Protokoll zur Vorlesung Iwasawatheorie WS 24/25

W. Bley

30. Januar 2025

1 Grundlegendes und Motivation

1.1 Grundlegende Definitionen

In dieser Vorlesung wird K in der Regel ein Zahlkörper sein.

Definition 1.1.1 Eine $\mathbb{Z}_p$ -Erweiterung von K ist eine Galoiserweiterung K_∞/K mit zu $\mathbb{Z}_p$ isomorpher Galoisgruppe. Dabei ist der Isomorphismus ein Isomorphismus von topologischen Gruppen.

Die zyklotomische $\mathbb{Z}_p$ -Erweiterung

Sei nun p eine Primzahl. Wir setzen $q := p$ für $p \neq 2$ und $q := 4$ für $p = 2$ und betrachten für $n \in \mathbb{N}$ den Körperturm $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_q) \subseteq \mathbb{Q}(\zeta_{qp^n})$. Sei

$$\text{Gal}(\mathbb{Q}(\zeta_{qp^n})/\mathbb{Q}) \simeq (\mathbb{Z}/qp^n\mathbb{Z})^\times \simeq \Delta \times \frac{1 + q\mathbb{Z}}{1 + qp^n\mathbb{Z}},$$

wobei Δ für $p \neq 2$ die Untergruppe der Ordnung $p - 1$ und im Fall $p = 2$ die von -1 erzeugte Untergruppe bezeichnet.

Dann ist $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_q)$ eine $\mathbb{Z}_p$ -Erweiterung, wobei wir hier $\mathbb{Q}(\zeta_{p^\infty}) := \bigcup_n \mathbb{Q}(\zeta_{p^n})$ setzen. Weiterhin ist

$$\mathbb{Q}_\infty := \mathbb{Q}(\zeta_{p^\infty})^\Delta$$

eine $\mathbb{Z}_p$ -Erweiterung von $\mathbb{Q}$ und heißt zyklotomische $\mathbb{Z}_p$ -Erweiterung von $\mathbb{Q}$. Für einen Zahlkörper K heißt $K\mathbb{Q}_\infty$ zyklotomische $\mathbb{Z}_p$ -Erweiterung von K .

Im Weiteren sei K_∞/K eine beliebige $\mathbb{Z}_p$ -Erweiterung. Wir schreiben $\Gamma := \text{Gal}(K_\infty/K)$ und notieren Γ multiplikativ. Sei $\gamma \in \Gamma$ ein topologischer Erzeuger von Γ . Die Untergruppen $\Gamma^{p^n} \simeq p^n\mathbb{Z}_p$ sind genau die nicht-trivialen abgeschlossenen Untergruppen von Γ . Wir setzen $\Gamma_n := \Gamma/\Gamma^{p^n}$. Dann ist Γ_n zyklisch von der Ordnung p^n . Setzt man $K_n := K_\infty^{\Gamma_n}$, so hat man also

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_n \subseteq \dots \subseteq K_\infty = \bigcup_n K_n$$

mit $\text{Gal}(K_n/K) \simeq \Gamma_n$ zyklisch von der Ordnung p^n .

Sei nun $F/\mathbb{Q}_p$ eine endliche Körpererweiterung und $\mathcal{O} = \mathcal{O}_F$ der Bewertungsring in F . Sei $\mathfrak{p} \subseteq \mathcal{O}$ das maximale Ideal und π ein Element vom Wert 1, also $\mathfrak{p} = (\pi)$.

Definition 1.1.2 $\mathcal{O}[[\Gamma]] := \varprojlim_n \mathcal{O}[\Gamma_n]$ heißt kompletierter Gruppenring.

Ein erstes Ziel der Vorlesung ist der Beweis von

Satz 1.1.3 Die Zuordnung $\gamma \mapsto 1 + T$ induziert einen (nicht-kanonischen) Isomorphismus

$$\mathcal{O}[[\Gamma]] \simeq \mathcal{O}[[T]].$$

Satz 1.1.4 (“Teilen mit Rest“) Seien $f, g \in \mathcal{O}[[T]]$,

$$f = a_0 + a_1T + a_2T^2 + \dots + a_{n-1}T^{n-1} + a_nT^n + \dots$$

mit $a_0, \dots, a_{n-1} \in \mathfrak{p}$ und $a_n \notin \mathfrak{p}$. Dann gibt es eindeutig bestimmte Elemente

$$q \in \mathcal{O}[[T]], r \in \mathcal{O}[T], r = 0 \text{ oder } \deg(r) < n,$$

so dass $g = qf + r$.

Definition 1.1.5 Ein Polynom $P(T) \in \mathcal{O}[T]$ heißt ausgezeichnet, falls

$$P(T) = T^n + a_{n-1}T^{n-1} + \dots + a_1T + a_0$$

mit $a_{n-1}, \dots, a_0 \in \mathfrak{p}$.

Satz 1.1.6 (“Weierstrass Preparation Theorem“) Sei $f(T) = \sum_{i=0}^{\infty} a_iT^i \in \mathcal{O}[[T]]$ mit $a_0, \dots, a_{n-1} \in \mathfrak{p}$, $a_n \notin \mathfrak{p}$. Dann kann man f eindeutig in der Form

$$f(T) = P(T)U(T)$$

schreiben, wobei $U(T) \in \mathcal{O}[[T]]^\times$ eine Einheit und $P(T) \in \mathcal{O}[T]$ ein ausgezeichnetes Polynom vom Grad n ist. Allgemeiner: Jedes $0 \neq f \in \mathcal{O}[[T]]$ kann man eindeutig in der Form

$$f(T) = p^\mu P(T)U(T)$$

mit $\mu \in \mathbb{Z}_{\geq 0}$, $U(T) \in \mathcal{O}[[T]]^\times$ und ausgezeichnetem $P(T) \in \mathcal{O}[T]$ schreiben.

Folgerung 1.1.7 Sei $0 \neq f \in \mathcal{O}[[T]]$. Dann gibt es nur endlich viele $x \in \mathbb{C}_p$ mit $|x|_p < 1$ und $f(x) = 0$.

Lemma 1.1.8 Sei $g(T) \in \mathcal{O}[T]$ und $P(T) \in \mathcal{O}[T]$ ausgezeichnet. Dann gilt:

$$\frac{g(T)}{P(T)} \in \mathcal{O}[[T]] \implies \frac{g(T)}{P(T)} \in \mathcal{O}[T].$$

Nach diesen Vorbereitungen wurde der Beweis von Satz 1.1.3 erbracht. Hier nochmals zur Erinnerung:

Satz 1.1.9 Die Zuordnung $\gamma \mapsto 1 + T$ induziert einen (nicht-kanonischen) Isomorphismus

$$\mathcal{O}[[\Gamma]] \simeq \mathcal{O}[[T]].$$

Im Weiteren schreiben wir stets $\Lambda = \mathcal{O}[[T]]$.

