Ruprecht-Karls-Universität Heidelberg
Mathematisches Institut

Bachelorarbeit

p-adische L-Funktionen und die Leopoldt-Vermutung

Martin Lüdtke

Betreuer: Prof. Dr. Kay Wingberg

3. Juli 2012

Zusammenfassung

Um die Arithmetik eines abelschen Zahlkörpers K zu studieren, betrachtet man eine Gruppe von ihm zugeordneten Dirichlet-Charakteren χ. Die zu χ gehörige Dirichletsche L-Funktion wurde 1964 von Kubota und Leopoldt ins p-adische übertragen. Durch die Untersuchung der p-adischen L-Funktionen $L_p(s,\chi)$ gelingt es, Kongruenzen zwischen speziellen Werten herzuleiten, welche wichtige Resultate über die Bernoullischen Zahlen und reguläre Primzahlen zur Folge haben. Das Verhalten von $L_p(s,\chi)$ in $s=1$ steht über eine p-adische Klassenzahlformel mit dem p-adischen Regulator, der Diskriminante und der Klassenzahl von K in Verbindung. Das Nichtverschwinden des Regulators $R_p(K)$ für allgemeine Zahlkörper ist Gegenstand der Leopoldt-Vermutung.
Das Ziel dieser Arbeit ist die Konstruktion der p-adischen L-Funktionen im Sinne von Kubota und Leopoldt, die Herleitung der Kummerschen Kongruenzen und der Resultate über reguläre Primzahlen sowie eine Darstellung der Leopoldt-Vermutung samt ihres Beweises für abelsche Zahlkörper.

Abstract

To study the arithmetic of an abelian number field K one may consider a corresponding group of Dirichlet characters χ. In 1964, the Dirichlet L-function of χ was given a p-adic analogue by Kubota and Leopoldt. By investigating these p-adic L-functions $L_p(s,\chi)$ one finds that some special values satisfy certain congruences which imply the Kummer congruences for Bernoulli numbers and results on regular prime numbers. The behaviour of $L_p(s.\chi)$ in $s=1$ is related to the class number, the p-adic regulator and the discriminant of K by a p-adic class number formula. The non-vanishing of the regulator $R_p(K)$ is the statement of Leopoldt's conjecture.
The aim of this thesis is the construction of p-adic L-functions in the spirit of Kubota and Leopoldt, the derivation of the Kummer congruences and the results on regular prime numbers as well as a presentation of Leopoldt's conjecture, including a proof for abelian number fields.

Inhaltsverzeichnis

1 Einleitung 5

2 Dirichlet-Charaktere 7

3 Dirichletsche L-Funktionen 9

4 Bernoulli-Zahlen 10

5 p-adische Analysis 14

6 p-adische L-Funktionen 17

7 Kummerkongruenzen 21

8 Reguläre Primzahlen 26

9 Der p-adische Regulator 28

10 Die Leopoldt-Vermutung 35

Literaturverzeichnis 39

1 Einleitung

Die p-adischen L-Funktionen wurden 1964 von Kubota und Leopoldt eingeführt, mit dem Ziel, die endlichen abelschen Erweiterungen von $\mathbb{Q}$ zu studieren. Nach dem Satz von Kronecker-Weber ist jeder abelsche Zahlkörper K ein Teilkörper einer Kreisteilungserweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, und jedem solchen Körper K ist eine endliche Gruppe X von Homomorphismen $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$, Dirichlet-Charaktere genannt, zugeordnet. Es stellt sich nun die Frage, in welcher Weise sich die Eigenschaften des Zahlkörpers K in der einfacher zu übersehenden Gruppe X widerspiegeln. Um in der Beantwortung dieser Frage Fortschritte zu erzielen, lohnt es sich, gewisse Objekte zu studieren, die mit den Charakteren $\chi \in X$ verknüpft sind. Dazu gehören die Führer f_χ, die Gaußschen Summen $\tau(\chi)$, die verallgemeinerten Bernoulli-Zahlen $B_{n,\chi}$ und schließlich die Dirichletschen L-Funktionen $L(s,\chi)$ und deren p-adische Entsprechungen $L_p(s,\chi)$. Für uns werden besonders letztere von Interesse sein. Die zu χ gehörige Dirichletsche L-Funktion $L(s,\chi)$ ist zunächst als Verallgemeinerung der Riemannschen Zetafunktion über eine in der komplexen Halbebene $\mathfrak{Re}(s) > 1$ konvergente Reihe definiert, lässt sich aber analytisch auf $\mathbb{C} \setminus \{1\}$ fortsetzen. Es stellt sich heraus, dass die Funktionswerte in den negativen ganzen Zahlen von besonders einfacher Gestalt sind: es gilt nämlich

$$L(1-n,\chi) = -B_{n,\chi}/n \quad \text{für } n \geq 1,$$

d. h. $L(1-n,\chi)$ ist im Wesentlichen durch die verallgemeinerte Bernoulli-Zahl $B_{n,\chi}$ gegeben. Diese Werte sind zunächst komplexe Zahlen, aber wir können $B_{n,\chi}$ auch als Element einer algebraischen Erweiterung von $\mathbb{Q}_p$ betrachten. Darüber hinaus genügen die (gewöhnlichen) Bernoulli-Zahlen sogenannten Kummerkongruenzen, die im Grunde eine p-adische Stetigkeitsbedingung der Funktion $n \mapsto -B_n/n$ ausdrücken. Es gelang Kubota und Leopoldt, durch Interpolation der Werte von $L(s,\chi)$ in den negativen ganzen Zahlen ein p-adisches Analogon $L_p(s,\chi)$ zu konstruieren, also eine Funktion, welche auf einer geeigneten Erweiterung von $\mathbb{Q}_p$ definiert ist, dort analytisch ist und in den negativen ganzen Zahlen mit der gewöhnlichen L-Funktion übereinstimmt. Wenngleich die Kummerschen Kongruenzen schon lange vor der Einführung der p-adischen L-Funktionen bekannt waren, werden wir den umgekehrten Weg gehen und zuerst die p-adischen L-Funktionen konstruieren. Es ergeben sich dann die Kummerkongruenzen als Korollar aus einer allgemeineren Klasse von Kongruenzen zwischen Werten von $L_p(s,\chi)$. Eine weitere Folgerung aus diesen Kongruenzen ist eine handliche Charakterisierung der regulären Primzahlen, also derjenigen Primzahlen $p > 2$, welche die Klassenzahl von $\mathbb{Q}(\zeta_p)$ nicht teilen. Die Bedeutung dieser Primzahlen ergibt sich aus einem Satz von Kummer, der besagt, dass die Fermatsche Gleichung $X^p + Y^p = Z^p$ keine nichttrivialen ganzzahligen Lösungen besitzt, wenn p eine reguläre Primzahl ist. Als Folgerung aus der Charakterisierung der regu-

lären Primzahlen erhalten wir die Aussage, dass die Anzahl der irregulären Primzahlen unendlich ist.

Bei der Untersuchung der Dirichletschen L-Funktionen spielen jedoch nicht nur die Funktionswerte in den negativen ganzen Zahlen eine wichtige Rolle, auch dem Wert an der Stelle $s = 1$ kommt eine besondere Bedeutung zu. Es ist ein tiefliegendes Resultat, dass für alle Dirichlet-Charaktere $L(1, \chi) \neq 0$ ist. Unter anderem folgt hieraus der Dirichletsche Primzahlsatz. Die Frage, ob für die p-adischen L-Funktionen die entsprechende Aussage $L_p(1, \chi) \neq 0$ gilt, wird durch eine p-adische Klassenzahlformel auf die Untersuchung des p-adischen Regulators $R_p(K)$ eines Zahlkörpers K zurückgeführt. Für abelsche Zahlkörper gilt $R_p(K) \neq 0$; dies liefert einen Beweis für das Nichtverschwinden von $L_p(1, \chi)$, wenn χ ein Dirichlet-Charakter mit $\chi(-1) = 1$ ist (anderenfalls ist $L_p(s, \chi)$ konstant 0). Tatsächlich wurde von Leopoldt die Vermutung aufgestellt, dass $R_p(K) \neq 0$ für *beliebige* Zahlkörper gilt. Die Vermutung wurde zwar in speziellen Fällen verifiziert, aber bis heute ist kein allgemeiner Beweis erbracht worden. Eine andere Version der Leopoldt-Vermutung, die für total-reelle Zahlkörper zum Nichtverschwinden von $R_p(K)$ äquivalent ist, besagt, dass gewisse Einheiten von K, welche über $\mathbb{Z}$ unabhängig sind, auch dann unabhängig bleiben, wenn man allgemeine Koeffizienten aus $\mathbb{Z}_p$ zulässt. Auch diese Formulierung der Leopoldt-Vermutung ist für abelsche Zahlkörper, aber noch nicht im allgemeinen Fall, bewiesen worden.

Nachfolgend sollen die eben umrissenen Themen im Detail ausgearbeitet werden. Wir orientieren uns dabei an L.C. Washingtons Darstellung in [4], welche als Vorlage zur Verfassung dieser Arbeit diente. Der Schwerpunkt liegt auf der Konstruktion der p-adischen L-Funktionen, ihrer Anwendung hinsichtlich der Kummerschen Kongruenzen und der regulären Primzahlen, sowie ihrem Bezug zur Leopoldt-Vermutung. In den Abschnitten zwei bis fünf werden zunächst die später benötigten Definitionen und Sätze zusammengefasst, wobei auf die Ausführung der Beweise in den meisten Fällen verzichtet wird. Im Einzelnen werden Dirichlet-Charaktere eingeführt und die Korrespondenz zwischen endlichen Gruppen von Dirichlet-Charakteren und abelschen Zahlkörpern hergestellt. Weiterhin werden in Abschnitt 3 die klassischen L-Funktionen definiert und die wichtigsten Aussagen zur späteren Bezugnahme bei der Konstruktion der p-adischen Analoga festgehalten. In Abschnitt 4 werden die gewöhnlichen und verallgemeinerten Bernoulli-Zahlen sowie die Bernoulli-Polynome definiert und später benötigte Formeln notiert. Des weiteren wird der Satz von von Staudt-Clausen bewiesen und der Bezug zwischen Bernoulli-Zahlen und speziellen Werten der L-Funktionen hergestellt. In Abschnitt 5 sind die Hilfsmittel der p-adischen Analysis zusammengefasst, mittels derer wir anschließend in Abschnitt 6 die p-adischen L-Funktionen konstruieren. Die zwei nachfolgenden Abschnitte enthalten die Herleitungen der Kummerkongruenzen und der Resultate über reguläre Primzahlen. In Abschnitt 9 werden wir den p-adischen Regulator einführen und dessen Nichtverschwinden für abelsche Zahlkörper beweisen. Schließlich werden wir in Abschnitt 10 zwei Formulierungen der Leopoldt-Vermutung sehen. Es wird gezeigt, dass die beiden Formulierungen für total-reelle Zahlkörper äquivalent sind, und dass die Leopoldt-Vermutung in der zweiten Formulierung für alle abelschen Zahlkörper gültig ist.

2 Dirichlet-Charaktere

Ein **Dirichlet-Charakter** modulo n ist ein Homomorphismus $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$. Ist m ein Vielfaches von n, so lässt sich ein Dirichlet-Charakter modulo n über die kanonische Projektion $(\mathbb{Z}/m\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ auch als Dirichlet-Charakter modulo m auffassen. Ist χ ein Dirichlet-Charakter modulo n und n minimal gewählt, so nennen wir n den **Führer** von χ und bezeichnen diesen mit f_χ. Meistens werden wir einen Dirichlet-Charakter χ vermöge der Projektion $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/f_\chi\mathbb{Z}$ als Abbildung $\mathbb{Z} \to \mathbb{C}$ ansehen, indem wir $\chi(a) := 0$ setzen, wenn a und f_χ nicht teilerfremd sind. Dies ist immer noch eine vollständig multiplikative Abbildung, denn es gilt $(ab, f_\chi) = 1$ genau dann, wenn $(a, f_\chi) = 1$ und $(b, f_\chi) = 1$ gilt. Dirichlet-Charaktere, die modulo ihrem Führer definiert sind, heißen **primitiv**. Wir werden im Folgenden stillschweigend alle Dirichlet-Charaktere als primitiv ansehen. Auf diese Weise haben wir nur einen trivialen Dirichlet-Charakter (vom Führer 1) und nicht für jeden Modulus einen. Wegen $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$ muss entweder $\chi(-1) = 1$ oder $\chi(-1) = -1$ gelten. Im ersten Fall nennen wir χ **gerade**, anderenfalls **ungerade**. Sind χ und ψ Dirichlet-Charaktere vom Führer f_χ und f_ψ, so definieren wir $\chi\psi$ als Dirichlet-Charakter modulo $\mathrm{kgV}(f_\chi, f_\psi)$ durch $(\chi\psi)(a) := \chi(a)\psi(a)$. Die Menge aller Dirichlet-Charaktere bildet bezüglich dieser Verknüpfung eine Gruppe mit dem trivialen Charakter $\chi = 1$ als neutralem Element.

Für eine abelsche Gruppe G bezeichne $\hat{G} := \mathrm{Hom}(G, \mathbb{C}^\times)$ die **duale Gruppe** von G. Man hat die kanonische nicht-ausgeartete Paarung

$$\begin{aligned} G \times \hat{G} &\to \mathbb{C}^\times, \\ (\sigma, \chi) &\mapsto \chi(\sigma). \end{aligned}$$

Ist speziell $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, so besteht $\hat{G}$ gerade aus den Dirichlet-Charakteren modulo n. Ist $X \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})^\wedge$ eine Gruppe von Dirichlet-Charakteren modulo n, $H := \bigcap_{\chi \in X} \ker \chi$ der Durchschnitt ihrer Kerne und $K := \mathbb{Q}(\zeta_n)^H$ der Fixkörper von H, so induziert die Paarung einen natürlichen Isomorphismus

$$X \cong \left(\frac{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})}{\mathrm{Gal}(K/\mathbb{Q})} \right)^\wedge \cong \mathrm{Gal}(K/\mathbb{Q})^\wedge.$$

K ist unabhängig von der Wahl von n und heißt der **zu X gehörige Körper**.

