Westfälische Wilhelms-Universität Münster
Fachbereich Mathematik und Informatik

Analogien zwischen Knotentheorie und Iwasawatheorie

Diplomarbeit
von
Julia Singer

September 2003

Aufgabenstellung und Betreuung:

Prof. Dr. Christopher Deninger,
Institut für Mathematik,
WWU Münster

Erklärung: „Hiermit versichere ich, dass ich diese Diplomarbeit selbstständig verfasst und nur die angegebenen Quellen und Hilfsmittel verwendet habe.“

Münster, den 6. Oktober 2003

Inhaltsverzeichnis

Einleitung

Der Ausgangspunkt für diese Arbeit ist ein nicht allzu ungewöhnliches Phänomen: das Auftreten von ähnlichen algebraischen Formalismen in völlig verschiedenen Bereichen der Mathematik, in diesem Fall einerseits in der Knotentheorie und andererseits in der Theorie der $\mathbb{Z}_p$-Erweiterungen von Zahlkörpern. Spannend wird die Analogie hier allerdings dadurch, dass sie sich eingliedert in eine Reihe weiterer Entsprechungen, die Objekte aus diesen beiden unterschiedlichen Gebieten miteinander in Verbindung bringen.

Ähnlichkeiten zwischen Objekten aus der Knotentheorie und Objekten aus der Iwasawatheorie sind schon in den 60er Jahren bemerkt worden. Bei der Berechnung bestimmter étaler Kohomologiegruppen von Zahlkörpern stellte B. Mazur ([27]) zum Beispiel fest, dass $\operatorname{Spec} \mathcal{O}_K$ als dreidimensionales Objekt angesehen werden sollte. Obwohl ein großer Teil der Analogie schon damals entwickelt wurde, findet man erst seit einigen Jahren Veröffentlichungen, die sich explizit mit diesem Thema befassen. Das seit etwa Mitte der 90er Jahre entstandene Gebiet wurde von A. Reznikov auf den Namen „Arithmetische Topologie" getauft; sein Kernstück besteht aus einem „Wörterbuch" ([38], [42]), das in verschiedenen Versionen Verbreitung findet und laufend weiter ergänzt wird. Hinter dem Ganzen steckt die Hoffnung, dass es sich nicht nur um zufällige Gemeinsamkeiten zwischen den beiden Bereichen handelt, sondern dass ein tiefer Zusammenhang der Grund für die Ähnlichkeiten ist.

Zunächst möchten wir hier ein paar Punkte zur Motivation beschreiben. Eine Untersuchung der étalen Kohomologiegruppen von $\operatorname{Spec} \mathbb{Z}$ und $\operatorname{Spec} \mathbb{F}_p$ legt nahe, die Einbettung $\operatorname{Spec} \mathbb{F}_p \to \operatorname{Spec} \mathbb{Z}$ mit der Einbettung eines Kreises S^1 in die 3-Sphäre S^3 zu vergleichen – also mit genau der Situation, die in der Knotentheorie vorliegt. Das Schema $\operatorname{Spec} \mathbb{Z}[\frac{1}{p}]$, das man durch Entfernen von (p) erhält, entspricht dann einem Knotenkomplement. Ähnliche Gründe sprechen dafür, dass jeder Zahlkörper K als ein dreidimensionales Objekt angesehen werden kann, das allgemeiner mit einer 3-Mannigfaltigkeit verglichen wird. Die Einbettung $\operatorname{Spec} \mathcal{O}_K/\mathfrak{p} \to \operatorname{Spec} \mathcal{O}_K$ eines abgeschlossenen Punktes entspricht in diesem Fall einem Knoten in einer 3-Mannigfaltigkeit.

Nachdem also einige Gemeinsamkeiten zwischen den Objekten der Knotentheorie und der Iwasawatheorie festgestellt werden können, fällt auf, dass sich die Konstruktion einer wichtigen Knoteninvariante, nämlich des Alexanderpolynoms, in der Iwasawatheorie ähnlich durchführen lässt und das Ergebnis im Wesentlichen ein Objekt ist, das dort unter dem Namen „Iwasawa-Zetafunktion" oder allgemeiner einfach als „charakteristisches Polynom" bekannt ist. Dieser Zusammenhang wurde ebenfalls schon in den 60er Jahren bemerkt, allerdings zunächst in keiner Veröffentlichung erwähnt.

Das Ziel dieser Arbeit soll sein, die Beziehung zwischen dem Alexanderpolynom und dem entsprechenden Polynom aus der Iwasawatheorie detailliert zu beschreiben und die Grundlagen und die Motivation dafür im Zusammenhang darzustellen. Außerdem werden Methoden zur Berechnung des Alexanderpolynoms und des charakteristischen Polynoms in einer einheitlichen Form beschrieben. Zum Schluss überlegen wir, welches Objekt man in der Iwasawatheorie erhält, wenn man anstelle eines Knotens das Alexanderpolynom einer Verschlingung betrachtet.

Zu den Kapiteln im Einzelnen: In Kapitel 1 wird das Alexanderpolynom eines Knotens vorgestellt, das von James W. Alexander ([1]) bereits im Jahr 1928 eingeführt wurde und das bis zur Entdeckung des Jones-Polynoms im Jahr 1984 als wahrscheinlich wichtigstes Werkzeug zur Unterscheidung von Knoten diente.

Das Alexanderpolynom kann mit Hilfe der universellen abelschen Überlagerung X_∞ des Knotenkomplements X definiert werden, indem man die erste Homologiegruppe von X_∞ als Modul über $\mathbb{Z}[H_1(X)]$ betrachtet. Das Alexanderpolynom ergibt sich dann als Erzeuger des 0. Fitting-Ideals dieses Moduls. Alternativ ist es möglich, eine Beschreibung mit Hilfe von Verschlingungszahlen und Seifert-Flächen zu geben, die eine Präsentationsmatrix für den Modul $H_1(X_\infty)$ liefert. Als Beispiel für die Berechnung des Alexanderpolynoms untersuchen wir das Alexanderpolynom eines Torusknotens.

Das zweite Kapitel beschreibt die Situation in der Iwasawatheorie. Zunächst werden als Grundlagen einige Ergebnisse aus der Klassenkörpertheorie und ein paar Tatsachen über proendliche Gruppen und $\mathbb{Z}_p$-Erweiterungen von Zahlkörpern bereitgestellt. Eine „typische“ $\mathbb{Z}_p$-Erweiterung bekommt man, wenn man die Erweiterung $\mathbb{Q}(\mu_{p^\infty})$, also den Körper, der alle Einheitswurzeln ζ_{p^n} mit p-Potenz-Ordnung enthält, über $\mathbb{Q}(\zeta_p)$ betrachtet. Als einzige Zwischenkörper erhält man die Kreisteilungskörper $\mathbb{Q}(\zeta_{p^n})$.

Die Methode, mit der in der Iwasawatheorie die Klassengruppen der Zwischenkörper in solchen Erweiterungen untersucht werden, beruht darauf, dass man bestimmte Galoisgruppen als Moduln über einer vollständigen Gruppenalgebra betrachtet. Diese so genannte „Iwasawa-Algebra“ ist isomorph zum Potenzreihenring $\mathbb{Z}_p[\![T]\!]$, und die Strukturtheorie für endlich erzeugte $\mathbb{Z}_p[\![T]\!]$-Moduln, die in den folgenden Abschnitten hergeleitet wird, kann dazu verwendet werden, um Aussagen über die verschiedenen auftretenden Galoisgruppen zu beweisen. Als Beispiel ergibt sich mit dieser Methode relativ schnell der berühmte Satz von Iwasawa ([16]) über das Verhalten des p-Anteils der Idealklassengruppen für die Zwischenkörper in einer $\mathbb{Z}_p$-Erweiterung.

Um das Objekt zu definieren, das als Analogon zum Alexanderpolynom angesehen wird, geht man zunächst von einem total reellen Zahlkörper K aus, betrachtet darüber die eindeutige $\mathbb{Z}_p$-Erweiterung, die sich als Teilerweiterung von $K(\mu_{p^\infty})$ ergibt, und darüber wiederum die maximale abelsche außerhalb von allen Stellen über p unverzweigte p-Erweiterung. Diese letzte Gruppe wird ein Modul über der Iwasawa-Algebra, und das Objekt, das wir „Iwasawa-Zetafunktion“ nennen, ergibt sich genau wie das Alexanderpolynom aus dem nullten Fitting-Ideal dieses Moduls. Um eine Erklärung für den Namen „Zetafunktion“ zu geben, folgt noch ein kurzer Abschnitt über die so genannte Hauptvermutung der Iwasawatheorie – ein Satz, der im Jahr 1990 endgültig bewiesen wurde und der den Zusammenhang herstellt zwischen der Iwasawa-Zetafunktion und den p-adischen Zetafunktionen, die sich durch Interpolation der Dedekind-Zetafunktionen für Zahlkörper ergeben.

Sowohl das Alexanderpolynom eines Knotens als auch die Iwasawa-Zetafunktion des Körpers $\mathbb{Q}$ lassen sich jeweils allein mit Hilfe einer Gruppe G definieren. Im ersten Fall ist diese Gruppe die Fundamentalgruppe des Knotenkomplements und der Alexandermodul ist der Modul $(G')^{ab}$ über dem Ring $\mathbb{Z}[G^{ab}]$. Im zweiten Fall ist G die Galoisgruppe der maximalen außerhalb von p unverzweigten p-Erweiterung von $\mathbb{Q}$, und man betrachtet die Gruppe $(G')^{ab}$ als $\mathbb{Z}_p[\![G^{ab}]\!]$-Modul.

Das dritte Kapitel liefert den wichtigsten Teil der Motivation für die Analogie zwischen Alexanderpolynom und Iwasawa-Zetafunktion. Dafür wird zunächst Grothendiecks Konstruktion einer Fundamentalgruppe für Schemata allgemein beschrieben und dann speziell auf den

Fall eines normalen Schemas und den für uns interessanten Fall $\operatorname{Spec}\mathbb{Z}[\frac{1}{p}]$ angewendet. Als Fundamentalgruppe ergibt sich für $\operatorname{Spec}\mathbb{Z}\backslash\{(p)\}$, also für dasjenige Schema, das wir als Analogon des Knotenkomplements auffassen, die Galoisgruppe der maximalen außerhalb von p unverzweigten Erweiterung von $\mathbb{Q}$.

Nachdem in den ersten zwei Kapiteln als Vorbereitung die Bereiche Topologie und Iwasawatheorie getrennt behandelt wurden, stellt das vierte Kapitel nun die Verbindung her: Es besteht aus einer Gegenüberstellung der Objekte in der Topologie und in der Zahlentheorie und fasst damit die Ergebnisse aus den ersten beiden Teilen zusammen.

Als Nächstes folgt ein Teil über das Berechnen des Alexanderpolynoms und des entsprechenden Objekts in der Iwasawatheorie. R. Fox entwickelte in den 50er Jahren den später nach ihm benannten Fox-Kalkül ([10], [11]), der es ermöglicht, das Alexanderpolynom mit Hilfe einer vorgegebenen Präsentation der Knotengruppe zu berechnen. Um diese Methode auf die Zahlentheorie übertragen zu können, formulieren wir die Ergebnisse noch einmal mit Hilfe von Gruppenhomologie.

Als Vorbereitung für die Situation im pro-endlichen Fall benötigt man zunächst einige Grundlagen über vollständige Tensorprodukte und Differentialmoduln über vollständigen Gruppenringen. Damit lässt sich der Formalismus – wie auch schon in [34] in einer etwas anderen Formulierung beschrieben – problemlos übertragen.

H. Koch führt in seinem Buch [21] mehrere Beispiele für Galoisgruppen an, deren Präsentationen als Pro-p-Gruppen bekannt sind. Die Situation entspricht aus verschiedenen Gründen allerdings nicht mehr einem Knoten in S^3, sondern einem allgemeineren Fall, der als Entsprechung einer Verschlingung mit mehreren Komponenten betrachtet werden kann.

Wir diskutieren also als Letztes die Möglichkeiten für eine Verallgemeinerung der Analogie auf Alexanderpolynome für Verschlingungen mit mehreren Komponenten. Die offensichtlichste Verallgemeinerung besteht darin, statt eines Punktes mehrere abgeschlossene Punkte aus $\operatorname{Spec}\mathbb{Z}$ zu entfernen. Bessere Analogien erhält man aber, wenn man stattdessen zu größeren Zahlkörpern übergeht und mehrfache $\mathbb{Z}_p$-Erweiterungen untersucht. Die Situation entspricht dann zunächst nicht mehr der einer Verschlingung in S^3, sondern allgemeiner einer Verschlingung in einer 3-Mannigfaltigkeit. Im Spezialfall eines imaginär-quadratischen Zahlkörpers der Klassenzahl 1 erhält man allerdings aus verschiedenen Gründen ein Objekt, das als genaues Analogon einer Verschlingung mit zwei Komponenten in der 3-Sphäre angesehen werden kann.

Zum Abschluss des Kapitels wird das „Wörterbuch“ aus dem vierten Kapitel um die Ergebnisse aus diesem Teil ergänzt, die noch einmal in Form einer Gegenüberstellung aufgelistet werden.

1 Knoten

Ein Knoten ist eine geschlossene Kurve, die in die 3-Sphäre S^3 eingebettet ist. Eine Verschlingung mit n Komponenten besteht aus n disjunkten Einbettungen solcher Kurven.

Da die Einbettungen nicht surjektiv sind, können wir uns vorstellen, dass unsere Knoten statt in S^3 in den dreidimensionalen Raum $\mathbb{R}^3$ eingebettet werden. Meistens werden die Knoten und Verschlingungen zusätzlich mit einer Orientierung versehen, auf jeder Komponente wird also eine Richtung vorgegeben.

Um mit den Knoten und Verschlingungen leichter umgehen zu können, werden wir immer annehmen, dass sie sich aus endlich vielen geraden Liniensegmenten zusammensetzen, wir betrachten also keine „wilden“ Knoten. Man stellt sich die Objekte natürlich trotzdem etwa so vor, wie Abbildung 2 andeutet – etwa mit der Begründung, dass die Liniensegmente so winzig sind, dass man sie mit bloßem Auge nicht mehr erkennen kann.

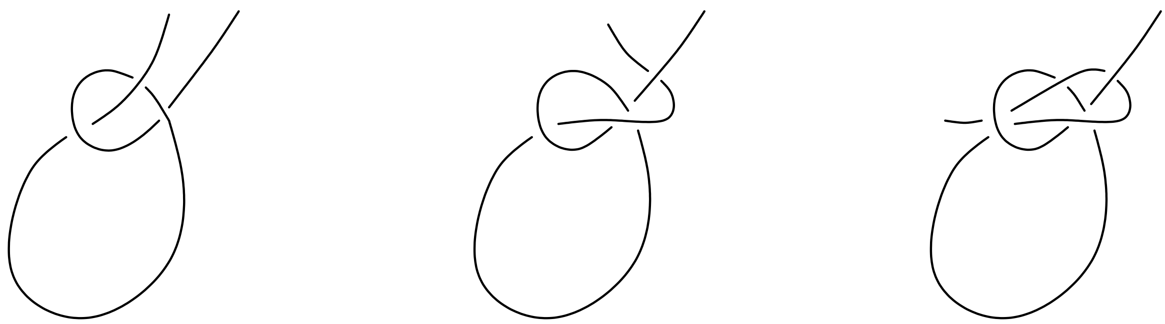


Abbildung 1: Palstek

Mit der oben angegebenen Definition wird zum Beispiel ein Palstek[1] zu einem Knoten, indem man die Enden des Seils zusammenklebt und das Seil als stückweise lineare eindimensionale Kurve betrachtet. Er lässt sich in einer Knotentabelle unter der Bezeichnung 6_2 wiederfinden.

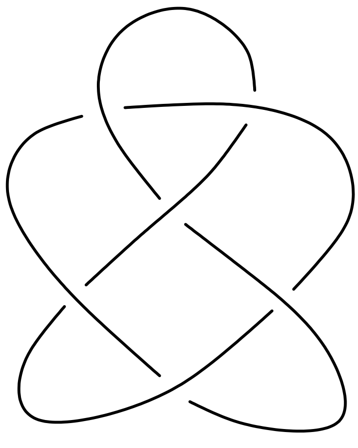


Abbildung 2: Projektion des Knotens 6_2

[1] „Krokodil kommt aus dem Teich, kriecht einmal um den Baum und taucht wieder in den Teich ein“

Die passende Äquivalenzrelation für unsere stückweise linearen Knoten und Verschlingungen ist die folgende:

Definition. Zwei Verschlingungen L_1 und L_2 sind isotop, wenn es einen orientierungserhaltenden stückweise linearen Homöomorphismus $\varphi : S^3 \to S^3$ gibt, der L_1 auf L_2 abbildet.

Bemerkung. Eine Möglichkeit, die Bedingung „stückweise linear" für die 3-Sphäre zu interpretieren, erhält man, wenn man S^3 als Rand des (n+1)-dimensionalen Standardsimplex Δ^{n+1} auffasst. „Stückweise linear" bedeutet dann, dass es zwei Unterteilungen von $\partial\Delta^{n+1}$ in kleinere Simplices gibt, auf denen die Abbildung φ linear ist.

Zu jedem Knoten können wir ein zweidimensionales Bild zeichnen, das es uns erlaubt, den Knoten (natürlich bis auf Isotopie) daraus wiederzugewinnen, wenn wir uns an jeder Kreuzung die zusätzliche Information merken, welche Linie die überkreuzende und welche die unterkreuzende sein soll. Eine solche Projektion, die außerdem die Eigenschaft hat, dass sich niemals drei Linien in einem Punkt schneiden und dass es nur endlich viele Kreuzungen gibt, nennt man Knotendiagramm. Zu einem stückweise linearen Knoten lässt sich ein solches Bild leicht finden. Ein Beispiel ist in Abbildung 2 angegeben.

1.1 Alexandermoduln

Die wichtigste Aufgabe, die sich die Knotentheorie stellt, ist die Klassifikation von Knoten bis auf Isotopie. Beim Unterscheiden von Knoten helfen so genannte Knoteninvarianten, also Objekte wie Zahlen oder Gruppen, die man Isotopieklassen von Knoten oder Verschlingungen zuordnen kann. Die Definitionen der Invarianten, die in den nächsten Abschnitten vorgestellt werden, kann man in fast allen einführenden Büchern über Knotentheorie nachlesen, zum Beispiel in [6] oder [24].

Offensichtlich ungeeignet ist als Knoteninvariante die erste Homologiegruppe des Knotenkomplements, wie der nächste Satz zeigt. Wenn nichts anderes angegeben wird, sind im Folgenden alle Homologiegruppen singuläre Homologiegruppen mit Koeffizienten in $\mathbb{Z}$.

Satz 1.1. *Für einen beliebigen Knoten K gilt $H_1(S^3\backslash K) \cong \mathbb{Z}$.*

Beweis. Sei V eine Torus-Umgebung des Knotens K in S^3. Dann gilt

$$\begin{aligned}
H_1(S^3\backslash K) &\cong H_1(S^3\backslash V^\circ) \\
&\cong H_2(S^3, S^3\backslash V^\circ) && \text{(lange exakte Sequenz für } (S^3, S^3\backslash V)) \\
&\cong H_2(V, \partial V) && \text{(Ausschneidung)} \\
&\cong H^1(V) && \text{(Poincaré-Dualität)} \\
&\cong H^1(K) \cong H^1(S^1) \cong \mathbb{Z}.
\end{aligned}$$

□

Sei K ein Knoten und $C = S^3\backslash K$ das Knotenkomplement. Die Fundamentalgruppe G von C nennt man Knotengruppe. Isotope Knoten haben homöomorphe Knotenkomplemente und damit auch isomorphe Knotengruppen. Wir stellen also sofort fest, dass wir schon zwei Knoteninvarianten gefunden haben, die sich im Gegensatz zur ersten Homologiegruppe als brauchbare Hilfsmittel erweisen. Mit ihrer Hilfe lassen sich weitere Knoteninvarianten konstruieren.

Definition. Die universelle abelsche Überlagerung eines wegzusammenhängenden, lokal wegzusammenhängenden, semilokal einfach zusammenhängenden topologischen Raums ist die maximale Überlagerung mit abelscher Decktransformationsgruppe.

Die universelle abelsche Überlagerung von C ist also die eindeutig bestimmte Überlagerung mit Fundamentalgruppe $G' = [G, G]$ und Decktransformationsgruppe $D = G/G'$.

Nach Satz 1.1 gilt $D = H_1(C) \cong \mathbb{Z}$, und wir erhalten folgendermaßen eine Operation dieser Gruppe auf $G'/[G', G']$: Als Gruppe der Deckbewegungen operiert D transitiv auf der universellen abelschen Überlagerung C_∞ von C mit Fundamentalgruppe $\pi_1(C_\infty) = G'$. Diese Operation induziert eine Operation von D auf $H_*(C_\infty)$, die die Homologiegruppen der Überlagerung C_∞ zu $\mathbb{Z}[D]$-Moduln macht. Insbesondere operiert D auf der ersten Homologiegruppe, die zu $G'/[G', G']$ kanonisch isomorph ist.

Lemma 1.2. *Die Operation der Gruppe der Deckbewegungen auf $H_1(C_\infty)$ stimmt mit der Operation von $G/[G, G]$ auf $G'/[G', G']$ durch innere Automorphismen überein.*

Beweis. Sei $g \in G$ ein Repräsentant eines Elements von $H_1(C)$ und $a \in G' = \pi_1(C_\infty)$. Das Element g entspricht einem Automorphismus von C_∞, der folgendermaßen einen Automorphismus der Fundamentalgruppe induziert: Der geschlossene Weg a wird abgebildet auf den geschlossenen Weg, den man erhält, wenn man zunächst die Hochhebung des Weges g, dann den Weg a, beginnend am Endpunkt dieses Weges, und schließlich die Hochhebung des Inversen von g durchläuft. Das entspricht genau der Konjugation mit g. $\square$

Definition. Den $\mathbb{Z}[D]$-Modul $H_1(C_\infty)$ mit der oben angegebenen D-Operation nennt man Alexandermodul von K.

Bemerkung. Der Ring $\mathbb{Z}[D] \cong \mathbb{Z}[\mathbb{Z}]$ ist offenbar isomorph zum Laurent-Polynomring $\mathbb{Z}[t, t^{-1}]$, wobei der Isomorphismus auf zwei verschiedene Arten gewählt werden kann, da ein Erzeuger der zyklischen Gruppe $\mathbb{Z}$ entweder auf t oder auf t^{-1} abgebildet werden kann.

1.2 Fitting-Ideale

Fitting-Ideale sind Invarianten von endlich erzeugten Moduln, mit deren Hilfe wir die Alexanderpolynome definieren werden. In der Literatur werden sie auch als Elementarideale oder Determinantenideale bezeichnet. Einen Abschnitt über Fitting-Ideale gibt es zum Beispiel in [23], XIX §2.

Sei R ein kommutativer Ring und M ein endlich erzeugter R-Modul.

Definition. Eine endliche Präsentation des R-Moduls M ist eine exakte Sequenz

$$R^m \to R^n \to M \to 0$$

mit $m, n \in \mathbb{N}_0$. Die Matrix, die die Abbildung $R^m \to R^n$ beschreibt, nennt man Präsentationsmatrix des Moduls M.

Wir betrachten im Folgenden nur Moduln über noetherschen Ringen, sodass jeder endlich erzeugte Modul eine endliche Präsentation besitzt. Im allgemeinen Fall kann man auch $m = \infty$ zulassen.

Definition. Das i-te Fitting-Ideal $F_i(M)$ ist das Ideal, das von den $(n-i)$-Minoren einer $(n \times m)$-Präsentationsmatrix von M erzeugt wird. Man setzt $F_i(M) = R$, falls $n - i \leq 0$ und $F_i(M) = 0$, falls $n - i \geq m$.

Falls A eine Präsentationsmatrix für M ist, bezeichnen wir $F_i(M)$ auch als i-tes Fitting-Ideal der Matrix A.

Der folgende Satz zeigt, dass die Fitting-Ideale tatsächlich Invarianten des Moduls sind und die Definition damit sinnvoll ist:

Satz 1.3. *Die Fitting-Ideale eines Moduls hängen nicht von der Wahl der Präsentation ab.*

Beweis. Seien A und B zwei Präsentationsmatrizen von M mit zugehörigen Erzeugendensystemen $\{a_1, \dots, a_n\}$ und $\{b_1, \dots, b_{n'}\}$ von M. Durch Hinzufügen von b_1 zum ersten Erzeugendensystem erhält man ein neues Erzeugendensystem und durch Hinzufügen einer Relation $b_1 = \sum_i r_i a_i$ mit $r_i \in R$ eine neue Präsentationsmatrix

$$\begin{pmatrix} * & 1 \\ A & 0 \end{pmatrix}$$

von M. Die $(n+1-i)$-Minoren dieser Matrix erzeugen offenbar dasselbe Ideal wie die $(n-i)$-Minoren von A.

Indem wir schrittweise alle Erzeuger b_i hinzufügen und dann mit demselben Argument alle Erzeuger a_i entfernen, können wir also annehmen, dass die zu den Präsentationsmatrizen A und B gehörigen Erzeugendensysteme von M gleich sind.

Da die Zeilen aus Relationen zwischen den Erzeugern bestehen und jede Matrix eine vollständige Menge von Relationen enthält, ist jetzt jede Zeile von B Linearkombination der Zeilen von A. Das Ideal, das von den $n-i$-Minoren von A erzeugt wird, ändert sich durch Hinzufügen der Zeilen aus B also nicht. Umgekehrt gilt dasselbe Argument für B. Die $(n-i)$-Minoren der Matrizen A, $\binom{A}{B}$ und B erzeugen also jeweils dasselbe Ideal. □

Die folgenden zwei Sätze werden in den nächsten Kapiteln nützlich sein:

Satz 1.4. *Sei K ein Körper, R der Polynomring $K[T]$ oder eine Lokalisierung von $K[T]$ und X ein endlich erzeugter Modul vom Rang 0 über R. Die Multiplikation mit T auf dem K-Vektorraum X bezeichnen wir mit φ, ihr charakteristisches Polynom mit p_φ. Dann erzeugt das Element $p_\varphi(T)$ das nullte Fitting-Ideal von X.*

Beweis. Zunächst sei $X = R/(g(T))$ mit einem beliebigen normierten Polynom $g(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ aus $K[T]$. Die Abbildung φ ist als K-lineare Abbildung bezüglich der Basis $\{1, \dots, T^{n-1}\}$ durch die folgende Matrix gegeben:

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Berechnet man das charakteristische Polynom dieser Abbildung und setzt das Element T ein, so erhält man genau das Polynom $g(T)$.

Für einen beliebigen endlich erzeugten R-Modul X gibt es nach dem Struktursatz für Moduln über Hauptidealringen Polynome $g_i(T) \in K[T]$, sodass $X \cong \bigoplus_{i=1}^{k} R/(g_i(T))$. Nach Voraussetzung ist keins der Polynome das Nullpolynom. Wir erhalten eine Präsentation

$$R^k \to R^k \to X \to 0,$$

wobei die erste Abbildung durch die Diagonalmatrix beschrieben wird, deren Einträge die Elemente $g_i(T)$ sind. Auch im Fall, dass R eine Lokalisierung des Polynomrings ist, können wir die $g_i(T)$ als Polynome wählen.

Das charakteristische Polynom von φ ist das Produkt der charakteristischen Polynome für die einzelnen Summanden, also gilt $p_\varphi(\lambda) = \prod g_i(\lambda)$, und durch Einsetzen von T ergibt sich die Determinante der Präsentationsmatrix und damit ein Erzeuger des gesuchten Fitting-Ideals. □

Definition. Für einen Modul M über einem noetherschen faktoriellen Ring bezeichnen wir den größten gemeinsamen Teiler der Elemente aus $F_d(M)$ mit $\Delta_d(M)$.

Bemerkung. Falls $F_d(M)$ ein Hauptideal ist, erzeugt $\Delta_d(M)$ dieses Ideal. Da $\Delta_d(M)$ nur bis auf Multiplikation mit Einheiten aus R eindeutig bestimmt ist, können wir es auch als Element von R/R^* auffassen.

Der folgende Satz impliziert insbesondere, dass $F_0(M) = (0)$, falls M positiven Rang hat:

Satz 1.5. *Sei R ein noetherscher faktorieller Ring und*

$$0 \to M' \to M \to M'' \to 0$$

eine exakte Sequenz endlich erzeugter R-Moduln, sodass M'' torsionsfreier Modul vom Rang r ist. Dann gilt $\Delta_d(M) = 0$, falls $d \leq r - 1$, und $\Delta_d(M) = \Delta_{d-r}(M')$, falls $d \geq r$.

Beweis. Sei π ein Primelement in R und π^k die höchste π-Potenz, die $\Delta_d(M)$ teilt. Analog sei $\pi^{k'}$ die höchste π-Potenz, die $\Delta_{d-r}(M')$ teilt. Es gilt also $\Delta_d(M) = \pi^k \cdot \alpha$ und $\Delta_{d-r}(M') = \pi^{k'} \cdot \alpha'$ mit zu π teilerfremden Elementen $\alpha, \alpha' \in R$.

Lokalisieren bei dem Primideal (π) liefert eine exakte Sequenz

$$0 \to M' \otimes_R R_{(\pi)} \to M \otimes_R R_{(\pi)} \to M'' \otimes_R R_{(\pi)} \to 0,$$

und wenn A eine Präsentationsmatrix des Moduls M über R ist, können wir A auch als Präsentationsmatrix von $M_{(\pi)} = M \otimes R_{(\pi)}$ über $R_{(\pi)}$ auffassen. Das einzige Primideal der Höhe 1 in diesem Ring ist π, also gilt über der Lokalisierung $\Delta_d(M) = \pi^k$ und $\Delta_{d-r}(M') = \pi^{k'}$ bis auf Einheiten.

Der Ring $R_{(\pi)}$ ist aber ein Hauptidealring, und nach dem Struktursatz für endlich erzeugte Moduln über Hauptidealringen haben $M_{(\pi)}$ und $M'_{(\pi)}$ quadratische Präsentationsmatrizen. Da $M''_{(\pi)}$ als torsionsfreier Modul über $R_{(\pi)}$ frei ist, haben wir Präsentationen

$$R_{(\pi)}^r \xrightarrow{0} R_{(\pi)}^r \to M''_{(\pi)} \to 0$$
$$R_{(\pi)}^k \xrightarrow{A} R_{(\pi)}^k \to M'_{(\pi)} \to 0,$$

und für $M_{(\pi)} = M'_{(\pi)} \oplus M''_{(\pi)}$ ergibt sich die Präsentationsmatrix $\left(\begin{smallmatrix} A & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Offenbar gilt also über $R_{(\pi)}$ die Gleichung $\Delta_d(M) = \Delta_{d-r}(M')$, mit anderen Worten, die höchste π-Potenz ist über R dieselbe. Da diese Gleichung für jedes beliebige Primelement aus R gilt, ist $\Delta_d(M) = \Delta_{d-r}(M')$ bis auf Multiplikation mit einer Einheit. □

1.3 Definition der Alexanderpolynome

Bisher haben wir uns an Knoteninvarianten das Knotenkomplement, die Knotengruppe und den Alexandermodul notiert. Knotenkomplement und Knotengruppe sind mächtige Invarianten: Seit 1989 ist bekannt, dass das Knotenkomplement für unsere stückweise linearen Knoten eine vollständige Invariante darstellt. Zwei Knoten sind mit anderen Worten genau dann isotop, wenn ihre Knotenkomplemente homöomorph sind. Für so genannte Primknoten, also Knoten, die sich nicht durch Aneinandersetzen von zwei anderen nichttrivialen Knoten ergeben, ist auch die Knotengruppe eine vollständige Invariante ([12]).

Hat man ein Knotendiagramm gegeben, ist es nicht schwierig, für die Knotengruppe eine Präsentation anzugeben. In Kapitel 11 von [24] wird eine Methode beschrieben, wie man durch einen einfachen Algorithmus aus einem Knotendiagramm mit n Segmenten eine Präsentation der Knotengruppe mit n Erzeugern und $n-1$ Relationen generieren kann. Das Resultat ist unter dem Namen Wirtinger-Präsentation bekannt.

Allerdings gelingt es im Allgemeinen nicht so leicht, nur an Hand von Präsentationen der Knotengruppe festzustellen, ob zwei Gruppen isomorph sind. Man sucht aus diesem Grund also weitere Invarianten, die vielleicht nicht alle Knoten unterscheiden können, aber den Vorteil haben, dass man besser mit ihnen umgehen kann.

Definition. Das i-te Alexander-Ideal des Knotens K ist das $(i-1)$-te Fitting-Ideal des $\mathbb{Z}[t, t^{-1}]$-Moduls $H_1(C_\infty)$. Das i-te Alexanderpolynom ist ein Erzeuger des kleinsten Hauptideals von $\mathbb{Z}[t, t^{-1}]$, das das i-te Alexander-Ideal enthält. Das erste Alexanderpolynom bezeichnet man auch als *das* Alexanderpolynom.

Das Alexanderpolynom ist also der größte gemeinsame Teiler $\Delta_0(H_1(C_\infty))$ der Elemente aus dem nullten Fitting-Ideal von $H_1(C_\infty)$. In der Literatur wird für das i-te Alexanderpolynom auch Δ_i geschrieben. Um Missverständnisse zu vermeiden, verwenden wir für das erste Alexanderpolynom keinen Index und bezeichnen es einfach mit $\Delta(t)$.

Eindeutigkeit erhält man für die Polynome wieder bis auf Multiplikation mit Einheiten aus $\mathbb{Z}[t, t^{-1}]$, also bis auf Multiplikation mit $\pm t^n$. Im Abschnitt 1.5 über Seifert-Flächen zeigen wir, dass sich das Alexanderpolynom durch Vertauschen von t und t^{-1} nicht ändert und dass der Modul $H_1(C_\infty)$ eine quadratische Präsentationsmatrix besitzt, sodass das erste Alexander-Ideal jedes Knotens ein Hauptideal ist. Außerdem wird mit Hilfe von Seifert-Flächen gezeigt, dass der Alexandermodul den Rang 0 hat und das Alexanderpolynom für keinen Knoten verschwindet.

1.4 Verschlingungszahlen

Die Verschlingungszahl einer Verschlingung mit zwei Komponenten kann man sich so vorstellen, dass sie angibt, wie oft der eine Knoten um den anderen „herumgewickelt“ wurde. Durch die Beschreibung von Verschlingungszahlen mit Hilfe von Seifert-Flächen lässt sich diese anschauliche Interpretation besonders gut verstehen.

Sei $L = J \dot{\cup} K$ eine orientierte Verschlingung mit zwei Komponenten und $C = S^3 \backslash J$ das Knotenkomplement der ersten Komponente. Durch die Orientierung ist ein Erzeuger von $H_1(C) \cong \mathbb{Z}$ vorgegeben, der durch einen Meridian m in C repräsentiert wird.

Definition. Die Homologieklasse, die der Knoten K in $H_1(C)$ repräsentiert, ist ein Vielfaches $\lambda \cdot [m]$ des Erzeugers. Die Zahl λ wird Verschlingungszahl von L genannt. Wir schreiben dafür $\lambda = \mathrm{lk}(J, K)$.

Definition. Eine Seifert-Fläche für einen orientierten Knoten K oder allgemein für eine Verschlingung in S^3 ist eine zusammenhängende kompakte orientierte Fläche, die in S^3 eingebettet ist und den orientierten Knoten K als Rand hat.

Zu jedem Knoten und jeder Verschlingung gibt es eine Seifert-Fläche. Für unsere stückweise linearen Verschlingungen können wir solche Flächen geometrisch mit Hilfe eines Knotendiagramms finden, wie in Abbildung 3 angedeutet.

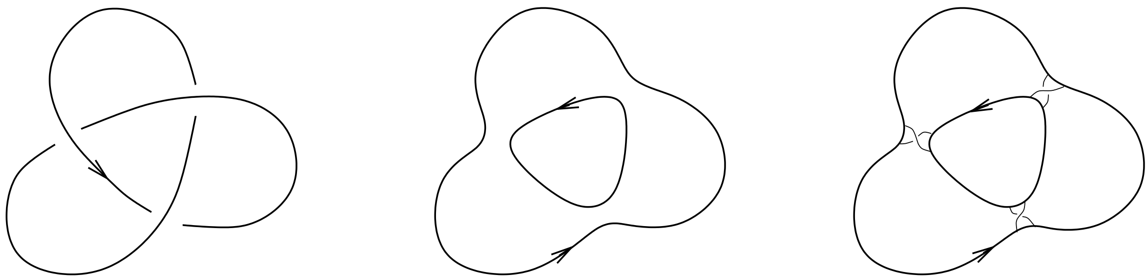


Abbildung 3: Seifert-Fläche

Jede Seifert-Fläche ist homöomorph zu einer Kreisscheibe mit g Paaren von ineinander verschlungenen angeklebten Henkeln. Die Zahl g hängt von der Wahl der Fläche ab und ist keine Invariante des Knotens. In Abbildung 4 kann man zwei verschiedene Seifert-Flächen des trivialen Knotens erkennen.

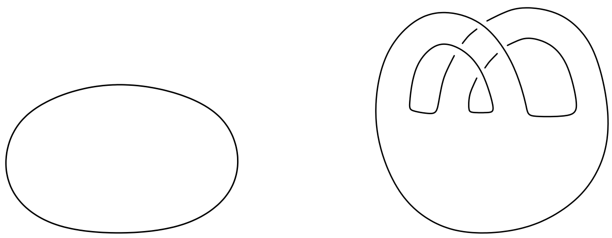


Abbildung 4: Zwei Seifert-Flächen mit verschiedenem Geschlecht

Definition. Das Geschlecht eines Knotens K ist die kleinste Zahl g, für die eine Seifert-Fläche vom Geschlecht g für K existiert.

Für eine Seifert-Fläche F können wir genau wie für einen Knoten eine Umgebung U in S^3 wählen, sodass F eine Deformationsretraktion der Umgebung ist. Wir bezeichnen U als reguläre Umgebung der Seifert-Fläche.

Mit Hilfe einer Seifert-Fläche und des Cup-Produkts auf der Kohomologie lassen sich Verschlingungszahlen ebenfalls beschreiben. Wie im folgenden Diagramm dargestellt, entspricht dem Cup-Produkt auf den Homologiegruppen von C die Schnittform: Für zwei Elemente $a \in H_1(C)$, $b \in H_2(C, \partial C)$ bezeichnen wir mit $a \cdot b \in H_0(C)$ das Element, das man erhält, indem man die Homologiegruppen via Lefschetz-Dualität mit den entsprechenden Kohomologiegruppen identifiziert und das Cup-Produkt bildet.

$$\begin{tikzcd}
H_1(C) \times H_2(C, \partial C) \arrow[r, "„\cdot“"] & H_0(C) \\
H^2(C, \partial C) \times H^1(C) \arrow[u] \arrow[r, "„\cup“"] & H^3(C, \partial C) \arrow[u]
\end{tikzcd}$$

Wenn $[F] \in H_2(C, \partial C)$ und $[K] \in H^1(C)$ durch eine Fläche und eine Kurve in C gegeben sind, die sich transversal schneiden, wird das Element $[F] \cdot [K] \in H_0(C)$ durch ihren Schnitt repräsentiert. Durch die Orientierung von C sind Isomorphismen $H_0(C) \cong \mathbb{Z}$, $H_3(C, \partial C) \cong \mathbb{Z}$ gegeben.

Lemma 1.6. *Für jede Seifert-Fläche F von J ist die Zahl, die dem Element $[F] \cdot [K]$ in $H_0(C)$ entspricht, genau die Verschlingungszahl von L.*

Beweis. Für eine beliebige Seifert-Fläche F von J und einen Meridian m von J gilt $[F] \cdot [m] = \pm 1$ in $H_0(C)$, da man den Meridian so wählen kann, dass er die Fläche genau einmal schneidet. Mit der passenden Orientierung von F gilt also $[F] \cdot [m] = +1$. Nach Definition der Verschlingungszahl ist $[K] = \mathrm{lk}(J, K) \cdot [m]$, und damit folgt

$$[F] \cdot [K] = \mathrm{lk}(J, K) \cdot [F] \cdot [m] = \mathrm{lk}(J, K).$$

□

Wenn man dieses Lemma und ein Knotendiagramm der Verschlingung L zur Hilfe nimmt, kann man erkennen, wie sich aus solchen Diagrammen die Verschlingungszahl direkt ablesen lässt:

Jedem Punkt des Diagramms, an dem sich die beiden Knoten kreuzen, ordnen wir wie in Abbildung 5 eine der Zahlen $\lambda = +\frac{1}{2}$ oder $\lambda = -\frac{1}{2}$ zu. Die Verschlingungszahl ergibt sich dann

(a) $\lambda = +\frac{1}{2}$ (b) $\lambda = -\frac{1}{2}$

Abbildung 5: Verschlingungszahlen

als die Summe aller dieser Zahlen.

Wenn man diese Definition der Verschlingungszahl zweier Knoten zugrunde legt, sieht man sofort, dass die Verschlingungszahl symmetrisch ist, also dass

$$\mathrm{lk}(J, K) = \mathrm{lk}(K, J)$$

für jede Verschlingung $L = J \,\dot\cup\, K$.

1.5 Bestimmen des Alexanderpolynoms mit Hilfe von Seifert-Flächen

Mit Hilfe von Verschlingungszahlen und Seifert-Flächen kann man eine Bilinearform finden, aus deren zugehöriger Matrix eine quadratische Präsentationsmatrix für den $\mathbb{Z}[t, t^{-1}]$-Modul $H_1(C_\infty)$ gewonnen werden kann. Das erste Alexander-Ideal ist also ein Hauptideal, und die Determinante der Präsentationsmatrix liefert das Alexanderpolynom. Das Ergebnis kann außerdem dazu verwendet werden zu zeigen, dass das Alexanderpolynom nicht von der Wahl des Isomorphismus $\mathbb{Z}[D] \to \mathbb{Z}[t, t^{-1}]$ abhängt. Mehr Details zu den folgenden Ausführungen stehen in Kapitel 6 von [24].

Satz 1.7. *Sei K ein Knoten und F eine Seifert-Fläche mit minimalem Geschlecht g. Dann sind die Homologiegruppen $H_1(F)$ und $H_1(S^3 \backslash F)$ isomorph und es gibt eine eindeutig bestimmte nicht ausgeartete Bilinearform*

$$\beta : H_1(S^3 \backslash F) \times H_1(F) \to \mathbb{Z},$$

sodass $\beta([c], [d])$ für alle orientierten einfachen geschlossenen Kurven c in $S^3 \backslash F$ und d in F durch die Verschlingungszahl $\mathrm{lk}(c, d)$ gegeben ist.

Beweis. Die Isomorphie ergibt sich aus dem Satz von Mayer-Vietoris. Sei dazu U eine reguläre Umgebung von F in S^3 und V eine offene Deformationsretraktion des Komplements von U, sodass $V \cap U \simeq \partial U$. Man kann sich U als eine Kugel mit $2g$ Henkeln vorstellen, sodass die Homologiegruppe $H_1(\partial U)$ zu $\mathbb{Z}^{4g}$ isomorph ist. Eine Basis bilden die Elemente $f_1', \ldots, f_{2g}', e_1, \ldots, e_{2g}$, die man wie in Abbildung 6 wählt:

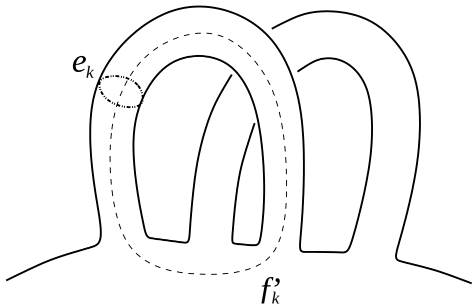


Abbildung 6: Erzeuger von $H_1(\partial U)$

Die Erzeuger f_i' werden unter der Inklusion $\partial U \to U$ auf die $2g$ Erzeuger $f_1, \ldots, f_{2g}$ von $H_1(U)$ abgebildet, und e_i ist jeweils der Rand einer Kreisscheibe, die durch Durchschneiden eines Henkels entsteht. In $H_1(U)$ wird e_i damit auf 0 abgebildet.

Die Mayer-Vietoris-Sequenz liefert wegen $H_1(S^3) = H_2(S^3) = 0$ einen Isomorphismus $H_1(U) \oplus H_1(V) \cong H_1(\partial U)$. Also gilt

$$H_1(F) \oplus H_1(S^3 \backslash F) \cong H_1(\partial U) \cong \mathbb{Z}^{4g},$$

und eine Basis für $H_1(S^3 \backslash F) \cong \mathbb{Z}^{2g}$ ist durch die Bilder der Erzeuger $e_1, \ldots, e_{2g}$ gegeben.

Wir können eine Bilinearform β auf diesen Basen $\{e_i\}$ und $\{f_j\}$ durch die Gleichungen

$$\beta([e_i], [f_j]) = \delta_{ij}$$

definieren. Wenn man die Orientierung von e_i und f_j passend wählt, erhält man für die Erzeuger genau die Verschlingungszahl $\mathrm{lk}(e_i, f_j)$. Für zwei beliebige orientierte einfache geschlossene

Kurven c in F und d in $S^3\backslash F$ mit $[c] = \sum \lambda_i[e_i]$ und $[d] = \sum \mu_j[f_j]$ gilt $\beta([c],[d]) = \sum \lambda_i\mu_i$. Die Verschlingungszahl $\mathrm{lk}(c, f_j)$ ist Summe der Verschlingungszahlen der einzelnen Komponenten e_i und f_j, da alle Zahlen, die den Kreuzungspunkten entsprechen, addiert werden. Also gilt $\mathrm{lk}(c, f_j) = \lambda_j$, und analog erhält man die Verschlingungszahl $\sum \lambda_i\mu_i$ für c und d. $\square$

Sei $F \times [-1;1]$ eine reguläre Umgebung der Seifert-Fläche F in S^3. Wir identifizieren die Fläche F mit $F \times \{0\}$ und wählen die Einbettung so, dass ein Meridian des Knotens die Umgebung in Richtung von -1 nach 1 durchläuft.

Seien i^+ und i^- die Einbettungen von F in die Umgebung $F \times [-1;1]$, die durch $i^+(x) = (x,1)$ bzw. $i^-(x) = (x,-1)$ gegeben sind. Diese Einbettungen induzieren Abbildungen von $H_1(F)$ in $H_1(S^3\backslash F)$.

Definition. Die zu der Seifert-Fläche F assoziierte Seifert-Form ist die Bilinearform

$$\alpha : H_1(F) \times H_1(F) \to \mathbb{Z},$$

die durch die Gleichung $\alpha(x, y) = \beta(i_*^-(x), y)$ definiert ist.

Bezeichnen wir die Bilder einer orientierten einfachen geschlossenen Kurve c in F unter den Abbildungen i^+, i^- mit c^+ bzw. c^-, so ist nach Definition von β

$$\alpha([c],[d]) = \mathrm{lk}(c^-, d) = \mathrm{lk}(c, d^+).$$

Nach Wahl einer Basis $\{f_1, \ldots, f_{2g}\}$ von $H_1(F)$ können wir die Bilinearform α durch eine Matrix A beschreiben, für die dann gilt

$$A = (a_{ij}) = (\alpha([f_i],[f_j])) = (\mathrm{lk}(f_i^+, f_j)) = (\mathrm{lk}(f_i, f_j^-)).$$

Definition. Eine Matrix, die die Seifert-Form zu einer Seifert-Fläche bezüglich irgendeiner Basis beschreibt, nennen wir Seifert-Matrix.