Satz 1.1.10 Λ ist ein kommutativer, nullteilerfreier, noetherscher und faktorieller lokaler Ring. Die irreduziblen Elemente sind gegeben durch π und die irreduziblen ausgezeichneten Polynome.

Lemma 1.1.11 Seien $f, g \in \Lambda$. Dann gilt:

$$f \text{ und } g \text{ sind zueinander prim} \iff |\Lambda/(f, g)| < \infty.$$

Bemerkung 1.1.12 Für alle $f \in \Lambda \setminus \Lambda^\times$ gilt $|\Lambda/(f)| = \infty$.

Satz 1.1.13 Λ ist ein lokaler Ring mit maximalem Ideal (π, T) . Die Primideale sind gegeben durch

$$0, (\pi, T), (\pi) \text{ und } (P(T)),$$

wobei $P(T)$ die ausgezeichneten irreduziblen Polynome durchläuft.

1.2 Struktursatz für e-e Λ -Moduln

Definition 1.2.1 a) Ein endlich-erzeugter Λ -Modul heißt pseudo-null, falls $|M| < \infty$.
b) Zwei endlich erzeugte Λ -Moduln M und M' heißen pseudo-isomorph, falls es einen Modulhomomorphismus $f: M \rightarrow M'$ gibt, so dass $\ker(f)$ und $\text{cok}(f)$ pseudo-null sind.
Wir schreiben dann: $M \sim M'$.

Wir werden später folgende Äquivalenz zeigen:

$$M \text{ pseudo-null} \iff M_{\mathfrak{p}} = 0 \text{ für alle Primideale } \mathfrak{p} \text{ mit } \text{ht}(\mathfrak{p}) = 1.$$

Man beachte, dass die Relation pseudo-isomorph nicht symmetrisch ist. Allerdings gilt

Bemerkung 1.2.2 Sind M und M' endlich erzeugte Λ -Torsionsmoduln. Dann gilt:

$$M \sim M' \iff M' \sim M.$$

Satz 1.2.3 (Struktursatz für endlich erzeugte Λ -Moduln)

Sei $\Lambda = \mathcal{O}[[T]]$ und M ein endlich erzeugter Λ -Modul. Dann hat man einen Pseudo-Isomorphismus

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^s \Lambda/(\pi^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^t \Lambda/(f_j(T)^{m_j}) \right)$$

wobei $r, s, t, n_i, m_j \in \mathbb{Z}_{\geq 0}$ und $f_j(T) \in \mathcal{O}[T]$ ausgezeichnet und irreduzibel ist. Die r, s, t, n_i, m_j und die f_j sind durch M eindeutig bestimmt.

Definition 1.2.4

- $r(M) := r$ heißt Rang von M .
- $\mu(M) := \sum_{i=1}^s n_i$ heißt Iwasawa μ -Invariante von M .
- $\lambda(M) := \sum_{j=1}^t m_j \deg(f_j)$ heißt Iwasawa λ -Invariante von M .
- Moduln der Form $\Lambda/(\pi^n)$ oder $\Lambda/(f(T)^m)$ mit $f \in \mathcal{O}[T]$ ausgezeichnet und irreduzibel nennt man elementar.
- $\text{char}(M) := \pi^{\mu(M)} \prod_{j=1}^t f_j(T)^{m_j}$ nennt man das charakteristische Polynom von M .

Beim Beweis von Satz 1.2.3 orientieren wir uns an Kap. V im Buch von NSW (Neukirch/Schmidt/Wingberg).

Sei ab jetzt A ein kommutativer, nullteilerfreier, noetherscher und ganz abgeschlossener Ring. Sei $K := \text{Quot}(A)$ der Quotientenkörper. Sei $P(A)$ die Menge der Primideale von A der Höhe 1.

Bemerkung 1.2.5

- Für $\mathfrak{p} \in P(A)$ ist $A_{\mathfrak{p}}$ ein diskreter Bewertungsring.
- Es gilt:

$$A = \bigcup_{\mathfrak{p} \in P(A)} A_{\mathfrak{p}}.$$

Definition 1.2.6 Sei M ein e-e A -Modul.

- $M^+ := \text{Hom}_A(M, A)$ nennen wir das A -lineare Dual von M .
- M heißt reflexiv, falls die kanonische Abbildung

$$\begin{aligned} \varphi_M: M &\longrightarrow M^{++}, \\ m &\longmapsto (f \mapsto f(m)) \end{aligned}$$

ein Isomorphismus ist.

Bemerkung 1.2.7 Falls M reflexiv ist, so ist M torsionsfrei.

Für e-e torsionsfreie A -Moduln M setzen wir $V := K \otimes_A M$ und $\hat{V} := \text{Hom}_K(V, K)$. Dann hat man kanonische Abbildungen

$$M \hookrightarrow V \text{ und } M^+ \hookrightarrow \hat{V}.$$

Mit dieser Identifizierung gilt:

$$\begin{aligned} M^+ &\simeq \{ \lambda \in V \mid \lambda(m) \in A, \forall m \in M \}, \\ (M^+)_\mathfrak{p} &\simeq \{ \lambda \in V \mid \lambda(m) \in A_\mathfrak{p}, \forall m \in M_\mathfrak{p} \} \simeq (M_\mathfrak{p})^+. \end{aligned}$$

Wir schreiben daher im weiteren $M_\mathfrak{p}^+$ für $(M^+)_\mathfrak{p}$ oder $(M_\mathfrak{p})^+$. Es sei außerdem

$$\mathbb{P}(A) := \{ \mathfrak{p} \mid \mathfrak{p} \text{ ist Primideal der Höhe } 1 \}.$$

Lemma 1.2.8 Sei M ein endlich erzeugter torsionsfreier A -Modul. Dann gilt:

- (a) $M^+ = \prod_{\mathfrak{p} \in \mathbb{P}(A)} M_\mathfrak{p}^+$.
- (b) $M^{++} = \prod_{\mathfrak{p} \in \mathbb{P}(A)} M_\mathfrak{p}$.
- (c) $M = \prod_{\mathfrak{p} \in \mathbb{P}(A)} M_\mathfrak{p} \iff M$ ist reflexiv.

Folgerung 1.2.9 Sei M ein endlich erzeugter torsionsfreier A -Modul. Dann ist M^+ reflexiv.

Wir geben nun eine weitere Definition des Begriffs “pseudo-null”.

Definition 1.2.10 Sei M ein endlich erzeugter A -Modul. Dann sind folgende Aussagen äquivalent:

- (i) $M_\mathfrak{p} = 0$ für alle $\mathfrak{p} \in \mathbb{P}(A)$.
- (ii) $\text{Ann}_A(M) \subseteq \mathfrak{p} \implies \text{ht}(\mathfrak{p}) \geq 2$.