Ist umgekehrt $K \subseteq \mathbb{Q}(\zeta_n)$ Teilkörper einer Kreisteilungserweiterung, so wird K die Gruppe

$$\{ \chi \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})^\wedge \mid \chi(\sigma) = 1 \ \forall \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K) \} \cong \mathrm{Gal}(K/\mathbb{Q})^\wedge$$

von Dirichlet-Charakteren modulo n zugeordnet. Dies liefert eine 1-zu-1-Korrespondenz zwischen endlichen Gruppen von Dirichlet-Charakteren und Teilkörpern von Kreisteilungserweiterungen:

$$\left\{\begin{array}{c}\text{endliche Gruppen}\\ \text{von Dirichlet-Charakteren}\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{Teilkörper von}\\ \text{Kreisteilungserweiterungen}\end{array}\right\}$$

Nach dem Satz von Kronecker-Weber ist sogar *jede* endliche abelsche Erweiterung von $\mathbb{Q}$ Teilkörper einer Kreisteilungserweiterung, aber wir werden diese Tatsache im Weiteren nicht benötigen.

Ist χ ein Dirichlet-Charakter, so wollen wir den Körper K, welcher der von χ erzeugten Gruppe $X = \langle\chi\rangle$ zugeordnet ist, kurz als den **zu χ gehörigen Körper** bezeichnen. Ist χ gerade, d. h. $\chi(-1) = 1$, so liegt die komplexe Konjugation $\zeta_n \mapsto \zeta_n^{-1}$ im Kern von χ, so dass K ein total-reeller Zahlkörper ist. Für ungerades χ ist umgekehrt K ein rein-imaginärer Zahlkörper.

3 Dirichletsche L-Funktionen

Die dem Dirichlet-Charakter χ zugeordnete **L-Reihe** ist definiert durch

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \mathfrak{Re}(s) > 1.$$

Die L-Reihe $L(s,\chi)$ definiert eine Funktion auf der komplexen Halbebene $\mathfrak{Re}(s) > 1$ und hat eine analytische Fortsetzung auf ganz $\mathbb{C}$, bis auf einen einfachen Pol in $s = 1$ im Falle $\chi = 1$ (in diesem Fall handelt es sich um die Riemannsche Zeta-Funktion). Die Funktion $L(\cdot,\chi)$ heißt die **Dirichletsche L-Funktion** zum Charakter χ. Es gilt die Eulersche Produktformel

$$L(s,\chi) = \prod_{p \text{ prim}} \left(1 - \chi(p)p^{-s}\right)^{-1}, \quad \mathfrak{Re}(s) > 1, \tag{3.1}$$

insbesondere hat $L(s,\chi)$ keine Nullstellen in der Halbebene $\mathfrak{Re}(s) > 1$. Ist F ein Vielfaches des Führers von χ, so gilt aufgrund der Periodizität von χ

$$L(s,\chi) = \sum_{a=1}^{F} \chi(a) \sum_{m \equiv a\ (F)} m^{-s} = \sum_{a=1}^{F} \chi(a) H(s,a,F), \quad \mathfrak{Re}(s) > 1 \tag{3.2}$$

mit den **partiellen Zeta-Funktionen** $H(s,a,F) = \sum_{n=0}^{\infty}(a+nF)^{-s}$. Mit der **Hurwitzschen Zeta-Funktion**

$$\zeta(s,b) = \sum_{n=0}^{\infty}(n+b)^{-s}, \quad \mathfrak{Re}(s) > 1, \quad 0 < b \leq 1$$

lassen sich die partiellen Zeta-Funktionen schreiben als

$$H(s,a,F) = \sum_{n=0}^{\infty}(a+nF)^{-s} = F^{-s}\zeta(s,a/F). \tag{3.3}$$

Sowohl die partiellen Zeta-Funktionen als auch die Hurwitzsche Zeta-Funktion lassen sich analytisch auf $\mathbb{C} \setminus \{1\}$ fortsetzen. Für alle $s \neq 1$ ergibt sich die Formel

$$L(s,\chi) = F^{-s} \sum_{a=1}^{F} \chi(a)\zeta(s,a/F). \tag{3.4}$$

4 Bernoulli-Zahlen

Die (gewöhnlichen) **Bernoulli-Zahlen** sind definiert als die eindeutig bestimmten Koeffizienten $B_n \in \mathbb{Q}$ in der Potenzreihe

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

Die ersten Bernoulli-Zahlen sind $B_0, B_1, B_2, \ldots = 1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, \frac{1}{42}, \ldots$ Da $\frac{t}{e^t-1} + t$ eine gerade Funktion ist, verschwinden alle Bernoulli-Zahlen B_{2n+1} mit ungeradem Index mit Ausnahme von $B_1 = -\frac{1}{2}$.

Für einen Dirichlet-Charakter χ vom Führer f sind die **verallgemeinerten Bernoulli-Zahlen** $B_{n,\chi}$ definiert durch

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

Die gewöhnlichen Bernoulli-Zahlen ergeben sich (mit Ausnahme von B_1) als Spezialfall der verallgemeinerten Bernoulli-Zahlen, wenn man für χ den trivialen Charakter wählt, denn

$$\sum_{n=0}^{\infty} B_{n,1} \frac{t^n}{n!} = \frac{te^t}{e^t - 1} = \frac{t}{e^t - 1} + t.$$

Für $n \neq 1$ gilt also $B_{n,1} = B_n$; für $n = 1$ gilt $B_{1,1} = \frac{1}{2}$ und $B_1 = -\frac{1}{2}$.

Ist $\chi \neq 1$ ein gerader Charakter, so ist die $B_{n,\chi}$ definierende Funktion gerade; ist χ ungerade, so ist sie ungerade. Haben n und χ unterschiedliche Parität, gilt daher $B_{n,\chi} = 0$.

Die **Bernoulli-Polynome** $B_n(X) \in \mathbb{Q}[X]$ sind definiert durch

$$\frac{te^{Xt}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(X) \frac{t^n}{n!}.$$

Aus

$$e^{Xt} \frac{t}{e^t - 1} = \left(\sum_{n=0}^{\infty} X^n \frac{t^n}{n!} \right) \left(\sum_{n=0}^{\infty} B_n \frac{t^n}{n!} \right)$$

erhält man durch Auflösen des Cauchy-Produkts die Formel

$$B_n(X) = \sum_{i=0}^{n} \binom{n}{i} B_i X^{n-i}. \tag{4.1}$$

Proposition 4.1. *Sei χ ein Dirichlet-Charakter und F ein Vielfaches des Führers. Dann gilt*

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n(a/F).$$

Beweis.

$$\begin{aligned}
&\sum_{n=0}^{\infty} F^{n-1} \sum_{a=1}^{F} \chi(a) B_n(a/F) \frac{t^n}{n!} \\
&\quad = \frac{1}{F} \sum_{a=1}^{F} \chi(a) \sum_{n=0}^{\infty} B_n(a/F) \frac{(Ft)^n}{n!} \\
&\quad = \frac{1}{F} \sum_{a=1}^{F} \chi(a) \frac{(Ft) e^{(a/F)(Ft)}}{e^{Ft} - 1} \quad \text{(nach Definition von } B_n(X)) \\
&\quad = \sum_{a=1}^{F} \chi(a) \frac{t e^{at}}{e^{Ft} - 1} \\
&\quad = \sum_{b=1}^{f} \sum_{c=0}^{F/f-1} \chi(b) \frac{t e^{(cf+b)t}}{e^{Ft} - 1} \quad \text{(mit } a = cf + b) \\
&\quad = \sum_{b=1}^{f} \chi(b) \frac{t e^{bt}}{e^{Ft} - 1} \sum_{c=0}^{F/f-1} e^{cft} \\
&\quad = \sum_{b=1}^{f} \chi(b) \frac{t e^{bt}}{e^{Ft} - 1} \frac{(e^{ft})^{F/f} - 1}{e^{ft} - 1} \quad \text{(geometrische Summenformel)} \\
&\quad = \sum_{b=1}^{f} \chi(b) \frac{t e^{bt}}{e^{ft} - 1} \\
&\quad = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!} \quad \text{(nach Definition von } B_{n,\chi})
\end{aligned}$$

Die Behauptung folgt durch Koeffizientenvergleich. □

Satz 4.2 (von Staudt-Clausen)**.** *Sei n eine positive gerade Zahl. Dann gilt*

$$B_n + \sum_{(p-1)|n} 1/p \in \mathbb{Z},$$

wobei sich die Summe über alle diejenigen Primzahlen p erstreckt, für welche $p-1$ ein Teiler von n ist. Insbesondere ist pB_n p-adisch ganz für alle Primzahlen p.

Bemerkung. Hier und im Folgenden heißt eine rationale Zahl x **p-adisch ganz**, wenn sie in $\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p$ liegt, d. h. wenn $x = a/b$ mit $p \nmid b$ gilt. Wir schreiben $x \equiv y \pmod{\mathbb{Z}_p}$, wenn $x - y$ p-adisch ganz ist.

Beweis. Wir zeigen, dass $B_n \equiv -1/p \pmod{\mathbb{Z}_p}$ gilt, falls $(p-1)|n$, und $B_n \equiv 0 \pmod{\mathbb{Z}_p}$ sonst. Dann ist $B_n + \sum_{(p-1)|n} 1/p$ für jede Primzahl p eine ganze p-adische Zahl und liegt somit in $\mathbb{Z}$.

Gelte die Behauptung für $m < n$, insbesondere ist dann $pB_m \in \mathbb{Z}_p$ für alle Primzahlen p und alle geraden positiven Zahlen $m < n$. Wegen $B_0 = 1$ und $B_1 = -1/2$ gilt dies auch für $m = 0, 1$. Mit Hilfe von Proposition 4.1 erhalten wir

$$\begin{aligned}
B_n = B_{n,1} &= p^{n-1} \sum_{a=1}^{p} B_n(a/p) \\
&= p^{n-1} \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} (B_j)(a/p)^{n-j} \quad \text{(nach Gleichung (4.1))} \\
&= \sum_{a=1}^{p} \sum_{j=0}^{n} \binom{n}{j} (pB_j) a^{n-j} p^{j-2} \\
&\overset{\text{Induktion}}{\equiv} \sum_{a=1}^{p} \left(pB_0 a^n p^{-2} + npB_1 a^{n-1} p^{-1} + pB_n p^{n-2} \right) \pmod{\mathbb{Z}_p} \\
&= \sum_{a=1}^{p} \left(a^n p^{-1} + nB_1 a^{n-1} \right) + p^n B_n.
\end{aligned}$$

Wegen $B_1 = -1/2$ und n gerade ist $nB_1 \in \mathbb{Z}_p$, also

$$B_n \equiv \frac{1}{p} \sum_{a=1}^{p} a^n + p^n B_n \pmod{\mathbb{Z}_p}$$

und somit

$$(1 - p^n) B_n \equiv \frac{1}{p} \sum_{a=1}^{p-1} a^n \pmod{\mathbb{Z}_p}.$$

Im Fall $(p-1)|n$ gilt $a^n \equiv 1 \pmod{p}$ für $a = 1, \ldots, p-1$, also

$$(1 - p^n) B_n \equiv \frac{1}{p} \sum_{a=1}^{p-1} 1 = \frac{p-1}{p} \equiv -1/p \pmod{\mathbb{Z}_p}.$$

Wegen $1 - p^n \equiv 1 \pmod{p}$ folgt $B_n \equiv -1/p \pmod{\mathbb{Z}_p}$, wie behauptet.

Im Fall $(p-1) \nmid n$ sei x eine Primitivwurzel modulo p, insbesondere $x^n \not\equiv 1 \pmod{p}$. Es gilt

$$(1 - x^n) \sum_{a=1}^{p-1} a^n = \sum_{a=1}^{p-1} a^n - \sum_{a=1}^{p-1} (ax)^n \equiv 0 \pmod{p},$$

also $\sum_{a=1}^{p-1} a^n \equiv 0 \pmod{p}$. Es folgt

$$(1 - p^n) B_n \equiv \frac{1}{p} \sum_{a=1}^{p-1} a^n \equiv 0 \pmod{\mathbb{Z}_p},$$

somit $B_n \equiv 0 \pmod{\mathbb{Z}_p}$ wegen $1 - p^n \in \mathbb{Z}_p^\times$. □

Es zeigt sich, dass die Werte von Dirichletschen L-Funktionen an den negativen ganzen Zahlen sich durch verallgemeinerte Bernoulli-Zahlen ausdrücken lassen.

Satz 4.3.

(a) $\zeta(1-n,b) = -B_n(b)/n \quad$ *für* $n \geq 1$ *und* $0 < b \leq 1$.

(b) $H(1-n,a,F) = -F^{n-1}B_n(a/F)/n \quad$ *für* $n \geq 1$ *und* $1 \leq a \leq F$.

(c) $L(1-n,\chi) = -B_{n,\chi}/n \quad$ *für* $n \geq 1$.

Die erste Aussage beweist man durch Betrachtung eines geeigneten komplexen Kurvenintegrals. Die Formeln für $H(1-n,a,F)$ und $L(1-n,\chi)$ folgen dann unter Benutzung von Proposition 4.1 aus den Gleichungen (3.3) und (3.4).