Lemma 1.8. *Sei C ein Knotenkomplement mit universeller abelscher Überlagerung C_∞. Schneiden wir C entlang einer beliebigen Seifert-Fläche F für den Knoten durch, so erhalten wir einen neuen Raum Y mit zwei Flächen F^+, $F^- \cong F$ als Rand, und die universelle abelsche Überlagerung ergibt sich durch Aneinanderkleben von abzählbar vielen Räumen $Y_i \cong Y$ mit Rändern F_i^+, $F_i^- \cong F$ entlang der Flächen F_i^+ und F_{i+1}^-.*

Beweis. Die erste Homologiegruppe des Knotenkomplements wird vom Meridian des Knotens erzeugt, der für eine beliebige Seifert-Fläche F so gewählt werden kann, dass er F genau einmal schneidet. Der Erzeuger der Deckbewegungsgruppe D kann durch die Hochhebung dieses Meridians repräsentiert werden, die von Y_0 nach Y_1 verläuft und den Durchschnitt von Y_0 und Y_1 damit ebenfalls einmal schneidet. Die Gruppen $H_1(C_\infty)$ und D sind also kanonisch isomorph, damit muss die Überlagerung C_∞ die eindeutig bestimmte Überlagerung mit Deckbewegungsgruppe G^{ab} sein. $\square$

Satz 1.9. *Sei F eine Seifert-Fläche für K und A eine Seifert-Matrix für F bezüglich irgendeiner Basis von $H_1(F)$. Dann ist $tA - A^t$ eine Präsentationsmatrix für den $\mathbb{Z}[t, t^{-1}]$-Modul $H_1(C_\infty)$ und das Alexanderpolynom ist damit die Determinante dieser Matrix.*

Beweis. Wir geben hier nur die wesentlichen Schritte wieder; für weitere Details siehe [24], Ch. 6.

Sei $Y_g = \dot\bigcup_{n\in\mathbb{Z}} Y_{2n}$ und $Y_u = \dot\bigcup_{n\in\mathbb{Z}} Y_{2n+1}$, sodass $Y_g \cup Y_u = C_\infty$ und $Y_g \cap Y_u = \dot\bigcup_{n\in\mathbb{Z}} F_n$. Da die kanonischen Abbildungen $C_\infty \to Y$, $Y_g \dot\cup Y_u \to Y$ und $Y_g \cap Y_u \to F$ jeweils Überlagerungen mit Decktransformationsgruppe $D \cong \mathbb{Z}$ sind, werden die Homologiegruppen $H_*(C_\infty)$, $H_*(Y_g) \oplus H_*(Y_u) = H_*(Y_g \dot\cup Y_u), H_*(Y_g \cap Y_u)$ zu $\mathbb{Z}[D]$-Moduln, und die Mayer-Vietoris-Sequenz liefert eine exakte Sequenz von $\mathbb{Z}[D]$-Moduln

$$H_1(Y_g \cap Y_u) \to H_1(Y_g) \oplus H_1(Y_u) \to H_1(C_\infty) \to H_0(Y_g \cap Y_u) \to H_0(Y_g) \oplus H_0(Y_u).$$

Da die letzte Abbildung injektiv ist, erhalten wir die gesuchte freie Präsentation

$$H_1(Y_g \cap Y_u) \to H_1(Y_g) \oplus H_1(Y_u) \to H_1(C_\infty) \to 0$$

des $\mathbb{Z}[D]$-Moduls $H_1(C_\infty)$ und müssen nur noch nachweisen, dass die angegebene Präsentationsmatrix die richtige ist.

Eine Basis von $H_1(Y_g \cap Y_u) = H_1(F) \otimes_{\mathbb{Z}} \mathbb{Z}[t, t^{-1}]$ als $\mathbb{Z}[t, t^{-1}]$-Modul erhält man aus der vorgegebenen $\mathbb{Z}$-Basis $\{[e_i]\}$ von $H_1(F)$; wir bezeichnen sie ebenfalls mit $\{[e_i]\}$. Aus einer bezüglich der Bilinearform β dualen $\mathbb{Z}$-Basis $\{[f_j]\}$ von $H_1(S^3 \backslash F) \cong H_1(Y)$ erhalten wir ähnlich eine $\mathbb{Z}[t, t^{-1}]$-Basis von $H_1(Y_g) \oplus H_1(Y_u) \cong H_1(Y) \otimes_{\mathbb{Z}} \mathbb{Z}[t, t^{-1}]$.

Die Abbildung $H_1(Y_g \cap Y_u) \to H_1(Y_g) \oplus H_1(Y_u)$ ist dann durch $[f_i] \mapsto -[f_i^+] + t \cdot [f_i^-]$ gegeben. Nach Definition von $A = (A_{ij})$ hat $[f_i^+]$ in $H_1(Y)$ die Darstellung $\sum_i A_{ij}[e_i]$ und $[f_i^-]$ hat die Darstellung $\sum_j A_{ij}[e_j]$. Der $\mathbb{Z}[t, t^{-1}]$-Modulhomomorphismus $H_1(Y_g \cap Y_u) \to H_1(Y_g) \oplus H_1(Y_u)$ wird bezüglich der angegebenen Basen also durch die Matrix $-A^t + tA$ dargestellt. □

Aus der Darstellung des Alexanderpolynoms als Determinante von $tA - A^t$ kann man ablesen, dass das Polynom bis auf Multiplikation mit Einheiten aus $\mathbb{Q}[t, t^{-1}]$ von der Wahl des Isomorphismus $\mathbb{Z}[D] \to \mathbb{Z}[t, t^{-1}]$ unabhängig ist: Setzt man anstelle von t das Element t^{-1} ein, so erhält man wegen $\det A \neq 0$

$$\begin{aligned} \det(t^{-1}A - A^t) &\sim \det(A(A^t)^{-1} - tE) \\ &= \det((A^{-1}A^t)^t - tE) \\ &= \det(A^{-1}A^t - tE) \\ &\sim \det(A^t - tA) \\ &\sim \det(tA - A^t). \end{aligned}$$

Das Zeichen „$\sim$“ steht hier für Gleichheit bis auf Multiplikation mit einer Einheit aus $\mathbb{Z}[t, t^{-1}]$. Wie angekündigt spielt es also keine Rolle, welcher Erzeuger von $H_1(C)$ auf das Element t abgebildet wird. Als weiteres Resultat ergibt sich aus dieser Darstellung:

Satz 1.10. *Für jeden Knoten gilt* $\Delta(1) = \pm 1$.

Beweis. Berechnet man die Determinante von $tA - A^t$ für $t = 1$, so ergibt sich für den Eintrag in der i-ten Zeile und j-ten Spalte:

$$\begin{aligned} a_{ij} - a_{ji} &= \mathrm{lk}(f_i^+, f_j) - \mathrm{lk}(f_j^+, f_i) \\ &= \mathrm{lk}(f_i^+, f_j) - \mathrm{lk}(f_i^-, f_j) \\ &= \mathrm{lk}(f_i^+, f_j) + \mathrm{lk}(-f_i^-, f_j) \\ &= \mathrm{lk}(g_i, f_j) \end{aligned}$$

wobei g_i einen eingebetteten Kreis in der 3-Sphäre bezeichnet, den man erhält, indem man f_i^- mit umgekehrter Orientierung und f_i^+ so verbindet, dass der resultierende Zykel in $H_1(S^3 \backslash f_j)$ dasselbe Element liefert wie $f_i^+ - f_i^-$. Diese Zahl erhält man nach Lemma 1.6 nach Wahl einer Seifert-Fläche A von g_i mit $[A] \in H_2(S^3, g_i)$ als Schnittzahl $[A] \cdot [f_j]$. Statt A kann man die Seifert-Fläche $A' = f_i \times [-1; 1]$ mit $[A'] \in H_2(S^3, f_i^+ \dot\cup f_i^-)$ wählen, die dieselbe Schnittzahl $[A'] \cdot [f_j]$ liefert.

(a) Die Fläche A

(b) Die Fläche A'

Abbildung 7: Seifert-Flächen

Da der Schnitt von A' und F genau die Kurve $f_i \subset F$ ist, gilt $[A'] \cdot [f_j] = \pm [f_i] \cdot [f_j]$. Also ist der Eintrag in der i-ten Zeile und j-ten Spalte von $A - A^t$ die Schnittzahl von f_i und f_j. Damit beschreibt die Matrix die Schnittform auf F, und ihre Determinante hat den Betrag 1. Daraus folgt $\Delta(1) = \pm 1 \neq 0$. ☐

Korollar 1.11. *Der Alexandermodul eines Knotens ist ein endlich erzeugter $\mathbb{Z}[t, t^{-1}]$-Modul vom Rang 0, und der $\mathbb{Q}[t, t^{-1}]$-Modul $H_1(C_\infty) \otimes \mathbb{Q}$ hat als $\mathbb{Q}$-Vektorraum endliche Dimension.*

Beweis. Da der Alexandermodul eine endliche Präsentationsmatrix besitzt, ist er offenbar endlich erzeugt. Nach Satz 1.5 ist das nullte Fitting-Ideal für Moduln mit positivem Rang das Nullideal, es gilt aber $\Delta(1) = \pm 1$ und damit $F_0(H_1(C_\infty)) \neq 0$.

Nach dem Struktursatz für endlich erzeugte Moduln über Hauptidealringen gilt

$$H_1(C_\infty) \otimes \mathbb{Q} = \bigoplus_{i=1}^{n} \mathbb{Q}[t, t^{-1}]/(g_i(t))$$

mit passenden Elementen $g_i(t) \in \mathbb{Q}[t, t^{-1}]$. Da wegen $g_i(t) \neq 0$ jeder Summand ein endlichdimensionaler $\mathbb{Q}$-Vektorraum ist, ist auch $H_1(C_\infty) \otimes \mathbb{Q}$ endlichdimensional. ☐

1.6 Beispiel: Das Alexanderpolynom eines Torusknotens

Der Torusknoten mit Parametern $a, b \in \mathbb{N}$ ist der Knoten, den man erhält, wenn man einen Bindfaden a-mal in Längsrichtung und b-mal in Richtung des Meridians um einen Torus wickelt. Der Knoten entspricht also der Einbettung

$$\begin{array}{rcl} S^1 & \to & S^1 \times S^1 \subset \mathbb{R}^3 \subset S^3, \\ z & \mapsto & (z^a, z^b). \end{array}$$

Wir setzen im Folgenden immer voraus, dass die Parameter a und b teilerfremd sind, damit diese Abbildung wirklich eine Einbettung ist.

Um das Alexanderpolynom eines Torusknotens berechnen zu können, bestimmen wir zunächst eine Präsentation der Knotengruppe ([15], Ex. 1.24) und daraus eine Präsentation des Alexandermoduls.

1.6.1 Die Knotengruppe eines Torusknotens

Satz 1.12. *Die Knotengruppe eines Torusknotens K mit Parametern a und b hat die Präsentation*

$$G = \langle x, y | x^a y^{-b} \rangle.$$

Beweis. Um $\pi_1(S^3 \backslash K)$ zu berechnen, teilen wir die 3-Sphäre auf in den Abschluss des „Inneren“ und des „Äußeren“ des Torus $S^1 \times S^1$:

$$S^3 = \partial D^4 = \partial(D^2 \times D^2) = \partial D^2 \times D^2 \cup D^2 \times \partial D^2$$

ist die Vereinigung von zwei Volltori, deren Schnitt den Torus ergibt, in den der Knoten K eingebettet ist.

Für diese beiden Teile geben wir dann Deformationsretraktionen in Mengen X_a und X_b an, für deren Vereinigung sich die Fundamentalgruppe mit Hilfe des Satzes von Seifert und van Kampen berechnen lässt.

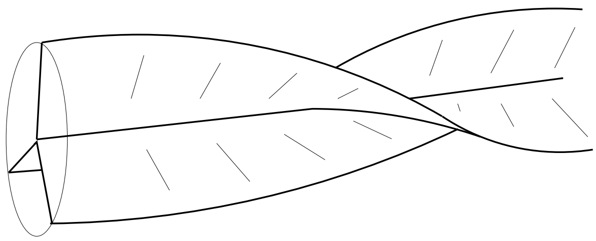


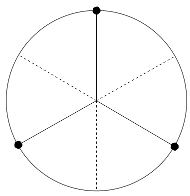
Abbildung 8: Die Menge X_a

Sei $X = S^1 \times I/((z,0) \sim (e^{2\pi i/a} \cdot z, 0), (z,1) \sim (e^{2\pi i/b} \cdot z, 1))$. Wir teilen den Raum X auf in

$$\begin{aligned} X_a &= S^1 \times [0, \frac{1}{2}]/((z,0) \sim (e^{2\pi i/a} \cdot z, 0)) \quad \text{und} \\ X_b &= S^1 \times [\frac{1}{2}, 1]/((z,1) \sim (e^{2\pi i/b} \cdot z, 1)), \end{aligned}$$

also in die beiden Abbildungszylinder der Abbildungen $z \mapsto z^a$ und $z \mapsto z^b$. Der Schnitt von X_a und X_b ist die Menge $S^1 \times \{\frac{1}{2}\}$. Die Menge X_a findet sich im Torus $S^1 \times D^2$ folgendermaßen wieder:

Abbildung 9: Schnitt durch den Torus



Für jeden Punkt $x \in S^1$ schneidet die Menge $\{x\} \times \partial D^2$ den Knoten K in a Punkten, die jeweils in gleichen Abständen zueinander auf dem Kreis S^1 liegen und durch a Radien dieses Kreises, jeweils in der Mitte zwischen zwei benachbarten Punkten, voneinander getrennt werden können. Abbildung 9 zeigt die Menge $\{x\} \times D$: Wenn x variiert, schneiden diese

Radien eine zu X_a homöomorphe Teilmenge von $S^1 \times D^2$ aus. Analog dazu findet man eine zu X_b homöomorphe Teilmenge im zweiten Volltorus. Der Schnitt dieser beiden Teilmengen ist die Menge, die in beiden Fällen durch die Endpunkte der Radien ausgeschnitten wird. In Abbildung 10 ist diese Menge eingezeichnet.

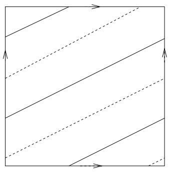


Abbildung 10: Torusoberfläche

Das Komplement von K im ersten Torus kann durch Deformationsretraktion auf die Menge X_a abgebildet werden. Analog bildet man das Komplement von K im zweiten Torus auf die Menge X_b ab. Diese Abbildungen können so gewählt werden, dass sie auf dem Schnitt dieser Komplemente, also auf dem Torus, der den inneren vom äußeren Volltorus trennt, übereinstimmen.

Um nun die Fundamentalgruppe des Raumes X zu berechnen, wenden wir den Satz von Seifert und van Kampen auf die beiden Teile X_a und X_b an, genauer also auf zwei passende offene Umgebungen. Die Mengen X_a, X_b und $X_a \cap X_b$ sind homotopieäquivalent zu Kreisen, haben also jeweils Fundamentalgruppe $\mathbb{Z}$. Ein Repräsentant eines Erzeugers von $\pi_1(X_a \cap X_b)$ ist in X_a homotop zu einer Schleife, die a-mal einen Erzeuger von $\pi_1(X_a)$ repräsentiert und entspricht in X_b analog dem b-fachen eines Erzeugers von $\pi_1(X_b)$. Die Fundamentalgruppe $\pi_1(X)$ ergibt sich als das amalgamierte Produkt

$$\pi_1(X_a) *_{\pi_1(X_a \cap X_b)} \pi_1(X_b)$$

und hat damit die Präsentation

$$\langle x, y | x^a y^{-b} \rangle.$$

□

1.6.2 Berechnen des Alexanderpolynoms

Sei t ein Erzeuger von $G/G' \cong \mathbb{Z}$ und $\varphi : G \to G/G' \cong \langle t \rangle$ die Quotientenabbildung. Die Erzeuger x und y von G werden jeweils auf eine Potenz von t abgebildet, und da ihre Bilder in $\langle t \rangle$ die Gruppe erzeugen, müssen die Exponenten teilerfremd sein. Aus der Relation $\varphi(x)^a \varphi(y)^{-b} = 1$ folgt damit $\varphi(x) = t^b$ und $\varphi(y) = t^a$ bis auf Vertauschen von t und $-t$.

Da das Alexanderpolynom nur von der Fundamentalgruppe des Knotenkomplements abhängt, können wir dieses durch einen CW-Komplex X mit dem Punkt P als einziger 0-Zelle, je einer 1-Zelle für x und y und einer 2-Zelle für die Relation $x^a y^{-b} = 1$ ersetzen und alle Konstruktionen mit diesem Raum durchführen.

Sei $p : X_\infty \to X$ die Überlagerung mit Fundamentalgruppe G'. Als Decktransformationsgruppe operiert $D = \langle t \rangle$ für jeden Punkt $Q \in X$ transitiv auf der Faser $p^{-1}(Q)$. Seien $\tilde{P}$ ein Punkt über P und $\tilde{x}, \tilde{y}$ die Hochhebungen von x und y, die bei $\tilde{P}$ beginnen. Wir können $\tilde{x}, \tilde{y}$ und die Hochhebung von $x^a y^{-b}$ bei $\tilde{P}$ als Elemente von $H_1(X_\infty, X_\infty^{(0)})$ auffassen.

Als $\mathbb{Z}[D]$-Modul wird $H_1(X_\infty, X_\infty^{(0)})$ von $\tilde{x}$ und $\tilde{y}$ erzeugt, da alle 1-Zellen $\mathbb{Z}[D]$-Vielfache von $\tilde{x}$ oder $\tilde{y}$ sind. Alle 2-Zellen sind $\mathbb{Z}[D]$-Vielfache der Hochhebung der einzigen 2-Zelle von X, also genügt für die Beschreibung des $\mathbb{Z}[D]$-Moduls $H_1(X_\infty, X_\infty^{(0)})$ eine einzige Relation r, die der Hochhebung von $x^a y^{-b}$ entspricht. Als $\mathbb{Z}[D]$-Linearkombination der Erzeuger $\tilde{x}$ und $\tilde{y}$ lässt sich diese Relation folgendermaßen schreiben:

$$\begin{aligned} r &= \widetilde{x^a y^{-b}} \\ &= \tilde{x} + \varphi(x)\tilde{x} + \varphi(x)^2\tilde{x} + \cdots + \varphi(x)^{a-1}\tilde{x} + \varphi(x)^a(-\varphi(y)\tilde{y}^{-1} - \varphi(y)^{-2}\tilde{y} - \cdots - \varphi(y)^{-b}\tilde{y}) \\ &= (1 + t^b + t^{2b} + \cdots + t^{b(a-1)}) \cdot \tilde{x} + t^{ab}(-t^a - t^{2a} - \cdots - t^{ab}) \cdot \tilde{y} \\ &= \frac{t^{ab}-1}{t^b-1} \cdot \tilde{x} - \frac{t^{ab}-1}{t^a-1} \cdot \tilde{y}. \end{aligned}$$

Die exakte Sequenz

$$\mathbb{Z}[D] \to \mathbb{Z}[D]^2 \to H_1(X_\infty, X_\infty^{(0)}) \to 0,$$

in der die erste Abbildung durch die Matrix $A = (\frac{t^{ab}-1}{t^b-1}\ \frac{t^{ab}-1}{t^a-1})^t$ beschrieben wird, ist also eine Präsentation von $H_1(X_\infty, X_\infty^{(0)})$ als $\mathbb{Z}[D]$-Modul.

Aus der langen exakten Sequenz für relative Homologie erhält man

$$0 \to H_1(X_\infty) \to H_1(X_\infty, X_\infty^{(0)}) \xrightarrow{\partial} H_0(X_\infty^{(0)}) \xrightarrow{i_*} H_0(X_\infty) \to 0,$$

wobei $H_0(X_\infty^{(0)}) \cong \mathbb{Z}[D]$, $H_0(X_\infty) \cong \mathbb{Z}$ und $\ker i_* = (t-1)$. Da $\ker i_*$ als Hauptideal ein freier $\mathbb{Z}[D]$-Modul vom Rang 1 ist, erhält man aus der exakten Sequenz

$$0 \to H_1(X_\infty) \to H_1(X_\infty, X_\infty^{(0)}) \to \ker i_* \to 0$$

und Satz 1.5 die Gleichung $\Delta(t) = \Delta_0(H_1(X_\infty)) = \Delta_1(H_1(X_\infty, X_\infty^{(0)}))$.

Das Alexanderpolynom des Torusknotens ergibt sich also als größter gemeinsamer Teiler der beiden Einträge von A. Das Polynom

$$\frac{t^{ab}-1}{t^b-1} \cdot \frac{t-1}{t^a-1} = \frac{t^{ab}-1}{t^a-1} \cdot \frac{t-1}{t^b-1}$$

erhält man aus diesen Einträgen, indem man durch $\frac{t^a-1}{t-1}$ bzw. $\frac{t^b-1}{t-1}$ teilt. Da diese beiden Polynome teilerfremd sind, ist $\frac{t^{ab}-1}{t^a-1} \cdot \frac{t-1}{t^b-1}$ der größte gemeinsame Teiler der Einträge und damit das gesuchte Alexanderpolynom.

Wie diese Beobachtungen zu einer allgemeinen Berechnungsmethode für das Alexanderpolynom ausgearbeitet werden können, wird am Anfang des fünften Kapitels beschrieben.

2 Iwasawatheorie

Die Untersuchung von unendlichen Erweiterungen von Zahlkörpern mit Galoisgruppe $\mathbb{Z}_p$ wurde von K. Iwasawa in [16] mit seinem inzwischen berühmten Resultat über das Wachstum der p-Klassenzahlen in einer solchen Erweiterung eingeleitet. In diesem Kapitel werden zunächst einige Hilfsmittel bereitgestellt, die man benötigt, um mittels der von Iwasawa ([16], [18] u.a.) entwickelten Theorie die Struktur bestimmter unendlicher Galoisgruppen zu untersuchen.

2.1 Ergebnisse aus der Klassenkörpertheorie

Die Klassenkörpertheorie vergleicht in ihrer einfachsten Form die Klassengruppen von Zahlkörpern mit Galoisgruppen bestimmter unverzweigter Erweiterungen. Iwasawa stellt in [16] sein Resultat zunächst als eine Version dieses Vergleichs für unendliche Zahlkörper dar.

Wir werden in diesem Kapitel Galoisgruppen als Moduln über der nach ihm benannten „Iwasawa-Algebra“ betrachten. Das ist ein vollständiger Gruppenring, der einerseits mit Hilfe von Idealklassengruppen und andererseits mit Hilfe von Galoisgruppen definiert werden kann. Dass beide Sichtweisen zum gleichen Ergebnis führen, folgt aus einigen grundlegenden Aussagen der Klassenkörpertheorie ([46], Anhang 3), die deshalb in diesem Abschnitt zusammengestellt sind.

Sei K'/K eine endliche galoissche unverzweigte Erweiterung von Zahlkörpern, $\mathfrak{p}$ ein Primideal in $\mathcal{O}_K$ mit Norm $N\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|$ und $\mathfrak{P}$ ein darüberliegendes Primideal in $\mathcal{O}_{K'}$. Der Restklassenkörper $\mathcal{O}_{K'}/\mathfrak{P}$ ist eine endliche galoissche Erweiterung von $\mathcal{O}_K/\mathfrak{p}$ mit zyklischer Galoisgruppe $\mathrm{Gal}((\mathcal{O}_{K'}/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$, die vom Frobenius-Automorphismus $x \mapsto x^{N\mathfrak{p}}$ erzeugt wird.

Da K'/K als unverzweigt vorausgesetzt wurde, ist die Zerlegungsgruppe $Z(\mathfrak{P}|\mathfrak{p})$ kanonisch isomorph zu $\mathrm{Gal}((\mathcal{O}_{K'}/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$. Dem Frobenius-Automorphismus wird unter diesem Isomorphismus der Automorphismus $\sigma_\mathfrak{P} \in \mathrm{Gal}(K'/K)$ zugeordnet, der durch die Angaben

$$\sigma_\mathfrak{P}(\mathfrak{P}) \subset \mathfrak{P} \quad \text{und} \quad \sigma_\mathfrak{P}(x) \equiv x^{N\mathfrak{p}} \mod \mathfrak{P} \text{ für alle } x \in \mathcal{O}_K$$

eindeutig bestimmt ist. Für jeden Automorphismus $\tau \in \mathrm{Gal}(K'/\mathbb{Q})$ gilt $\sigma_{\tau(\mathfrak{P})} = \tau\sigma_\mathfrak{P}\tau^{-1}$, denn für alle $x \in K'$ ist

$$\tau\sigma_\mathfrak{P}\tau^{-1}(x) - x^{N\tau(\mathfrak{p})} = \tau(\sigma_\mathfrak{P}(\tau^{-1}(x)) - \tau^{-1}(x)^{N\tau(\mathfrak{p})})) \in \tau(\mathfrak{P}),$$

da $N\tau(\mathfrak{p}) = N\mathfrak{p}$. Also ist $\tau\sigma_\mathfrak{P}\tau^{-1}(x) \equiv x^{N\tau(\mathfrak{p})} \mod \tau(\mathfrak{P})$ für alle $x \in \mathcal{O}_K$.

Falls K'/K eine abelsche Erweiterung ist, bedeutet das, dass der Automorphismus $\sigma_\mathfrak{P}$ nicht von der Wahl des Primideals $\mathfrak{P}$ über $\mathfrak{p}$ abhängt. In diesem Fall können wir jedem Primideal $\mathfrak{p} \subset \mathcal{O}_K$ den so definierten Automorphismus $\sigma_\mathfrak{P}$ zuordnen und mit $\sigma_\mathfrak{p}$ bezeichnen. Er wird auch Artin-Automorphismus genannt.

Sei $I(K)$ die Gruppe der gebrochenen Ideale von K und

$$\tilde{\varphi} : I(K) \to \mathrm{Gal}(K'/K)$$

die Fortsetzung der durch $\mathfrak{p} \mapsto \sigma_\mathfrak{p}$ definierten Abbildung zu einem Gruppenhomomorphismus. Eines der grundlegenden Ergebnisse aus der Klassenkörpertheorie ist der folgende Satz:

Satz 2.1. *Falls K'/K die maximale abelsche unverzweigte Erweiterung von K ist, induziert $\tilde{\varphi}$ einen Isomorphismus φ zwischen der Klassengruppe $\mathrm{Cl}(K)$ und der Galoisgruppe der Erweiterung.*

Der Körper K' wird in diesem Fall Hilbert'scher Klassenkörper von K genannt. Dass er über K endlichen Grad hat, ist aus der algebraischen Zahlentheorie bekannt. Nach dem vorhergehenden Satz ist diese Aussage äquivalent zur Endlichkeit der Klassenzahl.

Sei L/K eine beliebige galoissche Erweiterung von Zahlkörpern. Dann operiert die Galoisgruppe dieser Erweiterung auf der Idealklassengruppe von L: Falls $\tau \in \mathrm{Gal}(L/K)$ ist und $\mathfrak{a}$ ein gebrochenes Ideal in L, ist $\tau(\mathfrak{a})$ ein gebrochenes Ideal in L, und die durch τ definierte Abbildung induziert einen Automorphismus der Klassengruppe.

Lemma 2.2. *Sei L' der Hilbert-Klassenkörper von L. Dann wird die Operation von $\mathrm{Gal}(L/K)$ auf der Idealklassengruppe von L durch φ mit der Konjugationsoperation von $\mathrm{Gal}(L/K)$ auf $\mathrm{Gal}(L'/L)$ identifiziert.*

Beweis. Die Galoisgruppe $\mathrm{Gal}(L/K)$ operiert durch innere Automorphismen in $Gal(L'/K)$ kanonisch auf der abelschen Gruppe $\mathrm{Gal}(L'/L)$. Sei $\tau \in \mathrm{Gal}(L/K)$ und $\tilde{\tau}$ ein Urbild in $\mathrm{Gal}(L'/K)$. Mit der gleichen Rechnung wie oben folgt $\tau \circ \sigma_{\mathfrak{p}} = \tilde{\tau}\sigma_{\mathfrak{p}}\tilde{\tau}^{-1} = \sigma_{\tau(\mathfrak{p})}$, man erhält also durch Konjugation den Artin-Automorphismus zum Primideal $\tau(\mathfrak{p})$. $\square$

Sei L/K eine endliche galoissche Erweiterung von Zahlkörpern, $\mathfrak{P}$ ein Primideal in $\mathcal{O}_L$ und $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{K'}$. Wie üblich bezeichnen wir mit f den Trägheitsgrad von $\mathfrak{P}$ über $\mathfrak{p}$, also den Grad der Körpererweiterung $\mathcal{O}_L/\mathfrak{P} \supset \mathcal{O}_{K'}/\mathfrak{p}$.

Lemma 2.3. *Die Zuordnung $\mathfrak{P} \mapsto \mathfrak{p}^f$ definiert einen Homomorphismus*

$$\mathrm{Norm}_{L/K} : \mathrm{Cl}(L) \to \mathrm{Cl}(K)$$

zwischen den Klassengruppen von L und K.

Beweis. Zunächst kann man die Abbildung zu einem Homomorphismus zwischen den Gruppen der gebrochenen Ideale fortsetzen. Da Hauptideale auf Hauptideale abgebildet werden, erhält man nach Übergang zu den Quotienten eine Abbildung zwischen den Klassengruppen. $\square$

Lemma 2.4. *Seien K' und L' die Klassenkörper von K und L. Dann ist das folgende Diagramm kommutativ:*

$$\begin{array}{ccc} \mathrm{Cl}(L) & \xrightarrow{\varphi} & \mathrm{Gal}(L'/L) \\ {\scriptstyle \mathrm{Norm}_{L/K}}\downarrow & & \downarrow \\ \mathrm{Cl}(K) & \xrightarrow{\varphi} & \mathrm{Gal}(K'/K) \end{array}$$

Die Abbildung $\mathrm{Norm}_{L/K}$ zwischen den Idealklassengruppen wird durch den Isomorhismus φ mit der Abbildung zwischen den Galoisgruppen identifiziert, die man durch Einschränkung der Körperautomorphismen erhält.

Beweis. Sei $\mathfrak{P}$ ein Primideal in $\mathcal{O}_L$, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ und $f = f(\mathfrak{P}|\mathfrak{p})$ der Trägheitsgrad. Wir müssen zeigen, dass $\sigma_{\mathrm{Norm}(\mathfrak{P})} = \sigma_{\mathfrak{p}^f} = (\sigma_{\mathfrak{p}})^f$ mit der Einschränkung von $\sigma_{\mathfrak{P}}$ auf K' übereinstimmt. Falls $\mathfrak{P}'$ ein Primideal von L' über $\mathfrak{P}$ ist und $\mathfrak{p}' = \mathfrak{P}' \cap \mathcal{O}_{K'}$, ist diese Einschränkung eindeutig bestimmt durch die Eigenschaften

$$\sigma_{\mathfrak{P}}|_{K'}(\mathfrak{p}') \subset \mathfrak{p}' \quad \text{und} \quad \sigma_{\mathfrak{P}}(x) \equiv x^{N\mathfrak{P}} \mod \mathfrak{p}' \text{ für alle } x \in \mathcal{O}_{K'}.$$

Nach Definition von $\sigma_{\mathfrak{p}}$ und wegen $N\mathfrak{P} = N\mathfrak{p}^f$ hat $(\sigma_{\mathfrak{p}})^f$ ebenfalls diese Eigenschaften. $\square$

2.2 Pro-p-Gruppen

Die Körpererweiterungen, die im Folgenden auftreten, werden unendliche Erweiterungen sein, die sich als Vereinigung von endlichen p-Erweiterungen ergeben. Ihre Galoisgruppen sind also Pro-p-Gruppen. Einen kurzen Überblick über solche Gruppen findet man im ersten Kapitel von [40], ausführlicher werden sie in den beiden Büchern [39] und [47] über pro-endliche Gruppen behandelt.

Definition. Pro-endliche Gruppen sind diejenigen topologische Gruppen, die sich als projektive Limites von endlichen Gruppen ergeben. Pro-p-Gruppen erhält man, wenn man sich dabei auf p-Gruppen einschränkt.

Die pro-endlichen Gruppen sind genau die kompakten total unzusammenhängenden topologischen Gruppen. Die Pro-p-Gruppen sind diejenigen pro-endlichen Gruppen, für die der Index jedes offenen Normalteilers eine p-Potenz ist.

In der Kategorie der Pro-p-Gruppen kann man genau wie für abstrakte Gruppen freie Objekte definieren, die auf endlichen Mengen durch die gewohnte universelle Eigenschaft beschrieben werden. Nur für unendliche Indexmengen wird die Definition leicht modifiziert ([40], §1.5):

Definition. Wir nennen eine Teilmenge einer pro-endlichen Gruppe konvergent, wenn jeder offene Normalteiler fast alle Elemente der Menge enthält.

Definition. Die freie Pro-p-Gruppe auf der Menge I ist eine Pro-p-Gruppe F_I zusammen mit Elementen $s_i \in F_I$ für jedes $i \in I$, sodass die folgende universelle Eigenschaft erfüllt ist:

Für jede Abbildung φ von I in eine Pro-p-Gruppe G, deren Bild eine konvergente Teilmenge von G ist, gibt es einen eindeutig bestimmten Morphismus topologischer Gruppen $f_\varphi : F_I \to G$, sodass $f_\varphi(s_i) = \varphi(i)$ für alle i.

Freie Pro-p-Gruppen existieren für beliebige Indexmengen und können folgendermaßen konstruiert werden: Sei $F(I) = \langle s_i \rangle_{i \in I}$ die freie Gruppe auf der Menge I und $\mathfrak{N}$ die Menge aller Normalteiler N von $F(I)$, deren Index eine p-Potenz ist und die fast alle Elemente s_i enthalten. Dann ist

$$F_I = \varprojlim F(I)/N,$$

wobei N die Normalteiler aus $\mathfrak{N}$ durchläuft, die freie Pro-p-Gruppe auf der Menge I.

Im Folgenden ist mit einem Erzeugendensystem einer pro-endlichen Gruppe immer ein topologisches Erzeugendensystem gemeint, also eine Menge, die eine dichte Untergruppe erzeugt. Die freie Pro-p-Gruppe F_I wird topologisch von den Elementen s_i erzeugt.

Die freie Pro-p-Gruppe mit einem Erzeuger ist die Gruppe $\mathbb{Z}_p$, die man als projektiven Limes des Systems $\{\mathbb{Z}/p^n\mathbb{Z}\}$ mit den offensichtlichen Projektionsabbildungen erhält. Ihre abgeschlossenen Untergruppen sind die Gruppen $p^n\mathbb{Z}_p$ für $n \in \mathbb{N}_0$, die als topologische Gruppen wieder zu $\mathbb{Z}_p$ isomorph sind.

Die Pro-p-Gruppe $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ hat nicht nur eine Struktur als pro-endliche Gruppe, sondern ist sogar projektiver Limes von Ringen, also ein pro-endlicher topologischer Ring. Die Einheitengruppe in $\mathbb{Z}_p$ ist die Gruppe $\mathbb{Z}_p^* = \varprojlim(\mathbb{Z}/p^n\mathbb{Z})^*$. Ihr Torsionsanteil ist die Untergruppe der $(p-1)$-ten Einheitswurzeln, also eine zyklische Gruppe der Ordnung $p-1$, und als torsionsfreien Anteil enthält sie einen Faktor, der zur additiven Gruppe $\mathbb{Z}_p$ isomorph ist.

Bemerkung. So wie jede abelsche Gruppe ein $\mathbb{Z}$-Modul ist, hat jede abelsche Pro-p-Gruppe in kanonischer Weise eine Struktur als $\mathbb{Z}_p$-Modul.

Wie abstrakte Gruppen kann man Pro-p-Gruppen als Quotienten von freien Pro-p-Gruppen schreiben und Präsentationen solcher Gruppen angeben:

Lemma 2.5. *Jede Pro-p-Gruppe besitzt ein konvergentes Erzeugendensystem.*

Einen Beweis findet man in [39] (Proposition 2.2.4). Mit der universellen Eigenschaft von freien Pro-p-Gruppen ergibt sich aus dem Lemma unmittelbar:

Korollar 2.6. *Jede Pro-p-Gruppe ist Quotient einer freien Pro-p-Gruppe.*

Für eine Pro-p-Gruppe G kann man eine Präsentation angeben, indem man ein konvergentes Erzeugendensystem $\{e_i | i \in I\}$ wählt und den zugehörigen Epimorphismus von der freien Pro-p-Gruppe auf der Menge $\{e_i\}$ in G betrachtet. Der Kern R dieser Abbildung besitzt als Pro-p-Gruppe ebenfalls ein konvergentes Erzeugendensystem $\{r_j | j \in J\}$. Man schreibt wie gewohnt $G = \langle e_i | r_j \rangle$ und verwendet diese Schreibweise auch dann, wenn $\{r_j\}$ den Kern R nicht als Untergruppe, sondern als Normalteiler erzeugt.

2.3 $\mathbb{Z}_p$-Erweiterungen von Zahlkörpern

Eine $\mathbb{Z}_p$-Erweiterung eines Zahlkörpers K ist eine galoissche Körpererweiterung $K_\infty \supset K$, deren Galoisgruppe als topologische Gruppe zur additiven Gruppe $\mathbb{Z}_p$ isomorph ist. Iwasawas Artikel [16] ist die erste einer Reihe von Veröffentlichungen, die sich mit den Eigenschaften solcher Erweiterungen beschäftigen.

Da die abgeschlossenen Untergruppen von $\mathbb{Z}_p$ genau die Gruppen der Form $p^n\mathbb{Z}_p$ sind, erhält man eine Kette

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty,$$

wobei K_n jeweils der Fixkörper von $p^n\mathbb{Z}_p$ ist, und außer diesen Körpern gibt es in einer $\mathbb{Z}_p$-Erweiterung keine Zwischenkörper. Die Galoisgruppen der Teilerweiterungen K_n/K sind jeweils zyklische Gruppen der Ordnung p^n.

Der Körper der rationalen Zahlen hat, wie am Ende des Abschnitts gezeigt wird, genau eine $\mathbb{Z}_p$-Erweiterung. Der n-te Zwischenkörper dieser Erweiterung ist im Kreisteilungskörper $\mathbb{Q}(\zeta_{p^n})$ enthalten. Das Primideal (p) ist also in jedem Zwischenkörper voll verzweigt ([32], Ch. II, Prop. 7.13). Wir untersuchen im übrigen Teil des Abschnitts, welche Art von Verzweigung in $\mathbb{Z}_p$-Erweiterungen beliebiger Zahlkörper auftreten kann.

Im Zahlkörperfall sind die Ganzheitsringe Dedekindringe, sodass man den Begriff der Verzweigung mit Hilfe der eindeutigen Zerlegung von Idealen in Primideale definieren kann. Um den Fall unendlicher Zahlkörper einzuschließen, verwendet man für beliebige endliche oder unendliche galoissche Erweiterungen stattdessen die äquivalente Formulierung mit Trägheitsgruppen und Zerlegungsgruppen von Bewertungen ([32], II.9). Die oben genannte Beobachtung für $\mathbb{Q}$ ist ein Spezialfall der folgenden Aussage ([46], Lemma 13.3):

Lemma 2.7. *Sei K_∞/K eine $\mathbb{Z}_p$-Erweiterung mit Zwischenkörpern K_n. Dann gibt es eine Zahl n, sodass die Erweiterung $K_\infty \supset K_n$ bei allen verzweigten Fortsetzungen der p-adischen Bewertung von $\mathbb{Q}$ auf den Körper K_∞ voll verzweigt ist.*

Beweis. Seien $T_1, T_2, \dots, T_k$ die Trägheitsgruppen der in K_∞/K verzweigten Bewertungen. Die Gruppe $T = \bigcap_i T_i$ ist als endlicher Durchschnitt abgeschlossener Untergruppen von $\mathrm{Gal}(K_\infty/K)$ eine abgeschlossene Untergruppe, also von der Form $p^n\mathbb{Z}_p = \mathrm{Gal}(K_\infty/K_n)$ für ein

n. Da die Galoisgruppe des zugehörigen Fixkörpers K_n in allen Trägheitsgruppen T_i enthalten ist, ist die Trägheitsgruppe jeder Fortsetzung der p-adischen Bewertung in $\mathrm{Gal}(K_\infty/K_n)$ die ganze Galoisgruppe und diese Bewertungen sind damit voll verzweigt. □

Wir bezeichnen mit μ_n die Gruppe der n-ten Einheitswurzeln und mit μ_{p^∞} die Vereinigung der μ_{p^k}, also die Gruppe der Einheitswurzeln, deren Ordnung eine p-Potenz ist. Der Einfachheit halber werden wir in allen folgenden Abschnitten annehmen, dass p eine ungerade Primzahl ist, und damit die Schwierigkeiten umgehen, die bei $p = 2$ auftreten.

Ein weiterer Vorteil entsteht dadurch, dass wir uns über Verzweigung bei den archimedischen Stellen unserer Körper ab sofort keine Gedanken mehr machen müssen, da niemals Untergruppen oder Quotienten der Galoisgruppen mit Ordnung 2 auftreten. Wir können also vereinbaren, dass mit „unverzweigt“ im Folgenden immer „unverzweigt bei allen endlichen Stellen“ gemeint ist und uns dabei merken, dass die unendlichen Stellen für p-Erweiterungen keine Rolle spielen. Insbesondere werden in einer $\mathbb{Z}_p$-Erweiterung K_∞/K mit K auch alle Zwischenkörper total reell sein.

Definition. Die zyklotomische $\mathbb{Z}_p$-Erweiterung eines Zahlkörpers K ist die eindeutig bestimmte $\mathbb{Z}_p$-Erweiterung von K, die man in der Erweiterung $K(\mu_{p^\infty})/K$ findet.

Diese Teilerweiterung existiert tatsächlich, da $\mathrm{Gal}(K(\mu_{p^\infty})/K)$ zu einer offenen Untergruppe von $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^*$ isomorph ist und da damit der Fixkörper der Torsionsuntergruppe die eindeutige $\mathbb{Z}_p$-Erweiterung K_∞/K liefert.

Falls K die p-ten Einheitswurzeln enthält, bekommt man K_∞ einfach durch Adjunktion aller Einheitswurzeln, deren Ordnung eine p-Potenz ist, denn in diesem Fall ist $K(\mu_{p^\infty})/K$ bereits eine $\mathbb{Z}_p$-Erweiterung.

Satz 2.8. *In einer $\mathbb{Z}_p$-Erweiterung können nur die Stellen verzweigen, die über p liegen.*

Dieser Satz lässt sich elementar mit Hilfe der folgenden Aussage beweisen ([25], Ch. 6, Lemma 1.13):

Lemma 2.9. *Sei K ein Zahlkörper, L eine endliche abelsche galoissche Erweiterung von K und $T = T_\mathfrak{p}$ die Trägheitsgruppe zu einem Primideal $\mathfrak{p} \subset \mathcal{O}_K$, das kein Teiler von $[L : K]$ ist. Dann ist T zyklisch und die Ordnung von T ist ein Teiler von $N\mathfrak{p} - 1$.*

Beweis. Sei $D = D_\mathfrak{p}$ die Zerlegungsgruppe von $\mathfrak{p}$ und $\mathfrak{P}$ eine Ideal in $\mathcal{O}_L$ über $\mathfrak{p}$. Die Restklassenkörper bezeichnen wir mit κ_K und κ_L. Um zu zeigen, dass $|T|$ ein Teiler von $N\mathfrak{p} - 1 = |\kappa_K^*|$ ist, geben wir einen Gruppenhomomorphismus $\varphi : T \to \kappa_L^*$ an und zeigen, dass φ injektiv ist und dass das Bild eine Teilmenge von κ_K ist.

Sei π ein Element aus $\mathfrak{P}\backslash\mathfrak{P}^2$ und L^T der Fixkörper der Trägheitsgruppe, sodass die Erweiterung L/L^T bei $\mathfrak{P}$ voll verzweigt ist. Wie üblich bezeichnet $e(\mathfrak{P}|\mathfrak{p})$ den Verzweigungsindex und $f(\mathfrak{P}|\mathfrak{p})$ den Trägheitsgrad. Mit $\mathfrak{p}' = \mathfrak{P} \cap \mathcal{O}_{L^T}$ gilt also $e(\mathfrak{P}|\mathfrak{p}') = [L : L^T] = [L_\mathfrak{P} : L^T_{\mathfrak{p}'}]$ und $f(\mathfrak{P}|\mathfrak{p}') = 1$. Das Element π erzeugt die Vervollständigung $L_\mathfrak{P}$ über $L^T_{\mathfrak{p}'}$ und wegen der Gleichheit der Erweiterungsgrade gilt auch $L^T(\pi) = L$.

Sei $\tilde{\varphi} : D \to \kappa_L^*$ die durch $\tilde{\varphi}(\sigma) = \frac{\sigma(\pi)}{\pi} \mod \mathfrak{P}$ definierte Abbildung und φ die Einschränkung von $\tilde{\varphi}$ auf T. Seien $\sigma, \tau \in D$ mit $\sigma(\pi) \equiv \alpha\pi \mod \mathfrak{P}^2, \tau(\pi) \equiv \beta\pi \mod \mathfrak{P}^2$. Dann gilt $\sigma\tau(\pi) \equiv \alpha\sigma(\beta)\pi \mod \mathfrak{P}^2$, und damit

$$\tilde{\varphi}(\sigma\tau) = \tilde{\varphi}(\sigma)\overline{\sigma}(\tilde{\varphi}(\tau)),$$

wobei $\overline{\sigma}$ den von σ induzierten Automorphismus des Restklassenkörpers bezeichnet. Insbesondere haben wir $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$ für alle $\sigma, \tau \in T$, die Einschränkung ist also ein Homomorphismus.

Für den Nachweis der Injektivität wählen wir ein Element $\sigma \in \ker(\varphi)$ mit Ordnung m. Per Induktion beweisen wir nun für jedes $k \geq 2$ die Kongruenz $\sigma(\pi) \equiv \pi \mod \mathfrak{P}^k$. Zunächst gilt $\frac{\sigma(\pi)}{\pi} \equiv 1 \mod \mathfrak{P} \Rightarrow \sigma(\pi) \equiv \pi \mod \mathfrak{P}^2$, also die Aussage für $k = 2$. Sei $\sigma(\pi) \equiv \pi \mod \mathfrak{P}^k$ und $a \in \mathcal{O}_L$ mit $\sigma(\pi) \equiv \pi + a\pi^k \mod \mathfrak{P}^{k+1}$. Da $f(\mathfrak{P}|\mathfrak{p}') = 1$, also $\mathcal{O}_L/\mathfrak{P} \cong \mathcal{O}_{L^T}/\mathfrak{p}'$, können wir o.B.d.A. annehmen, dass a im Fixkörper von σ liegt. Dann gilt $\sigma^2(\pi) \equiv \pi + a\pi^k + a\sigma(\pi^k) \mod \mathfrak{P}^{k+1}$, und wiederholtes Anwenden von σ liefert

$$\pi = \sigma^m(\pi) \equiv \pi + a\pi^k + a\sigma(\pi^k) + \cdots + a\sigma^{m-1}(\pi^k) \mod \mathfrak{P}^{k+1}.$$

Da aus $\sigma(\pi) \equiv \pi + a\pi^k \mod \mathfrak{P}^{k+1}$ sofort $\sigma(\pi^k) \equiv \pi^k \mod \mathfrak{P}^{k+1}$ folgt, gilt $\pi \equiv \pi + m \cdot a\pi^k \mod \mathfrak{P}^{k+1}$. Das Element a muss in $\mathfrak{P}$ liegen, denn $\mathfrak{P}$ ist nach Voraussetzung kein Teiler von m. Damit ist

$$\sigma(\pi) \equiv \pi \mod \mathfrak{P}^{k+1}.$$

Da diese Kongruenz für jedes $k \geq 2$ gilt, haben wir $\sigma(\pi) = \pi$, und weil σ nach Voraussetzung außerdem auf L^T trivial operiert, gilt $\sigma = id$.