Falls M eine dieser äquivalenten Bedingungen erfüllt, so nennt man M pseudo-null.

Remarks 1.2.11 (1) M pseudo-null $\implies M_{(0)} = K \otimes_A M = 0$.

(2) Falls A ein Dedekindring ist, so gilt:

$$M \text{ pseudo-null} \iff M = 0.$$

(3) Sei A ein lokaler Ring der Dimension 2 mit maximalem Ideal $\mathfrak{m}$. Es gelte $|A/\mathfrak{m}| < \infty$. Dann gilt:

$$M \text{ pseudo-null} \iff |M| < \infty.$$

Wir setzen

$$\text{Supp}(M) := \{ \mathfrak{p} \mid M_\mathfrak{p} \neq 0 \}.$$

Lemma 1.2.12 Sei M ein endlich erzeugter A -Modul und sei $\alpha \in A \setminus \{0\}$. Es gelte

$$\text{Supp}(A/\alpha A) \cap (\text{Supp}(M) \cap \mathbb{P}(A)) = \emptyset.$$

Dann ist die Abbildung $M \longrightarrow M, m \mapsto \alpha m$, ein Pseudoisomorphismus.

Sei nun

$$\begin{aligned} T_A(M) &:= \text{Torsionsteilmodul von } M = \{ m \in M \mid \exists a \in A \setminus \{0\} \text{ mit } am = 0 \}, \\ F_A(M) &:= M/T_A(M). \end{aligned}$$

Satz 1.2.13 Sei M ein endlich erzeugter A -Modul.

(i) Dann gibt es einen Pseudoisomorphismus

$$f: M \xrightarrow{\sim} F_A(M) \oplus T_A(M).$$

(ii) Es gibt eine endliche Familie $\{\mathfrak{p}_i\}_{i \in I}$ von Primidealen der Höhe 1, natürliche Zahlen $\{n_i\}_{i \in I}$ und einen Pseudoisomorphismus

$$g: T_A(M) \xrightarrow{\sim} \bigoplus_{i \in I} A/\mathfrak{p}_i^{n_i}.$$

Die $\mathfrak{p}_i$ und n_i sind eindeutig durch M bestimmt.

Bemerkung 1.2.14 Für endlich erzeugte A -Torsionsmoduln ist Pseudoisomorphie symmetrisch, d.h. für endlich erzeugte A -Torsionsmoduln M und N gilt

$$M \xrightarrow{\sim} N \iff N \xrightarrow{\sim} M.$$

Satz 1.2.15 Sei M ein endlich erzeugter torsionsfreier A -Modul. Dann ist $\varphi_M: M \hookrightarrow M^{++}$ ein Pseudoisomorphismus. M^{++} ist reflexiv.

Satz 1.2.16 Ein reflexiver A -Modul über einem 2-dimensionalen lokalen regulären Ring ist frei.

2 Asymptotisches Wachstum von p -Klassengruppen in $\mathbb{Z}_p$ -Erweiterungen

In diesem Abschnitt ist K_∞/K stets eine $\mathbb{Z}_p$ -Erweiterung und wir setzen $\Gamma := \text{Gal}(K_\infty/K)$. Sei γ ein topologischer Erzeuger von Γ und $\Lambda = \mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]]$ der komplettierte Gruppenring.

Satz 2.0.1 Sei K_∞/K eine $\mathbb{Z}_p$ -Erweiterung. Sei

$$A_n := \mathbb{Z}_p \otimes_{\mathbb{Z}} \text{cl}_{K_n}$$

die p -Sylow-Untergruppe der Idealklassengruppe cl_{K_n} . Dann gibt es ganze Zahlen $\lambda \geq 0, \mu \geq 0$ und ν , allesamt unabhängig von n , und $n_0 \geq 0$, so dass

$$|A_n| = p^{e_n} \text{ mit } e_n = \lambda n + \mu p^n + \nu, \forall n \geq n_0.$$

Zusatz: Sei L_∞/K_∞ die maximal abelsche unverweigte p -Erweiterung von K_∞ und $X := \text{Gal}(L_\infty/K_\infty)$. Dann ist X ein e -e Λ -Torsionsmodul und es gilt :

$$\lambda = \lambda(X), \quad \mu = \mu(X).$$

Zum Beweis sei L_n der Hilbertsche p -Klassenkörper von K_n und $X_n := \text{Gal}(L_n/K_n)$. Dann liefert der Artinautomorphismus eine Isomorphie $A_n \simeq X_n$. Die Erweiterungen L_n/K sind galoissch und wir setzem $G_n := \text{Gal}(L_n/K)$.

Sei $L_\infty := \cup_n L_n$. Dann ist auch L_∞/K galois und wir setzen

$$X := \text{Gal}(L_\infty/K_\infty), \quad G := \text{Gal}(L_\infty/K).$$

Es gilt dann: $X = \varprojlim_n X_n \simeq \varprojlim_n A_n =: A_\infty$.

Wir werden später einsehen, dass in K_∞/K stets ein Primideal verzweigt und nehmen im Folgenden an

Voraussetzung (V): Alle Primideale, die in K_∞/K verzweigen, sind voll verzweigt.

Die exakten Sequenzen

$$0 \longrightarrow X_n \longrightarrow G_n \longrightarrow \Gamma_n \longrightarrow 0$$

induzieren eine Wirkung von Γ_n auf X_n , die verträglich ist mit $\Gamma_{n+1} \longrightarrow \Gamma_n$, $X_{n+1} \longrightarrow X_n$ und $A_{n+1} \longrightarrow A_n$ (mittels der Norm). Wir erhalten damit eine Wirkung von Γ auf $X \simeq A_\infty$, d.h. X wird zu einem Λ -Modul.

Im weiteren diskutieren wir Verzweigungstheorie in (nicht notwendig endlichen) Erweiterungen $k/\mathbb{Q}$. Hierzu sei auf [Was, Appendix, §2] verwiesen.

Allgemein, also ohne die Voraussetzung (V), gilt:

Satz 2.0.2 Sei K_∞/K eine $\mathbb{Z}_p$ -Erweiterung. Dann gilt:

- (a) Es gibt ein verzweigtes Primideal.
- (b) Falls $\mathfrak{p} \subseteq \mathcal{O}_K$ verzweigt, so ist $\mathfrak{p}|p$. D.h. K_∞/K ist p -verzweigt.
- (c) Es gibt ein $n_0 \geq 0$, so dass alle in K_∞/K verzweigten Primideale voll verzweigt sind in K_∞/K_{n_0} .

Obacht: Mindestens ein Primideal $\mathfrak{p}$ über p ist verzweigt, aber im Allgemeinen verzweigen nicht alle $\mathfrak{p}|p$.

