G, -)$ bzw. von $\mathrm{H}^*(H, f^*-)$ ein kommutatives Diagramm langer exakter Sequenzen. Dessen Übergang von der q-ten Spalte zur $(q+1)$-ten hat die Gestalt:

$$\begin{array}{ccccc}
H^q(G,B) & \xrightarrow{\delta} & H^{q+1}(G,A) & \longrightarrow & H^{q+1}(G, Ind^G A_0) = 0 \\
\downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\
H^q(H,B) & \xrightarrow{\delta} & H^{q+1}(H,A) & \longrightarrow & H^{q+1}(H, Ind^G A_0) = 0 \\
\downarrow{\scriptstyle \mathrm{cor}} & & \downarrow{\scriptstyle \mathrm{cor}} & & \downarrow{\scriptstyle \mathrm{cor}} \\
H^q(G,B) & \xrightarrow{\delta} & H^{q+1}(G,A) & \longrightarrow & H^{q+1}(G, Ind^G A_0) = 0
\end{array}$$

Nach Induktionsvoraussetzung ist die Komposition $\mathrm{cor} \circ \mathrm{res} = n \cdot \mathrm{id}$ in der ersten Spalte. Weitherhin kommutiert das Diagramm, da Restriktion und Corestriktion als Morphismen kohomologischer Funktoren mit den δ vertauschen. Die Nullen in der letzten Spalte sind Folge von Shapiros Lemma. Insgesamt folgt so die Behauptung für die $(q+1)$-te Spalte. □

Im Falle einer endlichen Gruppe G liefert dieses Resultat Aufschluss über die Struktur der höheren Kohomologiegruppen:

Korollar 9.17. *Sei G eine endliche Gruppe. Dann ist* $\mathrm{H}^q(G, A)$ *für* $q > 0$ *eine* $|G|$*-Torsionsgruppe.*

Beweis. Obiges für $H = 1$ liefert für $q \geq 1$ das kommutative Diagramm

$$\begin{array}{ccccc}
\mathrm{H}^q(G,A) & \xrightarrow{\mathrm{res}} & \mathrm{H}^q(1,A) = 0 & \xrightarrow{\mathrm{cor}} & \mathrm{H}^q(G,A) \\
& \searrow & & \nearrow{\scriptstyle |G|\cdot \mathrm{id}} & \\
& & & &
\end{array}$$

□

Korollar 9.18. *Ist G endlich und der G-Modul A als abelsche Gruppe endlich erzeugt, so sind die höheren Kohomologiegruppen endliche Torsionsgruppen.*

Beweis. Die Kokettenkonstruktion zeigt, daß auch die höheren Kohomologiegruppen endlich erzeugt sind. Nach dem vorangegangenen Resultat sind sie zudem auch Torsionsgruppen, insgesamt also endlich. □

Unsere bislang erworbenen Resultate finden nun eine praktische Anwendung in der Theorie endlicher Gruppen:

Satz 9.19 (Satz von Schur-Zassenhaus)**.** *Sind A und G zwei endliche Gruppen mit coprimen Ordnungen $m = |A|$ und $n = |G|$, so ist jede Extension von G mit A gespalten, d.h. jeder exakte Sequenz $1 \to A \to E \xrightarrow{\pi} G \to 1$ erlaubt einen Schnitt $s : G \to E$, also $s \circ \pi = \mathrm{id}$.*

Beweis. Ist A abelsch, so führen wir den Beweis mit Hilfe der in Vortrag 1 erläuterten Interpretation von $\mathrm{H}^2(G, A)$ als der Menge der Äquivalenzklassen von Gruppenextensionen von G mit A. Der allgemeine Fall wird sodann mit Hilfe einiger elementarer Resultate aus der Gruppentheorie auf den abelschen Fall zurückgeführt, den wir nun zunächst behandeln.

Die Gruppe $\mathrm{H}^2(G, A)$ wird von $m = \mathrm{H}^2(G, m \cdot \mathrm{id})$ und n, siehe oben, also auch deren größten gemeinsamen Teiler 1 annuliert. Daher ist $\mathrm{H}^2(G, M) = 0$.

Im allgemeinen Falle reicht es zu zeigen, daß E eine Untergruppe B der Ordnung n enthält, denn in diesem Falle ist $B = B/A \cap B \hookrightarrow E/A = G$

Wir zeigen dies durch Induktion nach $m = |A|$: Wähle einen Primteiler $p \mid m$ und eine p-Sylowgruppe $S \subset A$. Als p-Gruppe hat S nichtriviales Zentrum. Sei N der Normalisator von Z in E. Für ein Element $e \in E$ ist eSe^{-1} auch eine p-Sylowgruppe von A, daher nach den Sylowsätzen konjugiert zu S in A. Also gibt es ein $a \in A$, so dass $aSa^{-1} = eSe^{-1}$ und damit $a^{-1}e \in N$ oder $E = AN$. Daher ist $N \twoheadrightarrow G$ surjektiv und n teilt die Gruppenordnung von N.

Indem wir per Induktion E durch N erstzen, dürfen wir daher annehmen, dass E eine normale p-Sylowgruppe S enthält mit $p \mid m$. Per Induktion reicht also der Fall $A = S$, oder per Dévissage für p-Gruppen, der Fall einer abelschen p-Gruppe. Diesen Fall haben wir aber schon oben mittels $\mathrm{H}^2(G, A)$ behandelt. □

Vortrag 10

Kohomologie proendlicher Gruppen

Matthias Erbar
10.1.2006

Proendlich Gruppen tragen eine natürliche Topologie. In diesem Vortrag soll eine Kohomologietheorie entwickelt werden, die diese zusätzliche Struktur berücksichtigt: die stetige Kohomologie. Dazu werden wir Koeffizienten mit stetiger Gruppenoperation betrachten und in Analogie zum bisher Bekannten Kohomologie als derivierte Funktoren des Invariantennehmens auf dieser Kategorie definieren.

Anschließend werden wir die Kohomologie mit stetigen Koketten beschreiben. Als zentrales Resultat erhalten wir die Reduktion der Kohomologie proendlicher Gruppen auf den Fall endlicher Gruppen. Beispielhaft berechnen wir zum Schluß die Kohomologie von $\hat{\mathbb{Z}}$.

10.1 Stetige Kohomologie

Wir halten Folgendes zu proendlichen Gruppen fest: Der projektive Limes

$$(G, g_i) = \varprojlim_i G_i$$

eines gerichteten projektiven Systems endlicher Gruppen $(G_i)_{i\in I}$ heißt **proendliche Gruppe**. Die proendliche Gruppe G trägt die gröbste Topologie bezüglich der die g_i stetig sind; die G_i sind diskret.

Eine topologische Gruppe G ist proendlich, genau dann wennn G kompakt und total unzusammenhängend ist. Die offenen Normalteiler einer proendlichen Gruppe bilden eine Umgebungsbasis der $\mathbf{1}$.

Im Folgenden sei G eine proendliche Gruppe.

Definition 10.1 (diskrete Moduln)**.** $A \in G$-Mod heißt **diskreter G-Modul**, falls die Operation $G \times A \longrightarrow A$ stetig ist, wobei A mit der diskreten Topologie ausgestattet wird. $\mathscr{C}_G$ bezeichne die Kategorie der diskreten G-Moduln, wobei

$$\mathrm{Mor}_{\mathscr{C}_G}(A, B) = \mathrm{Mor}_{G\text{-Mod}}(A, B).$$

Diskrete G-Moduln lassen sich wie folgt charakterisieren.

Lemma 10.2. *Für $A \in G$-Mod gilt:*

$$A \in \mathscr{C}_G \Longleftrightarrow A = \bigcup_{U \lhd_o G} A^U \ ,$$

wobei die Notation $U \lhd_o G$ bedeutet, dass U ein offener Normalteiler in G ist.

Beweis. „⇒“: Sei $a \in A$. Betrachte $f : G \longrightarrow A\ ,\ g \mapsto g.a$ stetig. A diskret $\Rightarrow f^{-1}(a)$ offen $\Rightarrow$ ex. $U \lhd_o G$ mit $U \subseteq f^{-1}(a)\ \Rightarrow a \in A^U$.

„⇐“: Sei $a \in A$. Dann $a \in A^U$ für ein $U \lhd_o G$. Urbild von a unter Operation enthält mit (g, b) auch $Ug \times \{b\}$ offen. $\Rightarrow$ Urbild von a offen $\Rightarrow G \times A \longrightarrow A$ stetig. □

Proposition 10.3. *$\mathscr{C}_G$ ist eine abelsche Kategorie mit genügend Injektiven.*

Beweis. Sei $f \in \mathrm{Mor}_{\mathscr{C}_G}(A, B)$. In G-Mod existiert $\ker f$ und $\operatorname{coker} f$. Diese sind wieder diskret, denn: $G \times \ker f \hookrightarrow G \times A \longrightarrow A$ ist stetig und $G \times B \longrightarrow B \twoheadrightarrow \operatorname{coker} f$ faktorisiert über den topologischen Quotienten $G \times \operatorname{coker} f$ zur stetigen Abbildung $G \times \operatorname{coker} f \longrightarrow \operatorname{coker} f$. Die Gleichung $\operatorname{coker}\ker = \ker\operatorname{coker}$ erben wir von G-Mod. $\Rightarrow \mathscr{C}_G$ ist abelsche Kategorie.

Zu $M \in G$-Mod assoziieren wir: $M^* := \bigcup_{U \lhd_o G} M^U$. M^* ist ein Unter-G-Modul von G, denn: $m_1, m_2 \in M^*, g \in G \Rightarrow m_1 \in M^{U_1}, m_2 \in M^{U_2}$ für $U_1, U_2 \lhd_o G$ geeignet.
$\Rightarrow m_1 + m_2 \in M^{U_1 \cap U_2} \subseteq M^*,\ g.m_1 \in M^{gU_1g^{-1}} \subseteq M^*$. Nach Lemma 10.2. ist $M^* \in \mathscr{C}_G$.

Sei $f \in \mathrm{Hom}_G(M, N)$. Dann gilt $f(M^*) \subseteq N^*$, denn $f\left(M^U\right) \subseteq N^U$, alle $U \lhd_o G$. Wir erhalten also einen Funktor $(-)^* : G\text{-Mod} \longrightarrow \mathscr{C}_G$ und sehen

$$\mathrm{Hom}_G(M, N) = \mathrm{Hom}_{\mathscr{C}_G}(M, N^*)$$

für $M \in \mathscr{C}_G$. Der Funktor $(-)^G$ erhält nun Injektive. Denn: Betrachte folgendes Diagramm mit $M, N \in \mathscr{C}_G,\ I \in G$-Mod injektiv:

$$\begin{array}{ccccc} \mathbf{0} & \longrightarrow & M & \longrightarrow & N \\ & & \downarrow{\scriptstyle f} & & \vdots\ \exists! \\ & & I^* & \hookrightarrow & I \end{array}$$

Fassen wir dieses Diagramm in G-Mod und f als Abbildung nach I auf, so existiert eine eindeutige Fortsetzung von f auf N. Diese hat aber bereits Bild in I^*. Also ist I^* injektiv in $\mathscr{C}_G$.Damit folgt, dass $\mathscr{C}_G$ genügend Injektive besitzt: Sei $M \in \mathscr{C}_G$. Wir finden eine Einbettung $M \hookrightarrow I$ mit I injektiv in G-Mod. Diese hat aber bereits Bild in I^*, injektiv in $\mathscr{C}_G$. □

Da der Invariantenfunktor $(-)^G$ auch in $\mathscr{C}_G$ linksexakt ist, können wir Rechtsderivierte bilden und analog zum bisher Bekannten definieren:

Definition 10.4 (stetige Kohomologie)**.** Sei $A \in \mathscr{C}_G$. $\mathrm{H}^i_{\mathrm{cts}}(G, A) := \mathrm{R}^i(-)^G(A)$ heißen **stetige Kohomologiegruppen** von G mit Koeffizienten in A.

10.2 Beschreibung mit stetigen Koketten

Für konkrete Berechnungen hat sich bereits im Vortrag 4 die Beschreibung der Kohomologie mit inhomogenen Koketten als nützlich erwiesen. Analog wollen wir die stetige Kohomologie als Homologie des Komplexes der stetigen Koketten beschreiben.

Sei $A \in \mathscr{C}_G$. Für $n \geq 0$ definieren wir die stetigen n-Koketten

$$C^n(G, A) := \{f \in \mathrm{Abb}(G^n, A) \mid f \text{ stetig}\},$$

wobei $G^0 = \{1\}$, sowie die Differentiale $d^n : C^n(G,A) \longrightarrow C^{n+1}(G,A)$,

$$d^n f(g_1,\dots,g_{n+1}) := g_1.f(g_2,\cdots,g_{n+1}) + \sum_{i=1}^{n}(-1)^i f(g_1,\dots,g_ig_{i+1},\dots,g_{n+1})$$
$$+(-1)^{n+1} f(g_1,\cdots,g_n).$$

Wir erhalten einen Komplex $C^\bullet(G,A)$ abelscher Gruppen, wie man analog zu Vortrag 4 zeigt, und definieren

$$\mathscr{H}^i(G,A) := \mathrm{H}^i(C^\bullet(G,A)).$$

Bemerkung 10.5. Ist G endlich und diskret, so stellt die Stetigkeit keine zusätzliche Voraussetzung mehr dar und $\mathscr{H}^*(G,-)$ beschreibt die bekannte Kohomologie aus Vortrag 4.

Proposition 10.6. *$\mathscr{H}^*(G,-)$ ist ein kohomologischer δ-Funktor und als solcher isomorph zu $\mathrm{H}^*_{\mathrm{cts}}(G,-)$.*

Beweis. Um zu sehen, dass $\mathscr{H}^*(G,-)$ ein kohomologischer δ-Funktor ist, genügt zu zeigen: $C^n(G,-)$ ist exakt für alle $n \geq 0$. Denn dann erhalten wir aus einer kurzen exakten Sequenz

$$\mathbf{0} \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow \mathbf{0}$$

in $\mathscr{C}_G$ eine kurze exakte Sequenz

$$\mathbf{0} \longrightarrow C^\bullet(G,A) \longrightarrow C^\bullet(G,B) \longrightarrow C^\bullet(G,C) \longrightarrow \mathbf{0}$$

von Komplexen. Das Schlangenlemma liefert eine lange exakte Sequenz

$$\cdots \longrightarrow \mathrm{H}^i(C^\bullet(G,C)) \xrightarrow{\delta} \mathrm{H}^{i+1}(C^\bullet(G,A)) \longrightarrow \cdots$$

und die Funktorialität von δ liefert die gewünschte Kommutativität bei Abbildungen von kurzen exakten Sequenzen in $\mathscr{C}_G$.

Sei also

$$\mathbf{0} \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow \mathbf{0}$$

exakt in $\mathscr{C}_G$, somit auch exakt in G-Mod. Wir erhalten

$$\mathbf{0} \longrightarrow C^n(G,A) \xrightarrow{f\circ} C^n(G,B) \xrightarrow{g\circ} C^n(G,C) \longrightarrow \mathbf{0}.$$

Da f injektiv ist, ist auch $f\circ$ injektiv.

Die Gleichung $\mathrm{im}(f\circ) \subseteq \ker(f\circ)$ ist klar. Sei also $x \in C^n(G,B)$ mit $g \circ x = 0$. Dann hat x Bild in $\ker g = \mathrm{im}\, f$, und es existiert eine eindeutige Abbildung $y : G^{\times n} \to A$ mit $f \circ y = x$. Da A und B diskret sind und f injektiv ist, traegt A die bezüglich f induzierte Toplogogie. Somit ist y stetig, da $f \circ y = x$ stetig ist. Also ist $y \in C^n(G,A)$ ein Urbild von x unter $f\circ$.

Sei nun $z \in C^n(G,C)$. Da g surjektiv ist und die Topologien diskret sind, existiert eine stetige Abbildung von Mengen $k : C \longrightarrow B$ mit $g \circ k = \mathrm{id}_C$, also ein stetiger Schnitt. Mit $y := k \circ z \in C^n(G,B)$ folgt $g \circ y = g \circ k \circ z = z$.

Also ist obige Sequenz exakt und damit $\mathscr{H}^i(G,-)$ ein kohomologischer δ-Funktor.

Zur Isomorphie: Im Grad 0 besteht der natürliche Isomorphismus

$$\mathscr{H}^0(G,A) = \ker d^0 = \{f : \{1\} \longrightarrow A \mid g.f(1) - f(1) = 0,\ \forall\, g \in G\} \cong A^G = H^0_{\mathrm{cts}}(G,A).$$

Da $\mathrm{H}^*_{\mathrm{cts}}(G,-)$ als derivierter Funktor universell ist und $\mathscr{H}^*(G,-)$, wie wir später in Korollar 10.10 sehen, auslöschbar und damit auch universell ist, setzt sich dieser Isomorphismus zu einem Isomorphismus von kohomologischen δ-Funktoren fort. □

10.3 Verträglichkeit mit Limites in der Gruppe und den Koeffizienten

In diesem Abschnitt zeigen wir, wie sich die stetige Kohomologie proendlicher Gruppen auf den Fall endlicher Gruppen zurückführen lässt. Wir werden dies zunächst als Aussage über $\mathscr{H}$ formulieren. Zur Vorbereitung benötigen wir noch folgendes Lemma.

Lemma 10.7. *Seien $(A_i)_{i\in I}$, $(B_i)_{i\in I}$, $(C_i)_{i\in I}$ induktive Systeme abelscher Gruppen und*

$$(A_i) \xrightarrow{(f_i)} (B_i) \xrightarrow{(g_i)} (C_i)$$

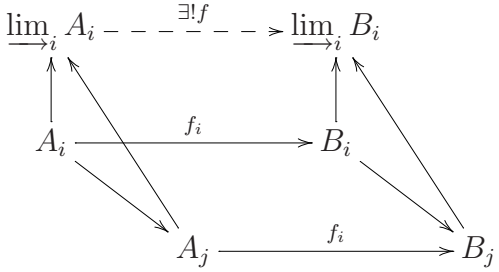
Homomorphismen zwischen diesen Systemen, d.h.:

$$\begin{array}{ccccc} A_i & \xrightarrow{f_i} & B_i & \xrightarrow{g_i} & C_i \\ \downarrow & & \downarrow & & \downarrow \\ A_j & \xrightarrow{f_j} & B_j & \xrightarrow{g_j} & C_j \end{array}$$

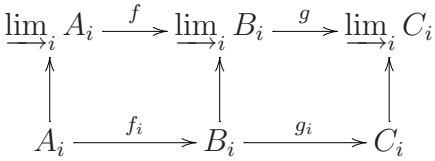
kommutativ für alle $i \le j$. Es sei $A_i \xrightarrow{f_i} B_i \xrightarrow{g_i} C_i$ exakt für alle $i \in I$. Dann erhalten wir eine exakte Sequenz

$$\varinjlim_i A_i \xrightarrow{f} \varinjlim_i B_i \xrightarrow{g} \varinjlim_i C_i$$

Beweis. Die Universelle Eigenschaft des Limes liefert f (analog g), so dass folgende Diagramme kommutieren, alle $i \le j$:



Für die Exaktheit betrachte:



Durch Übergang zu Repräsentanten sieht man: $g \circ f = 0$. Ist $b \in \ker g$, so können wir einen Repräsentanten $b_i \in \ker g_i$ wählen für ein $i \in I$. Dann ex. $a_i \in A_i$ mit $f_i(a_i) = b_i$ und $b = f(a)$, wobei a die Klasse von a_i ist. □

Sei G eine proendliche Gruppe und U offener Normalteiler. Dann ist G/U endlich, denn die Nebenklassen von U bilden eine offene, disjunkte Überdeckung der kompakten Menge

G. Weiter ist G/U diskret in der Quotiententopologie und somit selbst eine proendliche Gruppe. Die $(G/U)_{U\lhd_o G}$ bilden ein projektives System vermöge der Projektionen

$$p_{VU} : G/V \twoheadrightarrow G/U \quad \text{für } V \subseteq U.$$

Es gilt (Beweis am Ende des Abschnitts):

$$G = \varprojlim G/U, \tag{10.1}$$

wobei U die offenen Normalteiler von G durchläuft.

Ist nun $A \in \mathscr{C}_G$, so ist A^U ein G/U-Modul. $\left(A^U\right)_{U\lhd_o G}$ bilden vermöge der Inklusionen

$$i_{VU} : A^U \hookrightarrow A^V \quad \text{für } V \subseteq \mathrm{U}$$

ein induktives System und es gilt (siehe Ende):

$$A = \varinjlim A^U \ . \tag{10.2}$$

Damit bilden auch $\left(C^n\left(G/U, A^U\right)\right)_{U\lhd_o G}$ induktive Systeme vermöge

$$c_{VU} : C^n\left(G/U, A^U\right) \longrightarrow C^n\left(G/V, A^V\right), \ x \longmapsto i_{VU} \circ x \circ p_{VU}^{\times n}.$$

Da die c_{VU} mit den Differentialen kommutieren, erhalten wir induzierte Abbildungen auf der Homologie und damit induktive Systeme $\left(\mathscr{H}^i\left(G/U, A^U\right)\right)_{U\lhd_o G}$.

Wie wir nun sehen, ist $\mathscr{H}$ mit der Limesbildung verträglich.

Theorem 10.8. *Sei $A \in \mathscr{C}_G$. Dann gilt:*

$$\mathscr{H}^i(G, A) \cong \varinjlim \mathscr{H}^i\left(G/U, A^U\right), \quad i \geq 0,$$

wobei U die offenen Normalteiler von G durchläuft.

Beweis. Da die Differentiale Homomorphismen von induktiven Systemen sind, erhalten wir einen Komplex

$$\cdots \longrightarrow \varinjlim C^n\left(G/U, A^U\right) \longrightarrow \varinjlim C^{n+1}\left(G/U, A^U\right) \longrightarrow \cdots \ ,$$

den wir mit $\varinjlim C^\bullet(G/U, A^U)$ bezeichnen. Weiter haben wir Homomorphismen

$$c_U : C^n\left(G/U, A^U\right) \longrightarrow C^n(G, A), \quad x \longmapsto i_U \circ x \circ p_U^{\times n},$$

die mit den c_{VU} kommutieren, und erhalten daraus Homomorphismen

$$\varphi^n : \varinjlim C^n\left(G/U, A^U\right) \longrightarrow C^n(G, A).$$

Da die c_U mit den Differentialen kommutieren, gilt dies auch für die φ^n und wir erhalten

$$\varphi^\bullet : \varinjlim C^\bullet\left(G/U, A^U\right) \longrightarrow C^\bullet(G, A).$$

Dies ist ein Isomorphismus: φ^n injektiv, denn i_U ist injektiv und p_U surjektiv, somit

$$\mathbf{0} \longrightarrow C^n\left(G/U, A^U\right) \xrightarrow{c_U} C^n(G, A)$$

exakt. Mit Lemma 10.7 folgt

$$\mathbf{0} \longrightarrow \varinjlim C^n\left(G/U, A^U\right) \xrightarrow{\varphi^n} C^n(G,A)$$

exakt, wobei das erste und das letzte Objekt als konstante Limiten aufgefasst werden.

Es ist φ^n surjektiv: Sei $x \in C^n(G,A)$. Es genügt zu zeigen, dass $U \lhd_o G$ existiert mit x konstant auf den Nebenklassen von U^n und $\operatorname{im} x \subseteq A^U$. Dann faktorisiert x über eine Abbildung $(G/U)^n \xrightarrow{y} A^U$, d.h. $x = c_U(y)$ und x ist das Bild der Klasse von y unter φ^n.

(1) $n = 1$: A diskret $\Rightarrow$ x lokal konstant $\Rightarrow$ zu $g \in G$ existiert $N_g \lhd_o G$ mit $x|_{gN_g}$ konstant.

$$G = \bigcup_{g\in G} gN_g = \bigcup_{i=1}^{k} g_i N_{g_i} \ , \quad \text{da } G \text{ kompakt.}$$

Sei $N_0 := \bigcap_{i=1}^k N_{g_i} \lhd_o G$ und $g \in G$. Dann ist $gN_0 \subseteq gN_{g_i} \subseteq g_i N_{g_i}$ für ein geeignetes $i \in \{1,\dots,k\}$, also x konstant auf gN_0.

Da A diskret, hat x endliches Bild $\{a_1,\dots,a_m\}$. Es ist $a_i \in A^{N_i}$ für $N_1,\dots,N_m \lhd_o G$ geeignet. $U := \bigcap_{i=0}^m N_i$ ist also der gesuchte Normalteiler.

(2) $n \geq 2$: G^n ist wieder proendlich. Nach (i) existiert $N \lhd_o G^n$ mit x konstant auf Nebenklassen von N. Weiter existieren $U_1,\dots,U_n \lhd_o G$ mit $U_1 \times \cdots \times U_n \subseteq N$. Sei $U := U_1 \cap \cdots \cap U_n$, dann ist x konstant auf den Nebenklassen von U^n und durch evtl. Verkleinerung wie in (i) folgt $\operatorname{im} x \subseteq A^U$.

Die Abbildung $\varphi^\bullet$ induziert also einen Isorphismus

$$\mathscr{H}^i(G,A) = H^i(C^\bullet(G,A)) \cong \mathrm{H}^i(\varinjlim C^\bullet\left(G/U, A^U\right)).$$

Da, wie gesehen, der induktive Limes Exaktheit an jeder Stelle erhält, ist er verträglich mit der Bildung von Kernen und Cokernen und damit mit dem Übergang zur Homologie. Also ist

$$\mathscr{H}^i(G,A) \cong \mathrm{H}^i\left(\varinjlim C^\bullet\left(G/U, A^U\right)\right) \cong \varinjlim \mathrm{H}^i\left(C^\bullet\left(G/U, A^U\right)\right) = \varinjlim \mathscr{H}^i\left(G/U, A^U\right).$$

□

Definition 10.9. Sei A eine abelsche Gruppe. Der **stetige coinduzierte Modul** zu A ist

$$\mathrm{Cts}(G,A) := \{f \in \mathrm{Abb}(G,A) \text{ stetig}\}$$

mit der G-Operation $(g.f)(g') := f(g'g)$.