Als Letztes ist noch zu zeigen, dass das Bild von φ in κ_K liegt, also dass jedes Element $\varphi(\sigma)$ fest bleibt unter der Operation der Galoisgruppe $\mathrm{Gal}(\kappa_L/\kappa_K)$. Die Elemente dieser Galoisgruppe sind von der Form $\overline{\tau}$ mit $\tau \in D$. Da D nach Voraussetzung eine abelsche Gruppe ist, gilt

$$\varphi(\tau\sigma) = \varphi(\sigma\tau) \;\Rightarrow\; \varphi(\tau)\overline{\tau}(\varphi(\sigma)) = \varphi(\sigma)\varphi(\tau) \;\Rightarrow\; \varphi(\sigma) = \overline{\tau}(\varphi(\sigma))$$

und damit $\varphi(\sigma) \in \kappa_K$, da diese Gleichung für alle $\tau \in D$ erfüllt ist. □

Beweis von Satz 2.8 . Sei K_∞/K_0 eine $\mathbb{Z}_p$-Erweiterung mit Zwischenkörpern K_n und $\mathfrak{q}$ ein Primideal in K_0, das in K_∞ verzweigt. Dann ist der Fixkörper der Trägheitsgruppe $T = T_\mathfrak{q}$ einer der Zwischenkörper K_n. In einer Erweiterung K_m/K_n mit $m \geq n$ ist die Trägheitsgruppe jedes Ideals $\mathfrak{Q}$ über $\mathfrak{q}$ die gesamte Galoisgruppe, hat also Ordnung p^{m-n}. Nach dem letzten Lemma ist $\mathfrak{Q}$ ein Primideal über p oder $N\mathfrak{Q} - 1$ ist Vielfaches von p^{m-n} für jedes $m \geq n$. Da der zweite Fall nicht möglich ist, muss $\mathfrak{Q}$ über p liegen. □

Satz 2.10. *Die zyklotomische $\mathbb{Z}_p$-Erweiterung $\mathbb{Q}_\infty/\mathbb{Q}$ ist die maximale abelsche außerhalb von p unverzweigte Pro-p-Erweiterung von $\mathbb{Q}$, also die Vereinigung aller endlichen außerhalb von p unverzweigten p-Erweiterungen von $\mathbb{Q}$.*

Beweis. Wir müssen nach dem letzten Satz nur noch zeigen, dass jede endliche abelsche p-Erweiterung K von $\mathbb{Q}$, in der höchstens die Primstelle p verzweigt, in $\mathbb{Q}(\mu_{p^\infty})$ enthalten ist. Als p-Erweiterung ist sie dann auch in $\mathbb{Q}_\infty$ enthalten.

Nach dem Satz von Kronecker und Weber ist K ein Teilkörper eines Kreisteilungskörpers $\mathbb{Q}(\zeta_n)$. Falls l eine Primzahl ist, ist die Erweiterung $\mathbb{Q}(\zeta_l)/\mathbb{Q}$ nur bei l verzweigt, und damit auch jede nichttriviale Teilerweiterung, da es keine unverzweigten Erweiterungen von $\mathbb{Q}$ gibt. Damit gilt $K \cap \mathbb{Q}(\zeta_l) = \mathbb{Q}$ für $l \neq p$, also kann n als p-Potenz gewählt werden. □

2.4 Pro-endliche Ringe und die Iwasawa-Algebra

Die Iwasawa-Algebra Λ wird zunächst als vollständige Gruppenalgebra einer unendlichen Galoisgruppe definiert; das wichtigste Resultat in diesem Abschnitt wird allerdings sein, dass sie zum Potenzreihenring $\mathbb{Z}_p[\![T]\!]$ isomorph ist. Deshalb benötigen wir einige Aussagen über Potenzreihen mit Koeffizienten in $\mathbb{Z}_p$. Die Resultate aus diesem Abschnitt findet man in [33], Ch. V, §2-3 und [46], Ch. 7 wieder.

Definition. Für einen kommutativen pro-endlichen Ring R und eine pro-endliche Gruppe G definiert man die vollständige Gruppenalgebra $R[\![G]\!]$ als projektiven Limes $\varprojlim R[G/N]$, wobei N die offenen Normalteiler von G durchläuft.

Bemerkung.

1. Die Gruppenalgebra $R[G/N]$ ist als topologischer R-Modul isomorph zu $R^{[G:N]}$. Da die Multiplikation stetig ist, wird $R[G/N]$ ein topologischer Ring.
2. Man kann $R[\![G]\!]$ auch als projektiven Limes $\varprojlim (R/I)[G/N]$ definieren, wobei I dann die offenen Ideale von R durchläuft.

Der Potenzreihenring $\mathbb{Z}_p[\![T]\!]$ in einer Variablen über $\mathbb{Z}_p$ ist der Ring, den man als Vervollständigung von $\mathbb{Z}[T]$ bei dem maximalen Ideal (p, T) erhält, es gilt mit anderen Worten

$$\mathbb{Z}_p[\![T]\!] = \varprojlim \mathbb{Z}[T]/(p,T)^n.$$

Insbesondere ist $\mathbb{Z}_p[\![T]\!]$ mit der (p,T)-adischen Topologie ein kompakter topologischer Ring und als Vervollständigung eines noetherschen Rings bei einem maximalen Ideal wieder noethersch. Die Einheiten in $\mathbb{Z}_p[\![T]\!]$ sind genau die Potenzreihen, deren konstanter Koeffizient eine Einheit in $\mathbb{Z}_p$ ist. Der Ring $\mathbb{Z}_p[\![T]\!]$ ist also noetherscher lokaler Ring mit (p,T) als maximalem Ideal ([9], Thm. 7.1 bzw. Cor. 7.11).

Satz 2.11. *Sei $g = \sum_{i=0}^{\infty} a_i T^i \in \mathbb{Z}_p[\![T]\!] \backslash p\mathbb{Z}_p[\![T]\!]$ und d der kleinste Index, für den a_d nicht durch p teilbar ist. Dann gibt es zu jedem Element $f(T) \in \mathbb{Z}_p[\![T]\!]$ ein eindeutig bestimmtes Polynom $r(T) \in \mathbb{Z}_p[T]$ vom Grad $deg(r) < d$ und ein Element $h(T) \in \mathbb{Z}_p[\![T]\!]$, sodass $f(T) = g(T)h(T) + r(T)$.*

Beweis. Im Quotienten $\mathbb{Z}_p[\![T]\!]/p\mathbb{Z}_p[\![T]\!] \cong \mathbb{F}_p[\![T]\!]$ erzeugt das Bild $\bar{g} = T^d \sum_{i=d}^{\infty} \bar{a}_i T^{i-d}$ von g das Ideal (T^d), sodass sich jede Reihe aus $\mathbb{F}_p[\![T]\!]$ darstellen lässt als $\bar{g}(T)\bar{h}(T) + \bar{r}(T)$ mit einem Polynom $\bar{r}(T)$ vom Grad $deg(r) < d$. Insbesondere können wir also $r_1, h_1 \in \mathbb{Z}_p[\![T]\!]$ so wählen, dass $\bar{f}(T) = \bar{g}(T)\bar{h}_1(T) + \bar{r}_1(T)$ in $\mathbb{F}_p[\![T]\!]$. In $\mathbb{Z}_p[\![T]\!]$ findet man dann ein Element $f_1(T)$ mit $f(T) = g(T)h_1(T) + r_1(T) + pf_1(T)$. Anwenden desselben Arguments auf f_1 liefert Elemente $f_1', h_1', f_2 \in \mathbb{Z}_p[\![T]\!]$ mit $f_1(T) = g(T)h_1'(T) + r_1'(T) + pf_2(T)$, sodass

$$\begin{aligned} f(T) &= g(T)(h_1(T) + ph_1'(T)) + (r_1(T) + pr_1'(T)) + p^2 f_2(T) \\ &= g(T)h_2(T) + r_2(T) + p^2 f_2(T). \end{aligned}$$

Induktiv erhält man für jedes n eine Gleichung

$$f(T) = g(T)h_n(T) + r_n(T) + p^n f_n(T)$$

mit Polynomen r_n vom Grad kleiner als d und

$$h_{n+1}(T) \equiv h_n(T) \mod p^n\mathbb{Z}_p[\![T]\!], \quad r_{n+1}(T) \equiv r_n(T) \mod p^n\mathbb{Z}_p[T].$$

Für jeden Koeffizienten existiert der Grenzwert in $\mathbb{Z}_p$. Damit hat die Folge $h_n(T)$ einen Grenzwert $h(T)$ in $\mathbb{Z}_p[\![T]\!]$ und als Grenzwert von $r_n(T)$ erhält man ein Polynom $r(T)$, dessen Grad höchstens d ist.

Für den Beweis der Eindeutigkeit nehmen wir an, $f(T) = g(T)h'(T) + r'(T)$ sei eine weitere Darstellung von dieser Form, sodass $r(T) \neq r'(T)$. Sei $r(T) - r'(T) = p^k s(T)$ mit einem Polynom $s(T)$, das nicht durch p teilbar ist. Da p prim ist, folgt aus $r(T) - r'(T) = g(T)(h'(T) - h(T))$, dass $s(T)$ Vielfaches von $g(T)$ ist. In dem Quotienten $\mathbb{Z}_p[\![T]\!]/p\mathbb{Z}_p[\![T]\!]$ ist $s(T) \neq 0$ ein Polynom mit Grad höchstens $d-1$, und die ersten d Koeffizienten von g sind 0. Das ist ein Widerspruch. $\square$

Definition. Ein normiertes Polynom $T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in \mathbb{Z}_p[T]$, dessen Koeffizienten $a_0, \ldots, a_{n-1}$ im maximalen Ideal (p) von $\mathbb{Z}_p$ liegen, nennen wir Weierstraß-Polynom.

Korollar 2.12 (p-adischer Weierstraß'scher Vorbereitungssatz). *Jedes Element $g(T)$ aus $\mathbb{Z}_p[\![T]\!]\backslash p\mathbb{Z}_p[\![T]\!]$ lässt sich eindeutig als Produkt eines Weierstraß-Polynoms und einer Einheit aus $\mathbb{Z}_p[\![T]\!]$ schreiben. Der Grad des Polynoms ist der kleinste Index d, für den der Koeffizient von T^d in der Potenzreihe $g(T)$ nicht durch p teilbar ist.*

Beweis. Aus der Eindeutigkeit des Polynoms $r(T)$ in Satz 2.11 folgt, dass die Abbildung

$$\begin{array}{rccc} \varphi: & \mathbb{Z}_p[\![T]\!]/(g(T)) & \to & \mathbb{Z}_p[\![T]\!]/(T^d) \\ & f(T) + (g(T)) & \mapsto & r(T) \end{array}$$

ein Isomorphismus von $\mathbb{Z}_p$-Moduln ist. Damit ist $\mathbb{Z}_p[\![T]\!]/(g(T))$ als $\mathbb{Z}_p$-Modul isomorph zu $\mathbb{Z}_p^d$. Das Element T definiert eine lineare Abbildung $\mathbb{Z}_p[\![T]\!]/(g(T)) \to \mathbb{Z}_p[\![T]\!]/(g(T))$, deren charakteristisches Polynom $\chi(T)$, aufgefasst als Homomorphismus auf dem Modul, nach Cayley-Hamilton die Nullabbildung ist. Da $\chi(T)$ ein normiertes Polynom vom Grad d ist, haben wir wie oben einen Isomorphismus $\mathbb{Z}_p[\![T]\!]/(\chi(T)) \to \mathbb{Z}_p[\![T]\!]/(T^c)$, wobei $c \leq d$ der kleinste Index ist, sodass der dazugehörige Koeffizient von $\chi(T)$ nicht in (p) liegt.

Andererseits faktorisiert die Projektionsabbildung $\mathbb{Z}_p[\![T]\!] \to \mathbb{Z}_p[\![T]\!]/(g(T))$ über den Quotienten $\mathbb{Z}_p[\![T]\!]/(\chi(T))$, und damit gilt $d \leq c$. Die Abbildung zwischen $\mathbb{Z}_p[\![T]\!]/(\chi(T))$ und $\mathbb{Z}_p[\![T]\!]/(g(T))$ ist also ein Isomorphismus, das heißt, dass die Ideale $(\chi(T))$ und $(g(T))$ gleich sind, und wegen $c = d$ hat das Polynom $\chi(T)$ die gewünschte Form. Die Eindeutigkeit des Polynoms folgt sofort aus Satz 2.11 mit $f(T) = 0$. $\square$

Aus dem Vorbereitungssatz kann man insbesondere sehen, dass $\mathbb{Z}_p[\![T]\!]$ ein faktorieller Ring ist. Eine weitere Beobachtung, die sich sofort ergibt, ist das folgende Lemma:

Lemma 2.13. *Für jedes Element $f \in \mathbb{Z}_p[\![T]\!]$, das keine Einheit ist, hat der Quotient $\mathbb{Z}_p[\![T]\!]/(f)$ unendlich viele Elemente.*

Beweis. Falls f Vielfaches von p ist, ist $\mathbb{Z}_p[\![T]\!]/(p) = \mathbb{F}_p[\![T]\!]$ ein Quotient von $\mathbb{Z}_p[\![T]\!]/(f)$, und damit ist dieser unendlich. Falls $f \notin (p)$, können wir annehmen, dass f ein Weierstraß-Polynom vom Grad $d \leq 1$ ist, und in diesem Fall gilt $\mathbb{Z}_p[\![T]\!]/(f) \cong \mathbb{Z}_p^d$. $\square$

Lemma 2.14. *Für jedes Weierstraß-Polynom $h(T) \in \mathbb{Z}_p[T]$ ist die kanonische Abbildung*

$$\mathbb{Z}_p[T]/(h(T)) \to \mathbb{Z}_p[\![T]\!]/(h(T))$$

ein Isomorphismus.

Beweis. Die Abbildung ist offenbar injektiv. Sie ist surjektiv, denn nach Satz 2.11 lässt sich jedes Element $f(T) \in \mathbb{Z}_p[\![T]\!]$ schreiben als $f(T) = \alpha(T)h(T) + r(T)$ mit einem Element $\alpha(T) \in \mathbb{Z}_p[\![T]\!]$ und einem Polynom $r(T)$. $\square$

Lemma 2.15. *Sei $h_n(T) = (1+T)^{p^n} - 1$. Dann gilt $\mathbb{Z}_p[\![T]\!] \cong \varprojlim \mathbb{Z}_p[\![T]\!]/(h_n(T))$.*

Beweis. Da $h_{n+1}(T)$ jeweils das Produkt von $h_n(T)$ und dem Element $((1+T)^{p^n(p-1)} + \cdots + (1+T)^{p^n} + 1) \in (p,T)$ ist, sieht man induktiv, dass $h_n(T) \in (p,T)^n$ für jedes n. Damit ist die kanonische Abbildung $\varphi : \mathbb{Z}_p[\![T]\!] \to \varprojlim \mathbb{Z}_p[\![T]\!]/(h_n(T))$ wegen $\bigcap(h_n(T)) \subset \bigcap(p,T)^n = 0$ injektiv.

Sei $(f_n) \in \varprojlim \mathbb{Z}_p[\![T]\!]/(h_n(T))$ beliebig. Dann gilt $f_n \equiv f_m \mod (h_n(T))$ für $n < m$. Der Grenzwert $f = \lim_{n\to\infty} f_n$ existiert in $\mathbb{Z}_p[\![T]\!]$, denn $(h_n(T)) \subset (p,T)^n$ und $\mathbb{Z}_p[\![T]\!]$ ist vollständig in der (p,T)-adischen Topologie. Da φ den Grenzwert f auf (f_n) abbildet, ist die Abbildung surjektiv.

Als stetiger Homomorphismus zwischen kompakten Mengen ist φ ein Isomorphismus. $\square$

Bemerkung. Die Quotiententopologie auf $\mathbb{Z}_p[\![T]\!]/(h_n(T))$ stimmt mit der Produkttopologie überein, die man erhält, wenn man $\mathbb{Z}_p[\![T]\!]/(h_n(T))$ mit $\mathbb{Z}_p^{p^n}$ identifiziert.

Sei K_∞/K_0 eine $\mathbb{Z}_p$-Erweiterung des Zahlkörpers K_0 mit (multiplikativ geschriebener) Galoisgruppe $\Gamma = \mathrm{Gal}(K_\infty/K_0)$ und Zwischenkörpern K_n, die man als Fixkörper der abgeschlossenen Untergruppen $\Gamma^{p^n} = \{\alpha^{p^n} | \alpha \in \Gamma\}$ erhält. Die Galoisgruppe der Teilerweiterung K_n/K_0 bezeichnen wir mit Γ_n.

Definition. Die Iwasawa-Algebra Λ ist die vollständige Gruppenalgebra der Gruppe Γ mit Koeffizienten in $\mathbb{Z}_p$:

$$\Lambda = \mathbb{Z}_p[\![\Gamma]\!] = \varprojlim \mathbb{Z}_p[\Gamma_n].$$

Satz 2.16. *Sei γ ein topologischer Erzeuger von $\Gamma = \varprojlim \Gamma_n$. Dann ist die Abbildung*

$$\begin{array}{rcl} \mathbb{Z}_p[\![\Gamma]\!] & \to & \mathbb{Z}_p[\![T]\!], \\ \gamma & \mapsto & T+1, \end{array}$$

ein Isomorphismus topologischer Ringe.

Beweis. Als zyklische Gruppe der Ordnung p^n hat Γ_n die Präsentation $\langle \gamma | \gamma^{p^n} = 1 \rangle$. Die Abbildung

$$\mathbb{Z}_p[\Gamma_n] \to \mathbb{Z}_p[U]/(U^{p^n} - 1),$$
$$\gamma \mapsto U$$

ist offenbar ein Isomorphismus. Setzen wir $T = U - 1$, $h_n(T) = (1+T)^{p^n} - 1$, so ist h_n ein Weierstraß-Polynom, es gilt $\mathbb{Z}_p[U]/(U^{p^n} - 1) \cong \mathbb{Z}_p[T]/(h_n(T))$ und das Diagramm

$$\begin{array}{ccc} \mathbb{Z}_p[\Gamma_n] & \longrightarrow & \mathbb{Z}_p[T]/(h_n(T)) \\ \downarrow & & \downarrow \\ \mathbb{Z}_p[\Gamma_{n-1}] & \longrightarrow & \mathbb{Z}_p[T]/(h_{n-1}(T)) \end{array}$$

ist kommutativ. Aus Lemma 2.14 folgt $\varprojlim \mathbb{Z}_p[T]/(h_n(T)) \cong \varprojlim \mathbb{Z}_p[\![T]\!]/(h_n(T))$ und damit aus

$$\varprojlim \mathbb{Z}_p[\Gamma_n] \cong \varprojlim \mathbb{Z}_p[T]/(h_n(T)) \cong \varprojlim \mathbb{Z}_p[\![T]\!]/(h_n(T)) \cong \mathbb{Z}_p[\![T]\!]$$

die Behauptung. $\square$

Bemerkung. 1. Der Isomorphismus $\Lambda \to \mathbb{Z}_p[\![T]\!]$ ist nicht eindeutig, da er von der Wahl eines Erzeugers von Γ abhängt. Nützlich ist die Isomorphie vor allem, weil die Struktur von $\mathbb{Z}_p[\![T]\!]$-Moduln mit Hilfe von Polynomen und Potenzreihen untersucht werden kann.

2. Ein endlich erzeugter Λ-Modul M kann nur auf eine Weise zu einem topologischen Modul gemacht werden. Die Topologie, die man durch die 0-Umgebungen $(p, T)^n \cdot M$ auf M erhält, stimmt also immer mit der gegebenen Topologie überein. Außerdem sind alle Λ-Homomorphismen zwischen endlich erzeugten Moduln stetig ([33], Prop. 5.2.22). Solange wir also mit endlich erzeugten Moduln arbeiten, spielt es keine Rolle, ob wir Λ-Moduln oder topologische Λ-Moduln betrachten.

2.5 Galoisgruppen als Moduln über der Iwasawa-Algebra

Wir betrachten in den folgenden Abschnitten eine (zunächst beliebige) $\mathbb{Z}_p$-Erweiterung K_∞/K_0 eines Zahlkörpers K_0 mit Zwischenkörpern K_n. Um Regelmäßigkeiten im Verhalten der Klassengruppen dieser Körper untersuchen zu können, betrachtet man als Hilfsmittel die Galoisgruppe der maximalen abelschen unverzweigten p-Erweiterung von K_∞. Diese Gruppe wird ein Modul über der Iwasawa-Algebra, dessen Eigenschaften später bei der Untersuchung eines größeren Moduls nützlich sein werden.

Lemma 2.17. *Sei F eine endliche unverzweigte Erweiterung von K_∞. Dann gibt es eine Zahl n und eine endliche unverzweigte Erweiterung F_n/K_n, sodass $F = F_n K_\infty$.*

Beweis. Wir können eine endliche Erweiterung F_0 von K_0 wählen, sodass $F = F_0 K_\infty$. Sei $F_n = F_0 K_n$, sodass F die Vereinigung aller F_n ist und $F = F_n K_\infty$ für jedes n. Außerdem setzen wir

$$\begin{aligned} G_n &= \mathrm{Gal}(F/K_n), \quad G = \bigcap_{n=0}^{\infty} G_n = \mathrm{Gal}(F/K_\infty) \quad \text{und} \\ H_n &= \mathrm{Gal}(F/F_n). \end{aligned}$$

Die Gruppen G_n und H_n sind offene Untergruppen von $\mathrm{Gal}(F/K_0)$, und es gilt $G \cap H_n = \{1\}$.

Sei v eine Bewertung von K_0, die in der Erweiterung F_0/K_0 verzweigt, und T die Trägheitsgruppe einer Fortsetzung in $\mathrm{Gal}(F/K_0)$. Die Trägheitsgruppen der verschiedenen Fortsetzungen von v erhält man dann aus T durch Konjugation mit Elementen aus $\mathrm{Gal}(F/K_0)$. Da F/K_∞ als unverzweigt vorausgesetzt wurde, gilt $\sigma T \sigma^{-1} \cap G = \{1\}$ für alle $\sigma \in \mathrm{Gal}(F/K_0)$.

Es gilt $\bigcap (G_n \backslash H_n) = G \backslash \{1\}$, also

$$\bigcap_n (\sigma T \sigma^{-1} \cap (G_n \backslash H_n)) = \sigma T \sigma^{-1} \cap (G \backslash \{1\}) = \varnothing.$$

Wegen der Kompaktheit von $\mathrm{Gal}(F/K_0)$ gibt es einen Index n, ab dem $\sigma T \sigma^{-1} \cap (G_n \backslash H_n) = \varnothing$ und damit $\sigma T \sigma^{-1} \cap G_n \subset H_n$. Für alle Elemente $\tau \in H_n$ gilt dann ebenfalls $(\tau\sigma) T (\tau\sigma)^{-1} \cap G_n \subset H_n$. Jedes Element $\sigma \in \mathrm{Gal}(F/K_0)$ hat also eine offene Umgebung $H_n \sigma$, sodass für alle Elemente ρ aus $H_n \sigma$ derselbe Index n gewählt werden kann. Die Kompaktheit von $\mathrm{Gal}(F/K_0)$ impliziert dann, dass ein Index n_0 für alle σ gewählt werden kann. Das bedeutet, dass F_{n_0}/K_{n_0} bei allen Fortsetzungen von v unverzweigt ist. Da nur endlich viele Bewertungen von K_0 in F_0 verzweigen können, gibt es einen Index n_1, ab dem die Erweiterungen F_n/K_n bei allen darüberliegenden Stellen unverzweigt sind und damit dann bei allen Stellen. $\square$

Satz 2.18. *Für jedes n sei L_n die maximale abelsche unverzweigte p-Erweiterung von K_n. Dann ist die Vereinigung $L = \bigcup L_n$ die maximale abelsche unverzweigte p-Erweiterung von K_∞, und die Galoisgruppe der Erweiterung L/K_∞ ist als topologische Gruppe kanonisch isomorph zu $\varprojlim \operatorname{Gal}(L_n/K_n)$.*

Beweis. Für die erste Behauptung zeigen wir, dass sich jede endliche galoissche abelsche unverzweigte Erweiterung F/K_∞ durch Hochheben einer endlichen galoisschen abelschen unverzweigten Erweiterung eines der Zwischenkörper K_n ergibt, also dass es eine solche Erweiterung F_n von K_n gibt mit $F = F_n K_\infty$.

Sei F_0 zunächst irgendeine endliche Erweiterung von K_0 mit $K_\infty F_0 = F$. Nach Übergang zum normalen Abschluss können wir annehmen, dass die Erweiterung F_0/K_0 galoissch ist. Der Körper $K_\infty \cap F_0$ ist ein Zwischenkörper der Erweiterung K_∞/K_0, also von der Form K_n für ein $n \in \mathbb{N}_0$, und für dieses n gilt $\operatorname{Gal}(F_0/K_n) \cong \operatorname{Gal}(F/K_\infty)$. Die Erweiterung F_0/K_n ist damit abelsch, und die Erweiterung F/K_∞ ergibt sich durch Hochheben dieser Erweiterung. Nach Lemma 2.17 kann man n so groß wählen, dass F_0K_n/K_n unverzweigt ist.

Für die zweite Behauptung stellen wir zunächst fest, dass

$$\operatorname{Gal}(L/K_\infty) = \varprojlim \operatorname{Gal}(L_nK_\infty/K_\infty),$$

da $\bigcup_n L_n$ auch als Vereinigung $\bigcup_n L_nK_\infty$ geschrieben werden kann. Die Erweiterung $L_n \supset K_n$ ist unverzweigt für alle n, und wir können $N \in \mathbb{N}$ so groß wählen, dass die Erweiterung $K_\infty \supset K_n$ voll verzweigt ist, falls $n \geq N$. Dann gilt $L_n \cap K_\infty = K_n$ für $n \geq N$, also ist die Restriktionsabbildung $\operatorname{Gal}(L_nK_\infty/K_\infty) \to \operatorname{Gal}(L_n/K_n)$ ein Isomorphismus. Daraus folgt

$$\operatorname{Gal}(L/K_\infty) \cong \varprojlim \operatorname{Gal}(L_nK_\infty/K_\infty) \cong \varprojlim \operatorname{Gal}(L_n/K_n)$$

als topologische Gruppen. □

Die maximale abelsche unverzweigte p-Erweiterung X

Sei X_n die p-Klassengruppe von K_n, also der maximale p-Quotient der Idealklassengruppe von K_n. Als abelsche p-Gruppe ist X_n in kanonischer Weise ein $\mathbb{Z}_p$-Modul. Nach Klassenkörpertheorie gilt $X_n \cong \operatorname{Gal}(L_n/K_n)$, und die Abbildungen $\operatorname{Norm}_{L_n/K_n} : X_n \to X_{n-1}$ aus Abschnitt 2.1 werden durch diesen Isomorphismus mit den Restriktionsabbildungen auf den Galoisgruppen identifiziert.

Die Galoisgruppe $\Gamma_n = \operatorname{Gal}(K_n/K_0)$ operiert einerseits auf der Idealklassengruppe von K_n und dadurch auch auf X_n, andererseits durch Konjugation auf $\operatorname{Gal}(L_n/K_n)$. Dass sich diese Operationen identifizieren lassen, haben wir uns ebenfalls schon in Abschnitt 2.1 überlegt und erhalten deshalb eine eindeutige $\mathbb{Z}_p[\Gamma_n]$-Modulstruktur auf X_n. Sei

$$X = \operatorname{Gal}(L/K_\infty) = \varprojlim \operatorname{Gal}(L_n/K_n)$$

die Galoisgruppe der maximalen abelschen unverzweigten p-Erweiterung von K_∞. Das folgende Diagramm fasst die Situation noch einmal zusammen:

$$
\begin{tikzcd}
 & L \arrow[dd, dash] \\
K_\infty \arrow[ur, dash, "X"] \arrow[dd, dash] \arrow[ddd, dash, bend right, "\Gamma"'] & \\
 & L_n \\
K_n \arrow[ur, dash, "X_n"'] \arrow[d, dash, "\Gamma_n"] & \\
K_0 &
\end{tikzcd}
$$

Lemma 2.19. *Die $\mathbb{Z}_p[\Gamma_n]$-Modulstrukturen auf X_n induzieren eine Λ-Modulstruktur auf X, die diese Gruppe zu einem kompakten topologischen Λ-Modul macht.*

Beweis. Seien $(\tau_n) \in \varprojlim \Gamma_n$ und $(\sigma_n) \in \varprojlim X_n$ mit Elementen $\tau_n \in \mathrm{Gal}(K_n/K_0)$ und $\sigma_n \in \mathrm{Gal}(L_n/K_n)$. Die Operation von τ_n auf $\mathrm{Gal}(L_n/K_n)$ ist durch Konjugation mit einer Hochhebung $\tilde{\tau}_n$ in $\mathrm{Gal}(L_n/K_0)$ gegeben, und es gilt

$$\tilde{\tau}_n \sigma_n \tilde{\tau}_n^{-1}|_{L_{n-1}} = \tilde{\tau}_{n-1} \sigma_{n-1} \tilde{\tau}_{n-1}^{-1},$$

da $\tilde{\tau}_n|_{L_{n-1}}$ eine Hochhebung von $\tau_{n-1} = \tau_n|_{K_{n-1}}$ ist.

Also liegt $(\tau_n) \circ (\sigma_n) = (\tilde{\tau}_n \sigma_n \tilde{\tau}_n^{-1}) \in \prod_n X_n$ wieder in $\varprojlim X_n$, und damit wird X zu einem Λ-Modul. Die Operation ist als Einschränkung der stetigen Operation $\prod_n \Gamma_n \times \prod_n X_n \to \prod_n X_n$ auf den Teilraum $\varprojlim \Gamma_n \times \varprojlim X_n$ ebenfalls stetig. Als Galoisgruppe der maximalen abelschen unverzweigten Erweiterung von K_∞ ist X hausdorffsch und kompakt, also kompakter topologischer Λ-Modul. $\square$

Im restlichen Teil des Abschnitts folgen wir der Darstellung von Washington ([46], §13.3) und gehen zunächst von einer einfacheren Situation aus, die zum Beispiel für die zyklotomische $\mathbb{Z}_p$-Erweiterung $\mathbb{Q}_\infty/\mathbb{Q}$ vorliegt:

Annahme. *Alle in K_∞/K_0 verzweigten Stellen sind voll verzweigt.*

Dieser Fall lässt sich leichter behandeln und später auf den allgemeinen Fall anwenden, indem man K_0 durch einen Zwischenkörper K_n ersetzt, sodass die Annahme für K_∞/K_n gilt.

Lemma 2.20. *Sei γ ein Erzeuger von $\Gamma = \mathrm{Gal}(K_\infty/K_0)$. Dann ist der Abschluss der Kommutatoruntergruppe von $\mathrm{Gal}(L/K_0)$ durch $(\gamma - 1)X$ gegeben.*

Beweis. Sei v eine Bewertung von K_0, die in K_∞ voll verzweigt ist, und $T = T_v(K_\infty/K_0)$ die zugehörige Trägheitsgruppe in $\mathrm{Gal}(L/K_0)$. Dann wird T unter der Restriktionsabbildung $\mathrm{Gal}(L/K_0) \to \mathrm{Gal}(K_\infty/K_0)$ bijektiv auf $\Gamma = \mathrm{Gal}(K_\infty/K_0)$ abgebildet. Sei $[a, b] = aba^{-1}b^{-1}$ mit $a, b \in \mathrm{Gal}(L/K_0)$ ein Erzeuger der Kommutatoruntergruppe. Da $\mathrm{Gal}(L/K_0)$ semidirektes Produkt der Gruppen Γ und X ist, gibt es Elemente $\alpha, \beta \in T$ und $x, y \in X$ mit $a = \alpha x, b = \beta y$.

Wir schreiben „$\circ$“ für die Operation von Γ auf X und „$\cdot$“ für die Verknüpfung in der abelschen Gruppe X. Es gilt

$$\begin{aligned}
aba^{-1}b^{-1} &= \alpha x\beta y x^{-1}\alpha^{-1}y^{-1}\beta^{-1} \\
&= \alpha x\alpha^{-1}\alpha\beta y x^{-1}\alpha^{-1}y^{-1}\beta^{-1} \\
&= \alpha x\alpha^{-1}\alpha\beta y x^{-1}(\alpha\beta)^{-1}\alpha\beta\alpha^{-1}y^{-1}\beta^{-1} \\
&= \alpha x\alpha^{-1}\alpha\beta x^{-1}y(\alpha\beta)^{-1}\beta y^{-1}\beta^{-1} \\
&= (\alpha x\alpha^{-1})\cdot(\alpha\beta x^{-1}(\alpha\beta)^{-1})\cdot(\alpha\beta y(\alpha\beta)^{-1})\cdot(\beta y^{-1}\beta^{-1}) \\
&= (\alpha x\alpha^{-1})\cdot(\beta(\alpha x^{-1}\alpha^{-1})\beta^{-1})\cdot(\alpha(\beta y\beta^{-1})\alpha^{-1})\cdot(\beta y^{-1}\beta^{-1}) \\
&= (1-\beta)\circ(\alpha x^{-1}\alpha^{-1})\cdot(\alpha-1)\circ(\beta y\beta^{-1}).
\end{aligned}$$

Dabei identifizieren wir die Elemente α und β mit den entsprechenden Elementen aus Γ. Wegen $1-\beta \in (\gamma-1)$ und $\alpha - 1 \in (\gamma-1)$ gilt $aba^{-1}b^{-1} \in (\gamma-1)X$. Damit ist gezeigt, dass die Kommutatoruntergruppe in $(\gamma-1)X$ enthalten ist. Da die Menge $(\gamma-1)X$ als stetiges Bild der kompakten Menge X abgeschlossen ist, enthält sie auch den Abschluss der Kommutatoruntergruppe.

Umgekehrt: Für ein beliebiges Element $y \in X$ gilt

$$(1-\gamma)\circ y = y\cdot(\gamma y\gamma^{-1})^{-1} = (\gamma\circ 1)\cdot(1\circ y)\cdot(\gamma\circ 1)^{-1}\cdot(1\circ y)^{-1},$$

also ist der Untermodul $(\gamma-1)X$ in der Kommutatoruntergruppe von $\mathrm{Gal}(L/K_0)$ enthalten. $\square$

Seien $v_1,\dots,v_s$ die Bewertungen von K_0, die in K_∞ verzweigt sind, und $T_1,\dots,T_s$ die zugehörigen Trägheitsgruppen in $\mathrm{Gal}(L/K_0)$. Nach unserer Annahme ist die Zusammensetzung $T_i \hookrightarrow \mathrm{Gal}(L/K_0) \to \Gamma$ für alle i bijektiv und $T_i \cap X = \{id\}$. Sei σ_i das Urbild des Erzeugers γ in T_i und a_i für $i \geq 2$ das eindeutig bestimmte Element aus X mit $\sigma_i = a_i\sigma_1$.

Lemma 2.21. *Sei Y_0 der $\mathbb{Z}_p$-Untermodul von X, der von $(\gamma-1)X$ und den Elementen $a_2, a_3, \dots, a_s$ erzeugt wird, und für jedes $n \in \mathbb{N}$ sei $Y_n = (1+\gamma+\dots+\gamma^{p^n-1})Y_0$. Dann gilt $X_n = X/Y_n$ für jedes n.*

Beweis. Zunächst zeigen wir die Aussage für $n = 0$. Die Gruppe $X_0 = \mathrm{Gal}(L_0/K_0)$ ist die Galoisgruppe der größten abelschen unverzweigten p-Erweiterung von K_0. Da L eine p-Erweiterung ist, die L_0 enthält, ist L_0 die größte abelsche unverzweigte in L enthaltene Erweiterung von K_0. Die Galoisgruppe X_0 ist damit der Quotient von $\mathrm{Gal}(L/K_0)$ und der abgeschlossenen Untergruppe, die von der Kommutatoruntergruppe von $\mathrm{Gal}(L/K_0)$ und den Trägheitsgruppen T_i erzeugt wird. Also gilt

$$X_0 = \mathrm{Gal}(L/K_0)/\mathrm{Gal}(L/L_0) = XT_1/\overline{\langle(\gamma-1)X, T_1, a_2,\dots,a_s\rangle} = X/\overline{\langle(\gamma-1)X, a_2,\dots,a_s\rangle}.$$

Für $n \geq 1$ ist $\mathrm{Gal}(K_\infty/K_n) = \Gamma^{p^n} \cong \mathbb{Z}_p$, und die Trägheitsgruppen $\tilde{T}_i$ der verzweigten Bewertungen erhält man als Schnitt von T_i und $\mathrm{Gal}(L/K_n)$, also werden sie von den Elementen $\sigma_i^{p^n}$ erzeugt. Die Abbildung $\tilde{T}_i \to \mathrm{Gal}(L/K_n)/\mathrm{Gal}(L/K_\infty) = \Gamma^{p^n}$ ist für jedes i ein Isomorphismus, und $T_i = \langle\sigma_i^{p^n}\rangle = \langle(a_i\sigma_1)^{p^n}\rangle$. Das Element $(a_i\sigma_1)^{p^n}$ lässt sich schreiben als

$$(a_i\sigma_1)^{p^n} = a_i(\sigma_1 a_i\sigma_1^{-1})(\sigma_1^2 a_i\sigma_1^{-2})\cdots(\sigma_1^{p^n-1}a_i\sigma_1^{-p^n-1})\sigma_1^{p^n} = ((1+\gamma+\dots+\gamma^{p^n-1})\circ a_i)\sigma_1^{p^n}.$$

Damit wird die Galoisgruppe $\operatorname{Gal}(L/L_n)$ erzeugt von $\tilde{T}_1$, den Elementen $\sigma_i^{p^n} = ((1+\gamma+\cdots+\gamma^{p^n-1})\circ a_i)\sigma_1^{p^n}$ und der Kommutatoruntergruppe $(\gamma^{p^n}-1)X = (1+\gamma+\cdots+\gamma^{p^n-1})(1-\gamma)X$ von $\operatorname{Gal}(L/K)$. Wie im ersten Teil folgt jetzt

$$\begin{aligned} X_n &= \operatorname{Gal}(L/K_n)/\operatorname{Gal}(L/L_n) \\ &= X\tilde{T}_1/\overline{\langle(\gamma^{p^n}-1)X, \tilde{T}_1, (1+\gamma+\cdots+\gamma^{p^n-1})a_2, \ldots, (1+\gamma+\cdots+\gamma^{p^n-1})a_s\rangle} \\ &= X/\overline{\langle(\gamma^{p^n}-1)X, (1+\gamma+\cdots+\gamma^{p^n-1})a_2, \ldots, (1+\gamma+\cdots+\gamma^{p^n-1})a_s\rangle} \\ &= X/(1+\gamma+\cdots+\gamma^{p^n-1})Y_0 = X/Y_n. \end{aligned}$$

□

Für den **allgemeinen Fall**, dass die Erweiterung K_∞/K_0 nicht bei allen Stellen voll verzweigt ist, wählen wir mit Hilfe von Lemma 2.7 eine Zahl $e \geq 0$, sodass unsere Voraussetzung für K_∞/K_e gilt. Das Bild der Trägheitsgruppe $\tilde{T}_i$ einer voll verzweigten Bewertung unter der Restriktionsabbildung $\operatorname{Gal}(L/K_e) \to \operatorname{Gal}(K_\infty/K_e) = \Gamma^{p^e}$ ist dann wieder die ganze Gruppe. Ähnlich wie oben bezeichnen wir mit $\tilde{\sigma}_i$ das Urbild des Erzeugers γ^{p^e} von Γ^{p^e} und mit $\tilde{a}_i$ die entsprechenden Elemente aus X mit $\tilde{\sigma}_i = \tilde{a}_i\tilde{\sigma}_1$.

Betrachtet man also statt der Erweiterung K_∞/K_0 die Erweiterung K_∞/K_e, so hat das Lemma die folgende Form:

Lemma 2.22. *Sei Y_e der $\mathbb{Z}_p$-Untermodul von X, der von $(\gamma^{p^e}-1)X$ und den Elementen $\tilde{a}_2, \ldots, \tilde{a}_s$ erzeugt wird, und für $n \geq e$ sei $Y_n = (1+\gamma^{p^e}+\gamma^{2p^e}+\cdots+\gamma^{p^n-p^e})Y_e$. Dann gilt $X_n = X/Y_n$ für alle $n \geq e$.*

Satz 2.23 (Topologisches Nakayama-Lemma). *Sei R ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, der kompakt ist bezüglich der $\mathfrak{m}$-adischen Topologie. Ist M ein kompakter topologischer R-Modul, für den der Quotient $M/\mathfrak{m}M$ endliche Gruppe ist, so ist M als R-Modul endlich erzeugt.*

Beweis. Sei U eine beliebige Nullumgebung in M. Da die Abbildung $R \times M \to M$ stetig ist, gibt es zu jedem $z \in M$ eine Potenz $\mathfrak{m}^n$ des maximalen Ideals und eine Umgebung U_z von z mit $\mathfrak{m}^n U_z \subset U$. Aus der Kompaktheit von M folgt, dass eine Zahl $n \in \mathbb{N}$ existiert mit $\mathfrak{m}^n M \subset U$. Da U beliebig gewählt werden kann, folgt daraus, dass $\bigcap_n \mathfrak{m}^n M = \{0\}$.

Seien nun $x_1, \ldots, x_n$ endlich viele Elemente aus M, deren Bilder den $\mathbb{Z}$-Modul $M/\mathfrak{m}M$ erzeugen, und N der von $x_1, \ldots, x_n$ erzeugte R-Modul. Die Abbildung $R^n \to X$, die ein Tupel $(r_1, \ldots, r_n)$ auf das Element $r_1x_1 + \cdots + r_nx_n$ abbildet, ist stetig, und N als Bild einer kompakten Menge kompakt und damit abgeschlossen. Der Quotient M/N ist kompakter R-Modul. Nach Voraussetzung ist $M = N + \mathfrak{m}M$, also $\mathfrak{m}(M/N) = (\mathfrak{m}M + N)/N = (M/N)$ und damit auch $\mathfrak{m}^n(M/N) = (M/N)$ für alle n. Aus der Beobachtung oben, angewandt auf den kompakten Modul M/N, folgt $M/N = 0$, also ist $M = N$ ein endlich erzeugter R-Modul. □

Korollar 2.24. *Falls M ein kompakter topologischer $\mathbb{Z}_p[\![T]\!]$-Modul ist, für den der Quotient M/TM als $\mathbb{Z}_p$-Modul von endlich vielen Elementen erzeugt wird, ist M ein endlich erzeugter $\mathbb{Z}_p[\![T]\!]$-Modul.*

Beweis. $M/(p,T)M$ ist Quotient von M/TM nach (p) und damit als endlich erzeugter $\mathbb{F}_p$-Vektorraum endlich. Die Aussage folgt jetzt aus dem Satz. □

Satz 2.25. *Die Galoisgruppe X der maximalen abelschen unverzweigten p-Erweiterung von K_∞ ist ein endlich erzeugter Λ-Modul.*

Beweis. Sei $\mathfrak{m} = (p, T) = (p, \gamma - 1)$ das maximale Ideal der Iwasawa-Algebra Λ. Da der Quotient $X_e = X/Y_e$ als p-Klassengruppe von K_e endlich ist und das Element $1+\gamma^{p^e}+\gamma^{2p^e}+\cdots+\gamma^{p^{e+1}-p^e}$ in $\mathfrak{m}$ liegt, genügt es nach Nakayama, zu zeigen, dass $Y_e/(1+\gamma^{p^e}+\cdots+\gamma^{p^{e+1}-p^e})Y_e$ eine endliche Gruppe ist. Das folgt aus

$$Y_e/(1+\gamma^{p^e}+\cdots+\gamma^{p^{e+1}-p^e})Y_e = Y_e/Y_{e+1} \subset X/Y_{e+1} = X_{e+1},$$

da die Gruppe X_{e+1} als p-Klassengruppe von K_{e+1} endlich ist.

□

2.6 Endlich erzeugte Λ-Moduln

Für endlich erzeugte Moduln über der Iwasawa-Algebra bekommt man bis auf so genannte Pseudo-Isomorphismen, also Abbildungen mit endlichem Kern und Cokern, eine ähnliche Strukturaussage wie für Moduln über Hauptidealringen. Genauer ist das Ziel dieses Abschnitts das folgende Resultat:

Satz 2.26 (Struktur von endlich erzeugten Λ-Moduln). *Sei M ein endlich erzeugter Λ-Modul. Dann gibt es eindeutig bestimmte irreduzible Weierstraß-Polynome $f_j(T)$ und eindeutig bestimmte Zahlen $r, m_i, n_j \in \mathbb{N}_0$, sodass ein Homomorphismus*

$$M \to \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T))^{n_j}$$

existiert, dessen Kern und Cokern endlich sind.

Mit Hilfe dieses Satzes definiert man die Iwasawa-Invarianten μ und λ eines solchen Moduls durch

$$\begin{aligned} \mu &= \sum_{i=1}^{s} m_i, \\ \lambda &= \sum_{j=1}^{t} n_j \cdot \deg(f_j(T)). \end{aligned}$$

Diese Invarianten tauchten als Erstes in dem berühmten Satz von Iwasawa über das Wachstum des p-Anteils der Klassenzahlen in einer $\mathbb{Z}_p$-Erweiterung auf. J. P. Serre ([41]) interpretierte die Invarianten mit Hilfe der oben angegebenen Struktur von $\mathbb{Z}_p[\![T]\!]$-Moduln, die sich aus einer allgemeineren Aussage aus Bourbaki ([4], VII §4.4 Th. 4 und 5) ableiten lässt.

Den Struktursatz kann man mit ähnlich elementaren Mitteln wie im Fall von Hauptidealringen beweisen, wie zum Beispiel im Buch von Washington ([46]). Die nächsten Kapitel orientieren sich stattdessen an [33], Chapter V, §1 und [4].

Das erste Ziel ist es, die Untersuchung der Λ-Moduln auf die Untersuchung von Torsionsmoduln und torsionsfreien Moduln zu reduzieren, sodass diese zwei Fälle getrennt betrachtet werden können.

Lemma 2.27. *Die einzigen Primideale in Λ sind die folgenden Ideale:*
- (0)
- (p)
- $(f(T))$ *mit irreduziblen Weierstraß-Polynomen* $f(T)$
- *das maximale Ideal* $\mathfrak{m} = (p, T)$.

Beweis. Die oben genannten Ideale sind offenbar Primideale in Λ: Für ein irreduzibles Weierstraß-Polynom $f(T)$ gilt $\Lambda/(f(T)) \cong \mathbb{Z}_p[T]/(f(T))$, und dieser Ring ist nullteilerfrei.

Sei $\mathfrak{p}$ ein Primideal der Höhe 1, $\mathfrak{p} \neq p\Lambda$. Dann wird $\mathfrak{p}$ von einem irreduziblen Element $g(T) \in \Lambda \backslash p\Lambda$ erzeugt. Nach dem Weierstraß'schen Vorbereitungssatz kann man als Erzeuger des Ideals ein Weierstraß-Polynom wählen. Damit das Ideal ein Primideal ist, muss das Polynom irreduzibel sein.