Wir nehmen nun wieder (V) an. Seien $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ die verzweigten Primideale in K . Für $i = 1, \dots, s$ fixieren wir Primideale $\tilde{\mathfrak{p}}_i|\mathfrak{p}_i$ in L_∞/K und schreiben $I_i := I(\tilde{\mathfrak{p}}_i/\mathfrak{p}_i)$ für die jeweilige Verzweigungsgruppe. Dann gilt für $i = 1, \dots, s$

$$I_i \simeq G/X \simeq \Gamma \text{ und } G = I_i X = X I_i.$$

Unter $I_i \simeq G/X \simeq \Gamma$ gelte $\sigma_i \mapsto \gamma$. Dann gibt es für $i = 1, \dots, s$ ein eindeutig bestimmtes $a_i \in X$ mit $\sigma_i = a_i \sigma_1$.

Mit $\omega_n(T) = (1+T)^{p^n} - 1$ und der Identifikation $\gamma = 1+T$ setzen wir

$$\nu_n := \frac{\omega_n}{\omega_0} = 1 + \gamma + \dots + \gamma^{p^n - 1}.$$

Lemma 2.0.3 Es gelte (V). Sei

$$Y_0 := \overline{\langle X^{\gamma^{-1}}, a_2, \dots, a_s \rangle}$$

und $Y_n := \nu_n Y_0$. Dann gilt für alle $n \geq 0$:

$$X_n \simeq X/Y_n.$$

Im Beweis geht folgendes Lemma ein.

Lemma 2.0.4 Sei G' der Abschluss der Kommutatoruntergruppe von G . Dann gilt:

$$G' = X^{\gamma^{-1}} = TX.$$

Lemma 2.0.5 (Nakayamas Lemma)

Sei X ein kompakter Λ -Modul. Sei $\mathfrak{m} = (p, T)$ das maximale Ideal in Λ . Dann gilt:

- (i) $X = \mathfrak{m}X \iff X = 0$.
- (ii) X ist e-e über $\Lambda \iff X/\mathfrak{m}X$ ist endlich.
- (iii) Falls die Restklassen von $x_1, \dots, x_n \in X$ den $\mathbb{Z}$ -Modul $X/\mathfrak{m}X$ erzeugen, so erzeugen sie auch X als Λ -Modul.

Unter Verwendung von Nakayamas Lemma können wir nun den folgenden Satz zeigen.

Satz 2.0.6 Es gelte (V). Dann ist X ein endlich erzeugter Λ -Torsionsmodul.

Im Folgenden lösen wir uns von der Voraussetzung (V). Sei $e \geq 0$ groß genug, so dass K_∞/K_e die Voraussetzung (V) erfüllt. Sei $\Lambda' := \mathbb{Z}_p[[\text{Gal}(K_\infty/K_e)]]$. Dann ist X ein e-e Λ' -Torsionsmodul, der wegen $\Lambda' \subseteq \Lambda$ ebenfalls e-e als Λ -Modul ist.

Betrachten wir K_e als Grundkörper, so liefern die unter (V) erzielten Ergebnisse ein Y_0 bez. diesem Grundkörper. Dieses taufen wir jetzt Y_e . Es stimmt nicht mit dem alten $Y_e = \nu_e Y_0$ überein.

Setzt man

$$\nu_{n,e} := \frac{\nu_n}{\nu_e} = \frac{\omega_n}{\omega_e} = 1 + \gamma^{p^e} + \dots + \gamma^{p^e(p^{n-e}-1)}$$

so gilt mit $Y_n := \nu_{n,e} Y_e$

$$X_n \simeq X/\nu_{n,e} Y_e, \quad \forall n \geq e.$$

Wegen $X/Y_e \simeq X_e$ und $|X_e| < \infty$ gilt $Y_e \sim X$ und der Struktursatz für e-e Λ -Moduln liefert

$$Y_e \sim X \sim E$$

mit

$$E = \bigoplus_i \Lambda/(p^{m_i}) \oplus \bigoplus_j \Lambda/(f_j).$$

Hierbei sind die f_j ausgezeichneten Polynome.

Satz 2.0.7 Sei E ein elementarer Modul wie eben. Seien μ und λ die μ - und λ -Invariante von E . Sei $E/\nu_{n,e}E$ endlich für $n \geq n_0$. Dann gibt es eine Konstante $c \in \mathbb{Z}$ so dass gilt:

$$|E/\nu_{n,e}E| = p^{\mu p^n + \lambda n + c}, \quad \forall n \geq n_0.$$

Zum Beweis dieses Satzes zeigen wir:

$$\begin{aligned} V = \Lambda/p^m \Lambda &\implies |V/\nu_{n,e}V| = p^{mp^n + c}, \\ V = \Lambda/f \Lambda &\implies |V/\nu_{n,e}V| = p^{n \deg(f) + c}, \end{aligned}$$

wobei c jeweils eine von n unabhängige Konstante bezeichnet.

Zusammen mit dem nächsten Satz vervollständigt dies den Beweis von Iwasawas Satz.

Satz 2.0.8 Seien Y und E zwei Λ -Moduln mit $Y \sim E$ und elementarem E . Es gelte $|Y/\nu_{n,e}Y| < \infty$ für $n \geq e$. Dann gibt es eine Konstante c und $n_0 \in \mathbb{N}_0$, so dass

$$|Y/\nu_{n,e}Y| = p^c |E/\nu_{n,e}E|.$$

3 Dirichletsche L -Reihen

In diesem Abschnitt werden (ohne Beweise) zentrale Resultate aus der Theorie der Dirichletschen L -Reihen dargestellt.

Sei $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ ein Dirichletcharakter mit Führer $f = f_\chi$. Sei

$$\begin{aligned} L(s, \chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \text{Re}(s) > 1, \\ &= \prod_p \left(1 - \frac{\chi(p)}{p^s} \right)^{-1} \end{aligned}$$

die (primitive) Dirichletsche L -Reihe.

Bekannte Tatsachen:

1) $L(s, \chi)$ hat eine meromorphe Fortsetzung auf $\mathbb{C}$. Für $\chi \neq 1$ ist diese Fortsetzung holomorph. Für $\chi = 1$ ist $L(s, \chi)$ holomorph außer bei $s = 1$, wo ein Pol erster Ordnung vorliegt.

2) $L(s, \chi)$ genügt einer Funktionalgleichung der folgenden Form

$$\left(\frac{f}{\pi}\right)^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s, \chi) = W_\chi \left(\frac{f}{\pi}\right)^{(1-s)/2} \Gamma\left(\frac{1-s+\delta}{2}\right) L(1-s, \bar{\chi}),$$

wobei

$$\begin{aligned} W_\chi &= \frac{\tau(\chi)}{\sqrt{f} i^\delta}, \\ \tau(\chi) &= \sum_{a=1}^f \chi(a) e^{2\pi i a} f, \\ \delta &= \begin{cases} 0, & \chi(-1) = 1, \\ 1, & \chi(-1) = -1. \end{cases} \end{aligned}$$

W_χ nennt man Wurzelzahl. Es gilt $|W_\chi| = 1$.