5 p-adische Analysis

Unser Ziel ist es, ein p-adisches Analogon der Dirichletschen L-Funktionen zu finden. Diese p-adischen L-Funktionen werden nicht auf den gewöhnlichen komplexen Zahlen $\mathbb{C}$ definiert sein, sondern auf einer entsprechenden Erweiterung $\mathbb{C}_p$ des Körpers der p-adischen Zahlen $\mathbb{Q}_p$ für eine feste Primzahl p. Dieser Körper soll einerseits algebraisch abgeschlossen sein, damit verallgemeinerte Dirichlet-Charaktere $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}_p^\times$ Einheitswurzeln beliebiger Ordnung annehmen können, andererseits soll er vollständig sein, um analytische Betrachtungen zu vereinfachen. Gehen wir über zu einem algebraischen Abschluss $\overline{\mathbb{Q}}_p$ von $\mathbb{Q}_p$, so setzt sich der p-adische Absolutbetrag $|\cdot|_p$ eindeutig fort, allerdings ist $\overline{\mathbb{Q}}_p$ bezüglich dieses Absolutbetrags nicht vollständig. Man definiert $\mathbb{C}_p$ als die Vervollständigung von $\overline{\mathbb{Q}}_p$. Dann ist $\mathbb{C}_p$ nicht nur vollständig, sondern auch algebraisch abgeschlossen, wie man mit Hilfe des Krasnerschen Lemmas zeigen kann. Der Körper $\mathbb{C}_p$ verhält sich in vielerlei Hinsicht ähnlich wie die komplexen Zahlen, insbesondere ermöglicht er analytische Untersuchungen, die der komplexen Funktionentheorie entsprechen. So lassen sich auf $\mathbb{C}_p$ etwa eine p-adische Exponentialfunktion und ein p-adischen Logarithmus definieren. Im Folgenden sollen einige Definitionen und Resultate aus der p-adischen Analysis zusammengefasst werden. Wir werden diese Hilfsmittel im nächsten Kapitel benutzen, um die p-adischen L-Funktionen zu konstruieren.

Wir betrachten zunächst die Exponentialreihe

$$\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

Man sieht leicht, dass die p-Bewertung von $n!$ gegeben ist durch

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots < \frac{n}{p-1}.$$

Es folgt, dass die Exponentialreihe für $|X| < p^{-1/(p-1)}$ konvergiert, da in diesem Fall die Glieder eine Nullfolge bezüglich der nicht-archimedischen Bewertung $|\cdot| = |\cdot|_p$ bilden. Für $|X| > p^{-1/(p-1)}$ divergiert die Reihe, d. h. $p^{-1/(p-1)}$ ist der Konvergenzradius. Im Gegensatz zur auf ganz $\mathbb{C}$ konvergenten komplexen Exponentialfunktion ist die p-adische Exponentialfunktion nur auf einer Teilmenge von $\mathbb{C}_p$ definiert. So lässt sich wegen $p^{-1/(p-1)} < 1$ kein p-adisches Analogon der Eulerschen Konstante $e = \exp(1)$ definieren.

Die p-adische Logarithmus $\log_p$ ist ebenfalls über seine Potenzreihenentwicklung

$$\log_p(1+X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} X^n$$

definiert. Die Reihe hat den Konvergenzradius 1, tatsächlich lässt sie sich aber auf ganz $\mathbb{C}_p^\times$ fortsetzen. Dazu wählen wir für alle $r \in \mathbb{Q}$ ein festes Element p^r derart, dass $p^r p^s = p^{r+s}$ gilt (zum Beispiel, indem wir p^r als positive reelle r-te Potenz von p in $\overline{\mathbb{Q}}$ wählen und $\overline{\mathbb{Q}}$ in $\mathbb{C}_p$ einbetten). Jedes Element $\alpha \in \mathbb{C}_p^\times$ hat dann eine eindeutige Darstellung $\alpha = p^r \zeta x$, mit $r \in \mathbb{Q}$, $|x-1| < 1$ und einer Einheitswurzel ζ von zu p primer Ordnung. Durch $\log_p(\alpha) := \log_p(x)$ wird der p-adische Logarithmus auf $\mathbb{C}_p^\times$ fortgesetzt. Es gilt dann $\log_p(p) = 0$ und die gewohnte Funktionalgleichung

$$\log_p(xy) = \log_p(x) + \log_p(y) \quad \text{für alle } x, y \in \mathbb{C}_p^\times.$$

Die Fortsetzung ist durch diese Eigenschaften eindeutig bestimmt.

Lemma 5.1. *Sei $x \in \mathbb{C}_p^\times$ mit $|x| < p^{-1/(p-1)}$. Dann gilt $|\log_p(1+x)| = |x|$.*

Beweis. Für $2 \le n < p$ gilt $|n| = 1$ und somit $\left|\frac{x^n}{n}\right| = |x|^{n-1}\,|x| < |x|$. Wegen $p^{v_p(n)} \le n$ gilt allgemein $|n| > 1/n$ und daher

$$\left|\frac{x^n}{n}\right| < n|x|^n < np^{-(n-1)/(p-1)}|x|.$$

Der Ausdruck auf der rechten Seite ist gleich $|x|$ für $n = p$ und monoton fallend mit $n \ge p$. Es folgt $|x^n/n| < |x|$ für alle $n \ge 2$ und somit

$$\left|\log_p(1+x)\right| = \left|x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots\right| = |x|$$

nach den Eigenschaften des archimedischen Absolutbetrags. □

Lemma 5.2. *Für $\alpha \in \mathbb{C}_p^\times$ gilt $\log_p \alpha = 0$ genau dann, wenn $\alpha = p^r\zeta$ für ein $r \in \mathbb{Q}$ und eine Einheitswurzel ζ gilt.*

Beweis. Gelte zunächst $\alpha = p^r\zeta$ mit $r \in \mathbb{Q}$ und einer n-ten Einheitswurzel ζ. Dann gilt

$$\log_p \alpha = \log_p \zeta = \frac{1}{n}\log \zeta^n = \frac{1}{n}\log_p 1 = 0.$$

Gelte umgekehrt $\log_p \alpha = 0$. Wir schreiben $\alpha = p^r\zeta x$ mit $r \in \mathbb{Q}$, $|x-1| < 1$ und einer Einheitswurzel ζ von zu p primer Ordnung. Wir setzen $y := x - 1$. Für hinreichend große N gilt $|y^{p^N}| < p^{-1/(p-1)}$. Weiter gilt

$$x^{p^N} = (1+y)^{p^N} = 1 + p^N y + \ldots + \binom{p^N}{j} y^j + \ldots + y^{p^N}.$$

Für die mittleren Terme $(0 < j < p^N)$ gilt $\left|\binom{p^N}{j}\right| \le |py| < |p| \le p^{-1/(p-1)}$ und N is so gewählt, dass $|y^{p^N}| < p^{-1/(p-1)}$ gilt. Daraus folgt $|x^{p^N} - 1| < p^{-1/(p-1)}$ und wir erhalten mit Lemma 5.1

$$|x^{p^N} - 1| = |\log_p(x^{p^N})| = |p^N \log_p \alpha| = 0.$$

Somit ist x eine p^N-te Einheitswurzel und $\alpha = p^r(\zeta x)$ hat die behauptete Form. □

Für $|x| < p^{-1/(p-1)}$ gilt erwartungsgemäß

$$\log_p(\exp(x)) = x,$$
$$\exp(\log_p(1+x)) = 1+x,$$

wobei der zweite Ausdruck wegen Lemma 5.1 wohldefiniert ist.

Wir betrachten nun Reihen einer bestimmten Form. Dazu definieren wir für eine nichtnegative ganze Zahl n das Polynom

$$\binom{X}{n} := \frac{X(X-1)\cdots(X-n+1)}{n!} \in \mathbb{Q}[X].$$

Für $X \in \mathbb{N}$ ist $\binom{X}{n}$ der gewöhnliche Binomialkoeffizient, insbesondere eine ganze Zahl. Für $X \in \mathbb{Z}_p$ liegt daher aus Stetigkeitsgründen $\binom{X}{n}$ wieder in $\mathbb{Z}_p$. Ist $(a_n)_{n\in\mathbb{N}}$ eine Nullfolge in $\mathbb{Q}_p$, so ist

$$f(X) = \sum_{n=0}^{\infty} a_n \binom{X}{n}$$

als gleichmäßiger Limes stetiger Funktionen wieder eine stetige Funktion $\mathbb{Z}_p \to \mathbb{Q}_p$. Ein Satz von Mahler besagt, dass tatsächlich jede stetige Funktion $\mathbb{Z}_p \to \mathbb{Q}_p$ auf diese Weise dargestellt werden kann und dass die Koeffizienten a_n eindeutig durch die Funktion f bestimmt sind. Die folgende Proposition besagt, dass f sogar analytisch ist, wenn a_n hinreichend schnell gegen 0 konvergiert.

Proposition 5.3. *Sei $r < p^{-1/(p-1)}$ (< 1) und seien $a_n \in \mathbb{Q}_p$ mit $|a_n| \leq Mr^n$ für eine Konstante M. Dann wird die Funktion*

$$f(X) = \sum_{n=0}^{\infty} a_n \binom{X}{n}$$

durch eine Potenzreihe mit Konvergenzradius mindestens $r^{-1}p^{-1/(p-1)}$ (> 1) dargestellt.

6 p-adische L-Funktionen

Sei p im Weiteren stets eine fest gewählte Primzahl. Wir werden im folgenden Abschnitt die p-adischen L-Funktionen $L_p(s,\chi)$ konstruieren. In Analogie zu den Formeln aus Satz 4.3 werden die Werte der p-adischen L-Funktion $L_p(s,\chi)$ in den negativen ganzen Zahlen ebenfalls durch Bernoulli-Zahlen ausgedrückt werden können. Wir konstruieren zuerst Entsprechungen der partiellen Zetafunktionen $H(s,a,F)$ und setzen $L_p(s,\chi)$ gemäß Formel (3.2) aus diesen zusammen.

Wir führen zunächst die folgende Notation ein:

$$q := \begin{cases} p, & \text{falls } p \neq 2, \\ 4, & \text{falls } p = 2. \end{cases}$$

Für $a \in \mathbb{Z}_p$ mit $p \nmid a$ bezeichne $\omega(a)$ die eindeutig bestimmte $\varphi(q)$-te (d. h. $(p-1)$-te, falls $p \neq 2$) Einheitswurzel in $\mathbb{Z}_p$ mit $\omega(a) \equiv a \pmod q$. (Für $p \neq 2$ existiert diese nach dem Henselschen Lemma.) Wir setzen ferner

$$\langle a \rangle := a/\omega(a),$$

dann besitzt a die Zerlegung $a = \omega(a)\langle a \rangle$ mit $\langle a \rangle \equiv 1 \pmod q$. Da $\mathbb{C}_p$ und $\mathbb{C}$ algebraisch (aber nicht topologisch) isomorph sind, können wir $\omega : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}_p^\times$ bezüglich eines fest gewählten Isomorphismus als Dirichlet-Charakter auffassen. Sein Führer ist q, er ist von der Ordnung $\varphi(q)$ und wird **Teichmüller-Charakter** genannt.

Wir können nun die p-adischen partiellen Zetafunktionen konstruieren.

Satz 6.1. *Sei F ein Vielfaches von q und $1 \leq a \leq F$ mit $p \nmid a$. Dann existiert eine p-adisch meromorphe Funktion $H_p(s,a,F)$ auf $D := \{s \in \mathbb{C}_p \mid |s| < qp^{-1/(p-1)}\}$ mit*

$$H_p(1-n,a,F) = \omega^{-n}(a)H(1-n,a,F), \qquad n \geq 1. \tag{6.1}$$

Die Funktion H_p ist analytisch bis auf einen einfachen Pol in $s=1$ mit Residuum $1/F$.

Beweis. Sei

$$H_p(s,a,F) := \frac{1}{s-1}\frac{1}{F}\langle a \rangle^{1-s} \sum_{j=0}^{\infty} \binom{1-s}{j} (B_j)(F/a)^j.$$

Nach dem Satz von von Staudt-Clausen gilt $pB_j \in \mathbb{Z}_p$, also $|B_j| \leq p$. Es gilt

$$\left|(B_j)(F/a)^j\right| = \underbrace{|B_j|}_{\leq p} \underbrace{|F|}_{\leq |q|}^{j} \underbrace{|a|}_{=1}^{-j} \leq p|q|^j = pq^{-j}.$$

Nach Proposition 5.3 wird die Reihe $\sum_{j=0}^{\infty}\binom{s}{j}(B_j)(F/a)^j$ durch eine Potenzreihe dargestellt, welche auf D konvergiert. Für nicht-archimedische Beträge ist jeder Punkt einer Kugel Mittelpunkt, wegen $1 < qp^{-1/(p-1)}$ ist also

$$D = \left\{ s \in \mathbb{C}_p \;\middle|\; |1-s| < qp^{-1/(p-1)} \right\}.$$

Somit ist auch $\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)(F/a)^j$ auf D konvergent. Ferner ist

$$\langle a\rangle^{1-s} := \exp\left((1-s)\log_p\langle a\rangle\right)$$

nach Lemma 5.1 für $s \in D$ wohldefiniert und analytisch, somit ist $H_p(s,a,F)$ insgesamt in D analytisch bis auf einen möglichen einfachen Pol in $s=1$. Es gilt

$$(s-1)H(s,a,F)\big|_{s=1} = \frac{1}{F}\langle a\rangle^0 \sum_{j=0}^{\infty}\binom{0}{j}(B_j)(F/a)^j = \frac{1}{F}B_0(F/a)^0 = 1/F,$$

d. h. $H_p(s,a,F)$ hat in $s=1$ einen einfachen Pol mit Residuum $1/F$.

Für $n \geq 1$ gilt

$$\begin{aligned}
H_p(1-n,a,F) &= -\frac{1}{n}\frac{1}{F}\langle a\rangle^n \sum_{j=0}^{\infty}\binom{n}{j}(B_j)(F/a)^j \\
&= -\frac{\langle a\rangle^n}{a^n}\frac{F^{n-1}}{n}\sum_{j=0}^{n}\binom{n}{j}(B_j)(a/F)^{n-j} \\
&= -\omega^{-n}(a)\frac{F^{n-1}B_n(a/F)}{n} \quad \text{(nach Gleichung (4.1))} \\
&= \omega^{-n}(a)H(s,a,F) \quad \text{(nach Satz 4.3)},
\end{aligned}$$

$H_p(s,a,F)$ hat also die gewünschte Interpolationseigenschaft. □

Aus den p-adischen partiellen Zetafunktionen ergeben sich nun die p-adischen L-Funktionen. Sei im Folgenden χ ein Dirichlet-Charakter vom Führer f. Wir fixieren einen Isomorphismus zwischen $\mathbb{C}$ und $\mathbb{C}_p$; auf diese Weise können wir die Werte von χ als in $\mathbb{C}_p^\times$ liegend betrachten.