$\mathrm{Cts}(G,A)$ ist ein diskreter G-Modul, denn wir haben eben gesehen, dass zu jedem $x \in \mathrm{Abb}(G,A)$ stetig ein $U \lhd_0 G$ existiert, so dass x auf den U-Nebenklassen konstant ist, d.h. $(u.x)(g) = x(gu) = x(g)$, alle $u \in U, g \in G$. Also $x \in \mathrm{Cts}(G,A)^U$ und damit

$$\mathrm{Cts}(G,A) = \bigcup_{U \lhd_o G} \mathrm{Cts}(G,A)^U.$$

Korollar 10.10. *$\mathscr{H}^*(G,-)$ ist auslöschbar.*

Beweis. Sei A abelsche Gruppe und $U \lhd_o G$. Dann ist

$$\mathrm{Cts}(G,A)^U = \{x \in \mathrm{Cts}(G,A) \mid x \text{ konst. auf NK von } U\} = \mathrm{Abb}(G/U, A) = \mathrm{Ind}(G,A).$$

Damit folgt für $i > 0$:

$$\mathscr{H}^i(G, \mathrm{Cts}(G,A)) \cong \varinjlim \mathscr{H}^i\left(G/U, \mathrm{Cts}(G,A)^U\right) = \varinjlim \mathscr{H}^i(G/U, \mathrm{Ind}(G/U, A)) = \mathbf{0},$$

da die übliche Kohomologie endlicher Gruppen durch induzierte Moduln ausgelöscht wird. □

Bemerkung 10.11. Korollar 10.10 schließt die Lücke im Beweis von Proposition 10.6. Somit können wir $\mathscr{H}^*(G,-)$ und $\mathrm{H}^*_{\mathrm{cts}}(G,-)$ identifizieren und erhalten so die gewünschte Reduktionsaussage über die stetige Kohomologie.

Beweis von (10.1). Die Projektionen $G \overset{p_U}{\twoheadrightarrow} G/U$ induzieren einen Homomorphismus

$$\varphi : G \longrightarrow \varprojlim G/U \quad \text{mit} \quad \begin{array}{ccc} G & \xrightarrow{\varphi} & \varprojlim G/U \\ & \searrow^{p_U} & \downarrow \\ & & G/U \end{array} \quad \text{kommutativ, alle } U.$$

Dieser ist ein Isomorphismus.

Injektivität: Sei $\mathbf{1} \neq g \in G$. Da G hausdorffsch, ist $G - \{g\}$ offen und es ex. $U \lhd_o G$ mit $U \subseteq G - \{g\}$. $\Rightarrow gU \neq \mathbf{1}$ in $G/U \Rightarrow \varphi(g) \neq \mathbf{1}$.

Surjektivität: Sei $x = (x_U)_U \in \varprojlim G/U$. Es genügt zu zeigen:

$$\bigcap_U p_U^{-1}(x_U) \neq \emptyset.$$

Da $p_U^{-1}(x_U)$ abgeschlossen und G kompakt, genügt zu zeigen:

$$\bigcap_{i=1}^{n} p_{U_i}^{-1}(x_{U_i}) \neq \emptyset \ , \text{ für endlich viele } U_1, \ldots, U_n.$$

Sei $U_0 := \bigcap_{i=1}^n U_i \lhd_o G$ und $g \in p_{U_0}^{-1}(x_{U_0})$. Dann ist $p_{U_i}(g) = x_{U_i}$, alle $i = 1, \ldots, n$. □

Beweis von (10.2). Die Inklusionen $A^U \overset{i_U}{\hookrightarrow} A$ induzieren einen Homomorphismus

$$\psi : \varinjlim A^U \longrightarrow A \quad \text{mit} \quad \begin{array}{ccc} \varinjlim A^U & \xrightarrow{\psi} & A \\ & \nwarrow & \uparrow{\scriptstyle i_U} \\ & & A^U \end{array} \quad \text{kommutativ, alle } U.$$

Dieser ist ein Isomorphismus.

Injektivität: Sei $x \in \ker \psi$ und $x_U \in A^U$ ein Repräsentant.$\Rightarrow i_U(x_U) = \mathbf{0} \Rightarrow x_U = \mathbf{0}$ $\Rightarrow x = \mathbf{0}$.

Surjektivität: Sei $a \in A$. Nach Lemma 10.2 existiert $U \lhd_o G$ mit $a \in A^U$. Dann ist a Bild seiner Klasse in $\varinjlim A^U$. □

10.4 Interpretation in niedrigen Dimensionen

Die Beschreibung mit stetigen Koketten liefert uns analog zu Vortrag 4 eine Interpretation der stetigen Kohomologie in Dimension 0, 1 und 2.

$$\begin{aligned} \mathrm{H}^0_{\mathrm{cts}}(G,A) &= A^G, \\ \mathrm{H}^1_{\mathrm{cts}}(G,A) &= \{\text{stetige 1-Kozykel}\}/\{\text{stetige 1-Koränder}\}, \\ \mathrm{H}^2_{\mathrm{cts}}(G,A) &= \{\text{stetige 2-Kozykel}\}/\{\text{stetige 2-Koränder}\}. \end{aligned}$$

Für triviale G-Aktion auf den Koeffizienten A gilt insbesondere

$$\mathrm{H}^1_{\mathrm{cts}}(G,A) = \mathrm{Hom}_{\mathrm{stetig}}(G,A).$$

Analog zu Vortrag 1 kann man damit stetige Kohomologie in Graden 1 (bzw. 2) mit den Äquivalenzklassen von stetigen Spaltungen von stetigen semidirekten Produkten (bzw. stetigen Extensionen) identifizieren. Einzig die Existenz eines stetigen mengentheoretischen Schnitts wird noch benötigt, siehe [Ser94] I.1.2 Prop 1.

10.5 Inflation, Restriktion, Corestriktion

Analog zu Vortrag 9 werden wir nun Inflation, Restriktion und Corestriktion für die stetige Kohomologie definieren.

Sei $\varphi : G' \longrightarrow G$ ein stetiger Homomorphismus von proendlichen Gruppen und $A \in \mathscr{C}_G$. Dann wird A diskreter G'-Modul vermöge $g'.a := \varphi(g').a$, bezeichnet mit $\varphi^* A$. Da der Funktor $\varphi^* : \mathscr{C}_G \longrightarrow C_{G'}$ exakt, ist $\mathrm{H}^*_{\mathrm{cts}}(G', \varphi^*(-))$ ein kohomologischer δ-Funktor. Im Grad 0 besteht die natürliche Transformation

$$\mathrm{H}^0_{\mathrm{cts}}(G,A) = A^G \hookrightarrow (\varphi^* A)^{G'} = \mathrm{H}^0_{\mathrm{cts}}(G', \varphi^* A).$$

Diese setzt sich wegen der Universalität von $\mathrm{H}^*_{\mathrm{cts}}(G,-)$ zu einem Morphismus von kohomologischen δ-Funktoren fort und liefert insbesondere Homomorphismen

$$\mathrm{H}^i_{\mathrm{cts}}(G,A) \longrightarrow \mathrm{H}^i_{\mathrm{cts}}(G', \varphi^* A), \quad i \geq 0.$$

Sei nun $A' \in C_{G'}$ und $f : A \longrightarrow A'$ ein Homomorphismus abelscher Gruppen.

Das Paar (φ, f) heißt kompatibel, falls $f : \varphi^* A \longrightarrow A'$ ein G'-Modulhomomorphismus ist.

f induziert dann Homomorphismen auf den Kohomologiegruppen und wir erhalten zu einem kompatiblen Paar (φ, f) durch Verkettung mit den obigen folgende Homomorphismen:

$$\mathrm{H}^i_{\mathrm{cts}}(G,A) \longrightarrow \mathrm{H}^i_{\mathrm{cts}}(G', A'), \quad i \geq 0.$$

Anwendung:

(1) $H \subseteq G$ abgeschlossene Untergruppe und $A \in \mathscr{C}_G$. Dann ist H selbst proendlich, nämlich wieder kompakt und total unzusammenhängend, und $H \hookrightarrow G$, id_A sind kompatibel. Wir erhalten daraus die Restriktion

$$\mathrm{res}^G_H : \mathrm{H}^i_{\mathrm{cts}}(G,A) \longrightarrow \mathrm{H}^i_{\mathrm{cts}}(H,A), \quad i \geq 0.$$

(2) $N \subseteq G$ abgeschlossener Normalteiler und $A \in \mathscr{C}_G$. Dann ist G/N wieder proendlich. A^N ist diskreter G/N-Modul und $G \twoheadrightarrow G/N,\ A^N \hookrightarrow A$ sind kompatibel. Wir erhalten die Inflation

$$\inf_G^{G/N} : \mathrm{H}^i_{\mathrm{cts}}\left(G/N, A^N\right) \longrightarrow \mathrm{H}^i_{\mathrm{cts}}(G, A), \quad i \geq 0.$$

Die Corestriktion entsteht auf etwas andere Weise und existiert nur für offene Untergruppen: Sei $H \subseteq G$ offene Untergruppe. Dann hat H endlichen Index in G und ist selbst proendlich, nämlich wieder quasikompakt, Hausdorffsch und total unzshg. Für $A \in \mathscr{C}_G$ haben wir die Normabbildung

$$N_{G/H} : A^H \longrightarrow A^G \ , \ \ a \longmapsto \sum_{s \in G/H} s.a \ .$$

Bezeichnet $\varphi : H \hookrightarrow G$ die Inklusion, so liefert dies die natürliche Transformation

$$\mathrm{H}^0_{\mathrm{cts}}(H, \varphi^* A) = A^H \overset{N_{G/H}}{\longrightarrow} A^G = \mathrm{H}^0_{\mathrm{cts}}(G, A).$$

Lemma 10.12. $\mathrm{H}^*_{\mathrm{cts}}(H, \varphi^*(-))$ *ist auslöschbar und damit universell.*

Beweis. Sei M abelsche Gruppe. Wir haben einen Isomorphismus von H-Moduln:

$$\varphi^* \operatorname{Cts}(G, M) \longrightarrow \operatorname{Cts}(H, \operatorname{Abb}(G/H, M)) \ , \ \ x \longmapsto (h \longmapsto (g_i \longmapsto x(g_i h))) \ ,$$

wobei $(g_i)_{i=1,\ldots,k}$ ein fest gewähltes Repräsentantensystem von G/H ist.
Wir erhalten induzierte Isomorphismen

$$\mathrm{H}^i_{\mathrm{cts}}(H, \varphi^* \operatorname{Cts}(G, M)) \cong \mathrm{H}^i_{\mathrm{cts}}(H, \operatorname{Cts}(H, \operatorname{Abb}(G/H, M))) = \mathbf{0}, \quad i \geq 0.$$

□

Als eindeutige Fortsetzung von $N_{G/H}$ erhalten wir die Corestriktion

$$\mathrm{cor}^G_H : \mathrm{H}^i_{\mathrm{cts}}(H, A) \longrightarrow \mathrm{H}^i_{\mathrm{cts}}(G, A), \quad i \geq 0.$$

10.6 Die Kohomologie von $\hat{\mathbb{Z}}$

Die Gruppe $\hat{\mathbb{Z}}$ ist die Vervollständigung von $\mathbb{Z}$:

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \ .$$

Die Projektionen $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ liefern einen kanonischen Homomorphismus $\mathbb{Z} \longrightarrow \hat{\mathbb{Z}}$. Wir setzen $\mathfrak{g} := \hat{\mathbb{Z}}$ und $\mathfrak{g}_n := n\hat{\mathbb{Z}}$. Es ist $\mathfrak{g}_n = \ker(\mathfrak{g} \longrightarrow \mathbb{Z}/n\mathbb{Z})$ und daher $\mathfrak{g}/\mathfrak{g}_n \cong \mathbb{Z}/n\mathbb{Z}$, d.h. $\mathfrak{g}/\mathfrak{g}_n$ ist zyklisch von der Ordnung n und erzeugt vom Bild der 1.

Die Gruppen $(\mathfrak{g}_n)_n$ sind gerade die offenen Untergruppen von $\mathfrak{g}$: Sei $H \subseteq \mathfrak{g}$ offene Untergruppe. Dann $[\mathfrak{g} : H] = n < \infty$ für ein $n \in \mathbb{N}$. $\Rightarrow n(zH) = 0$ in $\mathfrak{g}/H$, alle $z \in \mathfrak{g} \Rightarrow \mathfrak{g}_n \subseteq H$.

Aber $\mathfrak{g}/H \cong (\mathfrak{g}/\mathfrak{g}_n)/(H/\mathfrak{g}_n)$ und $[\mathfrak{g} : H] = n = [\mathfrak{g}/\mathfrak{g}_n]$. $\Rightarrow H = \mathfrak{g}_n$. Wir können also schreiben:

$$\mathfrak{g} = \varprojlim_n \mathfrak{g}/\mathfrak{g}_n.$$

Ist nun $A \in C_\mathfrak{g}$, so haben wir einen Automorphismus F von A durch $F(a) = 1.a$. Wir setzten $N_n := (\mathrm{id} + F + \cdots + F^{n-1})$, für $n \in \mathbb{N}$.

Mit Hilfe von Theorem 10.8 und der Kenntnis der Kohomologie endlicher zyklischer Gruppen, können wir nun die Kohomologiegruppen von $\mathfrak{g}$ berechnen.

Proposition 10.13. *Sei $A' = \{a \in A \mid \exists\, n \text{ mit } N_n(a) = 0\}$. Dann gilt:*

$$\mathrm{H}^1_{\mathrm{cts}}(\mathfrak{g}, A) = A'/(F - \mathrm{id})A.$$

Beweis. Nach Vortrag 4 ist $\mathrm{H}^1_{\mathrm{cts}}(\mathfrak{g}/\mathfrak{g}_n, A^{\mathfrak{g}_n}) = \ker N_n/(F - \mathrm{id})A^{\mathfrak{g}_n}$. Die Behauptung folgt nun durch Übergang zum Limes:
Da die Inklusionen $\ker N_n/(F - \mathrm{id})A^{\mathfrak{g}_n} \hookrightarrow A'/(F - \mathrm{id})A$ mit den Transferabbildungen kommutieren, erhalten wir einen Homomorphismus

$$\varinjlim_n \mathrm{H}^1_{\mathrm{cts}}(\mathfrak{g}/\mathfrak{g}_n, A^{\mathfrak{g}_n}) \longrightarrow A'/(F - \mathrm{id})A.$$

Dieser ist offensichtlich injektiv und ferner surjektiv, denn:
Sei $a \in A'$. Dann existiert n mit $a \in A^{\mathfrak{g}_n}$ und $N_n(a) = 0$ und $a((F - \mathrm{id})A)$ ist Bild der Klasse von $a((F - \mathrm{id})A^{\mathfrak{g}_n})$ im Limes. Somit haben wir

$$\mathrm{H}^1_{\mathrm{cts}}(\mathfrak{g}, A) \cong \varinjlim_n \mathrm{H}^1_{\mathrm{cts}}(\mathfrak{g}/\mathfrak{g}_n, A^{\mathfrak{g}_n}) \cong A'/(F - \mathrm{id})A$$

□

Proposition 10.14. *Ist $A \in C_\mathfrak{g}$ endlich, so gilt:*

$$\mathrm{H}^2_{\mathrm{cts}}(\mathfrak{g}, A) = \mathbf{0}.$$

Beweis. Es ist $\mathrm{H}^2_{\mathrm{cts}}(\mathfrak{g}/\mathfrak{g}_n, A^{\mathfrak{g}_n}) = (A^{\mathfrak{g}_n})^{\mathfrak{g}/\mathfrak{g}^n}/N_n A^{\mathfrak{g}_n} = A^\mathfrak{g}/N_n A^{\mathfrak{g}_n}$
Die Transferabbildungen $A^\mathfrak{g}(N_n A^{\mathfrak{g}_n}) \longrightarrow A^\mathfrak{g}/N_{nm}A^{\mathfrak{g}_{nm}}$ sind induziert durch Multiplikation mit m.
Sei nun m ein Vielfaches der Ordnung von A. Sei $a \in \varinjlim_n A^\mathfrak{g}/N_n A^{\mathfrak{g}_n}$ und $a_n \in A^\mathfrak{g}/N_n A^{\mathfrak{g}_n}$ ein Repräsentant. a_n wird 0 in $A^\mathfrak{g}/N_{nm}A^{g_{nm}}$, also ist $a = 0 \in \varinjlim_n A^\mathfrak{g}/N_{nm}A^{g_{nm}}$. Somit ist $\mathrm{H}^2_{\mathrm{cts}}(\mathfrak{g}/\mathfrak{g}_n, A^{\mathfrak{g}_n}) = \mathbf{0}$ und folglich

$$\mathrm{H}^2_{\mathrm{cts}}(\mathfrak{g}, A) = \varinjlim_n \mathrm{H}^2_{\mathrm{cts}}(\mathfrak{g}/\mathfrak{g}_n, A^{\mathfrak{g}_n}) = \mathbf{0}.$$

□

Vortrag 11

Galoiskohomologie

Franz-Benjamin Mocnik
17.1.2006

Es ist ein Anliegen der Mathematiker, Galoiserweiterungen besser zu verstehen. In der Galoistheorie vergleicht man Galoiserweiterungen mit der Galoisgruppe. Die Kummertheorie und die Artin-Schreier Theorie vergleichen abelsche Galoiserweiterungen mit dem Körper selber.

Um die Kummertheorie und die Artin-Schreier Theorie entwickeln zu können, greifen wir auf das Konzept der Gruppenkohomologie zurück. So erhalten wir die wesentlichen Resultate relativ einfach. In diesem Sinne stimmt das folgende Zitat bezogen auf die Gruppenkohomologie:

Die Algebra ist großzügig – oft gibt sie mehr, als wonach man gefragt hat.

Jean d'Alembert (1717-1783)

11.1 Galoistheorie

Sei L ein Körper und $K \subset L$ ein UnterkörperUnterkoerper@Unterkörper. Dann nennen wir das Tupel $L|K$ eine *Körpererweiterung*. Als den Grad $[L|K]$ von L über K bezeichnen wir die Dimension von L als K-Vektorraum.

Wir werden Körpererweiterungen im Folgenden näher studieren. Dazu müssen wir uns jedoch auf Körpererweiterungen $L|K$ beschränken, bei denen L und K in einem noch näher zu definierendem Sinne nahe aneinander liegen. Sonst enthält L zu viel zusätzliche Struktur um eine hilfreiche Beschreibung der Unterschiede von L und K zu finden.

Im Folgenden werden wir deshalb Körpererweiterungen mit bestimmten Eigenschaften benennen:

Definition 11.1 (Algebraische Körpererweiterung)**.** (1) Ein Element $\alpha \in L$ heißt **algebraisch über K**, falls der Homomorphismus $\sigma_\alpha : K[X] \to L$, der X auf α schickt und K elementweise fix lässt einen nichtleeren Kern besitzt. Da $K[X]$ ein Hauptidealring ist, wird $\ker \sigma_\alpha$ von einem Polynom $p(X) \in K[X]$ erzeugt. Dieses Polynom $p(X)$ sei o.B.d.A. normiert. Dann nennt man $p(X)$ das **Minimalpolynom** von α.

(2) Eine Körpererweiterung $L|K$ heißt **algebraisch**, falls alle Elemente aus L algebraisch über K sind. Als einen **algebraische Abschluss** K^{alg} eines Körpers K bezeichnen wir einen maximalen Körper K^{alg}, so dass $K^{\text{alg}}|K$ algebraisch ist. Dieser existiert und ist bis auf Isomorphie eindeutig.

Definition 11.2 (Kompositum)**.** Das **Kompositum** endlich vieler Körper $K_1, \ldots, K_n$ ist ein minimaler Körper L, der $K_1, \ldots, K_n$ enthällt. Dieser exisitiert und ist bis auf Isomorphie eindeutig.

Definition 11.3 (Normale Körpererweiterung)**.** Wir nennen L einen **Zerfällungskörper** eines Polynoms $p(X) \in K[X]$ über dem Körper K, falls $p(X)$ über L in Linearfaktoren zerfällt und L mit dieser Eigeschaft minimal ist. Ein Zerfällungskörper eines Polynoms ist bis auf Isomorphie eindeutig.

Eine Körpererweiterung $L|K$ heißt **normal**, falls L Kompositum einer Familie von Zerfällungskörpern von Polynomen über K ist.

Definition 11.4 (Separable Körpererweiterung)**.** Ein Element α in L heißt **separabel** über K, falls sein Minimalpolynom $p(X) \subset K[X]$ keine mehrfachen Nullstellen besitzt.

Eine Körpererweiterung $L|K$ heißt **separabel**, falls jedes Element L separabel ist. Als einen **separablen Abschluss** K^{sep} eines Körpers K bezeichnen wir einen maximalen Körper K^{sep}, so dass $K^{\text{sep}}|K$ separabel ist. Dieser existiert und ist bis auf Isomorhpie eindeutig.

Definition 11.5 (Galoiserweiterungen[1])**.** Eine Körpererweiterung $L|K$ heißt **galoissch**, falls sie normal und separabel ist.

Die **Galoisgruppe** $\text{Gal}(L|K) \equiv \text{Gal}_{L|K}$ ist die Gruppe aller Automorphismen von L, die K elementweise fix lassen. Die Galoisgruppe $\text{Gal}(K^{\text{sep}}|K) \equiv \text{Gal}_K$ nennen wir die **absolute Galoisgruppe**.

Falls die Galoisgruppe einer Galoiserweiterung abelsch/zyklisch ist, so sprechen wir von einer **abelschen/zyklischen Erweiterung**. Eine Galoiserweiterung $L|K$ heißt **vom Exponenten** n, falls die Galoisgruppe $\text{Gal}(L|K)$ vom Exponent n ist, d.h. $\sigma^n = 1$ für alle $\sigma \in \text{Gal}(L|K)$.

Lemma 11.6. *Jede Galoiserweiterung von K lässt sich in einen gegebenen algebraischen Abschluss $K^{\text{alg}}|K$ einbetten.*

Wir werden deshalb im Folgenden immer die Situation $K^{\text{alg}}|L|K$ betrachten.

Satz 11.7. *Sei $L|K$ eine endliche Galoiserweiterung. Dann gilt*

$$\#\,\text{Gal}_{L|K} = [L : K] < \infty.$$

Lemma 11.8. *Sei $L|K$ eine Galoiserweiterung. Dann ist die Galoisgruppe pro-endlich.*

Theorem 11.9 (Hauptsatz der Galoistheorie)**.** *Sei $L|K$ eine Galoiserweiterung. Dann gibt es eine Bijektion zwischen den Teilerweiterungen $L|E|K$ und den abgeschlossenen Untergruppen der Galoisgruppe* $\text{Gal}_{L|K}$*:*

$$\left\{ \begin{array}{c} L|E|K \\ \textit{Teilerweiterung} \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} A \subset \text{Gal}(L|K) \\ \textit{abgeschlossene Untergruppe} \end{array} \right\}$$

$$\begin{array}{ccc} E & \longmapsto & \text{Gal}(L|E) \\ L^A & \longleftarrow & A. \end{array}$$

[1]Evariste Galois (1811-1832), französischer Mathematiker

11.2 Abelsche Garben

In diesem Abschnitt wollen wir eine einfache Notation für Koeffizienten von Galoiskohomologiegruppen einführen. Dazu definieren wir den Begriff einer abelschen Garbe auf der Kategorie der endlichen, separablen Teilerweiterungen einer Galoiserweiterung $L|K$ und rechtfertigen in einem Lemma die daraus folgende kurze Schreibweise. Der Vorteil dieser Schreibweise beruht darauf, dass man in Untersuchungen der Galoiskohomologie oftmals den Körper variiert und dann die Koeffitzienten nicht umständlich diesem Körperwechsel, der ja ein Gruppenwechsel ist, anpassen muss.

Definition 11.10 (Kategorie der endlichen, separablen Teilerweiterungen)**.** Sei $L|K$ eine Galoiserweiterung. Die **Kategorie der endlichen, separablen Teilerweiterungen** von $L|K$, geschrieben $\mathscr{B}_{L|K}$, wird definiert durch:

(i) Die Objekte

$$\mathrm{Ob}(\mathscr{B}_{L|K}) = \{E|K \text{ endlich, separabel} \mid \exists\, E \hookrightarrow L \text{ über } K\}.$$

(ii) Die Morphismen

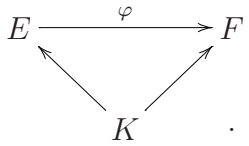
$$\mathrm{Mor}(E,F) = \mathrm{Hom}_K(E,F)$$

mit der üblichen Verknüpfung

$$\mathrm{Hom}_K(E,F) \times \mathrm{Hom}_K(D,E) \longrightarrow \mathrm{Hom}_K(D,F).$$

Notation 11.11. Wir wollen an Stelle $\mathscr{B}_{K^{\mathrm{sep}}|K}$ verkürzend $\mathscr{B}_K$ schreiben.

Bemerkung 11.12. Bei der Definition der Objekte wird nur die Existenz einer Einbettung in L gefordert. Diese gehört jedoch nicht mit zum Objekt selber. Bei der Definition der Morphismen müssen die Homomorphismen deshalb auch nicht kompatibel mit „einer Einbettung“ nach L sein. Es wird also lediglich gefordert, dass das folgende Diagramm kommutiert:



Definition 11.13 (Fixmodulfunktor einer Galoiserweiterung)**.** Sei $L|K$ eine Galoiserweiterung. Dann definieren wir den **Fixmodulfunktor** von $L|K$ als den Funktor

$$\begin{array}{rccc} (-)^{\mathrm{Gal}(L|K)}: & G\text{-Mod} & \longrightarrow & G\text{-Mod} \\ & M & \longmapsto & M^{\mathrm{Gal}(L|K)}, \end{array}$$

der jeden G-Modul M auf den Fixmodul unter der Galoisgrupe $\mathrm{Gal}(L|K)$ schickt.

Definition 11.14 (Abelsche Garbe)**.** Eine **abelsche Garbe** auf der Kategorie der endlichen, separablen Teilwerweiterungen $\mathscr{B}_{L|K}$ mit Werten in der Kategorie der abelschen Gruppen $\mathscr{A}$ ist ein Funktor

$$\begin{array}{rccc} A: & \mathscr{B}_{L|K} & \longrightarrow & \mathscr{A} \\ & E & \longmapsto & A_E, \end{array}$$

der folgende Eigenschaften erfüllt:

(i) Für jede Inklusion $\varphi : E \hookrightarrow F$ in $\mathscr{B}_{L|K}$ ist $A(\varphi) : A_E \hookrightarrow A_F$ eine Inklusion.

(ii) Für jede Inklusion $\varphi : E \hookrightarrow F$ mit $F|E$ galoissch gilt

$$A_E = (A_F)^{\mathrm{Gal}_{F|E}}.$$

Die Gleichheit ist dabei im Sinn der Inklusion $A(\varphi) : A_E \hookrightarrow A_F$ zu verstehen.