Das einzige Primideal der Höhe 2 ist das Ideal (p, T), da die Elemente aus $\Lambda \backslash (p, T)$ Einheiten sind und das Ideal damit das einzige maximale Ideal ist. Das Ideal hat tatsächlich Höhe 2, da jedes Ideal, das man durch Hinzufügen eines weiteren Elements aus $\Lambda \backslash (p)$ zu einem Primideal der Form $(f(T))$ bekommt, eine Potenz des maximalen Ideals enthält. □

Lemma 2.28. *Seien* $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ *Primideale der Höhe 1 in* Λ *und* $S = \bigcap_i \Lambda \backslash \mathfrak{p}_i$. *Dann ist der Ring* $S^{-1}\Lambda$ *ein Hauptidealring.*

Beweis. Die Primideale in $S^{-1}\Lambda$ sind die Ideale $\mathfrak{p}_1 S^{-1}\Lambda, \ldots, \mathfrak{p}_k S^{-1}\Lambda$ und (0). Die Lokalisierung nach einem maximalen Ideal $\mathfrak{p}_i S^{-1}\Lambda$ ist zu $\Lambda_{\mathfrak{p}_i}$ isomorph. Dieser Ring ist ganz abgeschlossen und eindimensional, also als Lokalisierung des noetherschen Rings Λ ein diskreter Bewertungsring. Damit ist $S^{-1}\Lambda$ ein Dedekindring, und nach [4], VII §2.2 Th. 1 sind semilokale Dedekindringe Hauptidealringe. □

Satz 2.29. *Sei N ein endlich erzeugter Λ-Modul, sodass $N_{\mathfrak{q}} = 0$ für alle Primideale $\mathfrak{q}$ der Höhe 1. Dann ist N endlich.*

Beweis. Sei $\{y_1, \ldots, y_m\}$ ein Erzeugendensystem von N. Wegen $(\Lambda y_i)_{\mathfrak{q}} = 0$ für alle $\mathfrak{q}$ ist $\operatorname{Ann}(y_i)$ für kein i in einem Primideal der Höhe 1 enthalten. Der Ring $\Lambda/\operatorname{Ann}(y_i)$ ist ein noetherscher Ring mit dem Bild des maximalen Ideals (p, T) als einzigem Primideal. Da in noetherschen Ringen das Nilradikal nilpotent ist, muss eine Potenz $(p, T)^n$ des maximalen Ideals in allen Idealen $\operatorname{Ann}(y_i)$ enthalten sein. Für jedes i ist der Modul $\Lambda/(\operatorname{Ann}(y_i))$ als Quotient von $\Lambda/(p, T)^n$ endlich, und der Modulhomomorphismus

$$\Lambda/(\operatorname{Ann}(y_1)) \times \cdots \times \Lambda/(\operatorname{Ann}(y_m)) \to N,$$

der sich aus den Abbildungen $\Lambda/(\operatorname{Ann}(y_i)) \to N,\ 1 \mapsto y_i$ zusammensetzt, ist surjektiv. Damit ist auch der Λ-Modul N endlich. □

Definition. Der Torsions-Untermodul eines Moduls M über einem kommutativen Ring R ist der Modul $\operatorname{Tors}(M) = \{x \in M \mid \exists r \in R \backslash \{0\} : r \cdot x = 0\}$. Falls $M = \operatorname{Tors}(M)$, heißt M Torsionsmodul.

Falls R nullteilerfrei ist, sind die Torsionsmoduln genau die Moduln vom Rang 0.

Definition. Eine Abbildung zwischen zwei Λ-Moduln, deren Kern und Cokern endliche Gruppen sind, nennen wir Pseudo-Isomorphismus.

Man sieht sofort, dass die Relation „Pseudo-Isomorphismus“ reflexiv und transitiv ist. Für Torsionsmoduln wird in Abschnitt 2.6.1 gezeigt, dass sie außerdem symmetrisch ist. Wir nennen zwei Torsionsmoduln also pseudo-isomorph, wenn es einen Pseudo-Isomorphismus zwischen ihnen gibt.

Um nachzuweisen, dass eine Abbildung ein Pseudo-Isomorphismus ist, genügt es, für jedes Primideal $\mathfrak{q}$ der Höhe 1 nachzuweisen, dass die Abbildung auf den Lokalisierungen nach $\mathfrak{q}$ einen Isomorphismus induziert. Das folgt aus Satz 2.29, da die Lokalisierungen $\Lambda_{\mathfrak{q}}$ flache Moduln sind.

Lemma 2.30. *Sei X ein endlich erzeugter Λ-Modul und M der Torsions-Untermodul. Dann gibt es einen Homomorphismus $g : X \to M$, sodass g auf dem Untermodul M durch Multiplikation mit einen Element aus Λ gegeben ist und sodass diese Einschränkung ein Pseudo-Isomorphismus ist.*

Beweis. Sei $\mathfrak{a} = \operatorname{Ann}(M)$. Da Λ noetherscher Integritätsbereich ist und X endlich erzeugt, ist $\mathfrak{a} \neq 0$. Aus der Form der Primideale von Λ kann man ablesen, dass $\mathfrak{a} \not\subset \mathfrak{q}$ für fast alle Primideale $\mathfrak{q}$ der Höhe 1, da ein beliebiges Polynom aus $\mathfrak{a}$ nur in endlich vielen der Primideale liegen kann. Seien also $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ genau die Primideale der Höhe 1, die $\mathfrak{a}$ enthalten, und $S = \bigcap_i (\Lambda \backslash \mathfrak{p}_i)$. Nach Lemma 2.28 ist der Ring $S^{-1}\Lambda$ ein Hauptidealring, über dem also torsionsfreie Moduln frei sind. Da die exakte Sequenz

$$0 \to S^{-1}M \to S^{-1}X \to S^{-1}X/S^{-1}M \to 0$$

spaltet, können wir einen Homomorphismus $f \in \operatorname{Hom}_{S^{-1}\Lambda}(S^{-1}X, S^{-1}M)$ wählen, der $S^{-1}X$ auf den Modul $S^{-1}M$ projiziert. Wegen der Bijektivität der kanonischen Abbildung

$$S^{-1}\operatorname{Hom}_\Lambda(X, M) \to \operatorname{Hom}_{S^{-1}\Lambda}(S^{-1}X, S^{-1}M)$$

ist dieser Homomorphismus f von der Form $f = s^{-1}\tilde{g}$ mit einem Element $s \in S$ und einem Homomorphismus $\tilde{g} \in \operatorname{Hom}_\Lambda(X, M)$. Für alle Elemente $t \in S^{-1}M$ gilt dann $f(t) = s^{-1}\tilde{g}(t) = t$ in $S^{-1}M$, also gibt es für jedes t aus dem Torsionsmodul M ein Element s_t mit $s_t\tilde{g}(t) = s_t s \cdot t$ in M. Da der Λ-Modul M endlich erzeugt ist, können wir ein Element $s' \in S$ so wählen, dass die Abbildung $s'\tilde{g}$ auf ganz M durch Multiplikation mit dem Element $s's$ gegeben ist.

Um zu zeigen, dass g ein Pseudo-Isomorphismus ist, müssen wir nachweisen, dass die induzierten Abbildungen auf den Lokalisierungen für alle Primideale der Höhe 1 bijektiv sind. Die Primideale $\mathfrak{q}$ der Höhe 1, für die $M_{\mathfrak{q}}$ nicht der Nullmodul ist, sind aber genau die Ideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ von Λ, die $\operatorname{Ann}(M)$ enthalten. Für diese Ideale ist die induzierte Abbildung $g_i : M_{\mathfrak{p}_i} \to M_{\mathfrak{p}_i}$ gegeben durch Multiplikation mit $s \cdot s'$, also mit einer Einheit, und damit ein Isomorphismus. □

Satz 2.31. *Sei X ein endlich erzeugter Λ-Modul und M der Torsions-Untermodul. Dann gibt es einen Pseudo-Isomorphismus $f : X \to M \oplus X/M$.*

Beweis. Sei f die Abbildung, die sich aus der Abbildung g aus Lemma 2.30 und der Projektionsabbildung $p : X \to X/M$ zusammensetzt und $h : M \to M$ die Einschränkung von g auf M. Wir haben das kommutative Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & X & \longrightarrow & X/M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle f} & & \| & & \\ 0 & \longrightarrow & M & \longrightarrow & M \oplus X/M & \longrightarrow & X/M & \longrightarrow & 0 \end{array}$$

in dem beide Zeilen exakt sind. Anwenden des Schlangenlemmas ergibt Isomorphismen $\ker(h) \to \ker(f)$ und $\operatorname{coker}(h) \to \operatorname{coker}(f)$, und da die Abbildung h nach Lemma 2.30 ein Pseudo-Isomorphismus ist, gilt das auch für f.

□

2.6.1 Torsionsmoduln

Satz 2.32. *Jeder endlich erzeugte Λ-Torsionsmodul M ist pseudo-isomorph zu einer endlichen direkten Summe*

$$\bigoplus \Lambda/(f_i(T)^{m_i}) \oplus \bigoplus \Lambda/(p^{n_j})$$

mit eindeutig bestimmten irreduziblen Weierstraß-Polynomen f_i und Zahlen m_i, n_j.

Beweis. Seien $\mathfrak{a} = \operatorname{Ann}(M)$ und $\mathfrak{p}_i$ und S wie im Beweis von Lemma 2.30, sodass der Ring $S^{-1}A$ ein Hauptidealring ist. Wir können nach dem Struktursatz für endlich erzeugte Moduln über Hauptidealringen einen Modul E der Form

$$E = \bigoplus_i \Lambda/\mathfrak{p}_i^{n_i}$$

mit Primidealen $\mathfrak{p}_i$ der Höhe 1 und Exponenten $n_i \in \mathbb{N}$ so wählen, dass es einen Isomorphismus $g_0 : S^{-1}M \to S^{-1}E$ gibt. Da

$$\operatorname{Hom}_{S^{-1}\Lambda}(S^{-1}M, S^{-1}E) = S^{-1}\operatorname{Hom}_\Lambda(M, E),$$

können wir wieder einen Morphismus $g : M \to E$ und ein Element $s \in S$ finden mit $g(x) = sg_0(x)$ für alle $x \in M$. Um zu zeigen, dass g ein Pseudo-Isomorphismus ist, müssen wir nachweisen, dass die induzierten Abbildungen auf den Lokalisierungen für alle Primideale der Höhe 1 bijektiv sind. Die Primideale $\mathfrak{q}$ der Höhe 1, für die $M_\mathfrak{q}$ nicht der Nullmodul ist, sind aber wieder genau die Ideale $\mathfrak{p}_i$, und für diese Ideale ist die induzierte Abbildung $g_i : T_{\mathfrak{p}_i} \to T_{\mathfrak{p}_i}$ durch Multiplikation mit der Einheit s gegeben.

Die Primideale der Höhe 1 in $\mathbb{Z}_p[\![T]\!]$ sind nach Lemma 2.27 von der Form (p) oder $(f(T))$ mit irreduziblen Weierstraß-Polynomen f.

Zur Eindeutigkeit: Lokalisieren nach einem beliebigen Primideal $\mathfrak{p}$ der Höhe 1 macht aus einem Pseudo-Isomorphismus von M in eine direkte Summe der oben angegebenen Form einen Isomorphismus zwischen den Moduln über $\Lambda_\mathfrak{p}$. Die Lokalisierung eines Summanden $\Lambda/\mathfrak{p}^k$ nach $\mathfrak{p}$ liefert den Modul $\Lambda_\mathfrak{p}/\mathfrak{p}^k\Lambda_\mathfrak{p}$, und die Lokalisierung nach allen anderen Primidealen verschwindet. Die Zahlen m_i und n_j sind also wie die Primideale $(f_i(T))$ eindeutig bestimmt.

□

Genau wie im Beweis dieses Satzes zeigt man, dass die Relation „Pseudo-Isomorphismus" auf Torsionsmoduln symmetrisch ist:

Satz 2.33. *Sei $f : M \to N$ ein Pseudo-Isomorphismus zwischen den Λ-Torsionsmoduln M und N. Dann existiert auch ein Pseudo-Isomorphismus $g : N \to M$.*

Beweis. Sei $P = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ eine endlich Menge von Primidealen der Höhe 1, sodass $M_\mathfrak{q} = N_\mathfrak{q} = 0$ für alle anderen Primideale $\mathfrak{q}$ der Höhe 1, und $S = \bigcap_i (\Lambda \backslash \mathfrak{p}_i)$. Dann ist der induzierte Homomorphismus $S^{-1}f : S^{-1}M \to S^{-1}N$ ein Isomorphismus, da die Lokalisierungen nach allen Primidealen von $S^{-1}A$ nach Voraussetzung Isomorphismen sind. Wie oben finden wir eine Abbildung $g : N \to M$ und ein Element $s \in S$ mit $S^{-1}g = sf^{-1}$. Diese Abbildung g ist dann ein Pseudo-Isomorphismus, da sie auf allen Lokalisierungen nach Primidealen $\mathfrak{p}_i$ aus P durch Multiplikation mit einer Einheit gegeben ist und $M_\mathfrak{q} = N_\mathfrak{q} = 0$ für die anderen Primideale der Höhe 1. □

2.6.2 Torsionsfreie Moduln

Wie im Fall von Hauptidealringen gilt für endlich erzeugte Moduln über der Iwasawa-Algebra, dass die torsionsfreien Moduln genau die freien Moduln sind. Eine allgemeinere Version dieser Aussage ist Proposition 5.1.9 in [33].

Satz 2.34. *Endlich erzeugte torsionsfreie Λ-Moduln sind frei.*

Beweis. Sei M ein endlich erzeugter torsionsfreier Λ-Modul und r die minimale Anzahl von Erzeugern. Dann ist Multiplikation mit $T \in \Lambda$ injektiv, wir haben also ein kommutatives Diagramm mit exakten Zeilen

$$\begin{tikzcd}
0 \arrow[r] & \Lambda^r \arrow[r, "\cdot T"] \arrow[d] & \Lambda^r \arrow[r] \arrow[d, "\varphi"] & (\Lambda/(T))^r \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M \arrow[r, "\cdot T"] & M \arrow[r] & M/TM \arrow[r] & 0
\end{tikzcd}$$

Der torsionsfreie $\Lambda/(T)$-Modul M/TM ist frei, da $\Lambda/(T) = \mathbb{Z}_p$ Hauptidealring ist. Falls $M/TM \cong \mathbb{Z}_p^s$ mit $s < r$, hat M nach Nakayama ein Erzeugendensystem mit weniger als r Elementen. Also ist $s = r$ und die Abbildung $(\Lambda/(T))^r \to \mathbb{Z}_p^r = M/TM$ ist ein Isomorphismus.

Aus dem kommutativen Diagramm kann man ablesen, dass das Urbild des Kerns K von $\varphi : \Lambda^r \to M$ unter der Abbildung $\cdot T : \Lambda^r \to \Lambda^r$ genau K ist. Nach Nakayama folgt aus dem Isomorphismus $K \cong TK$, dass $K = 0$, und damit ist die Abbildung φ bijektiv. □

2.7 Maximale abelsche unverzweigte p-Erweiterungen

In Abschnitt 2.5 wurde gezeigt, dass die Galoisgruppe der maximalen abelschen unverzweigten p-Erweiterung von K_∞ ein endlich erzeugter topologischer Λ-Modul wird. Mit den Strukturaussagen der letzten Abschnitte folgt jetzt, dass der torsionsfreie Anteil verschwindet. Dieses Resultat wird später helfen, dieselbe Eigenschaft für einen größeren Λ-Modul herzuleiten.

Satz 2.35. *Sei K_0 ein Zahlkörper, K_∞/K_0 eine $\mathbb{Z}_p$-Erweiterung und L die maximale abelsche unverzweigte p-Erweiterung von K_∞. Dann ist $X = \mathrm{Gal}(L/K_\infty)$ ein endlich erzeugter Λ-Torsionsmodul.*

Beweis. Wir wissen aus Lemma 2.22, dass es eine Zahl $e \geq 0$ und $\mathbb{Z}_p$-Untermoduln $Y_e, Y_{e+1}, \dots$ von X mit $Y_n = (1 + \gamma^{p^e} + \cdots + \gamma^{p^n - p^e})Y_e$ für alle $n \geq e$ gibt, sodass X/Y_n als p-Klassengruppe eines Zwischenkörpers K_n jeweils eine endliche Gruppe ist. Nach Satz 2.31 gibt es einen Pseudo-Isomorphismus

$$X \to \Lambda^r \oplus M$$

mit $r \in \mathbb{N}_0$ und einem Λ-Torsionsmodul M. Die Inklusionen $Y_{e+1} \subset Y_e \subset X$ liefern Abbildungen in $\Lambda^r \oplus M$, die ebenfalls endlichen Kern und Cokern haben. Diese Abbildungen induzieren

$$Y_e/Y_{e+1} \to (\Lambda^r \oplus M)/((1 + \gamma^{p^e} + \cdots + \gamma^{p^{e+1}-p^e})(\Lambda^r \oplus M)),$$

und diese Abbildung hat wieder endlichen Cokern. Der Modul $(\Lambda^r \oplus M)/((1 + \gamma^{p^e} + \cdots + \gamma^{p^n-p^e})(\Lambda^r \oplus M))$ enthält als Untermodul den Modul $\Lambda/((1+\gamma^{p^e}+\cdots+\gamma^{p^n-p^e})\Lambda)$, falls $r > 0$, und dieser Modul hat unendlich viele Elemente. Wir haben nun eine exakte Sequenz

$$Y_e/Y_{e+1} \to (\Lambda^r \oplus M)/((1 + \gamma^{p^e} + \cdots + \gamma^{p^{e+1}-p^e})(\Lambda^r \oplus M)) \to C \to 0,$$

in der die Moduln Y_e/Y_{e+1} und C endlich sind, also auch der Quotient in der Mitte. Daraus folgt $r = 0$, also ist X pseudo-isomorph zu einem Torsionsmodul und damit selbst Torsionsmodul. $\square$

Bemerkung. Wenn man genauer untersucht, wie sich die p-Klassengruppen X_n als Quotienten von X ergeben, erhält man das folgende Resultat von Iwasawa ([16], [41]):

Sei K_∞/K_0 eine $\mathbb{Z}_p$-Erweiterung eines Zahlkörpers K_0 mit Zwischenkörpern K_n und p^{e_n} die Ordnung der p-Klassengruppe von K_n. Dann gibt es $\lambda, \mu \in \mathbb{N}_0, \nu \in \mathbb{Z}$ und einen Index N, sodass

$$e_n = \lambda n + \mu p^n + \nu$$

für alle $n \geq N$. Die Zahlen λ und μ stimmen mit den gleichnamigen Invarianten des Moduls X überein.

2.8 Noch mehr Klassenkörpertheorie

Als Hauptziel dieses Kapitels soll die Galoisgruppe der maximalen außerhalb von p unverzweigten p-Erweiterung eines Zahlkörpers untersucht werden. Dazu benötigen wir noch einige Ergebnisse aus der globalen Klassenkörpertheorie ([46], §13.1 und Anhang 3).

Sei K ein Zahlkörper und $\mathfrak{p}$ ein Primideal in $\mathcal{O}_K$. In der Vervollständigung $K_\mathfrak{p}$ von K bezeichnen wir mit $U_\mathfrak{p}$ die Einheiten und mit $U_\mathfrak{p}^{(1)}$ die Untergruppe derjenigen Einheiten, die kongruent zu $1 \mod \mathfrak{p}$ sind. Wie üblich bezeichnet $\mathfrak{p}$ sowohl das Primideal im Ganzheitsring von K als auch das entsprechende Ideal in der Vervollständigung bezüglich $\mathfrak{p}$. Für unendliche Stellen setzen wir $U_\mathfrak{p} = K_\mathfrak{p}^*$.

Wir bezeichnen mit J die Idelgruppe von K, d.h. die Teilmenge von $\prod K_\mathfrak{p}^*$ der Elemente $(x_\mathfrak{p})$ mit $x_\mathfrak{p} \in U_\mathfrak{p}$ für fast alle $\mathfrak{p}$. Sei $U = \prod_\mathfrak{q} U_\mathfrak{q}$, wobei $\mathfrak{q}$ hier über die endlichen und unendlichen Stellen von K laufen soll. Die Topologie von J ist durch die Produkttopologie auf U und die Festsetzung, dass U eine offene Teilmenge von J sein soll, gegeben. Mit der Multiplikation als Verknüpfung wird J dadurch eine lokalkompakte topologische Gruppe.

Die Gruppen

$$U_p = \prod_{\mathfrak{p}|p} U_\mathfrak{p} \quad \text{und} \quad U_{[p]} = \prod_{\mathfrak{q}\nmid p} U_\mathfrak{q}$$

fassen wir als Untergruppen von U auf.

Als wichtigstes Werkzeug werden wir im nächsten Abschnitt die folgende Aussage verwenden:

Satz 2.36. *Die abelschen algebraischen Erweiterungen von K entsprechen genau den abgeschlossenen Untergruppen H von J mit $K^* \subset H$, sodass der Quotient J/H eine total unzusammenhängende topologische Gruppe ist. Die Galoisgruppe einer solchen Erweiterung $L \supset K$ ist isomorph zu J/H, und ein Primideal $\mathfrak{q}$ von K ist genau dann unverzweigt in L, wenn $U_\mathfrak{q} \subset H$.*

Wie die Bestandteile $U_\mathfrak{p}$ der Idelgruppe aussehen, ist aus der Zahlentheorie bekannt ([32], Satz 5.7 in Kapitel II):

Satz 2.37 (Einheitengruppe der lokalen Körper). *Sei K ein Zahlkörper und $\mathfrak{p}$ ein Primideal von K über p. Die Vervollständigung $K_\mathfrak{p}$ habe den Grad d über $\mathbb{Q}_p$ und den Restklassenkörper $\mathbb{F}_q$. Dann gilt für die Einheitengruppe $U_\mathfrak{p}$ von $K_\mathfrak{p}$:*

$$U_\mathfrak{p} = \mu_{q-1} \times U_\mathfrak{p}^{(1)} = \mu_{q-1} \times \mu_{p^a} \times V$$

mit einer Zahl $a \in \mathbb{N}_0$ und einer abelschen Pro-p-Gruppe V, die als $\mathbb{Z}_p$-Modul frei vom Rang d ist.

Die Gleichheit gilt auch, wenn man alle Gruppen als topologische Gruppen auffasst und V dabei mit der Topologie von $\mathbb{Z}_p^d$ versieht.

Lemma 2.38. *Sei E die Einheitengruppe in K und $\sigma_p : E \to U_p$ die kanonische Inklusion $x \mapsto (x) \in \prod_{\mathfrak{p}|p} U_\mathfrak{p}$. Dann gilt*

$$U_p \cap \overline{U_{[p]}K^*} = \overline{\sigma_p(E)}.$$

Beweis. Sei $U_p^{(n)}$ die Gruppe der Einheiten u in U_p mit $u \equiv 1 \mod p^n$. Die Gruppen $U_p^{(n)}$ bilden dann eine Umgebungsbasis der 1 in U_p; die Gruppen $U_p^{(n)}U_{[p]}K^* \cap U_p$ bilden damit eine Umgebungsbasis von $U_{[p]}K^* \cap U_p$ und ihr Durchschnitt ist der Abschluss von $U_{[p]}K^* \cap U_p$. Es gilt $U_p^{(n)}U_{[p]}K^* \cap U_p \subset EU_p^{(n)}$, da die Komponenten bei U_l mit $l \nmid p$ alle 1 sind und die Komponenten bei $U_\mathfrak{p}$ mit $\mathfrak{p}|p$ Einheiten aus K sein müssen. Umgekehrt gilt $EU_p^{(n)} \subset U_p^{(n)}U_{[p]}K^*$ für alle n.

Der Schnitt aller $EU_p^{(n)}$ enthält sicherlich $\overline{\sigma_p(E)}$, da $E \subset EU_p^{(n)}$ für jedes n. Für die umgekehrte Inklusion sei x ein beliebiges Element aus $\bigcap_n EU_p^{(n)}$. Für jedes n lässt sich x dann schreiben als $x = e_n \cdot (1 + p_1^{(n)}, \ldots, 1 + p_r^{(n)})$ mit $e_n \in E$ und $p_i^{(n)} \in \mathfrak{p}_i^n$. Also liegt das Element $(x - e_n)_i$ jeweils in $\mathfrak{p}_i^n$, und damit ist $x_i = \lim_{n\to\infty}(x - e_n)_i$ in der $\mathfrak{p}_i$-adischen Topologie, also $x \in \overline{\sigma_p(E)}$ in U_p. □

Die Leopoldt'sche Vermutung

Nach dem Dirichlet'schen Einheitensatz hat die Gruppe E der Einheiten in einem Zahlkörper K als $\mathbb{Z}$-Modul den Rang $r_1 + r_2 - 1$, wobei r_1 und r_2 wie üblich die Anzahlen der reellen bzw. Paare von komplexen Einbettungen von K bezeichnen. Da die Untergruppe E_1 derjenigen Einheiten, die in jeder Vervollständigung $K_\mathfrak{p}$ mit $\mathfrak{p}|p$ kongruent zu 1 mod $\mathfrak{p}$ sind, endlichen Index hat, hat sie als $\mathbb{Z}$-Modul denselben Rang $r_1 + r_2 - 1$.

Eine von mehreren äquivalenten Formulierungen der Vermutung, die Leopoldt aufgestellt hat, ist die folgende Aussage:

Vermutung. *Der Rang des Abschlusses von $\sigma_p(E_1)$ in U_p als $\mathbb{Z}_p$-Modul ist ebenfalls r_1+r_2-1.*

Bisher wurde die Vermutung nur in Spezialfällen bewiesen; zum Beispiel weiß man, dass sie für abelsche Zahlkörper richtig ist ([33], Th. 10.3.16). Wir werden im nächsten Abschnitt eine schwächere Version der Leopoldt'schen Vermutung für $\mathbb{Z}_p$-Erweiterungen brauchen.

2.9 Maximale abelsche p-verzweigte p-Erweiterungen

In diesem Abschnitt wird mit Hilfe von Klassenkörpertheorie gezeigt, dass der Iwasawa-Modul, den man der maximalen p-verzweigten p-Erweiterung eines total reellen Zahlkörpers zuordnet, ein Torsionsmodul ist. Der Beweis ist im Wesentlichen aus Kapitel 13 von [46] entnommen.

Wir verwenden dieselben Bezeichnungen wie im letzten Abschnitt; zusätzlich bezeichnen wir die maximale abelsche außerhalb von p unverzweigte p-Erweiterung eines Zahlkörpers K mit $M_p(K)$ und die zugehörige Galoisgruppe $\mathrm{Gal}(M_p(K)/K)$ mit $G_p^{ab}(K)$. Eine Körpererweiterung nennen wir „außerhalb von p unverzweigt" oder kurz „p-verzweigt", wenn sie bei allen Stellen über der Primzahl p unverzweigt ist.

Satz 2.39. *Es gibt einen Homomorphismus mit endlichem Kern und Cokern von $G_p^{ab}(K)$ in den Quotienten $U_p/\overline{\sigma_p(E)}$.*

Beweis. Der maximalen außerhalb von p unverzweigten Erweiterung von K entspricht nach Klassenkörpertheorie eine abgeschlosse Untergruppe H von J, sodass J/H total unzusammenhängende Gruppe ist. Genauer ist H die kleinste solche Gruppe, die $K^*U_{[p]}$ enthält.

Wir betrachten zunächst den Quotienten $J/\overline{U_{[p]}K^*}$. Es gilt $\overline{U_{[p]}K^*} \subset U_pU_{[p]}K^* \subset J$, da $U_pU_{[p]}K^*$ als offene Untergruppe von J auch abgeschlossen ist, und der Quotient $J/U_pU_{[p]}K^*$ ist isomorph zur Klassengruppe von K und damit endlich. Wir betrachten also nur den anderen Quotienten $U_pU_{[p]}K^*/\overline{U_{[p]}K^*} \cong U_p/(\overline{U_{[p]}K^*} \cap U_p)$. Nach Lemma 2.38 ist dieser Quotient isomorph zu $U_p/\overline{\sigma_p(E)}$.

Der Abschluss $\overline{K^*U_{[p]}}$ ist also die gesuchte Untergruppe, denn der Quotient J/K^*U ist diskret und $UK^*/\overline{U_{[p]}K^*}$ ist total unzusammenhängend. Die Gruppe $G_p^{ab}(K)$ ist nun nach Klassenkörpertheorie isomorph zum maximalen p-Quotienten von $J/\overline{U_{[p]}K^*}$.

Für $\mathfrak{p}|p$ ist die Einheitengruppe $U_\mathfrak{p}$ von $K_\mathfrak{p}$ das Produkt von $U_\mathfrak{p}^{(1)}$ und einer endlichen Untergruppe. Die gesamte Gruppe U_p ist also Produkt von $U_p^{(1)} = \prod_{\mathfrak{p}|p} U_\mathfrak{p}^{(1)}$ und einer endlichen Gruppe.

Damit ist $U_p^{(1)}/(U_p^{(1)} \cap \overline{\sigma_p(E)})$ ein Pro-p-Quotient von $U_p/\overline{\sigma_p(E)}$ mit endlichem Index, und man erhält aus diesen Abbildungen einen Homomorphismus $G_p^{ab}(K) \to U_p/\overline{\sigma_p(E)}$ mit endlichem Kern und Cokern. □

Eine einfache Verallgemeinerung dieses Satzes erhält man, wenn man statt $G_p^{ab}(K)$ eine endliche Menge S von Stellen des Körpers K wählt, die alle Stellen über p enthält, und die maximale abelsche außerhalb von S unverzweigte p-Erweiterung $M_S(K)$ betrachtet. Analog zu den Bezeichnungen für den Spezialfall verwenden wir die Notationen

$$\begin{aligned} G_S^{ab}(K) &= \mathrm{Gal}(M_S(K)/K) \\ U_S &= \prod_{\mathfrak{q}\in S} U_\mathfrak{q} \subset J \end{aligned}$$

und $\sigma_S : K \to U_S$ für die diagonale Einbettung von K in U_S.

Korollar 2.40. *Sei S eine endliche Menge von Primzahlen mit $p \in S$. Dann ist die Galoisgruppe $G_S^{ab}(K)$ der maximalen abelschen außerhalb von S unverzweigten p-Erweiterung von K ebenfalls bis auf endlichen Kern und Cokern isomorph zu $U_p/\overline{\sigma_p(E)}$.*

Beweis. Genau wie oben beweist man, dass $G_S^{ab}(K)$ bis auf endlichen Kern und Cokern zum maximalen p-Quotienten der Gruppe $U_S/\overline{\sigma_S(E)}$ isomorph ist. Es gilt $U_S = U_p \times U_{S'}$, wobei S' die Stellen aus S enthält, die nicht über p liegen. Da die Faktoren von $U_{S'}$ jeweils nur endlichen p-Anteil haben, ist $G_S^{ab}(K)$ bis auf endlichen Kern und Cokern isomorph zum maximalen p-Quotienten der Gruppe $U_p/\overline{\sigma_S(E)} \cap U_p$. Falls $\pi : U_S \to U_p$ die Projektion bezeichnet, gilt aber $\pi(\sigma_S(E)) = \sigma_p(E)$, und wegen der Kompaktheit folgt

$$\overline{\sigma_S(E)} \cap U_p = \pi(\overline{\sigma_S(E)}) = \overline{\sigma_p(E)}.$$

Wir erhalten also wieder dieselbe Gruppe wie oben. □

Für den Rest des Abschnitts vereinbaren wir als Abkürzung die Schreibweise $\overline{E}$ für den Abschluss von $\sigma_p(E)$ in U_p; analog schreiben wir $\overline{E}_1$ für $\overline{\sigma_p(E_1)}$.

Sei $\delta(K)$ diejenige natürliche Zahl, für die der $\mathbb{Z}_p$-Modul $\overline{E}_1$ den Rang $r_1 + r_2 - 1 - \delta(K)$ hat, also die Abweichung von der Aussage der Leopoldt-Vermutung.

Satz 2.41. *Die Gruppe $G_p^{ab}(K)$ hat als $\mathbb{Z}_p$-Modul den Rang $r_2 + 1 + \delta(K)$.*

Beweis. Aus dem Beweis des letzten Satzes erhält man einen Pseudo-Isomorphismus

$$G_p^{ab}(K) \to U_p^{(1)}/\overline{E}_1,$$

und der $\mathbb{Z}_p$-Rang von $U_p^{(1)} = \prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^{(1)}$ ist die Summe der Zahlen $\mathrm{rg}_{\mathbb{Z}_p} U_{\mathfrak{p}}^{(1)} = [K_{\mathfrak{p}} : \mathbb{Q}_p]$ für $\mathfrak{p}|p$. Diese Summe ist genau der Grad von K über $\mathbb{Q}$. Der $\mathbb{Z}_p$-Rang von $U_p^{(1)}/\overline{E}$ ist also durch die Differenz $(r_1 + 2r_2) - (r_1 + r_2 - 1 - \delta(K)) = r_2 + 1 + \delta(K)$ gegeben und stimmt mit dem Rang von $G_p^{ab}(K)$ überein. □

Bemerkung. Als Korollar erhält man wie oben wieder dieselbe Aussage für die Galoisgruppe $G_S^{ab}(K)$.

Wenn die Leopoldt'sche Vermutung für alle Zwischenkörper einer total reellen $\mathbb{Z}_p$-Erweiterung von Zahlkörpern richtig ist, also zum Beispiel im Fall der zyklotomischen $\mathbb{Z}_p$-Erweiterung $\mathbb{Q}_\infty/\mathbb{Q}$, sieht man sofort, dass die Galoisgruppen $\mathrm{Gal}(M_p(K_n)/K_n)$ der maximalen abelschen p-verzweigten p-Erweiterungen den $\mathbb{Z}_p$-Rang 1 haben. Die Gruppen $\mathrm{Gal}(M_p(K_n)/K_\infty)$ haben also den Rang 0, und mit derselben Begründung wie in Abschnitt 2.7 für den Modul X kann man dann beweisen, dass der Modul $\mathrm{Gal}(\bigcup M_p(K_n)/K_\infty)$ ein endlich erzeugter Λ-Torsionsmodul ist.

Ohne dieses Resultat zu verwenden, zeigen wir für beliebige zyklotomische $\mathbb{Z}_p$-Erweiterungen die folgende Aussage ([46], §13.5), die für allgemeine $\mathbb{Z}_p$-Erweiterungen auch als schwache Leopoldt-Vermutung bezeichnet wird:

Satz 2.42. *Sei $K_\infty \supset K_0$ die zyklotomische $\mathbb{Z}_p$-Erweiterung mit Zwischenkörpern K_n. Dann ist die Menge der Zahlen $\delta_n = \delta(K_n)$ beschränkt.*

Für den Beweis benötigen wir zwei Hilfsaussagen:

Lemma 2.43. *Sei K ein Zahlkörper, der die p^n-ten Einheitswurzeln enthält und $\delta = \delta(K)$. Dann hat die Klassengruppe von K einen zu $(\mathbb{Z}/p^n\mathbb{Z})^\delta$ isomorphen Quotienten.*

Beweis. Angenommen, $\delta = \delta(K) > 0$. Sei $\{\epsilon_1, \dots, \epsilon_r\}$ eine $\mathbb{Z}$-Basis für $E_1(K)$, sodass die Elemente $\{\epsilon_{\delta+1}, \dots, \epsilon_r\}$ eine $\mathbb{Z}_p$-Basis von $\overline{E}_1$ bilden. Dann gibt es für $i \leq \delta$ eine Darstellung $\epsilon_i = \prod_{j>\delta} \epsilon_j^{a_{ij}}$. Sei a'_{ij} die n-te Partialsumme der p-adischen Darstellung $a_{ij} = \sum b_\ell p^\ell$ und

$$\alpha_i = \prod_{j>\delta} \epsilon_j^{a_{ij}-a'_{ij}} = \epsilon_i \cdot \prod_{j>\delta} \epsilon_j^{-a'_{ij}}.$$

Dann ist α_i in $\overline{E}_1$ eine p^n-te Potenz, und da die Menge $\{\epsilon_1, \dots, \epsilon_r\}$ eine $\mathbb{Z}$-Basis für $E_1(K)$ ist, erzeugen die Elemente $\alpha_1, \dots, \alpha_\delta$ eine zu $(\mathbb{Z}/p^n\mathbb{Z})^\delta$ isomorphe Untergruppe von $K^*/(K^*)^{p^n}$. Da wir $\zeta_{p^n} \in K$ angenommen haben, entspricht dieser Untergruppe die Kummer-Erweiterung $K(\sqrt[p^n]{\alpha_1}, \dots, \sqrt[p^n]{\alpha_\delta})/K$ mit Galoisgruppe $(\mathbb{Z}/p^n\mathbb{Z})^\delta$.

Die Erweiterung $K(\sqrt[p^n]{\alpha_i})/K$ ist außerhalb von p unverzweigt, da für ein Primideal $\mathfrak{q} \nmid p$ das Minimalpolynom von $\sqrt[p^n]{\alpha_i}$ über der Vervollständigung $K_\mathfrak{q}$ separabel über dem Restklassenkörper bleibt. Die Erweiterung $K(\sqrt[p^n]{\alpha_i})/K$ ist auch bei p unverzweigt, da $K_\mathfrak{q}$ die p^n-ten Wurzeln von α_i bereits enthält. Also ist $K(\sqrt[p^n]{\alpha_1}, \dots, \sqrt[p^n]{\alpha_\delta})$ abelsche und als Zusammensetzung von unverzweigten Erweiterungen unverzweigte Erweiterung von K. Die Galoisgruppe der maximalen abelschen unverzweigten Erweiterung von K hat damit die Gruppe $(\mathbb{Z}/p^n\mathbb{Z})^\delta$ als Quotienten. $\square$

Lemma 2.44. *Für einen Teilkörper K eines Zahlkörpers L gilt $\delta(K) \leq \delta(L)$.*

Beweis. Die Zahl δ ist die Differenz der Dimensionen $dim_\mathbb{Q}(E_1 \otimes_\mathbb{Z} \mathbb{Q})$ und $dim_{\mathbb{Q}_p}(\overline{E}_1 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$. Da $E_1(K) \otimes \mathbb{Q}$ und $\overline{E_1(K)} \otimes \mathbb{Q}_p$ jeweils als Untervektorräume von $E_1(L) \otimes \mathbb{Q}$ und $\overline{E_1(L)} \otimes \mathbb{Q}_p$ aufgefasst werden können, ist die Differenz $\delta(L)$ mindestens so groß wie $\delta(K)$. $\square$

Beweis von Satz 2.42. Sei K_∞/K_0 eine zyklotomische $\mathbb{Z}_p$-Erweiterung. Nach dem letzten Lemma können wir annehmen, dass K_0 die p-ten Einheitswurzeln enthält und die Zwischenkörper K_n in der zyklotomischen $\mathbb{Z}_p$-Erweiterung von K_0 damit jeweils die p^n-ten Einheitswurzeln. Außerdem können wir annehmen, dass alle verzweigten Stellen in der Erweiterung K_∞/K_0 voll verzweigt sind; sonst ersetzen wir K_0 durch einen mit Hilfe von Lemma 2.7 passend gewählten Zwischenkörper K_e und erhalten wieder eine $\mathbb{Z}_p$-Erweiterung K_∞/K_e mit Zwischenkörpern $K_e = \tilde{K}_0 \subset \tilde{K}_1 \subset \dots$, sodass $\tilde{K}_n$ jeweils die p^n-ten Einheitswurzeln enthält.

Sei γ ein Erzeuger von Γ, der einen Isomorphismus $\mathbb{Z}_p[\![\Gamma]\!] \to \mathbb{Z}_p[\![T]\!]$ bestimmt. Die p-Klassengruppe von K_n ergibt sich als Quotient X/Y_n, wobei Y_n wie in Lemma 2.21 gewählt werden kann, also $Y_n = (1 + \gamma + \dots + \gamma^{p^n-1})Y_0$. Der Isomorphismus $\Lambda \to \mathbb{Z}_p[\![T]\!]$ bildet $1 + \gamma + \dots + \gamma^{p^n-1}$ auf das Polynom $\nu_n(T) = 1 + (T+1) + \dots + (T+1)^{p^n-1}$ ab.

Der Λ-Modul X ist als endlich erzeugter Torsionsmodul nach Abschnitt 2.6.1 pseudoisomorph zu einer endlichen direkten Summe $E = \bigoplus \Lambda/(p^{n_i}) \oplus \bigoplus \Lambda/(f_i(T))$ mit Weierstraß-Polynomen f_i. Eine Untersuchung dieses Moduls ergibt, dass er nicht groß genug ist, um in den Quotienten X_n Untergruppen der Form $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$ für eine unbeschränkte Folge (δ_n) Platz zu bieten.

Genauer: Es gibt eine exakte Sequenz

$$0 \to K \to \bigoplus \Lambda/(p^{n_i}) \oplus \bigoplus \Lambda/(f_i(T)) \to X \to C \to 0$$

mit endlichen Moduln K und C, die durch Tensorieren mit $\Lambda/(\nu_n(T))$ für jedes $n \in \mathbb{N}$ die exakten Sequenzen

$$\bigoplus \Lambda/(p^{n_i}, \nu_n(T)) \oplus \bigoplus \Lambda/(f_i(T), \nu_n(T)) \to X/\nu_n(T)X \to C/\nu_n(T)C \to 0$$

liefert.

Wir nehmen nun an, die Folge $(\delta_n) = (\delta(K_n))$ sei unbeschränkt. Dann hat die Gruppe $X/Y_n = X/\nu_n(T)Y_0$ jeweils einen Quotienten der Form $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_n}$. Da X/Y_0 endlich ist, gibt es dann auch eine unbeschränkte Folge (λ'_n), sodass man in $X/\nu_n(T)X$ jeweils $(\mathbb{Z}/p^n\mathbb{Z})^{\lambda'_n}$ als Quotienten finden kann und eine unbeschränkte Folge (λ_n), sodass der Modul $E/\nu_n(T)E$ jeweils einen Quotienten der Form $(\mathbb{Z}/p^n\mathbb{Z})^{\lambda_n}$ besitzt. Wir untersuchen nun die einzelnen Summanden von E auf solche Quotienten.

Aus einem Summanden der Form $\Lambda/(p^k)$ erhält man offenbar für $n > k$ keinen Quotienten der gewünschten Form. Falls $f(T)$ ein Weierstraß-Polynom vom Grad d ist, ergibt sich aus $\Lambda/(f(T)) \cong \mathbb{Z}_p^d$ höchstens ein Quotient der Form $(\mathbb{Z}/p^n\mathbb{Z})^d$. Wir erhalten also einen Widerspruch zur Annahme, dass (δ_n) unbeschränkt ist. $\square$

Satz 2.45. *Sei $K_\infty \supset K_0$ eine $\mathbb{Z}_p$-Erweiterung mit Zwischenkörpern K_n. Dann gilt $M_p(K_\infty) = \bigcup_n M_p(K_n)$.*

Beweis. Sicherlich gilt $M_p(K_n) \subset M_p(K_\infty)$ für jedes n. Für die andere Richtung genügt es zu zeigen, dass jede endliche algebraische außerhalb von p unverzweigte p-Erweiterung F von K_∞ in einem der Körper $M_p(K_n)$ enthalten ist.

Jede solche Erweiterung F ergibt sich durch Hochheben einer endlichen Erweiterung F_0/K_0, und der Schnitt $F_0 \cap K_\infty$ ist einer der Zwischenkörper K_n. Es gilt $\mathrm{Gal}(F_0/K_n) \cong \mathrm{Gal}(F/K_\infty)$, also ist F_0/K_n eine abelsche p-Erweiterung und damit auch F_0K_∞/K_n als Zusammensetzung von zwei abelschen p-Erweiterungen. Da die beiden Erweiterungen F_0/K_n und K_∞/K_n außerhalb von p unverzweigt sind, gilt das auch für F/K_n. Insgesamt ist F als abelsche außerhalb von p unverzweigte p-Erweiterung von K_n in $M_p(K_n)$ enthalten. $\square$

Lemma 2.46. *Sei $\mathcal{X}_\infty = \mathrm{Gal}(M_p(K_\infty)/K_\infty)$ und γ ein topologischer Erzeuger von $\Gamma = \mathrm{Gal}(K_\infty/K_0)$. Dann ist der Abschluss der Kommutatoruntergruppe von $\mathrm{Gal}(M_p(K_\infty)/K_n)$ der Untermodul $(\gamma^{p^n} - 1) \cdot \mathcal{X}_\infty$.*

Beweis. Sei zunächst $n = 0$. Für ein Element $(\gamma - 1)x \in (\gamma - 1)\mathcal{X}_\infty$ und eine Hochhebung $\tilde{\gamma}$ von γ ist

$$(\gamma - 1)x = \tilde{\gamma}x\tilde{\gamma}^{-1}x^{-1}$$

in der Kommutatoruntergruppe enthalten.

Umgekehrt: In $\mathrm{Gal}(M_p(K_\infty)/K_0)$ erzeugt ein Urbild $\tilde{\gamma}$ des Erzeugers $\gamma \in \Gamma$ eine Untergruppe $\tilde{\Gamma}$, die unter der Projektion $\pi : \mathrm{Gal}(M_p(K_\infty)/K_0) \to \Gamma$ bijektiv auf Γ abgebildet wird.

Aus der exakten Sequenz

$$1 \to \mathcal{X}_\infty \to \mathrm{Gal}(M_p(K_\infty)/K_0) \to \Gamma \to 1$$

erhalten wir für jedes Element aus $\mathrm{Gal}(M_p(K_\infty)/K_0)$ eine Darstellung der Form $\alpha \cdot x$ mit $\alpha \in \tilde{\Gamma}$ und $x \in \mathcal{X}_\infty$. Für zwei solche Elemente $a, b \in \mathrm{Gal}(M_p(K_\infty)/K_0)$ ergibt sich die Inklusion $aba^{-1}b^{-1} \in (\gamma - 1) \cdot \mathcal{X}_\infty$ jetzt mit derselben Rechnung wie in Lemma 2.20. Der Abschluss der Kommutatoruntergruppe ist ebenfalls eine Teilmenge von $(\gamma - 1) \cdot \mathcal{X}_\infty$, da diese Menge als stetiges Bild der kompakten Menge $\mathcal{X}_\infty$ kompakte und damit abgeschlossene Untergruppe ist. Die Aussage für $n > 0$ erhält man durch Ersetzen von Γ durch $\Gamma^{p^n} = \mathrm{Gal}(K_\infty/K_0)$ und von γ durch γ^{p^n}. $\square$

Korollar 2.47. *Die Gruppe* $\mathrm{Gal}(M_p(K_n)/K_\infty)$ *erhält man aus dem* Λ*-Modul* $\mathcal{X}_\infty$ *als Quotient* $\mathcal{X}_\infty/(\gamma^{p^n}-1)\cdot\mathcal{X}_\infty$.

Mit diesen Vorbereitungen können wir jetzt das schon angekündigte Resultat zeigen:

Satz 2.48. *Falls* K *ein total reeller Zahlkörper ist und* K_∞/K *seine zyklotomische* $\mathbb{Z}_p$*-Erweiterung, ist die Galoisgruppe* $\mathcal{X}_\infty$ *der maximalen außerhalb von* p *unverzweigten* p*-Erweiterung von* K_∞ *ein endlich erzeugter* Λ*-Torsionsmodul.*

Beweis. Aus dem Korollar folgt, dass der Quotient $\mathcal{X}_\infty/(\gamma-1)\cdot\mathcal{X}_\infty$ als $\mathbb{Z}_p$-Modul endlich erzeugt ist, da sogar die Gruppe $\mathrm{Gal}(M_p(K_0)/K_0)$ ein endlich erzeugter $\mathbb{Z}_p$-Modul ist. Nach dem Korollar zum topologischen Nakayama-Lemma ist $\mathcal{X}_\infty$ deshalb als Λ-Modul endlich erzeugt.

Die Gruppe $\mathcal{X}_n = \mathrm{Gal}(M_p(K_n)/K_n) = \mathcal{X}_\infty/(\gamma^{p^n}-1)\cdot\mathcal{X}_\infty$ hat als $\mathbb{Z}_p$-Modul den Rang $1+\delta(K_n)$, wobei die Zahlen $\delta(K_n)$ beschränkt sind (Satz 2.41 bzw. 2.42). Da K nach Voraussetzung total reell ist, gilt auch für alle Zwischenkörper $r_2 = 0$.