3) Aus der Eulerproduktentwicklung folgt $L(s, \chi) \neq 0$ für $\operatorname{Re}(s) > 1$. Es gilt ebenfalls $L(1, \chi) \neq 0$.

4) Die Funktionalgleichung zusammen mit den Eigenschaften der Γ -Funktion impliziert für $n \in \mathbb{Z}_{\geq 1}$

$$\begin{aligned} L(1-n, \chi) &\neq 0, \text{ falls } n \equiv \delta \pmod{2}, \\ L(1-n, \chi) &= 0, \text{ falls } n \not\equiv \delta \pmod{2}, \end{aligned}$$

sowie $L(0, \chi_0) = \zeta(0) = -1/2$. Hierbei schreiben wir oft χ_0 für den trivialen Character (mit Führer 1).

Die Bernoullischen Zahlen sind definiert durch

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

Die verallgemeinerten Bernoullischen Zahlen sind definiert durch

$$\sum_{a=1}^f \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n, \chi} \frac{t^n}{n!}.$$

Offensichtlich gilt: $B_{n, \chi} \in \mathbb{Q}(\chi)$, wobei $\mathbb{Q}(\chi) := \mathbb{Q}(\chi(a) : a \in (\mathbb{Z}/m\mathbb{Z})^\times)$.

Satz 3.0.1 Für alle $n \geq 1$ gilt $L(1-n, \chi) = -\frac{B_{n, \chi}}{n}$. Insbesondere ist $L(1-n, \chi) \in \mathbb{Q}(\chi)$ für $n \geq 1$.

Satz 3.0.2 Es gilt

$$\begin{aligned} L(1, \chi) &= \pi i \frac{\tau(\chi)}{f} B_{1, \bar{\chi}}, \text{ falls } \chi(-1) = -1, \\ L(1, \chi) &= -\frac{\tau(\chi)}{f} \sum_{a=1}^f \bar{\chi}(a) \log |1 - \zeta_f^a|, \text{ falls } \chi(-1) = 1 \text{ und } \chi \neq \chi_0. \end{aligned}$$

Hierbei ist $\zeta_f := e^{2\pi i/f}$.

4 Stickelbergers Satz

4.1 Gaußsche Summen

Sei $q = p^n$ und $\zeta_p \in \mathbb{C}^\times$ eine fixierte primitive p -te Einheitswurzel. Sei $T: \mathbb{F}_q \rightarrow \mathbb{F}_p$ der Spuroperator und $\chi: \mathbb{F}_q^\times \rightarrow \mathbb{C}^\times$ ein Charakter. Wir setzen $\chi(0) := 0$.

Wir definieren einen additiven Charakter

$$\psi: \mathbb{F}_q \rightarrow \mathbb{C}^\times, \quad x \mapsto \zeta_p^{T(x)}.$$

Definition 4.1.1 Die Gaußsche Summe zu χ ist definiert durch

$$g(\chi) := - \sum_{a \in \mathbb{F}_q} \chi(a) \psi(a).$$

Falls $\chi^m = 1$ gilt, so folgt $g(\chi) \in \mathbb{Q}(\zeta_{mp})$. Ferner gilt: $g(1) = 1$, wobei hier 1 den trivialen Charakter bezeichnet.

Lemma 4.1.2 (a) $g(\bar{\chi}) = \chi(-1) \overline{g(\chi)}$.

(b) Falls $\chi \neq 1$, so gilt: $g(\chi)g(\bar{\chi}) = \chi(-1)q$.

(c) Falls $\chi \neq 1$, so gilt: $g(\chi)\overline{g(\chi)} = q$.

Definition 4.1.3 Für zwei Charaktere $\chi_1, \chi_2: \mathbb{F}_q^\times \rightarrow \mathbb{C}^\times$ nennt man

$$J(\chi_1, \chi_2) := - \sum_{a \in \mathbb{F}_q} \chi_1(a) \chi_2(1-a)$$

die Jacobische Summe von χ_1 und χ_2 .

Lemma 4.1.4 1. $J(1, 1) = 2 - q$.

2. Für $\chi \neq 1$ gilt $J(1, \chi) = J(\chi, 1) = 1$.

3. Für $\chi \neq 1$ gilt $J(\chi, \bar{\chi}) = \chi(-1)$.

4. Falls $\chi_1 \neq 1, \chi_2 \neq 1$ und $\chi_1 \chi_2 \neq 1$, so gilt:

$$J(\chi_1, \chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1 \chi_2)}.$$

Folgerung 4.1.5 Falls $\text{ord}(\chi_1)$ und $\text{ord}(\chi_2)$ Teiler von m sind, so gilt

$$\frac{g(\chi_1)g(\chi_2)}{g(\chi_1 \chi_2)} \in \mathbb{Z}[\zeta_m].$$

Für $(p, m) = 1$ und $b \in \mathbb{Z}$ mit $(b, m) = 1$ definieren wir $\sigma_b \in \text{Gal}(\mathbb{Q}(\zeta_p, \zeta_m)/\mathbb{Q})$ durch $\sigma_b(\zeta_p) := \zeta_p$ und $\sigma_b(\zeta_m) := \zeta_m^b$.

Lemma 4.1.6 Sei $(p, m) = 1$ und $\chi^m = 1$. Dann gilt:

1. $\frac{g(\chi)^b}{g(\chi)^{\sigma_b}} = g(\chi)^{b-\sigma_b} \in \mathbb{Q}(\zeta_m)$.

2. $g(\chi)^m \in \mathbb{Q}(\zeta_m)$.

4.2 Stickelbergerelemente und Stickelbergers Satz

Sei $M/\mathbb{Q}$ abelsch mit Gruppe G und m minimal mit $M \subseteq \mathbb{Q}(\zeta_m)$. Wir nennen dann m den Führer von M . Für $a \in \mathbb{Z}$ mit $(a, m) = 1$ sei $\sigma_a \in \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ definiert durch $\sigma_a(\zeta_m) := \zeta_m^a$. Wir schreiben ebenfalls σ_a für die Restriktion von σ_a auf M .

Für $x \in \mathbb{R}$ schreiben wir $\{x\}$ für den gebrochenen Anteil von x , d.h. $x - \{x\} \in \mathbb{Z}$ und $0 \leq \{x\} < 1$.

Definition 4.2.1 1. Das Stickelbergerelement zu M ist definiert durch

$$\Theta = \Theta(M) := \sum_{\substack{a \bmod m \\ (a, m) = 1}} \left\{ \frac{a}{m} \right\} \sigma_a^{-1} \in \mathbb{Q}[G].$$

2. $I(M) := \mathbb{Z}[G] \cap \Theta \mathbb{Z}[G]$ nennt man das Stickelbergerideal zu M .