Satz 6.2. *Es existiert eine p-adisch meromorphe Funktion $L_p(s,\chi)$ auf D mit*

$$L_p(1-n,\chi) = \left(1-\chi\omega^{-n}(p)p^{n-1}\right)\left(-B_{n,\chi\omega^{-n}}/n\right), \qquad (n \geq 1). \tag{6.2}$$

Für $\chi \neq 1$ ist die Funktion $L_p(s,\chi)$ analytisch; für $\chi = 1$ hat sie einen einfachen Pol in $s=1$ mit Residuum $1-1/p$.

Bemerkungen.

1. Hier bezeichnet $\chi\omega^{-n}$ das in Abschnitt 2 definierte Produkt von Charakteren, d. h. für $a \in \mathbb{Z}$ mit $(a,fq)=1$ ist $(\chi\omega^{-n})(a) := \chi(a)\omega(a)^{-n}$. Falls a nicht zu fq teilerfremd ist, gilt im Allgemeinen $(\chi\omega^{-n})(a) \neq \chi(a)\omega(a)^{-n}$. Für $\chi = \omega^n \neq 1$ ist etwa $(\chi\omega^{-n})(a) = 1$, aber $\chi(p) = \omega^{-n}(p) = 0$.

2. Da wir $H_p(s,a,F)$ nur für $p \nmid a$ konstruieren können, kann die p-adische L-Funktion nur die Werte von
$$\sum_{\substack{m=1\\ p\nmid m}}^{\infty} \frac{\chi\omega^{-n}(m)}{m^s} = \left(1-\chi\omega^{-n}(p)p^{-s}\right) L(s,\chi\omega^{-n})$$
an den negativen ganzen Zahlen interpolieren. Der Faktor $(1-\chi\omega^{-n}(p)p^{-s})$ ist der zur Primzahl p gehörige Faktor aus der Eulerproduktdarstellung (Formel 3.1) von $L(s,\chi\omega^{-n})$.

3. Nach der p-adischen Entsprechung des Identitätssatzes aus der Funktionentheorie ist $L_p(s,\chi)$ durch die Interpolationseigenschaft (6.2) eindeutig bestimmt, da 0 Häufungspunkt der negativen ganzen Zahlen ist.

4. Ist χ ein ungerader Charakter, so haben n und $\chi\omega^{-n}$ unterschiedliche Parität und es gilt $B_{n,\chi\omega^{-n}} = 0$ für alle natürlichen Zahlen n. Dann verschwindet $L_p(s,\chi)$ an den negativen ganzen Zahlen, ist also konstant 0 nach dem Identitätssatz.

Beweis. Sei F ein Vielfaches von q und f. Wir definieren
$$L_p(s,\chi) := \sum_{\substack{a=1\\ p\nmid a}}^{F} \chi(a) H_p(s,a,F).$$
Da $H_p(s,a,F)$ für $s \neq 1$ analytisch ist, gilt dies auch für $L_p(s,\chi)$. In $s=1$ hat $H_p(s,a,F)$ Residuum $1/F$, also gilt
$$\operatorname{res}\big|_{s=1} L_p(s,\chi) = \frac{1}{F}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a) = \frac{1}{F}\sum_{a=1}^{F}\chi(a) - \frac{1}{F}\sum_{b=1}^{F/p}\chi(pb).$$
Für $\chi = 1$ ist
$$\operatorname{res}\big|_{s=1} L_p(s,1) = \frac{1}{F}\sum_{\substack{a=1\\ p\nmid a}}^{F} 1 = \frac{1}{F}\left(F - \frac{F}{p}\right) = 1 - 1/p.$$
Für $\chi \neq 1$ sei $x \in (\mathbb{Z}/F\mathbb{Z})^\times$ mit $\chi(x) \neq 1$. Dann gilt
$$\big(1-\chi(x)\big)\sum_{a=1}^{F}\chi(a) = \sum_{a=1}^{F}\chi(a) - \sum_{a=1}^{F}\chi(ax) = 0,$$
also $\sum_{a=1}^{F}\chi(a) = 0$. Falls $p|f$, dann ist $\chi(p) = 0$ und somit $\sum_{b=1}^{F/p}\chi(pb) = 0$. Anderenfalls gilt $f|\frac{F}{p}$ und es folgt wiederum $\sum_{b=1}^{F/p}\chi(pb) = 0$ nach dem gleichen Argument wie oben. Insgesamt folgt
$$\operatorname{res}\big|_{s=1} L_p(s,\chi) = \frac{1}{F}\sum_{a=1}^{F}\chi(a) - \frac{1}{F}\sum_{b=1}^{F/p}\chi(pb) = 0,$$

d. h. $L_p(s,\chi)$ hat in $s=1$ keinen Pol und ist auf ganz D analytisch.
Für $n \geq 1$ gilt

$$\begin{aligned}
L_p(1-n,\chi) &= \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a) H_p(1-n,a,F) \\
&= -\frac{F^{n-1}}{n} \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi\omega^{-n}(a) B_n(a/F) \quad \text{(nach (6.1) und Satz 4.3)} \\
&= -\frac{1}{n} F^{n-1} \sum_{a=1}^{F} \chi\omega^{-n}(a) B_n(a/F) + \frac{1}{n} p^{n-1} (F/p)^{n-1} \sum_{b=1}^{F/p} \chi\omega^{-n}(pb) B_n\left(\frac{b}{F/p}\right) \\
&= -\frac{1}{n} B_{n,\chi\omega^{-n}} + \frac{1}{n} \chi\omega^{-n}(p) p^{n-1} B_{n,\chi\omega^{-n}} \quad \text{(nach Proposition 4.1)} \\
&= \left(1-\chi\omega^{-n}(p)p^{n-1}\right)\left(-B_{n,\chi\omega^{-n}}/n\right) \\
&= \left(1-\chi\omega^{-n}(p)p^{n-1}\right) L(1-n,\chi\omega^{-n}),
\end{aligned}$$

d. h. $L_p(s,\chi)$ besitzt die gewünschte Interpolationseigenschaft. □

7 Kummerkongruenzen

Im vorigen Abschnitt haben wir Dirichletsche L-Funktionen, Objekte der komplexen Funktionentheorie, in die Welt der p-adischen Zahlen übertragen. Der Körper $\mathbb{C}_p$ ist nun zugleich von analytischer sowie zahlentheoretischer Natur. Dies ermöglicht es uns, Kongruenzen zwischen den Werten der p-adischen L-Funktionen herzuleiten. Insbesondere erhalten wir auf diese Weise Kongruenzen zwischen Bernoulli-Zahlen, die sogenannten Kummerkongruenzen. Die Kummerschen Kongruenzen waren schon lange vor der Einführung der p-adischen L-Funktionen bewiesen worden. Tatsächlich drücken sie eine Art p-adischer Stetigkeitsbedingung zwischen den Werten der Riemannschen Zetafunktion in den negativen ganzen Zahlen aus, welche zu der Vermutung Anlass gaben, man könne sie durch Interpolation stetig auf einen größeren Bereich fortsetzen. Wie wir im letzten Abschnitt gesehen haben, ist eine solche Fortsetzung tatsächlich möglich – nicht nur für die Riemannsche Zetafunktion, sondern allgemeiner für beliebige Dirichletsche L-Funktionen – und die Fortsetzung ist sogar analytisch auf einer Kreisscheibe in $\mathbb{C}_p$.

Die zahlentheoretische Natur von $\mathbb{C}_p$ ergibt sich aus der Tatsache, dass $\mathbb{C}_p$ im Gegensatz zu den gewöhnlichen komplexen Zahlen einen *nicht-archimedischen* Absolutbetrag trägt, so dass die Einheitskreisscheibe

$$\mathcal{O} = \{\, x \in \mathbb{C}_p \mid |x| \leq 1 \,\}$$

einen Ring bildet, den **Bewertungsring** von $\mathbb{C}_p$. Wir nennen $x \in \mathbb{C}_p$ **p-adisch ganz**, wenn $x \in O$ gilt (diese Definition stimmt für rationale Zahlen mit der aus Abschnitt 4 überein). Es ist $\mathbb{C}_p$ auf natürliche Weise ein $\mathcal{O}$-Modul, was zu dem folgenden Teilbarkeitsbegriff auf $\mathbb{C}_p$ führt: Für $x, y \in \mathbb{C}_p$ schreiben wir $x \mid y$, wenn eine der folgenden äquivalenten Bedingungen gilt:

(i) $y = ax$ für ein $a \in \mathcal{O}$,

(ii) $|y| \leq |x|$,

(iii) $x = y = 0$ oder $y/x \in \mathcal{O}$.

Für $x, y, z \in \mathbb{C}_p$ schreiben wir ferner $x \equiv y \pmod{z}$, wenn $z \mid x - y$ gilt.

Satz 7.1. *Sei $\chi \neq 1$ und gelte $pq \nmid f$. Sei*

$$L_p(s, \chi) = a_0 + a_1(s-1) + a_2(s-1)^2 + \ldots$$

die Potenzreihenentwicklung von $L_p(s, \chi)$ um $s = 1$. Für die Koeffizienten gilt dann $|a_0| \leq 1$ und $p \mid a_k$ für $k \geq 1$.

Bemerkung. Da für $s = 2$ die Reihe $L_p(2, \chi) = \sum_{k=0}^{\infty} a_k$ konvergiert, bilden die Koeffizienten a_k eine Nullfolge, so dass a priori $p \mid a_k$ für hinreichend große k gilt.

Beweis. Wegen $pq \nmid f$ können wir F als Vielfaches von q und f mit $pq \nmid F$ wählen. Seien

$$\sum_{j=0}^{\infty} b_{a,j}(s-1)^j = \langle a\rangle^{1-s},$$
$$\sum_{j=0}^{\infty} c_{a,j}(s-1)^j = \frac{1}{F}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)(F/a)^j$$

die jeweiligen Reihenentwicklungen in $s = 1$, dann gilt

$$\begin{aligned} L_p(s,\chi) &= \frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\langle a\rangle^{1-s}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)(F/a)^j \\ &= \frac{1}{s-1}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\left(\sum_{j=0}^{\infty} b_{a,j}(s-1)^j\right)\left(\sum_{j=0}^{\infty} c_{a,j}(s-1)^j\right) \end{aligned}$$

und somit

$$a_k = \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\sum_{j=0}^{k+1} b_{a,j}\, c_{a,k+1-j}, \qquad (k \geq 0).$$

Wir betrachten zuerst getrennt die Koeffizienten $b_{a,j}$ und $c_{a,j}$ und folgern daraus die behaupteten Abschätzungen für die a_k. Es gilt

$$\langle a\rangle^{1-s} = \exp\big((1-s)\log_p\langle a\rangle\big) = \sum_{j=0}^{\infty}\frac{(-\log_p\langle a\rangle)^j}{j!}(s-1)^j,$$

also $b_{a,j} = (-\log_p\langle a\rangle)^j/j!$. Nach Lemma 5.1 gilt $|\log_p\langle a\rangle| \leq |q|$. Eine kurze Rechnung unter Benutzung von $v_p(j!) < \frac{j}{p-1}$ zeigt $b_{a,j} \in \mathcal{O}$ für $j \geq 0$ und $pq \mid b_{a,j}$ für $j \geq 2$.

Für die $c_{a,j}$ gilt

$$\begin{aligned} \sum_{j=0}^{\infty}(-1)^j c_{a,j}(1-s)^j &= \frac{1}{F}\sum_{j=0}^{\infty}\binom{1-s}{j}(B_j)(F/a)^j \\ &= \sum_{j=0}^{\infty}\prod_{i=0}^{j-1}((1-s)-i)\,\frac{B_j}{j!}\frac{F^{j-1}}{a^j}. \end{aligned}$$

Nach dem Satz von von Staudt-Clausen gilt $|pB_j| \leq p$, damit folgt

$$\left|\frac{B_j}{j!}\frac{F^{j-1}}{a^j}\right| = |B_j|\,|j!|^{-1}\,|F|^{j-1} \leq p\,p^{j/(p-1)}q^{1-j}.$$

Für $j \geq 6$ ist die rechte Seite $\leq |q|$. Für $j = 3, 4, 5$ prüft man leicht, dass ebenfalls $\left|\frac{B_j}{j!}\frac{F^{j-1}}{a^j}\right| \leq |q|$ gilt. Wir haben also $q \mid \frac{B_j}{j!}\frac{F^{j-1}}{a^j}$ für $j \geq 3$. Es folgt

$$\begin{aligned}\sum_{j=0}^{\infty}(-1)^j c_{a,j} X^j &= \sum_{j=0}^{\infty}\prod_{i=0}^{j-1}(X-i)\,\frac{B_j}{j!}\frac{F^{j-1}}{a^j} \\ &\equiv \frac{B_0}{0!}\frac{F^{-1}}{a^0} + \frac{B_1}{1!}\frac{F^0}{a^1}X + \frac{B_2}{2!}\frac{F^1}{a^2}X(X-1) \pmod q \\ &= \frac{1}{F} - \left(\frac{1}{2a} + \frac{F}{12a^2}\right)X + \frac{F}{12a^2}X^2.\end{aligned}$$

Wir erhalten durch Koeffizientenvergleich

$$\begin{aligned} c_{a,0} &\equiv \frac{1}{F} \pmod q, \\ c_{a,1} &\equiv \frac{1}{2a} + \frac{F}{12a^2} \pmod q, \\ c_{a,2} &\equiv \frac{F}{12a^2} \pmod q, \\ c_{a,i} &\equiv 0 \pmod q \qquad \text{für } i \geq 3. \end{aligned}$$

Nun betrachten wir die Koeffizienten a_k in der Reihenentwicklung von $L_p(s,\chi)$. Es gilt

$$\begin{aligned} a_0 &= \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\big(\underbrace{b_{a,0}}_{=1}\,c_{a,1} + \underbrace{b_{a,1}}_{=-\log_p\langle a\rangle}\,c_{a,0}\big) \\ &\equiv \sum_{\substack{a=1\\ p\nmid a}}^{F}\chi(a)\left(\frac{1}{2a} + \underbrace{\frac{F}{12a^2}}_{\in\mathcal{O}} - \underbrace{\frac{\log_p\langle a\rangle}{F}}_{\in\mathcal{O}}\right) \pmod q \\ &\equiv \frac{1}{2}\sum_{\substack{a=1\\ p\nmid a}}^{F}\frac{\chi(a)}{a} \pmod 1 \\ &\equiv \frac{1}{2}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi\omega^{-1}(a) \pmod 1. \end{aligned}$$

Falls $\chi\omega^{-1} = 1$, dann gilt

$$\frac{1}{2}\sum_{\substack{a=1\\ p\nmid a}}^{F}\chi\omega^{-1}(a) = \frac{1}{2}F(1-1/p) = \frac{F}{2p}(p-1) \in \mathbb{Z}_p.$$

Falls $\chi\omega^{-1} \neq 1$, argumentieren wir wie im Beweis von Satz 6.2 und erhalten $a_0 \equiv 0 \pmod 1$. In jedem Fall gilt $|a_0| \leq 1$.