Definition 11.15 (Kategorie der abelschen Garben)**.** Die **Kategorie der abelschen Garben** auf $\mathscr{B}_{L|K}$ mit Werten in $\mathscr{A}$ wird definiert durch:

- Die Objekte sind die abelschen Garben auf $\mathscr{B}_{L|K}$ mit Werten in $\mathscr{A}$.
- Die Morphismen in $\mathrm{Mor}(A, B)$ sind die natürlichen Transformationen $\eta : A \to B$, d.h. die Abbildungen, die jeder Teilerweiterung $E \in \mathscr{B}_{L|K}$ einen Gruppenhomomorphismus $\eta_E : A_E \to B_E$ zuordnet, so dass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} A_E & \hookrightarrow & A_F \\ {\scriptstyle \eta_E}\downarrow & & \downarrow{\scriptstyle \eta_F} \\ B_E & \hookrightarrow & B_F. \end{array}$$

Satz 11.16. *Es gilt die folgende Kategorienäquivalenz:*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{abelsche Garben} \\ \textit{auf } \mathscr{B}_{L|K} \end{array} \right\} & \overset{1:1}{\longleftrightarrow} & \left\{ \begin{array}{c} \textit{diskrete} \\ \mathrm{Gal}_{L|K}\textit{-Moduln} \end{array} \right\} \\ A & \overset{\varphi}{\longmapsto} & \varinjlim_E A_E =: A_L \\ A_E := \mathrm{Abb}_{\mathrm{Gal}_{L|K}}(\mathrm{Hom}_K(E, L), M) & \overset{\psi}{\longmapsto} & M, \end{array}$$

wobei der Limes über alle Teilerweiterungen $L|E|K$ gebildet wird, so dass $E|K$ endlich und galoisch ist und alle Transferabbildungen mit der Einbettung in L verträglich sind.

Beweis. Zunächst stellen wir fest, dass die Teilerweiterungen $L|E|K$ derart, dass $E|K$ endlich und galoissch ist und alle Transferabbildungen mit der Einbettung in L verträglich sind, ein gerichtetes Indexsystem bilden.

Bezeichne nun $\imath : E \to L$ eine Inklusion. Die Zuordnung

$$\mathrm{Abb}_{\mathrm{Gal}_{L|K}}(\mathrm{Hom}_K(E, L), M)) \longrightarrow M\ , \qquad ((\imath : E \longrightarrow L) \longmapsto m) \longmapsto m$$

beschränkt sich im Bild auf $M^{\mathrm{Gal}_{L|E}}$, denn es gilt im Fall einer galoisschen Erweiterung

$$\mathrm{Hom}_K(E, L) = \mathrm{Gal}_{L|K} \,/\, \mathrm{Gal}_{L|E}\,. \tag{$*$}$$

Im Fall einer nicht-galoisschen Erweiterung ist dieser Ausdruck als Menge der Nebenklassen zu verstehen. Dies folgt unmittelbar daraus, dass jeder K-Homomorphismus von E nach L die Einschränkung eines K-Automorphismus von L ist. Wir erhalten bzgl. der gewählten Inklusion $\imath : E \to L$ also einen Isomorphismus

$$\mathrm{Abb}_{\mathrm{Gal}_{L|K}}(\mathrm{Hom}_K(E, L), M)) \cong M^{\mathrm{Gal}_{L|E}}.$$

Es genügt zum Nachweis der Kategorienequivalenz zu zeigen, dass die Funktoren zueinander invers sind:

Sei M ein diskreter $\mathrm{Gal}_{L|K}$-Modul. Dieser wird unter $\varphi \circ \psi$ abgebildet auf

$$\varinjlim_{E} M^{\mathrm{Gal}_{L|E}} = M.$$

Sei umgekehrt A eine abelsche Garbe auf $\mathscr{B}_{L|K}$. Diese wird unter $\psi \circ \varphi$ abgebildet auf die abelsche Garbe B mit

$$B_E = \mathrm{Abb}_{\mathrm{Gal}_{L|K}}(\mathrm{Hom}_K(E, L), A_L) = (A_L)^{\mathrm{Gal}_{L|E}} = A_E.$$

Die zweite Gleichheit gilt wegen $(*)$. □

Sei $L|K$ eine Galoiserweiterung. Wir wollen die Kohomologiegruppe der Galoisgruppe $\mathrm{Gal}_{L|K}$ mit Koeffizienten in einem abelschen $\mathrm{Gal}_{L|K}$-Modul M untersuchen:

$$\mathrm{H}^q(\mathrm{Gal}_{L|K}, M).$$

Wir können solche $\mathrm{Gal}_{L|K}$-Moduln notieren, indem eine abelsche Garbe $A : \mathscr{B}_{K^{\mathrm{sep}}|K} \to \mathscr{A}$ auf die Teilerweiterung $L|K$ anwenden. So können wir $\mathrm{Gal}_{L|K}$-Moduln auf einfache Weise beschreiben.

Lemma 11.17. *Seien $L_i|K_i$, $i = 1, 2$ zwei Galoiserweiterungen. Sei $\imath : K_1 \to K_2$ eine Injektion. Es existiere eine Fortsetzung $\jmath : L_1 \to L_2$, die ebenfalls eine Injektion ist. Dann erhalten wir einen Homomorphismus*

$$\mathrm{H}^q(\mathrm{Gal}_{L_1|K_1}, A_{L_1}) \longrightarrow \mathrm{H}^q(\mathrm{Gal}_{L_2|K_2}, A_{L_2}),$$

die nur von $\imath$ abhängig ist.

Beweis. Die Injektion $\jmath$ liefert einen Homomorphismus $\mathrm{Gal}(L_2|K_2) \to \mathrm{Gal}(L_1|K_1)$ durch die Einschränkung und eine Injektion $A_{L_1} \to A_{L_2}$. Diese sind kompatibel. Somit erhalten wir einen Morphismus

$$\mathrm{H}^q(\mathrm{Gal}_{L_1|K_1}, A_{L_1}) \longrightarrow \mathrm{H}^q(\mathrm{Gal}_{L_2|K_2}, A_{L_2}).$$

Dieser Morphismus ist von der Wahl von $\jmath$ unabhängig, denn zwei mögliche $\jmath$ unterscheiden sich nur durch Konjugation mit einem $\sigma \in G(L_2|K_2)$. In Vortrag 9 wurde gezeigt, dass $\mathrm{Gal}(L_2|K_2)$ jedoch trivial auf $\mathrm{H}^q(\mathrm{Gal}(L_2|K_2), M)$ für jeden $\mathrm{Gal}(L_2|K_2)$-Modul M operiert. □

Korollar 11.18. *Die Kohomologiegruppe der absoluten Galoisgruppe*

$$\mathrm{H}^q(\mathrm{Gal}_{K^s|K}, A(K^s|K))$$

ist bis auf Isomorphie von der Wahl des separablen Abschlusses unabhängig.

Beweis. Offensichtlich. □

Nun können wir die Notation der Kohomologie der Galoisgruppe verkürzen:

Notation 11.19. Sei A eine abelsche Garbe auf $\mathscr{B}_K$. Dann schreiben wir für eine Galoiserweiterung $L|K$ verkürzend:

$$\mathrm{H}^q(L|K, A) := \mathrm{H}^q(\mathrm{Gal}_{L|K}, A(L|K)).$$

Aus Vortrag 10, Theorem 10.8 folgt für eine beliebige Galoiserweiterung $L|K$ die Gleichung

$$\mathrm{H}^q(L|K, A) = \varinjlim_{E} \mathrm{H}^q(E|K, A),$$

wobei der Limes über alle Teilerweiterungen $L|E|K$ gebildet wird, so dass $E|K$ endlich und galoisch ist.

Falls $L = K^{\mathrm{sep}}$ der separable Abschluss von K ist, so erlaubt uns Korollar 11.18 die Schreibweise

$$\mathrm{H}^q(K, A) := \mathrm{H}^q(L|K, A).$$

Seien $F, E \in \mathscr{B}_K$ mit $F|E|K$. Dann können wir die Inflationsabbildung kurz schreiben als

$$\inf : \mathrm{H}^q(E|K, A) \longrightarrow \mathrm{H}^q(F|K, A),$$

wobei wir die Gleichheit $A_E = (A_F)^{\mathrm{Gal}(F|E)}$ benutzen.

Beispiel 11.20. Beispiele für abelsche Garben auf $\mathscr{B}_K$ sind

(1) $$\mathbb{G}_a : \mathscr{B}_K \longrightarrow \mathscr{A} \qquad \text{mittels} \qquad L \longmapsto (L, +)$$

(2) $$\mathbb{G}_m : \mathscr{B}_K \longrightarrow \mathscr{A} \qquad \text{mittels} \qquad L \longmapsto (L^\times, \cdot).$$

Notation 11.21. Falls im Kontext ersichtlich ist, auf welche Körpererweiterung $\mathbb{G}_a$ oder $\mathbb{G}_m$ angewandt werden, so wird das Argument weggelassen.

11.3 Normalbasensatz

Definition 11.22 (Normalbasis)**.** Sei $L|K$ eine endliche Galoiserweiterung. Eine K-Basis der Form $(\sigma_i\alpha)_i$ mit $\sigma_i \in \mathrm{Gal}_{L|K}$ und $\alpha \in L$ von L heißt **Normalbasis**.

Lemma 11.23. *Eine endliche Körpererweiterung $L|K$ eines endlichen Körpers ist galoissch und zyklisch mit Erzeuger $\sigma : \alpha \mapsto \alpha^{\#K}$.*

Beweis. Bis auf Isomorphie ist $K = \mathbb{F}_p^n$ und $L = \mathbb{F}_p^{n\cdot m}$ für natürliche Zahlen n und m. Somit gilt $\#K = p^n$. Der Frobeniusautomorphismus $\sigma : \alpha \mapsto \alpha^{p^n}$ lässt folglich alle Elemente aus $K^\times$ fix, denn

$$\sigma(\alpha) = \alpha \cdot \alpha^{\#K^\times} = \alpha.$$

Das Polynom $\alpha^{p^{nd}-1}$ besitzt maximal $(p^{nd} - 1)$ viele Nullstellen, also hat der Frobeniusautomorphismus $\sigma^d : \alpha \mapsto \alpha^{p^{nd}}$ maximal so viele Fixpunkte in $L^\times$. Damit hat σ die Ordnung m und es gilt

$$m = \#\langle\sigma\rangle \leq \#\,\mathrm{Aut}(L|K) \leq [L|K] = m.$$

Es gilt also Gleichheit, $L|K$ ist galoissch mit Galoisgruppe $\mathrm{Gal}(L|K)$ erzeugt von σ. □

Lemma 11.24 (Dedekinds Satz[2])**.** *Sei K ein Körper und G eine Gruppe. Dann sind endlich viele, paarweise verschiedene Homomorphismen $\varphi_1, \ldots, \varphi_n : G \to K^\times$ im K-Vektorraum* $\mathrm{Abb}(G, K)$ *linear unabhängig.*

Bemerkung 11.25. Ein Homomorphismus $\varphi : G \to K^\times$ im K-Vektorraum $\mathrm{Abb}(G, K)$ wird oft K-wertiger Charakter auf G genannt.

Beweis. Wir zeigen die Behauptung per Induktion. Für $n = 1$ ist die Behauptung offensichtlich. Seien also $\varphi_1, \ldots, \varphi_n$ verschiedene Homomorphismen. Wir nehmen an, dass für für $\alpha_1, \ldots, \alpha_n \in K$ und alle $\sigma \in G$ gilt:

$$\sum_{i=1}^{n} \alpha_i \cdot \varphi_i(\sigma) = 0.$$

Wir wollen nun zeigen, dass α_j mit $j \neq 1$ verschwindet. Da φ_1 und φ_j verschieden sind, existiert ein τ, an dem φ_1 und φ_j verschiedene Werte annehmen. Ersetzen wir σ durch $\tau\sigma$, so erhalten wir

$$\sum_{i=1}^{n} \alpha_i \cdot \varphi_i(\tau)\varphi_i(\sigma) = 0.$$

Multiplizieren wir die ursprüngliche Gleichung mit $\varphi_1(\tau)$ und subtrahieren diese von der vorherigen, erhalten wir

$$\sum_{i=1}^{n} \alpha_i \cdot \varphi_i(\tau)\varphi_i(\sigma) - \sum_{i=1}^{n} \alpha_i \cdot \varphi_1(\tau)\varphi_i(\sigma) = \sum_{i=1}^{n} \alpha_i \cdot (\varphi_i(\tau) - \varphi_1(\tau))\varphi_i(\sigma) = 0.$$

Der 1-te Summand fällt dabei weg. Die neuen Koeffizienten $\alpha_i' := \alpha_i \cdot (\varphi_i(\tau) - \varphi_1(\tau))$ müssen nach Induktionsvoraussetzung verschwinden, denn es handelt sich nun um eine Linearkombination mit $n - 1$ Summanden. Da jedoch $\varphi_1(\tau)$ und $\varphi_j(\tau)$ verschieden sind, verschwindet auch α_j:

$$\alpha_j = \alpha_j' \cdot (\varphi_j(\tau) - \varphi_1(\tau))^{-1} = 0.$$

Da somit also jedes α_j mit $j \neq 1$ verschwindet, verschwindet auch $\alpha_1 \cdot \varphi_1(\sigma)$ für jedes $\sigma \in G$, also auch α_1. □

Korollar 11.26. *Seien $K_1|K$ und $K_2|K$ Körpererweiterungen. Dann sind endlich viele verschiedene Homomorphismen $\chi_1, \ldots, \chi_n : K_1 \to K_2$ im K_2-Vektorraum* $\mathrm{Hom}_K(K_1, K_2)$ *linear unabhängig.*

Beweis. Wende Dedekinds Satz auf $\chi_i|_{K_1^\times} : K_1^\times \to K_2^\times$ mit $G = K_1^\times$ an. □

Korollar 11.27. *Sei $L|K$ eine endliche, galoissche Körpererweiterung und $(\mu_1, \ldots, \mu_n)$ eine Basis von L über K. Sei* $\mathrm{Gal}(L|K) = \{\sigma_1, \ldots, \sigma_n\}$*, dann ist die Matrix $\Gamma := (\sigma_i\mu_j)_{ij} \in \mathscr{M}_n(L)$ invertierbar.*

Beweis. Nach Korollar 11.26 wissen wir, dass die K-Homomorphismen σ_i über L linear unabhängig sind. Somit sind auch die Zeilenvektoren $(\sigma_i\mu_j)_j \in \mathscr{M}_{1\times n}(L)$ der Matrix Γ über L linear unabhängig. Folglich ist die Matrix Γ invertierbar. □

[2]Richard Dedekind (1831-1916), deutscher Mathematiker

Lemma 11.28. *Sei K unendlich und $f(X_1, \ldots, X_n) \in K[X]$ mit $f(\alpha_1, \ldots, \alpha_n) = 0$ für alle $\alpha_1, \ldots, \alpha_n \in K$. Dann gilt $f \equiv 0$.*

Beweis. Wir beweisen die Aussage per Induktion über die Anzahl der Variablen n. Im Fall $n = 1$ folgt die Behauptung direkt aus dem Umstand, dass jedes nichtverschwindende Polynom in einer Variablen nur endlich viele Nullstellen besitzt.

Sei also die Behauptung für n wahr. Wir folgern die Behauptung für $n + 1$. Dazu schreiben wir das Polynom als

$$f(X_1, \ldots, X_{n+1}) = \sum_i \lambda_i(X_1, \ldots, X_n) \cdot X_{n+1}^i$$

mit Koeffizienten $\lambda_i(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$. Wir können auf diese Weise f als ein Polynom in nur einer Variablen X_{n+1} betrachten. Wieder folgt aus dem Umstand, dass jedes nichtverschwindende Polynom (in einer Variablen) nur endlich viele Nullstellen besitzt, dass alle Koeffizienten für alle $(a_1, \ldots, a_n) \in K \times \ldots \times K$ verschwinden. Nach Induktionsvoraussetzung sind die Koeffizienten also auch Nullpolynome. □

Korollar 11.29. *Sei $L|K$ eine endliche Galoiserweiterung und K unendlich. Weiter seien $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}(L|K)$ die Elemente der Galoisgruppe. Sei $f(X_1, \ldots, X_n) \in K[X]$ mit $f(\sigma_1\alpha, \ldots, \sigma_n\alpha) = 0$ für alle $\alpha \in L$. Dann gilt $f \equiv 0$.*

Beweis. Sei $\mu_i, \ldots, \mu_n$ eine K-Basis von L. Dann definieren wir ein Polynom

$$g(Y_1, \ldots, Y_n) := f\left(\sum_{i=1}^n Y_i\sigma_1\mu_i, \ldots, \sum_{i=1}^n Y_i\sigma_n\mu_i\right) \in K[Y_1, \ldots, Y_n].$$

Wegen $f(\sigma_1\alpha, \ldots, \sigma_n\alpha) = 0$ für alle $\alpha \in L$ verschwindet auch

$$\begin{aligned} g(\alpha_1, \ldots, \alpha_n) &= f\left(\sum_{i=1}^n \alpha_i\sigma_1\mu_i, \ldots, \sum_{i=1}^n \alpha_i\sigma_n\mu_i\right) \\ &= f\left(\sum_{i=1}^n \sigma_1\alpha_i\mu_i, \ldots, \sum_{i=1}^n \sigma_n\alpha_i\mu_i\right) \\ &= f(\sigma_1\alpha, \ldots, \sigma_n\alpha) \end{aligned}$$

für alle $\alpha_1, \ldots, \alpha_n \in K$. Somit ist $g(Y_1, \ldots, Y_n)$ das Nullpolynom.

Nach Korollar 11.27 ist die Matrix $(\sigma_i\mu_j)_{ij}$ invertierbar. Die Variablen $X_1, \ldots, X_n$ lassen sich also als Linearkombination der Variablen $Y_1, \ldots, Y_n$ darstellen. Somit ist auch f das Nullpolynom. □

Satz 11.30 (Normalbasensatz)**.** *Jede endliche Galoiserweiterung $L|K$ besitzt eine Normalbasis $(\sigma_i\alpha)_i$.*

Beweis. Wir unterscheiden die beiden Fälle, dass K endlich bzw. unendlich ist. Wir geben jeweils einen Beweis des Satzes. Diese beiden Beweise sind voneinander unabhängig und besitzen eine grundsätzlich andere Struktur.

***K* endlich.** Nach Lemma 11.23 ist $G(L|K)$ zyklisch, generiert von einem Element σ der Ordnung n. Sei $p(X) \in K[X]$ das Minimalpolynom von σ. Jedes Polynom mit

$q(\sigma) = 0$ wird vom Minimalpolynom geteilt. Wegen $\sigma^n = 1$ mit $n := [L : K]$ teilt also das Minimalpolynom $p(X)$ das Polynom $X^n - 1$.

Andererseits gilt: Nach Lemma 11.24 sind $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$ linear unabhängig über K. Folglich muss das Minimalpolynom mindestens vom Grad n sein. Da es $X^n - 1$ teilt, ist $p(X) = X^n - 1$.

Somit ist L als $K[X]$-Modul (X operiere wie σ auf L) isomorph zu $K[X]/(X^n-1)$ (mittels einer Abbildung, die $1 \in K[X]/(X^n-1)$ auf ein $\alpha \in L$ schickt). Dann ist $1, X, \ldots, X^{n-1}$ eine K-Basis von $K[X]/(X^n - 1)$, also $\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)$ eine K-Basis von L.

***K* unendlich.** Es seien $\sigma_1, \ldots, \sigma_n$ die Elemente der Galoisgruppe $\mathrm{Gal}(L|K)$. Wir betrachten nun das Polynom

$$f(X_1, \ldots, X_n) := \det(A) \in L[X_1, \ldots, X_n],$$

wobei A die $n \times n$-Matrix ist mit $A_{ij} = X_k$, falls $\sigma_i\sigma_j = \sigma_k$. Nun ist $f(1, 0, \ldots, 0)$ die Determinante einer Matrix, die in jeder Zeile und jeder Spalte genau eine 1 hat. Demnach ist $f(1, 0, \ldots, 0) = \pm 1$, also nicht verschwindend. Somit ist $f(X_1, \ldots, X_n)$ nicht das Nullpolynom.

Nach Lemma 11.29 existiert also ein $\alpha \in L$, so dass $f(\sigma_1\alpha, \ldots, \sigma_n\alpha) = \det((\sigma_i\sigma_j\alpha)_{ij})$ nicht verschwindet. Dies verwenden wir gleich.

Wir zeigen nun die lineare Unabhängigkeit der $\sigma_1\alpha, \ldots, \sigma_n\alpha$: Seien $\lambda_1, \ldots, \lambda_n$ derart, dass

$$\sum_{i=1}^{n} \lambda_i\sigma_i\alpha = 0.$$

Durch Anwenden der σ_j erhalten wir das Gleichungssystem

$$\sum_{i=1}^{n} \lambda_i\sigma_j\sigma_i\alpha = 0$$

in den Unbekannten $\lambda_1, \ldots, \lambda_n$. Da jedoch die Determinante $\det((\sigma_i\sigma_j\alpha)_{ij})$ nicht verschwindet, existiert nur eine Lösung, nämlich die triviale. Somit sind die $\sigma_1\alpha, \ldots, \sigma_n\alpha$ über K linear unabhängig.

Wegen $\#\,\mathrm{Gal}(L|K) = n$ besteht eine Basis nach dem Satz von Artin aus n Elementen. Also ist $\sigma_1\alpha, \ldots, \sigma_n\alpha$ eine Normalbasis. □

11.4 Galoiskohomologie

Satz 11.31. *Sei $L|K$ eine Galoiserweiterung. Dann gilt für $q > 0$*

$$\mathrm{H}^q(L|K, \mathbb{G}_a) = 0 \qquad \textit{und} \qquad \mathrm{H}^0(L|K, \mathbb{G}_a) = K.$$

Beweis. Wir beweisen zuerst die Behauptung für den Fall $q > 0$. Sei zunächst $L|K$ endlich. Dann ist nach dem Normalbasensatz $L \cong K[\mathrm{Gal}_{L|K}] \cong \mathrm{Ind}_1^{\mathrm{Gal}_{L|K}}(K)$ als $\mathrm{Gal}_{L|K}$-Modul. Somit folgt

$$\mathrm{H}^q(L|K, \mathbb{G}_a) = \mathrm{H}^q\left(\mathrm{Gal}_{L|K}, \mathrm{Ind}_1^{\mathrm{Gal}_{L|K}}(K)\right) = \mathrm{H}^q(1, K) = 0.$$

Falls $L|K$ unendlich ist, so ergibt sich die Behauptung aus dem endlichen Fall:

Die Galoisgruppe einer beliebigen Galoiserweiterung $L|K$ lässt sich als der projektive Limes über alle Galoisgruppen von endlichen Galoiserweiterungen $E|K$ schreiben:

$$\mathrm{Gal}(L|K) = \varprojlim_{L|E|K \text{ endlich}} \mathrm{Gal}(E|K).$$

Mit der Schreibweise „$L|E|K$ endlich“ sei gemeint, dass $L|E|K$ Körpererweiterungen sind und $E|K$ endlich. Weiter gilt

$$\mathrm{H}^q(L|K, \mathbb{G}_a) = \varinjlim_{L|E|K \text{ endlich}} \mathrm{H}^q(E|K, \mathbb{G}_a).$$

Die Behauptung für den Fall $q = 0$ folgt direkt aus dem Umstand, dass $L|K$ eine Galoiserweiterung ist, also genau K unter der Galoisgruppe $\mathrm{Gal}(L|K)$ fix ist:

$$\mathrm{H}^0(L|K, \mathbb{G}_a) = L^{\mathrm{Gal}(L|K)} = K.$$

□

Satz 11.32. *Sei $L|K$ eine Galoiserweiterung. Dann gilt*

$$\mathrm{H}^0(L|K, \mathbb{G}_m) = K^\times.$$

Beweis. Die Behauptung wird analog zu der Behauptung des vorherigen Satzes im Fall $q = 0$ bewiesen. □

Satz 11.33 (Hilbert 90[3])**.** *Sei $L|K$ eine Galoiserweiterung. Dann gilt*

$$\mathrm{H}^1(L|K, \mathbb{G}_m) = 1.$$

Beweis. Sei zunächst $L|K$ endlich. Sei $\varphi : \mathrm{Gal}_{L|K} \to L^\times$ mittels $\sigma \mapsto \varphi_\sigma$ ein 1-Kozykel und sei $\alpha \in L^\times$. Dann definieren wir

$$\beta := \sum_{\sigma \in \mathrm{Gal}_{L|K}} \varphi_\sigma \, \sigma(\alpha).$$

Nach Dedekinds Satz (Lemma 11.24) folgt die L-lineare Unabhängigkeit aller $\sigma \in \mathrm{Gal}_{L|K}$ im K-Vektorraum $\mathrm{Hom}_K(L, L)$. Also können wir α so wählen, dass β nicht verschwindet.

Da φ ein 1-Kozykel ist, gilt

$$\varphi_{\tau\sigma} = \tau(\varphi_\sigma)\varphi_\tau.$$

Daraus folgt für ein beliebiges $\tau \in \mathrm{Gal}_{L|K}$

$$\tau(\beta) = \sum_{\sigma \in \mathrm{Gal}_{L|K}} \tau(\varphi_\sigma) \cdot \tau\sigma(\alpha) = \sum_{\sigma \in \mathrm{Gal}_{L|K}} \varphi_\tau^{-1} \cdot \varphi_{\tau\sigma} \cdot \tau\sigma(\alpha) = \varphi_\tau^{-1} \cdot \sum_{\tau\sigma \in \mathrm{Gal}^{L|K}} \varphi_{\tau\sigma} \cdot \tau\sigma(\alpha) = \varphi_\tau^{-1}\beta.$$

Somit erhalten wir

$$\varphi_\tau = \beta \cdot \tau(\beta)^{-1}.$$

Also ist φ ein 1-Korand. Da also jeder 1-Kozykel ein 1-Korand ist, folgt die Trivialität der Kohomologie.

Falls $L|K$ unendlich ist, so ergibt sich die Behauptung wieder durch Limesbildung. □

[3]David Hilbert (1862-1943), deutscher Mathematiker. Der Satz „Hilbert 90“ trägt seinen Namen, weil Hilbert diesen in seiner *Theorie der algebraischen Zahlenkörper* unter der Nummer 90 aufgeführt hat.

11.5 Kummertheorie

Mit Hilfe der Kohomologie profiniter Gruppen wollen wir nun die abelschen Erweiterungen eines Körpers untersuchen. Diese Theorie wird Kummertheorie[4] genannt.

Notation 11.34. Wir definieren $G/n := G/G^n$ für eine abelsche Gruppe G.