Satz 4.2.2 (Stickelberger) $I(M)$ annulliert cl_M , oder explizit: Sei $\mathfrak{a} \in I_M$ ein gebrochenes Ideal und $\beta \in \mathbb{Z}[G]$, so dass $\Theta \beta \in \mathbb{Z}[G]$ gilt. Dann ist $\mathfrak{a}^{\beta \Theta}$ ein Hauptideal.

4.3 Beweis von Stickelbergers Satz

Sei p eine Primzahl und $q = p^f$. Sei $L = \mathbb{Q}(\zeta_{q-1})$ und $\mathfrak{p}$ ein fixiertes Primideal von $\mathcal{O}_L$ über p . Dann gilt $\mathcal{O}_L/\mathfrak{p} \simeq \mathbb{F}_q$. Wir definieren einen Teichmüllercharakter

$$\omega = \omega_{\mathfrak{p}}: \mathbb{F}_q^\times \longrightarrow \mu_{q-1}$$

durch die Forderung $\omega(a) \equiv a \pmod{\mathfrak{p}}$, $\forall a \in \mathcal{O}_L \setminus \mathfrak{p}$.

Betrachte nun den Körperturm $\mathbb{Q}(\zeta_{q-1}, \zeta_p)/\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}$. Das Primideal $\mathfrak{p}$ ist voll verzweigt (vom Grad $p-1$) in $\mathbb{Q}(\zeta_{q-1}, \zeta_p)/\mathbb{Q}(\zeta_{q-1})$ und wir bezeichnen das Primideal über $\mathfrak{p}$ mit $\tilde{\mathfrak{P}}$.

Definition 4.3.1 Für $\alpha \in \mathbb{Z}$ setzen wir $s(\alpha) := v_{\tilde{\mathfrak{P}}}(g(\omega^{-\alpha}))$.

Lemma 4.3.2 1. $s(0) = 0$.

$$2. 0 \leq s(\alpha + \beta) \leq s(\alpha) + s(\beta).$$

$$3. s(\alpha + \beta) \equiv s(\alpha) + s(\beta) \pmod{p-1}.$$

$$4. s(p\alpha) = s(\alpha).$$

$$5. \sum_{\alpha=1}^{q-2} s(\alpha) = (q-2)f(p-1)/2.$$

Lemma 4.3.3 $s(1) = 1$ und $s(\alpha) > 0$, falls $\alpha \not\equiv 0 \pmod{q-1}$.

Proposition 4.3.4 Sei $0 \leq \alpha < q-1$ und

$$\alpha = a_0 + a_1p + a_2p^2 + \dots + a_{f-1}p^{f-1} \text{ mit } 0 \leq a_i < p.$$

Dann gilt:

$$s(\alpha) = a_0 + a_1 + \dots + a_{f-1}.$$

Nach diesen Vorbereitungen kommen wir zum eigentlichen Beweis von Stickelbergers Satz.

Schritt 1: Sei $\mathfrak{p}_0$ ein Primideal in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ über der Primzahl p . Es gelte $(m, p) = 1$. Wir werden zeigen, dass $\mathfrak{p}_0^{m\theta}$ ein Hauptideal ist.

Sei $f := \text{ord}(p)$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ und $q := p^f$. Dann ist m ein Teiler von $q-1$ und wir setzen $d := (q-1)/m$.

Wir wählen nun ein Primideal $\mathfrak{P}_0$ über $\mathfrak{p}_0$ in $\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}(\zeta_m)$ und betrachten den Teichmüllercharakter

$$\omega = \omega_{\mathfrak{P}_0}: \mathbb{F}_q^\times \longrightarrow \mu_{q-1}.$$

Dann ist $\chi := \omega^{-d}$ ein Charakter der Ordnung m und somit $g(\chi) \in \mathbb{Q}(\zeta_m, \zeta_p)$ und $g(\chi)^m \in \mathbb{Q}(\zeta_m)$. Man zeigt nun:

$$(g(\chi)^m) = \mathfrak{p}_0^{m\theta}.$$

Insbesondere folgt hieraus, dass $m\theta$ die Idealklassengruppe von $\mathbb{Q}(\zeta_m)$ annulliert.

Schritt 2: Sei nun $M \subseteq \mathbb{Q}(\zeta_m)$ mit dem Führer m von M . Sei $\mathfrak{a}$ ein ganzes, zu m teilerfremdes Ideal von M . Wir schreiben

$$\mathfrak{a}\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \prod_i \mathfrak{p}_i$$

mit (nicht notwendig verschiedenen) Primidealen $\mathfrak{p}_i$ von $\mathbb{Q}(\zeta_m)$. Das Teilresultat aus dem ersten Schritt liefert

$$(\mathfrak{a}\mathcal{O}_{\mathbb{Q}(\zeta_m)})^{m\theta} = \left(\prod_i g(\chi_{\mathfrak{p}_i})^m \right)$$

mit Charakteren $\chi_{\mathfrak{p}_i}$, die a priori von der Wahl eines Primideals $\mathfrak{P}_i$ über $\mathfrak{p}_i$ abhängen. In Schritt 3 zeigt man jedoch, dass dies tatsächlich nicht der Fall ist.

Für $\beta \in \mathbb{Z}[G]$ mit $\beta\theta \in \mathbb{Z}[G]$ erhalten wir dann

$$(\mathfrak{a}_{\mathbb{Q}(\zeta_m)})^{m\beta\theta} = (\gamma^{\beta m}) \text{ mit } \gamma = \prod_i g(\chi_{\mathfrak{p}_i}).$$

Es gilt: $\gamma \in \mathbb{Q}(\zeta_{mP})$ mit $P := \prod_i p_i$. Wir wollen zunächst in der obigen Gleichung m aus dem Exponenten eliminieren.

Dazu zeigt man, dass $\mathbb{Q}(\zeta_m, \gamma^\beta)/\mathbb{Q}(\zeta_m)$ unverzweigt an allen endlichen Stellen ist. Hieraus folgt $\mathbb{Q}(\zeta_m, \gamma^\beta) = \mathbb{Q}(\zeta_m)$. Die Beweise zu diesen beiden Aussagen stehen noch aus und sind als pdf angefügt.

Es folgt $\gamma^\beta \in \mathbb{Q}(\zeta_m)$ und daher

$$(\mathfrak{a}_{\mathbb{Q}(\zeta_m)})^{\beta\theta} = (\gamma^\beta).$$

Schritt 3: Abschließend zeigt man $\gamma^\beta \in M$, woraus

$$\mathfrak{a}^{\beta\theta} = (\gamma^\beta)$$

folgt.