Für a_1 gilt

$$\begin{aligned} a_1 &= \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a)\,(b_{a,0}\,c_{a,2} + b_{a,1}\,c_{a,1} + b_{a,2}\,c_{a,0}) \\ &\equiv \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a)\left(\frac{F}{12a^2} - \frac{\log_p\langle a\rangle}{2a} - \frac{F}{12a^2}\log_p\langle a\rangle + \frac{b_{a,2}}{F}\right) \pmod q. \end{aligned}$$

Wegen $pq \mid b_{a,2}$ und $|F| = |q|$ gilt $p \,\Big|\, \frac{b_{a,2}}{F}$. Wegen $q \,\Big|\, \log_p\langle a\rangle$ und $F/12 \in \mathbb{Z}_p$ gilt $p \,\Big|\, \frac{\log_p\langle a\rangle}{2a}$ und $p \,\Big|\, \frac{F}{12a^2}\log_p\langle a\rangle$. Somit folgt

$$a_1 \equiv \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a)\frac{F}{12a^2} \pmod p.$$

Für $p \geq 5$ gilt $p \mid \frac{F}{12}$ und damit $p \mid a_1$. Für $p = 2, 3$ gilt $a^2 \equiv 1 \pmod p$, also

$$a_1 \equiv \frac{F}{12}\sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a) = 0 \pmod p.$$

Für a_2 gilt

$$\begin{aligned} a_2 &= \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a)\big(\underbrace{b_{a,0}}_{=1}\underbrace{c_{a,3}}_{\equiv 0} + \underbrace{b_{a,1}}_{\equiv 0}\underbrace{c_{a,2}}_{\in\mathcal{O}} + b_{a,2}\,c_{a,1} + b_{a,3}\,c_{a,0}\big) \\ &\equiv \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a)\left(b_{a,2}\left(\frac{1}{2a} + \frac{F}{12a^2}\right) + b_{a,3}\frac{1}{F}\right) \pmod p. \end{aligned}$$

Wegen $pq \mid b_{a,2}$ und $pq \mid b_{a,3}$ sind alle Summanden durch p teilbar, also $p \mid a_2$.

Für $k \geq 3$ gilt schließlich

$$a_k = \sum_{\substack{a=1 \\ p\nmid a}}^{F} \chi(a)\sum_{j=0}^{k+1} b_{a,j}\,c_{a,k+1-j}.$$

Für $j \leq 1$ gilt $|b_{a,j}| \leq 1$ und $p \mid c_{a,k+1-j}$; für $j \geq 2$ gilt umgekehrt $p \mid b_{a,j}$ und $|c_{a,k+1-j}| \leq 1$. Somit sind alle Summanden durch p teilbar und es folgt $p \mid a_k$. □

Korollar 7.2. *Sei $\chi \neq 1$ und gelte $pq \nmid f$. Seien ferner $m, n \in \mathbb{Z}$. Dann gilt*

$$L_p(m,\chi) \equiv L_p(n,\chi) \pmod p$$

und beide Seiten sind p-adisch ganz.

Beweis. Beide Seiten sind kongruent zu $a_0 \in \mathcal{O}$. □

Korollar 7.3 (Kummerkongruenzen)**.**
Seien m und n positive gerade Zahlen mit $m \equiv n \not\equiv 0 \pmod{p-1}$. Dann gilt

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p}.$$

Allgemeiner: Gilt $m \equiv n \pmod{(p-1)p^a}$ und $m, n \not\equiv 0 \pmod{p-1}$, so gilt

$$\left(1 - p^{m-1}\right) \frac{B_m}{m} \equiv \left(1 - p^{n-1}\right) \frac{B_n}{n} \pmod{p^{a+1}}.$$

Beweis. Die Voraussetzung $m, n \not\equiv 0 \pmod{p-1}$ impliziert $p \neq 2$. Da der Teichmüller-Charakter ω Ordnung $p-1$ hat, gilt $\omega^m = \omega^n \neq 1$. Wegen $p \mid a_k$ für $k \geq 1$ und $m \equiv n \pmod{p^a}$ gilt

$$\begin{aligned}
\left(1 - p^{m-1}\right) \frac{B_m}{m} &= L_p(1-m, \omega^m) \\
&= a_0 + a_1(-m) + a_2(-m)^2 + \dots \\
&\equiv a_0 + a_1(-n) + a_2(-n)^2 + \dots \pmod{p^{a+1}} \\
&= L_p(1-n, \omega^n) \\
&= \left(1 - p^{n-1}\right) \frac{B_n}{n}.
\end{aligned}$$

□

Korollar 7.4. *Sei n eine positive ungerade Zahl mit $n \not\equiv -1 \pmod{p-1}$. Dann gilt*

$$B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \pmod{p}$$

und beide Seiten sind p-adisch ganz.

Beweis. Wegen $n+1 \not\equiv 0 \pmod{p-1}$ gilt $\omega^{n+1} \neq 1$. Da p ungerade sein muss, ist $p-1$ gerade, also kein Teiler von n. Es folgt $\omega^n \neq 1$ und somit $\omega^n(p) = 0$. Nach Korollar 7.2 gilt

$$\begin{aligned}
B_{1,\omega^n} &= (1 - \omega^n(p))\, B_{1,\omega^n} = -L_p(0, \omega^{n+1}) \\
&\equiv -L_p(1-(n+1), \omega^{n+1}) = (1 - p^n)\, \frac{B_{n+1}}{n+1} \\
&\equiv \frac{B_{n+1}}{n+1} \pmod{p}.
\end{aligned}$$

Aus Korollar 7.2 folgt auch, dass beide Seiten p-adisch ganz sind. □

8 Reguläre Primzahlen

Ein berühmter Satz von Kummer besagt, dass die Fermatsche Gleichung

$$X^p + Y^p = Z^p$$

keine nichttrivialen Lösungen in den ganzen Zahlen besitzt, wenn p eine ungerade Primzahl ist, welche die Klassenzahl h_p des Kreisteilungskörpers $\mathbb{Q}(\zeta_p)$ nicht teilt. Die Primzahlen mit dieser Eigenschaft heißen **reguläre Primzahlen**. Es stellt sich die Frage, wie man zu einer gegebenen Primzahl bestimmen kann, ob sie regulär ist, und wie viele irreguläre Primzahlen es gibt. Im folgenden Abschnitt werden wir mit Hilfe der eben hergeleiteten Kongruenzen ein Kriterium dafür angeben, wann eine Primzahl regulär ist. Ferner werden wir beweisen, dass die Zahl der irregulären Primzahlen unendlich ist.

Satz 8.1. *Eine ungerade Primzahl p ist genau dann irregulär, wenn p eine der Bernoulli-Zahlen $B_2, B_4, \ldots, B_{p-3}$ teilt.*

Beweis. Sei $\mathbb{Q}(\zeta_p)^+$ der maximal reelle Teilkörper von $\mathbb{Q}(\zeta_p)$ und h_p^+ die Klassenzahl von $\mathbb{Q}(\zeta_p)^+$. Es gilt dann $h_p^+ \mid h_p$ und p ist genau dann regulär, wenn p die **relative Klassenzahl** $h_p^- := h_p/h_p^+$ teilt. Diese Tatsache soll hier nicht gezeigt werden; für den Beweis siehe Kapitel 4 in [4]. Wir verwenden ferner ohne Beweis die Formel

$$h_p^- = 2p \prod_{\substack{j=1 \\ 2 \nmid j}}^{p-2} \left(-\frac{1}{2} B_{1,\omega^j} \right).$$

Mit Proposition 4.1 folgt

$$B_{1,\omega^{p-2}} = B_{1,\omega^{-1}} = \sum_{a=1}^{p} \omega^{-1}(a) \frac{a}{p} = \frac{1}{p} \sum_{a=1}^{p-1} \langle a \rangle,$$

damit folgt

$$2p \left(-\frac{1}{2} B_{1,\omega^{p-2}} \right) = -\sum_{a=1}^{p-1} \langle a \rangle \equiv -(p-1) \equiv 1 \pmod{p}.$$

Nach Korollar 7.4 gilt

$$h_p^- = (2p) \left(-\frac{1}{2} B_{1,\omega^{p-2}} \right) \prod_{\substack{j=1 \\ 2 \nmid j}}^{p-4} \left(-\frac{1}{2} B_{1,\omega^j} \right) \equiv \prod_{\substack{j=1 \\ 2 \nmid j}}^{p-4} \left(-\frac{1}{2} \frac{B_{j+1}}{j+1} \right) \pmod{p}.$$

Die relative Klassenzahl h_p^- ist genau dann durch p teilbar, wenn einer der Faktoren durch p teilbar ist. Da 2 und $j+1$ Einheiten in $\mathbb{Z}_p$ sind, folgt die Behauptung. □

Satz 8.2. *Es gibt unendlich viele irreguläre Primzahlen.*

Beweis. Angenommen, $p_1, \ldots, p_r$ sind alle irregulären Primzahlen. Wir setzen $m := N(p_1 - 1) \cdots (p_r - 1)$ mit einer noch zu wählenden Zahl N. Ohne Beweis verwenden wir $|B_{2n}/2n| \to \infty$ $(n \to \infty)$. Wir können also N so wählen, dass $|B_m/m| > 1$ gilt. Sei p eine Primzahl mit $p \mid \frac{B_m}{m}$. Nach dem Satz von von Staudt-Clausen treten die p_i im Nenner von B_m auf, also muss p von $p_1, \ldots, p_r$ verschieden sein. Aus dem gleichen Grund muss $(p-1) \nmid m$ gelten, somit gilt $m \equiv m' \pmod{p-1}$ mit $0 < m' < p - 1$. Nach den Kummerkongruenzen gilt

$$\frac{B_{m'}}{m'} \equiv \frac{B_m}{m} \equiv 0 \pmod{p},$$

damit ist aber p irregulär nach Satz 8.1. Widerspruch! □

9 Der p-adische Regulator

Es ist eine tiefliegende Tatsache, dass $L(1,\chi)$ nicht verschwindet. Tatsächlich gilt wie im komplexen Fall $L_p(1,\chi) \neq 0$, aber dies ist ebenfalls ein tiefliegendes Resultat, welches wir im Folgenden beweisen wollen. Wir führen dazu den p-adischen Regulator $R_p(K)$ eines Zahlkörpers K ein. Das Nichtverschwinden von $L_p(1,\chi)$ hängt dann über die Leopoldtsche p-adische Klassenzahlformel eng mit dem Nichtverschwinden eines p-adischen Regulators zusammen. Die bis heute unbewiesene Leopoldt-Vermutung lautet, dass $R_p(K) \neq 0$ für alle Zahlkörper K gilt. Wir werden die Aussage jedoch für den Fall abelscher Zahlkörper beweisen können.

In einem einfachen Spezialfall können wir $L_p(1,\chi) \neq 0$ sofort mit Hilfe der Kongruenzen aus Abschnitt 7 zeigen.

Proposition 9.1. *Sei p eine reguläre Primzahl und $k \in \mathbb{Z}$ gerade mit $k \not\equiv 0 \pmod{p-1}$. Dann gilt $L_p(1,\omega^k) \not\equiv 0 \pmod{p}$, insbesondere $L_p(1,\omega^k) \neq 0$.*

Beweis. Nach Korollar 7.2 gilt

$$L_p(1,\omega^k) \equiv L_p(1-k,\omega^k) = -(1-p^{k-1})\frac{B_k}{k} \pmod{p}.$$

Da p regulär ist, gilt $p \nmid B_k$, somit ist die rechte Seite $\not\equiv 0 \pmod{p}$. □

Um den allgemeinen Fall zu behandeln, führen wir den p-adischen Regulator ein. Sei K ein algebraischer Zahlkörper. Fixieren wir eine Einbettung $\mathbb{C}_p \hookrightarrow \mathbb{C}$, so liefert jede Einbettung $\sigma : K \hookrightarrow \mathbb{C}_p$ eine Einbettung $K \hookrightarrow \mathbb{C}$, so dass wir σ eine *komplexe* oder *reelle* Einbettung nennen können, je nachdem ob die induzierte Einbettung $K \hookrightarrow \mathbb{C}$ reell oder komplex ist. Seien $\sigma_1, \ldots, \sigma_{r_1}$ die reellen Einbettungen und $\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$ die Paare komplexer Einbettungen. Sei $r := r_1 + r_2 - 1$ der Rang der Einheitengruppe von K gemäß dem Dirichletschen Einheitensatz. Wir setzen ferner $\delta_i := 1$, falls σ_i reell ist, anderenfalls $\delta_i := 2$.

Definition 9.2. Seien $\varepsilon_1, \ldots, \varepsilon_r$ unabhängige Einheiten des Zahlkörpers K. Dann heißt

$$R_{K,p}(\varepsilon_1, \ldots, \varepsilon_r) := \det(\delta_i \log_p(\sigma_i \varepsilon_j))_{1 \leq i,j \leq r}$$

der **p-adische Regulator** von $\varepsilon_1, \ldots, \varepsilon_r$. Ist $\{\varepsilon_1, \ldots, \varepsilon_r\}$ eine Basis der Einheitengruppe von K modulo Einheitswurzeln, so heißt $R_p(K) := R_{K,p}(\varepsilon_1, \ldots, \varepsilon_r)$ der **p-adische Regulator des Zahlkörpers** K.