Sei $L = K^{\text{sep}}$ der separable Abschluss von K. Weiter sei n eine ganze Zahl, die prim zur Charakteristik von L ist und $K^\times$ die Gruppe der n-ten Einheitswurzeln μ_n enthält. Dann erhalten wir die kurze exakte Sequenz

$$1 \longrightarrow \mu_n \xrightarrow{\imath} L^\times \xrightarrow{(-)^n} L^\times \longrightarrow 1$$

mit der Gruppenhomomorphismus $(-)^n : L^\times \to L^\times$ mittels $\alpha \mapsto \alpha^n$. Dieser ist surjektiv, da die Gleichung $X^n - \alpha = 0$ für jedes $\alpha \in L^*$ separabel ist. Diese Sequenz erzeugt die exakte Kohomologiesequenz

$$\ldots \longrightarrow \mathrm{H}^0(L|K, \mathbb{G}_m) \xrightarrow{(-)^n} \mathrm{H}^0(L|K, \mathbb{G}_m) \xrightarrow{\delta_0} \mathrm{H}^1(\mathrm{Gal}_K, \mu_n) \longrightarrow \mathrm{H}^1(K, \mathbb{G}_m) \longrightarrow \ldots$$

Wenden wir hierauf den Satz Hilbert 90 (Satz 11.33) und Satz 11.32 an, so erhalten wir die exakte Sequenz

$$K^\times \xrightarrow{(-)^n} K^\times \xrightarrow{\delta_0} \mathrm{H}^1(\mathrm{Gal}_K, \mu_n) \longrightarrow \mathrm{H}^1(K, \mathbb{G}_m) = 1.$$

Lemma 11.35. *Es gilt*

$$\delta_0 : K^\times/n \xrightarrow{\sim} \mathrm{H}^1(\mathrm{Gal}_K, \mu_n).$$

Der Isomorphismus ist dabei gegeben durch die Abbildungsvorschrift

$$\alpha \longmapsto \left(\sigma \longmapsto \frac{\sigma(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}}\right),$$

wobei $\sqrt[n]{\alpha} \in \mathbb{B}_m$ eine n-te Wurzel von α ist. Die Abbildungsvorschrift ist unabhängig von der Wahl dieser Wurzel.

Bemerkung 11.36. Dieses Lemma setzt nicht voraus, dass $K^\times$ die Gruppe der n-ten Einheitswurzeln enthält.

Beweis. Teilt man aus $K^\times$ den Kern der Abbildung δ_0, also das Bild der Abbildung $(-)^n$ raus, so erhält man $K^\times/n$. Auf diese Weise induziert der Verbindungshomomorphismus $\delta_0 : K^\times \to \mathrm{H}^1(\mathrm{Gal}_K, \mu_n)$ den behaupteten Isomorphismus $\delta_0 : K^\times/n \to \mathrm{H}^1(\mathrm{Gal}_K, \mu_n)$.

Um die Abbildungsvorschrift zu erhalten, müssen wir die Konstruktion des Verbindungshomomorphismus δ_0 nachvollziehen. Wir betrachten nochmals die exakte Sequenz

$$1 \xrightarrow{\imath} \mu_n \longrightarrow L^\times \xrightarrow{(-)^n} L^\times \longrightarrow 1.$$

Sei $\alpha \in K^\times \subset \mathbb{G}_m$. Dann existiert ein Urbild a unter $(-)^n$. Nun liegt $\sigma(a)/a$ im Kern der Abbildung $(-)^n$, denn es gilt

$$\left(\frac{\sigma a}{a}\right)^n = \frac{\sigma(a^n)}{a^n} = \frac{\sigma(\alpha)}{\alpha} = \frac{\alpha}{\alpha} = 1.$$

[4] Ernst Eduard Kummer (1810-1893), deutscher Mathematiker

Damit liegt $\sigma(a)/a$ im Bild von $\imath$, d.h. wegen $\mu_n \subset K^\times$ liegt $\sigma(a)/a$ in μ_n. Nun ist die Abbildung

$$\sigma \longmapsto \frac{\sigma(a)}{a}$$

ein gekreuzter Homomorphismus in $\mathrm{H}^1(\mathrm{Gal}_K, \mu_n)$. Der Verbindungshomorphismus $\delta_0 : K^\times \to \mathrm{H}^1(\mathrm{Gal}_K, \mu_n)$ ergibt sich folglich mittels

$$\alpha \longmapsto \left(\sigma \longmapsto \frac{\sigma(a)}{a}\right).$$

Die Konstruktion von δ_0 ist dabei von der Wahl des Urbildes a unter $(-)^n$ unabhängig, denn zwei Urbilder a_1 und a_2 unterscheiden sich um eine n-te Einheitswurzel $\zeta \in \mu_n \subset K^\times$. Somit gilt

$$\frac{\sigma(a_1)}{a_1} = \frac{\sigma(a_2\zeta)}{a_2\zeta} = \frac{\sigma(a_2)\sigma(\zeta)}{a_2\zeta} = \frac{\sigma(a_2)\zeta}{a_2\zeta} = \frac{\sigma(a_2)}{a_2}.$$

Dies rechtfertigt die Schreibweise $\sqrt[n]{\alpha}$ in der Abbildungsvorschrift. □

Im Folgenden werden wir versuchen mit Hilfe dieser Gleichheit die Galoisgruppe so gut wie möglich zu beschreiben. Dazu benötigen wir den folgenden Satz.

Satz 11.37 (Pontrjagin-Dualität[5])**.** *Sei G eine proendliche, abelsche Gruppe, A ein diskreter Torsionsmodul. Weiter sei $\eta : G \times A \to \mathbb{Q}/\mathbb{Z}$ eine Paarung. Dann sind äquivalent:*

(a) Die Abbildung $G \to \mathrm{Hom}_{\mathrm{stetig}}(A, \mathbb{Q}/\mathbb{Z})$ ist ein Isomorphismus.

(b) Die Abbildung $A \to \mathrm{Hom}_{\mathrm{stetig}}(G, \mathbb{Q}/\mathbb{Z})$ ist ein Isomorphismus.

(c) Die Paarung η ist nicht ausgeartet.

Beweis. Die Behauptung kann relativ leicht für endliches G bewiesen und dann durch Limitenbildung für beliebiges G verallgemeinert werden. □

Notation 11.38. Wir wollen im Folgenden an Stelle von $\mathrm{Hom}_{\mathrm{stetig}}$ nur noch Hom schreiben.

Definition 11.39 (Abelisierung[6])**.** Sei G eine proendliche Gruppe. Dann bezeichnen wir mit G^{ab} die **Abelisierung** von G, d.h. die Faktorgruppe der Gruppe G und des Abschlusses der Kommutatorgruppe von G:

$$G^{\mathrm{ab}} := G/\overline{[G, G]}.$$

Theorem 11.40. *Es enthalte $K^\times$ die Gruppe der n-ten Einheitswurzeln μ_n. Dann gilt:*

$$\mathrm{Gal}_K^{\mathrm{ab}}\,/n \cong \mathrm{Hom}(K^\times/n, \mu_n).$$

[5]Lev Semjonovič Pontrjagin (1908-1988), russischer Mathematiker
[6]Niels Henrik Abel (1802-1829), norwegischer Mathematiker

Beweis. Da μ_n eine Untergruppe von $K^\times$ ist, liegt μ_n im Fixkörper von Gal_K. Somit operiert Gal_K trivial auf μ_n. Es gilt also nach Lemma 11.35

$$K^\times/n = \mathrm{H}^1(\mathrm{Gal}_K, \mu_n) = \mathrm{Hom}(\mathrm{Gal}_K, \mu_n).$$

Wir wollen nun die Pontrjagin-Dualität hierauf anwenden. Dazu müssen wir jedoch von der proendlichen Gruppe G zu ihrer Abelisierung übergehen und die Gleichung umschreiben: Da die Gruppe der n-ten Einheitswurzeln μ_n kommutativ und zyklisch von der Ordnung n ist, folgern wir

$$K^\times/n = \mathrm{Hom}(\mathrm{Gal}_K, \mu_n) \cong \mathrm{Hom}\left(\mathrm{Gal}_K^{\mathrm{ab}}, \mu_n\right) \cong \mathrm{Hom}\left(\mathrm{Gal}_K^{\mathrm{ab}}/n, \mu_n\right).$$

Die stetigen Homomorphismen von der Gruppe $\mathrm{Gal}_K^{\mathrm{ab}}/n, \mu_n$ der Ordnung n in $\mathbb{Q}/\mathbb{Z}$ beschränken sich auf $\mathbb{Z}/n \cong \mu_n$ im Bild. Allerdings müssen wir für den Isomorphismus $\mathbb{Z}/n \cong \mu_n$ eine primitive Einheitswurzel wählen. Somit gilt

$$K^\times/n \cong \mathrm{Hom}\left(\mathrm{Gal}_K^{\mathrm{ab}}/n, \mu_n\right) = \mathrm{Hom}\left(\mathrm{Gal}_K^{\mathrm{ab}}/n, \mathbb{Q}/\mathbb{Z}\right).$$

Wir erhalten die exakte Paarung

$$\langle -, - \rangle : \mathrm{Gal}_K^{\mathrm{ab}}/n \times K^\times/n \longrightarrow \mu_n\ , \qquad (\sigma, \alpha) \longmapsto \frac{\sigma(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}}.$$

Diese Paarung heißt Kummerpaarung von K. Identifizieren wir nun μ_n mit seinem Bild in $\mathbb{Q}/\mathbb{Z}$, so können wir die Pontrjagin-Dualität auf diese Paarung anwenden. Wir erhalten

$$\mathrm{Gal}_K^{\mathrm{ab}}/n \cong \mathrm{Hom}(K^\times/n, \mathbb{Q}/\mathbb{Z}).$$

Die Behauptung folgt wiederum aus der Tatsache, dass sich Homomorphismen der Gruppe $K^\times/n$ der Ordnung n in $\mathbb{Q}/\mathbb{Z}$ auf $\mathbb{Z}/n \cong \mu_n$ im Bild beschränken. Wir wenden an dieser Stelle nochmals den Isomorphismus $\mathbb{Z}/n \cong \mu_n$ an, diesmal jedoch in umgekehrter Richtung. Das Ergebnis ist somit unabhängig von der obigen Wahl der primitiven Einheitswurzel. □

Notation 11.41. Sei $\alpha \in K$. Dann ist die n-te Wurzel $\sqrt[n]{\alpha}$ nicht eindeutig definiert. Der Körper $K(\sqrt[n]{\alpha})$ ist jedoch unabhängig davon, welche Wurzel gewählt wird.

Definition 11.42. Wir bezeichnen mit $K^{\mathrm{ab},n}$ das Kompositum aller abelschen Erweiterungen vom Exponent n.

Notation 11.43. Sei $A \subset K^\times/n$ eine Untergruppe. Dann benutzen wir die Kurzschreibweise

$$K(\sqrt[n]{A}) := K\left(\sqrt[n]{\mathrm{pr}^{-1}(A)}\right)$$

mit der Projektion $\mathrm{pr} : K^\times \to K^\times/n$.

Theorem 11.44 (Hauptsatz der Kummertheorie)**.** *Sei K ein Körper, der die Gruppe der n-ten Einheitswurzeln μ_n enthält. Dann gibt es eine Bijektion zwischen den abelschen Erweiterungen $L|K$ vom Exponent n und den Untergruppen A von $K^\times/n$:*

$$\left\{\begin{array}{c} L|K \text{ abelsch} \\ \text{vom Exponent } n \end{array}\right\} \overset{1:1}{\longleftrightarrow} \left\{\begin{array}{c} A \subset K^\times/n \\ \text{Untergruppe} \end{array}\right\}$$

$$L \longmapsto (K^\times \cap (L^\times)^n)/(K^\times)^n$$

$$K(\sqrt[n]{A}) \longleftarrow A.$$

Beweis. Die Bijektion erhalten erhalten wir, indem wir folgende Situation betrachten:

$$\begin{array}{ccccc} \left\{ \begin{array}{c} L|K \text{ abelsch} \\ \text{vom Exponent } n \end{array} \right\} & \overset{\text{(i)}}{\underset{1:1}{\longleftrightarrow}} & \left\{ \begin{array}{c} G \subset \mathrm{Gal}_K^{\mathrm{ab}}/n \\ \text{abg. Untergruppe} \end{array} \right\} & \overset{\text{(ii)}}{\underset{1:1}{\longleftrightarrow}} & \left\{ \begin{array}{c} A \subset K^\times/n \\ \text{Untergruppe} \end{array} \right\} \\ L & \longmapsto & \mathrm{Gal}(K^{\mathrm{ab},n}|L) & \longmapsto & (K^\times \cap (L^\times)^n)/(K^\times)^n \\ K(\sqrt[n]{A}) & \longmapsto & \mathrm{Gal}(K^{\mathrm{ab},n}|K(\sqrt[n]{A})) & \longmapsto & A. \end{array}$$

Die Bijektion (i) folgt unmittelbar aus dem Hauptsatz der Galoistheorie. Wenden wir uns also der Bijektion (ii) zu.

Aus Theorem 11.40 erhalten wir die Kummerpaarung

$$\langle -,- \rangle : \mathrm{Gal}_K^{\mathrm{ab}}/n \times K^\times/n \longrightarrow \mu_n\ , \qquad (\sigma, \alpha) \longmapsto \frac{\sigma(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}}.$$

Seien nun $G \subset \mathrm{Gal}_K^{\mathrm{ab}}/n$ und $A \subset K^\times/n$ Untergruppen. Dann erhalten wir die Bijektion (ii), indem wir die Untergruppen auf ihr bzgl. dieser Paarung orthogonales Komplement schicken, d.h. G auf $G^\perp$ und A auf $A^\perp$. Dies ist genau die oben angegebene Zuordnung, denn: Sei $G = \mathrm{Gal}(K^{\mathrm{ab},n}|L)$. Dann ist nach Definition

$$G^\perp = \{\alpha \in K^\times/n \mid \langle \sigma, \alpha \rangle = 1 \text{ für alle } \sigma \in G\}.$$

Das orthogonale Komplement $G^\perp$ besteht also aus den $\alpha \in K^\times/n$, so dass alle $\sigma \in G$ trivial auf $\sqrt[n]{\alpha}$ operieren. Da die Gruppe G gerade L fix lässt, ist $\sqrt[n]{\alpha}$ in $L^\times$, also α in $(L^\times)^n$. Somit gilt

$$G^\perp = (K^\times \cap (L^\times)^n)/(K^\times)^n.$$

Das orthogonale Komplement von A ist nach Definition

$$A^\perp = \left\{\sigma \in \mathrm{Gal}_K^{\mathrm{ab}}/n \mid \langle \sigma, \alpha \rangle = 1 \text{ für alle } \alpha \in A\right\}.$$

Es besteht also aus den $\sigma \in \mathrm{Gal}_K^{\mathrm{ab}}/n$, die $\sqrt[n]{\alpha}$ für alle $\alpha \in A$, also $\sqrt[n]{A}$ fix lassen. Das ist jedoch gerade bei der Galoisgruppe der Erweiterung $K^{\mathrm{ab},n}|K(\sqrt[n]{A})$ der Fall. Es folgt

$$A^\perp = \mathrm{Gal}\left(K^{ab,n} \,\middle|\, K\left(\sqrt[n]{A}\right)\right).$$

□

11.6 Artin-Schreier Theorie

Die Artin[7]-Schreier[8] Theorie beschäftigt sich mit zyklischen Galoiserweiterungen in positiver Charakteristik.

Sei K ein Körper der Charakteristik $p > 0$ und $L := K^{\mathrm{sep}}$ sein separabler Abschluss.

[7]Emil Artin (1898-1962), österreichischer Mathematiker
[8]Otto Schreier (1901-1929), österreichischer Mathematiker

Lemma 11.45. *Der Gruppenhomomorphismus*

$$\wp : L \longrightarrow L, \quad x \longmapsto x^p - x$$

ist surjektiv.

Beweis. Das Polynom $p(x) = x^p - x - a$ mit $a \in L$ ist separabel, denn: Ist α eine Nullstelle, so auch $\alpha+1, \ldots, \alpha+p-1$. Somit ist $L(\alpha)|L$ eine separable Erweiterung, also $\alpha \in L$ wegen $L = K^{\text{sep}}$. Somit ist α Urbild von a unter $\wp$. □

Auf Grund des Lemma erhalten wir die kurze exakte Sequenz

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow L \xrightarrow{\wp} L \longrightarrow 0.$$

Diese Sequenz erzeugt die exakte Kohomologiesequenz

$$\ldots \longrightarrow \mathrm{H}^0(L|K, \mathbb{G}_a) \xrightarrow{\wp} \mathrm{H}^0(L|K, \mathbb{G}_a) \xrightarrow{\delta_0} \mathrm{H}^1(\mathrm{Gal}_{L|K}, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{H}^1(\mathrm{Gal}_{L|K}, \mathbb{G}_a) \longrightarrow \ldots$$

Nach Satz 11.31 ist jedoch $\mathrm{H}^1(\mathrm{Gal}_{L|K}, \mathbb{G}_a)$ trivial und $\mathrm{H}^0(L|K, \mathbb{G}_a)$ der Körper K selber. Es folgt also die exakte Sequenz

$$K \xrightarrow{\wp} K \longrightarrow \mathrm{H}^1(\mathrm{Gal}_{L|K}, \mathbb{Z}/p\mathbb{Z}) \longrightarrow 0.$$

Auf diese Weise erhalten wir einen Isomorphismus zwischen den stetigen Homomorphismen von $\mathrm{Gal}_{L|K} \to \mathbb{Z}/p\mathbb{Z}$ nach $K/\wp(K)$:

$$\mathrm{H}^1(\mathrm{Gal}_{L|K}, \mathbb{Z}/p\mathbb{Z}) \cong K/\wp(K).$$

Ähnlich wie bei der Kummertheorie können wir hier auch einen analogen Hauptsatz formulieren, dessen analogen Beweis wir allerdings auslassen:

Theorem 11.46 (Hauptsatz der Artin-Schreier Theorie)**.** *Sei K ein Körper der Charakteristik p. Dann gibt es eine Bijektion zwischen den abelschen Erweiterungen $L|K$ vom Exponent p und den Untergruppen A von $K/\wp(K)$:*

$$\left\{ \begin{array}{c} L|K \text{ abelsch} \\ \text{vom Exponent } p \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{c} A \subset K/\wp(K) \\ \text{Untergruppe} \end{array} \right\}$$

$$\begin{array}{ccc} L & \longmapsto & (K \cap \wp(L))/\wp(K) \\ K(\wp^{-1}(A)) & \longleftarrow & A. \end{array}$$

Vortrag 12

Kohomologische Dimension

Stephan Hähne, Maria Castillo Perez
24.1.2006

12.1 Proendliche Gruppen

Im Folgenden sei G stets eine proendliche Gruppe.

Definition 12.1. Eine **supernatürliche Zahl** ist ein formales Produkt $\prod_p p^{n(p)}$ mit $n(p) \in \mathbb{N}$ oder $n(p) = \infty$. Entsprechend werde für eine natürliche Zahl n der Exponent des Primfaktors p mit $n(p)$ bezeichnet. Für supernatürliche Zahlen $(n_i)_{i\in I}$ wird das Produkt und das kleinste gemeinsame Vielfache wie folgt definiert:

$$\prod_i n_i := \prod_p p^{\sum_i n_i(p)},$$

$$\mathrm{kgV}_i(n_i) := \prod_p p^{\max_i n_i(p)}.$$

Definition 12.2. Sei $H <_c G$, also H eine abgeschlossene Untergruppe von G. Dann heißt

$$(G : H) := \mathrm{kgV}_{U \lhd_o G}[G/U : HU/U]$$

der **Index** von H in G. Die **Ordnung** von G ist $\#G = (G : 1)$.

Einige Eigenschaften des Index werden nun aufgeführt in:

Proposition 12.3. *Für $H <_c G$ gilt:*

(1) $H = \bigcap_{N \lhd_o G} HN = \bigcap_{H \subseteq M <_o G} M$

(2) Sei $\mathscr{U}' \subset \{U \lhd_o G\} := \mathscr{U}$ eine Umgebungsbasis der 1 in G. Dann gilt:

$$(G : H) = \mathrm{kgV}_{U' \in \mathscr{U}'}[G : HU'].$$

(3) $H <_o G \iff (G : H) < \infty$

(4) $K <_c H <_c G$ *dann* $(G : K) = (G : H)(H : K)$

Beweis. (1) Siehe Vorlesung.

(2) Zu zeigen ist: $\mathrm{kgV}_{U'\in\mathscr{U}'}[G:HU'] = \mathrm{kgV}_{U\in\mathscr{U}}[G:HU]$, und $[G/U : HU/U] = [G:HU]$ für $U \lhd_o G$. Letzteres ist klar, denn $[G:HU] < \infty$ also $G = \dot{\bigcup}_i g_i HU \Rightarrow G/U = \dot{\bigcup}_i \overline{g_i} HU/U$. Ersteres folgt aus $\mathscr{U}' \subset \mathscr{U}$ und: Da $\mathscr{U}'$ Umgebungsbasis der 1 ist, gilt $\forall\, U \in \mathscr{U} \exists\, U' \in \mathscr{U}' : U' \subset U$, also $[G:HU][HU:HU'] = [G:HU']$.

(3) $\Rightarrow$: Weil H in G offen ist, ist $[G:H]$ endlich. Für alle $U \lhd_o G$ gilt

$$[G:HU] \leq [G:HU][HU:H] = [G:H].$$

Somit $(G:H) < \infty$.

$\Leftarrow$: Wegen $n := (G:H) < \infty$ gibt es ein $U \lhd_o G$ mit $[G:HU] = n$, gegebenfalls nach Schneiden endlich vieler offener Normalteiler. Es genügt dann $HU = H$ zu zeigen, weil H in G abgeschlossen ist und mit $[G:H]$ endlich auch offen ist. Annahme: $HU \supsetneq H$. Also existiert ein $u \in U$ mit $u \notin H$. Nach (i) gilt aber: $\exists\, U_1 \lhd_o G$ mit $u \notin HU_1$. Sei nun $U_2 := U_1 \cap U \lhd_o G$. Dann gilt: $HU \supsetneq HU_2$, da $u \notin HU_2 \subset HU_1$. Damit ergibt

$$[G:HU_2] = [G:HU][HU:HU_2] > [G:HU]$$

einen Widerspruch zu $[G:HU] = n$.

(4) Seien dazu $n = (G:K)(p)$, $n_1 = (G:H)(p)$, $n_2 = (H:K)(p)$, wobei p eine Primzahl ist. Zu zeigen ist $n = n_1 + n_2$. Für $U \lhd_o G$ gilt: $[G:KU] = [G:HU][HU:KU]$ und $[HU:KU] = [H:K(H\cap U)]$, da $K = \dot{\bigcup}_{i\in I} k_i H(K\cap U) \Rightarrow KU = \dot{\bigcup}_{i\in I} k_i HU$. Mit (2) angewendet auf H, K und $\mathscr{U}' = \{H\cap U; U \lhd_o G\}$ (H trägt die Unterraumtopologie) folgt: $(H:K) = \mathrm{kgV}_{U\in\mathscr{U}}[H : K(H\cap U)]$. Der Fall, dass ein Exponent unendlich ist, ist klar, genauso wie $n \leq n_1 + n_2$. Seien daher $U_1, U_2 \lhd_o G$ mit

$$n_1 = [G:HU_1](p), n_2 = [HU_2 : KU_2](p).$$

Für $U = U_1 \cap U_2 \lhd_o G$ ist aber

$$\begin{aligned} n &\geq [G:KU](p) \\ &= [G:HU](p) + [H:K(H\cap U)](p) \\ &\geq [G:HU_1](p) + [H:K(H\cap U_2)](p) \\ &= n_1 + n_2. \end{aligned}$$

□

Lemma–Definition 12.4. *(1) Eine* **pro-p-Gruppe** *H ist ein projektiver Limes von p-Gruppen. Äquivalent: H ist eine proendliche Gruppe von p-Potenz-Ordnung.*

(2) Eine abgeschlossene Untergruppe H von G heißt **pro-p-Sylow(unter)gruppe** *von G, falls H pro-p-Gruppe mit $p \nmid (G:H)$ ist.*

Beweis. $\Leftarrow$: Dies folgt unmittelbar aus $H = \varprojlim_{N\lhd_o H} H/N$ und $\#H = \mathrm{kgV}_{N\lhd_o H} \#H/N$.

$\Rightarrow$: Seien $\varphi_i : H \to H_i$ die Projektionen auf die Faktoren. Weil $\ker\varphi_i$ eine Umgebungsbasis der 1 ist und $H/\ker\varphi_i \cong \varphi_i(H) \subseteq H_i$ eine p-Gruppe ist, ist $\#H = \mathrm{kgV}_i \#H/\ker\varphi_i$ eine p-Potenz. □

Proposition 12.5. *Eine proendliche Gruppe G besitzt eine pro-p-Sylowgruppe.*

Beweis. Sei $G = \varprojlim_{i\in I} G_i$ der projektive Limes eines surjektiven projektiven Systems (G_i, φ_{ij}, I) aus endlichen Gruppen, mit surjektiven Projektionsabbildungen (φ_i). Sei $\mathscr{H}_i$ die Menge der p-Sylowuntergruppen von G_i. Dann bildet $(\mathscr{H}_i, \varphi_{ij}, I)$ ein projektives System aus nichtleeren endlichen Mengen, also diskreten kompakten topologischen Räumen, denn wegen der Surjektivität ist für $H_j \in \mathscr{H}_j$ $\varphi_{ij}(H_j) = H_j/(\ker\varphi_{ij} \cap H_j)$ eine p-Gruppe mit

$$p \nmid [G_i : \varphi_{ij}(H_j)] = \frac{|G_j/\ker\varphi_{ij}|}{|\varphi_{ij}(H_j)|} = \frac{[G_j : H_j]}{[\ker\varphi_{ij} : \ker\varphi_{ij} \cap H_j]},$$

also $\varphi_{ij}(H_j) \in \mathscr{H}_i$. Der projektive Limes $\mathscr{H} = \varprojlim_{i\in I} \mathscr{H}_i$ ist nichtleer, sei $(H_i) \in \mathscr{H}$. Dann bildet (H_i, φ_{ij}, I) ein surjektives projektives System. Behauptung: die Untergruppe $H = \varprojlim_{i\in I} H_i \subset G$ ist eine pro-p-Sylowuntergruppe. Begündung: zu zeigen ist, dass H in G abgeschlossen ist und $\#H$ eine p-Potenz ist und $p \nmid (G : H)$. Seien φ_i' die zu H gehörigen Projektionen, die also surjektiv sind. Wegen $H = \bigcap_i \varphi_i^{-1}(H_i)$ ist H in G abschlossen. Es gilt

$$\#H = \mathrm{kgV}_{i\in I}[H : \ker\varphi_i'] = \mathrm{kgV}_{i\in I}\, \#\varphi_i'(H) = \mathrm{kgV}_{i\in I}\, \#H_i,$$

was eine p-Potenz ist. Ferner wird

$$(G : H) = \mathrm{kgV}_{i\in I}[G/\ker\varphi_i : H\ker\varphi_i/\ker\varphi_i] = \mathrm{kgV}_{i\in I}[G_i : \varphi_i'(H)] = \mathrm{kgV}_{i\in I}[G_i : H_i]$$

nicht von p geteilt. □

12.2 Kohomologische Dimension

Sei G stets eine proendliche Gruppe und p eine Primzahl.