Der Struktursatz für endlich erzeugte Λ-Moduln liefert eine exakte Sequenz

$$0 \to K \to \mathcal{X}_\infty \to \Lambda^r \oplus M \to C \to 0$$

mit endlichen Gruppen K und C und einem Λ-Torsionsmodul M. Durch Bildung des Quotienten nach $(\gamma^{p^n}-1)\cdot\mathcal{X}_\infty$ bzw. Tensorieren der Sequenz mit $\Lambda/(\gamma^{p^n}-1)$ erhält man die exakte Sequenz

$$\mathcal{X}_n \to (\Lambda/(\gamma^{p^n}-1))^r \oplus M/(\gamma^{p^n}-1)M \to C\otimes_\Lambda \Lambda/(\gamma^{p^n}-1) \to 0.$$

Da der Term $C\otimes_\Lambda \Lambda/(\gamma^{p^n}-1)$ wieder endlich ist, hat $\mathcal{X}_n$ mindestens so großen $\mathbb{Z}_p$-Rang wie der Summand $(\Lambda/(\gamma^{p^n}-1))^r$. Der Rang dieses Moduls lässt sich leicht berechnen: Als $\mathbb{Z}_p$-Rang von $\Lambda/(\gamma^{p^n}-1)$ erhält man die Zahl p^n, für $(\Lambda/(\gamma^{p^n}-1))^r$ also den Rang rp^n. Da der Rang von $\mathcal{X}_n$ beschränkt ist, sieht man sofort, dass sich als einzige Möglichkeit $r=0$ ergibt, das heißt, $\mathcal{X}_\infty$ ist pseudo-isomorph zu einem Torsionsmodul und damit selbst Torsionsmodul. $\square$

2.10 Das charakteristische Polynom eines Iwasawa-Moduls

Jeder endlich erzeugte Torsionsmodul M über der Iwasawa-Algebra $\Lambda = \mathbb{Z}_p[\![T]\!]$ ist nach den Ergebnissen aus Abschnitt 2.6 bis auf endlichen Kern und Cokern isomorph zu einem Modul der Form

$$\bigoplus_{i=1}^{m} \Lambda/(g_i^{k_i}) \oplus \bigoplus_{j=1}^{n} \Lambda/(p^{\ell_j})$$

mit eindeutig bestimmten irreduziblen Weierstraß-Polynomen $g_i \in \mathbb{Z}_p[T]$ und Zahlen k_i, ℓ_j.

Definition. Das charakteristische Polynom von M ist das Produkt der durch einen solchen Pseudo-Isomorphismus gegebenen Polynome $g_i^{k_i}$.

Jeder der Summanden $\Lambda/(g_i^{k_i})$ ist als $\mathbb{Z}_p$-Modul frei und endlich erzeugt. Bei Tensorieren mit $\mathbb{Q}_p$ werden diese Summanden also zu endlichdimensionalen $\mathbb{Q}_p$-Vektorräumen, und die restlichen Summanden verschwinden. Durch die Λ-Modulstruktur auf M ist eine $\mathbb{Z}_p$-lineare Abbildung $\tau : M \to M$ definiert, die durch Multiplikation mit dem Element $T \in \mathbb{Z}_p[\![T]\!]$ gegeben ist. Diese Abbildung induziert einen Vektorraumendomorphismus des endlichdimensionalen $\mathbb{Q}_p$-Vektorraums $M\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$, dessen charakteristisches Polynom wir mit p_τ bezeichnen.

Satz 2.49. *Die folgenden Polynome über $\mathbb{Q}_p$ stimmen bis auf Einheiten aus $\mathbb{Q}_p[T]$ mit dem charakteristischen Polynom von M überein:*

- $p_\tau(T)$
- $\Delta_0(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$, *der Erzeuger des nullten Fitting-Ideals über* $\mathbb{Q}_p[\![T]\!]$
- $\Delta_0(M)$, *der größte gemeinsame Teiler der Elemente aus dem nullten Fitting-Ideal über* $\mathbb{Z}_p[\![T]\!]$.

Beweis. Durch Tensorieren mit $\mathbb{Q}_p$ erhält man aus dem Pseudo-Isomorphismus

$$M \to \bigoplus \Lambda/(g_i^{k_i}) \oplus \bigoplus \Lambda/(p^{k_j})$$

einen Isomorphismus

$$M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \xrightarrow{\simeq} \bigoplus \mathbb{Q}_p[\![T]\!]/(g_i^{k_i}) = \bigoplus \mathbb{Q}_p[T]/(g_i^{k_i}).$$

Wir können $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ also als endlich erzeugten Modul über dem Polynomring $\mathbb{Q}_p[T]$ auffassen. Sowohl das Element $p_\tau(T)$ als auch der Erzeuger des nullten Fitting-Ideals ergeben sich dann mit Satz 1.4 als Produkt der Polynome $g_i^{k_i}$.

Das nullte Fitting-Ideal $F_0(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ ist das von $F_0(M)$ erzeugte Ideal in $\mathbb{Q}_p[\![T]\!]$, da eine Präsentationsmatrix von M über $\mathbb{Z}_p[\![T]\!]$ auch als Präsentationsmatrix von $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ über $\mathbb{Q}_p[\![T]\!]$ aufgefasst werden kann. Der größte gemeinsame Teiler der Elemente aus $F_0(M)$ ist also ein Erzeuger des nullten Fitting-Ideals von $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. □

Definition. Das charakteristische Polynom des Iwasawa-Moduls $\mathcal{X}_\infty$, den man wie im vorhergehenden Abschnitt aus der maximalen p-verzweigten p-Erweiterung eines total reellen Zahlkörpers K erhält, nennen wir Iwasawa-Zetafunktion. Wir bezeichnen es mit $Z_{K,p}(T)$.

In Abschnitt 2.9 wurde gezeigt, dass $\mathcal{X}_\infty$ tatsächlich ein Λ-Torsionsmodul ist, sodass diese Definition sinnvoll ist. Allgemeiner treffen wir für endlich erzeugte Λ-Moduln die folgende Vereinbarung:

Falls M ein endlich erzeugter Λ-Modul M mit positivem Rang ρ ist, definieren wir das charakteristische Polynom von M als charakteristisches Polynom seines Torsions-Untermoduls. Man erhält es nach Satz 1.5 als größten gemeinsamen Teiler des ρ-ten Fitting-Ideals von M.

2.11 Die Hauptvermutung

Die Vermutung, die als Hauptvermutung der Iwasawatheorie für Zahlkörper bekannt wurde, ist Ende der 60er Jahre von Iwasawa aufgestellt worden und wurde 1984 für abelsche Zahlkörper und 1990 im allgemeinen Fall bewiesen.[2] Der Satz stellt den Zusammenhang her zwischen dem Polynom, das wir Iwasawa-Zetafunktion genannt haben, und den arithmetischen p-adischen Zetafunktionen, die sich durch Interpolation der Dedekind-Zetafunktion ergeben.

Wir stellen hier kurz eine einfache Version der Hauptvermutung vor, um das Objekt „Iwasawa-Zetafunktion“ besser einordnen zu können und eine Antwort auf die Frage zu geben, warum unser Polynom den Namen „Zetafunktion“ trägt. p-adische Zeta- und L-Funktionen werden in den Büchern von Washington [46], Koblitz [20] und Iwasawa [17] behandelt. Eine zusammenfassende Darstellung der Hauptvermutung mit weiteren Referenzen findet man in Kapitel XI, §6 von [33], an dem wir uns hier orientieren.

In diesem Abschnitt bezeichnen wir mit p wieder eine ungerade Primzahl.

[2] Die Bezeichnung „Hauptvermutung“ wird also inzwischen nur noch aus historischen Gründen verwendet.

2.11.1 p-adische Zetafunktionen

Die Riemann'sche Zetafunktion, die für $s \in \mathbb{C}$ mit $\Re(s) > 1$ durch

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prim}} \frac{1}{1 - p^{-s}}$$

gegeben ist, ist bekanntlich eine auf der Menge $\mathbb{C} \backslash \{1\}$ holomorphe Funktion mit einem einfachen Pol bei $s = 1$.

Dass der Versuch, eine p-adische Zetafunktion auf dieselbe Weise durch eine unendliche Summe zu definieren, nicht gelingen kann, sieht man sofort: Im Körper $\mathbb{Q}_p$ konvergiert eine Reihe genau dann, wenn die zugehörige Folge gegen 0 konvergiert. Für die Riemann'sche Zetafunktion stellt man fest, dass die Reihe für $s \in \mathbb{N}$ p-adisch nicht konvergiert, da die Summanden $(p^k)^{-s}$ jeweils Norm p^{sk} haben und alle anderen Summanden die Norm 1 haben.

Selbst wenn man die Summanden für die Vielfachen von p, deren p-adische Bewertung beliebig groß wird, entfernt, ist die Definition einer Zetafunktion als unendliche Summe im p-adischen Fall also nicht möglich.

Stattdessen fanden T. Kubota und H.-W. Leopoldt in den 60er Jahren heraus, dass gewisse Kongruenzrelationen, die schon von Kummer entdeckt worden waren, es erlauben, die Riemann'sche Zetafunktion an den negativen ganzzahligen Stellen p-adisch zu interpolieren, wenn man die oben genannten „großen“ Summanden entfernt, also nur die Funktion

$$\sum_{p \nmid n} \frac{1}{n^s} = \prod_{q \neq p} \frac{1}{1 - q^{-s}} = \zeta(s) \cdot (1 - p^{-s})$$

betrachtet.

Die Werte der Zetafunktion bei den negativen ganzen Zahlen lassen sich durch die Bernoulli-Zahlen ausdrücken:

$$\zeta(1-k) = -\frac{B_k}{k},$$

wobei die k-te Bernoulli-Zahl B_k durch die Potenzreihe

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \cdot \frac{t^k}{k!}$$

definiert wird. Diese Zahlen sind also insbesondere rationale Zahlen. Sie erfüllen die folgenden Kongruenzrelationen ([20], II.6 Th. 7):

Satz 2.50 (Kummer-Kongruenzen). *Falls $p - 1 \nmid k$ und $k' \equiv k \mod (p-1)p^N$, gilt*

$$(1 - p^{-(1-k)}) \cdot \frac{B_k}{k} \equiv (1 - p^{-(1-k')}) \cdot \frac{B_{k'}}{k'} \mod p^{N+1}.$$

Zwei solche Zahlen k und k' liegen p-adisch nah beieinander, und der Satz sagt aus, dass dasselbe für die Werte der modifizierten Zetafunktion bei k und k' gilt. Er liefert also eine erste notwendige Bedingung für die Existenz einer stetigen Fortsetzung dieser Funktion auf $\mathbb{Z}_p$.

p-adische Zetafunktionen kann man nicht nur aus der Riemann'schen Zetafunktion gewinnen, sondern auch aus den Verallgemeinerungen dieser Funktion. Jedem Zahlkörper K wird die durch

$$\zeta_K(s) = \sum_{\mathfrak{a}} N\mathfrak{a}^{-s} = \prod_{\mathfrak{p}} \frac{1}{1 - N\mathfrak{p}^{-s}}$$

definierte Dedekind-Zetafunktion zugeordnet, wobei $\mathfrak{a}$ die Ideale von $\mathcal{O}_K$ durchläuft und $\mathfrak{p}$ entsprechend die Primideale. Die Riemann'sche Zetafunktion ergibt sich hier im Spezialfall $K = \mathbb{Q}$. Die Reihen konvergieren absolut und gleichmäßig im Bereich $\Re(s) \geq 1 + \delta$ für jedes $\delta > 0$ und lassen sich meromorph auf $\mathbb{C}$ fortsetzen. Wie im Fall der Riemann'schen Zetafunktion ist bekannt, dass $\zeta_K(1-n)$ für jede natürliche Zahl n eine rationale Zahl ist und dass gewisse Kongruenzrelationen erfüllt sind, die auch hier eine Interpolation erlauben:

Satz 2.51. *Sei K ein total reeller Zahlkörper mit Dedekind-Zetafunktion ζ_K. Dann gibt es eine eindeutig bestimmte stetige Funktion $\zeta_{K,p} : \mathbb{Z}_p \backslash \{1\} \to \mathbb{Q}_p$, die für alle Vielfachen n von $d = [K(\mu_{2p}) : K]$ die Gleichung*

$$\zeta_{K,p}(1-n) = \zeta_K(1-n) \prod_{\mathfrak{p}|p} (1 - N\mathfrak{p}^{-(1-n)})$$

erfüllt.

Die Funktion $\zeta_{K,p}(s)$ ist p-adisch analytisch und hat höchstens einen einfachen Pol an der Stelle $s = 1$.

2.11.2 Die Aussage der Hauptvermutung von Iwasawa

Um die Hauptvermutung zu formulieren, betrachten wir wieder einen total reellen Zahlkörper K und seine zyklotomische $\mathbb{Z}_p$-Erweiterung K_∞.

Die Automorphismengruppe von μ_{p^∞} ist kanonisch isomorph zu der Gruppe der Einheiten in $\mathbb{Z}_p$; der Isomorphismus

$$f : \mathrm{Aut}(\mu_{p^\infty}) \xrightarrow{\simeq} \mathbb{Z}_p^* = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^*$$

ist durch die folgenden Homomorphismen $f_n : \mathrm{Aut}(\mu_{p^\infty}) \to (\mathbb{Z}/p^n\mathbb{Z})^*$ gegeben:

Falls $\varphi \in \mathrm{Aut}(\mu_{p^\infty})$ eine primitive p^n-te Einheitswurzel ζ_n auf ζ_n^α abbildet, setzt man $f_n(\varphi) = \alpha \in (\mathbb{Z}/p^n\mathbb{Z})^*$. Diese Homomorphismen setzen sich offenbar zu einem Homomorphismus von $\mathrm{Aut}(\mu_{p^\infty})$ nach $\mathbb{Z}_p^*$ zusammen. Die Umkehrabbildung g kann durch die Gleichung $g(a)(\zeta_n) = \zeta_n(\overline{a})$ beschrieben werden, wobei $\overline{a}$ die Restklasse von a modulo $p^n\mathbb{Z}_p$ bezeichnet. Also ist f ein Isomorphismus.

Sei nun

$$\kappa : \Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathrm{Gal}(K(\mu_{p^\infty})/K(\mu_p)) \hookrightarrow \mathrm{Gal}(K(\mu_{p^\infty})/K) \to \mathrm{Aut}(\mu_{p^\infty}) \cong \mathbb{Z}_p^*$$

die Abbildung, die man durch die Operation der Galoisgruppe $\mathrm{Gal}(K(\mu_{p^\infty})/K)$ auf μ_{p^∞} erhält.

Wir wählen einen Erzeuger γ von Γ und bezeichnen sein Bild in $\mathbb{Z}_p^*$ unter der Abbildung κ mit q.

Satz 2.52. *Es gibt eine eindeutig bestimmte Potenzreihe $G_{K,p} \in \mathbb{Z}_p[\![T]\!]$, sodass*

$$\zeta_{K,p}(s) = \frac{G_{K,p}(q^{1-s} - 1)}{q^{1-s} - 1}.$$

Da bei $s = 1$ eine einfache Polstelle von $\zeta_{K,p}$ vermutet wird, entwickelt man die Funktion an dieser Stelle, um eine Potenzreihe $G_{K,p}$ zu erhalten.

Bemerkung. Für ein Schema X von endlichem Typ über einem endlichen Körper $\mathbb{F}_q$ definiert man einerseits $Z(X,t) = \exp \sum_{r=1}^{\infty} N_r \frac{t^r}{r}$, wobei N_r die Anzahl der Punkte mit Koordinaten in $\mathbb{F}_{q^r}$ bezeichnet. Andererseits ist die Zetafunktion von X durch $\zeta(X,s) = \prod \frac{1}{1-N(x)^{-s}}$ gegeben, wobei x die abgeschlossenen Punkte durchläuft und $N(x)$ die Anzahl der Punkte im Restklassenkörper bezeichnet. Zwischen diesen Funktionen besteht der Zusammenhang $Z(X,q^{-s}) = \zeta(X,s)$, die erste Funktion ergibt sich also aus der zweiten einfach durch eine Variablensubstitution und es handelt sich im Prinzip um dasselbe Objekt.

Die Rolle der Zahl q, also der Anzahl der Elemente im Grundkörper, übernimmt in unserem Fall ein Erzeuger der Galoisgruppe $\mathrm{Gal}(K_\infty/K)$, aufgefasst als Element der additiven Gruppe $\mathbb{Z}_p$.

Satz 2.53 (Hauptvermutung). *Sei K ein total reeller Zahlkörper, $G_{K,p}(T)$ die Potenzreihe, die sich wie oben aus der p-adischen Zetafunktion $\zeta_{K,p}(s)$ ergibt und $Z_{K,p}(T)$ das charakteristische Polynom des Iwasawa-Moduls $\mathcal{X}_\infty$. Dann gibt es eine Einheit $u(T) \in \mathbb{Z}_p[\![T]\!]^*$, sodass*

$$G_{K,p}(T) = u(T) \cdot p^{\mu(\mathcal{X}_\infty)} \cdot Z_{K,p}(T).$$

Dieser Satz wurde zunächst für abelsche Zahlkörper bewiesen, für die man sogar weiß, dass die μ-Invariante $\mu(\mathcal{X}_\infty)$ verschwindet. Für allgemeine total reelle Zahlkörper ist die Aussage der Hauptvermutung seit 1990 bekannt, und es wird vermutet, dass μ im allgemeinen Fall ebenfalls verschwindet.

Bemerkung. 1. Das Element $Z_{K,p}(T)$ hängt von der Wahl eines Erzeugers $\gamma \in \Gamma$ ab, der den Isomorphismus $\mathbb{Z}_p[\![\Gamma]\!] \to \mathbb{Z}_p[\![T]\!]$ bestimmt. Die Aussage der Hauptvermutung ist allerdings invariant unter einer Änderung dieses Erzeugers:

Sei $\gamma' = \gamma^\alpha$ mit $\alpha \in \mathbb{Z}_p^*$ ein anderer Erzeuger von Γ. Unter dem Isomorphismus $\gamma \mapsto T+1$ wird γ' auf $(T+1)^\alpha$ abgebildet, die Variable T wird also durch $(T+1)^\alpha - 1$ ersetzt, und wegen $\kappa(\gamma') = \kappa(\gamma)^\alpha$ wird gleichzeitig q durch q^α ersetzt.

Zwischen den Potenzreihen $G_{K,p}(T)$ und $G'_{K,p}(T)$, die man durch die Wahl von γ bzw. γ' aus Satz 2.52 erhält, besteht der Zusammenhang

$$\frac{G_{K,p}(q^{1-s}-1)}{q^{1-s}-1} = \frac{G'_{K,p}(q^{(1-s)\alpha}-1)}{q^{(1-s)\alpha}-1},$$

und durch Einsetzen von T für $q^{1-s} - 1$ erhält man daraus

$$\frac{G_{K,p}(T)}{T} = \frac{G'_{K,p}((T+1)^\alpha - 1)}{(T+1)^\alpha - 1}.$$

Da die Polynome $Z_{K,p}(T)$ und $Z'_{K,p}((T+1)^\alpha - 1)$ bis auf Multiplikation mit einer Einheit übereinstimmen und auch die Elemente T und $(T+1)^\alpha - 1$ sich nur um Multiplikation mit einer Einheit aus $\mathbb{Z}_p[\![T]\!]$ unterscheiden, bleibt die Aussage der Hauptvermutung im zweiten Fall äquivalent.

2. In [2] wird das als Iwasawa-Zetafunktion bezeichnete Objekt für einen Zahlkörper K und eine Primzahl p folgendermaßen eingeführt: Für den wie in Abschnitt 2.9 definierten

Modul $\mathcal{X}_\infty$ gibt es einen Pseudo-Isomorphismus

$$\mathcal{X}_\infty \to \bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T))^{n_j}$$

mit irreduziblen Weierstraß-Polynomen $f_j(T)$. Sei $f(T)$ das Produkt der Polynome $f_j(T)$ und $\mu = \sum_i m_i$ die μ-Invariante von $\mathcal{X}_\infty$. Dann wird

$$\zeta_I(s) = \frac{p^\mu f(q^{1-s} - 1)}{1 - q^{1-s}}$$

Iwasawa-Zetafunktion von K genannt. Im Wesentlichen ist ζ_I bis auf den Übergang von T zu s dasselbe Objekt wie das Polynom $Z_{K,p}(T)$, dem wir im vorhergehenden Abschnitt denselben Namen gegeben haben.

Nach der Hauptvermutung stimmt die so definierte Funktion bis auf eine Einheit mit der p-adischen Zetafunktion von K überein:

$$\zeta_I(s) = u(q^{1-s} - 1) \cdot \zeta_{K,p}(s)$$

mit einem Element $u(T) \in \mathbb{Z}_p[\![T]\!]^*$. Ähnlich wie das Polynom $Z_{K,p}$ kann man ζ_I als „rationalen Teil“ der p-adischen Zetafunktion auffassen. In dieser Form hängt die Zetafunktion nicht von der Wahl eines Erzeugers ab.

3 Algebraische Fundamentalgruppe

In diesem Kapitel wird Grothendiecks Konstruktion einer Fundamentalgruppe für Schemata vorgestellt und die Gruppe in einem für uns interessanten Spezialfall berechnet. Das Ergebnis liefert die Grundlage für die Gegenüberstellung von Topologie und Zahlentheorie im nächsten Kapitel.

3.1 Motivation: Die topologische Fundamentalgruppe

Die Fundamentalgruppe eines topologischen Raums X wird üblicherweise definiert als die Gruppe der Homotopieklassen von Schleifen $S^1 \to X$ mit fest gewähltem Basispunkt, wobei sich die Gruppenstruktur durch Zusammensetzen von Schleifen ergibt.

Falls X ein wegzusammenhängender, lokal wegzusammenhängender, semilokal einfach zusammenhängender topologischer Raum ist, kann man mit Hilfe der universellen Überlagerung eine weitere Beschreibung der Fundamentalgruppe finden, die den Vorteil hat, dass sie sich auf die algebraische Geometrie übertragen lässt.

Die universelle Überlagerung $(\tilde{X}, \tilde{x}) \to (X, x)$ des Raums X mit Basispunkt x kann durch die folgende universelle Eigenschaft charakterisiert werden:

Für jede zusammenhängende Überlagerung $Y \xrightarrow{p} X$ und jeden Punkt $y \in p^{-1}(x)$ gibt es einen eindeutigen Morphismus von Überlagerungen $\tilde{X} \to Y$, der $\tilde{x}$ auf y abbildet. Anders ausgedrückt gibt es einen funktoriellen Isomorphismus

$$p^{-1}(x) \xrightarrow{\simeq} \mathrm{Hom}_X(\tilde{X}, Y).$$

Die Automorphismengruppe der universellen Überlagerung über X ist kanonisch isomorph zu ihrer Decktransformationsgruppe, und diese ist wiederum kanonisch isomorph zur Fundamentalgruppe des Raums X. Insgesamt kann man $\pi_1(X, x)$ definieren als Automorphismengruppe desjenigen Objekts in der Kategorie $\mathrm{Cov}_{(X,x)}$ der zusammenhängenden Überlagerungen von X, das den Funktor

$$\begin{array}{rrcl} F : & \mathrm{Cov}_{(X,x)} & \to & \mathit{Ens} \\ & (Y \xrightarrow{p} X) & \mapsto & p^{-1}(x) \end{array}$$

(co-)darstellt.

3.2 Stetige Abbildungen und lokale Homöomorphismen

Um Überlagerungen auf die algebraische Geometrie zu übertragen, braucht man Entsprechungen für Begriffe wie Stetigkeit und lokale Homöomorphismen. Für beide Eigenschaften von Abbildungen liefert die Zariski-Topologie keine geeigneten Ergebnisse. Stattdessen hat sich herausgebildet, dass die „richtigen“ Abbildungen durch flache und unverzweigte Morphismen gegeben sind. Die zwei folgenden kurzen Beispiele sollen diese Wahl motivieren:

Eine Familie von Schemata ist gegeben durch einen Morphismus $\pi : X \to B$ von Schemata. Die einzelnen Schemata in der Familie sind dann die Fasern des Morphismus. Die Familie heißt flach, wenn der Morphismus π flach ist. Flache Familien haben die Eigenschaft, dass die Fasern in einem gewissen Sinn „stetig variieren“. Als **Beispiel** nennen wir den folgenden Satz ([14], Chapter III, Corollary 9.6):

Satz 3.1. *Sei $f : X \to Y$ ein flacher Morphismus von Schemata X, Y von endlichem Typ über dem Körper k und Y außerdem irreduzibel. Falls jede irreduzible Komponente von X die Dimension $n + \dim Y$ hat, gilt für jeden Punkt $y \in Y$: Jede irreduzible Komponente der Faser $X_y = X \times_Y \operatorname{Spec} \kappa(y)$ hat die Dimension n.*

Unverzweigte Morphismen kann man sich als Analogon zu lokal trivialen Abbildungen vorstellen:

Beispiel 3.2. Sei k ein algebraisch abgeschlossener Körper und $\varphi : k[T] \to k[X]$ die Abbildung $T \mapsto X^2$. Die abgeschlossenen Punkte von $k[T]$ entsprechen Idealen der Form $(T - a)$, und die Urbilder eines Punkts $(T - a^2)$ unter der Abbildung $\operatorname{Spec} \varphi : \operatorname{Spec} k[X] \to \operatorname{Spec} k[T]$ sind die Ideale $(X - a)$ und $(X + a)$, falls $a \neq 0$, sonst nur der Punkt (X). Wir stellen uns diese Situation vor wie in Abbildung 11 dargestellt.

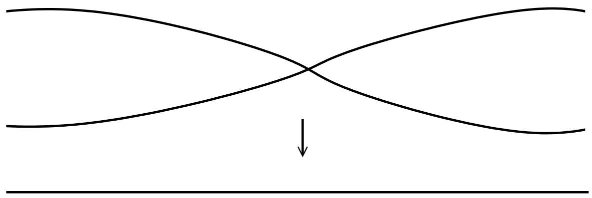


Abbildung 11: Verzweigung

Hier sieht der Morphismus bei allen Punkten aus $\operatorname{Spec} k[X]$ außer (X) aus wie ein lokaler Homöomorphismus, auch wenn die Zariski-Topologie – wie schon bemerkt – nicht die geeignete Topologie ist, da es keine Zariski-Umgebung eines Punktes $(X - a)$ gibt, sodass die Einschränkung injektiv ist. Der einzige Punkt, bei dem hier Verzweigung auftritt, ist der Punkt (X).

3.3 Unverzweigte und étale Morphismen

In diesem Abschnitt, der die für uns wichtigen Aussagen aus [29], § I.3 enthält, definieren wir unverzweigte und étale Morphismen und stellen einige Eigenschaften zusammen, um im nächsten Abschnitt die étale Fundamentalgruppe einführen zu können. Wir nehmen im Folgenden an, dass alle Ringe noethersch sind und alle Morphismen lokal von endlichem Typ.

Definition. Seien $(A, \mathfrak{m}_A)$ und $(B, \mathfrak{m}_B)$ lokale Ringe und $f : A \to B$ ein lokaler Homomorphismus. f heißt unverzweigt, falls $f(\mathfrak{m}_A)$ das maximale Ideal von B erzeugt und falls die Körpererweiterung $A/\mathfrak{m}_A \subset B/\mathfrak{m}_B$ endlich und separabel ist.

Ein Homomorphismus $f : A \to B$ zwischen beliebigen Ringen heißt unverzweigt, falls für jedes Primideal $\mathfrak{q} \subset B$ die Lokalisierung $A_{f^{-1}(\mathfrak{q})} \to B_{\mathfrak{q}}$ unverzweigt ist.

Bemerkung. Für die Ganzheitsringe von Zahlkörpern stimmt diese Definition von „unverzweigt bei einem Primideal $\mathfrak{p}$“ mit der Definition überein, die man aus der Zahlentheorie kennt.

Satz 3.3. *Eine endlich erzeugte Algebra A über einem Körper K ist genau dann unverzweigt über K, wenn sie endliches Produkt von endlichen separablen Körpererweiterungen von K ist.*

Beweis. Jede endlich erzeugte Algebra dieser Form ist offenbar unverzweigt über k. Umgekehrt: Sei A unverzweigt über K. Da das maximale Ideal jeder Lokalisierung $A_{\mathfrak{p}}$ von A von

(0) erzeugt wird, ist jede Lokalisierung von A nach einem Primideal ein Körper, und alle Primideale sind damit maximal.

Sei N das Nilradikal von A. Dann ist $N_\mathfrak{p} = 0$ für alle Primideale $\mathfrak{p}$, also $N = 0$. Nach dem chinesischen Restsatz ist $A = \Pi A/\mathfrak{p} = \Pi K_i$ ein Produkt von Körpern.

Für die Homomorphismen $K \to K_i$ folgt nun sofort aus der Definition, dass sie genau dann unverzweigt sind, wenn K_i separabel über K ist. □

Definition. Sei $f : Y \to X$ ein Morphismus von Schemata von endlichem Typ. f heißt unverzweigt bei $y \in Y$, wenn der lokale Ringhomomorphismus $\mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ unverzweigt ist. Der Morphismus heißt unverzweigt, wenn er an jedem Punkt unverzweigt ist.

Bemerkung. Ein Morphismus zwischen affinen Schemata ist also genau dann unverzweigt, wenn der entsprechende Ringhomomorphismus unverzweigt ist.

Satz 3.4. *Ein Morphismus $f : Y \to X$ von endlichem Typ ist genau dann unverzweigt, wenn die Faser $Y_x \to \operatorname{Spec} \kappa(x)$ für jedes $x \in X$ unverzweigt ist.*

Beweis. Für den lokalen Ring $\mathcal{O}_{Y_x,y}$ an dem Punkt, der einem über x liegenden Punkt $y \in Y$ entspricht, gilt $\mathcal{O}_{Y_x,y} \cong \mathcal{O}_{Y,y}/\mathfrak{m}_{X,x}\mathcal{O}_{Y,y}$. Die Ringerweiterung $\kappa(x) \to \mathcal{O}_{Y_x,y}$ ist genau dann unverzweigt, wenn $\mathcal{O}_{X,x} \to \mathcal{O}_{Y,y}$ unverzweigt ist. □

Satz 3.5. *a) Offene Immersionen sind unverzweigt.*

b) Zusammensetzungen von unverzweigten Morphismen sind unverzweigt.

c) Jeder Basiswechsel eines unverzweigten Morphismus ist unverzweigt.

Beweis. Die ersten beiden Behauptungen sind klar. Für die dritte Behauptung reicht es nach Satz 3.4, einen Morphismus der Form $X \to \operatorname{Spec} K$ und den Basiswechsel mit $\operatorname{Spec} L \to \operatorname{Spec} K$ für eine beliebige Körpererweiterung $L \supset K$ zu betrachten. Außerdem können wir annehmen, dass X affin ist.

Falls $X = \operatorname{Spec} A$, ist A nach Satz 3.3 endliches Produkt von endlichen separablen Körpererweiterungen K_i von K. Es gilt also $A = \Pi K[T]/(f_i(T))$ mit irreduziblen Polynomen f_i, sodass $(f_i, f_i') = 1$. Dann ist $L \otimes_K A = \Pi L[T]/(f_i(T))$, und jeder Faktor ist wieder Produkt von endlich vielen separablen Körpererweiterungen von L. Damit ist $L \otimes_K A$ separable L-Algebra. □

Satz 3.6. *Sei $f : Y \to X$ von endlichem Typ. f ist genau dann unverzweigt, wenn der Diagonalmorphismus $\Delta : Y \to Y \times_X Y$ eine offene Immersion ist.*

Beweis. Wir benötigen nur die Richtung „ $\Rightarrow$ “; ein Beweis für die andere Implikation findet sich in [29], Proposition 3.5.

Sei f also unverzweigt. Da die Diagonalabbildung immer lokal abgeschlossene Immersion ist, können wir eine offene Teilmenge W von $Y \times_X Y$ wählen, sodass $i : Y \to W$ eine abgeschlossene Immersion ist. Sei $\mathcal{I}$ der Kern der Abbildung $i^\sharp : \mathcal{O}_W \to i_*\mathcal{O}_Y$. Um zu zeigen, dass die Diagonale eine offene Immersion ist, reicht es zu zeigen, dass die lokalen Ringe $\mathcal{I}_y$ für alle Punkte y im Bild von Y verschwinden, da dann $\mathcal{I} = 0$ auf einer offenen Teilmenge V von W, die Y enthält. Daraus folgt dann $Y = V$ als Unterschemata von W, und Y ist offenes Unterschema von W und damit auch von $Y \times_X Y$.

Die Garbe $\mathcal{I}/\mathcal{I}^2$ ist als Garbe auf Y isomorph zu der Garbe $\Omega_{Y/X}$ der Differentiale auf Y.[3] Um zu zeigen, dass $\mathcal{I}_y$ verschwindet, reicht es nach Nakayama, zu zeigen, dass $\mathcal{I}_y/\mathcal{I}_y^2 = (\mathcal{I}/\mathcal{I}^2)_y = 0$.

Da man die Garbe der Differentiale erhält, wenn man die entsprechenden Garben für affine Überdeckungen von X und Y zusammenklebt, können wir annehmen, dass $X = \operatorname{Spec} A$ und $Y = \operatorname{Spec} B$ affin sind und $\Omega_{Y/X} = \widetilde{\Omega_{B/A}}$. Sei $(\Omega_{Y/X})_y$ die Lokalisierung am Punkt y, der dem Primideal $\mathfrak{q}$ von B entspricht, und $\mathfrak{p}$ das zugehörige Primideal in A. Dann ist $(\Omega_{Y/X})_y \cong (\Omega_{B/A})_\mathfrak{q} \cong \Omega_{B_\mathfrak{q}/A} = \Omega_{B_\mathfrak{q}/A_\mathfrak{p}}$.

Seien $K = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ und $L = B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q}$ die Restklassenkörper in den Punkten $[\mathfrak{p}]$ und $[\mathfrak{q}]$.

Es gilt $L = K \otimes_{A_\mathfrak{p}} B_\mathfrak{q}$, da $A_\mathfrak{p} \to B_\mathfrak{q}$ unverzweigt ist, und $\Omega_{L/K} = \Omega_{B_\mathfrak{q}/A_\mathfrak{p}} \otimes_{B_\mathfrak{q}} L$. Dieser Modul verschwindet, da die Körpererweiterung $L \supset K$ endlich und separabel ist. Damit gilt nach Nakayama auch $\Omega_{B_\mathfrak{q}/A_\mathfrak{p}} = 0$. □

Definition. Ein Morphismus von endlichem Typ heißt étale, wenn er flach und unverzweigt ist. Er heißt étale Überlagerung, wenn er zusätzlich endlich ist.

Bemerkung. Für zwei S-Schemata X und Y und einen S-Morphismus $f : X \to Y$ ist der Graph von f die Abbildung

$$\Gamma_f : X \xrightarrow{1\times f} X \times_S Y,$$

die man auch durch Basiswechsel mit f aus der Diagonalabbildung $\Delta : Y \to Y \times_S Y$ erhält.

Satz 3.7. *Seien $f : X \to S$ und $g : Y \to X$ zwei Morphismen von endlichem Typ. Falls f unverzweigt ist und die Zusammensetzung von f und g étale, so ist auch g étale.*

Beweis. Der Morphismus g setzt sich zusammen aus dem Graph Γ_g und der Projektion $p_2 : Y \times_S X \to X$ auf den zweiten Faktor. Nach Satz 3.6 ist die Diagonalabbildung $\Delta_{X/S} : X \to X \times_S X$ offene Immersion, also étale. Der Morphismus Γ_g ergibt sich durch Basiswechsel von $\Delta_{X/S}$ mit $g \times 1 : Y \times_S X \to X \times_S X$ und ist damit étale. Genauso ist die Projektion p_2 als Basiswechsel des étalen Morphismus $fg : Y \to S$ étale. Daraus folgt die Behauptung. □

Satz 3.8. *Eine abgeschlossene Immersion ist genau dann flach, wenn sie gleichzeitig offene Immersion ist.*

Beweis. [29], Chapter I, Proposition 3.10. □

Satz 3.9. *Sei X zusammenhängend und $f : Y \to X$ étale und separiert. Dann ist jeder Schnitt von f ein Isomorphismus auf eine Zusammenhangskomponente von Y. Insbesondere ist ein Schnitt von f festgelegt durch seinen Wert an einem Punkt.*

Beweis. Sei s ein Schnitt von f, also $fs = 1$. Dann ist s abgeschlossene Immersion, denn s ergibt sich aus der abgeschlossenen Immersion $\Delta : Y \to Y \times_X Y$ durch Basiswechsel mit $s \times 1$. Nach Satz 3.7 ist s damit étale, also mit Satz 3.8 gleichzeitig abgeschlossene und offene Immersion. □

Die folgende Eigenschaft von étalen Morphismen erinnert an die Überlagerungen, die wir aus der Topologie kennen:

[3]Einen Abschnitt über Garben von Differentialen findet man in [14], II.8

Korollar 3.10. *Seien Y_1 und Y_2 zwei separierte étale X-Schemata und Y_1 außerdem zusammenhängend. Falls zwei Morphismen $f, g : Y_1 \to Y_2$ an einem Punkt $y \in Y_1$ übereinstimmen, sodass auch die Abbildungen zwischen den Restklassenkörpern an den Punkten y und $f(y)$ übereinstimmen, gilt $f = g$.*

Beweis. Sei $p_1 : Y_1 \times_X Y_2 \to Y_1$ die Projektion auf die erste Komponente. Dann sind durch die Graphen $\Gamma_f, \Gamma_g : Y_1 \to Y_1 \times_X Y_2$ zwei Schnitte von p_1 gegeben, die an einem Punkt übereinstimmen. Der Morphismus p_1 ist als Basiswechsel von $Y_2 \to X$ étale, und damit folgt aus dem vorherigen Satz $\Gamma_f = \Gamma_g$. Die Morphismen f bzw. g ergeben sich aus dem Graphen durch Zusammensetzen mit der Projektion $p_2 : Y_1 \times_X Y_2 \to Y_2$ auf die zweite Komponente, also gilt damit auch $f = g$. □

3.4 Definition der Fundamentalgruppe

Einen kurzen Abschnitt über die Fundamentalgruppe findet man im Buch von Milne [29], Chapter I, §5, an dem wir uns hier orientieren; eine vollständige Darstellung mit Beweis gibt es in [30] und natürlich in [13].

Sei X ein zusammenhängendes Schema und $\overline{x}$ ein geometrischer Punkt von X, d. h. ein Morphismus $\operatorname{Spec} K \to X$ mit einem separabel algebraisch abgeschlossenen Körper K. Ein geometrischer Punkt ist mit anderen Worten ein Punkt x von X zusammen mit einer Einbettung $\mathcal{O}_{X,x}/\mathfrak{m}_{X,x} \to K$. Wir bezeichnen mit FEt/X die Kategorie der étalen Überlagerungen $Y \to X$ und definieren einen Funktor $F : \mathrm{FEt}/X \to \mathit{Ens}$ durch $F(Y) = \operatorname{Hom}_X(\overline{x}, Y)$. Ein Element aus $F(Y)$ ist ein Punkt $y \in Y$ über x zusammen mit einem $\kappa(x)$-Homomorphismus $\kappa(y) \to \kappa(\overline{x}) = K$.

Für ein Objekt $Y \in \mathrm{FEt}/X$ sei $\operatorname{Aut}_X(Y)$ die Gruppe von X-Automorphismen von Y, die von rechts auf Y operiert. Die Gruppe operiert dann ebenfalls von rechts auf $F(Y)$. Falls Y zusammenhängend ist, ist die Abbildung $\operatorname{Aut}_X(Y) \to F(Y)$, $\sigma \mapsto \sigma \circ g$, nach Korollar 3.10 für jedes Element $g \in F(Y)$ injektiv.

Definition. Ein zusammenhängendes Schema Y aus FEt/X heißt galoissch über X, wenn $\operatorname{Aut}_X(Y)$ transitiv auf $F(Y)$ operiert. Für jedes $g \in F(Y)$ ist die durch $\operatorname{Aut}_X(Y) \to F(Y)$, $\sigma \mapsto \sigma \circ g$ definierte Abbildung in diesem Fall also bijektiv.

Definition. Sei $\mathcal{C}$ eine Kategorie und $\mathcal{G} : \mathcal{C} \to \mathit{Ens}$ ein Funktor. Dann heißt $\mathcal{G}$ pro-darstellbar, wenn ein projektives System $(X_i, \varphi_{ij})_{i \in I}$ in $\mathcal{C}$ mit Objekten $f_i \in \mathcal{G}(X_i)$ für jedes i existiert, sodass gilt

- $f_i = \mathcal{G}(\varphi_{ij})(f_j)$ für $i \leq j$
- Für jedes Objekt Z aus $\mathcal{C}$ ist die natürliche Abbildung

$$\varinjlim \operatorname{Hom}_{\mathcal{C}}(X_i, Z) \to \mathcal{G}(Z)$$

  bijektiv.

Satz 3.11. *Der Funktor F ist pro-darstellbar.*

Wir können sogar ein projektives System (X_i, φ_{ij}) in FEt/X angeben, das den Funktor darstellt: Als Objekte X_i wählt man aus jeder Isomorphieklasse von galoisschen étalen Überlagerungen von X einen Vertreter aus. Für jedes X_i wählt man wiederum einen geometrischen

Punkt f_i aus $F(X_i)$. Die Ordnung auf der Indexmenge I ergibt sich nun von allein: Falls es einen Morphismus $\varphi_{ij} : X_j \to X_i$ gibt, der verträglich mit der Wahl der geometrischen Punkte ist, also für den $f_i = \varphi_{ij} \circ f_j$, ist dieser Morphismus eindeutig bestimmt. In diesem Fall soll also $i \leq j$ gelten.

Die Objekte X_i bilden zusammen mit den Morphismen φ_{ij}, die sich so ergeben, ein projektives System, durch das der Funktor F dargestellt wird. Zu je zwei Objekten X_i und X_j ist $X_k = X_i \times_X X_j$ ebenfalls galoissche étale Überlagerung mit durch die Projektionen gegebenem geometrischen Punkt. Durch das Faserprodukt erhält man also einen Index $k \in I$ mit $k \geq i$ und $k \geq j$.

Es gibt im Allgemeinen kein Objekt in FEt/X, das den Funktor F darstellt, aber der Satz sagt uns, dass F immerhin pro-darstellbar ist. Als Fundamentalgruppe wählen wir also statt der Automorphismengruppe eines darstellenden Objekts für F die Automorphismengruppe dieses projektiven Systems:

Für $i \leq j$ können wir eine Abbildung $\psi_{ij} : \mathrm{Aut}_X(X_j) \to \mathrm{Aut}_X(X_i)$ definieren durch $\psi_{ij}(\sigma) \circ f_i = \varphi_{ij} \circ \sigma \circ f_j$ für $\sigma \in \mathrm{Aut}_X(X_j)$. Durch diese Angaben sind die Abbildungen eindeutig definiert und existieren, da die Objekte X_i als galoissch gewählt wurden.

Das folgende Diagramm ist also für alle i, j kommutativ,

$$\begin{array}{ccc} X_i & \xrightarrow{\psi_{ij}(\sigma)} & X_i \\ {\scriptstyle \varphi_{ij}}\uparrow & & \uparrow{\scriptstyle \varphi_{ij}} \\ X_j & \xrightarrow{\sigma} & X_j \end{array}$$

und die Abbildungen sind tatsächlich Gruppenhomomorphismen.

Definition. Die algebraische Fundamentalgruppe von X ist definiert als der Limes

$$\pi_1(X, \overline{x}) = \varprojlim \mathrm{Aut}_X(X_i)$$

mit den Übergangsabbildungen ψ_{ij}.

3.5 Etale Überlagerungen von normalen Schemata

Die Fundamentalgruppe, die uns interessieren wird, ist die des affinen Schemas $\mathrm{Spec}\,\mathbb{Z}\backslash\{(p)\}$. Deshalb überlegen wir uns zunächst etwas allgemeiner, was das Ergebnis im Fall eines normalen Schemas ist.

Beweise für die folgenden zwei Sätze gibt es in [36], Chapitre IV, Corollaire 2 bzw. in [29], Proposition 3.17. Einen Abschnitt über étale Überlagerungen von normalen Schemata findet man in SGA 1 ([13], §I.10).

Satz 3.12 (Spezialfall von Zariskis Hauptsatz für affine Schemata). *Sei B eine quasi-endliche A-Algebra, über jedem Primideal von A liegen also nur endlich viele Primideale von B. Sei A' der ganze Abschluss von A in B. Dann ist die Abbildung $\mathrm{Spec}\,B \to \mathrm{Spec}\,A'$ eine offene Immersion.*

Satz 3.13. *Sei $f : Y \to X$ étale. Falls X ein normales Schema ist, ist auch Y normal.*

Satz 3.14. *Die zusammenhängenden étalen Überlagerungen eines zusammenhängenden normalen Schemas X mit Funktionenkörper K sind genau die Normalisierungen von X in den Körpern L, sodass L endliche separable Körpererweiterung von K ist und die Normalisierung unverzweigt über X ist.*

Beweis. Wir brauchen den Satz nur für den Fall, dass X affin ist und beweisen deshalb nur diesen Spezialfall. Die allgemeine Aussage findet man in [13], Corollaire 10.2 in Kapitel I.

Falls $X = \operatorname{Spec} A$, ist $Y = \operatorname{Spec} B$ ebenfalls affin mit einer endlichen A-Algebra B. Nach Satz 3.12 ist Y mit den Bezeichnungen aus diesem Satz ein offenes Unterschema von $\operatorname{Spec} A'$. Da Y auch endlich über $\operatorname{Spec} A'$ ist, ist der Morphismus $Y \to \operatorname{Spec} A'$ abgeschlossen. Y ist also ein irreduzibles Unterschema von $\operatorname{Spec} A'$. $\operatorname{Spec} B$ ist nach Satz 3.13 normal und damit ist B nullteilerfrei, sodass auch A' nullteilerfrei und $\operatorname{Spec} A'$ deshalb selbst irreduzibel ist. Damit gilt $Y = \operatorname{Spec} A'$.

Umgekehrt müssen wir zeigen, dass diese Morphismen $\operatorname{Spec} B \to \operatorname{Spec} A'$ wirklich étale Überlagerungen sind. Für den ganzen Abschluss B eines normalen noetherschen Integritätsbereichs A in einer endlichen separablen Körpererweiterung von $\operatorname{Quot}(A)$ gilt, dass B als A-Modul endlich erzeugt ist. ([9], Proposition 13.14) Als A-Algebra hat B die Form $B = A[b_1, \dots, b_s]$, und da b_{i+1} jeweils ganz über $A[b_1, \dots, b_i]$ ist, ist $A[b_1, \dots, b_{i+1}]$ flache $A[b_1, \dots, b_i]$-Algebra. Damit ist B flache A-Algebra, und nach Voraussetzung ist B unverzweigt über A. $\square$

Beispiel 3.15. Die étalen Überlagerungen von $\operatorname{Spec} \mathbb{Z} \backslash \{(p)\}$ sind genau die Spektren von Normalisierungen B von $\mathbb{Z}[\frac{1}{p}]$ in endlichen, außerhalb von p unverzweigten Körpererweiterungen L von $\mathbb{Q}$.

Beweis. Für eine solche Normalisierung B ist der Morphismus $\varphi : \operatorname{Spec} B \to \operatorname{Spec} \mathbb{Z} \backslash (p)$ die Einschränkung der Abbildung $\psi : \operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathbb{Z}$ auf das offene Unterschema $\operatorname{Spec} B = \operatorname{Spec} \mathcal{O}_L[\frac{1}{p}]$.

Der Morphismus φ ist also genau dann unverzweigt, wenn ψ an allen Punkten, die nicht über (p) liegen, unverzweigt ist. Das ist offenbar genau dann der Fall, wenn die Körpererweiterung $L \supset \mathbb{Q}$ an allen von p verschiedenen Stellen unverzweigt ist. $\square$

Lemma 3.16. *Die galoisschen étalen Überlagerungen sind unter diesen Überlagerungen genau diejenigen, für die die Körpererweiterung $L/\mathbb{Q}$ galoissch ist.*

Beweis. Die Automorphismengruppe $\operatorname{Aut}_{\operatorname{Spec} \mathbb{Z}[\frac{1}{p}]}(\operatorname{Spec} B)$ ist kanonisch isomorph zu $\operatorname{Aut}_{\mathbb{Q}}(L)$: Durch Übergang zu den Homomorphismen am generischen Punkt von $\operatorname{Spec} B$ erhält man aus jedem Element von $\operatorname{Aut}_{\operatorname{Spec} \mathbb{Z}[\frac{1}{p}]}(\operatorname{Spec} B)$ einen Automorphismus von L. Umgekehrt bildet jeder Automorphismus von L den Unterring B als ganzen Abschluss von $\mathbb{Z}[\frac{1}{p}]$ wieder in sich selbst ab und liefert durch Einschränken einen Automorphismus von B über $\mathbb{Z}[\frac{1}{p}]$ und damit einen Automorphismus von $\operatorname{Spec} B$ über $\operatorname{Spec} \mathbb{Z}[\frac{1}{p}]$.