Der p-adische Regulator ist hierbei nur bis aufs Vorzeichen bestimmt, da die Determinante sich bei anderer Nummerierung der Einheiten ε_j um den Faktor -1 ändern kann.

Außerdem hängt p-adische Regulator von der Nummerierung der Einbettungen σ_i ab, wenn K nicht reell oder ein CM-Körper (eine rein-imaginäre, quadratische Erweiterung eines reellen Zahlkörpers) ist. Wir werden den p-adischen Regulator deshalb nur in diesen Fällen betrachten.

Die Beziehung zwischen dem p-adischen Regulator und dem Nicht-Verschwinden von $L_p(1,\chi)$ beruht auf dem folgenden Satz.

Satz 9.3 (Leopoldtsche p-adische Klassenzahlformel)**.** *Sei K ein total-reeller abelscher Zahlkörper vom Grad n, der zu einer Gruppe X von Dirichlet-Charakteren gehört. Dann gilt*

$$\frac{2^{n-1}h(K)R_p(K)}{\sqrt{d(K)}} = \prod_{\substack{\chi\in X\\ \chi\neq 1}} \left(1-\frac{\chi(p)}{p}\right)^{-1} L_p(1,\chi),$$

wobei $h(K)$ die Klassenzahl und $d(K)$ die Diskriminante von K bezeichnet.

(Da $R_p(K)$ und $\sqrt{d(K)}$ nur bis aufs Vorzeichen bestimmt sind, ist die Formel so zu verstehen, dass bei geeigneter Wahl der Vorzeichen Gleichheit erreicht wird.)

Der Satz soll hier nicht bewiesen werden; ein Beweis wird in Kapitel 8 von [4] gegeben. Wir werden zeigen, dass für abelsche Zahlkörper $R_p(K) \neq 0$ gilt, dann folgt aus der Klassenzahlformel das Nichtverschwinden von $L_p(1,\chi)$ für $\chi \in X$. Zum Beweis benötigen wir zunächst einige Hilfsresultate.

Lemma 9.4. *Sei G eine endliche abelsche Gruppe, F ein Körper der Charakteristik 0 und $f : G \to F$ eine Funktion auf G mit Werten in F. Bezeichne $\hat{G}$ die Charaktergruppe von G. Dann gilt:*

(a) $\det(f(\sigma\tau^{-1}))_{\sigma,\tau\in G} = \prod_{\chi\in\hat{G}} \sum_{\sigma\in G} \chi(\sigma) f(\sigma)$.

(b) $\det(f(\sigma\tau^{-1}) - f(\sigma))_{\sigma,\tau\neq 1} = \prod_{\chi\neq 1} \sum_{\sigma\in G} \chi(\sigma) f(\sigma)$.

(c) Falls $\sum_\sigma f(\sigma) = 0$*, so gilt* $\det(f(\sigma\tau^{-1}))_{\sigma,\tau\neq 1} = |G|^{-1} \prod_{\chi\neq 1} \sum_{\sigma\in G} \chi(\sigma) f(\sigma)$.

Beweis. (a) Wir können ohne Einschränkung annehmen, dass F algebraisch abgeschlossen ist, also $\hat{G} = \mathrm{Hom}(G, F^\times)$. Sei V der F-Vektorraum der F-wertigen Funktionen auf G. Es operiert G auf V durch Translation: $(\sigma h)(X) := h(\sigma X)$. Wir definieren die lineare Transformation $T = \sum_\sigma f(\sigma)\sigma$. Ferner sei $\phi_\tau \in V$ die charakteristische Funktion von τ, d. h.

$$\phi_\tau(\sigma) = \begin{cases} 1 & \text{für } \sigma = \tau, \\ 0 & \text{für } \sigma \neq \tau. \end{cases}$$

Die charakteristischen Funktionen $\{\phi_\tau\}_{\tau\in G}$ bilden offenbar eine Basis von V. Es gilt

$$\begin{aligned} T\phi_\tau(X) &= \sum_\sigma f(\sigma)\phi_\tau(\sigma X) \\ &= \sum_\sigma f(\sigma)\phi_{\sigma^{-1}\tau}(X) \\ &= \sum_\sigma f(\tau\sigma^{-1})\phi_\sigma(X), \end{aligned}$$

somit ist $(f(\tau\sigma^{-1}))_{\sigma,\tau\in G}$ die Darstellungsmatrix für T bezüglich dieser Basis und es gilt

$$\det T = \det\left(f(\tau\sigma^{-1})\right)_{\sigma,\tau\in G} = \det\left(f(\sigma\tau^{-1})\right)_{\sigma,\tau\in G}.$$

Die Charaktere $\chi \in \hat{G}$ sind nach einem Satz von Artin linear unabhängig und bilden wegen $|\hat{G}| = |G| = \dim V$ ebenfalls eine Basis von V. Für $\chi \in \hat{G}$ gilt

$$T\chi(X) = \sum_\sigma f(\sigma)\chi(\sigma X) = \left(\sum_\sigma f(\sigma)\chi(\sigma)\right)\chi(X),$$

d. h. χ ist ein Eigenvektor von T zum Eigenwert $\sum_\sigma f(\sigma)\chi(\sigma)$. Bezüglich der Basis $\{\chi\}_{\chi\in\hat{G}}$ wird T durch eine Diagonalmatrix mit Einträgen $\sum_\sigma f(\sigma)\chi(\sigma)$ auf der Diagonalen dargestellt. Es folgt

$$\det T = \prod_{\chi\in\hat{G}} \sum_\sigma f(\sigma)\chi(\sigma),$$

was die erste Behauptung zeigt.

(b) Sei $W \subset V$ der $(|G|-1)$-dimensionale Unterraum der Funktionen $h : G \to F$ mit $\sum_\sigma h(\sigma) = 0$. Für $\tau \in G$ sei $\psi_\tau(X) := \phi_\tau(X) - \frac{1}{|G|}$. Die Funktionen $\psi_\tau \in W$ erzeugen W, denn für $h \in W$ gilt

$$h = \sum_\tau h(\tau)\phi_\tau = \sum_\tau h(\tau)\phi_\tau - \frac{1}{|G|}\sum_\tau h(\tau) = \sum_\tau h(\tau)\psi_\tau.$$

Wegen $\sum_\tau \psi_\tau = \sum_\tau \phi_\tau - \sum_\tau \frac{1}{|G|} = 1 - 1 = 0$ bilden die $|G|-1$ Funktionen $\{\psi_\tau\}_{\tau\neq 1}$ eine Basis von W. Es gilt

$$\begin{aligned} T\psi_\tau(X) &= \sum_\sigma f(\sigma)\psi_\tau(\sigma X) \\ &= \sum_\sigma f(\tau\sigma^{-1})\psi_\sigma(X) \\ &= \sum_{\sigma\neq 1} f(\tau\sigma^{-1})\psi_\sigma(X) + f(\tau)\psi_1(X) \\ &= \sum_{\sigma\neq 1} \big(f(\tau\sigma^{-1}) - f(\tau)\big)\,\psi_\sigma(X), \end{aligned}$$

d. h. $T|_W$ hat bezüglich $\{\psi_\tau\}_{\tau\neq 1}$ die Darstellungsmatrix $(f(\tau\sigma^{-1}) - f(\tau))_{\sigma,\tau\neq 1}$ mit Determinante

$$\det T|_W = \det\ \big(f(\tau\sigma^{-1}) - f(\tau)\big)_{\sigma,\tau\neq 1} = \det\ \big(f(\sigma\tau^{-1}) - f(\sigma)\big)_{\sigma,\tau\neq 1}.$$

Ist $1 \neq \chi \in \hat{G}$ ein Charakter mit $\chi(\tau) \neq 1$, so gilt

$$(1-\chi(\tau))\sum_\sigma \chi(\sigma) = \sum_\sigma \chi(\sigma) - \sum_\sigma \chi(\tau\sigma) = 0,$$

also $\sum_\sigma \chi(\sigma) = 0$. Die $|G| - 1$ linear unabhängigen Charaktere $\{\chi\}_{\chi \neq 1}$ bilden somit eine Basis von W. Wie in (a) sind die $\chi \neq 1$ Eigenvektoren von T, es folgt

$$\det T|_W = \prod_{\chi \neq 1} \sum_\sigma f(\sigma)\chi(\sigma).$$

(c) Nach (b) ist $\prod_{\chi\neq 1} \sum_\sigma f(\sigma)\chi(\sigma)$ die Determinante von

$$\left(\begin{array}{c|cc} 1 & 0 & \dots \\ \hline f(\sigma) & f(\sigma\tau^{-1}) - f(\sigma) & \cdots \\ \vdots & \vdots & \ddots \end{array}\right).$$

Addieren wir die erste Spalte auf die übrigen, ergibt sich die Matrix

$$\left(\begin{array}{c|cc} 1 & 1 & \dots \\ \hline f(\sigma) & f(\sigma\tau^{-1}) & \cdots \\ \vdots & \vdots & \ddots \end{array}\right).$$

Nun addieren wir alle übrigen Spalten zur ersten und erhalten

$$\left(\begin{array}{c|cc} |G| & 1 & \dots \\ \hline 0 & f(\sigma\tau^{-1}) & \cdots \\ \vdots & \vdots & \ddots \end{array}\right)$$

unter Benutzung von $\sum_\tau f(\sigma\tau^{-1}) = \sum_\tau f(\tau) = 0$. Da die Determinante invariant unter den Spaltenoperationen ist, folgt

$$\prod_{\chi\neq 1} \sum_{\sigma\in G} f(\sigma)\chi(\sigma) = |G| \det\left(f(\sigma\tau^{-1})\right)_{\sigma,\tau\neq 1}.$$

□

Lemma 9.5. *Sei (a_{ij}) eine quadratische Matrix mit reellen Einträgen. Es gelte*

(i) $a_{ii} > 0$ *für alle* i,

(ii) $a_{ij} \leq 0$ *für* $i \neq j$,

(iii) $\sum_i a_{ij} > 0$ *für alle* j.

Dann gilt $\det(a_{ij}) \neq 0$.

Beweis. Angenommen, die Matrix ist singulär. Dann existiert ein Vektor $x = (x_i) \neq 0$ mit $\sum_i a_{ij}x_i = 0$ für alle j. Sei $|x_k|$ maximal unter den Einträgen von x. Ohne Einschränkung sei $x_k > 0$, anderenfalls betrachten wir $-x$ anstelle von x. Es gilt dann $x_k \geq x_i$ für alle i und es folgt

$$0 = \sum_i \underbrace{a_{ik}}_{\leq 0\ (i\neq k)} \underbrace{x_i}_{\leq x_k} \geq \underbrace{\left(\sum_i a_{ik}\right)}_{>0} \underbrace{x_k}_{>0} > 0,$$

Widerspruch! Also muss $\det(a_{ij}) \neq 0$ gelten. □

Lemma 9.6. *Sei $K/\mathbb{Q}$ eine endliche Galoiserweiterung, welche als Teilkörper von $\mathbb{C}$ aufgefasst sei. Wenn K reell ist, seien $\sigma_1, \ldots, \sigma_{r+1}$ die Elemente der Galoisgruppe $\mathrm{Gal}(K/\mathbb{Q})$, anderenfalls $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_{r+1}, \overline{\sigma_{r+1}}$. Dann existiert eine Einheit ε von K, so dass die Einheiten $\{\varepsilon^{\sigma_i} \mid 1 \leq i \leq r\}$ multiplikativ unabhängig sind, also nach dem Dirichletschen Einheitensatz eine Untergruppe von endlichem Index in der Einheitengruppe von K erzeugen. Eine solche Einheit heißt* ***Minkowski-Einheit****.*

Beweis. Wir zeigen, dass eine Einheit ε existiert mit $|\varepsilon^{\sigma_1}| > 1$ und $|\varepsilon^{\sigma_i}| < 1$ für $i \neq 1$ (wobei $|\cdot|$ der archimedische Absolutbetrag auf $\mathbb{C}$ ist). Bezeichne E die Gruppe der Einheiten des Zahlkörpers K und sei $\Gamma \subset \mathbb{R}^r$ das Bild der Abbildung

$$l : E \to \mathbb{R}^r,\ \eta \mapsto (\log|\eta^{\sigma_2}|, \ldots, \log|\eta^{\sigma_{r+1}}|)\,.$$

Nach der multiplikativen Minkowski-Theorie (siehe Kapitel I.5 in [3]) ist Γ ein vollständiges Gitter in $\mathbb{R}^r$. Insbesondere liegt ein Gitterpunkt von Γ im „Quadranten“

$$Q := \{\ (x_2, \ldots, x_{r+1}) \in \mathbb{R}^r \mid x_i < 0 \text{ für } 2 \leq i \leq r+1\ \},$$

d. h. es existiert ein $\varepsilon \in E$ mit $\log|\varepsilon^{\sigma_i}| < 0$ für $2 \leq i \leq r+1$. Wegen

$$1 = |N_{K/\mathbb{Q}}(\varepsilon)| = |\varepsilon^{\sigma_1}| \prod_{i\neq 1} |\varepsilon^{\sigma_i}|$$

und $|\varepsilon^{\sigma_i}| < 1$ für $i \neq 1$ folgt $|\varepsilon^{\sigma_1}| > 1$.

Durch geeignete Nummerierung der σ_i können wir $\sigma_1 = \mathrm{id}$ annehmen. Wir setzen

$$a_{ij} := \delta_i \log|\varepsilon^{\sigma_j\sigma_i^{-1}}|, \quad 1 \leq i, j \leq r+1.$$

Hierbei ist $\delta := \delta_i \in \{1, 2\}$ unabhängig von i, da alle Einbettungen reell oder komplex sind, jenachdem ob der galoissche Zahlkörper K reell oder komplex ist. Die Matrix $(a_{ij})_{1\leq i,j\leq r}$ erfüllt nun die Voraussetzungen von Lemma 9.5:

(i) $a_{ii} = \delta \log|\varepsilon^{\sigma_i\sigma_i^{-1}}| = \delta \log|\varepsilon^{\sigma_1}| > 0$.

(ii) Für $i \neq j$ ist $\sigma_j\sigma_i^{-1} \neq \sigma_1$, somit $a_{ij} = \delta \log|\varepsilon^{\sigma_j\sigma_i^{-1}}| < 0$.