12.2.1 Kohomologische Dimension

Definition 12.6. Sei A eine abelsche Gruppe. Dann heißt

$$A(p) := \{a \in A; \exists\, n \in \mathbb{N} : p^n a = 0\}$$

der ***p*-primäre Teil** von A. A heißt ***p*-primär**, wenn $A = A(p)$.

Bemerkung 12.7. Sei A ein Torsionsmodul, d.h. $A = A_{\mathrm{tor}}$. In den Übungen zur Vorlesung haben wir gesehen: $A = \bigoplus_p A(p)$.

Bemerkung 12.8. $-(p) : A \mapsto A(p)$ ist ein Funktor und erhält für Torsionsmodule die Exaktheit.

Beweis. Die Funktorialität ist klar, da die Morphismen $\mathbb{Z}$-Modulhomomorphismen sind. Sei $A \xrightarrow{\iota} B \xrightarrow{\pi} C$ eine exakte Sequenz abelscher Gruppen. Dann ist die Exaktheit von $A(p) \xrightarrow{\widehat{\iota}} B(p) \xrightarrow{\widehat{\pi}} C(p)$ zu zeigen. Klar ist: $\mathrm{im}(\widehat{\iota}) \subseteq \ker(\widehat{\pi})$. Sei $b \in \ker(\widehat{\pi})$. Dann existiert $a \in A$ mit $\iota(a) = b$. Sei $a = \sum_{p'} a_{p'}$ die Zerlegung in p'-primäre Teile von a. Dann folgt $\sum_{p'} \iota(a_{p'}) = \iota(a) \in B(p)$. Wegen der Eindeutigkeit der Zerlegung ist: $b = \iota(a) = \iota(a_p)$, also $b \in \mathrm{im}(\widehat{\iota})$.

□

Proposition 12.9. *Seien $A \in C_G$ und $H <_c G$. Dann gilt:*

(1) Sei A ein Torsionsmodul. Mit $\mathscr{A} = \{A' \in C_G; A' \subseteq A, \text{endlich}\}$ lässt sich schreiben

$$A = \bigcup_{A' \in \mathscr{A}} A' = \varinjlim_{A' \in \mathscr{A}} A'.$$

(2) $\mathrm{Ind}_H^G(A)$ und $\mathrm{H}^q(G, A)$ sind p-primär, falls A p-primär ist, und $\mathrm{Ind}_H^G(A)$ ist ein Torsionsmodul, falls A Torsionsmodul ist.

(3) Es ist $\mathrm{Ind}_H^G(A) \in C_G$.

Beweis. (1) Sei $a \in A$ und A' der von a erzeugte Untermodul von A in C_G. Dann genügt zu zeigen, dass A' endlich ist. Zunächst ist $G.a$ endlich, denn das Bild des kompakten Unterraums $G \times \{a\}$, homöomorph zu G, unter der stetigen Abbildung $G \times A \to A$ ist kompakt, also endlich, weil A diskret ist. Der Orbit $G.a$ ist ein Erzeugendensystem von A' als $\mathbb{Z}$-Modul. Jedes Element von $G.a$ hat endliche Ordnung, also $\exists n > 0 : nG.a = 0$. Damit hat A' höchstens $n\#G.a$ Elemente, ist also endlich.

(2) Dies folgt aus folgender allgemeiner Betrachtung: Sei $f : X \to Y$ eine stetige Abbildung, X kompakt und Y diskret. Dann muss die disjunkte offene Überdeckung

$$\bigcup_{x \in \mathrm{im}(f)} f^{-1}(\{x\})$$

von X endlich sein. Also ist $\mathrm{im}(f)$ endlich. Falls Y zusätzlich eine p-primäre abelsche Gruppe bzw. ein Torsionsmodul ist, ist f p-primär, d.h. $p^n \,\mathrm{im}(f) = 0$ für ein n, bzw. f Torsionselement, d.h. $n \,\mathrm{im}(f) = 0$ für ein $n > 0$.

(3) Dazu genügt zu zeigen, dass $\forall\, f \in \mathrm{Ind}_H^G(A) : \mathrm{Stab}_G f \subseteq G$ offen ist. Da $\forall\, x \in \mathrm{im}(f)$ das Urbild $f^{-1}(\{x\})$ Vereinigung von offenen Mengen der Form gN mit $N \lhd_o G$ ist, und G kompakt ist, folgt, dass es eine endliche Überdeckung von G gibt: $G = \bigcup_{i=1}^r U_i$ mit $U_i = g_i N_i \subseteq f^{-1}(\{x_i\})$, $N_i \lhd_o G$, $x_i \in \mathrm{im}(f)$. Sei $N = \bigcap_{i=1}^r N_i \lhd_o G$ und $g \in \mathrm{Stab}_G f$ (d.h. $\forall\, g' \in G : f(g') = (gf)(g') = f(g'g)$). Die Offenheit von $\mathrm{Stab}_G f$ folgt dann aus $Ng \subseteq \mathrm{Stab}_G f$. Für $n \in N$ und $g' \in G$, also $g' = g_i n_i$ mit $n_i \in N_i$, gilt $f(g'(ng)) = f(g'n) = f(g_i n_i n) = f(g_i n_i) = f(g')$, d.h. $ng \in \mathrm{Stab}_G f$.

□

Definition 12.10. Sei p prim und $A \in C_G$ ein Torsionmodul. Dann heißt

$$\mathrm{cd}_p(G) = \inf\{n \in \mathbb{N}; \forall\, q > n, A \in C_G \text{ Torsionsmodul} : \mathrm{H}^q(G, A)(p) = 0\}$$

die ***p*-kohomologische Dimension** von G. Die Zahl

$$\mathrm{cd}(G) = \sup_p \mathrm{cd}_p(G)$$

heißt **kohomologische Dimension** von G.

Eine Charakterisierung liefert die

Proposition 12.11. *Sei $n \in \mathbb{N}$. Dann sind äquivalent:*

(1) $\mathrm{cd}_p(G) \leq n$.

(2) $\mathrm{H}^q(G, A) = 0$ *für alle* $q > n$ *und jeden p-primäre Torsionsmodul* $A \in C_G$.

(3) $\mathrm{H}^{n+1}(G, A) = 0$ *für alle einfachen Moduln* $A \in C_G$ *mit* $pA = 0$.

Beweis. (1) $\Leftrightarrow$ (2): Sei $A \in C_G$ Torsionsmodul. Es folgt aus: $\mathrm{H}^q(G, A_p) = \mathrm{H}^q(G, A)(p)$. Der Funktor $\mathrm{H}^q(G, -)$ vertauscht mit direkten Summen, da dieser additiv ist und mit direkten Limites vertauscht. Also gilt

$$\mathrm{H}^q(G, A) = \bigoplus_{\ell} \mathrm{H}^q(G, A(\ell))$$

nach der Bemerkung. Dabei sind die $\mathrm{H}^q(G, A(\ell))$ selbst ℓ-primär. Aus der Eindeutigkeit der Zerlegung in p-primäre Teile, folgt: $\mathrm{H}^q(G, A(p)) = \mathrm{H}^q(G, A)(p)$.

(2) $\Rightarrow$ (3): Klar.

(3) $\Rightarrow$ (2): Sei $A \in C_G$ ein p-primäres Torsionsmodul. Zunächst für $q = n + 1$:

- A endlich. Induktion nach $\#A$: $\#A = 0$ ist klar. Sei $\#A > 0$. Dann hat A einen einfachen Untermodul $S \neq 0$. Es gilt $pS = 0$, da sonst $S = pS = p^r S = 0$, für ein $r \in \mathbb{N}$.

$$0 \longrightarrow S \longrightarrow A \longrightarrow A/S \longrightarrow 0 \text{ ist exakt}$$

$$\Rightarrow \underbrace{\mathrm{H}^{n+1}(G, S)}_{=0 \text{ (3)}} \longrightarrow \underbrace{\mathrm{H}^{n+1}(G, A)}_{\Rightarrow = 0} \longrightarrow \underbrace{\mathrm{H}^{n+1}(G, A/S)}_{=0 \text{ da } \#\mathrm{A/S} < \#\mathrm{A}} \text{ ist exakt.}$$

- A beliebiger p-primärer Torsionsmodul in C_G. Wegen der Vertauschbarkeit mit Limites und der Proposition 12.9:

$$\mathrm{H}^{n+1}(G, A) = \varinjlim_{A' \in \mathscr{A}} \mathrm{H}^{n+1}(G, A') = 0.$$

Für $q > n + 1$ mit Induktion. Wir haben eine kurze exakte Sequenz:

$$0 \longrightarrow A \xrightarrow{i} \mathrm{Ind}^G(A) \longrightarrow \mathrm{Ind}^G(A)/A \longrightarrow 0$$

mit $i(a) : x \mapsto x \cdot a$, $a \in A$. Dazu gehört:

$$\ldots \longrightarrow \mathrm{H}^{q-1}\left(G, \mathrm{Ind}^G(A)/A\right) \longrightarrow \mathrm{H}^q(G, A) \longrightarrow \mathrm{H}^q\left(G, \mathrm{Ind}^G(A)\right) \longrightarrow \ldots$$

und wir wissen: $\mathrm{H}^q\left(G, \mathrm{Ind}^G(A)\right) = 0$ sowie $\mathrm{H}^{q-1}\left(G, \mathrm{Ind}^G(A)/A\right) = 0$ nach Induktionsvoraussetzung, da $\mathrm{Ind}_G(A) \in C_G$ p-primär ist. Also $\mathrm{H}^q(G, A) = 0$. □

12.2.2 Strikte kohomologische Dimension

Definition 12.12. Die Zahl

$$\mathrm{scd}_p(G) = \inf\{n \in \mathbb{N}; \forall\, q > n, A \in C_G : \mathrm{H}^q(G, A)(p) = 0\}$$

heißt **strikte p-kohomologische Dimension** von G, und

$$\mathrm{scd}(G) = \sup_p \mathrm{scd}_p(G)$$

heißt **strikte kohomologische Dimension** von G.

Den Unterschied zur $\mathrm{cd}_p(G)$ zeigt die

Proposition 12.13. *Es gilt stets* $\mathrm{cd}_p(G) \leq \mathrm{scd}_p(G) \leq \mathrm{cd}_p(G) + 1$.

Beweis. Noch zu zeigen ist: $\mathrm{scd}_p(G) \leq \mathrm{cd}_p(G) + 1$. Sei $q > \mathrm{cd}_p(G) + 1$ und $A \in C_G$. Zu zeigen ist $\mathrm{H}^q(G, A)(p) = 0$. Für die Multiplikation mit p gibt es zwei exakte Sequenzen:

$$0 \longrightarrow \ker(p) \hookrightarrow A \xrightarrow{p} pA \longrightarrow 0$$

$$0 \longrightarrow pA \longrightarrow A \longrightarrow A/pA \longrightarrow 0,$$

wobei $A \xrightarrow{p} pA \to A$ gleich $A \xrightarrow{p} A$ ist.

Nach Proposition 12.11 gilt $\mathrm{H}^q(G, \ker(p)) = 0$ und $\mathrm{H}^{q-1}(G, A/pA) = 0$, da $\ker(p)$ und A/pA p-primär sind. Aus den langen exakten Sequenzen zeigen folgt die Injektivität von $\mathrm{H}^q(G, A) \xrightarrow{p} \mathrm{H}^q(G, pA)$ und $\mathrm{H}^q(G, pA) \to \mathrm{H}^q(G, A)$, deren Verkettung

$$\mathrm{H}^q(G, A) \xrightarrow{p} \mathrm{H}^q(G, A)$$

auch injektiv ist. Also $\mathrm{H}^q(G, A)(p) = 0$. □

Beispiel 12.14. Für $G = \widehat{\mathbb{Z}}$ gilt: $\mathrm{cd}_p\left(\widehat{\mathbb{Z}}\right) = 1$ und andererseits $\mathrm{scd}_p\left(\widehat{\mathbb{Z}}\right) = 2$. Dies sieht man wie folgt. Weil $\mathbb{Q}$ als trivialer G-Modul eindeutig divisibel ist, d.h. für jedes $n > 0$ ist die Multiplikation mit n ein Automorphismus von $\mathbb{Q}$, gilt entsprechendes für die Kohomologiegruppen $\mathrm{H}^q\left(\widehat{\mathbb{Z}}, \mathbb{Q}\right)$. Diese sind aber für $q > 0$ nach Vortrag 10 Torsionsgruppen und müssen daher verschwinden: für $q \geq 1$ gilt $\mathrm{H}^q\left(\widehat{\mathbb{Z}}, \mathbb{Q}\right) = 0$. Die Sequenz

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

liefert $\mathrm{H}^2\left(\widehat{\mathbb{Z}}, \mathbb{Z}\right) = \mathrm{H}^1\left(\widehat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}\right) = \mathbb{Q}/\mathbb{Z}$ nach Vortrag 10. Daher gilt $\mathrm{scd}_p\left(\widehat{\mathbb{Z}}\right) \geq 2$.

Für einen Torsionsmodul $A \in C_G$ ist

$$\mathrm{H}^2\left(\widehat{\mathbb{Z}}, A\right) = \varinjlim_{A' \subset A \text{ endl.}} \mathrm{H}^2\left(\widehat{\mathbb{Z}}, A'\right) = 0$$

nach Vortrag 10. Also mit Proposition 12.11 $\mathrm{cd}_p\left(\widehat{\mathbb{Z}}\right) \leq 1$. Aus Proposition 12.13 folgt die Behauptung.

12.2.3 Untergruppen

Proposition 12.15. *Für $H <_c G$ gilt:*

$$\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G) \text{ und } \mathrm{scd}_p(H) \leq \mathrm{scd}_p(G)$$

mit Gleichheit in den Fällen:

(i) $p \nmid (G : H)$,

(ii) H *ist offen in* G *und* $\mathrm{cd}_p(G) < \infty$.

Beweis. Wir behandeln nur cd_p, der Fall scd_p geht ganz analog. Sei $A \in C_H$ ein Torsionsmodul und $q > \mathrm{cd}_p(G)$, falls $\mathrm{cd}_p(G)$ endlich ist. Mit Shapiros Lemma folgt:

$$\mathrm{H}^q(H, A) = \mathrm{H}^q\left(G, \mathrm{Ind}_H^G(A)\right) = 0,$$

weil $\mathrm{Ind}_H^G(A) \in C_G$ ein Torsionsmodul ist. Also gilt $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$. Die Gleichheiten folgen aus folgendem Lemma: □

Lemma 12.16. *Sei $A \in C_G$ und $H <_c G$.*

(1) Falls $p \nmid (G : H)$, so ist die Einschränkung: $\mathrm{res} : \mathrm{H}^q(G, A)(p) \to \mathrm{H}^q(H, A)(p)$ *injektiv.*

(2) Sei $H <_o G$. Sei A ein Torsionsmodul und $n = \mathrm{cd}_p(G) \in \mathbb{N}$, (bzw. sei A ein Modul und $n = \mathrm{scd}_p(G) \in \mathbb{N}$). Dann ist $\mathrm{cor} : \mathrm{H}^n(H, A)(p) \twoheadrightarrow \mathrm{H}^n(G, A)(p)$ *surjektiv.*

Beweis. (1) Mit $\mathscr{V} = \{V <_o G; V \supseteq H\}$ ist $H = \bigcap_{V \in \mathscr{V}} V = \varprojlim_{V \in \mathscr{V}} V$.

$$\Rightarrow \mathrm{H}^q(H, A) = \varinjlim_{V \in \mathscr{V}} \mathrm{H}^q(V, A),$$

wobei der Limes entlang der Restriktionsbbildungen res_H^V gebildet wird. Sei nun $x \in \mathrm{H}^q(G, A)(p)$ mit $\mathrm{res}_H^G(x) = 0 \in \mathrm{H}^q(H, A)$. Wegen $\mathrm{res}_H^V \mathrm{res}_V^G = \mathrm{res}_H^G$, $V \in \mathscr{V}$, folgt $\exists\, V \in \mathscr{V} : \mathrm{res}_V^G(x) = 0$.

Für $p \nmid (G : V) < \infty$ ist die Einschränkung von res_V^G auf $\mathrm{H}^q(G, A)(p)$ mit dem üblichen Korestriktionsargument injektiv. Somit folgt $x = 0$.

(2) Sei $\{t_i\}$ ein Repräsentantensystem mit 1 von $H\backslash G$. Wir definiere den offensichtlich surjektiven Homomorphismus

$$\pi : \mathrm{Ind}_H^G(A) \longrightarrow A, \quad \pi(f) = \sum_i t_i^{-1}.f(t_i),$$

Dann ist π ein G-Modulhomomorphismus, denn sei $t_i g = h_i t_{\alpha(i)}$ mit $h_i \in H$ und der richtigen Permutation α, dann gilt

$$\pi(g.f) = \sum_i t_i^{-1}.(g.f)(t_i) = g.\sum_i (t_i g)^{-1}.f(t_i g) = g.\sum_i k\left(h_i t_{\alpha(i)}\right)^{-1}.f(h_i t_{\alpha(i)})$$

$$= g.\sum_i t_{\alpha(i)}^{-1}.h_i^{-1}.h_i.f(t_{\alpha(i)}) = g.\sum_i t_{\alpha(i)}^{-1} f(t_{\alpha(i)}) = g.\pi(f)\ .$$

Nun ist $\ker \pi \subseteq \mathrm{Ind}_H^G(A)$ ein diskretes (Torsions-)modul. Die exakte Sequenz zu π liefert

$$\mathrm{H}^n\left(G, \mathrm{Ind}_H^G(A)\right)(p) \xrightarrow{\pi_*} \mathrm{H}^n(G,A)(p) \xrightarrow{\delta} \mathrm{H}^{n+1}(G, \ker\pi)(p) = 0.$$

Die Korestriktion cor ergibt sich als Verkettung des Isomorphismus aus Shapiros Lemma und von π_* und ist daher hier surjektiv auf den p-primären Anteilen:

$$\mathrm{H}^n(H,A)(p) \cong \mathrm{H}^n\left(G, \mathrm{Ind}_H^G(A)\right)(p) \xrightarrow{\pi_*} \mathrm{H}^n(G,A)(p),$$

wie behauptet.

□

Als Anwendung erhalten wir:

Korollar 12.17. *Sei G_p eine pro-p-Sylowgruppe von G. Dann gilt*

$$\mathrm{cd}_p(G) = \mathrm{cd}_p(G_p) = \mathrm{cd}(G_p),$$

$$\mathrm{scd}_p(G) = \mathrm{scd}_p(G_p) = \mathrm{scd}(G_p).$$

Korollar 12.18. *Es gilt $\mathrm{cd}_p(G) = 0 \Leftrightarrow p \nmid \#G$.*

Beweis. $\Leftarrow$: Nach dem Korollar gilt $\mathrm{cd}_p(G) = \mathrm{cd}_p(G_p) = \mathrm{cd}_p(1) = 0$.

$\Rightarrow$: Es genügt zu zeigen, dass für eine pro-p-Gruppe $G \neq 1$ ein nichttrivialer stetiger Homomorphismus $G \to \mathbb{Z}/p\mathbb{Z}$ existiert, denn dann ist $\mathrm{cd}_p(G) \geq 1$ (dabei hat $\mathbb{Z}/p\mathbb{Z} \in C_G$ die triviale G-Operation). Es ist G projektiver Limes eines surjektiven projektiven Systems aus p-Gruppen, so dass die Projektionen auch surjektiv sind. Daher existiert ein surjektiver statiger Homomorphismus $G \twoheadrightarrow G' \neq 1$ auf eine endliche nichttriviale p-Gruppe G'. Dieses G' hat einen Quotienten $\mathbb{Z}/p\mathbb{Z}$. □

Korollar 12.19. *Wenn $\mathrm{cd}_p(G) \neq 0, \infty$ dann ist $(\#G)(p) = \infty$.*

Beweis. Wir können annehmen aufgrund des vorherigen Korollars 12.17 und der Multiplikativität des Index, dass G pro-p-Gruppe ist. Falls $\#G$ endlich ist, so ist $\{1\}$ offen. Mit Proposition 12.15 folgt $\mathrm{cd}_p(G) = \mathrm{cd}_p(1) = 0$, ein Widerspruch. □

12.3 $\mathrm{H}^2(G,A)$ and extensions of profinite groups

The goal in the second part of this talk is to characterize profinite groups G of $\mathrm{cd}_p(G) \leq 1$. For the main result we need the interpretation of cohomology classes in $\mathrm{H}^2(G,A)$ as extensions (see also talk 1).

Consider a short exact sequence

$$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$$

of profinite groups and continuous homomorphisms, with A finite abelian. Let $\sigma : G \to E$ be a continuous section, i.e $p \circ \sigma = \mathrm{id}_G$, which exists by [Ser94] I.1.2 Prop 1. Define an action $G \times A \to A$ of G on A by $(g,a) \mapsto \sigma_x a \sigma_x^{-1} \quad (x \in G, a \in A)$. Clearly this action is continuous. This action makes A into a discrete G-module, as one easily verifies. This

action is independent of the chosen section because A is abelian. Moreover, recall that given a profinite group G and a finite G-module A, an extension X of A by H is defined to be an exact sequence

$$X: \quad 0 \longrightarrow A \longrightarrow E \xrightarrow{p} G \longrightarrow 1$$

with continuous homomorphisms, where E is a profinite group. We shall assume that the canonical action of G on A described above is precisely the given action of G on A, namely $i(g.a) = \bar{g}i(a)\bar{g}^{-1}$, where $\bar{g}$ is any element in $p^{-1}(g)$. If X and X' are two extensions of A by G, we say that they are *equivalent* if there exists a continuous homomorphism (necessarily an isomorphism) $E \to E'$ such that the following diagram:

$$\begin{array}{lccccccc} X: & 0 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{p} & G & \longrightarrow 1 \\ & & & \| & & \downarrow & & \| & \\ X': & 0 & \longrightarrow & A & \longrightarrow & E' & \xrightarrow[p']{} & G & \longrightarrow 1 \end{array}$$

commmutes.

One can ask here the following question: How many groups E' are there, which have the G-module A as a normal subgroup and G as the factor group? More precisely, we search for extension classes under the equivalence relation defined above. Denote by $\mathrm{Ext}(G,A)$ the set of extension classes. The following theorem answers the given question in a very powerful way:

Theorem 12.20. *There is a one-to-one correspondence between extension classes of the profinite group G by the finite abelian G-module A and $\mathrm{H}^2(G,A)$: We have an isomorphism*

$$\mathrm{Ext}(G,A) \cong \mathrm{H}^2(G,A).$$

Proof. We do the proof without considerations of the topology, since the profinite case is analogous with appropriate insertion of "continuous" at various places.

The proof consists of three steps:

Step 1: From each extension we construct a cohomology class (cochain class).

Step 2: From each cochain class we construct an extension.

Step 3: We show that the constrcutions given in step 1 and step 2 are mutually inverse.

Step 1: Suppose given an extension

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$$

and choose a section $\sigma : G \to E$, i.e. a set map with $p \circ \sigma = \mathrm{id}_G$. Note that this is always possible since p is surjective. Even more, because $p(1) = 1$, we can choose σ such that $\sigma(1) = 1$. Further we will work with such a section σ.

Now let $c \in \mathrm{Z}(G,A)$ be the inhomogeneous 2-cochain, i.e. a continuous function $G^2 \to A$, defined by

$$c(g_1,g_2) := \sigma(g_1)\sigma(g_2)\sigma(g_1g_2)^{-1}.$$

This definition is correct, because $\sigma(g_1)\sigma(g_2)\sigma(g_1g_2)^{-1} \in \ker(p) = \mathrm{im}(i)$. This c measures the failure of σ to be a group homomorphism. If we can show that:

(1) c is a cocycle, i.e $d(c) = 0$, and

(2) the class $[c]$ doesn't depend on the choice of σ, and

(3) equivalent extensions give the same cohomology class,

then we are done with step 1. For (1) we just calculate as follows. Note that we switch summands which are in A, since A is abelian.

$$\begin{aligned} dc(g_0,g_1,g_2) &= g_0.c(g_1,g_2) - c(g_0g_1,g_2) + c(g_0,g_1g_2) - c(g_0,g_1) \\ &= g_0.c(g_1,g_2) + c(g_0,g_1g_2) - c(g_0g_1,g_2) - c(g_0,g_1) \\ &= \sigma(g_0)\sigma(g_1)\sigma(g_2)\sigma(g_1g_2)^{-1}\sigma(g_0)^{-1}\sigma(g_0)\sigma(g_1g_2)\sigma(g_0g_1g_2)^{-1} \\ &\quad (\sigma(g_0g_1)\sigma(g_2)\sigma(g_0g_1g_2)^{-1})^{-1}\,(\sigma(g_0)\sigma(g_1)\sigma(g_0g_1)^{-1})^{-1} = 1. \end{aligned}$$

(2) Suppose that $\rho : G \to E$ is another section with $p(1) = 1$, giving $b \in \mathrm{Z}^2(G,A)$:

$$b(g_1,g_2) = \rho(g_1)\rho(g_2)\rho(g_1g_2)^{-1}$$

and consider $f : G \to A$ defined by $f(g) = \sigma(g)\rho(g)^{-1}$. We prove that $c - b = df$, so c and b define the same cohomology class. Indeed,

$$\begin{aligned} df(g_1,g_2) &= g_1f(g_2) - f(g_1g_2) + f(g_1) \\ &= f(g_1) + g_1.f(g_2) - f(g_1g_2) \\ &= (\sigma(g_1)\rho(g_1)^{-1})\,\rho(g_1)\,(\sigma(g_2)\rho(g_2)^{-1})\,\rho(g_1)^{-1} \\ &\quad [\rho(g_1g_2)\rho(g_2)^{-1}\rho(g_1)^{-1}]\,[\rho(g_1)\rho(g_2)\sigma(g_1g_2)^{-1}] \\ &= \sigma(g_1)\sigma(g_2)\rho(g_2)^{-1}\rho(g_1)^{-1}\,[\rho(g_1)\rho(g_2)\sigma(g_1g_2)^{-1}]\,[\rho(g_1g_2)\rho(g_2)^{-1}\rho(g_1)^{-1}] \\ &= (\sigma(g_1)\sigma(g_2)\sigma(g_1g_2)^{-1})\,(\rho(g_1g_2)\rho(g_2)^{-1}\rho(g_1)^{-1}) \\ &= c(g_1,g_2) - b(g_1,g_2) \end{aligned}$$

The square brackets commute as they are elements in A.

(3) Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & E & \xrightarrow{p} & G & \longrightarrow & 1 \\ & & \| & & \varphi\downarrow & & \| & & \\ 0 & \longrightarrow & A & \xrightarrow{i'} & E' & \xrightarrow{p'} & G & \longrightarrow & 1 \end{array}$$

be an equivalence of extensions, and σ a section (with $\sigma(1) = 1$) of p. By 2), it is enough to choose the section $\sigma' = \varphi\sigma$ of p' and now we can easily see that the induced cocycles c and c' give the same cohomology class in $\mathrm{H}^2(G,A)$.