Die Operation von $\operatorname{Aut}_{\operatorname{Spec} A}(\operatorname{Spec} B)$ auf $F(\operatorname{Spec} B) = \operatorname{Hom}_{\operatorname{Spec} A}(\operatorname{Spec} \overline{\mathbb{Q}}, \operatorname{Spec} B)$ entspricht dabei der zugehörigen Operation von $\operatorname{Aut}_{\mathbb{Q}}(L)$ auf $\operatorname{Hom}_A(B, \overline{\mathbb{Q}})$. Die Gruppe $\operatorname{Aut}_{\mathbb{Q}}(L)$ operiert aber bekanntlich genau dann transitiv auf $\operatorname{Hom}_{\mathbb{Q}}(L, \overline{\mathbb{Q}})$, wenn die Körpererweiterung $L/\mathbb{Q}$ galoissch ist. $\square$

Satz 3.17. *Die algebraische Fundamentalgruppe von* $\operatorname{Spec} \mathbb{Z} \backslash (p)$ *ist die Galoisgruppe der maximalen außerhalb von p unverzweigten Erweiterung von $\mathbb{Q}$.*

Beweis. Das projektive System von Überlagerungen, das unseren Funktor darstellt, besteht in diesem Fall aus den Überlagerungen $\operatorname{Spec} B \to \operatorname{Spec} \mathbb{Z}[\frac{1}{p}]$, wobei B der ganze Abschluss von $\mathbb{Z}[\frac{1}{p}]$ in einer endlichen separablen außerhalb p unverzweigten Körpererweiterung L von $\mathbb{Q}$ ist. Die Automorphismengruppen sind jeweils isomorph zur Galoisgruppe $\operatorname{Gal}(L/\mathbb{Q})$, und die Übergangshomomorphismen entsprechen den kanonischen Abbildungen zwischen den Galoisgruppen. Als Limes erhalten wir also die Galoisgruppe der maximalen außerhalb von p unverzweigten Körpererweiterung von $\mathbb{Q}$. $\square$

4 Arithmetische Topologie

Eine Untersuchung der étalen Kohomologiegruppen[4] von $\operatorname{Spec} \mathcal{O}_K$ für Zahlkörper K liefert im Wesentlichen das Resultat, dass es sich bei diesen Schemata um dreidimensionale Objekte handelt.[5] Genauer hat man für total imaginäre Zahlkörper den folgenden Satz ([27]):

Satz 4.1. *Sei X das Spektrum des Ganzheitsrings in einem total imaginären Zahlkörper K, $\mathbb{G}_m$ die multiplikative Gruppe des Körpers. Dann gilt*

$$\begin{aligned} H^0(X, \mathbb{G}_m) &= \mathcal{O}_K^*, \\ H^1(X, \mathbb{G}_m) &= \mathrm{Cl}(K), \\ H^2(X, \mathbb{G}_m) &= 0, \\ H^3(X, \mathbb{G}_m) &= \mathbb{Q}/\mathbb{Z}, \\ H^q(X, \mathbb{G}_m) &= 0, \quad \textit{falls } q > 3. \end{aligned}$$

Wenn K nicht total imaginär ist, gilt bis auf $\mathbb{Z}/2\mathbb{Z}$-Torsion ein ähnliches Resultat ([28], Prop. 2.1). Für $K = \mathbb{Q}$ haben wir zum Beispiel

$$\begin{aligned} H^0(\operatorname{Spec} \mathbb{Z}, \mathbb{G}_m) &= \mathbb{Z}/2\mathbb{Z}, \\ H^1(\operatorname{Spec} \mathbb{Z}, \mathbb{G}_m) &= H^2(\operatorname{Spec} \mathbb{Z}, \mathbb{G}_m) = 0, \\ H^3(\operatorname{Spec} \mathbb{Z}, \mathbb{G}_m) &= \mathbb{Q}/\mathbb{Z}, \end{aligned}$$

und wenn wir $\mathbb{Z}/2\mathbb{Z}$-Torsion in den höheren Dimensionen ignorieren oder zu 2 teilerfremde Torsionskoeffizienten wählen, ist $\operatorname{Spec} \mathbb{Z}$ ebenfalls ein dreidimensionales Objekt.

Zusätzlich folgt aus Satz 3.14 und dem Satz von Minkowski, dass die algebraische Fundamentalgruppe von $\operatorname{Spec} \mathbb{Z}$ die triviale Gruppe ist; in topologischer Sprechweise ist $\operatorname{Spec} \mathbb{Z}$ also einfach zusammenhängend. Wenn man die étale Kohomologie als Äquivalent der topologischen Kohomologietheorien auffasst, fällt auf, dass Objekte wie $\operatorname{Spec} \mathbb{Z}$ mit den hier aufgeführten Eigenschaften bereits seit Poincaré gerne verdächtigt werden, auszusehen wie eine 3-Sphäre.

Für das Spektrum eines Körpers stimmt die étale Kohomologie mit der Galoiskohomologie des Körpers überein ([29], III.1 Ex. 1.7). Da die absolute Galoisgruppe eines endlichen Körpers die kohomologische Dimension 1 hat ([40], Chap. II, §3.3), werden die abgeschlossenen Punkte $\operatorname{Spec} \mathbb{F}_q = \operatorname{Spec} \mathcal{O}_K/\mathfrak{p} \subset \operatorname{Spec} \mathcal{O}_K$ als eindimensionale Objekte angesehen, die mit einem Kreis S^1 verglichen werden können.

Als Anmerkung zu seinem Artikel [27] über étale Kohomologie von Zahlkörpern notierte sich B. Mazur, dass man das Entfernen eines Primideals aus $\operatorname{Spec} \mathbb{Z}$ als Analogon eines Knotenkomplements in S^3 auffassen kann. Ihm fiel ebenfalls auf, dass die Definition des Alexanderpolynoms in ähnlicher Form in der Iwasawatheorie wieder auftaucht. Diese und weitere Analogien zwischen Objekten in der Topologie und Objekten in der Zahlentheorie, die schon in den 60er Jahren bemerkt wurden, erschienen allerdings zunächst in keiner Veröffentlichung.

Aufgegriffen und ergänzt wurden die Ideen vor einigen Jahren in einem Vortrag von M. Kapranov und A. Reznikov am MPI, in dem die erste Version eines „Wörterbuchs“ vorgestellt wurde, das einige Objekte aus Knotentheorie und Zahlentheorie, die als Entsprechungen angesehen werden, auflistet. Das so entstandene Gebiet wurde von Reznikov auf den Namen

[4] Eine Einführung in die étale Kohomologie findet man in [29].

[5] J. Neukirch gibt in seinem Übersichtsartikel [31] eine Begründung dafür, dass dieses Resultat anschaulich das richtige ist.

„Arithmetische Topologie" getauft. Seitdem sind verschiedene Versionen des Wörterbuchs erschienen: die grundlegende Fassung findet man im Preprint [37], weitere Ergänzungen in [42], [38], [35] oder [8].

4.1 Wörterbuch, Teil 1

Für eine detaillierte Gegenüberstellung der Objekte und Ergebnisse aus den ersten zwei Kapiteln wählen wir hier ebenfalls die Form eines solchen Wörterbuchs.

Topologie	**Zahlentheorie**
• S^3 • Knoten • Verschlingungen	• $\operatorname{Spec}\mathbb{Z}$ • Primzahlen • natürliche Zahlen

Wie in der Einleitung zu diesem Kapitel beschrieben, hat die Kohomologie von $\operatorname{Spec}\mathbb{Z}$ genau wie die der 3-Sphäre die Eigenschaft, dass sie nur in den Dimensionen 0 und 3 nicht verschwindet.[6] Knoten und Primzahlen, also genauer S^1 und $\operatorname{Spec}\mathbb{F}_p$, sind eindimensionale Objekte, die sich jeweils in diese größeren Objekte einbetten lassen. Aus diesen eindimensionalen Objekten setzen sich Verschlingungen und natürliche Zahlen zusammen.

• Geschlossene orientierbare zusammenhängende 3-Mannigfaltigkeiten M	• $\operatorname{Spec}\mathcal{O}_K$ für Zahlkörper K
• Einbettungen von S^1 in M, also Knoten in M	• Primideale in $\mathcal{O}_K$
• Verschlingungen in M	• Ideale in $\mathcal{O}_K$

Allgemeiner stellt man einer dreidimensionalen Mannigfaltigkeit das Spektrum des Ganzheitsrings $\mathcal{O}_K$ eines Zahlkörpers gegenüber.[7] In diesem Fall erhält man anstelle von Primzahlen die Primideale der Höhe 1 in $\mathcal{O}_K$. Die Ideale, die sich aus diesen Primidealen zusammensetzen, stehen im allgemeineren Fall statt der ganzen Zahlen für Verschlingungen in einer Mannigfaltigkeit.

• zusammenhängende Überlagerungen von M	• unverzweigte Körpererweiterungen von K
• S^3 hat keine nichttriviale zusammenhängende Überlagerung	• $\mathbb{Q}$ hat keine nichttriviale unverzweigte Erweiterung

[6] mit Koeffizienten in $\mathbb{G}_m$ wie oben bemerkt nur bis auf $\mathbb{Z}/2\mathbb{Z}$-Torsion

[7] In der neueren Version [38] des Wörterbuchs nennt A. Reznikov als Entsprechungen von Zahlkörpern so genannte „$3\frac{1}{2}$-Mannigfaltigkeiten". Wie [35] und [42] orientieren wir uns aber an der einfacheren Fassung [37].

Den zusammenhängenden Überlagerungen einer Mannigfaltigkeit entsprechen nach Kapitel 3 die zusammenhängenden étalen Überlagerungen von $\operatorname{Spec} \mathcal{O}_K$. Diese sind nach Satz 3.14 genau die Morphismen $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$ für unverzweigte Körpererweiterungen L/K. Wie die 3-Sphäre besitzt $\operatorname{Spec} \mathbb{Z}$ keine nichttriviale Überlagerung, ist also „einfach zusammenhängend“.

• Knotenkomplement C	• $\operatorname{Spec} \mathbb{Z}[\frac{1}{p}]$

Das Knotenkomplement erhält man durch Entfernen eines eingebetteten Kreises aus der 3-Sphäre. Wenn man einen abgeschlossenen Punkt (p) aus $\operatorname{Spec} \mathbb{Z}$ entfernt, erhält man das offene Unterschema $\operatorname{Spec} \mathbb{Z}[\frac{1}{p}]$.

• maximale abelsche Überlagerung C_∞ des Knotenkomplements	• zyklotomische $\mathbb{Z}_p$-Erweiterung $\mathbb{Q}_\infty/\mathbb{Q}$

Einer zusammenhängenden Überlagerung des Knotenkomplements entspricht eine zusammenhängende étale Überlagerung von $\operatorname{Spec} \mathbb{Z}[\frac{1}{p}]$. Diese Überlagerungen entsprechen wiederum den p-verzweigten Körpererweiterungen von $\mathbb{Q}$ (Beispiel 3.15). Der maximalen abelschen Überlagerung eines Knotenkomplements wird also die maximale abelsche außerhalb von p unverzweigte Erweiterung von $\mathbb{Q}$ zugeordnet. Der p-Anteil dieser Erweiterung, also die maximale abelsche p-verzweigte p-Erweiterung von $\mathbb{Q}$, ist nach Satz 2.10 die zyklotomische $\mathbb{Z}_p$-Erweiterung $\mathbb{Q}_\infty/\mathbb{Q}$.

• Knotengruppe G	• Galoisgruppe G der maximalen p-verzweigten p-Erweiterung von $\mathbb{Q}$
• Decktransformationsgruppe D der maximalen abelschen Überlagerung	• Galoisgruppe Γ der zyklotomischen $\mathbb{Z}_p$-Erweiterung $\mathbb{Q}_\infty/\mathbb{Q}$
• $D = G^{ab} \cong \mathbb{Z}$	• $\Gamma = G^{ab} \cong \mathbb{Z}_p$

Die Knotengruppe eines Knotens ist nach Definition die Fundamentalgruppe des Knotenkomplements. Nach Satz 3.17 ist die Galoisgruppe G genau der maximale Pro-p-Quotient der algebraischen Fundamentalgruppe des korrespondierenden Schemas $\operatorname{Spec} \mathbb{Z} \setminus \{(p)\} = \operatorname{Spec} \mathbb{Z}[\frac{1}{p}]$. Die Rolle der Decktransformationsgruppe, also der Automorphismengruppe von C_∞ über C, übernimmt die Galoisgruppe $\operatorname{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, also die Automorphismengruppe von $\mathbb{Q}_\infty$ über $\mathbb{Q}$.

Ganz allgemein ersetzt man hier im zahlentheoretischen Fall abstrakte Gruppen durch Pro-p-Gruppen und Untergruppen durch abgeschlossene Untergruppen. Insbesondere wird die Kommutatoruntergruppe durch den Normalteiler ersetzt, der topologisch von den Kommutatoren erzeugt wird. Die Isomorphie $D \cong \mathbb{Z}$ entspricht der Tatsache, dass Γ eine freie Pro-p-Gruppe mit einem Erzeuger ist.

• $(G')^{ab} = H_1(C_\infty)$	• $(G')^{ab} = \operatorname{Gal}(M_p(\mathbb{Q}_\infty)/\mathbb{Q}_\infty) = G_p^{ab}(\mathbb{Q}_\infty)$
• $\mathbb{Z}[D] \cong \mathbb{Z}[T, T^{-1}]$	• $\mathbb{Z}_p[\![\Gamma]\!] \cong \mathbb{Z}_p[\![T]\!]$

Bildet man den Quotienten von G' nach der Kommutatoruntergruppe G'', so erhält man die erste Homologiegruppe der maximalen abelschen Überlagerung von C bzw. die Galoisgruppe der maximalen abelschen p-verzweigten p-Erweiterung von $\mathbb{Q}_\infty$.

Der Gruppenring über G^{ab} wird im ersten Fall mit Koeffizienten in $\mathbb{Z}$ gebildet und im zweiten Fall als vollständiger Gruppenring (§2.4) mit Koeffizienten in $\mathbb{Z}_p$. Einen Isomorphismus zwischen dem Gruppenring und dem Laurent-Polynomring $\mathbb{Z}[T, T^{-1}]$ bzw. dem Potenzreihenring $\mathbb{Z}_p[\![T]\!]$ erhält man durch Wahl eines Erzeugers von D bzw. eines topologischen Erzeugers von Γ (Satz 2.16). Die Gruppe G^{ab} operiert in beiden Situationen auf G'^{ab} und macht damit die korrespondierenden Objekte $H_1(C_\infty)$ und $G_p^{ab}(\mathbb{Q}_\infty)$ jeweils zu einem Modul über dem Gruppenring.

• Operation von T auf $H_1(C_\infty)$ • $p_T(T) = \Delta_0(H_1(C_\infty))$	• Operation von T auf $G_p^{ab}(\mathbb{Q}_\infty)$ • $p_T(T) = \Delta_0(G_p^{ab}(\mathbb{Q}_\infty)) = Z_{\mathbb{Q},p}(T)$

Das Element T aus dem Gruppenring induziert jeweils einen Automorphismus des Moduls und damit auch einen Automorphismus des endlichdimensionalen Vektorraums, den man durch Tensorieren mit $\mathbb{Q}$ bzw. $\mathbb{Q}_p$ erhält. Das charakteristische Polynom ist nach Satz 1.4 bis auf Multiplikation mit einer Einheit das nullte Fitting-Ideal des jeweiligen Moduls. Für den Knoten erhält man als Invariante das Alexanderpolynom, für die Galoisgruppe ist das Resultat die Iwasawa-Zetafunktion.

5 Berechnungen und Verallgemeinerungen

In diesem Kapitel sollen Methoden zur Beschreibung und Berechnung des Alexanderpolynoms auf den zahlentheoretischen Fall übertragen werden. Als zweiter Punkt werden verschiedene Möglichkeiten diskutiert, das Alexanderpolynom von Verschlingungen mit mehreren Komponenten in der Iwasawatheorie wiederzufinden.

5.1 Fox-Kalkül

Das Alexanderpolynom eines Knotens mit Knotenkomplement C und universeller abelscher Überlagerung $p : C_\infty \to C$ lässt sich mit Hilfe einer Präsentationsmatrix des $\mathbb{Z}[\mathbb{Z}]$-Moduls $H_1(C_\infty, C_\infty^{(0)})$ berechnen. R. Fox ([10], [11]) stellt eine Methode vor, mit der man diesen Modul durch Erzeuger und Relationen beschreiben kann, wenn Erzeuger und Relationen der Knotengruppe G bekannt sind.

5.1.1 Geometrisch: G-CW-Komplexe

In Kapitel 9A von [6] wird die anschauliche geometrische Grundlage der Berechnungen dargestellt, die wir hier wiedergeben.

Da die Konstruktionen nur von der Fundamentalgruppe des Knotenkomplements abhängen, können wir wieder annehmen, dass C ein CW-Komplex mit einer 0-Zelle P, einer 1-Zelle für jeden Erzeuger von G und einer 2-Zelle für jede Relation ist. Wir wählen einen Punkt $\tilde{P}$ über P in der Überlagerung C_∞ und bezeichnen mit D die Decktransformationsgruppe der Überlagerung. Der Raum C_∞ ist dann ein D-CW-Komplex, der für jede Zelle von C eine äquivariante Zelle besitzt.

Seien $s_1, \ldots, s_n$ die Erzeuger von $\pi_1(C, P)$, die den 1-Zellen entsprechen. Die freie Gruppe $\mathcal{F}$, die von den Elementen $s_1, \ldots, s_n$ erzeugt wird, ist dann die Fundamentalgruppe des 1-Gerüsts $C^{(1)}$, und die Hochhebungen $\tilde{s}_1, \ldots, \tilde{s}_n$ am Punkt $\tilde{P}$ repräsentieren die äquivarianten 1-Zellen des D-CW-Komplexes C_∞.

Sei w ein geschlossener Weg in $C^{(1)}$, der einem Element von $\mathcal{F}$ entspricht. Die Hochhebung von w am Punkt $\tilde{P}$ kann als Repräsentant eines Zykels aus $Z_1(C_\infty, C_\infty^{(0)})$ aufgefasst werden. Diese Zykel haben eine eindeutige Darstellung der Form $\Sigma \xi_i \tilde{s}_i$ mit Elementen $\xi_i \in \mathbb{Z}[D]$, wodurch für jedes i eine Abbildung

$$\begin{array}{rcl} \mathcal{F} & \to & \mathbb{Z}[D] \\ w & \mapsto & \xi_i \end{array}$$

definiert wird.

In D verschwinden alle Elemente, die geschlossenen Wegen in $C_\infty^{(1)}$ entsprechen. Der Kern der gerade definierten Abbildungen enthält damit alle Relatoren r_j der Gruppe G, da die Hochhebungen der entsprechenden 2-Zellen in der Überlagerung wieder 2-Zellen sind. Die Abbildungen faktorisieren also über G und können linear fortgesetzt werden zu Abbildungen

$$\frac{\partial}{\partial s_i} : \mathbb{Z}[G] \to \mathbb{Z}[D].$$

Lemma 5.1. *Eigenschaften der Abbildungen* $\frac{\partial}{\partial s_i}$*:*

1) $\frac{\partial}{\partial s_i}$ *ist* $\mathbb{Z}$*-linear.*

2) $\frac{\partial}{\partial s_i}(s_k) = \delta_{ik}$

3) Für zwei Elemente $w, w' \in G$ *gilt* $\frac{\partial}{\partial s_i}(ww') = \frac{\partial}{\partial s_i}(w) + \overline{w}\frac{\partial}{\partial s_i}(w')$*, wobei* $\overline{w}$ *das Bild von* w *in* D *bezeichnet.*

4) Falls w *ein geschlossener Weg in* $C^{(1)}$ *ist, gilt für seine Hochhebung* $\tilde{w}$ *am Punkt* $\tilde{P}$ *die Gleichung*

$$\tilde{w} = \Sigma \frac{\partial}{\partial s_j}(w) \cdot \tilde{s}_j.$$

Beweis. 1, 2, 4) folgen direkt aus der Definition der Abbildungen.

3) Seien $\tilde{w} = \Sigma_i \xi_i \tilde{s}_i$ und $\tilde{w}' = \Sigma_i \xi_i' \tilde{s}_i$ die eindeutigen Darstellungen als Linearkombinationen der $\tilde{s}_i$. Dann ist der Endpunkt der Hochhebung $\tilde{w}$ der Punkt $\tilde{w} \cdot \tilde{P}$, und die Hochhebung von w', die am Punkt $\tilde{w} \cdot \tilde{P}$ beginnt, ist durch $\overline{w} \cdot \tilde{w}'$ gegeben.

□

Satz 5.2. *Sei* $\pi_1(C)$ *durch die Präsentation* $\langle s_1, \ldots, s_n | r_1, \ldots, r_m \rangle$ *gegeben. Dann ist die „Jacobi-Matrix“*

$$\left(\frac{\partial r_j}{\partial s_i}\right) \in M(n \times m, \mathbb{Z}[D])$$

eine Präsentationsmatrix des $\mathbb{Z}[D]$*-Moduls* $H_1(C_\infty, C_\infty^{(0)})$.

Beweis. Als D-CW-Komplex besteht C_∞ aus einer 0-Zelle, den 1-Zellen $\tilde{s}_1, \ldots, \tilde{s}_n$ und den 2-Zellen $\tilde{r}_1, \ldots, \tilde{r}_m$, also hat $H_1(C_\infty, C_\infty^{(0)})$ als $\mathbb{Z}[D]$-Modul n Erzeuger, die den 1-Zellen entsprechen, und die m Relationen $\tilde{r}_1 = \cdots = \tilde{r}_m = 0$. Die zugehörige Präsentation

$$\mathbb{Z}[D]^m \to \mathbb{Z}[D]^n \to H_1(C_\infty, C_\infty^{(0)}) \to 0$$

besitzt wegen der Formel $\tilde{r}_j = \Sigma \frac{\partial r_j}{\partial s_i} \cdot \tilde{s}_i$ die angegebene Jacobi-Matrix als Präsentationsmatrix. □

5.1.2 Algebraisch: Differentialrechnung in Gruppenringen

Unser Ziel ist hier – wie im Folgenden auch noch häufiger – die geometrischen Konstruktionen rein algebraisch zu beschreiben, um Analogien zur Situation in der Zahlentheorie herstellen zu können. Der Fox-Kalkül stellt eine Methode bereit, die oben genannten Abbildungen mit Hilfe von Derivationen und Differentialmoduln über Gruppenringen zu beschreiben ([6], Ch. 9B). Die dafür benötigten Eigenschaften sind hier kurz zusammengefasst.

Definition. Sei G eine (nicht unbedingt kommutative) Gruppe und M ein $\mathbb{Z}[G]$-Linksmodul. Eine $\mathbb{Z}$-lineare Abbildung $\Delta : \mathbb{Z}[G] \to M$ heißt Derivation, falls alle $\xi, \eta \in \mathbb{Z}[G]$ die Gleichung

$$\Delta(\xi \cdot \eta) = \Delta(\xi) \cdot \varepsilon(\eta) + \xi \cdot \Delta(\eta).$$

erfüllen. Dabei bezeichnet $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$ die Augmentationsabbildung, durch die M auch als $\mathbb{Z}[G]$-Rechtsmodul aufgefasst werden kann.

Lemma 5.3. *Eigenschaften von Derivationen:*
1) $\Delta(m) = 0$ *für alle* $m \in \mathbb{Z}$.
2) $\Delta(g^{-1}) = -g^{-1}\Delta(g)$ *für alle* $g \in G$.
3) $\Delta(g^n) = (1 + g + \cdots + g^{n-1})\Delta(g)$ *für alle* $g \in G$.
4) $\Delta(g^{-n}) = -(g^{-1} + g^{-2} + \cdots + g^{-n})\Delta(g)$ *für alle* $g \in G$.

Beweis. Die Eigenschaften lassen sich mit Hilfe der Definition sofort nachrechnen. □

Satz 5.4. *Sei* F *die freie Gruppe auf den Elementen* $s_i, i \in I$, *und* M *ein* $\mathbb{Z}[F]$*-Modul. Dann gibt es zu jeder Wahl von Elementen* $m_i \in M$ *genau eine Derivation* $\Delta : \mathbb{Z}[F] \to M$ *mit* $\Delta(s_i) = m_i$ *für jedes* i.

Beweis. Durch diese Angaben ist Δ auf $\mathbb{Z}[F]$ festgelegt; da F frei ist, ist die Abbildung auch wohldefiniert. □

Definition. Für die freie Gruppe F auf der Menge $\{s_i | i \in I\}$ ist die partielle Derivation

$$\frac{\partial}{\partial s_i} : \mathbb{Z}[F] \to \mathbb{Z}[F]$$

definiert als die eindeutig bestimmte Derivation mit $\frac{\partial}{\partial s_i}(s_j) = \delta_{ij} \cdot 1$ für alle $j \in I$.

Satz 5.5. *Sei* F *die freie Gruppe auf der Menge* $\{s_1, \ldots, s_n\}$. *Für jedes Element* $\alpha \in F$ *gilt dann*

$$\alpha - 1 = \sum_{i=1}^{n} \frac{\partial \alpha}{\partial s_i}(s_i - 1).$$

Beweis. Die linke Seite der Gleichung definiert eine Derivation, denn für $\alpha, \beta \in F$ gilt $\alpha\beta - 1 = (\alpha - 1) \cdot 1 + \alpha(\beta - 1)$. Als Linearkombination der partiellen Derivationen $\frac{\partial}{\partial s_i}$ ist auch die rechte Seite eine Derivation. Auf den Erzeugern von F stimmen diese beiden Derivationen offensichtlich überein und sind damit gleich. □

Satz 5.6. *Sei* G *eine Gruppe und* $\mathbb{Z}[G]$ *der zugehörige Gruppenring über* $\mathbb{Z}$. *Dann existiert ein* $\mathbb{Z}[G]$*-Linksmodul* Ω_G *zusammen mit einer Derivation* $d : \mathbb{Z}[G] \to \Omega_G$, *sodass die folgende universelle Eigenschaft erfüllt ist:*

Zu jeder Derivation $D : \mathbb{Z}[G] \to M$ *von* $\mathbb{Z}[G]$ *in einen* $\mathbb{Z}[G]$*-Linksmodul* M *existiert genau ein* $\mathbb{Z}[G]$*-Modulhomomorphismus* $\varphi : \Omega_G \to M$, *sodass* $D = \varphi \circ d$.

Beweis. Der gesuchte $\mathbb{Z}[G]$-Modul wird folgendermaßen konstruiert: Wir bilden zunächst den freien Modul $\bigoplus_{x \in \mathbb{Z}[G]} \mathbb{Z}[G] \cdot dx$ auf den Elementen von $\mathbb{Z}[G]$. Sei N der Untermodul, der von den Elementen $d(x + y) - dx - dy$ und $d(xy) - dx \cdot \varepsilon(x) - xdy$ für $x, y \in \mathbb{Z}[G]$ erzeugt wird. Der Quotient $\Omega_G = \bigoplus_{x \in \mathbb{Z}[G]} \mathbb{Z}[G] \cdot dx / N$ zusammen mit der Abbildung

$$\begin{aligned} d : \mathbb{Z}[G] &\to \Omega_G, \\ \sigma &\mapsto d\sigma, \end{aligned}$$

hat dann offenbar die gewünschte universelle Eigenschaft. □

Bemerkung. Der Modul Ω_G wird von den Elementen $d\sigma, \sigma \in G$, erzeugt.

Für eine Gruppe G bezeichnen wir mit I_G im Folgenden immer das zugehörige Augmentationsideal, also den Kern der Abbildung $\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$, $\Sigma \alpha_i g_i \mapsto \Sigma \alpha_i$.

Satz 5.7. *Der Differentialmodul Ω_G ist kanonisch isomorph zum Augmentationsideal I_G. Der $\mathbb{Z}[G]$-Isomorphismus $\varphi : \Omega_G \to I_G$ ist für Elemente σ aus G durch die Gleichung $\varphi(d\sigma) = \sigma - 1$ gegeben.*

Beweis. Der Homomorphismus φ ist wohldefiniert, denn für zwei Elemente σ, τ aus G gilt $\varphi(d(\sigma\tau)) = \sigma\tau - 1 = \sigma - 1 + \sigma(\tau - 1) = \varphi(d\sigma + \sigma d\tau)$. Die Umkehrabbildung $I_G \to \Omega_G$, gegeben durch $\sigma - 1 \mapsto d\sigma$, ist ebenfalls wohldefiniert. □

Satz 5.8. *Für die freie Gruppe F auf der Menge $\{e_1, \ldots, e_d\}$ ist der Modul Ω_F ein freier $\mathbb{Z}[F]$-Modul mit Basis $\{de_1, \ldots, de_d\}$.*

Beweis. Für jede Wahl von Elementen $a_1, \ldots, a_d$ in einem F-Modul M gibt es nach Satz 5.4 genau eine Derivation $D : \mathbb{Z}[F] \to M$ mit $D(e_i) = a_i$ für $i = 1, \ldots, d$.

Aus der universellen Eigenschaft des Differentialmoduls Ω_F erhalten wir damit sofort die universelle Eigenschaft, die einen freien $\mathbb{Z}[F]$-Modul charakterisiert. □

Bemerkung. Die Derivation $\tau : \mathbb{Z}[F] \to \mathbb{Z}[F]$, die via der Identifikation $\Omega_F \cong I_F$ der Inklusion $I_F \hookrightarrow \mathbb{Z}[F]$ entspricht, ist für Elemente $f \in F$ gegeben durch $\tau(f) = f - 1$. Die Gleichung, die man für Elemente in Ω_F aus Satz 5.5 erhält, hat damit für jedes $f \in F$ die Form

$$df = \sum_{i=1}^{d} \frac{\partial f}{\partial e_i} de_i.$$

5.1.3 Differentialrechnung in vollständigen Gruppenringen

Man erhält ähnliche Aussagen wie im letzten Teilabschnitt, wenn man G durch eine Pro-p-Gruppe ersetzt, den Gruppenring durch den vollständigen Gruppenring $\mathbb{Z}_p[\![G]\!]$ und die Kategorie der Moduln über $\mathbb{Z}[G]$ durch die Kategorie der pro-endlichen Moduln über $\mathbb{Z}_p[\![G]\!]$ ([33], Ch. V §6). Wir betrachten also diejenigen topologischen $\mathbb{Z}_p[\![G]\!]$-Moduln, deren zugrunde liegende abelsche Gruppe selbst pro-endlich ist.

Definition. Sei M ein pro-endlicher $\mathbb{Z}_p[\![G]\!]$-Linksmodul. Eine stetige $\mathbb{Z}_p$-lineare Abbildung $\Delta : \mathbb{Z}_p[\![G]\!] \to M$ heißt Derivation, falls alle $\xi, \eta \in \mathbb{Z}_p[\![G]\!]$ die Gleichung

$$\Delta(\xi \cdot \eta) = \Delta(\xi) \cdot \varepsilon(\eta) + \xi \cdot \Delta(\eta)$$

erfüllen. Dabei bezeichnet $\varepsilon : \mathbb{Z}_p[\![G]\!] \to \mathbb{Z}_p$ wieder die Augmentationsabbildung.

Lemma 5.9. *Sei F eine freie Pro-p-Gruppe und M ein pro-endlicher $\mathbb{Z}_p[\![F]\!]$-Linksmodul. Dann ist $M \rtimes F$ eine pro-endliche topologische Gruppe, und die Derivationen $\mathbb{Z}_p[\![F]\!] \to M$ entsprechen genau den ersten Komponenten von stetigen Schnitten der Abbildung $M \rtimes F \to F, (m, f) \mapsto f$.*

Beweis. Die Verknüpfung $(m_1, f_1)(m_2, f_2) = (m_1 + f_1 m_2, f_1 f_2)$ in $M \rtimes F$ ist stetig, wenn man die Produkttopologie zugrunde legt, und als Produkt von pro-endlichen topologischen Räumen ist $M \rtimes F$ auch ein pro-endlicher Raum und damit eine pro-endliche topologische Gruppe. Sie ist eine Pro-p-Gruppe, weil der Index jeder offenen Untergruppe eine p-Potenz ist.

Sei $s = d \times 1 : F \to M \rtimes F$ ein stetiger Schnitt. Dann gilt $s(gh) = s(g) \circ s(h) = (dg, g) \circ (dh, h)$ für alle $g, h \in F$, nach Definition der Verknüpfung auf $M \rtimes F$ ist also

$s(gh) = (d(gh), gh) = (dg + g \cdot dh, gh)$. Die Abbildung $s = d \times 1$ ist also genau dann ein Gruppenhomomorphismus, wenn d die Gleichung $d(gh) = dg + g\ dh$ für alle $g, h \in F$ erfüllt, und genau dann stetig, wenn d stetig ist.

Da die Derivationen $\Delta : \mathbb{Z}_p[\![F]\!] \to M$ genau die Fortsetzungen solcher Abbildungen d auf den Gruppenring sind, folgt daraus die Behauptung. □

Satz 5.10. *Sei F die freie Pro-p-Gruppe auf den Elementen $f_i, i \in I$, und M ein pro-endlicher $\mathbb{Z}_p[\![F]\!]$-Linksmodul. Dann gibt es zu jeder konvergenten Teilmenge $\{m_i | i \in I\}$ von M genau eine Derivation $\Delta : \mathbb{Z}_p[\![F]\!] \to M$ mit $\Delta(f_i) = m_i$ für jedes i.*

Beweis. Wegen der universellen Eigenschaft von F gibt es genau einen stetigen Gruppenhomomorphismus $s : F \to M \rtimes F$ mit $s(f_i) = (m_i, f_i)$. Auf der zweiten Komponente ist s offenbar die Identität. Die Zusammensetzung mit der Projektion auf die erste Komponente ergibt nach dem Lemma eine Derivation $d : F \to M$, die durch die Angabe der Bilder der f_i eindeutig bestimmt ist. □

Definition. Für die freie Pro-p-Gruppe F auf der Menge $\{s_i | i \in I\}$ ist die partielle Derivation

$$\frac{\partial}{\partial s_i} : \mathbb{Z}_p[\![F]\!] \to \mathbb{Z}_p[\![F]\!]$$

definiert als die eindeutig bestimmte Derivation mit $\frac{\partial}{\partial s_i}(s_j) = \delta_{ij} \cdot 1$ für alle $j \in I$.

Genau wie in Abschnitt 5.1.2 zeigt man die folgende Aussage:

Satz 5.11. *Sei F die freie Pro-p-Gruppe auf der Menge $\{s_1, \ldots, s_n\}$. Für jedes Element $\alpha \in F$ gilt dann*

$$\alpha - 1 = \sum_{i=1}^{n} \frac{\partial \alpha}{\partial s_i}(s_i - 1).$$

Definition. Der freie pro-endliche $\mathbb{Z}_p[\![G]\!]$-Modul auf der Menge I ist ein $\mathbb{Z}_p[\![G]\!]$-Modul Z zusammen mit einer Abbildung $\iota : I \to Z$, sodass die folgende universelle Eigenschaft erfüllt ist:

Für jeden pro-endlichen Modul M und jede konvergente Teilmenge $\{m_i | i \in I\}$ von M gibt es genau einen stetigen $\mathbb{Z}_p[\![G]\!]$-Modulhomomorphismus $\varphi : Z \to M$ mit $\varphi(\iota(i)) = m_i$ für alle $i \in I$.

Der freie pro-endliche $\mathbb{Z}_p[\![G]\!]$-Modul auf einer Menge I existiert für jede Indexmenge und kann folgendermaßen konstruiert werden: Anstelle einer direkten Summe bildet man das Produkt $\prod_{i \in I} \mathbb{Z}_p[\![G]\!]$ zusammen mit der offensichtlichen Abbildung $I \to \prod_{i \in I} \mathbb{Z}_p[\![G]\!],\ i \mapsto 1_i$.

Die universelle Eigenschaft ist dann für jeden pro-endlichen Modul M erfüllt: Sei $\{m_i \in M | i \in I\}$ eine konvergente Teilmenge von M. Als topologischer Modul ist M isomorph zum projektiven Limes $\varprojlim M/U$, wobei U die offenen Untermoduln durchläuft. Für jeden der endlichen Moduln können wir einen $\mathbb{Z}_p[\![G]\!]$-Modulhomomorphismus $\prod_{i \in I} \mathbb{Z}_p[\![G]\!] \to M/U$ durch $1_i \mapsto \overline{m}_i$ definieren, da in M/U fast alle Elemente $\overline{m}_i$ verschwinden. Die so definierten Abbildungen sind stetig und setzen sich zu einem Homomorphismus $\prod_{i \in I} \mathbb{Z}_p[\![G]\!] \to M$ zusammen.

Satz 5.12. *Sei G eine Gruppe, $\mathbb{Z}_p[\![G]\!]$ der zugehörige Gruppenring über $\mathbb{Z}_p$. Dann existiert ein $\mathbb{Z}_p[\![G]\!]$-Modul Ω_G zusammen mit einer Derivation $d : \mathbb{Z}_p[\![G]\!] \to \Omega_G$, sodass die folgende universelle Eigenschaft erfüllt ist:*

Zu jeder Derivation $D : \mathbb{Z}_p[\![G]\!] \to M$ von $\mathbb{Z}_p[\![G]\!]$ in einen pro-endlichen G-Modul M existiert genau ein stetiger $\mathbb{Z}_p[\![G]\!]$-Modulhomomorphismus $\varphi : \Omega_G \to M$, sodass $D = \varphi \circ d$.

Beweis. Der Modul Ω_G wird konstruiert als Quotient des freien pro-endlichen Moduls $\Pi\mathbb{Z}_p[\![G]\!]\cdot dx$ auf den Elementen x von $\mathbb{Z}_p[\![G]\!]$ nach dem abgeschlossenen Untermodul, der wie im diskreten Fall von den Relationen $d(x+y)-dx-dy$ und $d(xy)-dx\cdot\varepsilon(y)-xdy$ erzeugt wird. $\square$

Wir bezeichnen mit I_G im Folgenden wieder das Augmentationsideal der Gruppe G, hier also den Kern der Abbildung $\varepsilon : \mathbb{Z}_p[\![G]\!] \to \mathbb{Z}_p,\ \Sigma\alpha_i g_i \mapsto \Sigma\alpha_i$. Genau wie in Abschnitt 5.1.2 beweist man die folgenden Sätze:

Satz 5.13. *Der Differentialmodul Ω_G ist kanonisch isomorph zum Augmentationsideal I_G. Der $\mathbb{Z}_p[\![G]\!]$-Isomorphismus $\varphi : \Omega_G \to I_G$ ist für Elemente σ aus G durch die Gleichung $\varphi(d\sigma) = \sigma - 1$ gegeben.*

Satz 5.14. *Für die freie Gruppe F auf der Menge $\{e_1,\dots,e_d\}$ ist der Modul Ω_F ein freier $\mathbb{Z}_p[\![F]\!]$-Modul mit Basis $\{de_1,\dots,de_d\}$.*

Die Derivation $d : \mathbb{Z}_p[\![F]\!] \to \Omega_F$ ist auch in diesem Fall auf Elementen $f \in F$ durch die folgende Formel gegeben:

$$df = \sum_{i=1}^{d} \frac{\partial f}{\partial e_i} de_i.$$

Beispiel 5.15. Sei Γ die (multiplikativ geschriebene) freie Pro-p-Gruppe mit einem Erzeuger γ. Jedes Element $x \in \Gamma$ hat dann eine eindeutige Darstellung der Form $x = \gamma^\alpha$ mit $\alpha \in \mathbb{Z}_p$. Die p-adische Zahl α können wir uns als $\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots$ mit $\alpha_i \in \{0,\dots,p-1\}$ vorstellen. Diese Schreibweise soll ausdrücken, dass $\alpha(n) = \alpha_0 + \alpha_1 p + \dots + \alpha_{n-1}p^{n-1}$ jeweils das Bild von α unter der Projektion $\mathbb{Z}_p \to \mathbb{Z}_p/p^n\mathbb{Z}_p = \mathbb{Z}/p^n\mathbb{Z}$ ist. Es gilt

$$\gamma^\alpha = \lim_{n\to\infty} \gamma^{\alpha(n)},$$

also ergibt sich die partielle Derivation $\frac{\partial x}{\partial \gamma}$ als Grenzwert

$$\lim_{n\to\infty} \frac{\partial \gamma^{\alpha(n)}}{\partial \gamma}.$$

Mit Hilfe der Rechenregeln für Derivationen erhält man

$$\frac{\partial \gamma^{\alpha(n)}}{\partial \gamma} = 1 + \gamma + \gamma^2 + \dots + \gamma^{\alpha(n)-1} \in \mathbb{Z}_p[\![\Gamma]\!].$$

Als Element im Potenzreihenring $\mathbb{Z}_p[\![T]\!]$ ergibt sich mit dem wie in Satz 2.16 durch die Wahl des Erzeugers gegebenen Isomorphismus $\gamma \mapsto T+1$ das Polynom

$$1 + (T+1) + (T+1)^2 + \dots + (T+1)^{\alpha(n)-1} = \frac{(T+1)^{\alpha(n)} - 1}{(T+1) - 1} = \sum_{k=1}^{\alpha(n)} \binom{\alpha(n)}{k} T^{k-1}.$$

Als Grenzwert erhalten wir also das Element

$$\frac{\partial}{\partial \gamma}\gamma^\alpha = \lim_{n\to\infty} \frac{\partial \gamma^{\alpha(n)}}{\partial \gamma} = \sum_{k=1}^{\infty} \binom{\alpha}{k} T^{k-1},$$

wobei die „Binomialkoeffizienten“ wie üblich durch die Gleichung

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{k!}$$

definiert sind.

5.2 Vollständige Tensorprodukte

Dem Tensorprodukt von Moduln entspricht in der Kategorie der pro-endlichen $\mathbb{Z}_p[\![G]\!]$-Moduln das so genannte vollständige Tensorprodukt.

Sei M ein pro-endlicher $\mathbb{Z}_p[\![G]\!]$-Rechtsmodul und N ein pro-endlicher $\mathbb{Z}_p[\![G]\!]$-Linksmodul. Für $\mathbb{Z}_p[\![G]\!]$ schreiben wir kürzer auch Λ. Mit einer $\mathbb{Z}_p[\![G]\!]$-bilinearen Abbildung $\varphi : M \times N \to A$ in einen pro-endlichen $\mathbb{Z}_p$-Modul A ist wie für gewöhnliche Moduln eine Abbildung mit den Eigenschaften

- $\varphi(m + m', n) = \varphi(m, n) + \varphi(m', n)$
- $\varphi(m, n + n') = \varphi(m, n) + \varphi(m, n')$
- $\varphi(m \cdot r, n) = \varphi(m, r \cdot n)$

für alle $m, m' \in M$, $n, n' \in N$ und $r \in \mathbb{Z}_p[\![G]\!]$ gemeint. Das vollständige Tensorprodukt $M \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} N$ ist analog zum gewöhnlichen Tensorprodukt durch die folgende universelle Eigenschaft definiert ([33], Ch. V §2):

Definition. Das vollständige Tensorprodukt von M und N ist ein pro-endlicher $\mathbb{Z}_p$-Modul $M \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} N$ zusammen mit einer $\mathbb{Z}_p[\![G]\!]$-bilinearen stetigen Abbildung

$$\varphi : M \times N \to M \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} N,$$

sodass für jede weitere $\mathbb{Z}_p[\![G]\!]$-bilineare stetige Abbildung $\psi : M \times N \to A$ in einen pro-endlichen $\mathbb{Z}_p$-Modul A genau ein $\mathbb{Z}_p$-linearer stetiger Homomorphismus $f : M \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} N \to A$ existiert mit $f \circ \varphi = \psi$.

Den Modul $M \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} N$ kann man konstruieren als

$$M \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} N = \varprojlim (M/U \otimes_{\mathbb{Z}_p[\![G]\!]} N/V),$$

wobei U und V die offenen Untermoduln von M bzw. N durchlaufen. Die Abbildung $M \times N \to M \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} N$ ergibt sich aus den Abbildungen $M \times N \to M/U \otimes_{\mathbb{Z}_p[\![G]\!]} N/V$. Dieser Limes ist als Limes der endlichen Moduln $M/U \otimes_{\mathbb{Z}_p[\![G]\!]} N/V$ tatsächlich pro-endlicher $\mathbb{Z}_p$-Modul.

$M \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} N$ ergibt sich mit anderen Worten als Vervollständigung von $M \otimes_{\mathbb{Z}_p[\![G]\!]} N$ in der Topologie, die als Umgebungsbasis der Null die Mengen $\ker(M \otimes_{\mathbb{Z}_p[\![G]\!]} N \to M/U \otimes_{\mathbb{Z}_p[\![G]\!]} N/V)$ hat.

Um die abgeleiteten Funktoren $\mathrm{Tor}_*^\Lambda(\_, \_)$ definieren zu können, fassen wir hier kurz einige Eigenschaften pro-endlicher $\mathbb{Z}_p[\![G]\!]$-Moduln zusammen ([39], Ch. 5.4):

Die Kategorie der pro-endlichen $\mathbb{Z}_p[\![G]\!]$-Moduln ist eine abelsche Kategorie.[8] Die projektiven Moduln in dieser Kategorie sind genau die direkten Summanden von freien Moduln, und jeder Modul ist Quotient eines freien Moduls. Insbesondere hat die Kategorie genügend viele projektive Objekte. Die Funktoren $\_ \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} N$ und $M \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} \_$ sind additiv und rechtsexakt. Man kann also die Linksableitung der Funktoren bilden, die auch für das vollständige Tensorprodukt mit $\mathrm{Tor}_*^\Lambda(M, N)$ bezeichnet wird. Wie für das gewöhnliche Tensorprodukt ist das Ergebnis in beiden Fällen dasselbe.

Für eine abgeschlossene Untergruppe H der Gruppe G ist $\mathbb{Z}_p[\![G]\!]$ ein freier pro-endlicher $\mathbb{Z}_p[\![H]\!]$-Modul. Die projektiven $\mathbb{Z}_p[\![G]\!]$-Moduln sind wie gewohnt die direkten Summanden von freien Moduln ([39], Cor. 5.7.2 bzw. Prop. 5.4.2).

[8] Stetige Homomorphismen sind abgeschlossen, Quotienten können also wie gewohnt gebildet werden. Bijektive stetige Abbildungen sind Isomorphismen.

Lemma 5.16. *Falls der pro-endliche Rechtsmodul M oder der pro-endliche Linksmodul N endlich erzeugt ist, gilt $M\hat{\otimes}_{\mathbb{Z}_p[\![G]\!]}N = M \otimes_{\mathbb{Z}_p[\![G]\!]} N$.*

Beweis. Für $N = \Lambda$ liefert die universelle Eigenschaft sofort die Gleichung $M\hat{\otimes}_\Lambda\Lambda = M$, und da der Funktor $\_\hat{\otimes}N$ genau wie $\_ \otimes N$ additiv ist, gilt auch $\Lambda^n\hat{\otimes}N = \Lambda^n \otimes N$ für alle $n \in \mathbb{N}$.

Für den allgemeinen Fall nehmen wir zunächst an, dass M ein Erzeugendensystem aus n Elementen besitzt. Sei $\varphi : \Lambda^n \to M$ der zugehörige Epimorphismus von pro-endlichen Rechtsmoduln. Der Homomorphismus φ induziert einen Epimorphismus $\Lambda^n \otimes N \to M \otimes_\Lambda N$, der stetig ist, falls man $M \otimes_\Lambda N$ als Teilraum von $M\hat{\otimes}_\Lambda N$ auffasst. Das Bild ist also kompakt und damit abgeschlossen in $M\hat{\otimes}_\Lambda N$, und da $M \otimes_\Lambda N$ eine dichte Teilmenge ist, gilt $M \otimes_\Lambda N = M\hat{\otimes}_\Lambda N$.