(iii) Für $j = 1, \ldots, r$ gilt $\sum_i a_{ij} = \delta \log \prod_i |\varepsilon^{\sigma_j\sigma_i^{-1}}| = \delta \log|N_{K/\mathbb{Q}}(\varepsilon)| = 0$, damit folgt $\sum_{i=1}^r a_{ij} = -a_{r+1,j} < 0$.

Nach Lemma 9.5 gilt nun

$$R_K(\varepsilon^{\sigma_1}, \ldots, \varepsilon^{\sigma_r}) = |\det(a_{ij})| \neq 0.$$

Die Einheiten $\varepsilon^{\sigma_1}, \ldots, \varepsilon^{\sigma_r}$ müssen daher multiplikativ unabhängig sein, anderenfalls wären die Zeilen der Matrix (a_{ij}) linear abhängig. Die von $\varepsilon^{\sigma_1}, \ldots, \varepsilon^{\sigma_r}$ erzeugte Untergruppe von E hat also den Rang r. Nach dem Dirichletschen Einheitensatz ist der Rang von E ebenfalls r, damit erzeugen die $\varepsilon^{\sigma_1}, \ldots, \varepsilon^{\sigma_r}$ eine Untergruppe von endlichem Index. □

Lemma 9.7. *Sei K ein Zahlkörper und seien $\varepsilon_1, \ldots, \varepsilon_r$ multiplikativ unabhängige Einheiten von K. Fassen wir K bezüglich einer festen Einbettung als Teilkörper von $\mathbb{C}_p$ auf, so sind $\log_p \varepsilon_1, \ldots, \log_p \varepsilon_r$ linear unabhängig über $\mathbb{Q}$.*

Beweis. Gelte $\sum_{i=1}^{r} a_i \log_p \varepsilon_i = 0$ mit $a_i \in \mathbb{Q}$. Durch Multiplikation mit dem Hauptnenner können wir $a_i \in \mathbb{Z}$ erreichen. Es gilt nun

$$\log_p \prod_{i=1}^{r} \varepsilon_i^{a_i} = \sum_{i=1}^{r} a_i \log_p \varepsilon_i = 0.$$

Nach Lemma 5.2 existieren $r \in \mathbb{Q}$ und eine Einheitswurzel ζ mit $\prod_{i=1}^{r} \varepsilon_i^{a_i} = p^r \zeta$. Durch Potenzieren beider Seiten mit der Ordnung von ζ können wir ohne Einschränkung $\zeta = 1$ annehmen. Wiederum durch geeignetes Potenzieren erreichen wir $r \in \mathbb{Z}$. Nun gilt

$$1 = \prod_{i=1}^{r} |N_{K/\mathbb{Q}}(\varepsilon_i)|^{a_i} = N_{K/\mathbb{Q}}(p^r) = p^{[K:\mathbb{Q}]r},$$

es folgt $r = 0$ und somit $\prod_{i=1}^{r} \varepsilon_i^{a_i} = 1$. Da nach Voraussetzung $\varepsilon_1, \ldots, \varepsilon_r$ multiplikativ unabhängig sind, folgt $a_1 = \ldots = a_r = 0$. □

Wir benötigen noch den folgenden Satz von Brumer, das p-adische Analogon eines Satzes von Baker. Für einen Beweis wird auf [1] verwiesen.

Satz 9.8. *Seien $\alpha_1, \ldots, \alpha_n \in \mathbb{C}_p$ algebraisch über $\mathbb{Q}$ und $\log_p(\alpha_1), \ldots, \log_p(\alpha_n)$ $\mathbb{Q}$-linear unabhängig. Dann sind $\log_p(\alpha_1), \ldots, \log_p(\alpha_n)$ sogar linear unabhängig über dem algebraischen Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$ in $\mathbb{C}_p$.*

Mit diesen Vorbereitungen können wir für abelsche Zahlkörper das Nichtverschwinden des p-adischen Regulators beweisen.

Satz 9.9. *Sei K ein abelscher Zahlkörper. Dann gilt $R_p(K) \neq 0$.*

Beweis. Falls K imaginär ist, betrachten wir den maximal reellen Teilkörper K^+. Zwischen $R_p(K)$ und $R_p(K^+)$ besteht die Beziehung

$$R_p(K) = \frac{1}{Q} 2^r R_p(K^+) \quad \text{mit } r = \frac{1}{2}[K:\mathbb{Q}] - 1 \text{ und } Q \in \{1, 2\},$$

so dass das Nichtverschwinden von $R_p(K)$ äquivalent zum Nichtverschwinden von $R_p(K^+)$ ist. (Für den Beweis der Formel siehe Proposition 4.16 in [4].) Wir können also ohne Einschränkung annehmen, dass K reell ist.

Bezüglich einer festen Einbettung $K \hookrightarrow \mathbb{C}_p$ fassen wir K als Teilkörper von $\mathbb{C}_p$ auf. Sei $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_{r+1}\}$ mit $\sigma_1 = \mathrm{id}$ und sei ε eine Minkowski-Einheit gemäß Lemma 9.6. Da G als abelsch vorausgesetzt ist, können wir Lemma 9.4 anwenden und erhalten

$$\begin{aligned} R_p(\varepsilon^{\sigma_2}, \ldots, \varepsilon^{\sigma_{r+1}}) &= \det \left(\log_p \left(\varepsilon^{\sigma_i \sigma_j^{-1}} \right) \right)_{2 \le i,j \le r+1} \\ &= \frac{1}{|G|} \prod_{\substack{\chi \in \hat{G} \\ \chi \neq 1}} \sum_{\sigma} \chi(\sigma) \log_p(\varepsilon^{\sigma}). \end{aligned}$$

Aus $1 = |N_{K/\mathbb{Q}}(\varepsilon)|$ erhalten wir $\log_p \varepsilon^{\sigma_{r+1}} = -\sum_{i=1}^{r} \log_p(\varepsilon^{\sigma_i})$ und somit

$$R_p(\varepsilon^{\sigma_2}, \ldots, \varepsilon^{\sigma_{r+1}}) = \frac{1}{|G|} \prod_{\chi \neq 1} \sum_{i=1}^{r} (\chi(\sigma_i) - \chi(\sigma_{r+1})) \log_p(\varepsilon^{\sigma_i}).$$

Für $\chi \neq 1$ gibt es zumindest ein i mit $\chi(\sigma_i) \neq \chi(\sigma_{r+1})$, d. h. die Faktoren in obigem Produkt sind nicht-triviale Linearkombinationen von $\log_p(\varepsilon^{\sigma_i})$, $1 \le i \le r$. Nun sind $\varepsilon^{\sigma_1}, \ldots, \varepsilon^{\sigma_r}$ nach Wahl von ε multiplikativ unabhängig, so dass nach Lemma 9.7 die Elemente $\log_p(\varepsilon^{\sigma_1}), \ldots, \log_p(\varepsilon^{\sigma_r})$ linear unabhängig über $\mathbb{Q}$ sind. Nach dem Satz 9.8 von Brumer sind sie sogar über $\overline{\mathbb{Q}}$, dem algebraischen Abschluss von $\mathbb{Q}$ in $\mathbb{C}_p$, linear unabhängig. Damit verschwindet keiner der Faktoren in obigem Produkt und wir erhalten $R_p(\varepsilon^{\sigma_2}, \ldots, \varepsilon^{\sigma_{r+1}}) \neq 0$.

Sei E die Einheitengruppe von K und E' die von $\varepsilon^{\sigma_2}, \ldots, \varepsilon^{\sigma_{r+1}}$ und ± 1 erzeugte Untergruppe. Wegen $\prod_{i=1}^{r} \varepsilon^{\sigma_i} = \pm 1$ wird E' auch von $\varepsilon^{\sigma_1}, \ldots, \varepsilon^{\sigma_r}$ erzeugt. Da diese Einheiten multiplikativ unabhängig sind, ist der Index $(E : E')$ endlich. Ist $\eta_1, \ldots, \eta_r$ eine $\mathbb{Z}$-Basis von E modulo ± 1 und T die Übergangsmatrix von $\{\eta_i\}$ zu $\{\pm \varepsilon^{\sigma_i} \mid 2 \le i \le r+1\}$, so gilt $|\det T| = (E : E')$ und

$$\left(\log_p(\varepsilon^{\sigma_j \sigma_i})\right)_{\substack{2 \le i \le r+1 \\ 1 \le j \le r}} = T \cdot \left(\log_p(\eta_i^{\sigma_j})\right)_{1 \le i,j \le r}.$$

Es folgt $R_p(\varepsilon^{\sigma_2}, \ldots, \varepsilon^{\sigma_{r+1}}) = (E : E')\, R_p(K)$ und somit $R_p(K) \neq 0$. □

Korollar 9.10. *Sei $\chi \neq 1$ ein gerader Dirichlet-Charakter. Dann gilt $L_p(1, \chi) \neq 0$.*

Beweis. Ist X die von χ erzeugte Gruppe und K der zu X gehörige Körper, so ist K ein total-reeller abelscher Zahlkörper. Die Behauptung folgt dann direkt aus der p-adischen Klassenzahlformel (Satz 9.3). □

10 Die Leopoldt-Vermutung

Im letzten Abschnitt haben wir gezeigt, dass der p-adische Regulator eines abelschen Zahlkörpers nicht verschwindet. Es ist eine naheliegende Frage, ob dies auch für allgemeine Zahlkörper gilt. Dies ist gerade der Inhalt der Leopoldtschen Vermutung, welche zwar in speziellen Situationen verfiziert, aber bis heute nicht allgemein bewiesen werden konnte.

Leopoldt-Vermutung (vorläufige Formulierung)**.** $R_p(K) \neq 0$ für alle Zahlkörper K.

Im Folgenden werden wir noch eine weitere Version der Leopoldt-Vermutung formulieren und nachweisen, dass sie für total-reelle und für abelsche Zahlkörper mit der oben gegebenen übereinstimmt.

Sei K ein Zahlkörper und p eine fest gewählte Primzahl. Für jedes über p liegende Primideal $\mathfrak{p}$ von K bezeichne $U_\mathfrak{p}$ die Gruppe der lokalen Einheiten von $K_\mathfrak{p}$ und

$$U_\mathfrak{p}^{(n)} = \{\varepsilon \in U_\mathfrak{p} \mid \varepsilon \equiv 1 \pmod{\mathfrak{p}^n}\}$$

die Gruppe der lokalen n-ten Einseinheiten. Für $\mathfrak{p}|p$ ist $U_\mathfrak{p}^{(1)}/U_\mathfrak{p}^{(n+1)} \cong \mathcal{O}_K/\mathfrak{p}^n$ in natürlicher Weise ein $\mathbb{Z}/q^n\mathbb{Z}$-Modul, wobei $q = \mathfrak{N}(\mathfrak{p}) = p^f$ und $f = f(\mathfrak{p}|p)$ der Trägheitsgrad von $\mathfrak{p}|p$ ist. Durch den Übergang zu den projektiven Limiten

$$U_\mathfrak{p}^{(1)} = \varprojlim_n U_\mathfrak{p}^{(1)}/U_\mathfrak{p}^{(n+1)} \quad \text{und} \quad \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/q^n\mathbb{Z}$$

erhält $U_\mathfrak{p}^{(1)}$ eine kanonische $\mathbb{Z}_p$-Modul-Struktur. Für $a \in \mathbb{Z}$ und $\varepsilon \in U_\mathfrak{p}^{(1)}$ hat ε^a die gewöhnliche Bedeutung. Für festes $\varepsilon \in U_\mathfrak{p}^{(1)}$ ist die Abbildung $\mathbb{Z}_p \to U_\mathfrak{p}^{(1)}$, $a \mapsto \varepsilon^a$ stetig, denn die Umgebung $q^n\mathbb{Z}_p$ der Null wird wegen $(U_\mathfrak{p}^{(1)} : U_\mathfrak{p}^{(n+1)}) = q^n$ auf die Umgebung $U_\mathfrak{p}^{(n+1)}$ der Eins abgebildet. Für $a = \lim_{i\to\infty} a_i \in \mathbb{Z}_p$ mit $a_i \in \mathbb{Z}$ gilt somit $\varepsilon^a = \lim_{i\to\infty} \varepsilon^{a_i}$.

Wir definieren

$$U := \prod_{\mathfrak{p}|p} U_\mathfrak{p} \quad \text{und} \quad U^{(1)} := \prod_{\mathfrak{p}|p} U_\mathfrak{p}^{(1)}.$$

Hierbei ist $U^{(1)}$ mit der Produkttopologie versehen und trägt eine kanonische $\mathbb{Z}_p$-Modul-Struktur. Die globale Einheitengruppe E können wir diagonal in U einbetten:

$$\begin{aligned} E &\hookrightarrow U, \\ \varepsilon &\mapsto (\varepsilon, \ldots, \varepsilon). \end{aligned}$$

Sei E_1 die Untergruppe der $\varepsilon \in E$, die in $U^{(1)}$ eingebettet werden. Wegen $U_\mathfrak{p}/U_\mathfrak{p}^{(1)} \cong (\mathcal{O}_K/\mathfrak{p})^\times$ gilt $\varepsilon^{\mathfrak{N}(\mathfrak{p})-1} \in U_\mathfrak{p}^{(1)}$ für alle $\varepsilon \in E$, somit hat E_1 in E endlichen Index. Nach dem Dirichletschen Einheitensatz ist E eine abelsche Gruppe vom Rang $r = r_1 + r_2 - 1$, wobei r_1 die Anzahl der reellen und r_2 die Anzahl der Paare komplexer Einbettungen $K \hookrightarrow \mathbb{C}$ ist. Nach der allgemeinen Theorie der Moduln über Hauptidealringen hat E_1 als Untergruppe von endlichem Index ebenfalls den Rang r. Sei nun $\overline{E_1}$ der topologische Abschluss von E_1 in $U^{(1)}$. Es ist $\overline{E_1}$ ein $\mathbb{Z}_p$-Untermodul von $U^{(1)}$. Was ist sein Rang?

Leopoldt-Vermutung. Der $\mathbb{Z}_p$-Rang von $\overline{E_1}$ ist $r_1 + r_2 - 1$.

