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 $\tau(\mathfrak{p})$. □

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. □

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. □

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 $T_1, T_2, \ldots, T_k$ 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. $\square$

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 $r(T)$. □

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. □

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

$$\begin{tikzcd} \mathbb{Z}_p[\Gamma_n] \arrow[r] \arrow[d] & \mathbb{Z}_p[T]/(h_n(T)) \arrow[d] \\ \mathbb{Z}_p[\Gamma_{n-1}] \arrow[r] & \mathbb{Z}_p[T]/(h_{n-1}(T)) \end{tikzcd}$$

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. □

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 $F = F_nK_\infty$.*

Beweis. Wir können eine endliche Erweiterung F_0 von K_0 wählen, sodass $F = F_0K_\infty$. Sei $F_n = F_0K_n$, sodass F die Vereinigung aller F_n ist und $F = F_nK_\infty$ 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:

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

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. □

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 $v_1,\ldots,v_s$ die Bewertungen von K_0, die in K_∞ verzweigt sind, und $T_1,\ldots,T_s$ 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 $a_2,a_3,\ldots,a_s$ erzeugt wird, und für jedes $n\in\mathbb{N}$ sei $Y_n=(1+\gamma+\cdots+\gamma^{p^n-1})Y_0$. 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

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

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

$$(a_i\sigma_1)^{p^n}=a_i(\sigma_1a_i\sigma_1^{-1})(\sigma_1^2a_i\sigma_1^{-2})\cdots(\sigma_1^{p^n-1}a_i\sigma_1^{-p^n-1})\sigma_1^{p^n}=((1+\gamma+\cdots+\gamma^{p^n-1})\circ a_i)\sigma_1^{p^n}.$$

Damit wird die Galoisgruppe $\mathrm{Gal}(L/L_n)$ 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 $\mathrm{Gal}(L/K)$. Wie im ersten Teil folgt jetzt

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

□

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 $\mathrm{Gal}(L/K_e) \to \mathrm{Gal}(K_\infty/K_e) = \Gamma^{p^e}$ 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 $\mathrm{Ann}(y_i)$ für kein i in einem Primideal der Höhe 1 enthalten. Der Ring $\Lambda/\mathrm{Ann}(y_i)$ 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 $\mathrm{Ann}(y_i)$ enthalten sein. Für jedes i ist der Modul $\Lambda/(\mathrm{Ann}(y_i))$ als Quotient von $\Lambda/(p, T)^n$ endlich, und der Modulhomomorphismus

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

der sich aus den Abbildungen $\Lambda/(\mathrm{Ann}(y_i)) \to N,\ 1 \mapsto y_i$ 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 $\mathrm{Tors}(M) = \{x \in M \mid \exists r \in R\backslash\{0\} : r \cdot x = 0\}$. Falls $M = \mathrm{Tors}(M)$, 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 $\mathfrak{a} = \mathrm{Ann}(M)$. 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 $f \in \mathrm{Hom}_{S^{-1}\Lambda}(S^{-1}X, S^{-1}M)$ wählen, der $S^{-1}X$ auf den Modul $S^{-1}M$ projiziert. Wegen der Bijektivität der kanonischen Abbildung

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

ist dieser Homomorphismus f von der Form $f = s^{-1}\tilde{g}$ mit einem Element $s \in S$ und einem Homomorphismus $\tilde{g} \in \mathrm{Hom}_\Lambda(X, M)$. 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 $\mathrm{Ann}(M)$ 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

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "h"] & X \arrow[r] \arrow[d, "f"] & X/M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & M \arrow[r] & M \oplus X/M \arrow[r] & X/M \arrow[r] & 0
\end{tikzcd}$$

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 $P = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ 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 $Y_e, Y_{e+1}, \ldots$ 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 $\operatorname{rg}_{\mathbb{Z}_p} U_{\mathfrak{p}}^{(1)} = [K_{\mathfrak{p}} : \mathbb{Q}_p]$ 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 $\operatorname{Gal}(M_p(K_n)/K_n)$ der maximalen abelschen p-verzweigten p-Erweiterungen den $\mathbb{Z}_p$-Rang 1 haben. Die Gruppen $\operatorname{Gal}(M_p(K_n)/K_\infty)$ 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 $\operatorname{Gal}(\bigcup M_p(K_n)/K_\infty)$ 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. □

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. □

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}. □

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. □

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.