Step 2: We will construct an extension from a given cocycle. Notice that the inhomogeneouos cocycle c constrcuted in "step 1" has the property that $c(1,g) = c(g,1) = 0$. We say that a inhomogeneouos cocycle $c \in \mathrm{H}^2(G,A)$ is *normal* if $c(g,1) = c(1,g) = 0$ for every $g \in G$.

A cohomology class $u \in \mathrm{H}^2(G,A)$ can always be represented by a normal cocycle. Indeed, if $u = [c]$, then let

$$f(g) = c(g,1)$$

and consider

$$c' = c - df.$$

Clearly, $[c'] = [c]$ and for all $g, h, \in G$,

$$\begin{array}{rcl} df(g,h) = gf(h) - f(gh) + f(g) & = & gc(1,h) - c(1,gh) + c(1,g) \\ gc(1,h) - dc(1,g,h) & = & gc(1,h) \end{array}$$

By taking $g = 1$, we get

$$c'(1,h) = c(1,h) - df(1,h) = 0 \tag{12.1}$$

Since c' is a cocycle,

$$0 = dc'(g,h,1) = gc'(h,1) - c'(gh,1) + c'(g,h) - c'(g,h) = gc'(h,1) - c'(gh,1)$$

and taking $h = 1$ and using (12.1), we have for all $g \in G$

$$c'(g,1) = 0.$$

Then, it follows from (12.1) that c' is normal.

Let us construct the map $\mathrm{H}^2(G,A) \to \mathrm{Ext}(G,A)$ which will be the inverse to the construction $\mathrm{Ext}(G,A) \to \mathrm{H}^2(G,A)$ we have discussed. Let $u \in \mathrm{H}^2(G,A)$ and $c \in \mathrm{Z}(G,A)$ such that c is normal and $[c] = u$. Then define a group $A \rtimes_c G$ which is $A \times G$ as a set with the multiplication

$$(a,g).(b,h) = (a + gb + c(g,h), gh)$$

for all $g, h \in G$ and $a, b \in A$. We claim:

(1) This is a group structure.

(2) It fits into an extension, namely $0 \to A \xrightarrow{i} A \rtimes_c G \xrightarrow{p} G \to 1$.

(3) It is independent of the choice of c.

Beweis. (1) By the cocycle condition, for $g_1, g_2, g_3 \in G$

$$0 = dc(g_1,g_2,g_3) = g_1c(g_2,g_3) - c(g_1g_2,g_3) + c(g_1,g_2g_3) - c(g_1,g_2)$$

and we have

$$g_1c(g_2,g_3) + c(g_1,g_2g_3) = c(g_1g_2,g_3) + c(g_1,g_2). \tag{12.2}$$

By the definition of the multiplication,

$$(a_1,g_1).((a_2,g_2).(a_3,g_3)) = (a_1 + g_1a_2 + g_1g_2a_3 + g_1c(g_2,g_3) + c(g_1,g_2g_3,g_1g_2g_3))$$

And by (12.2), this expression is equal to

$$(a_1, g_1a_2 + g_1g_2a_3 + c(g_1,g_2) + c(g_1g_2,g_3), g_1, g_2g_3) = ((a_1,g_1).(a_2,g_2)).(a_3,g_3).$$

thus we have the associativity. Now, for proving the existence of inverse element set $(a,g)^{-1} := \left(-g^{-1}a - c\left(g^{-1},g\right), g^{-1}\right)$. Since c is a normal cocycle,

$$0 = dc\left(g,g^{-1},g\right) = gc\left(g^{-1},g\right) - c(1,g) + c(g,1) - c\left(g,g^{-1}\right)$$

and this implies

$$gc\left(g^{-1},g\right) = c\left(g,g^{-1}\right).$$

Hence we have

$$(a,g).\left(-g^{-1}a - c\left(g^{-1},g\right), g^{-1}\right) = \left(a - a - gc\left(g^{-1},g\right) + c\left(g,g^{-1},1\right)\right) = (0,1).$$

(2) Clearly, the sequence $0 \to A \xrightarrow{i} A \rtimes_c G \xrightarrow{p} G \to 1$ where $i(a) = (a, 1)$ and $p(a, g) = g$ is an extension.

(3) Let c, c' be normal cocycles such that $[c] = [c'] = u$, $u \in \mathrm{H}^2(G, A)$. Then $c' = c + df$ and by normality $f(1) = 0$. In order to prove that the extensions corresponding to c and c' are equivalent, define the map $\varphi : A \rtimes_{c'} G \to A \rtimes_c G$ as $\varphi(a, g) := (a + f(g), g)$. We need to show that φ is an homomorphism.

Since $c' = c + df$, we have $c'(g_1, g_2) + f(g_1, g_2) = c(g_1, g_2) + g_1 f(g_2) + f(g_1)$. Therefore, for $(a_1, g_1), (a_2, g_2) \in A \rtimes_{c'} G$

$$\begin{aligned} \varphi((a_1, g_1).(a_2, g_2)) &= (a_1 + g_1 a_2 + c'(g_1, g_2) + f(g_1, g_2), g_1 g_2) \\ &= (a_1 + g_1 a_2 + c(g_1, g_2) + g_1 f(g_2) + f(g_1), g_1 g_2) \\ &= \varphi(a_1, g_1)\varphi(a_2, g_2) \end{aligned}$$

□

Step 3: In order to complete the proof, we have to check that our constructions are inverse each other.

One way around, for a cocycle c and the corresponding extension

$$0 \longrightarrow A \xrightarrow{i} A \rtimes_c G \xrightarrow{p} G \longrightarrow 1$$

choose the "obvious" section $s : G \to A \rtimes_c G$ defined by $\sigma(g) = (0, g)$. This extension gives us another cocycle $c'((g_1, g_2) := \sigma(g_1)\sigma(g_2)\sigma(g_1 g_2)^{-1}$. It is enough to show $c = c'$. As c is normalized, $gc(g^{-1}, g) = c(g, g^{-1})$ for all $g \in G$. So, we have

$$\begin{aligned} c'(g_1, g_2) &= \sigma(g_1)\sigma(g_2)\sigma(g_1 g_2)^{-1} \\ &= (c(g_1, g_2), g_1 g_2).(-c((g_1 g_2)^{-1}, g_1 g_2), (g_1 g_2)1^{-1}) \\ &= (c(g_1, g_2), 1) = c(g_1, g_2) \end{aligned}$$

The other way around, for an extension

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} G \longrightarrow 1$$

and a section $\sigma : G \to E$, we have the normal cocycle c with $c(g_1, g_2) = \sigma(g_1)\sigma(g_2)\sigma(g_1 g_2)^{-1}$ and the group extension

$$0 \longrightarrow A \longrightarrow A \rtimes_c G \longrightarrow G \longrightarrow 1.$$

To prove the equivalence of the extensions, define the map $\psi : A \rtimes_c G \to E$ as

$$\psi(a, g) = i(a)\sigma(g).$$

If we prove that ψ is an homomorphism, we will be done. And, it is as follows:

$$\begin{aligned} \psi((a_1, g_1).(a_2, g_2)) &= \psi(a_1 + g_1 a_2 + c(g_1, g_2), g_1 g_2) \\ &= i(a)i(g_1 a_2)i(c(g_1, g_2))\sigma(g_1 g_2) \\ &= i(a_1)\sigma(g_1)i(a_2)\sigma(g_1)^{-1}\sigma(g_1)\sigma(g_2)\sigma(g_1 g_2)^{-1}\sigma(g_1 g_2) \\ &= \psi(a_1, g_1)\psi(a_2, g_2) \end{aligned}$$

□

12.4 Profinite Groups G of $\mathrm{cd}_p(G) \leq 1$

Proposition 12.21. *Let G be a profinite group and p a prime. The following properties are equivalent:*

(a) $\mathrm{cd}_p(G) \leq 1$.

(b) The group G possesses the lifting property for the extensions

$$1 \longrightarrow P \longrightarrow E \longrightarrow W \longrightarrow 1,$$

where E is finite, and where P is an abelian p-group killed by p.

(c) Every extension of G by a finite abelian p-group by P splits.

(d) The group G possesses the lifting property for the extensions

$$1 \longrightarrow P \longrightarrow E \longrightarrow W \longrightarrow 1,$$

where P is a pro-p-group.

(e) Every extension of G by a pro-p-group splits.

As a corollary:

Corollary 12.22. *A free pro-p-group has cohomological dimension ≤ 1.*

We begin the proof with a lemma and some definitions.

Lemma 12.23. *Let H be a closed normal subgroup of the profinite group E, and let H' be an open subgroup of H. Then there exists an open subgroup H'' of H, contained in H', and normal in E. Moreover, if H' is normal in H and H/H' is abelian then H/H'' is abelian.*

Proof. Let $N = N(H')$ be the normalizer of H' in E, $N(H') = \{x \in E \mid xH'x^{-1} = H'\}$. We let E 'act' on H' by conjugation $\mu : E \times H' \to H$, which ends up in H, because H' is not normal in E.

Notice $N = E - pr_1\left(\mu^{-1}(R)\right)$, where $pr_1 : E \times H' \to E$, and $R = H - H'$. Verbally: the complement of the normalizer is the set of $e \in E$ such that there exists $h' \in H'$ which disproves that e belongs to the normalizer: $eh'e^{-1}$ is not in H'.

Now μ is continuous and H' is open, it implies $\mu^{-1}(R)$ is closed, but pr_1 is proper, which implies $pr_1\left(\mu^{-1}(R)\right)$ is closed, it implies then N is open. Therefore the number of conjugates of H' is finite. Set $H'' = \bigcap_{g \in E} gH'g^{-1}$, which is clearly normal in E and by the above, being a finite intersection of subgroups of finite index in $H = gHg^{-1}$, is itself of finite index in H.

For the last part, if H' is normal in H and H/H' is abelian, then the injective homomorphism

$$H/H'' \to \prod_{\sigma \in E} H/\sigma H'\sigma^{-1}$$

shows that H/H'' is abelian. □

Definition 12.24. Let E, G and W be groups. Let $f : G \to W$ be a group homomorphism. The **pull-back** of E by f is defined as:

$$E_f := E \times_W G = \{(e, g) \in E \times G \mid \pi(e) = f(g)\}.$$

It makes the following square commutative:

$$\begin{array}{ccc} E_f & \longrightarrow & G \\ \downarrow & & \downarrow f \\ E & \xrightarrow{\pi} & W \end{array}$$

Definition 12.25. The group G has the **extension lifting property** if for every extension $1 \longrightarrow P \longrightarrow E \xrightarrow{\pi} W \longrightarrow 1$ of profinite groups, every $f : G \to W$ lifts to a morphism $f' : G \to E$, i.e. if there exists an f' such that $f = \pi \circ f'$.

$$\begin{array}{ccc} & & G \\ & \overset{f'}{\swarrow} & \downarrow f \\ E & \xrightarrow[\pi]{} & W \end{array}$$

This is equivalent to saying that the extension

$$1 \longrightarrow P \longrightarrow E_f \longrightarrow G \longrightarrow 1,$$

splits, where E_f is the pull-back of E by f. The equivalence follows using the diagram,

$$\begin{array}{ccccccc} 1 & \longrightarrow & P & \longrightarrow & E & \xrightarrow{\pi} & W \\ & & \| & & \uparrow & \overset{f'}{\swarrow} & \uparrow f \\ 1 & \longrightarrow & P & \longrightarrow & E_f & \longrightarrow & G \end{array}$$

by defining $f' = s \circ g$. In the other direction take $W = G$ and $f = \mathrm{id}_G$.

Proof of Proposition 12.21. $(a) \Longrightarrow (c)$: If $\mathrm{cd}_p \leq 1$, then the cocycle must be a coboundary. $c = db$, i.e

$$c(g_1, g_2) = \sigma.b(g_1) - b(g_1 g_2) + b(g_1) \tag{12.3}$$

We change the settheoretical section σ to a map $t : G \to E$ "translating" with b^{-1}, i.e $t(g) := b(g)^{-1}\sigma(g)$, but now notice that, the equation (12.3) presicely means that t is a group homomorphism

$$\sigma(g_1)\sigma(g_2)\sigma(g_1 g_2)^{-1} = c(g_1, g_2) = g_1 b(g_2) - b(g_1 g_2) + b(g_1)$$

The first equality follows from the definition of $c(g_1, g_2)$ and the last equality follows from (12.3), and moreover the last term is equal to

$$\sigma(g_1)b(g_2)\sigma(g_1)^{-1} - b(g_1 g_2) + b(g_1)$$

if we rearrange:

$$\sigma(g_1)b(g_2)\sigma(g_1)^{-1}$$

we get

$$\sigma(g_1)\sigma(g_2)\sigma(g_1g_2)^{-1} = \sigma(g_1)b(g_2)\sigma(g_1)^{-1} + b(g_1) - b(g_1g_2)$$

Rearranging again and canceling $\sigma(g_1)$, we write multiplicatively:

$$\sigma(g_1)\left[b(g_2)^{-1}\sigma(g_2)\right] = b(g_1)\left[b(g_1g_2)^{-1}\sigma(g_1g_2)\right]$$

Now, if we move $b(g_1)$ to the other side of the last equation and we use the definition of t, we get $t(g_1)t(g_2) = t(g_1g_2)$. Beware that additive notation means composition in the abelian group A, whereas multiplicative notation is composition in the not necessary abelian group E. This finally proves $(a) \Longrightarrow (c)$

$(c) \Longrightarrow (a)$: Let P be a finite abelian p-group if (c) holds, then every group extension of G

$$1 \longrightarrow P \longrightarrow E \longrightarrow G \longrightarrow 1$$

splits. By theorem 12.20 $\mathrm{H}^2(G, P) \cong \mathrm{Ext}(G, P)$, hence $\mathrm{H}^2(G, P) = 0$. An arbitrary G-module A killed by p is the union of its finite submodules. Taking the inductive limit, we see that $\mathrm{H}^2(G, A) = 0$, hence $\mathrm{cd}_p G \leq 1$.

$(c) \Longrightarrow (b)$: Is clear, because we know that liftings $f' : G \to E$ of f are in $1-1$ correspondence with sections $s : G \to E_f$ of $E_f \to G$.

$(b) \Longrightarrow (c)$: Consider an extension

$$1 \longrightarrow P \longrightarrow E_0 \longrightarrow G \longrightarrow 1$$

of G by a finite abelian group P killed by p. Let us choose a normal subgroup H of E_0 such that $H \cap P = 1$; the projection $E_0 \to G$ identifies H with an open normal subgroup of G. Set $E = E_0/H$ and $W = G/H$. We have an exact sequence

$$1 \longrightarrow P \longrightarrow E \longrightarrow W \longrightarrow 1$$

By (b) the morphism $G \to W$ lifts to E. Since the square

$$\begin{array}{ccc} E_0 & \longrightarrow & G \\ \downarrow & & \uparrow \\ E & \longrightarrow & W \end{array}$$

is Cartesian, i.e, E_0 is the pullback, one deduces that G lifts to E_0, i.e E_0 splits.

It is clear $(e) \Longrightarrow (c)$.

Thus it remainds to show that $(c) \Longrightarrow (e)$ Suppose

$$1 \longrightarrow P \longrightarrow E \longrightarrow G \longrightarrow 1$$

is an extension of G by a pro-p-group P: Let X be the set of pairs (P', s), where P' is closed in P and normal in E, and where s is the lifting of G into the extension

$$1 \longrightarrow P/P' \longrightarrow E/P' \longrightarrow G \longrightarrow 1$$

We order X by defining $(P_1', s_1') \geq (P_2', s_2')$ if $P_1' \subset P_2'$ and if S_2 is the composition of s_1 with the map $E/P_1' \to E/P_2'$. The ordered set is inductive. By Zorn's lemma there exists a maximal element (P', s). We have to show $P' = \{1\}$. Assume $P' \neq \{1\}$ then by the first Sylow theorem for finite groups, there exists a normal open subgroup P_0 of P' of index p. By lemma 12.23

$$\bar{P}_0 = \bigcap_{\sigma \in E} \sigma P_0 \sigma^{-1}$$

is open in P', normal in E and $P'/\bar{P}_0$ is abelian.

Consider the diagram:

$$\begin{array}{ccccccccc} & & & & & & G & & \\ & & & & & \overset{\bar{s}}{\swarrow} & \downarrow{\scriptstyle s'} & & \\ 1 & \longrightarrow & P'/\bar{P}_0 & \longrightarrow & E/\bar{P}_0 & \xrightarrow{\pi} & E/P' & \longrightarrow & 1 \end{array}$$

Since $P'/\bar{P}_0$ is finite abelian, there exists a lifting $\bar{s} : G \to E/\bar{P}_0$ of s'. The composition with

$$E/\bar{P}_0 \xrightarrow{\pi} E/P' \xrightarrow{\pi'} G$$

gives

$$(\pi_0 \circ \pi) \circ \bar{s} = \pi_1 \circ s' = \mathrm{id},$$

hence $\bar{s}$ is a section of $E/\bar{P}_0 \to G$ which lifts s', i.e, $\left(\bar{P}_0, \bar{s}\right) > (P', s')$, which contradicts the maximality of (P', s') □

Definition 12.26. Let I be a set, and let $L(I)$ be the free group generated by the elements x_i indexed by I. Let X be the family of normal subgroups M of $L(I)$ such that:

(i) $L(I)/M$ is a finite p-group,

(ii) M contains almost all the x_i (i.e, all but a finite number).

Set $F(I) = \lim L(I)/M$. The group $F(I)$ is a pro-p-group which one calls the **free pro-p-group generated by the x_i**.

The adjective free is justified by the following result:

Proposition 12.27. *If G is a pro-p-group, the morphisms of $F(I)$ into G are in bijective correspondence with the families $(g_i)_{i \in I}$ of elements of G which tend to zero along the filter made up of the complements of finite subsets.*

More precisely, one associates to the morphism $f : F(I) \to G(I)$ the family

$$(g_i) = (f(x_i)).$$

Bemerkung 12.28. Convergence in a not necesarily countable set S to a point x in a topology space means, that any open neighborhood of x contains all but finitely many of the elements of S. In our situation, the topology has a base of neighborhood of $1 \in G$ consisting of open normal subgroups. Hence a set S convergest to 1 if and only if for every continuos map $G \to A$ (finite group), all but finitely many elements of S are "killed" i.e are mapped to $1 \in A$.. The set I of standar generators of a free pro-p-group $F(I)$ do exactly this by construction, as $F(I)$ is the profinite limit of precisely those quotient of the free group on the set I which kill almost all elements.

Proof of Corollary 12.22. We will check property (e). Let $E/P = G$ be an extension of $G = F(I)$ by a profinite p-group P, and let x_i be the canonical generators of $F(I)$. Let $U : G \to E$ be a continuos section includind the neutral element and let $e_i = s(x_i)$. Since the x_i converges to 1, this is also true for the e_i, and Proposition 12.27 shows that there exists a morphism $s : G \to E$ such that $s(x_i) = e_i$. Therefore the extension E splits. □

Vortrag 13

Kohomologie von pro-p Gruppen

Alexander Ivanov
31.1.2006

Konvention. Es bezeichnet im Folgenden stets p eine Primzahl, n eine ganze positive Zahl, I eine beliebige Indexmenge. Dies wird aus Übersichtlichkeitsgründen im gesamten Vortrag verwendet. $\#(X)$ bezeichne die Kardinalität von X.

13.1 Einfache Moduln

Definition 13.1. Ein R-Modul M heißt **einfach**, genau dann wenn M keine nicht-trivialen Untermoduln enthält. Das heißt, Untermoduln von M sind nur 0 und M selber.

Proposition 13.2. *Sei G eine pro-p-Gruppe, $A \in \mathcal{C}_G$ ein einfacher Modul mit $pA = 0$. Dann ist $A \simeq \mathbb{Z}/p\mathbb{Z}$, mit trivialer Operation.*

Beweis. Sei $a \in A, a \neq 0$. Da G auf A diskret operiert, ist der Stabilisator

$$U := \mathrm{Stab}_G(a) = \{x \in G \mid xa = a\}$$

offen in G. Die Anzahl der Konjugierten von a ist damit gleich $k := (G : U) < \infty$, da U offen in G, und offene Untergruppen haben in proendlichen Gruppen immer einen endlichen Index.

Dann ist offensichtlich das Erzeugnis von a in A als $\mathbb{Z}[G]$-Modul $\langle a\rangle_{\mathbb{Z}[G]} = \langle a_1, \ldots, a_k\rangle_{\mathbb{Z}}$, wobei $a_1, \ldots, a_k$ alle Konjugierten von a sind. Da $a \neq 0$, ist $0 \neq \langle a\rangle_{\mathbb{Z}[G]}$ ein Untermodul von A, also muss $A = \langle a\rangle_{\mathbb{Z}[G]} = \langle a_1, \ldots, a_k\rangle_{\mathbb{Z}}$ gelten. Daher ist A als ein $\mathbb{Z}$-Modul endlich erzeugt. Da $pA = 0$, ist A auch noch ein Torsionsmodul und da jede endlich erzeugte Torsionsgruppe endlich ist, ist A somit endlich.

Dann gibt es einen offenen Normalteiler $U \triangleleft G$, sodass die endliche Gruppe G/U dann diskret auf A operiert; die maximale Wahl von U ist der Schnitt der Konjugierten von $\mathrm{Stab}_G(a)$.

G ist eine pro-p-Gruppe $\Rightarrow G/U$ ist eine p-Gruppe. $pA = 0 \Rightarrow p \mid \#(A)$. Wir schreiben nun die Bahnengleichung der Operation von G/U auf A auf:

$$\#(A) = \#\left(A^{G/U}\right) + \#\left(\bigcup_{\#(G/U.x)>1} G/U.x\right).$$

Es ist aber auch $p \mid \#(G/U.x)$ für alle $x \in A$, mit $\#(G/U.x) > 1$, da Anzahl der Elemente einer endlichen Bahn ein Teiler der Ordnung der operierender Gruppe ist, und diese ist eine p-Potenz. Damit muss auch $p \mid \#\left(A^{G/U}\right)$ gelten, und da $0 \in A^{G/U}$, ist $\#\left(A^{G/U}\right) > p$.

Also ist $0 \neq A^{G/U}$ ein G/U-Untermodul von A, und damit auch ein G-Untermodul von A. Da er ungleich 0 ist, muss er ganz A sein, da A einfach $\Rightarrow A = A^G$. Offensichtlich muss $A^G = \mathbb{Z}/p\mathbb{Z}$ gelten, da $pA = 0$, A einfach ist. Es folgt: $A = A^G = \mathbb{Z}/p\mathbb{Z}$, mit trivialer Operation. □

Korollar 13.3. *Jeder endliche diskrete p-primäre G-Modul A hat eine Kompositionsreihe, deren aufeinanderfolgende Quotienten isomorph zu $\mathbb{Z}/p\mathbb{Z}$ sind.*

Beweis. Dies folgt trivial aus der Proposition 13.2. Man muss nur induktiv die zu $\mathbb{Z}/p\mathbb{Z}$ isomorphen G-Untermoduln von dem wegen der Endlichkeit von A, wie im Beweis der Proposition gezeigt, nichttrivialen Untermodul A^G aus A rausteilen. □

Proposition 13.4. *Es gilt:* $\mathrm{cd}(G) \leq n \iff \mathrm{H}^{n+1}(G, \mathbb{Z}/p\mathbb{Z})$. *Hier trägt $\mathbb{Z}/p\mathbb{Z}$ die triviale G-Operation.*

Beweis. Aus Proposition 12.11 aus Vortrag 12 folgt:

$$\mathrm{cd}_p(G) \leq n \iff \mathrm{H}^{n+1}(G, A)$$

für jedes einfache $A \in \mathscr{C}_G$, mit $pA = 0$. Mit der Proposition 13.2 ist dann $A = \mathbb{Z}/p\mathbb{Z}$, es gilt also: $\mathrm{cd}_p(G) \leq n \iff \mathrm{H}^{n+1}(G, \mathbb{Z}/p\mathbb{Z})$.

Sei $\ell \neq p$ eine weitere Primzahl. Wir wissen $\mathrm{H}^q(G, A) = \varinjlim \mathrm{H}^q(G/N, A^N)$ und alle G/N sind endliche p-Gruppen, Nun wenden wir Proposition 12.11 auf ℓ an: Ist A ein ℓ-primärer G-Modul, so ist für geeignete i und j:

$$p^i \,\mathrm{H}^q(G, A) = \ell^j \,\mathrm{H}^q(G, A) = 0,$$

und da p und ℓ prim, sind p^i und ℓ^j teilerfremd, also für geeignete k und s die Gleichung $1 = kp^i + s\ell^j$ gilt, folgt damit

$$\mathrm{H}^q(G, A) = (kp^i + sl^j)\,\mathrm{H}^q(G, A) = 0.$$

Somit folgt $\mathrm{cd}_\ell(G) = 0$ und folglich $\mathrm{cd}(G) = \sup\{\mathrm{cd}_\ell(G) \mid \ell \text{ prim}\} = \mathrm{cd}_p(G)$. Damit ist die Proposition bewiesen. □

Korollar 13.5. *Sei* $\mathrm{cd}(G) = n$ *und* $A \neq 0$ *ein endlicher p-primärer diskreter G-Modul. Dann ist* $\mathrm{H}^n(G, A) \neq 0$.

Beweis. Mit dem Korollar zur Proposition 13.2 existiert ein surjektives $f : A \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$. Dann ist auch die erzeugte Abbildung $\mathrm{H}^n(G, A) \twoheadrightarrow \mathrm{H}^n(G, \mathbb{Z}/p\mathbb{Z})$ surjektiv, da $\mathrm{cd}(G) \leq n$. Wäre $\mathrm{H}^n(G, \mathbb{Z}/p\mathbb{Z}) = 0$, so wäre $\mathrm{cd}(G) \leq (n-1)$ nach der Proposition 13.4 im Widerspruch zur Voraussetzung. □

13.2 H^1 und Erzeuger

Konvention. Ab sofort kürzen wir bei der Schreibweise wie folgt ab:

$$\mathrm{H}^i(G) := \mathrm{H}^i(G, \mathbb{Z}/p\mathbb{Z}),$$

wobei $\mathbb{Z}/p\mathbb{Z}$ mit der trivialen Operation versehen ist.

Wir haben insbesondere: $\mathrm{H}^1(G) = \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$. Weiterhin können wir für Gruppen G_1, G_2 und ein Homomorphismus $f : G_1 \to G_2$, die auf den ersten Kohomologiegruppen induzierte Abbildung $\mathrm{H}^1(f) : \mathrm{H}^1(G_2) \to \mathrm{H}^1(G_1)$ identifizieren als $(\circ f) : \mathrm{Hom}(G_2, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Hom}(G_1, \mathbb{Z}/p\mathbb{Z}), \alpha \mapsto \alpha \circ f$, welche durch Vorschalten von f definiert ist.