Dasselbe Argument lässt sich selbstverständlich auch auf ein endliches Erzeugendensystem des Linksmoduls N anwenden. ◻

Falls wir uns also auf endlich erzeugte Moduln einschränken, hat das gewöhnliche Tensorprodukt die universelle Eigenschaft auch in der Kategorie der pro-endlichen Λ-Moduln.

Wählt man für G die triviale Gruppe $\{1\}$, so ist $M\hat{\otimes}_{\mathbb{Z}_p[\![G]\!]}N = M\hat{\otimes}_{\mathbb{Z}_p}N$ das vollständige Tensorprodukt über $\mathbb{Z}_p$, für das wir im Folgenden einfach $M\hat{\otimes}N$ schreiben.

5.3 Gruppenhomologie

Anstatt die Objekte $H_1(C_\infty)$ und $H_1(C)$ mit Hilfe von singulärer Homologie zu untersuchen, kann man die Homologiegruppen und zugehörige Abbildungen und Operationen auch als Objekte in der Gruppenhomologie, ausgehend von der Knotengruppe, auffassen. Analog erhält man die Iwasawa-Moduln als Homologiegruppen der entsprechenden Galoisgruppe. Diese Beschreibung erlaubt also eine einheitliche Behandlung der Situationen in der Knotentheorie und der Zahlentheorie. Wir stellen hier zunächst einige Eigenschaften der Gruppenhomologie von abstrakten Gruppen und Pro-p-Gruppen zusammen. Für abstrakte Gruppen findet man die Ergebnisse zum Beispiel in [5], für pro-endliche Gruppen in [33] oder [47].

5.3.1 Abstrakte Gruppen

Sei G eine Gruppe und M ein $\mathbb{Z}[G]$-Modul. Die i-te Homologiegruppe von G mit Koeffizienten in M ist die Gruppe

$$H_i(G, M) = \mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, M).$$

Die Gruppenhomologie einer Gruppe G bekommt man also als Linksableitung des Funktors $\mathbb{Z} \otimes_{\mathbb{Z}[G]} \_$. Für die Homologiegruppen mit Koeffizienten in $\mathbb{Z}$ schreiben wir auch $H_i(G)$.

Lemma 5.17. $H_1(G, \mathbb{Z}) \cong G^{ab}$.

Beweis. Die exakte Sequenz $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, die sich aus der Augmentationsabbildung ergibt, liefert eine lange exakte Sequenz

$$\cdots \to \mathrm{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}[G]) \to \mathrm{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}) \to \mathrm{Tor}_0^{\mathbb{Z}[G]}(\mathbb{Z}, I_G) \to \mathrm{Tor}_0^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}[G]) \to \dots,$$

wobei $\mathrm{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}[G]) = 0$ und $\mathrm{Tor}_0^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}[G]) = \mathbb{Z}\otimes_G\mathbb{Z}[G] \cong \mathbb{Z}$, sodass die letzte Abbildung die Nullabbildung ist. Wir haben also einen Isomorphismus $\mathrm{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}) \cong \mathrm{Tor}_0^{\mathbb{Z}[G]}(\mathbb{Z}, I_G) = I_G \otimes_G \mathbb{Z}$.

Der Modul $I_G \otimes_G \mathbb{Z}$ ist kanonisch isomorph zum trivialen G-Modul G^{ab}, indem man das Element $(g-1) \otimes 1$ für $g \in G$ auf die Restklasse $\overline{g}$ in G^{ab} abbildet. Diese Definition liefert einen wohldefinierten bijektiven Homomorphismus. $\square$

Lemma 5.18. *Sei $N \subset G$ ein Normalteiler. Dann induziert die Konjugation mit Elementen aus G eine Operation von G/N auf $H_*(N)$.*

Beweis. Sei $\alpha_g : N \to N$ der Isomorphismus $n \mapsto gng^{-1}$. Eine projektive Auflösung von $\mathbb{Z}$ als N-Modul kann durch die Abbildung α_g mit anderen N-Modulstrukturen der Komponenten versehen werden und liefert so eine weitere projektive Auflösung von $\mathbb{Z}$ als N-Modul. Die neue N-Modulstruktur auf den Komponenten ist dann für ein Element n aus dem Normalteiler und x aus dem Modul durch die Vorschrift $n \circ x = (gng^{-1})x$ gegeben.

Die Identität $\mathbb{Z} \to \mathbb{Z}$ besitzt eine bis auf Homotopie eindeutige Fortsetzung zu einer Abbildung dieser beiden Sequenzen. Diese Abbildung liefert eine Abbildung zwischen den Komplexen, die man nach Tensorieren mit $\mathbb{Z}$ über $\mathbb{Z}[N]$ erhält. Also erhält man Abbildungen

$$(\alpha_g)_* : H_*(N) \to H_*(N),$$

die eine Operation von G auf $H_*(N)$ induzieren.

Falls das Element g im Normalteiler enthalten ist, kann man als Fortsetzung der Identität auf $\mathbb{Z}$ die Abbildung τ wählen, die auf jedem der Moduln durch $x \mapsto gx$ definiert ist. Wegen $g(nx) = gng^{-1}(gx) = n \circ (gx)$ ist diese Abbildung verträglich mit den N-Modulstrukturen. Auf den Komplexen, die man nach dem Tensorieren mit $\mathbb{Z}$ erhält, induziert τ aber offenbar die Identität. Damit operiert N trivial auf $H_*(N)$ und induziert eine Operation von G/N auf $H_*(N)$. $\square$

Lemma 5.19. *Identifiziert man $H_1(G')$ mit $(G')^{ab}$ wie in Lemma 5.17, so entspricht die oben definierte Operation von G/G' auf $H_1(G')$ der Operation von G/G' auf $(G')^{ab}$ durch Konjugation.*

Beweis. Die Operation von G/G' auf $H_1(G')$ erhält man für ein Element $g \in G$, indem man die Gruppe G', wie im Beweis von Lemma 5.18 beschrieben, durch $gG'g^{-1}$ ersetzt und die Modulstrukturen der beteiligten Moduln entsprechend ändert. Die Konjugation mit g lässt sich auf $\mathbb{Z}[G']$ fortsetzen, also auch zu einem Automorphismus der kurzen exakten Sequenz $0 \to I_{G'} \to \mathbb{Z}[G'] \to \mathbb{Z} \to 0$, wobei die Abbildung $\mathbb{Z} \to \mathbb{Z}$ auf den Quotienten die Identität ist. Dadurch erhält man eine Abbildung zwischen den langen exakten Sequenzen, und die Abbildung auf $I_{G'} \otimes_{\mathbb{Z}[G']} \mathbb{Z} = \mathrm{Tor}_0(I_{G'}, \mathbb{Z}) \cong H_1(G')$ ist durch Konjugation mit g gegeben. Die Operation entspricht also der Operation von G/G' auf $(G')^{ab}$ durch Konjugation. $\square$

Lemma 5.20 (Shapiro). *Falls H eine Untergruppe von G ist und M ein H-Linksmodul, gibt es natürliche Isomorphismen*

$$H_*(H, M) \cong H_*(G, \mathbb{Z}[G] \otimes_H M).$$

Beweis. Die Funktoren $H_*(H, \_)$ und $H_*(G, \mathbb{Z}[G] \otimes_H \_)$ sind universelle homologische δ-Funktoren von H-Mod in die Kategorie der abelschen Gruppen, da $\mathbb{Z}[G] \otimes_H \_$ freie Objekte auf freie abbildet und $H_*(G, \mathbb{Z}[G] \otimes_H \_)$ damit coeffaçabel ist.[9] Es genügt also, die Isomorphie für $n = 0$ nachzuweisen. In diesem Fall gilt

$$H_0(G, \mathbb{Z}[G] \otimes_H M) = \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M = \mathbb{Z} \otimes_{\mathbb{Z}[H]} M = H_0(H, M).$$

[9] Einen Überblick über abgeleitete Funktoren und δ-Funktoren gibt es zum Beispiel in [14], [33] oder [39].

$\square$

Korollar 5.21. *Für einen Normalteiler H der Gruppe G gilt $H_*(H) \cong H_*(G, \mathbb{Z}[G/H])$ als $\mathbb{Z}[G/H]$-Modul.*

Beweis. Die Aussage folgt wegen $\mathbb{Z}[G/H] \cong \mathbb{Z}[G] \otimes_H \mathbb{Z}$ aus dem Lemma von Shapiro. Nach Lemma 5.18 ist $H_i(H)$ ein G/H-Modul, und die Modulstrukturen stimmen auf den nullten Homologiegruppen überein. $\square$

Lemma 5.22. *Sei H ein Normalteiler in G. Dann gilt für jeden $\mathbb{Z}[H]$-Rechtsmodul M*

$$M \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G/H] = M \otimes_{\mathbb{Z}[H]} \mathbb{Z} = M/MI_H.$$

Beweis. Die erste Gleichung ist klar nach dem letzten Korollar, und der Kern der Abbildung $M \to M \otimes_{\mathbb{Z}[H]} \mathbb{Z}$ ist genau durch den Modul MI_H gegeben. $\square$

Bemerkung. Statt die Homologiegruppen als Ableitung des Funktors $\mathbb{Z} \otimes_{\mathbb{Z}[G]} \_$ zu definieren, formuliert man die Definition häufig mit Hilfe des Funktors, der einem H-Modul M die Gruppe der Co-Invarianten M_H zuordnet. Bis auf Vertauschen von Rechts- und Linksmoduln findet man die Aussage des Lemmas also in der Äquivalenz dieser beiden Definitionen wieder.

5.3.2 Pro-p-Gruppen

In Analogie zur Gruppenhomologie von abstrakten Gruppen definieren wir die i-te Homologiegruppe der Pro-p-Gruppe G mit Koeffizienten in einem pro-endlichen topologischen $\mathbb{Z}_p[\![G]\!]$-Modul M als

$$H_i(G, M) = \mathrm{Tor}_i^{\mathbb{Z}_p[\![G]\!]}(\mathbb{Z}_p, M)$$

([39], §6.3).

Die Aussagen aus Abschnitt 5.3.1 lassen sich auf diesen Fall übertragen:

- $H_1(G, \mathbb{Z}_p) \cong \mathrm{Tor}_1^{\mathbb{Z}_p[\![G]\!]}(\mathbb{Z}_p, \mathbb{Z}_p) \cong I_G \hat{\otimes}_{\mathbb{Z}_p[\![G]\!]} \mathbb{Z}_p \cong G^{ab}$.
- Für einen abgeschlossenen Normalteiler $N \subset G$ induziert die Konjugation mit Elementen aus G eine Operation von G/N auf $H_*(N, \mathbb{Z}_p)$. Dabei beweist man wie in Abschnitt 5.3.1:

Lemma 5.23. *Sei $G' \subset G$ der Abschluss der Kommutatoruntergruppe von G. Identifiziert man $H_1(G', \mathbb{Z}_p)$ mit $(G')^{ab}$, so entspricht die Operation von G/G' auf $H_1(G', \mathbb{Z}_p)$ der Operation von G/G' auf $(G')^{ab}$ durch Konjugation.*

Lemma 5.24 (Shapiro). *Für einen abgeschlossenen Normalteiler H der Gruppe G gilt*

$$H_*(H, \mathbb{Z}_p) \cong H_*(G, \mathbb{Z}_p[\![G/H]\!]).$$

Die Operation von G/H auf $H_*(H, \mathbb{Z}_p)$ stimmt mit dieser Identifizierung mit der Operation von G/H überein, die man auf $H_*(G, \mathbb{Z}_p[\![G/H]\!])$ erhält, die Bijektion ist also ein $\mathbb{Z}_p[\![G/H]\!]$-Modulisomorphismus.

5.3.3 Relative Gruppenhomologie

Aus der anschaulichen Beschreibung des Fox-Kalküls geht hervor, dass es sich dabei geometrisch um die Berechnung einer relativen Homologiegruppe handelt. Um das Verfahren in möglichst ähnlicher Form mittels Gruppenhomologie beschreiben zu können, führen wir relative Gruppenhomologie ein.

Für eine Gruppe G und eine Untergruppe H kann man relative Homologiegruppen $H_i(G, H)$ mit Hilfe von Eilenberg-MacLane-Räumen definieren, also indem man auf topologische Homologietheorien für Paare von Räumen zurückgreift. Das Ziel ist es aber auch hier wieder, diese relativen Homologiegruppen rein algebraisch zu definieren. Dafür beschreiben wir den einfachsten Fall der Konstruktion von H. F. Trotter ([44]), der allgemeiner Homologie für Systeme von Gruppen $(G, G_i, \varphi_i : G_i \to G)$ einführt.

Definition. Sei G eine Gruppe und H eine Untergruppe. Eine projektive Auflösung von $\mathbb{Z}$ über dem System (G, H) ist ein Paar von Komplexen $(X., Y.)$, für die gilt:

- $X.$ ist eine projektive Auflösung von $\mathbb{Z}$ über $\mathbb{Z}[G]$,
- $Y.$ ist von der Form $Y. = \mathbb{Z}[G] \otimes_H \overline{Y}.$ mit einer projektiven Auflösung $\overline{Y}. \to \mathbb{Z} \to 0$ von $\mathbb{Z}$ als $\mathbb{Z}[H]$-Modul,
- $Y.$ ist ein direkter Summand von $X.$

Den $\mathbb{Z}[G]$-Modulhomomorphismus $Y_0 \to \mathbb{Z}$ erhält man aus $Y_0 \to \mathbb{Z}[G] \otimes_H \mathbb{Z}$ durch Zusammensetzen mit der Abbildung $(\varepsilon, \mathrm{id}) : \mathbb{Z}[G] \otimes_H \mathbb{Z} \to \mathbb{Z}$.

Ein Morphismus zwischen zwei solchen projektiven Auflösungen $(X., Y.)$ und $(X.', Y.')$ ist ein Paar $(f., g.)$ von Morphismen von Komplexen, sodass die folgenden Diagramme kommutieren

$$\begin{tikzcd} X. \arrow[r] \arrow[d, "f."] & \mathbb{Z} \arrow[d, equal] \\ X'. \arrow[r] & \mathbb{Z} \end{tikzcd} \qquad \begin{tikzcd} \overline{Y}. \arrow[r] \arrow[d, "g."] & \mathbb{Z} \arrow[d, equal] \\ \overline{Y'}. \arrow[r] & \mathbb{Z} \end{tikzcd}$$

und die Einschränkung von $f.$ auf den direkten Summanden $Y.$ die Abbildung $id \otimes g.$ ist.

Ähnlich definiert man Homotopien zwischen projektiven Auflösungen.

Lemma 5.25. *Für jede Wahl von G und H existieren projektive Auflösungen von $\mathbb{Z}$ über (G, H). Falls zwei solche projektive Auflösungen $(X., Y.)$ und $(X.', Y.')$ gegeben sind, gibt es einen bis auf Homotopie eindeutigen Morphismus $(X., Y.) \to (X.', Y.')$.*

Beweis. Zunächst wählt man eine projektive Auflösung $\overline{Y}.$ von $\mathbb{Z}$ über $\mathbb{Z}[H]$, die durch Tensorieren mit $\mathbb{Z}[G]$ und Zusammensetzen mit $\mathbb{Z}[G] \otimes_H \mathbb{Z} \to \mathbb{Z}$ einen Komplex $Y. = \overline{Y}. \otimes \mathbb{Z}[G] \to \mathbb{Z} \to 0$ liefert. Dieser Komplex lässt sich schrittweise durch Hinzufügen von direkten Summanden zu den Komponenten Y_i zu einer exakten Sequenz $X. \to \mathbb{Z} \to 0$ von $\mathbb{Z}[G]$-Moduln ergänzen.

Genauso verfährt man auch mit den Morphismen von solchen Auflösungen und mit Homotopien: Zunächst konstruiert man wie gewohnt einen Morphismus $\overline{Y}. \to \overline{Y}.'$, der einen Morphismus $Y. \to Y.'$ induziert. Diesen kann man dann auf den Komplex $X.$ fortsetzen, da die direkten Summanden, auf denen die Abbildung noch definiert werden muss, jeweils projektive Moduln sind. Dasselbe Verfahren funktioniert auch für Homotopien. □

Insbesondere sind jeweils zwei projektive Auflösungen homotop, und eine Homotopie zwischen $(X., Y.)$ und $(X.', Y.')$ induziert eine Homotopie zwischen den Quotienten $X./Y.$ und $X.'/Y.'$. Die Homologie von $X./Y.$ hängt damit nicht von der Wahl der projektiven Auflösung ab.

Definition. Die relative Homologie $H_*(G, H; A)$ ist definiert als die Homologie des Komplexes $(X./Y.) \otimes A$ für eine projektive Auflösung $(X., Y.)$ von $\mathbb{Z}$ über (G, H).

Falls G eine Pro-p-Gruppe ist und H eine abgeschlossene Untergruppe von G, definiert man projektive Auflösungen über (G, H), indem man $\mathbb{Z}$ durch $\mathbb{Z}_p$ ersetzt, das Tensorprodukt durch das vollständige Tensorprodukt und alle Gruppenringe durch die korrespondierenden vollständigen Gruppenringe. Die relativen Homologiegruppen sind dann die Homologiegruppen des Komplexes $(X./Y.)\hat{\otimes}A$ für eine projektive Auflösung $(X., Y.)$ von $\mathbb{Z}_p$ über (G, H).

Sei G eine Gruppe, H eine Untergruppe und $(X., Y.)$ eine projektive Auflösung von $\mathbb{Z}$ über (G, H). Da die exakten Sequenzen

$$0 \to Y_n \to X_n \to X_n/Y_n \to 0$$

spalten, erhält man eine exakte Sequenz

$$0 \to Y. \otimes A \to X. \otimes A \to X./Y. \otimes A \to 0$$

und damit, wie man es von der relativen Homologie erwartet, eine lange exakte Sequenz der Homologiegruppen

$$\begin{array}{ccccccccccc}
\cdots \longrightarrow & H_n(Y. \otimes A) & \longrightarrow & H_n(X. \otimes A) & \longrightarrow & H_n(X./Y. \otimes A) & \xrightarrow{\partial} & H_{n-1}(Y. \otimes A) & \longrightarrow \cdots \\
& \| & & \| & & \| & & \| & \\
\cdots \longrightarrow & H_n(H; A) & \longrightarrow & H_n(G; A) & \longrightarrow & H_n(G, H; A) & \xrightarrow{\partial} & H_{n-1}(H; A) & \longrightarrow \cdots
\end{array}$$

Für Pro-p-Gruppen erhält man dieselbe Aussage, wenn man das Tensorprodukt durch das vollständige Tensorprodukt ersetzt.

5.4 Jacobi-Matrizen über Gruppenringen

Mit diesen Hilfsmitteln kann man ohne die anschauliche Beschreibung durch CW-Komplexe eine Präsentationsmatrix der Homologiegruppen bestimmen. Die dafür verwendete freie Auflösung von $\mathbb{Z}$ wurde zuerst von R. C. Lyndon ([26]) beschrieben. Eine Herleitung der Lyndon-Auflösung im pro-endlichen Fall ohne die explizite Beschreibung durch eine Jacobi-Matrix findet man in [33], Ch. V, §6.

5.4.1 Die Lyndon-Auflösung

Sei F die freie Gruppe auf der Menge $\{e_1, \ldots, e_d\}$, $R \subset F$ ein Normalteiler, der (als Normalteiler) von den Elementen $r_j, j \in J$, erzeugt wird, und G der Quotient F/R. Die Gruppe G ist also durch die Präsentation $G = \langle e_i | r_j \rangle$ gegeben.

Lemma 5.26. *Sei X_1 der freie $\mathbb{Z}[G]$-Rechtsmodul auf der Menge $\{a_1, \dots, a_d\}$, sodass die Elemente a_i den Erzeugern e_i von F entsprechen, und X_2 der freie $\mathbb{Z}[G]$-Rechtsmodul auf der Menge $\{b_j\}$, wobei die Elemente b_j den Relatoren r_i entsprechen.*

Dann gibt es eine exakte Sequenz

$$X_2 \xrightarrow{d_2} X_1 \to \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

in der die Abbildung d_2 durch die Jacobi-Matrix $(\frac{\partial r_j}{\partial e_i})$ gegeben ist. Mit $\frac{\partial r_j}{\partial e_i}$ ist in diesem Fall das Bild des entsprechenden Elements aus $\mathbb{Z}[F]$ in $\mathbb{Z}[G]$ gemeint.

Die Sequenz kann damit als Teil einer freien Auflösung von $\mathbb{Z}$ als $\mathbb{Z}[G]$-Modul aufgefasst werden.

Beweis. Die exakte Sequenz

$$0 \to I_F \to \mathbb{Z}[F] \to \mathbb{Z} \to 0$$

liefert durch Tensorieren mit dem $\mathbb{Z}[F]$-Modul $\mathbb{Z}[G]$ eine exakte Sequenz

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, equal] & I_F \otimes_{\mathbb{Z}[F]} \mathbb{Z}[G] \arrow[r] \arrow[d, equal] & \mathbb{Z}[F] \otimes_{\mathbb{Z}[F]} \mathbb{Z}[G] \arrow[r] \arrow[d, equal] & \mathbb{Z} \otimes_{\mathbb{Z}[F]} \mathbb{Z}[G] \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & K \arrow[r] & I_F/I_F I_R \arrow[r] & \mathbb{Z}[F]/\mathbb{Z}[F] I_R \arrow[r] & \mathbb{Z} \arrow[r] & 0,
\end{tikzcd}$$

wobei die Untergruppe $K \subset I_F/I_F I_R$ so gewählt ist, dass die Sequenz exakt wird. Die vertikalen Gleichungen erhält man aus Lemma 5.22. Der Kern K ist einerseits durch den Modul $\mathbb{Z}[F]I_R/I_F I_R$ gegeben, andererseits erhalten wir durch die lange exakte Sequenz für $\mathrm{Tor}_*^{\mathbb{Z}[F]}(\_, \mathbb{Z}[G])$ die folgende Fortsetzung der Sequenz:

$$0 = \mathrm{Tor}_1^{\mathbb{Z}[F]}(\mathbb{Z}[F], \mathbb{Z}[G]) \to \mathrm{Tor}_1^{\mathbb{Z}[F]}(\mathbb{Z}, \mathbb{Z}[G]) \to I_F \otimes_{\mathbb{Z}[F]} \mathbb{Z}[G] \to \mathbb{Z}[F] \otimes_{\mathbb{Z}[F]} \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

Der Kern K ist also andererseits gegeben durch den Modul

$$\mathrm{Tor}_1^{\mathbb{Z}[F]}(\mathbb{Z}, \mathbb{Z}[G]) \cong \mathrm{Tor}_1^{\mathbb{Z}[R]}(\mathbb{Z}, \mathbb{Z}) \cong R^{ab}.$$

Wir bestimmen nun den G-Modulhomomorphismus $R^{ab} \to I_F \otimes_{\mathbb{Z}[F]} \mathbb{Z}[G]$, der der Abbildung $\mathbb{Z}[F]I_R/I_F I_R \to I_F/I_F I_R$ entspricht. Da I_F ein freier $\mathbb{Z}[F]$-Modul ist und isomorph zu Ω_F, erhalten wir einen Isomorphismus

$$I_F \otimes_{\mathbb{Z}[F]} \mathbb{Z}[G] \cong \Omega_F \otimes_{\mathbb{Z}[F]} \mathbb{Z}[G] \cong \mathbb{Z}[G]^d = X_1,$$

der auf dem Modul $\Omega_F \otimes_{\mathbb{Z}[F]} \mathbb{Z}[G]$ durch $de_i \otimes 1 \mapsto a_i$ gegeben ist.

Die kanonische Abbildung $I_R \to \mathbb{Z}[F]I_R/I_F I_R$ ist surjektiv, und da ihr Kern durch I_R^2 gegeben ist, induziert sie einen Isomorphismus $R^{ab} \cong I_R/I_R^2 \cong \mathbb{Z}[F]I_R/I_F I_R$.

Ersetzen wir I_F durch den kanonisch isomorphen Modul Ω_F, so erhalten wir ein kommutatives Diagramm

$$\begin{tikzcd}
R \arrow[r] \arrow[d] & F \arrow[r, "d"] & \Omega_F \arrow[r] & \Omega_F/I_F I_R \arrow[d, "\cong"] & & \\
I_R/I_R^2 \arrow[rrr, "\varphi"] & & & \mathbb{Z}[G]^d \arrow[r] & \mathbb{Z}[G] \arrow[r] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

sodass die Abbildung φ über die Derivation $F \to \Omega_F$ faktorisiert.

Der G-Modul R^{ab} kann als Quotient des freien $\mathbb{Z}[G]$-Moduls X_2 geschrieben werden, indem wir das Basiselement $b_j \in X_2$ auf $\overline{r}_j \in R^{ab}$ abbilden. Zusammensetzen dieser Abbildung $X_2 \to R^{ab}$ mit der Abbildung $\varphi : R^{ab} \to \mathbb{Z}[G]^d$ liefert die gesuchte Sequenz

$$X_2 \xrightarrow{d_2} X_1 \to \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

Wir müssen nun noch verifizieren, dass die Abbildung d_2 durch die oben angegebene Matrix gegeben ist. Mit Hilfe des kommutativen Diagramms lassen sich die Bilder der Basiselemente von X_2 unter der Abbildung d_2 beschreiben:

Das Element $r_j \in R$, das dem Erzeuger b_j entspricht, wird zunächst auf $dr_j \in \Omega_F$ abgebildet und hat dort nach der Formel aus Abschnitt 5.1.2 die Darstellung $\Sigma_i \frac{\partial r_j}{\partial e_i} de_i$. Nach Übergang zum Quotienten $\mathbb{Z}[G]^d$ erhalten wir als Bild also das Element $\Sigma_i \frac{\partial r_j}{\partial e_i} a_i$. □

In Anlehnung an [7] kann das Resultat mit Hilfe von relativen Homologiegruppen folgendermaßen formuliert werden:

Satz 5.27. *Sei $G = \langle e_i | r_j \rangle$ wie oben und $H \subset G$ ein Normalteiler. Dann ist die Matrix $(\overline{\frac{\partial r_j}{\partial e_i}})$ eine Präsentationsmatrix über $\mathbb{Z}[G/H]$ für die relative Homologiegruppe $H_1(G, 1; \mathbb{Z}[G/H])$.*

Beweis. Wir haben oben einen Teil einer projektiven Auflösung

$$X_2 \to X_1 \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

für den $\mathbb{Z}[G]$-Modul $\mathbb{Z}$ konstruiert. Für den $\mathbb{Z}[1]$-Modul $\mathbb{Z}$ wählen wir einfach die Auflösung

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

Die relative Gruppenhomologie von $(G, 1)$ mit Koeffizienten in $\mathbb{Z}[G/H]$ ergibt sich durch Tensorieren der beiden Komplexe mit $\mathbb{Z}[G/H]$ und Berechnen der Homologie des Quotienten. Aus dem ersten Komplex bekommen wir

$$X_2 \otimes_G \mathbb{Z}[G/H] \xrightarrow{d_2} X_1 \otimes_G \mathbb{Z}[G/H] \to \mathbb{Z}[G/H] \to 0,$$

wobei die erste Abbildung durch Reduktion der Jacobi-Matrix mod H, also durch die Matrix $(\overline{\frac{\partial r_j}{\partial e_i}}) \in \mathbb{Z}[G/H]$, gegeben ist. Als zweiten Komplex bekommen wir

$$0 \to \mathbb{Z}[G/H] \to 0.$$

Bilden des Quotienten liefert den Komplex

$$X_2 \otimes_G \mathbb{Z}[G/H] \xrightarrow{d_2} X_1 \otimes_G \mathbb{Z}[G/H] \to 0 \to 0,$$

und die erste Homologiegruppe ist durch den Quotienten $X_1 \otimes_G \mathbb{Z}[G/H] / \operatorname{im}(d_2)$ gegeben. Wir haben also eine exakte Sequenz

$$X_2 \otimes_G \mathbb{Z}[G/H] \xrightarrow{d_2} X_1 \otimes_G \mathbb{Z}[G/H] \to H_1(G, 1; \mathbb{Z}[G/H]) \to 0$$

konstruiert, mit anderen Worten eine Präsentation des $\mathbb{Z}[G/H]$-Moduls $H_1(G, 1; \mathbb{Z}[G/H])$ mit Präsentationsmatrix $(\overline{\frac{\partial r_j}{\partial e_i}})$. □

Im pro-endlichen Fall lassen sich die in diesem Abschnitt aufgeführten Sätze mit Hilfe der Ergebnisse, die wir über Differentialmoduln und Gruppenhomologie in diesem Fall zusammengestellt haben, genauso beweisen. In [34], §4.1 wird eine andere Formulierung verwendet, das Ergebnis ist aber im Wesentlichen dasselbe:

Satz 5.28. *Sei $\langle e_1, \ldots, e_n | r_1, \ldots, r_m \rangle$ eine Präsentation der Pro-p-Gruppe G und H ein abgeschlossener Normalteiler von G. Dann ist die Matrix $(\overline{\frac{\partial r_j}{\partial e_i}})$ eine Präsentationsmatrix über $\mathbb{Z}_p[\![G/H]\!]$ für die relative Homologiegruppe $H_1(G, 1; \mathbb{Z}_p[\![G/H]\!])$.*

5.4.2 Anwendung auf das Alexanderpolynom

Der Alexandermodul eines Knotens wurde in Abschnitt 1.1 als erste Homologiegruppe der maximalen abelschen Überlagerung seines Knotenkomplements definiert. Aus der Knotengruppe G erhält man diese Gruppe als maximalen abelschen Quotienten der Kommutatorgruppe G'. Mit Hilfe von Gruppenhomologie findet man eine weitere Beschreibung:

Satz 5.29. *Der Alexandermodul ist als $\mathbb{Z}[G^{ab}]$-Modul isomorph zu $H_1(G, \mathbb{Z}[G^{ab}])$.*

Beweis. Nach dem Lemma von Shapiro ist $H_1(G, \mathbb{Z}[G^{ab}])$ als $\mathbb{Z}[G^{ab}]$-Modul isomorph zu $H_1(G', \mathbb{Z})$. Diese Homologiegruppe ist nach den Ergebnissen aus Abschnitt 5.3.1 isomorph zum $\mathbb{Z}[G^{ab}]$-Modul $(G')^{ab}$ und damit der Alexandermodul. □

Die Beziehung zwischen dem Alexandermodul und der relativen Homologiegruppe aus dem letzten Abschnitt wird durch die folgende Beobachtung hergestellt:

Sei G eine abstrakte Gruppe oder eine Pro-p-Gruppe. Sei D ein (Pro-p-)Quotient von G und A der zugehörige (vollständige) Gruppenring. Aus der langen exakten Sequenz des Paares $(G, 1)$ mit Koeffizienten in A erhält man wegen $H_1(1, A) = 0$ den Teil

$$0 \to H_1(G; A) \to H_1(G, 1; A) \to I_D \to 0,$$

wobei I_D das Augmentationsideal des Gruppenrings A bezeichnet. Falls der Gruppenring ein noetherscher faktorieller Ring ist, ist sein Augmentationsideal ein torsionsfreier Modul, und wenn $r \in \mathbb{N}_0$ sein Rang ist, bekommen wir aus dieser Sequenz und Satz 1.5 die Gleichung $\Delta_0(H_1(G; A)) = \Delta_r(H_1(G, 1; A))$. Insbesondere gilt:

Korollar 5.30. *Für einen Knoten mit Knotengruppe G ist $\Delta(t) = \Delta_1(H_1(G, 1; \mathbb{Z}[t, t^{-1}]))$.*

5.5 Beispiele

Mit Hilfe der Präsentationsmatrix aus dem letzten Abschnitt werden wir für einige Beispiele aus der Knotentheorie und der Zahlentheorie die Invarianten Δ_i bestimmen.

Wie nützlich die Methode ist, kann man erkennen, wenn man damit noch einmal das Alexanderpolynom eines Torusknoten berechnet. Als praxisnahe Anwendung bestimmen wir das Alexanderpolynom eines Palsteks, und als Beispiel aus der Zahlentheorie untersuchen wir Galoisgruppen von p-Erweiterungen mit vorgegebener Präsentation durch Erzeuger und Relationen.

5.5.1 Torusknoten

Die Knotengruppe eines Torusknotens mit Parametern a und b hat nach Abschnitt 1.6.1 die Präsentation $G = \langle x, y | x^a y^{-b} \rangle$, wobei die Projektion $G \to G/G' \cong \langle t \rangle$ die Erzeuger x und y auf t^b bzw. t^a abbildet. Berechnen der partiellen Derivationen liefert die Jacobi-Matrix

$$\begin{pmatrix} \dfrac{\partial(x^a y^{-b})}{\partial x} \\ \dfrac{\partial(x^a y^{-b})}{\partial y} \end{pmatrix} = \begin{pmatrix} 1 + x + \cdots + x^{a-1} \\ \\ x^a(-y^{-1} - \cdots - y^{-b}) \end{pmatrix}.$$

Die Präsentationsmatrix A der relativen Homologiegruppe $H_1(G, 1; \mathbb{Z}[\langle t \rangle])$ über $\mathbb{Z}[\langle t \rangle]$ erhält man durch Einsetzen von t^a für x und t^b für y:

$$A = \begin{pmatrix} \dfrac{1 - t^{ab}}{1 - t^b} \\ \dfrac{-t^{ab} t^{-a}(1 - t^{-ab})}{1 - t^{-a}} \end{pmatrix}.$$

Nach Korollar 5.30 ist das Alexanderpolynom $\Delta(t)$ der größte gemeinsame Teiler der Einträge von A, also das Element $\Delta_1(H_1(G, 1; \mathbb{Z}[\langle t \rangle])$. Wir erhalten die schon aus Abschnitt 1.6.2 bekannte Aussage:

Satz 5.31. *Das Alexanderpolynom eines Torusknotens mit Parametern a und b ist das Polynom*

$$\Delta(t) = \frac{(1 - t)(1 - t^{ab})}{(1 - t^a)(1 - t^b)}.$$

5.5.2 Palstek

Als zweites Beispiel berechnen wir das Alexanderpolynom für den im ersten Kapitel schon erwähnten Knoten mit der Nummer 6_2.

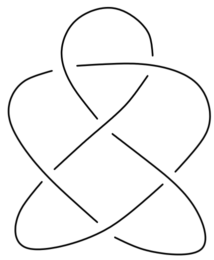


Abbildung 12: Palstek

Eine Wirtinger-Präsentation der Knotengruppe ist gegeben durch

$$G = \langle x_1, x_2, x_3, x_4, x_5, x_6 | x_3 x_6 x_3^{-1} x_1^{-1}, x_2^{-1} x_4^{-1} x_1 x_4, x_6 x_2 x_6^{-1} x_3^{-1}, x_5 x_3 x_5^{-1} x_4^{-1}, x_5^{-1} x_1^{-1} x_4 x_1 \rangle.$$

Man sieht sofort, dass als Quotientenabbildung $G \to G^{ab} = \langle t \rangle$ die Abbildung gewählt werden kann, die jeden der sechs Erzeuger auf t abbildet. Die zugehörige Präsentationsmatrix von $H_1(G,1;\mathbb{Z}[t,t^{-1}])$ über $\mathbb{Z}[t,t^{-1}]$ ist die Matrix

$$\begin{pmatrix} -1 & t^{-2} & 0 & 0 & -t^{-2}+t^{-1} \\ 0 & -t^{-1} & t & 0 & 0 \\ 1-t & 0 & -1 & t & 0 \\ 0 & -t^{-2}+t^{-1} & 0 & -1 & t^{-2} \\ 0 & 0 & 0 & 1-t & -t^{-1} \\ t & 0 & 1-t & 0 & 0 \end{pmatrix}.$$

Als Determinante der 5x5-Teilmatrizen erhält man bis auf Multiplikation mit $\pm t^k$ jeweils $1-t^{-1}-3t+3t^2-t^3$. Dieses Element erzeugt also das erste Fitting-Ideal der Matrix, und damit gilt:

Satz 5.32. *Das Alexanderpolynom eines Palsteks ist das Polynom*

$$\Delta(t) = t^4 - 3t^3 + 3t^2 - 3t + 1.$$

5.5.3 Erweiterungen mit vorgegebenen Verzweigungsstellen

In seinem Buch [21] gibt H. Koch mehrere Beispiele von Galoisgruppen an, für die er eine Präsentation als Pro-p-Gruppe durch Erzeuger und Relationen bestimmen konnte ([22]). Für zwei dieser Beispiele berechnen wir hier die zugehörigen charakteristischen Polynome.

1) Sei $K=\mathbb{Q}$, p eine ungerade Primzahl, q eine Primzahl mit $q\equiv 1 \mod p$, aber $q \not\equiv 1 \mod p^2$, und $S=\{p,q\}$. Dann hat die Galoisgruppe der maximalen außerhalb von S unverzweigten p-Erweiterung von K eine Präsentation mit zwei Erzeugern s und t und der Relation $r=t^{q-1}[t^{-1},s^{-1}]$:

$$G_S(p) = \langle s,t \mid t^{q-1}[t^{-1},s^{-1}]\rangle.$$

Dabei wird für die Kommutatoren hier die Konvention $[a,b]=a^{-1}b^{-1}ab$ verwendet.

Der Quotient nach der von t erzeugten Untergruppe liefert eine zu $\mathbb{Z}_p$ isomorphe Gruppe mit Erzeuger $\overline{s}$. Die Jacobi-Matrix mit Einträgen in $\mathbb{Z}_p[\![\mathbb{Z}_p]\!]$ ist gegeben durch

$$\begin{pmatrix} \frac{\partial r}{\partial s} \\ \frac{\partial r}{\partial t} \end{pmatrix} = \begin{pmatrix} 0 \\ q+\overline{s} \end{pmatrix}.$$

Das erste Fitting-Ideal ist offenbar das Hauptideal $(q+\overline{s})$. Wählen wir den Isomorphismus $\mathbb{Z}_p[\![\mathbb{Z}_p]\!] \to \mathbb{Z}_p[\![T]\!]$ so, dass $\overline{s}$ auf $T+1$ abgebildet wird, so erhalten wir als Ideal im Potenzreihenring das Ideal $(T+1+q)$.

2) Sei $K=\mathbb{Q}(\sqrt{-23})$, $p=3$ und $S=\{\mathfrak{p}_1,\mathfrak{p}_2,q,\mathfrak{p}\}$, wobei $\mathfrak{p}_1$ und $\mathfrak{p}_2$ die beiden Teiler von (3) in K sind, $q\not\equiv 1 \mod 9$ eine Primzahl, die in K ebenfalls prim ist, und $\mathfrak{p}$ ein Primideal, das kein Hauptideal ist. Dann ist

$$G = \langle s_q, t_q, s_\mathfrak{p}, t_\mathfrak{p} | t_q^{q-1}[t_q^{-1}, s_q^{-1}], t_\mathfrak{p}^{N\mathfrak{p}-1}[t_\mathfrak{p}^{-1}, s_\mathfrak{p}^{-1}]\rangle$$

eine Präsentation der maximalen außerhalb von 3 unverzweigten Pro-3-Erweiterung von K.

Der maximale abelsche Quotient hat als $\mathbb{Z}_3$-Modul den Rang 2, und die Bilder von s_q und $s_\mathfrak{p}$ erzeugen den maximalen torsionsfreien abelschen Quotienten $\Gamma\cong\mathbb{Z}_p^2$. Der zugehörige

Gruppenring ist isomorph zu $\mathbb{Z}_p[\![T_1, T_2]\!]$, wobei wir den Isomorphismus $\mathbb{Z}_p[\![\Gamma]\!] \to \mathbb{Z}_p[\![T_1, T_2]\!]$ so wählen, dass das Bild von s_q auf $T_1 + 1$ und das Bild von $s_\mathfrak{p}$ auf $T_2 + 1$ abgebildet werden.

Die Jacobi-Matrix mit Einträgen im Potenzreihenring ist die Matrix

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \\ T_1 + 1 + q & 0 \\ 0 & T_2 + 1 + N\mathfrak{p} \end{pmatrix}$$

und das zweite Fitting-Ideal von $H_1(G, 1; \mathbb{Z}_p[\![T_1, T_2]\!])$ ist das Ideal $((T_1 + 1 + q)(T_2 + 1 + N\mathfrak{p}))$.

Wenn wir den Torsions-Untermodul von $H_1(G, 1; \mathbb{Z}_p[\![T_1, T_2]\!])$ mit M bezeichnen, ist der Erzeuger $(T_1 + 1 + q)(T_2 + 1 + N\mathfrak{p})$ nach Satz 1.5 das Element $\Delta_0(M)$. Aus der exakten Sequenz

$$0 \to H_1(G; \mathbb{Z}_p[\![T_1, T_2]\!]) \to H_1(G, 1; \mathbb{Z}_p[\![T_1, T_2]\!]) \to I_\Gamma \to 0$$

kann man ablesen, dass die Torsions-Untermoduln der Homologiegruppen $H_1(G, 1; \mathbb{Z}_p[\![T_1, T_2]\!])$ und $H_1(G; \mathbb{Z}_p[\![T_1, T_2]\!])$ übereinstimmen. Das Polynom ist also das charakteristische Polynom von $H_1(G; \mathbb{Z}_p[\![T_1, T_2]\!])$.

Die nächsten Abschnitte befassen sich damit, wie diese Beispiele im Rahmen der Analogie zwischen Knotentheorie und Iwasawatheorie eingeordnet werden können.

5.6 Alexanderpolynome von Verschlingungen

Die Knoteninvarianten aus dem ersten Teil lassen sich auf Verschlingungen, die aus mehr als einer Komponente bestehen, verallgemeinern; als Alexanderpolynom erhält man dann ein Laurent-Polynom in mehreren Variablen. Einen kurzen Überblick über Alexanderpolynome von Verschlingungen findet man in Kapitel 7 von [19], aus dem wir hier alles Nötige wiedergeben.

Lemma 5.33. *Die erste Homologiegruppe des Komplements einer Verschlingung L mit k Komponenten ist isomorph zu $\mathbb{Z}^k$.*

Beweis. Die Aussage lässt sich genauso beweisen wie Satz 1.1: Falls V eine Umgebung der Verschlingung L in S^3 ist, die aus k Volltori besteht, gilt

$$H_1(S^3 \backslash L) \cong H_1(S^3 \backslash V^\circ) \cong H_2(S^3, S^3 \backslash V^\circ) \cong H_2(V, \partial V) \cong H^1(V) \cong H^1(L) \cong \mathbb{Z}^k.$$

□

Sei C das Komplement der Verschlingung und C_∞ seine universelle abelsche Überlagerung. Die Decktransformationsgruppe D ist nach dem Lemma eine freie abelsche Gruppe vom Rang k, und der Gruppenring, der in diesem Fall den Laurent-Polynomring $\mathbb{Z}[\mathbb{Z}] \cong \mathbb{Z}[T, T^{-1}]$ ersetzt, ist der Ring $\mathbb{Z}[\mathbb{Z}^k]$.

Lemma 5.34. *Der Gruppenring $\mathbb{Z}[\mathbb{Z}^k]$ ist zum Laurent-Polynomring $\mathbb{Z}[T_1, T_1^{-1}, \ldots, T_k, T_k^{-1}]$ isomorph, und dieser Ring ist noethersch und faktoriell.*

Beweis. Einen Isomorphismus erhält man durch Auswahl von k Erzeugern von $\mathbb{Z}^k$, die auf $T_1, \ldots, T_k$ abgebildet werden. Der Laurent-Polynomring ist als Lokalisierung eines Polynomrings über $\mathbb{Z}$ noethersch und faktoriell. □

Definition. Der Alexandermodul $A(L)$ der Verschlingung ist der $\mathbb{Z}[D]$-Modul $H_1(C_\infty)$. Das Alexanderpolynom von L ist der größte gemeinsame Teiler $\Delta_0(H_1(C_\infty))$ der Elemente aus dem nullten Fitting-Ideal des Alexandermoduls.

Im Fall eines Knotens mit Knotengruppe G haben wir gezeigt, dass das Alexanderpolynom ein Erzeuger des nullten Fitting-Ideals von $H_1(G;\mathbb{Z}[G^{ab}])$ ist oder alternativ aus dem ersten Fitting-Ideal der relativen Homologiegruppe $H_1(G,1;\mathbb{Z}[G^{ab}])$ bestimmt werden kann. Für eine Verschlingung mit $\pi_1(C) = G$ folgt aus der Beobachtung in Abschnitt 5.4.2 dasselbe Resultat, da das Augmentationsideal I_D auch hier ein torsionsfreier Modul vom Rang 1 ist.

Satz 5.35. *Falls $k > 1$, ist das erste Fitting-Ideal des Moduls $H_1(G,1;\mathbb{Z}[D])$ von der Form $I_D \cdot (\Delta)$ mit $\Delta \in \mathbb{Z}[D]$.*

Beweis. Sei $G = \langle e_i | r_j \rangle$ eine Wirtinger-Präsentation der Fundamentalgruppe von $S^3 \backslash L$ mit n Erzeugern und $n-1$ Relationen.[10] Die Matrix $(\overline{\frac{\partial r_j}{\partial e_i}})$ ist nach Abschnitt 5.4 eine Präsentationsmatrix von $H_1(G,1;\mathbb{Z}[D])$ als $\mathbb{Z}[D]$-Modul. Sei D_i die Determinante der Teilmatrix, die man durch Streichen der i-ten Spalte a_i erhält. Aus der Formel

$$r_k - 1 = \sum_i \frac{\partial r_k}{\partial e_i}(e_i - 1)$$

(Satz 5.5) folgt, dass $\sum_i a_i(e_i - 1) = 0$ in $\mathbb{Z}[G]$ und damit $\sum_i a_i(\overline{e}_i - 1) = 0$ in $\mathbb{Z}[D]$. Also gilt für $j \neq i$:

$$\begin{aligned} D_j(\overline{e}_i - 1) &= \det(a_1, \ldots, a_i(\overline{e}_i - 1), \ldots, \hat{a_j}, \ldots, a_n) \\ &= \det(a_1, \ldots, -\sum_{k \neq i} a_k(\overline{e}_k - 1), \ldots, \hat{a_j}, \ldots, a_n) \\ &= \det(a_1, \ldots, -a_j(\overline{e}_j - 1), \ldots, \hat{a_j}, \ldots, a_n) \\ &= \pm D_i(\overline{e}_j - 1). \end{aligned}$$

Falls $\overline{e}_i \neq \overline{e}_j$ in D, folgt daraus $(\overline{e}_i - 1)|D_i$, also gibt es $\Delta_i \in \mathbb{Z}[D]$ mit $\Delta_i(\overline{e}_i - 1) = D_i$. Da $\mathbb{Z}[D]$ faktoriell ist und wir vorausgesetzt haben, dass mindestens zwei Elemente $\overline{e}_i$ verschieden sind, folgt aus $\Delta_i(\overline{e}_i - 1)(\overline{e}_j - 1) = \Delta_j(\overline{e}_j - 1)(\overline{e}_i - 1)$, dass alle Δ_i bis auf Vorzeichen übereinstimmen. Die Elemente $\overline{e}_i - 1$ erzeugen das Augmentationsideal von D, und das erste Fitting-Ideal wird von den Minoren $D_i = \Delta_1(\overline{e}_i - 1)$ erzeugt, ist also von der Form $I_D \cdot (\Delta)$ □

Das Alexanderpolynom der Verschlingung ist der größte gemeinsame Teiler der Elemente aus $F_1(H_1(G,1;\mathbb{Z}[D]))$, also das Element $\Delta = \Delta(T_1, \ldots, T_k)$ aus dem Satz.

Bemerkung. Als Polynom hängt $\Delta(T_1, \ldots, T_k)$ von der Wahl des Isomorphismus

$$\mathbb{Z}[\mathbb{Z}^k] \to \mathbb{Z}[T_1, T_1^{-1}, \ldots, T_k, T_k^{-1}]$$

ab; indem man als Erzeuger von $\mathbb{Z}^k$ jeweils Meridiane der einzelnen Knoten wählt, erhält man aber Eindeutigkeit zumindest bis auf Vertauschen von T_i und T_i^{-1}. Genau wie für Knoten ist in diesem Fall bekannt, dass sich das Ideal (Δ) dadurch nicht ändert ([19], Th. 7.4.1).

