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) $\Delta(g^n) = (1 + g + \dots + g^{n-1})\Delta(g)$ *für alle* $g \in G$.
4) $\Delta(g^{-n}) = -(g^{-1} + g^{-2} + \dots + g^{-n})\Delta(g)$ *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* $\{s_1, \dots, s_n\}$. *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 $\alpha=\alpha_0+\alpha_1p+\alpha_2p^2+\dots$ mit $\alpha_i\in\{0,\dots,p-1\}$ vorstellen. Diese Schreibweise soll ausdrücken, dass $\alpha(n)=\alpha_0+\alpha_1p+\dots+\alpha_{n-1}p^{n-1}$ 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

$$H_i(G, M) = \operatorname{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, M).$$

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

$$\cdots \to \operatorname{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}[G]) \to \operatorname{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}) \to \operatorname{Tor}_0^{\mathbb{Z}[G]}(\mathbb{Z}, I_G) \to \operatorname{Tor}_0^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}[G]) \to \dots,$$

wobei $\operatorname{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}[G]) = 0$ und $\operatorname{Tor}_0^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}[G]) = \mathbb{Z} \otimes_G \mathbb{Z}[G] \cong \mathbb{Z}$, sodass die letzte Abbildung die Nullabbildung ist. Wir haben also einen Isomorphismus $\operatorname{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}) \cong \operatorname{Tor}_0^{\mathbb{Z}[G]}(\mathbb{Z}, I_G) = I_G \otimes_G \mathbb{Z}$.

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. □

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 $H_*(N)$. □

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. □

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].

□

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. □

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. □

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

$$\begin{tikzcd}
\cdots \arrow[r] & H_n(Y. \otimes A) \arrow[r] \arrow[d, equal] & H_n(X. \otimes A) \arrow[r] \arrow[d, equal] & H_n(X./Y. \otimes A) \arrow[r, "\partial"] \arrow[d, equal] & H_{n-1}(Y. \otimes A) \arrow[r] \arrow[d, equal] & \cdots \\
\cdots \arrow[r] & H_n(H;A) \arrow[r] & H_n(G;A) \arrow[r] & H_n(G,H;A) \arrow[r, "\partial"] & H_{n-1}(H;A) \arrow[r] & \cdots
\end{tikzcd}$$

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 $\{a_1, \ldots, a_d\}$, 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 $\langle e_1, \dots, e_n | r_1, \dots, r_m \rangle$ 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.

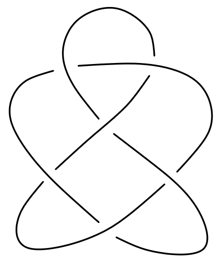

Abbildung 12: Palstek

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 $j \neq i$:

$$\begin{aligned}
D_j(\overline{e}_i - 1) &= \det(a_1, \dots, a_i(\overline{e}_i - 1), \dots, \hat{a}_j, \dots, a_n) \\
&= \det(a_1, \dots, -\sum_{k \neq i} a_k(\overline{e}_k - 1), \dots, \hat{a}_j, \dots, a_n) \\
&= \det(a_1, \dots, -a_j(\overline{e}_j - 1), \dots, \hat{a}_j, \dots, a_n) \\
&= \pm D_i(\overline{e}_j - 1).
\end{aligned}$$

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 $\Delta = \Delta(T_1, \dots, T_k)$ aus dem Satz.

Bemerkung. Als Polynom hängt $\Delta(T_1, \dots, T_k)$ von der Wahl des Isomorphismus

$$\mathbb{Z}[\mathbb{Z}^k] \to \mathbb{Z}[T_1, T_1^{-1}, \dots, T_k, T_k^{-1}]$$

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 $T_i x$ mit $x \in \mathcal{X}$ ist ein Kommutator, da $T_i x = (\gamma_i - 1)x = \gamma_i x \gamma_i^{-1} x^{-1}$. 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 $J = U_pU_{[p]}K^*$, und wir erhalten mit Lemma 2.38

$$U_pU_{[p]}K^*/\overline{K^*U_{[p]}} \cong U_p/U_p \cap \overline{K^*U_{[p]}} \cong U_p/\overline{E}.$$

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 $G = \langle e_i \vert r_j\rangle$ der Knotengruppe	• Präsentationen $G = \langle e_i \vert r_j\rangle$ 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.