Proposition 13.6. *Seien G_1, G_2 pro-p-Gruppen, $f : G_1 \to G_2$. Dann gilt: f surjektiv $\iff$ $\mathrm{H}^1(f)$ injektiv.*

Beweis. „$\Rightarrow$“ : Sei f surjektiv, $\alpha, \beta \in \mathrm{H}^1(G_2)$ mit $\mathrm{H}^1(f)(\alpha) = \mathrm{H}^1(f)(\beta)$. Es folgt:

$$\alpha f = \mathrm{H}^1(f)(\alpha) = \mathrm{H}^1(f)(\beta) = \beta f \Rightarrow \forall\, x \in G_1 : \alpha f(x) = \beta f(x) \Rightarrow \alpha(y) = \beta(y) \forall\, y \in G_2,$$

da f surjektiv. Es folgt $\alpha = \beta$, und damit die Injektivität von $\mathrm{H}^1(f)$.

„$\Leftarrow$“ : Nehmen wir an $f(G_1) \neq G_2$. Wir wollen zeigen, dass dann $\mathrm{H}^1(f)$ nicht injektiv ist. Es gibt ein $P_2 = G_2/H$, $H \lhd G$, H offen in G, also $\#(P_2) < \infty$, mit $\overline{f} : G_1 \to P_2$ nicht surjektiv (sonst, falls $\overline{f} : G_1 \to G_2/U$ surjektiv für alle offenen Normalteiler U von G_2, wäre auch $f : G_1 \to \lim G_2/U = G_2$ surjektiv). Es sei $P_1 = \overline{f}(G_1) \subsetneq P_2$. Das Ziel ist nun ein $P \lhd P_2$ mit $P_1 \subset P$ und $(P_2 : P) = p$ zu konstruieren. Wir haben: P_2 ist eine p-Gruppe, und damit ist $Z(P_2) \neq 1$, wobei $Z(X)$ das Zentrum der Gruppe X sein soll.

Wir beiweisen die Existenz von P induktiv. Die Induktion geht nach

$$s := \#(P_2) + (P_2 : P_1).$$

Dabei unterscheinden wir die zwei folgenden Fälle:

Fall 1. $Z(P_2) \bigcap P_1 \neq 1$: in diesem Fall wird $1 \neq Z(P_2) \bigcap P_1 \lhd P_2$ aus P_2 komponentenweise rausgeteilt, dabei heißt komponentenweise, dass man jeweils die zu $\mathbb{Z}/p\mathbb{Z}$ isomophen Glieder der Kompositionsreihe von $Z(P_2) \bigcap P_1$, die als Untergruppen des Zentrums von P_2 in P_2 sowie in P_1 normal sind, rausteilt. Damit wird $\#(P_2)$ und damit auch s kleiner.

Fall 2. $Z(P_2) \bigcap P_1 = 1$: man betrachte einfach $Z(P_2) \bigcap P_1$ anstatt von P_1. Da das Zentrum nicht-trivial ist, ist auch $Z(P_2)P_1 \supsetneq P_1$, und offensichtlich $P_1 \lhd Z(P_2)P_1$. Der betrachtete Index $(P_2 : P_1)$ wird kleiner, und damit auch s.

Irgendwann müssen wir also induktiv bei $P_1 = 1$ ankommen. Da wir ständig nur zu *Normalteilern* der betrachteten Gruppen Übergangen sind, und da wir *nur p-Gruppen* betrachten, lassen sich immer Kompoitionsreihen konstruiern, die in trivialer Weise zum Resultat führen. Somit läßt sich auch das gesuchte P auf die gleiche Weise konstruieren: nun haben wir also: $P_1 \subset P \lhd P_2$, mit $P_2/P \cong \mathbb{Z}/p\mathbb{Z}$. Damit haben wir die folgenden Abbildungen:

$$G_1 \xrightarrow{f} G_2 \xrightarrow{\pi_1} P_2 \xrightarrow{\pi_2} P_2/P \xrightarrow{\backsim} \mathbb{Z}/p\mathbb{Z},$$

wobei π_1, π_2 kanonische Projektionen sind, und die letzte Abbildung ein Isomorphismus. $\pi_2 \circ \pi_1$ ist damit ein Element von $\mathrm{H}^1(G_2)$ Es ist aber auch $\pi_1 \circ f(G_1) = P_1 \subset P$, wird also von π_2 auf 0 abgebildet, also: $\mathrm{H}^1(f)(\pi_2 \circ \pi_1) = 0$. Dabei waren aber π_1, π_2 kanonische Projektionen, also ist $\pi_2 \circ \pi_1 \neq 0$. Damit $0 \neq \pi_2 \circ \pi_1 \in \ker(\mathrm{H}^1(f))$, also $\mathrm{H}^1(f)$ nicht injektiv. Damit ist der Satz bewiesen. □

Sei nun

$$G^* := \bigcap_{G \xrightarrow{f} \mathbb{Z}/p\mathbb{Z}, \text{stetig}} \ker(f).$$

Lemma 13.7. *Es gilt*

$$G^* = \langle G^p, \overline{(G,G)} \rangle$$

Beweis. „$\supseteq$“: klar, dass $G^p \subseteq G^*$ weil die Abbildungen nach $\mathbb{Z}/p\mathbb{Z}$ gehen, und nur stetige Abbildungen betrachtet werden. $\overline{(G,G)} \subseteq G^*$ da $\mathbb{Z}/p\mathbb{Z}$ abelsch. Damit muss auch $\langle G^p, \overline{(G,G)} \rangle \subseteq G^*$.

„$\subseteq$“: Es ist $G^p \lhd G$, $\overline{(G,G)} \lhd G$. Damit auch $\langle G^p, \overline{(G,G)} \rangle \lhd G$. Wir teilen es raus. Es ist $G/\langle G^p, \overline{(G,G)} \rangle \cong \prod_I \mathbb{Z}/p\mathbb{Z}$, da es ja eine abelsche Gruppe (Kommutator wird rausgeteilt), die von p gekillt wird (p-Potenzen werden rausgeteilt), ist. Damit haben wir die kanonischen Projektionen:

$$\overline{\pi_i} : G/\langle G^p, \overline{(G,G)} \rangle \longrightarrow \mathbb{Z}/p\mathbb{Z}, \quad \overline{\pi_i}((g_j)_{j \in I}) = g_i.$$

Der Schnitt der Kerne dieser Projektionen ist schon 0. Schaltet man noch vor jede von denen die Projektion von G nach $G/\langle G^p, \overline{(G,G)} \rangle$, so erhält man Abbildungen von G nach $\mathbb{Z}/p\mathbb{Z}$, Schnitt derer Kerne in $\langle G^p, \overline{(G,G)} \rangle$ liegt. Damit ist $G^* \subseteq \langle G^p, \overline{(G,G)} \rangle$. □

G/G^* ist abelsch. Das duale zu G/G^* ist $\mathrm{Hom}(G/G^*, \mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z}) = \mathrm{H}^1(G)$.

Damit haben wir eine wichtige Folgerung aus dem Lemma: G/G^* und $\mathrm{H}^1(G)$ sind dual zu einander. Die Proposition 13.6 läßt sich damit umformulieren:

Proposition 13.8. *$f : G_1 \to G_2$ surjektiv $\iff$ $\overline{f} : G_1/G_1^* \to G_2/G_2^*$ surjektiv.*

Proposition 13.9. *Sei $\theta : \mathrm{H}^1(G) \to (\mathbb{Z}/p\mathbb{Z})^{(I)}$ ein Homomorphismus. Dann gilt:*

(1) Es gibt ein $f : F(I) \to G$ mit $\theta = \mathrm{H}^1(f)$.

(2) θ injektiv $\iff$ f surjektiv.

(3) θ bijektiv, $\mathrm{cd}(G) \leq 1 \Rightarrow f$ ist ein Isomorphismus.

Beweis. (1) Wir dualisieren $\theta : \mathrm{H}^1(G) \to (\mathbb{Z}/p\mathbb{Z})^{(I)}$ und erhalten: $\theta^\vee : (\mathbb{Z}/p\mathbb{Z})^I \to G/G^*$ ein Homomorphismus. Damit haben wir ein Homomorphismus:

$$\overline{f} : F(I) \longrightarrow F(I)/F(I)^* = (\mathbb{Z}/p\mathbb{Z})^I \longrightarrow G/G^*.$$

Diesen liften wir mit der Liftungseigenschaft von $F(I)$ zu $f : F(I) \to G$. Damit haben wir das f gefunden. Nun müssen wir noch zeigen, dass $\mathrm{H}^1(f) = \theta$ gilt. Wir erinnern uns an $\mathrm{H}^1(f) = (\circ f)$ Vorschalten von f. Das vorschalten von $f : F(I) \to G$ ist aber nichts anderes als das Vorschalten von $\overline{f} : F(I)/F(I)^* \to G/G^*$, da sich f und $\overline{f}$ *im Wesentlichen* nicht unterscheiden. Das zu $\overline{f}$ duale Objekt ist aber gerade θ, das folgt aus der Konstruktion von $\overline{f}$. Damit haben wir:

$$\theta = f^\vee = (\circ \overline{f}) = (\circ f) = \mathrm{H}^1(f).$$

(2) folgt aus der Proposition 13.6.

(3) im letzten Vortrag wurde bewiesen, dass aus $\mathrm{cd}(G) \leq 1$ die Existenz von einem Homomorphismus $g : G \to F(I)$ mit $f \circ g = 1$ folgt. Dualisiert ergibt: $\mathrm{H}^1(g) \circ \mathrm{H}^1(f) = 1$. Ist nun auch noch $\theta = \mathrm{H}^1(f)$ bijektiv so ist auch $\mathrm{H}^1(g)$ bijektiv, insbesondere auch injektiv. Nach (b) ist damit g surjektiv. Mit $f \circ g = 1$ folgt dass f, g Isomorphismen.

□

Korollar 13.10. *$G \cong F(I)/R$ für ein $R \triangleleft F(I) \iff \mathrm{H}^1(G)$ hat als $\mathbb{Z}/p\mathbb{Z}$-Vektorraum ein Basis mit Kardinalität kleiner als $\#(I)$.*

Beweis. „⇐“: Sei B eine Basis von $\mathrm{H}^1(G)$ als $\mathbb{Z}/p\mathbb{Z}$-Vektorraum mit $\#(B) < \#(I)$. Dann haben wir in kanonischer Weise eine Injektion: $\theta : \mathrm{H}^1(G) \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^{(I)}$. Damit gibt es mit dem Teil (1) der Proposition ein $f : F(I) \to G$ mit $\mathrm{H}^1(f) = \theta$. θ ist nach Konstruktion injektiv, damit ist nach Teil (2) der Proposition f surjektiv. Man setze nun einfach $R := \ker(f)$.

„⇒“: ist $G \cong F(I)/R$, so k[nnen wir $\overline{f} : F(I)/R \to G$, den Isomorphismus zu einer surjektiven Abblidung $f : F(I) \to G$ liften. Nach Teil (2) der Proposition ist dann $\mathrm{H}^1(f)$ injektiv. Damit haben wir eine Einbettung $\theta : \mathrm{H}^1(G) \to (\mathbb{Z}/p\mathbb{Z})^{(I)}$. Dies sind zwei $\mathbb{Z}/p\mathbb{Z}$-Vektorräume, θ ein injektiver (Vektorraum-) Homomorphismus zwischen denen. Damit ist die Dimension von $\mathrm{H}^1(G)$, gleich der Kardinalität jeder Basis von $\mathrm{H}^1(G)$ kleiner als die Dimension von $(\mathbb{Z}/p\mathbb{Z})^{(I)}$, die gleich der Kardinalität von I ist. □

Korollar 13.11. *G frei $\iff \mathrm{cd}(G) \leq 1$.*

Beweis. „⇐“: bekannt aus dem Vortrag 12.

„⇒“: $\mathrm{cd}(G) \leq 1$, $(e_i)_{i \in I}$ Basis von $\mathrm{H}^1(G)$. Dann haben wir: $\theta : \mathrm{H}^1(G) \to (\mathbb{Z}/p\mathbb{Z})^{(I)}$ ein Isomorphismus. Mit Teil (3) der Proposition folgt nun $G \cong F(I)$. □

Korollar 13.12. *Sei G frei, H eine abgeschlossene Untergruppe von G. Dann ist auch H frei.*

Beweis. G frei $\Rightarrow \mathrm{cd}(G) \leq 1$, H abgeschlossene Untergruppe von $G \Rightarrow \mathrm{cd}(H) \leq \mathrm{cd}(G) \leq 1 \Rightarrow H$ frei, nach dem letzten Korollar. □

Definition 13.13. Seien $\forall\ i \in I$: $g_i \in G$. Man sagt die (g_i) **erzeugen G topologisch** genau dann, wenn die algerbraisch von den g_i's erzeugte Gruppe $\langle g_i \mid i \in I \rangle$ dicht in G liegt. Dies ist äquivalent dazu dass, für jeden offenen Normalteiler $U \triangleleft G$ gilt: $G/U = \langle g_i \mid i \in I \rangle$.

Proposition 13.14. *Sei hier $I = 1, 2, \ldots, n$. Seien $g_1, \ldots, g_n \in G$. Dann sind die folgenden Aussagen äquivalent:*

(a) $g_1, \ldots, g_n$ erzeugen G topologisch.

(b) $g : F(I) \to G$, erzeugt bei den g_i's ist surjektiv.

(c) $G/G^* = \langle \overline{g_i} \mid i \in I \rangle$, G/G^* wird durch die Nebenklassen von den g_i's erzeugt.

(d) $\forall\ \pi \in \mathrm{H}^1(G), \pi(g_i) = 0$, gilt $\pi = 0$.

Beweis. Es sei

$$F(I) = \lim_{M \lhd L, \text{offen}} L(x_1, \ldots, x_n)/M, \quad G = \lim_{U \lhd G, \text{offen}} /U.$$

(a) $\Rightarrow$ (b): zu jedem offenen Normalteiler U von G haben wir die surjektive Abbildung $f : L(n) \to G$, gegeben durch $f(x_i) = g_i$. Ist $M = \ker(f)$, so haben wir einen Isomorphismus $L(n)/M \cong G/U$. Nun ist diese Relation für alle offenen Normalteiler von G kompatibel, das heißt das folgende Diagramm für alle U_1, U_2 mit $U_1 \subset U_2$ kommutiert:

$$\begin{array}{ccc} L(n)/M_1 & \xrightarrow{\sim} & G/U_1 \\ \downarrow & & \downarrow \\ L(n)/M_2 & \xrightarrow{\sim} & G/U_2 \end{array}.$$

Dies ist aber kanonisch erfüllt, da die Abbildungen ja entweder einfache Projektionen sind, oder x_i nach g_i schicken. Damit kann man nun zum Limes übergehen, und man hat die surjektive Abbildung

$$F(I) = \lim_{M \lhd L(I), \text{offen}} L(I)/M \twoheadrightarrow \lim_{U \lhd G, \text{offen}} G/U = G,$$

die bei den g_i's gegeben ist.

(b) $\Rightarrow$ (a): Sei $F(n) \twoheadrightarrow G$, $x_i \mapsto g_i$ ein surjektiver Homomorphismus. Damit haben wir die surjektiven Homomorphismen: $L(n) \twoheadrightarrow G/U$ für alle offenen Normalteiler U von G. Ist M_U Kern eines solchen, dann ist $L(n)/M_U \cong G/U$, dabei ist: $x_i \mapsto \overline{g_i}$. Damit sieht man, dass G/U durch die $\overline{g_i}$'s erzeugt wird, da die Abbildung surjektiv ist, und da U offen, ist G/U endlich. Damit ist für jeden offenen Normalteiler U von G, G/U durch die Bilder der g_i's erzeugt. Dies ist dazu äquivalent, dass $g_1, \ldots, g_n$ G topologisch erzeugen.

(b) $\Rightarrow$ (c): Wir verwenden hier die Proposition 13.6 bis: Ist $F(n) \twoheadrightarrow G$ surjektiv, so auch die induzierte Abbildung $(\mathbb{Z}/p\mathbb{Z})^n = F(I)/F(I)^* \twoheadrightarrow G/G^*$, die Abbildung ist aber durch $x_i \mapsto \overline{g_i}$ gegeben, und damit wird G/G^* durch die $\overline{g}$ erzeugt. Ist umgekehrt $G/G^* = \langle \overline{g_i} \mid i \in I \rangle$, so ist die Abbildung $F(I)/F(I)^* \twoheadrightarrow G/G^*, x_i \mapsto \overline{g_i}$ surjektiv. Damit ist nach der Proposition 13.6 bis auch die Abbildung $F(I) \to G, x_i \mapsto g_i$ surjektiv.

(c) $\Rightarrow$ (d): Sei $G/G^* = \langle \overline{g_i} \mid i \in I \rangle$, $\pi : G \to \mathbb{Z}/p\mathbb{Z}$, $\pi(g_i) = 0$. $G^* \lhd G$ und $G^* \subset \ker(\pi) \Rightarrow \exists\ \tilde{\pi} : G/G^* \to \mathbb{Z}/p\mathbb{Z}$ mit $\tilde{\pi}(\overline{x}) = \pi(x)$. Damit ist $0 = \pi(g_i) = \tilde{\pi}(\overline{g_i})$, also $\tilde{\pi}(G/G^*) = \langle \tilde{\pi}(\overline{g_i}) \mid i \in I \rangle = 0$, da Da $G^* \subset \ker(\pi)$ ist

$$\operatorname{im}(\pi) = \operatorname{im}\left(\widetilde{(\pi)}\right) = 0.$$

Es folgt $\pi = 0$.

(d) $\Rightarrow$ (c): Sei (d) erfüllt. Nehmen wir weiter an, $\langle \overline{g_i} \mid i \in I \rangle \subsetneq G/G^*$. G/G^* ist abelsch, damit ist jede Untergruppe ein Normalteiler: $\langle \overline{g_i} \mid i \in I \rangle \lhd G/G^*$, und zwar ein echter dank der Annahme. Nachdem wir ihn rausteilen definieren wir: $(G/G^*)/\langle \overline{g_i} \mid i \in I \rangle := R$. Dabei ist dieses R immer noch von der Form $\prod_s \mathbb{Z}/p\mathbb{Z}$, wo $0 < s \leq n$. Es gibt also ein Homomorphismus $\overline{\pi} : R \to \mathbb{Z}/p\mathbb{Z}$, $\overline{\pi} \neq 0$. Damit haben wir auch:

$$G \twoheadrightarrow G/G^* \twoheadrightarrow R \xrightarrow{\overline{\pi}} \mathbb{Z}/p\mathbb{Z}.$$

Die Komposition dieser Abbildungen liefert uns ein nichttrivialen Homomorphismus von G nach $\mathbb{Z}/p\mathbb{Z}$, der aber nach Konstruktion auf allen g_i's verschwindet. Das ist ein Widerspruch zur Annahme von (d). $\square$

Korollar 13.15. *Die minimale Anzahl von (topologischen) Erzugern von G ist gleich* $\dim \mathrm{H}^1(G)$ *(als $\mathbb{Z}/p\mathbb{Z}$-Vektorraum).*

Beweis. Erzeugen $g_1, \ldots, g_n$ G topologisch, so haben wir mit der Proposition 13.14, (a) $\Rightarrow$ (b) einen surjektiven Homomorphismus

$$f : F(n) \twoheadrightarrow G, x_i \longmapsto g_i$$

($L(n)$ ist dabei die freie Gruppe auf der Menge $\{x_1, \ldots, x_n\}$). Mit Proposition 13.6 ist dann $\mathrm{H}^1(f) : \mathrm{H}^1(G) \hookrightarrow \mathrm{H}^1(F(n)) = (\mathbb{Z}/p\mathbb{Z})^n$ injektiv. Diese Abbildung als $\mathbb{Z}/p\mathbb{Z}$-Vektorraumhomomorphismus angesehen, liefert uns $\dim \mathrm{H}^1(G) \leq n$. Ist umgekehrt $\dim \mathrm{H}^1(G) \leq n$, so haben wir eine injektive Abbildung $\mathrm{H}^1(G) \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^n$. Die liefert uns wiederum mit der Proposition 13.6 eine surjektive $F(n) \twoheadrightarrow G$, und mit der Proposition 13.14, (b) $\Rightarrow$ (a), haben wir ein topologisches Erzeugendenszstem $g_1, \ldots, g_n$ von G. □

Definition 13.16. (1) Diese Zahl n wird **Rang** von G genannt. Sei $I = 1, \ldots, n$, F eine pro-p-Gruppe, R ein abgeschlossener Normalteiler von F. Seien $r_1, \ldots, r_n \in R$.

(2) Man sagt, $r_1, \ldots, r_n$ **erzeugen $\boldsymbol{R}$ als Normalteiler von $\boldsymbol{F}$**, falls $\langle gr_ig^{-1} \mid i \in I, g \in F\rangle := R'$ dicht in R liegt.

13.3 H^2 und Relationen

Proposition 13.17. *Ist R ein abgeschlossener Normalteiler einer pro-p-Gruppe F, so gilt: $r_1, \ldots, r_n \in R$ erzeugen R als Normalteiler von F $\iff$ für alle $\pi \in \mathrm{H}^1(R)^{F/R}$ mit $\pi(r_i) = 0$ gilt $\pi = 0$.*

Bemerkung 13.18. Man hat $\mathrm{H}^1(R) = \mathrm{Hom}(R/R^*, \mathbb{Z}/p\mathbb{Z})$, F/R operiert auf R/R^* durch innere Automorphismen: $g \in F/R$, $r \in R/R^*$, so $g.r = grg^{-1}$. Damit operiert es auch auf $\mathrm{H}^1(R)$ durch: $\sigma \in \mathrm{H}^1(R)$, $\sigma : R/R^* \to \mathbb{Z}/p\mathbb{Z}$, $g \in F/R$: $g.\sigma(x) = \sigma(gxg^{-1})$

Beweis. „⇒“: Seien $(r_i)_{i\in I}$ Erzeuger von R als Normalteiler von F. Das äquivalent dazu, dass die gr_ig^{-1} eine dichte Untergruppe R' in R erzeugen. Sei $\pi \in \mathrm{H}^1(R)^{F/R}$, $\pi(r_i) = 0$. Dann ist $\pi(gxg^{-1}) = \pi(x)$ für alle $x \in R$, $g \in F/R$. Dann gilt für alle gr_ig^{-1}:

$$\pi(gr_ig^{-1}) = \pi(r_i) = 0.$$

Also auch $\pi(R') = 0$. Da π stetig ist, und R' dicht in R, ist auch $\pi(R) = 0$.

„⇐“: Sei $\forall\ \pi \in \mathrm{H}^1(R)^{F/R}$, $\pi(gr_ig^{-1}) = \pi(r_i) = 0 \Rightarrow \pi = 0$. Sei R' der kleinste Normalteiler von F, der durch die r_i's erzeugt wird. Trivialerweise ist $R' \subseteq R$. Dann haben wir eine Injektion: $R' \hookrightarrow R$, und damit ein $f : \mathrm{H}^1(R) \to \mathrm{H}^1(R')$. Ist $\pi \in \mathrm{H}^1(R)^F$, so gilt für alle $g \in F, r \in R$:

$$\pi(gr_ig^{-1}) = \pi(r_i), f \circ \pi(grg^{-1}) = f(\pi(grg^{-1})) = f(\pi(r)) = (f \circ \pi)(r) \Rightarrow f \circ \pi \in \mathrm{H}^1(R')^F.$$

Wir können also die Restriktion betrachten: $\overline{f} : \mathrm{H}^1(R)^F \to \mathrm{H}^1(R')^F$. Ist $\pi \in \ker(\overline{f})$, so $\pi \in \mathrm{H}^1(R)^F$ mit $f \circ \pi = 0$. f ist aber nichts anderes als das Vorschalten der kanonischen

Injektion $\Rightarrow f \circ \pi|_{R'} = \pi|_{R'} \Rightarrow \pi|_{R'} = f \circ \pi = 0 \Rightarrow \pi(R') = 0 \Rightarrow \pi(R) = 0$, nach Voraussetzung. Also ist $\overline{f}$ injektiv, und mit dem Korrolar zur Proposition 13.2 folgt, dass f injektiv ist. Mit der Proposition 13.6 folgt nun dass die ursprüngliche Injektion $R' \hookleftarrow R$ auch surjektiv ist $\Rightarrow R' = R$. □

Korollar 13.19. *R erzeugt von n Elementen als Normalteiler von F genau dann, wenn*

$$\dim \mathrm{H}^1(R)^{F/R} \leq n.$$

Beweis. „⇒“: Sei $R := \langle r_i \mid i \in I \rangle$ als Normalteiler von F. Sei $R' = \langle r_i \mid i \in I \rangle$ (topologisch). Wir haben einen (nach der Proposition 13.14, (a) ⇒ (b)) surjektiven Homomorphismus $F(n) \twoheadrightarrow R'$, gegeben durch die r_i's. Damit haben wir eine Injektion $\mathrm{H}^1(f) : \mathrm{H}^1(R') \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^n = \mathrm{H}^1(F(n))$. Ist $\pi \in \mathrm{H}^1(R)^{F/R}$, so entspricht es in eineindutiger Weise dem Homomorphismus $\pi|_{R'} \in \mathrm{H}^1(R')$. Diese Zuordnung ist eineindeutig, da auch jedes $\tilde{\pi} \in \mathrm{H}^1(R)$ sich in eindeutiger Weise zu einem $\pi \in \mathrm{H}^1(R)^{F/R}$ erweitern läßt, weil ja $\pi(gr_ig^{-1}) = \pi(r_i)$ für alle $g \in F$, alle r_i und alle $i \in I$ gelten muss und $R = \langle gr_ig^{-1} \rangle$ topologisch. Damit haben wir also $\mathrm{H}^1(R)^{F/R} \cong \mathrm{H}^1(R') \hookrightarrow (\mathbb{Z}/p\mathbb{Z})^n \Rightarrow \dim \mathrm{H}^1(R)^{F/R} \leq n$.

„⇐“: $\dim \mathrm{H}^1(R)^{F/R} \leq n \Rightarrow$ haben wir wegen der Dualität zwischen $\mathrm{H}^1(R)$ und R/R^* ein Satz von Erzeugenden $(r_i)_{i\in I}$ mit der Eigenschaft, dass für alle $\pi \in \mathrm{H}^1(R)^{F/R}$ gilt: $\pi(r_i) = 0 \Rightarrow \pi = 0$. Das sagt nichts anderes aus, als dass die Abbildung

$$\varphi : (R/R^*)^n \times \mathrm{H}^1(R)^{F/R} \hookrightarrow (\mathbb{Z}/p\mathbb{Z}), \varphi((x_i)_{i\in I} \times \pi) = \pi(x_1) \times \ldots \times \pi(x_n)$$

injektiv ist. Sei $\pi \in \mathrm{H}^1(R)^{F/R}$, $\pi(r_i) = 0$. Dann $\varphi\pi = 0 \Rightarrow \pi \in \ker(\varphi) \Rightarrow \pi = 0$. Damit müssen nach der Proposition 13.17 die $(r_i)_{i\in I}$ den Ring R als Normalteiler von F erzeugen. □

Definition 13.20. Die Dimension von $\mathrm{H}^1(R)^{F/R}$ wird **Rang des abgeschlossenen Normalteilers** R von F genannt.