Wir beschäftigen uns zuerst mit der einfacheren Ungleichung $\mathbb{Z}_p$-Rang$(\overline{E_1}) \leq r_1+r_2-1$.

Proposition 10.1. $\mathbb{Z}_p$-Rang$(\overline{E_1}) \leq r_1 + r_2 - 1$.

Beweis. Sei $\varepsilon_1, \ldots, \varepsilon_r$ eine $\mathbb{Z}$-Basis von E_1 modulo Torsion. Es genügt zu zeigen, dass $\overline{E_1}$ (modulo Torsion) über $\mathbb{Z}_p$ von $\varepsilon_1, \ldots, \varepsilon_r$ erzeugt wird, also

$$\overline{\langle \varepsilon_1, \ldots, \varepsilon_r \rangle_\mathbb{Z}} = \langle \varepsilon_1, \ldots, \varepsilon_r \rangle_{\mathbb{Z}_p}.$$

Die Inklusionen $\langle \varepsilon_1, \ldots, \varepsilon_r \rangle_\mathbb{Z} \subseteq \langle \varepsilon_1, \ldots, \varepsilon_r \rangle_{\mathbb{Z}_p}$ und $\langle \varepsilon_1, \ldots, \varepsilon_r \rangle_{\mathbb{Z}_p} \subseteq \overline{\langle \varepsilon_1, \ldots, \varepsilon_r \rangle_\mathbb{Z}}$ sind klar, daher genügt es zu zeigen, dass $\langle \varepsilon_1, \ldots, \varepsilon_r \rangle_{\mathbb{Z}_p}$ in $U^{(1)}$ abgeschlossen ist. Offenbar ist $\langle \varepsilon_1, \ldots, \varepsilon_r \rangle_{\mathbb{Z}_p}$ das Bild des Homomorphismus

$$\begin{aligned} \mathbb{Z}_p^r &\to U^{(1)}, \\ (a_1, \ldots, a_r) &\mapsto \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}. \end{aligned}$$

Da die Abbildungen $\mathbb{Z}_p \to U_\mathfrak{p}^{(1)}$, $a \mapsto \varepsilon_i^a$ für alle $\mathfrak{p}|p$ und $1 \leq i \leq r$ stetig sind, ist obige Abbildung als Produkt von stetigen Abbildungen wieder stetig. Da $\mathbb{Z}_p^r$ kompakt ist, ist das Bild $\langle \varepsilon_1, \ldots, \varepsilon_r \rangle_{\mathbb{Z}_p}$ ebenfalls kompakt und somit abgeschlossen. □

Bemerkung. Folgendes Beispiel zeigt, dass Elemente eines $\mathbb{Z}_p$-Moduls, die über $\mathbb{Z}$ unabhängig sind, durchaus über $\mathbb{Z}_p$ abhängig sein können: Die von 7 und 13 erzeugte Untergruppe von $\mathbb{Q}_3^\times$ hat über $\mathbb{Z}$ den Rang 2. Allerdings gilt nach Lemma 5.1

$$\left| \frac{\log_3 13}{\log_3 7} \right| = \frac{|12|}{|6|} = |6| < 1,$$

also $\log_3 13 / \log_3 7 \in \mathbb{Z}_3$. Wegen $13 = 7^{\log_3 13/\log_3 7}$ wird der Abschluss der Gruppe über $\mathbb{Z}_3$ allein von 7 erzeugt, hat also den $\mathbb{Z}_3$-Rang 1.

Wir weisen nun nach, dass die zweite Formulierung der Leopoldtschen Vermutung mit der anfangs gegebenen übereinstimmt, wenn K ein total reeller Zahlkörper ist.

Satz 10.2. *Sei K ein total-reeller Zahlkörper. Dann gilt $R_p(K) \neq 0$ genau dann, wenn der $\mathbb{Z}_p$-Rang von $\overline{E_1}$ gleich $r_1 - 1$ ist.*

Beweis. Angenommen, es gilt $\mathbb{Z}_p$-Rang$(\overline{E_1}) < r_1 - 1$. Sei $\varepsilon_1, \ldots, \varepsilon_r$ eine $\mathbb{Z}$-Basis von E_1 modulo Einheitswurzeln, dann sind $\varepsilon_1, \ldots, \varepsilon_r$ $\mathbb{Z}_p$-abhängig in $U^{(1)}$, etwa

$$\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} = 1 \quad \text{mit } a_i \in \mathbb{Z}_p, \text{ nicht alle } a_i = 0.$$

Da $\mathbb{Z}$ dicht in $\mathbb{Z}_p$ liegt, existiert für alle i eine Folge $(a_{i,n})$ in $\mathbb{Z}$ mit $\lim_{n\to\infty} a_{i,n} = a_i$. Es gilt dann

$$\lim_{n\to\infty} \varepsilon_1^{a_{1,n}} \cdots \varepsilon_r^{a_{r,n}} = 1 \quad \text{in } K_\mathfrak{p} \text{ für alle } \mathfrak{p}|p.$$

Sei L die normale Hülle von $K/\mathbb{Q}$, welche wir als Teilkörper von $\mathbb{C}_p$ auffassen wollen. Sei $\mathfrak{p}_0|p$ ein festes Primideal von K und $\mathfrak{P}_0|\mathfrak{p}_0$ ein festes über $\mathfrak{p}_0$ liegendes Primideal von L. Sei ferner $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, $\mathfrak{P} := \sigma^{-1}\mathfrak{P}_0$ und $\mathfrak{p} := \mathfrak{P} \cap K$. Dann ist $\mathfrak{p}$ ein über p liegendes Primideal von K, also gilt $\lim_{n\to\infty} \varepsilon_1^{a_{1,n}} \cdots \varepsilon_r^{a_{r,n}} = 1$ in $K_\mathfrak{p}$ und somit auch in $L_\mathfrak{P}$:

$$\left|\varepsilon_1^{a_{1,n}} \cdots \varepsilon_r^{a_{r,n}} - 1\right|_\mathfrak{P} \longrightarrow 0 \quad (n \to \infty).$$

Für $x \in L$ gilt offenbar $|\sigma x|_{\sigma\mathfrak{P}} = |x|_\mathfrak{P}$, somit folgt

$$|(\sigma\varepsilon_1)^{a_{1,n}} \cdots (\sigma\varepsilon_r)^{a_{r,n}} - 1|_{\mathfrak{P}_0} \longrightarrow 0 \quad (n \to \infty),$$

d. h. $(\sigma\varepsilon_1)^{a_1} \cdots (\sigma\varepsilon_r)^{a_r} = 1$ in $L_{\mathfrak{P}_0}$. Wir erhalten

$$\sum_{j=1}^{r} a_j \log_p(\sigma\varepsilon_j) = 0 \quad \text{für alle } \sigma \in \mathrm{Gal}(L/\mathbb{Q}).$$

Da die Einbettungen $\sigma_1, \ldots, \sigma_{r+1} : K \hookrightarrow \mathbb{C}_p$ durch Einschränkung der Automorphismen $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ entstehen, sind die Zeilen der Regulatormatrix $\big(\log_p(\sigma_i\varepsilon_j)\big)_{1\le i,j\le r}$ über $\mathbb{Z}_p$ linear abhängig und es folgt $R_p(K) = 0$.

Für die Umkehrung nehmen wir an, es gilt $R_p(K) = 0$. Da die Einträge der Regulatormatrix in L liegen, sind die Zeilen L-linear abhängig, d. h. es existieren $a_1, \ldots, a_r \in L$, nicht alle Null, mit

$$\sum_{j=1}^{r} a_j \log_p(\sigma_i\varepsilon_j) = 0 \quad \text{für } i = 1, \ldots, r.$$

Wegen $\sum_{i=1}^{r+1} \log_p(\sigma_i\varepsilon_j) = 0$ für alle j gilt dies auch für $i = r+1$, also

$$\sum_{j=1}^{r} a_j \log_p(\sigma\varepsilon_j) = 0 \quad \text{für alle } \sigma \in \mathrm{Gal}(L/\mathbb{Q}).$$

Ohne Einschränkung können wir annehmen, dass ein $a_j = 1$ ist. Wir wollen nun zeigen, dass die a_j in $\mathbb{Z}_p$ gewählt werden können. Nach der allgemeinen Theorie der Bewertungen (siehe Kapitel II.9 in [3]) ist $L_{\mathfrak{P}_0}/\mathbb{Q}_p$ eine galoissche Erweiterung mit einer zur Zerlegungsgruppe $\mathrm{Gal}(L/\mathbb{Q})_{\mathfrak{P}_0}$ isomorphen Galoisgruppe. Für jeden Automorphismus $\tau \in \mathrm{Gal}(L_{\mathfrak{P}_0}/\mathbb{Q}_p)$ gilt

$$0 = \tau\left(\sum_{j=1}^{r} a_j \log_p(\sigma\varepsilon_j)\right) = \sum_{j=1}^{r} \tau(a_j) \log_p(\tau\sigma\varepsilon_j) \quad \text{für alle } \sigma \in \mathrm{Gal}(L/\mathbb{Q}).$$

Da $L/\mathbb{Q}$ normal ist, ist mit $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ auch $\tau \circ \sigma$ ein Element von $\mathrm{Gal}(L/\mathbb{Q})$, d. h. τ permutiert die σ. Es gilt folglich

$$\sum_{j=1}^{r} \tau(a_j) \log_p(\sigma\varepsilon_j) = 0 \quad \text{für alle } \sigma \in \mathrm{Gal}(L/\mathbb{Q}).$$

Bezeichne nun Tr die Spur von $L_{\mathfrak{P}_0}/\mathbb{Q}_p$, dann gilt

$$\sum_{j=1}^{r} \mathrm{Tr}(a_j) \log_p(\sigma\varepsilon_j) = \sum_{j=1}^{r} \sum_{\tau} \tau(a_j) \log_p(\sigma\varepsilon_j) = 0 \quad \text{für alle } \sigma \in \mathrm{Gal}(L/\mathbb{Q}).$$

Da ein $a_j = 1$ ist, ist zumindest ein $\mathrm{Tr}(a_j) \neq 0$. Auf diese Weise haben wir nichttriviale Relationen $\sum_{j=1}^{r} a_j \log_p(\sigma\varepsilon_j) = 0$ mit Koeffizienten $a_j \in \mathbb{Q}_p$ gefunden. Nach Multiplikation mit dem Hauptnenner können wir sogar $a_j \in \mathbb{Z}_p$ erreichen. Wie im Beweis von Lemma 9.7 erhalten wir nichttriviale Relationen

$$\prod_{j=1}^{r} (\sigma\varepsilon_j)^{a_j} = 1 \quad \text{für alle } \sigma \in \mathrm{Gal}(L/\mathbb{Q}).$$

Für jedes Primideal $\mathfrak{p}|p$ von K finden wir ein über $\mathfrak{p}$ liegendes Primideal $\mathfrak{P}$ von L und ein $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ mit $\sigma^{-1}\mathfrak{P} = \mathfrak{P}_0$, da die Galoisgruppe transitiv auf den über p liegenden Primidealen von L operiert. Mit der gleichen Argumentation wie in der ersten Implikation erhalten wir

$$\prod_{j=1}^{r} \varepsilon_j^{a_j} = 1 \quad \text{in } K_{\mathfrak{p}}$$

und, da $\mathfrak{p}|p$ beliebig war, $\prod_{j=1}^{r} \varepsilon_j^{a_j} = 1$ in $U^{(1)}$. Die Einheiten $\varepsilon_1, \ldots, \varepsilon_r$ sind also in $U^{(1)}$ über $\mathbb{Z}_p$ abhängig. Da aber $\overline{E_1}$ (modulo Torsion) über $\mathbb{Z}_p$ von den ε_j erzeugt wird, gilt $\mathbb{Z}_p\text{-Rang}(\overline{E_1}) < r$. □

Korollar 10.3. *Sei K ein abelscher Zahlkörper. Dann gilt $\mathbb{Z}_p\text{-Rang}(\overline{E_1}) = r_1 + r_2 - 1$.*

Beweis. Nach Satz 9.9 gilt $R_p(K) \neq 0$. Ist K reell, so folgt die Behauptung aus dem eben gezeigten Satz 10.2. Ist K imaginär, so gilt die Behauptung zunächst für den maximal reellen Teilkörper K^+. Wegen

$$r_1(K^+) = [K^+ : \mathbb{Q}] = \frac{1}{2}[K : \mathbb{Q}] = r_2(K)$$

stimmt die Größe $r_1 + r_2 - 1$ für K und K^+ überein (man beachte: K ist rein-imaginär und K^+ total-reell). Nun ist $\overline{E_1^+}$ ein $\mathbb{Z}_p$-Untermodul von $\overline{E_1}$, daher ist der $\mathbb{Z}_p$-Rang von $\overline{E_1}$ mindestens $r_1 + r_2 - 1$. Mit Proposition 10.1 folgt die Gleichheit. □

Literaturverzeichnis

[1] Brumer, Armand: *On the units of algebraic number fields.* Mathematika, 14:121–124, 1967.

[2] H.W. Leopoldt, T. Kubota: *Eine p-adische Theorie der Zetawerte. Einführung der p-adischen Dirichletschen L-Funktionen.* Journal für die reine und angewandte Mathematik, 1964.

[3] Neukirch, Jürgen: *Algebraische Zahlentheorie.* Springer-Verlag Berlin Heidelberg, 2006.

[4] Washington, L.C.: *Introduction to Cyclotomic Fields.* Graduate texts in mathematics. Springer, 1997.

Selbstständigkeitserklärung

Der Verfasser erklärt an Eides statt, dass er die vorliegende Arbeit selbständig, ohne fremde Hilfe und ohne Benutzung anderer als die angegebenen Hilfsmittel angefertigt hat. Die aus fremden Quellen (einschließlich elektronischer Quellen) direkt oder indirekt übernommenen Gedanken sind ausnahmslos als solche kenntlich gemacht. Die Arbeit ist in gleicher oder ähnlicher Form oder auszugsweise im Rahmen einer anderen Prüfung noch nicht vorgelegt worden.

Heidelberg, den 3. Juli 2012