5 Iwasawas Konstruktion der p -adischen L -Funktionen

Sei p eine Primzahl und $q := p$ falls $p \neq 2$, bzw. $q = 4$, falls $p = 2$. Für $d \in \mathbb{N}$ mit $(p, d) = 1$ und $d \not\equiv 2 \pmod{4}$ setzen wir

$$q_n := qp^n d, \quad K_n := \mathbb{Q}(\zeta_{q_n}), \quad K_\infty := \cup_n K_n.$$

Dann ist K_∞/K_0 eine $\mathbb{Z}_p$ -Erweiterung. Wir setzen wie üblich

$$\Gamma := \text{Gal}(K_\infty/K_0), \quad \Gamma_n := \Gamma/\Gamma^{p^n} = \text{Gal}(K_n/K_0).$$

Dann gilt

$$\text{Gal}(K_n/\mathbb{Q}) \simeq \Delta \times \Gamma_n,$$

wobei wir Δ mit $\text{Gal}(K_0/\mathbb{Q})$ identifizieren.

Für $a \in \mathbb{Z}$ mit $(a, q_0) = 1$ sei $\sigma_a \in \text{Gal}(K_n/\mathbb{Q})$ definiert durch $\sigma_a(\zeta_{qp^n d}) = \zeta_{qp^n d}^a$. Wir schreiben

$$\sigma_a = \delta(a)\gamma_n(a) \text{ mit } \delta(a) \in \Delta, \gamma_n(a) \in \Gamma_n.$$

Sei nun χ ein Dirichletcharakter mit Führer $f_\chi = dp^j, j \geq 0$. Falls $\mathbb{Q}(\zeta_{dp^j}) \subseteq K_n$, so kann man χ als Charakter von $\text{Gal}(K_n/\mathbb{Q})$ auffassen und wir schreiben dann

$$\chi = \theta\psi \text{ mit } \theta \in \hat{\Delta}, \psi \in \hat{\Gamma}_n.$$

Definition 5.0.1

$$(a) \xi_n := -\text{Stickelbererelement zu } K_n/\mathbb{Q} = -\frac{1}{q_n} \sum_{\substack{a=1 \\ (a, q_0)=1}}^{q_n} a\delta(a)^{-1}\gamma_n(a)^{-1}.$$

$$(b) \eta_n := (1 - (1 + q_0)\gamma_n(1 + q_0)^{-1}) \xi_n.$$

Sei nun $\chi = \theta\psi$ ein gerader Dirichletcharakter (vom Führer dp^j wie oben). Wir setzen $\theta^* := \omega\theta^{-1}$, wobei ω den Teichmüllercharakter bezeichnet.

Für $\theta \in \hat{\Delta}$ bezeichne $\varepsilon_\theta \in \mathbb{Q}_p[\Delta]$ das übliche Idempotent,

$$\varepsilon_\theta := \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \theta(\delta)\delta^{-1}.$$

Dann gilt

$$\mathbb{C}_p[\text{Gal}(K_n/\mathbb{Q})] \simeq \sum_{\theta \in \Delta} \mathbb{C}_p[\Gamma_n], \quad \lambda \mapsto (\lambda \varepsilon_\theta).$$

Es gilt

$$\varepsilon_{\theta^*} \xi_n = \xi_n(\theta) \varepsilon_{\theta^*}, \quad \varepsilon_{\theta^*} \eta_n = \eta_n(\theta) \varepsilon_{\theta^*},$$

wobei

$$\begin{aligned} \xi_n(\theta) &:= -\frac{1}{q_n} \sum_{\substack{a=1 \\ (a, q_0)=1}} (\theta \omega^{-1})(a) \gamma_n(a)^{-1}, \\ \eta_n(\theta) &:= (1 - (1 + q_0) \gamma_n(1 + q_0)^{-1}) \xi_n(\theta). \end{aligned}$$

Sei nun $K_\theta := \mathbb{Q}_p(\theta(\delta) : \delta \in \Delta)$ und $\mathcal{O}_\theta \subseteq K_\theta$ der Bewertungsring in K_θ . Dann gilt:

$$\xi_n(\theta) \in K_\theta[\Gamma_n], \quad \eta_\theta \in \mathcal{O}_\theta[\Gamma_n].$$

Satz 5.0.2

- (a) $\frac{1}{2} \eta_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$.
- (b) $\frac{1}{2} \xi_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$, falls $\theta \neq 1$.
- (c) $\eta_m(\theta) \mapsto \eta_n(\theta)$, $\xi_m(\theta) \mapsto \xi_n(\theta)$, falls $m \geq n$.

Wir definieren nun Potenzreihen $g(T, \theta), h(T, \theta)$ vermöge

$$\begin{aligned} \mathcal{O}_\theta[[\Gamma]] &= \varprojlim_n \mathcal{O}_\theta[\Gamma_n] \simeq \mathcal{O}_\theta[[T]], \\ \{\eta_n(\theta)\}_{n=0}^\infty &\mapsto g(T, \theta), \\ \{1 - (1 + q_0) \gamma_n(1 + q_0)\}_{n=0}^\infty &\mapsto h(T, \theta), \end{aligned}$$

und setzen

$$f(T, \theta) := \frac{g(T, \theta)}{h(T, \theta)}.$$

Satz 5.0.3 Sei $\chi = \theta\psi$ ein gerader Dirichletcharakter. Sei

$$\zeta_\psi := \psi(1 + q_0) = \chi(1 + q_0).$$

Dann gilt:

$$L_p(s, \chi) = f(\zeta_\psi(1 + q_0)^s - 1, \theta).$$

Die p -adische L-Funktion $L_p(s, \chi)$ ist eine auf $\{s \in \mathbb{C}_p \mid |s| < qp^{-1/(p-1)}\}$ meromorphe (analytisch falls $\chi \neq 1$) definierte p -adische Funktion, die durch die Interpolationsbedingung

$$\begin{aligned} L_p(1 - m, \chi) &= -(1 - \chi \omega^{-m}(p) p^{m-1}) \frac{B_{m, \chi \omega^{-m}}}{m} \\ &= (1 - \chi \omega^{-m}(p) p^{m-1}) L(1 - m, \chi \omega^{-m}). \end{aligned}$$

eindeutig bestimmt ist. Es ist also zu zeigen, dass auch die rechte Seite dieser Interpolationsbedingung genügt.

6 $\mu = 0$

Satz 6.0.1 Sei $K/\mathbb{Q}$ abelsch und K_∞/K die zyklotomische $\mathbb{Z}_p$ -Erweiterung. Sei $A_\infty = \varprojlim_n A_n$, wobei A_n die p -Sylowuntergruppen der Idealklassengruppen von cl_{K_n} bezeichnet. Dann gilt:

$$\mu(A_\infty) = 0.$$

Es bezeichne $h_n = h(\mathbb{Q}(\zeta_{q_n}))$ die Klassenzahl von $\mathbb{Q}(\zeta_{q_n})$ und $h_n^+ = h(\mathbb{Q}(\zeta_{q_n})^+)$ die Klassenzahl des maximal reellen Teilkörpers $\mathbb{Q}(\zeta_{q_n})^+$ von $\mathbb{Q}(\zeta_{q_n})$. Dann ist

$$h_n^- := \frac{h_n}{h_n^+}$$

eine ganze Zahl.