Ab nun sei $F := F(n)$ die freie pro-p-Gruppe, erzeugt von n Elementen, R ein abgeschlossener Normalteiler von F, $G := F/R$, also ist G durch Erzeuger und Relationen gegeben.

Proposition 13.21. *Die folgenden Aussagen sind äquivalent:*

(a) Eine Untergruppe R von G ist als abgeschlossener Normalteiler von F vom endlichen Rang.

(b) $\mathrm{H}^2(G)$ hat eine endliche Dimension.

Falls (a) und (b) erfüllt, so gilt: $r = n - h_1 + h_2$, wobei $r = \mathrm{Rank}(R)$ und $h_i = \dim \mathrm{H}^i(G)$ für $i = 1, 2$.

Beweis. Wir haben $\mathrm{H}^2(F(n)) = 0$. Weiter nehmen wir ohne Beweis die Existenz der folgenden exakten Sequenz an:

$$0 \longrightarrow \mathrm{H}^1(G) \xrightarrow{\inf} \mathrm{H}^1(F(n)) \xrightarrow{\mathrm{res}} \mathrm{H}^1(R)^G \xrightarrow{\delta} \mathrm{H}^2(G) \longrightarrow 0 = \mathrm{H}^2(F(n)).$$

(ohne Beweis wird nur die Existenz von δ genommen, der Rest ist aus früheren Vorträgen bekannt, das $(\ )^G$ über dem $\mathrm{H}^1(R)$ kommt daher, dass das Bild der Restriktion unter G festgehalten wird:

$$g.\varphi(x) = \varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(x)).$$

Wegen der Exaktheit der Sequenz sieht man, dass $\mathrm{H}^1(R)$ und $\mathrm{H}^2(G)$ entweder beide endlich oder beide unendlich sind. Damit folgt (a) $\Rightarrow$ (b). Weiter hat man in der exakten Sequenz die alternierde Summe der Dimensionen, die gleich 0 ist:

$$h_1 + r = \dim \mathrm{H}^1(G) + \dim \mathrm{H}^1(R)^G = \dim \mathrm{H}^1(F(n)) + \dim \mathrm{H}^2(G) = n + h_2 \Rightarrow r = n - h_1 + h_2.$$

□

Korollar 13.22. *Sei G eine pro-p-Gruppe, so dass $\mathrm{H}^1(G)$, $\mathrm{H}^2(G)$ endlich. Sei $(x_1, \ldots, x_n)$ ein minimales System von Erzeugern von G. Die Anzahl der Relationen zwischen den x_i's ist gleich $\dim \mathrm{H}^2(G)$. (Man hat $g : F(n) \twoheadrightarrow G$, $g(f_i) = x_i$, wobei $F(n)$ durch die $(f_i)_{i\in I}$ erzeugt ist, mit*

$$\ker(g) =: R, \mathrm{Rank}(R) := \textit{(Anzahl der Relationen zwischen den } x_i\textit{'s)}).$$

Beweis. Wir haben nach dem Korollar zur Proposition 13.14

$$n = \dim \mathrm{H}^1(G),$$

da $(x_1, \ldots, x_n)$ minimales Erzeugendensystem von $G \Rightarrow n = h_1 \Rightarrow$ folgt mit der Proposition 13.21:

$$r = n - h_1 + h_2 = h_2.$$

□

13.4 Die Ungleichung von Golod und Shafarevich

Theorem 13.23 (Golod-Shafarevich-Ungleichung)**.** *Ist G eine pro-p-Gruppe, dann gilt:*

$$G \textit{ endlich} \quad \Longrightarrow \quad r(G) > \frac{1}{4} d(G)^2.$$

Dabei ist $r(G)$ die Anzahl der Relationen, durch die G gegeben ist, und $d(G)$ die minimale Anzahl der Erzeuger von G.

Zum Beweis brauchen wir das folgende Lemma (3.9.8) aus [NSW99]:

Lemma 13.24. *Sei G eine endliche pro-p-Gruppe, und A ein endlicher G-Modul mit $pA = 0$. Sei $\Lambda = \mathbb{F}_p[G]$. Dann gibt es ein exakte Sequenz der Form*

$$0 \longrightarrow A \longrightarrow \Lambda^{b_0} \longrightarrow \Lambda^{b_1} \xrightarrow{\delta} \Lambda^{b_2} \xrightarrow{\delta} \ldots,$$

wobei $\delta\left((\Lambda^{b_n})^G\right) = 0$ und $b_i = \dim \mathrm{H}^i(G, A)$.

Beweis von Theorem 13.23. Für jeden endlichen G-Modul A mit $pA = 0$ hat man eine folgende Zerlegung:

$$0 = A_0 \subseteq A_1 \subseteq \ldots \subseteq A_m = A, A_0 = 0, A_m = A, A_1 = A^G, A_{n+1}/A_n = (A/A_n)^G.$$

Dabei gilt (ohne Beweis):

$$A_n \neq A_{n+1}.$$

Ist $h : A \hookrightarrow B$ ein injektiver G-Homomorphismus, so folgt induktiv: $A_n = h^{-1}(B_n)$. Es sei im weiteren $c_n(A) = \dim(A_{n+1}/A_n)$, $P_A(t) = \sum_{i=0}^{n} c_i(A)t^n$. Für $0 < T < 1$ haben wir

$$\frac{1}{1-T} = 1 + T + T^2 + \ldots \text{ und } P_A(t)\frac{1}{1-t} = \sum_{n\geq 0} s_n(A)t^n,$$

wobei

$$s_n(A) = \sum_{i=0}^{n} c_i(A) = \dim(A^{n+1}).$$

Wir wenden nun das Lemma auf $A = \mathbb{F}_p$ an. Nun ist $\mathbb{F}_p[G]^G = \mathbb{F}_p[G] \Rightarrow (\mathbb{F}_p[G])_1 = \mathbb{F}_p$, und man erhält die folgende exankte Sequenz:

$$0 \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{F}_p[G] \twoheadrightarrow (\mathbb{F}_p[G])^G = \mathbb{F}_p[G]/\mathbb{F}_p =: E \hookrightarrow \mathbb{F}_p[G]^d =: D \longrightarrow \mathbb{F}_p[G]^r =: R$$

oder einfach:

$$0 \longrightarrow E \longrightarrow D \longrightarrow R.$$

Es sei weiterhin $P(t) := P_{\mathbb{F}_p[G]}(t)$ und $E_n = \mathbb{F}_p[G]_{n+1}/\mathbb{F}_p$: Man hat also eine Verschiebung der Koeffiziententen im Polynom P_E um 1 nach hinten:

$$1 + tP_E(t) = P_{\mathbb{F}_p[G]}(t) \Rightarrow P_E(t) = \frac{P(t)-1}{t}.$$

Weiter hat man noch $\delta(D_1) \subseteq R_0$ und induktiv folgt: $\delta(D_n) \subseteq R_{n-1}$, damit also die folgende exakte Sequenz:

$$0 \longrightarrow E_n \longrightarrow D_n \longrightarrow R_{n-1}.$$

Für die Längen gilt also:

$$l(E_n) + l(R_{n-1}) \geq l(D_n) \Rightarrow s(D_n) \leq s_n(E) + s_{n-1}(R).$$

Nun können wir mit der Potenzreihe $\frac{1}{1-t}$ multiplizieren $(0 < t < 1)$:

$$P_D(t)\frac{1}{1-t} \leq P_E(t)\frac{1}{1-t} + P_R(t)\frac{1}{1-t}.$$

Es ist

$$P_D(t) = P_{\mathbb{F}_p[G]^d}(t) = P_{\bigoplus_{i=1}^{d}\mathbb{F}_p[G]}(t) = dP(t), _E(t) = \frac{P(t)-1}{t}, P_R(t) = rtP(t).$$

Hier haben wir wieder Koefizentenshifting um 1 runter. Es folgt:

$$dP(t) \leq \frac{P(t)-1}{t} + rtP(t) \quad \Rightarrow \quad 1 \leq P(t)(1 - dt + rt^2) \qquad \text{für } 0 < t < 1.$$

Dieser Ausdruck ist ein Polynom in t, auf $(0,1)$ definiert. Damit ist es auf $(0,1]$ stetig erweiterbar und wir erhalten:

$$1 \leq P(t)(1 - dt + rt^2) \qquad \text{für } 0 < t \leq 1.$$

$P(t)$ hat nur Koefizienten $\geq 0 \Rightarrow P(t) > 0$, falls $t \geq 0$ (muss echt größer 0 sein, da sonst die obige Ungleichung falsch wäre). Damit kann man durch $P(t)$ teilen:

$$0 < \frac{1}{P(t)} < 1 - dtrt^2.$$

Setzen wir nun $t = 1$ ein, so erhälten wir: $1 - d + r > 0 \Rightarrow 0 < d < r + 1$, also ist

$$0 < \frac{d}{2r} < \frac{r+1}{2r} \leq 1,$$

nun können wir also $t = \frac{d}{2r}$ in die Ungleichung einsetzen und wir erhalten:

$$\begin{aligned} 0 < 1 - d\frac{d}{2r} + r\frac{d^2}{4r^2} = 1 - \frac{d^2}{2r} + \frac{d^2}{4r} = 1 - \frac{d^2}{4r} \\ \Longrightarrow \quad d^2 < 4r \\ \Longrightarrow \quad r > \frac{1}{4}d^2. \end{aligned}$$

□

Literaturverzeichnis

[Ada01] Michael Adam, *Einführung in die Gruppenkohomologie*, `www.uni-math.gwdg.de/mad/seminar-algebra/Gruppen-Kohomologie.dvi`, 2001.

[Bos03] Siegfried Bosch, *Algebra*, 5. ed., Springer, 2003.

[Bro82] Kenneth S. Brown, *Cohomology of Groups*, 2. ed., GTM **87**, Springer, New York, 1982.

[Gro57] Alexander Grothendieck, *Sur quelques points d'algébre homologique*, Tohoku Math. Journal **9** (1957), 119–221.

[HS96] Peter J. Hilton and Urs Stammbach, *A course in Homological Algebra*, GTM **4**, Springer, New York, 1996.

[Lan02] Serge Lang, *Algebra*, 3. ed., GTM **211**, Springer, New York, 2002.

[Mil97] James S. Milne, *Class Field Theory*, `www.jmilne.org/math/CourseNotes/math776.dvi`, 1997.

[Neu69] Jürgen Neukirch, *Klassenkörpertheorie*, BI-Hochschulskripten, 1969.

[Neu92] ———, *Algebraische Zahlentheorie*, Springer, New York, 1992.

[NSW99] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, Grundlehren **323**, Springer, New York, 1999.

[Ser79] Jean-Pierre Serre, *Local fields*, GTM **67**, Springer, New York, 1979.

[Ser94] ———, *Galois Cohomology*, 5. ed., LNM **5**, Springer, New York, 1994.

[Wei94] Charles A. Weibel, *An introduction to homological algebra*, Cambridge Univ. Press, Cambridge, 1994.

Stichwortverzeichnis

Im Stichwortverzeichnis sind die Seitenzahlen der Definitionen in **fett** gesetzt, die der Lemmata, Sätze und Theoreme in ***fett und kursiv*** und die der Beispiele mit einem Stern* markiert.

Anhang: Vortragsliste

Universität Bonn
Mathematisches Institut
Prof. Dr. O. Venjakob, Dr. J. Stix

universitätbonn

Vortragsliste für das Seminar

Kohomologie (pro-)endlicher Gruppen

— **Wintersemester 2005/2006, 14–16 Uhr, SR C** —

1. Matthias Klotz:

   Gruppenkohomologie in Graden 0, 1 und 2. G-Moduln, exakte Sequenz von abelschen Gruppen, G-Invarianten, Beispiele für nicht Linksexaktheit des Invariantennehmens [Ada01] 1.1+2; 1-Kozykel, 1-Ränder, $\mathrm{H}^1(G, A)$, die lange exakte Sequenz in Graden 0 & 1 [Ada01] 1.3; 2-Kozykel, 2-Ränder, $\mathrm{H}^2(G, A)$ [Ada01] 1.4; Extensionen einer Gruppe G mit einem G-Modul, semidirekte Produkte und Spaltungen, Äquivalenzklassen von Spaltungen und H^1 [Bro82] IV.1+2; Isomorphieklassen von Extensionen und H^2 [Wei94] Thm 6.6.3, [Bro82] IV.3.

2. Nicolas Poettering:

   Homologische Algebra I: Projektive und injektive Moduln. Moduln über einem Ring, Beispiele, Homomorphismen, exakte Sequenzen von R-Moduln [Lan02] III §1; der R-Modul $\mathrm{Hom}_R(M, N)$ [Lan02] III §2; direkte Summen, gespaltene exakte Sequenzen [Lan02] III §3 Prop 3.2; freie und projektive Moduln [Lan02] III §4; Beispiel: projektive Moduln über Hauptidealringen (etwa $\mathbb{Z}$) [Lan02] III Thm 7.1; Dualitätsprinzip (Pfeile umdrehen), injektive Moduln, Beispiel: injektive Moduln über Hauptidealringen (etwa $\mathbb{Z}$) [Lan02] XX §4 Lemma 4.2.

3. Tobias Lessmeister:

   Homologische Algebra II: Auflösungen. Komplexe, Abbildungen von Komplexen [Lan02] XX §1; Definition der Homologie eines Komplexes und der Homologieabbildung einer Abbildung von Komplexen, Verträglichkeit mit Komposition [Lan02] XX §2; Homotopien, homotope Abbildungen stimmen auf der Homologie überein [Lan02] XX §5 Lemma 5.1; es gibt genügend viele injektive/projektive Moduln, [Lan02] XX Thm 4.1; injektive/projektive Auflösungen, Isomorphie zwischen $\mathrm{Hom}_R(M, N)$ und Homotopieklassen von Homomorphismen zwischen Auflösungen von M und N [Lan02] XX §5 Lemma 5.2.

   Betone injektive Auflösungen (Vortrag 6, 7, 8, ...), obwohl Vortrag 4 projektive Auflsungen braucht.

4. Boryana Dimitrova:

Gruppenkohomologie I: Die Standardauflösung. Der Gruppenring $\mathbb{Z}[G]$, Augmentationsabbildung $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$, Augmentationsideal I_G [HS96] VI.1; G-Moduln und $\mathbb{Z}[G]$-Moduln [Ser79] VII §1; Definition von $\mathrm{H}^*(G, M)$ via projektiver Auflösung von $\mathbb{Z}$, genauer: wir fixieren eine projektive Auflösung $P^\bullet \to \mathbb{Z}$ des trivialen G-Moduls $\mathbb{Z}$ und definieren $\mathrm{H}^i_{P^\bullet}(G, M) = \mathrm{H}^i(\mathrm{Hom}_G(P^\bullet, M))$, nach Vortrag 3 kann man $\mathrm{id}_\mathbb{Z}$ für projektive Auflösungen $P^\bullet, Q^\bullet$ zu einer Abbildung $P^\bullet \to Q^\bullet$ liften, dieser Lift liefert nach Anwendung von $\mathrm{Hom}_G(-, M)$ und Homologie einen Homomorphismus

$$\Phi_{P^\bullet,Q^\bullet} : \mathrm{H}^i_{Q^\bullet}(G, M) \to \mathrm{H}^i_{P^\bullet}(G, M),$$

mit $\Phi_{P^\bullet,P^\bullet} = \mathrm{id}$ und $\Phi_{P^\bullet,R^\bullet} = \Phi_{P^\bullet,Q^\bullet} \circ \Phi_{Q^\bullet,R^\bullet}$ Daher ist $\Phi_{P^\bullet,Q^\bullet}$ ein kanonischer Isomorphismus zwischen der bzgl. $Q^\bullet$ und jener bzgl. $P^\bullet$ definierten Kohomologie, wir setzen daher gefahrlos $\mathrm{H}^i(G, M) = \mathrm{H}^i_{P^\bullet}(G, M)$ [Ser79] VII §2; die Standardauflösung und (in-)homogene Koketten, Vergleich mit H^i, $i = 0, 1, 2$ aus Vortrag 1, H^1 mit trivialen Koeffizienten [Ser79] VII §3, [Mil97] II S. 47–48; Beispiel: die Kohomologie zyklischer Gruppen $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}$ [Wei94] 6.2.1+2, 6.1.4.

5. Sebastian Hensel:

Kategorielle Sprache. Kategorie, Beispiele: R-Mod und $\mathrm{Ch}^\diamond(R\text{-Mod})$ für einen Ring R und $\diamond \in \{+, -, b\}$ [Mil97] II.4, [Gro57] I.1, [Wei94] Appendix A.1.2+3 + nach 1.1.5; Funktor, natürliche Transformation [Mil97] II.4, [Gro57] I.2, [Wei94] Appendix A.2.1+A.3; direkte Summe, Nullobjekt, additive Kategorie [Mil97] II.4, [Gro57] I.1+3; Kern, Cokern, abelsche Kategorie, Freyd'scher Einbettungssatz (ohne Beweis), additiver Funktor, (links- bzw. rechts-) exakter Funktor [Mil97] II.4, [Gro57] I.4; opponierte Kategorie, Dualitätsprinzip, kontravariante Funktoren [HS96] II.2+3, [Gro57], I.1 [Wei94] Appendix A.1.7+2.5.

Adjungierte Funktoren, adjungierte sind halbexakt, falls ein Rechtsadjungierter einen exakten linksadjungierten Funktor hat, so erhält er injektive, duale Aussage, Beispiel $M \mapsto M^G$.

6. Frank Weilandt:

Homologische Algebra III: δ-Funktoren. Schlangenlemma (inklusive Funktorialität in Abbildungen von kurzen exakten Sequenzen) [Wei94] Snake Lemma 1.3.2 + Addendum 1.3.3, 5er-Lemma [Wei94] Ex 1.3.3; Konstruktion einer kanonischen langen exakten Sequenz aus einer kurzen exakten Sequenz von Komplexen von Moduln [Wei94] Thm 1.3.1 + Prop 1.3.4; (exakte) kohomologische δ-Funktoren [Wei94] 2.1.1; Beispiel: Gruppenkohomologie, genauer: $\mathrm{H}^i(G, -)$ als Funktor (ein G-Homomorphismus $f : M \to N$ liefert eine Abbildung $f\circ : \mathrm{Hom}_G(P^\bullet, M) \to \mathrm{Hom}_G(P^\bullet, N)$, dessen Homologie die Abbildung $f_* = \mathrm{H}^*(G, f)$ liefert), zu einer kurzen exakten Sequenz $0 \to M' \to M \to M'' \to 0$ von G-Moduln gehört eine kurze exakte Sequenz von Komplexen abelscher Gruppen

$$0 \longrightarrow \mathrm{Hom}_G(P^\bullet, M') \longrightarrow \mathrm{Hom}_G(P^\bullet, M) \longrightarrow \mathrm{Hom}_G(P^\bullet, M'') \longrightarrow 0,$$

aus welcher der δ-Homomorphismus der Gruppenkohomologie gewonnen wird.

7. Michael Riess, Katja Hutschenreuter :

   Homologische Algebra IV: Derivierte Funktoren. 3×3–Lemma [Wei94] Ex. 1.3.2; „Hufeisenlemma" [Lan02] XX §6 Seite 794 (aus Beweis von Thm 6.1), [Wei94] 2.2.8 dualisiert für injektive; rechtsderivierte Funktoren für additive linksexakte Funktoren auf Kategorien von Moduln, Natürlichkeit des Verbindungshomomorphismus δ (impliziert die Unabhängigkeit von δ von der Wahl der Auflösungen) [Wei94] 2.5.1 (dual zu 2.4.1-6); Beispiele: (a) $\mathrm{Ext}^*_R(M,-)$, (b) $\mathrm{R}^i F(-)$ für exaktes F, (c) $\mathrm{R}^i(GF) \cong G(\mathrm{R}^i F)$ für G exakt und F linksexakt [Wei94] 2.5.2; universelle kohomologische δ-Funktoren [Gro57] II.1+2, [Wei94] Def 2.1.4, auslöschbar, Auslöschbarkeit von exakten kohomologischen δ-Funktoren impliziert universell [Gro57] II.2.1, [Wei94] 2.4.7 (dualisiert+modifiziert); rechtsderivierte Funktoren sind universell [Wei94] Cor 2.4.2 (dualisiert), Beispiel: der universelle kohomologische δ-Funktor des Funktors Kern auf der Kategorie der Pfeile hat nur einen ersten Derivierten: den Cokern, und die lange exakte Sequenz kommt aus dem Schlangenlemma.

8. Tobias Polley:

   Gruppenkohomologie II: Dimensionsshift. Definition von $\mathrm{H}^*(G,M)$ als derivierter Funktor des Invariantenfunktors und als $\mathrm{Ext}^*_{\mathbb{Z}[G]}(\mathbb{Z},-)$ [Ser79] VII §2; Vergleich mit der alten Definition aus Vortrag 4, genauer: Vortrag 7 und Universalität definiert einen Morphismus von δ-Funktoren $\varphi^* : \mathrm{R}^*(\ )^G(-) \to \mathrm{H}^*(G,-)$, wobei $\mathrm{H}^*(G,-)$ die Kohomologie nach alter Definition von Vortrag 4 ist, dieser ist ein Iso im Grad 0 und $\mathrm{H}^*(G,-)$ ist auslöschbar durch injektive/alternativ coinduzierte Moduln, daher ist φ^* ein Iso; (co-)induzierte Moduln, Shapiros Lemma [Wei94] 6.3.1-5, [Mil97] II.1; Dimensionsshift [Ser79] VII §2 Corollary, [Mil97] II.1.13, [Lan02] XX §7.

9. Jonathan Pfaff, Cornelius Probst:

   Gruppenkohomologie III: Funktorialität in der Gruppe. Restriktion, Inflation, und allgemeiner die Abbildung zu einem Paar von Gruppenhomomorphismus und passendem Modulhomomorphismus, explizite Beschreibung auf (in-)homogenen Koketten, innere Automorphismen operieren trivial [Ser79] VII §5, [Neu69] I §4.1+2; die inf/res-Sequenz im Grad 1 [Ser79] VII §6; inf ∘ inf = inf, res ∘ res = res, die Corestriktion, cor ∘ res ist Multiplikation mit dem Index, [Ser79] VII §7, cor ∘ cor = cor, Doppelnebenklassenformel res ∘ cor = ...; Anwendung: $\mathrm{H}^*(G,M)$ ist $\#G$-Torsion für eine endliche Gruppe G und $* > 0$ [Ser79] VIII §2, Satz von Schur-Zassenhaus [Wei94] Thm 6.6.9.

10. Matthias Erbar:

    Kohomologie proendlicher Gruppen. Diskrete G-Moduln [Ser94] I §2.1; Vergleich dreier Definitionen von stetiger Kohomologie proendlicher Gruppen mit diskreten Koeffizienten: stetige Koketten, ad hoc via $\varinjlim \mathrm{H}^q(G/N, M^N)$ über Inflation, als abgeleiteter Funktor auf der Kategorie der diskreten G-Moduln, es gibt genügend viele injektive diskrete G-Moduln [Ser94] I §2.5, [NSW99] I §3 1.3.6+7) [Ser94] I §2.2, [NSW99] I §2 1.2.6, [Mil97] II.3 Prop 3.2 + Aside 3.4; Verträglichkeit mit Limites in der Gruppe und den Koeffizienten [Ser94] I §2.2; Interpretation in Graden $0, 1$ und 2 [Ser94] I §2.3; Inflation, Restriktion, Corestriktion [NSW99] I §5; Beispiel: Kohomologie von $\hat{\mathbb{Z}}$ [Ser79] XIII §1.

11. Franz-Benjamin Mocnik:

Galoiskohomologie. Gruppenkohomologie der Galoisgruppe einer Körpererweiterung/der absoluten Galoisgruppe, alternative Beschreibung von diskreten Moduln A durch $L/K \mapsto A_L = A^{\mathrm{Gal}_L}$, additive Gruppe $\mathbb{G}_a : L/K \mapsto (L, +)$, multiplikative Gruppe $\mathbb{G}_m : L/K \mapsto (L^*, \cdot)$ [Ser94] II §1.1; Normalbasensatz, $\mathrm{H}^i(K, \mathbb{G}_a)$ [Ser79] X §1 Prop 1, [NSW99] VI §1 6.1.1; Hilbert 90, $\mathrm{H}^1(K, \mathbb{G}_m)$ [Ser79] X §1 Prop 2, [NSW99] VI §2 6.2.1; Pontrjagindualität Kummertheorie, Artin-Schreier-Theorie [Ser79] X §3, [NSW99] VI §1+2, [Neu92] IV §3 Thm 3.3, Kor 3.6.

12. Stephan Hähne, Maria Castillo Perez:

Kohomologische Dimension. Kohomologische Dimension [Ser94] I §3.1 Prop 11, [NSW99] III §3; strikte kohomologische Dimension [Ser94] I §3.2 Prop 13; kohomologische Dimension von Untergruppen [Ser94] I §3.3 Prop 14; pro-p Sylowtheorie [Ser94] I §1.4; $\mathrm{cd}_p(G) = 0$ [Ser94] I §3.3 Corollary 1–3; freie pro-p Gruppen [Ser94] I §1.5; $\mathrm{cd}_p(G) \leq 1$ [Ser94] I §3.4, [NSW99] III §5, Existenz von stetigen mengentheoretischen Schnitten [Ser94] I §1.2 Prop 1.

13. Alexander Ivanov:

Kohomologie von pro-p Gruppen. Einfache Moduln [Ser94] I §4.1 Prop 20+21; H^1 und Erzeuger, Definition von Rang [Ser94] I §4.2 Prop 23+24+Cor2+Cor3a + Cor; H^2 und Relationen [Ser94] I §4.3 Prop 26+27+Cor; Golod-Shafarevich-Ungleichung [Ser94] I §4.4 + I Appendix 2, [NSW99] III §9.

Vortrag	Literatur
1	[Ada01], [Bro82], [Wei94]
2	[Lan02]
3	[Lan02]
4	[Ser79], [Mil97], [HS96], [Wei94]
5	[Mil97], [Gro57], [Wei94], [HS96]
6	[Wei94]
7	[Wei94], [Gro57]
8	[Ser79], [Mil97], [Wei94], [Lan02]
9	[Ser79], [Wei94], [Neu69]
10	[Ser94], [NSW99], [Mil97], [Ser79]
11	[Ser94], [Ser79], [NSW99], [Neu92]
12	[Ser94], [NSW99]
13	[Ser94], [NSW99]