[10] s. Abschnitt 1.3 und [24], Ch. 11

Verschlingungen in 3-Mannigfaltigkeiten

Um das Alexanderpolynom von Knoten oder Verschlingungen definieren zu können, haben wir bis auf die Homologiegruppen keine speziellen Eigenschaften der 3-Sphäre verwendet. Man sieht also sofort, dass sich die Definition ohne Änderungen auf Knoten und Verschlingungen in Homologie-3-Sphären, also 3-Mannigfaltigkeiten mit derselben Homologie wie S^3, übertragen lässt. Falls M eine 3-Mannigfaltigkeit mit nichttrivialer erster Homologiegruppe ist, können wir folgendermaßen trotzdem eine ähnliche Invariante konstruieren (vgl. [45], §11.2):

Sei L eine Verschlingung in M und $C = M\backslash L$ ihr Komplement mit Fundamentalgruppe G. Die universelle freie abelsche Überlagerung $\overline{C}$ von C ist die eindeutig bestimmte Überlagerung mit Decktransformationsgruppe $D = G^{ab}/\operatorname{Tors}(G^{ab})$, also die maximale Überlagerung, deren Decktransformationsgruppe eine freie abelsche Gruppe ist. Falls k den Rang von D bezeichnet, ist der Gruppenring $\mathbb{Z}[D]$ wieder isomorph zum Laurent-Polynomring $\mathbb{Z}[T_1, T_1^{-1}, \ldots, T_k, T_k^{-1}]$.

Definition. Den $\mathbb{Z}[D]$-Modul $H_1(\overline{C})$ bezeichnen wir als Alexandermodul der Verschlingung.

Aus dem Alexandermodul erhält man als Invariante den größten gemeinsamen Teiler $\Delta_0(H_1(\overline{C}))$ der Elemente aus dem nullten Fitting-Ideal. Zunächst ist $\Delta_0(H_1(\overline{C}))$ ein Element von $\mathbb{Z}[D]/\pm D$, nach Wahl eines Isomorphismus $D \to \mathbb{Z}^k$ erhalten wir ein Laurent-Polynom $\Delta_0(H_1(\overline{C}))$ in den Variablen $T_1, \ldots, T_k$. Wir bezeichnen es als Alexanderpolynom der Verschlingung in M.

5.7 Maximale S-verzweigte p-Erweiterungen

Eine offensichtliche Verallgemeinerung im zahlentheoretischen Fall, die als Analogon einer Verschlingung aufgefasst werden kann, besteht darin, statt einer einzigen Primzahl p eine endliche Menge S von Primzahlen zu betrachten. Das Komplement einer Verschlingung entspricht dann der Menge $\operatorname{Spec}\mathbb{Z}\backslash S$, wobei wir die Menge der zugehörigen Ideale ebenfalls mit S bezeichnen.

Genau wie in Satz 3.17 erhält man als Fundamentalgruppe von $\operatorname{Spec}\mathbb{Z}\backslash S$ die Galoisgruppe der maximalen außerhalb von S unverzweigten Erweiterung von $\mathbb{Q}$. Wir wählen wieder eine ungerade Primzahl p und betrachten nur solche Mengen S, die die Menge S_p aller Stellen über p enthalten.

Bemerkung. Eine Stelle $\mathfrak{p}$ eines Zahlkörpers, die nicht über p liegt, kann in einer p-Erweiterung nur dann verzweigen, wenn $N\mathfrak{p} \equiv 1 \mod p$ ([33], Ch. X §6). Wir können also vereinbaren, dass S keine unendlichen Stellen und keine Stellen mit $N\mathfrak{p} \not\equiv 0; 1 \mod p$ enthalten soll.

Falls K ein total reeller Zahlkörper ist, impliziert die Leopoldt-Vermutung nach Satz 2.41, dass die zyklotomische $\mathbb{Z}_p$-Erweiterung K_∞/K die einzige $\mathbb{Z}_p$-Erweiterung ist. Wir können wie im Fall $S = S_p$ die maximale abelsche p-Erweiterung von K_∞ betrachten, die bei allen Stellen aus S unverzweigt ist.

Satz 5.36. *Sei K_∞/K die zyklotomische $\mathbb{Z}_p$-Erweiterung von K und $\mathcal{X}_\infty^{(S)}$ die Galoisgruppe der maximalen abelschen S-verzweigten p-Erweiterung von K_∞. Dann ist $\mathcal{X}_\infty^{(S)}$ ein endlich erzeugter Torsionsmodul über der Iwasawa-Algebra $\Lambda = \mathbb{Z}_p[\![T]\!]$. Das charakteristische Polynom ergibt sich als größter gemeinsamer Teiler der Elemente des nullten Fitting-Ideals von $\mathcal{X}_\infty^{(S)}$ oder als charakteristisches Polynom der Abbildung $T \otimes id : \mathcal{X}_\infty^{(S)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to \mathcal{X}_\infty^{(S)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.*

Beweis. Unter Beachtung der Bemerkung zu Satz 2.41 folgt die erste Aussage mit demselben Argument wie im Fall $S = S_p$ (Satz 2.48). Die zweite Aussage wurde in Satz 2.49 bereits gezeigt. □

5.8 Mehrfache $\mathbb{Z}_p$-Erweiterungen

Bisher haben wir uns auf total reelle Zahlkörper beschränkt, für die die Leopoldt-Vermutung impliziert, dass die zyklotomische $\mathbb{Z}_p$-Erweiterung die einzige $\mathbb{Z}_p$-Erweiterung ist. Im Allgemeinen haben Zahlkörper aber mehr als eine $\mathbb{Z}_p$-Erweiterung.

Wir bezeichnen mit $\delta(K)$ wieder die Abweichung von der Leopoldt-Vermutung für den Körper K. Als Folgerung aus Satz 2.41 ergibt sich:

Satz 5.37. *Die Galoisgruppe der Zusammensetzung $\tilde{K}$ aller $\mathbb{Z}_p$-Erweiterungen eines Zahlkörpers K ist isomorph zu $\mathbb{Z}_p^{r_2+1+\delta(K)}$. Man erhält sie aus der Galoisgruppe der maximalen abelschen p-verzweigten p-Erweiterung $M_p(K)$ über K als Quotient nach der Torsionsuntergruppe.*

Beweis. Jede $\mathbb{Z}_p$-Erweiterung ist außerhalb von p unverzweigt, also ist $\tilde{K}$ in $M_p(K)$ enthalten. Die Galoisgruppe $\mathrm{Gal}(M_p(K)/K)$ ist nach Satz 2.41 ein endlich erzeugter $\mathbb{Z}_p$-Modul vom Rang $r_2+1+\delta(K)$, also von der Form $\mathbb{Z}_p^{r_2+1+\delta(K)} \times A$ mit einer endlichen p-Gruppe A. Die Zusammensetzung aller $\mathbb{Z}_p$-Erweiterungen enthält dann offenbar den Fixkörper der Torsionsuntergruppe A, und andererseits ist jede $\mathbb{Z}_p$-Erweiterung in diesem Fixkörper enthalten. Also ist die gesuchte Galoisgruppe $\mathrm{Gal}(\tilde{K}/K)$ genau der torsionsfreie Anteil $\mathbb{Z}_p^{r_2+1+\delta(K)}$. □

Der Gruppenring, der in diesem Fall die Iwasawa-Algebra $\mathbb{Z}_p[\![\Gamma]\!]$ ersetzt, ist nach dem letzten Satz der Ring $\mathbb{Z}_p[\![\mathbb{Z}_p^d]\!]$ mit $d = r_2 + 1 + \delta$. Wir bezeichnen ihn wieder mit Λ.

Lemma 5.38. *Es gilt $\Lambda \cong \mathbb{Z}_p[\![T_1, \dots, T_d]\!]$, und dieser Ring ist noethersch und faktoriell. Λ ist lokaler Ring mit dem maximalen Ideal $\mathfrak{m} = (p, T_1, \dots, T_d)$ und in der $\mathfrak{m}$-adischen Topologie kompakt und vollständig.*

Beweis. Einerseits ist $\mathbb{Z}_p[\![\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p]\!] \cong \mathbb{Z}_p[\![\mathbb{Z}_p]\!]\hat{\otimes} \dots \hat{\otimes}\mathbb{Z}_p[\![\mathbb{Z}_p]\!]$, da für zwei Pro-$p$-Gruppen G und G' mit Systemen von offenen Normalteilern $\{N\}, \{N'\}$ gilt

$$\begin{aligned}
\mathbb{Z}_p[\![G]\!]\hat{\otimes}\mathbb{Z}_p[\![G']\!] &= \varprojlim\, (\mathbb{Z}/p^m\mathbb{Z})[G/N] \otimes (\mathbb{Z}/p^n\mathbb{Z})[G'/N'] \\
&= \varprojlim\, (\mathbb{Z}/p^n\mathbb{Z})[G/N \times G'/N'].
\end{aligned}$$

Andererseits ergibt sich auch $\mathbb{Z}_p[\![T_1, \dots, T_d]\!]$ als das d-fache vollständige Tensorprodukt von $\mathbb{Z}_p[\![T]\!]$:

$$\begin{aligned}
\mathbb{Z}_p[\![T_1, \dots, T_d]\!] &= \varprojlim \mathbb{Z}_p[\![T_1, \dots, T_d]\!]/(T_1, \dots, T_d)^n \\
&= \varprojlim \mathbb{Z}_p[T_1, \dots, T_d]/(T_1^{n_1}, \dots, T_d^{n_d}) \\
&= \varprojlim (\mathbb{Z}_p[T_1]/(T_1^{n_1}) \otimes \cdots \otimes \mathbb{Z}_p[T_d]/(T_1^{n_d})) \\
&= \mathbb{Z}_p[\![T_1]\!]\hat{\otimes} \dots \hat{\otimes}\mathbb{Z}_p[\![T_d]\!].
\end{aligned}$$

Die erste Behauptung ergibt sich jetzt also aus Satz 2.16, wo die Aussage für den Fall $d = 1$ gezeigt wurde. Wie in diesem Fall sind Potenzreihen, deren konstanter Koeffizient eine Einheit in $\mathbb{Z}_p$ ist, invertierbar. Das einzige maximale Ideal ist also $(p, T_1, \dots, T_d)$.

Als Vervollständigung eines noetherschen Rings ist Λ wieder noethersch und nach Definition der $\mathfrak{m}$-adischen Topologie vollständig und kompakt. Potenzreihenringe in d Variablen über einem diskreten Bewertungsring sind nach [4], VII.3.9, Prop. 8 faktoriell. □

Bemerkung. Ein Isomorphismus ist wie im Fall einer einfachen $\mathbb{Z}_p$-Erweiterung gegeben, indem man d Erzeuger der Gruppe $\mathbb{Z}_p^d$ auswählt und auf die Elemente $T_1 + 1, \dots, T_d + 1$ abbildet.

Beim Übergang von Knoten zu Verschlingungen wurde die Gruppenalgebra $\mathbb{Z}[T,T^{-1}]$ durch den Laurent-Polynomring $\mathbb{Z}[T_1,T_1^{-1},\dots,T_k,T_k^{-1}]$ in mehreren Variablen ersetzt. Der Übergang von $\mathbb{Q}$ zu Zahlkörpern mit komplexen Einbettungen entspricht dieser Situation insofern, als hier die Iwasawa-Algebra $\mathbb{Z}_p[\![T]\!]$ durch den Potenzreihenring $\mathbb{Z}_p[\![T_1,\dots,T_d]\!]$ in mehreren Variablen ersetzt wird. Die Zusammensetzung aller $\mathbb{Z}_p$-Erweiterungen wird allerdings im Allgemeinen nicht mit der maximalen p-verzweigten p-Erweiterung von K übereinstimmen. Die Situation ähnelt eher der einer Verschlingung in einer 3-Mannigfaltigkeit M, wo die erste Homologiegruppe des Komplements im Allgemeinen ebenfalls nicht torsionsfrei ist.

Als allgemeinsten Fall, der als Ersatz einer Verschlingung in der Topologie angesehen werden kann, betrachten wir die Zusammensetzung $\tilde{K}/K$ aller $\mathbb{Z}_p$-Erweiterungen von K und die maximale abelsche außerhalb einer endlichen Menge $S \supseteq S_p$ unverzweigte p-Erweiterung $M_S(\tilde{K})$. Die Galoisgruppe der Erweiterung $M_S(\tilde{K})/\tilde{K}$ bezeichnen wir mit $\mathcal{X}$.

Lemma 5.39. *Sei $\{\gamma_1,\dots,\gamma_k\}$ ein Erzeugendensystem von $\Gamma = \mathrm{Gal}(\tilde{K}/K)$, das einen Isomorphismus $\mathbb{Z}_p[\![\Gamma]\!] \to \mathbb{Z}_p[\![T_1,\dots,T_k]\!]$ bestimmt. Dann ist der Abschluss der Kommutatoruntergruppe von $\mathrm{Gal}(M_S(\tilde{K})/K)$ der Λ-Modul $(T_1,\dots,T_k)\mathcal{X}$.*

Beweis. Jedes Element T_ix mit $x \in \mathcal{X}$ ist ein Kommutator, da $T_ix = (\gamma_i - 1)x = \gamma_i x \gamma_i^{-1} x^{-1}$. Umgekehrt: Wir haben die exakte Sequenz

$$1 \to \mathcal{X} \to \mathrm{Gal}(M_S(\tilde{K})/K) \to \Gamma \to 1.$$

Seien $\tilde{\gamma}_1,\dots,\tilde{\gamma}_k$ Hochhebungen der Erzeuger von Γ in $\mathrm{Gal}(M_S(\tilde{K})/K)$. Für ein beliebiges Element $g \in \mathrm{Gal}(M_S(\tilde{K})/K)$ mit Bild $\gamma_1^{e_1}\dots\gamma_k^{e_k}$ im Quotienten Γ ist das Element $x = (\tilde{\gamma}_1^{e_1}\dots\tilde{\gamma}_k^{e_k})^{-1}g$ im Kern $\mathcal{X}$, also gilt $g = (\tilde{\gamma}_1^{e_1}\dots\tilde{\gamma}_k^{e_k})^{-1}x$ mit $x \in \mathcal{X}$.

Seien a und b zwei beliebige Elemente aus $\mathrm{Gal}(M_S(\tilde{K})/K)$ mit Darstellungen $a = \alpha x,\ b = \beta y$, wobei α,β die Form $\tilde{\gamma}_1^{e_1}\dots\tilde{\gamma}_k^{e_k}$ haben und $x,y \in \mathcal{X}$. Mit derselben Rechnung wie in Lemma 2.20 ergibt sich $aba^{-1}b^{-1} = (1-\beta)\circ(\alpha x^{-1}\alpha^{-1})\cdot(\alpha-1)\circ(\beta y \beta^{-1})$. Da $\alpha x^{-1}\alpha^{-1}, \beta y\beta^{-1} \in \mathcal{X}$ und $1-\beta, \alpha-1 \in (T_1,\dots,T_k)$, folgt wie in Lemma 2.20 auch die umgekehrte Inklusion. □

Satz 5.40. *$\mathcal{X}$ ist ein endlich erzeugter Λ-Modul.*

Beweis. Die Gruppe

$$\mathcal{X}/(T_1,\dots,T_k)\mathcal{X} = \mathrm{Gal}(M_S(\tilde{K})/\tilde{K})/\,\mathrm{Gal}(M_S(\tilde{K})/M_S(K)) = \mathrm{Gal}(M_S(K)/\tilde{K})$$

ist nach dem Korollar zu Satz 2.41 als $\mathbb{Z}_p$-Modul endlich erzeugt, und nach dem topologischen Nakayama-Lemma ist $\mathcal{X}$ damit als Λ-Modul endlich erzeugt. □

In dieser Situation ist $\mathcal{X}$ allerdings im Allgemeinen kein Λ-Torsionsmodul mehr. Einen Hinweis darauf, wie Invarianten in diesem Fall sinnvoll zu wählen sind, gibt Satz 1.5, aus dem sich direkt die folgende Aussage ableiten lässt:

Satz 5.41. *Sei ρ der Λ-Rang von $\mathcal{X}$. Dann ergibt sich das charakteristische Polynom des Torsions-Untermoduls von $\mathcal{X}$ als größter gemeinsamer Teiler der Elemente aus dem ρ-ten Fitting-Ideal von $\mathcal{X}$.*

Wenn G die Galoisgruppe der maximalen außerhalb von S unverzweigten p-Erweiterung von K bezeichnet, ist $\mathcal{X}$ isomorph zu $H_1(G,\mathbb{Z}_p[\![\Gamma]\!])$. Da das Augmentationsideal I_Γ ein torsionsfreier Modul vom Rang 1 ist, folgt aus der Beobachtung in Abschnitt 5.4.2, dass die Torsions-Untermoduln von $H_1(G;\mathbb{Z}_p[\![\Gamma]\!])$ und $H_1(G,1;\mathbb{Z}_p[\![\Gamma]\!])$ übereinstimmen, und damit die folgende Aussage:

Satz 5.42. *Das charakteristische Polynom von $\mathcal{X}$ erhält man als größten gemeinsamen Teiler der Elemente aus dem $\rho+1$-ten Fitting-Ideal von $H_1(G,1;\mathbb{Z}_p[\![\Gamma]\!])$.*

5.9 Homologie-3-Sphären

In der Topologie bezeichnet man dreidimensionale Mannigfaltigkeiten, deren Homologiegruppen mit denen der 3-Sphäre übereinstimmen, als Homologie-3-Sphären.

In der Zahlentheorie entsprechen den Homologie-3-Sphären in der einfachsten Sichtweise Zahlkörper K, für die die Kohomologiegruppen $H^q(\operatorname{Spec}\mathcal{O}_K,\mathbb{G}_m)$ bis auf die Dimensionen 0 und 3 verschwinden. Aus der Bedingung $H^1(\operatorname{Spec}\mathcal{O}_K,\mathbb{G}_m)=0$ erhält man mit Satz 4.1 die Voraussetzung, dass die Klassenzahl des Körpers 1 sein muss. Um $\operatorname{Spec}\mathbb{Z}$ einzuschließen, können wir vereinbaren, dass wir $\mathbb{Z}/2\mathbb{Z}$-Torsion wie in Kapitel 4 in den Dimensionen $q>3$ ignorieren.

Im Wörterbuch in [42] wird der torsionsfreie Anteil der Einheitengruppe eines Zahlkörpers dem maximalen torsionsfreien Quotienten $H_1(M)/\operatorname{Tors}(M)$ für eine Mannigfaltigkeit M gegenübergestellt. Das führt zu der folgenden Definition (vgl. [35]):

Definition. Wir nennen $\operatorname{Spec}\mathcal{O}_K$ Homologie-3-Sphäre, wenn $H^i(\operatorname{Spec}\mathcal{O}_K,\mathbb{G}_m)=0$ für $i\neq 0,3$ und wenn $H^0(\operatorname{Spec}\mathcal{O}_K,\mathbb{G}_m)$ eine Torsionsgruppe ist. Wir nennen $\operatorname{Spec}\mathcal{O}_K$ Homotopie-3-Sphäre, wenn die étale Fundamentalgruppe verschwindet.

Satz 5.43. *Die arithmetischen Homologie-3-Sphären sind die imaginär-quadratischen Zahlkörper mit Klassenzahl 1.*

Beweis. Zunächst erhalten wir aus der Eigenschaft

$$\operatorname{rg}_{\mathbb{Z}}(H^0(\operatorname{Spec}\mathcal{O}_K,\mathbb{G}_m))=\operatorname{rg}_{\mathbb{Z}}\mathcal{O}_K^*=0$$

und dem Dirichlet'schen Einheitensatz die Gleichung $r_1+r_2-1=0$, die für $\mathbb{Q}$ und imaginär-quadratische Zahlkörper erfüllt ist. Die Bedingung $H^1(\operatorname{Spec}\mathcal{O}_K,\mathbb{G}_m)=0$ liefert die Klassenzahl 1. Wenn wir $\mathbb{Z}/2\mathbb{Z}$-Torsion in höheren Dimensionen ignorieren, erhalten wir zusätzlich $\operatorname{Spec}\mathbb{Z}$, sonst nur die imaginär-quadratischen Zahlkörper mit Klassenzahl 1. ☐

Im Gegensatz zur Situation in der Topologie erhält man mit diesen Definitionen das folgende Ergebnis ([35]):

Satz 5.44. *Jede Homologie-3-Sphäre* $\operatorname{Spec}\mathcal{O}_K$ *ist bereits eine Homotopie-3-Sphäre.*

Setzen wir die Aussage der Poincaré-Vermutung voraus, so erhalten wir außer $\mathbb{Q}$ damit noch weitere Zahlkörper K, für die $\operatorname{Spec}\mathcal{O}_K$ als Analogon der 3-Sphäre angesehen werden sollte, nämlich die imaginär-quadratischen Zahlkörper mit Klassenzahl 1. Die Vermutung von Gauß, die in den 60er Jahren schließlich von H. Stark ([43]) endgültig bestätigt wurde, sagt aus, dass das genau die Körper $\mathbb{Q}(\sqrt{-d})$ mit $d\in\{1,2,3,7,11,19,43,67,163\}$ sind. In diesen Fällen ist $\operatorname{Spec}\mathcal{O}_K$ gleichzeitig Homologie-3-Sphäre und Homotopie-3-Sphäre. Wenn wir die Poincaré-Vermutung in der Version „Es gibt nur eine Homologie-3-Sphäre, die gleichzeitig eine Homotopie-3-Sphäre ist“ formulieren, ist ihr Analogon in der Zahlentheorie falsch.

Für $K=\mathbb{Q}$ haben wir in Satz 2.10 gezeigt, dass die Galoisgruppe der maximalen abelschen p-verzweigten p-Erweiterung zu $\mathbb{Z}_p$ isomorph ist. Der folgende Satz liefert eine ähnliche Aussage für unsere anderen arithmetischen Homologie-3-Sphären. In der Topologie entspricht dieser

Satz der Aussage, dass die erste Homologiegruppe des Komplements einer Verschlingung mit zwei Komponenten die torsionsfreie Gruppe $\mathbb{Z}^2$ ist. Dieser Zusammenhang wird im zweiten Teil des Wörterbuchs (§5.10) noch einmal aufgegriffen.

Satz 5.45. *Sei K ein imaginär-quadratischer Zahlkörper mit Klassenzahl 1 und p eine ungerade Primzahl, die in K in zwei verschiedene Primideale $\mathfrak{p}_1, \mathfrak{p}_2$ zerfällt. Dann ist die Galoisgruppe der maximalen abelschen außerhalb von p unverzweigten p-Erweiterung von K isomorph zu $\mathbb{Z}_p^2$.*

Beweis. Mit den Bezeichnungen aus Abschnitt 2.8 erhält man die Galoisgruppe wie im Beweis von Satz 2.39 als maximalen Pro-p-Quotienten von $J/\overline{K^* U_{[p]}}$. Da die Klassengruppe nach Voraussetzung trivial ist, gilt $J = U_p U_{[p]} K^*$, und wir erhalten mit Lemma 2.38

$$U_p U_{[p]} K^* / \overline{K^* U_{[p]}} \cong U_p / U_p \cap \overline{K^* U_{[p]}} \cong U_p / \overline{E}.$$

Die Einheitengruppe ist für imaginär-quadratische Zahlkörper nach dem Dirichlet'schen Einheitensatz endlich und damit in U_p bereits abgeschlossen. Die Gruppe U_p hat als Bestandteile die beiden Faktoren $U_{\mathfrak{p}_1}$ und $U_{\mathfrak{p}_2}$, die beide isomorph zu $\mathbb{Z}_p \times \mu_{p-1}$ sind: Da p in dieser Erweiterung voll zerlegt ist, gilt $K_{\mathfrak{p}_1} = K_{\mathfrak{p}_2} = \mathbb{Q}_p$. Die Einheitengruppe dieser lokalen Körper ist jeweils die Gruppe $\mathbb{Z}_p^*$ und hat den p-Anteil $\mathbb{Z}_p$. Da E im endlichen Anteil von U_p enthalten ist, bekommt man als p-Anteil des Quotienten genau $\mathbb{Z}_p^2$. □

Bemerkung. Die Primzahlen, die in einem solchen Körper $\mathbb{Q}(\sqrt{-d})$ in zwei verschiedene Primideale zerfallen, sind die Primzahlen der Form $a^2 + db^2$ mit $a, b \in \mathbb{N}$.

5.10 Wörterbuch, Teil 2

Die Ergebnisse aus Kapitel 5 werden hier noch einmal wie in Kapitel 4 in „Wörterbuch-Form" zusammengefasst.

Die Fundamentalgruppe eines Knotenkomplements C und die Galoisgruppe der maximalen p-verzweigten p-Erweiterung von $\mathbb{Q}$ bezeichnen wir wieder mit G.

Topologie	**Zahlentheorie**
• $H_1(G, \mathbb{Z}) = G^{ab} = H_1(C)$	• $H_1(G, \mathbb{Z}_p) = G^{ab} = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$
• $H_1(G, \mathbb{Z}[G^{ab}]) = H_1(C_\infty)$	• $H_1(G, \mathbb{Z}_p[\![G^{ab}]\!]) = \mathrm{Gal}(M_p(\mathbb{Q}_\infty)/\mathbb{Q}_\infty)$

Die Decktransformationsgruppe der maximalen abelschen Überlagerung C_∞ und die Galoisgruppe der zyklotomischen $\mathbb{Z}_p$-Erweiterung $\mathbb{Q}_\infty/\mathbb{Q}$ ergeben sich jeweils als erste Homologiegruppe von G. Indem man als Koeffizienten den Gruppenring dieser Gruppe G^{ab} wählt, erhält man den Modul, mit dessen Hilfe das Alexanderpolynom bzw. die Iwasawa-Zetafunktion definiert werden.

• Präsentationen $G = \langle e_i \| r_j \rangle$ der Knotengruppe	• Präsentationen $G = \langle e_i \| r_j \rangle$ der Galoisgruppe als Pro-p-Gruppe
• $(\overline{\frac{\partial r_j}{\partial e_i}})$ ist Präsentationsmatrix von $H_1(G, 1; \mathbb{Z}[G^{ab}])$ als $\mathbb{Z}[G^{ab}]$-Modul	• $(\overline{\frac{\partial r_j}{\partial e_i}})$ ist Präsentationsmatrix von $H_1(G, 1; \mathbb{Z}_p[\![G^{ab}]\!])$ als $\mathbb{Z}_p[\![G^{ab}]\!]$-Modul
• $\Delta_1(H_1(G, 1; \mathbb{Z}[G^{ab}]))$ liefert das Alexanderpolynom des Knotens	• $\Delta_1(H_1(G, 1; \mathbb{Z}_p[\![G^{ab}]\!]))$ liefert die Iwasawa-Zetafunktion

Der Fox-Kalkül stellt in beiden Fällen eine Methode bereit, mit der man aus einer Präsentation der Gruppe G eine Präsentation der relativen Homologiegruppe bestimmen kann (§5.4). Das nullte Fitting-Ideal des Alexandermoduls bzw. der Galoisgruppe $\mathrm{Gal}(M_p(\mathbb{Q}_\infty)/\mathbb{Q}_\infty)$ kann durch das erste Fitting-Ideal dieser relativen Homologiegruppe ersetzt werden (Kor. 5.30).

Als nächstes Ziel haben wir in diesem Kapitel Alexanderpolynome von Verschlingungen und mögliche Entsprechungen untersucht. In der einfachsten Fassung entspricht dem Komplement einer Verschlingung das Entfernen mehrerer abgeschlossener Punkte aus $\mathrm{Spec}\,\mathbb{Z}$:

• Komplement C einer Verschlingung in S^3	• $\mathrm{Spec}\,\mathbb{Z}\backslash S$
• Fundamentalgruppe von C	• Galoisgruppe der maximalen S-verzweigten p-Erweiterung von $\mathbb{Q}$

Die algebraische Fundamentalgruppe von $\mathrm{Spec}\,\mathbb{Z}\backslash S$ ist die Galoisgruppe der maximalen außerhalb von S unverzweigten Erweiterung von $\mathbb{Q}$ (§3.5). Wenn man für S eine endliche Menge wählt, die die Primzahl p enthält, ist die Galoisgruppe $\mathcal{X}_\infty^{(S)}$ der maximalen S-verzweigten p-Erweiterung von $\mathbb{Q}_\infty$ nach Satz 5.36 ein $\mathbb{Z}_p[\![T]\!]$-Torsionsmodul.

Als Analogon des Alexanderpolynoms von Verschlingungen erhält man mit diesem Vergleich das charakteristische Polynom von $\mathcal{X}_\infty^{(S)}$, also ein Polynom in einer Variablen.

Um als charakteristisches Polynom ein Polynom in mehreren Variablen zu bekommen, haben wir als zweite Möglichkeit mehrfache $\mathbb{Z}_p$-Erweiterungen betrachtet. Hierfür legt man statt $\mathbb{Q}$ einen Zahlkörper mit komplexen Einbettungen zugrunde, denn die Leopoldt-Vermutung impliziert, dass jeder Zahlkörper $r_2 + 1$ unabhängige $\mathbb{Z}_p$-Erweiterungen besitzt. Im Allgemeinen betrachten wir $\operatorname{Spec} \mathcal{O}_K$, wie im ersten Teil des Wörterbuchs notiert, als Entsprechung einer 3-Mannigfaltigkeit.

• Verschlingungen in einer 3-Mannigfaltigkeit mit Komplement C	• $\operatorname{Spec} \mathcal{O}_K \backslash S$
• $H = H_1(C)$	• Galoisgruppe H der maximalen abelschen S-verzweigten Erweiterung von K
• Überlagerung C_∞ mit Decktransformationsgruppe $D = H/\operatorname{Tors}(H)$	• Zusammensetzung $\tilde{K}$ aller $\mathbb{Z}_p$-Erweiterungen von K mit Galoisgruppe $\Gamma = H/\operatorname{Tors}(H)$
• $D \cong \mathbb{Z}^k$	• $\Gamma \cong \mathbb{Z}_p^k$

Für S wählen wir die Menge S_p aller Stellen über p oder eine größere endliche Menge von Stellen des Körpers K. Die Zusammensetzung $\tilde{K}$ aller $\mathbb{Z}_p$-Erweiterungen ist dann in der maximalen abelschen S-verzweigten p-Erweiterung von K enthalten. Ihre Galoisgruppe ist der Quotient von H nach der Torsionsuntergruppe $\operatorname{Tors}(H)$ (Satz 5.37). Dieser Erweiterung entspricht die universelle freie abelsche Überlagerung des Komplements C (§5.6).

• $\mathbb{Z}[D] \cong \mathbb{Z}[T_1, T_1^{-1}, \ldots, T_k, T_k^{-1}]$	• $\mathbb{Z}_p[\![\Gamma]\!] \cong \mathbb{Z}_p[\![T_1, \ldots, T_k]\!]$
• $H_1(C_\infty)$ als $\mathbb{Z}[D]$-Modul	• Galoisgruppe $\mathcal{X}$ der maximalen abelschen S-verzweigten p-Erweiterung von $\tilde{K}$ als $\mathbb{Z}_p[\![\Gamma]\!]$-Modul
• Alexanderpolynom der Verschlingung	• charakteristisches Polynom von $\mathcal{X}$

Der zugehörige Gruppenring dieser torsionsfreien Gruppen ist isomorph zum Laurent-Polynomring über $\mathbb{Z}$ in k Variablen bzw. zum Potenzreihenring über $\mathbb{Z}_p$ in k Variablen.

Die Invariante, die analog zum Alexanderpolynom einer Verschlingung definiert wird, ist das charakteristische Polynom der Galoisgruppe $\mathcal{X}$ als $\mathbb{Z}_p[\![T_1, \ldots, T_k]\!]$-Modul.

Wie im Fall eines Knotens lassen sich die Moduln hier wieder durch Homologiegruppen beschreiben, und die charakteristischen Polynome können wieder wie in Abschnitt 5.4 mit Hilfe des Fox-Kalküls berechnet werden.

Ein genaueres Analogon von Verschlingungen mit zwei Komponenten erhält man im Spezialfall von arithmetischen Homotopie-3-Sphären, der in Abschnitt 5.9 behandelt wird:

• Homologie-3-Sphäre	• $\operatorname{Spec} \mathcal{O}_K$ für imaginär-quadratische Zahlkörper K
• Homotopie-3-Sphäre	• $\operatorname{Spec} \mathcal{O}_K$ für imaginär-quadratische Zahlkörper K mit Klassenzahl 1

Wenn die étale Kohomologie an die Stelle der topologischen Homologie- und Kohomologietheorien und die étale Fundamentalgruppe an die Stelle der topologischen Fundamentalgruppe treten, erhält man wie in Abschnitt 5.9 beschrieben den arithmetischen Ersatz einer Homologie- bzw. Homotopie-3-Sphäre. Im Gegensatz zur Situation in der Topologie bekommt man sofort neun verschiedene imaginär-quadratische Zahlkörper, für die $\operatorname{Spec} \mathcal{O}_K$ die Eigenschaften einer Homotopie-3-Sphäre hat. Mit derselben Begründung wie im Fall $K = \mathbb{Q}$ können wir uns diese neun Objekte als Analogon der 3-Sphäre vorstellen.

• Verschlingungen mit zwei Komponenten in S^3	• zwei abgeschlossene Punkte $[\mathfrak{p}_1]$, $[\mathfrak{p}_2]$ mit $p = \mathfrak{p}_1\mathfrak{p}_2$ in einer Homotopie-3-Sphäre $\operatorname{Spec} \mathcal{O}_K$
• universelle abelsche Überlagerung C_∞ des Komplements C	• maximale abelsche p-verzweigte p-Erweiterung $\tilde{K}$ von K
• $H_1(C) \cong \mathbb{Z}^2$	• $\operatorname{Gal}(\tilde{K}/K) \cong \mathbb{Z}_p^2$

In einer arithmetischen Homotopie-3-Sphäre kann man anstelle einer Primzahl zwei abgeschlossene Punkte wählen, die über einer Primzahl p liegen – man wählt mit anderen Worten ein Primideal von $\mathbb{Z}$, das in $\mathcal{O}_K$ in zwei Primfaktoren zerfällt. Das Entfernen dieser zwei Punkte aus $\operatorname{Spec} \mathcal{O}_K$ entspricht dem Entfernen von zwei Kreisen, also einer Verschlingung mit zwei Komponenten, aus der 3-Sphäre.

Der Fundamentalgruppe von C wird wieder wie bisher der p-Anteil der algebraischen Fundamentalgruppe des entsprechenden Schemas zugeordnet. Das ist hier die Galoisgruppe der maximalen p-Erweiterung von K, in der höchstens die Stellen $\mathfrak{p}_1$ und $\mathfrak{p}_2$ verzweigen.

An dieser Stelle stimmt die Analogie für unsere arithmetischen Homotopie-3-Sphären wieder genau wie im Fall von $\operatorname{Spec} \mathbb{Z}$: Als maximalen abelschen p-Quotienten der Fundamentalgruppe, der der maximalen abelschen Überlagerung von C entspricht, erhält man genau die Zusammensetzung der $\mathbb{Z}_p$-Erweiterungen von K (Satz 5.45), und die Galoisgruppe der maximalen abelschen p-verzweigten p-Erweiterung von K ist isomorph zu $\mathbb{Z}_p^2$. Der dazugehörige Gruppenring über $\mathbb{Z}_p$ ist isomorph zum Potenzreihenring $\mathbb{Z}_p[\![T_1, T_2]\!]$ in zwei Variablen.

Als Modul über diesem Gruppenring betrachtet man wie im vorhergehenden Fall die Galoisgruppe der maximalen abelschen p-verzweigten p-Erweiterung von $\tilde{K}$. Sein charakteristisches Polynom kann als Analogon des Alexanderpolynoms einer Verschlingung mit zwei Komponenten verstanden werden.

Symbolverzeichnis

$\mathrm{Cl}(K)$	Idealklassengruppe von K, Seite 22
C_∞	universelle abelsche Überlagerung des Knotenkomplements C, Seite 9
Ens	Kategorie der Mengen, Seite 53
$\overline{E}$	Abschluss der Einheitengruppe des Zahlkörpers in U_p, Seite 44
$F_d(M)$	d-tes Fitting-Ideal von M, Seite 11
I_G	Augmentationsideal, Seite 67
K_∞	$\mathbb{Z}_p$-Erweiterung des Zahlkörpers K, Seite 25
K_e	kleinster Zwischenkörper, sodass K_∞/K_e bei p voll verzweigt ist, Seite 35
$\tilde{K}$	Zusammensetzung aller $\mathbb{Z}_p$-Erweiterungen von K, Seite 85
$M_p(K)$	maximale abelsche p-verzweigte p-Erweiterung von K, Seite 43
$\mathcal{O}_K$	Ring der ganzen Zahlen eines Zahlkörpers, Seite 26
$U_\mathfrak{p}$	Einheitengruppe eines lokalen Körpers, Seite 41
U_p	Produkt der lokalen Einheiten für Stellen über p, Seite 41
$U_{[p]}$	Produkt der lokalen Einheiten für die übrigen Stellen, Seite 41
$\mathcal{X}_\infty$	Galoisgruppe der maximalen abelschen p-verzweigten p-Erweiterung, Seite 46
X	Galoisgruppe der maximalen abelschen unverzweigten p-Erweiterung, Seite 32
X_n	p-Klassengruppe des Zwischenkörpers K_n, Seite 32
$e(\mathfrak{P}\vert\mathfrak{p})$	Verzweigungsindex, Seite 26
$f(\mathfrak{P}\vert\mathfrak{p})$	Trägheitsgrad, Seite 23
$\mathrm{lk}(J,K)$	Verschlingungszahl, Seite 12
Γ	multiplikativ geschriebene Galoisgruppe einer $\mathbb{Z}_p$-Erweiterung, Seite 33
Γ_n	Galoisgruppe der Teilerweiterung K_n/K_0 einer $\mathbb{Z}_p$-Erweiterung, Seite 30
$\Delta(t)$	Alexanderpolynom, Seite 12
$\Delta_d(M)$	größter gemeinsamer Teiler der Elemente aus $F_d(M)$, Seite 11
Λ	Iwasawa-Algebra, Seite 30
Ω_G	Differentialmodul von G, Seite 67
γ	topologischer Erzeuger von Γ, Seite 33
$\delta(K)$	Abweichung von der Leopoldt-Vermutung, Seite 44

λ	Iwasawa-λ-Invariante, Seite 36
μ	Iwasawa-μ-Invariante, Seite 36
μ_{p^∞}	Gruppe der Einheitswurzeln mit p-Potenz-Ordnung, Seite 26
$\sigma_\mathfrak{p}$	Artin-Automorphismus, Seite 22
S_p	Menge der Primstellen eines Zahlkörpers über p, Seite 84
$\frac{\partial}{\partial s_i}$	partielle Derivation, Seite 67

Literatur

[1] Alexander, J. W. : Topological invariants of knots and links. In: *Trans. Amer. Math. Soc.* 30 (1928), Nr. 2, S. 275–306. – ISSN 0002–9947

[2] Báyer, P. ; Neukirch, J. : On values of zeta functions and l-adic Euler characteristics. In: *Invent. Math.* 50 (1978/79), Nr. 1, S. 35–64. – ISSN 0020–9910

[3] Bolle, L. : *Knoten.* 6. Auflage. Edition Maritim, 2002. – Mit über 100 praxisgerechten Fotos. – ISBN 3–89225–354–4

[4] Bourbaki, N. : *Commutative algebra. Chapters 1–7.* Berlin: Springer-Verlag, 1998 (Elements of Mathematics). – Translated from the French, Reprint of the 1989 English translation. – ISBN 3–540–64239–0

[5] Brown, K. S. : *Cohomology of groups.* New York: Springer-Verlag, 1982. – Graduate Texts in Mathematics, Bd. 87. – ISBN 0–387–90688–6

[6] Burde, G. ; Zieschang, H. : *Knots.* Berlin: Walter de Gruyter & Co., 1985 (de Gruyter Studies in Mathematics, Bd. 5). – ISBN 3–11–008675–1

[7] Crowell, R. H. : Corresponding group and module sequences. In: *Nagoya Math. J.* 19 (1961), S. 27–40

[8] Deninger, C. : A note on arithmetic topology and dynamical systems. In: *Algebraic number theory and algebraic geometry* Bd. 300. Providence, RI: Amer. Math. Soc., 2002, S. 99–114

[9] Eisenbud, D. : *Commutative algebra.* With a view toward algebraic geometry. New York: Springer-Verlag, 1995. – Graduate Texts in Mathematics, Bd. 150. – ISBN 0–387–94268–8; 0–387–94269–6

[10] Fox, R. H. : Free differential calculus. I. Derivation in the free group ring. In: *Ann. of Math. (2)* 57 (1953), S. 547–560

[11] Fox, R. H. : Free differential calculus. II. The isomorphism problem of groups. In: *Ann. of Math. (2)* 59 (1954), S. 196–210

[12] Gordon, C. M. ; Luecke, J. : Knots are determined by their complements. In: *J. Amer. Math. Soc.* 2 (1989), Nr. 2, S. 371–415. – ISSN 0894–0347

[13] Grothendieck, A. : *Revêtements étales et groupe fondamental.* Berlin: Springer-Verlag, 1971. – Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Lecture Notes in Mathematics, Vol. 224

[14] Hartshorne, R. : *Algebraic geometry.* New York: Springer-Verlag, 1977. – Graduate Texts in Mathematics, Bd. 52. – ISBN 0–387–90244–9

[15] Hatcher, A. : *Algebraic topology.* Cambridge: Cambridge University Press, 2002. – ISBN 0–521–79160–X; 0–521–79540–0

[16] Iwasawa, K. : On Γ-extensions of algebraic number fields. In: *Bull. Amer. Math. Soc.* 65 (1959), S. 183–226

[17] Iwasawa, K. : *Lectures on p-adic L-functions.* Princeton, New Jersey: Princeton University Press, 1972. – ISBN 0–691–08112–3

[18] Iwasawa, K. : On $\mathbb{Z}_l$-extensions of algebraic number fields. In: *Ann. of Math. (2)* 98 (1973), S. 246–326

[19] Kawauchi, A. : *A survey of knot theory.* Basel: Birkhäuser Verlag, 1996. – Translated and revised from the 1990 Japanese original by the author. – ISBN 3–7643–5124–1

[20] Koblitz, N. : *p-adic numbers, p-adic analysis, and zeta-functions.* Second edition. New York: Springer-Verlag, 1984. – Graduate Texts in Mathematics, Bd. 58. – ISBN 0–387–96017–1

[21] Koch, H. : *Galoissche Theorie der p-Erweiterungen.* Berlin: Springer-Verlag, 1970. – Mit einem Geleitwort von I. R. Šafarevič

[22] Koch, H. : l-Erweiterungen mit vorgegebenen Verzweigungsstellen. In: *J. Reine Angew. Math.* 219 (1965), S. 30–61

[23] Lang, S. : *Algebra.* 3rd edition. New York: Springer-Verlag, 2002. – Graduate Texts in Mathematics, Bd. 211. – ISBN 0–387–95385–X

[24] Lickorish, W. B. R. : *An introduction to knot theory.* New York: Springer-Verlag, 1997. – Graduate Texts in Mathematics, Bd. 175. – ISBN 0–387–98254–X

[25] Long, R. L. : *Algebraic number theory.* New York: Marcel Dekker Inc., 1977. – Monographs and Textbooks in Pure and Applied Mathematics, Vol. 41. – ISBN 0–8247–6540–0

[26] Lyndon, R. C. : Cohomology theory of groups with a single defining relation. In: *Ann. of Math. (2)* 52 (1950), S. 650–665

[27] Mazur, B. : Notes on étale cohomology of number fields. In: *Ann. Sci. École Norm. Sup. (4)* 6 (1973), S. 521–552 (1974)

[28] Milne, J. S. : *Arithmetic duality theorems.* Boston, MA: Academic Press Inc., 1986. – Perspectives in Mathematics, Bd. 1. – ISBN 0–12–498040–6

[29] Milne, J. S. : *Étale cohomology.* Princeton, N.J.: Princeton University Press, 1980. – Princeton Mathematical Series, Bd. 33. – ISBN 0–691–08238–3

[30] Murre, J. P. : *Lectures on an introduction to Grothendieck's theory of the fundamental group.* Bombay: Tata Institute of Fundamental Research, 1967. – Notes by S. Anantharaman, Tata Institute of Fundamental Research Lectures on Mathmatics, No 40

[31] Neukirch, J. : Algebraische Zahlentheorie. In: *Ein Jahrhundert Mathematik 1890–1990* Bd. 6. Braunschweig: Vieweg, 1990, S. 587–628

[32] Neukirch, J. : *Algebraic number theory.* Berlin: Springer-Verlag, 1999 (Grundlehren der Mathematischen Wissenschaften, Bd. 322). – Translated from the 1992 German original. – ISBN 3–540–65399–6

[33] Neukirch, J. ; Schmidt, A. ; Wingberg, K. : *Cohomology of number fields.* Berlin: Springer-Verlag, 2000 (Grundlehren der Mathematischen Wissenschaften, Bd. 323). – ISBN 3–540–66671–0

[34] Nguyễn-Quang-Đỗ, T. : Formations de classes et modules d'Iwasawa. In: *Number theory, Noordwijkerhout 1983.* Berlin: Springer, 1984. – Lecture Notes in Mathematics, Bd. 1068, S. 167–185

[35] Ramachandran, N. : A note on arithmetic topology. In: *C. R. Math. Acad. Sci. Soc. R. Can.* 23 (2001), Nr. 4, S. 130–135. – ISSN 0706–1994

[36] Raynaud, M. : *Anneaux locaux henséliens.* Berlin: Springer-Verlag, 1970 (Lecture Notes in Mathematics, Vol. 169)

[37] Reznikov, A. : *Hakenness and b_1.* – Preprint 1998, www.arxiv.org/abs/math.DG/9903064

[38] Reznikov, A. : Embedded incompressible surfaces and homology of ramified coverings of three-manifolds. In: *Selecta Math. (N.S.)* 6 (2000), Nr. 1, S. 1–39. – ISSN 1022–1824

[39] Ribes, L. ; Zalesskii, P. : *Profinite groups.* Berlin: Springer-Verlag, 2000 (Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, Bd. 40). – ISBN 3–540–66986–8

[40] Serre, J.-P. : *Cohomologie galoisienne.* Cinquième édition. Berlin: Springer-Verlag, 1994 (Lecture Notes in Mathematics, Bd. 5). – ISBN 3–540–58002–6

[41] Serre, J.-P. : Classes des corps cyclotomiques (d'après K. Iwasawa). In: *Séminaire Bourbaki, Vol. 5,.* Paris: Soc. Math. France, 1995, Exp. No. 174, S. 83–93

[42] Sikora, A. S. : *Analogies between group actions on 3-manifolds and number fields.* – Preprint 2003 (revised v2), www.arxiv.org/abs/math.GT/0107210

[43] Stark, H. M. : A complete determination of the complex quadratic fields of class-number one. In: *Michigan Math. J.* 14 (1967), S. 1–27

[44] Trotter, H. F. : Homology of group systems with applications to knot theory. In: *Ann. of Math. (2)* 76 (1962), S. 464–498

[45] Turaev, V. : *Introduction to combinatorial torsions.* Basel: Birkhäuser Verlag, 2001 (Lectures in Mathematics ETH Zürich). – Notes taken by Felix Schlenk. – ISBN 3–7643–6403–3

[46] Washington, L. C. : *Introduction to cyclotomic fields.* Second edition. New York: Springer-Verlag, 1997. – Graduate Texts in Mathematics, Bd. 83. – ISBN 0–387–94762–0

[47] Wilson, J. S. : *Profinite groups.* New York: The Clarendon Press Oxford University Press, 1998 (London Mathematical Society Monographs. New Series. Bd. 19). – ISBN 0–19–850082–3