Satz 6.0.2 Es gilt:

$$\frac{h_n^-}{h_0^-} = \left(\prod_{\zeta \neq 1, f_\theta | q_0, \theta \text{ gerade}} \prod_{\substack{\zeta^{p^n} = 1 \\ \zeta \neq 1}} f(\theta - 1, \theta) \right) \cdot u$$

mit einer Einheit $u \in \mathbb{Z}_p^\times$.

Satz 6.0.3 Sei $e_n^- = v_p(h_n^-)$. Dann gibt es ganze Zahlen $\lambda^- \geq 0, \mu^- \geq 0$ und ν^- , so dass

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

für alle $n \geq n_0$, n_0 geeignet.

Bemerkung 6.0.4 Der Beweis zeigt, dass $\mu^- = 0$ gilt, falls keines der $f(T, \theta) \in \mathcal{O}_\theta[[T]]$ durch p teilbar ist.

Im folgenden schreiben wir $\mu(K)$ für die μ -Invariante $\mu(A_\infty)$ in Satz 6.0.1. Die Aussage $\mu(K) = 0$ wird zurückgeführt auf den Beweis von $\mu^- = 0$. In der Vorlesung begnügen wir uns damit, die Rückführung zu beschreiben.

Man benötigt die folgenden Tatsachen:

1. Für beliebige Zahlkörper $K \subseteq K'$ gilt $\mu(K) \leq \mu(K')$.
2. Falls $\zeta_p \in K$, so gilt für $\mu = \mu(K)$

$$\mu = \mu^+ + \mu^- \text{ und } \mu^+ = 0, \text{ falls } \mu^- = 0.$$

Hierbei legen wir die Zerlegung $A_\infty = A_\infty^+ \oplus A_\infty^-$ mit

$$\begin{aligned} A_\infty^+ &:= \{a \in A_\infty \mid J(a) = a\}, \\ A_\infty^- &:= \{a \in A_\infty \mid J(a) = -a\}, \end{aligned}$$

zugrunde und setzen

$$\mu^{\pm 1} := \mu(A_\infty^{\pm 1}).$$

J bezeichnet die komplexe Konjugation.

3. Falls $e_n = \lambda n + \mu p^n + \nu$ für K_∞/K und $K' := K_m$, so gilt für die Invarianten von K_∞/K'

$$\lambda' = \lambda, \quad \mu' = p^m \mu, \quad \nu' = \nu + \lambda m.$$

7 Die Leopoldtvermutung

Sei K ein Zahlkörper und p eine Primzahl. Für $\mathfrak{p} \mid p$ in $K/\mathbb{Q}$ bezeichne $U_{\mathfrak{p}}^1 \leq U_{\mathfrak{p}} := \mathcal{O}_{K_{\mathfrak{p}}}^{\times}$ die Gruppe der Einseinheiten. Wir setzen

$$U := \prod_{\mathfrak{p} \mid p} U_{\mathfrak{p}}, \quad U^1 := \prod_{\mathfrak{p} \mid p} U_{\mathfrak{p}}^1$$

und betrachten für $E := \mathcal{O}_K^{\times}$ die Einbettung

$$\iota: E \longrightarrow U, \quad \varepsilon \mapsto (\varepsilon, \dots, \varepsilon).$$

Sei $E_1 := \iota^{-1}(U^1)$ das Urbild der Einseinheiten und $\bar{E}_1$ der topologische Abschluss in U^1 . Dann ist $\bar{E}_1$ ebenfalls ein $\mathbb{Z}_p$ -Modul und es gilt $\text{rk}_{\mathbb{Z}_p}(\bar{E}_1) \leq \text{rk}_{\mathbb{Z}}(E_1) = \text{rk}_{\mathbb{Z}}(E) = r_1 + r_2 - 1$.

Leopoldts Vermutung:

$$\text{rk}_{\mathbb{Z}_p}(\bar{E}_1) = r_1 + r_2 - 1.$$

Im weiteren sei K total reell. Sei $\varepsilon_1, \dots, \varepsilon_r$ ein System von Fundamenteleinheiten von E , wobei $r := r_1 - 1$ den Einheitenrang bezeichnet. Seien $\sigma_1, \dots, \sigma_{r+1}: K \longrightarrow \mathbb{C}_p$ die Einbettungen von K in $\mathbb{C}_p$.

Definition 7.0.1

$$R_p(K) := \det (\log_p(\sigma_i(\varepsilon_j)))_{1 \leq i, j \leq r}$$

heißt p -adischer Regulator von K .

Der p -adische Regulator ist bis auf das Vorzeichen wohlbestimmt.

Satz 7.0.2 Sei K total reell. Dann gilt:

$$R_p(K) \neq 0 \iff \text{rk}_{\mathbb{Z}_p}(\bar{E}_1) = r_1 - 1 \iff \text{Leopoldt für } K \text{ gilt.}$$

Sei nun $K/\mathbb{Q}$ abelsch. Mit transzendenten Methoden kann man $R_p(K^+) \neq 0$ zeigen. Es folgt:

Satz 7.0.3 Sei $K/\mathbb{Q}$ abelsch. Dann gilt Leopoldts Vermutung für K .

Bemerkung 7.0.4 Leopoldts Vermutung ist ebenfalls für abelsche Erweiterungen eines imaginär-quadratischen Zahlkörpers bewiesen.

Definition 7.0.5 Sei $\text{rk}_{\mathbb{Z}_p}(\bar{E}_1) = r_1 + r_2 - 1 - \delta$ mit $\delta \geq 0$. Dann nennt man $\delta = \delta(K)$ den Leopoldtdefekt.

Satz 7.0.6 Sei K ein Zahlkörper und $\tilde{K}$ das Kompositum aller $\mathbb{Z}_p$ -Erweiterungen von K . Dann gilt:

$$\text{Gal}(\tilde{K}/K) \simeq \mathbb{Z}_p^{r_2+1+\delta}.$$

Bemerkung 7.0.7 1) Falls K total reell ist und Leopoldts Vermutung für K gilt, so gibt es nur die zyklotomische $\mathbb{Z}_p$ -Erweiterung.

2) Für einen imaginär-quadratischen Zahlkörper K ist $\text{Gal}(\tilde{K}/K) \simeq \mathbb{Z}_p^2$. Es gilt

$$\tilde{K} = K_{cyc} K_{anti}$$

mit der zyklotomischen $\mathbb{Z}_p$ -Erweiterung K_{cyc}/K und der anti-zyklotomischen $\mathbb{Z}_p$ -Erweiterung K_{anti}/K