Arithmetik nichtabelscher partieller Zetawerte

Diplomarbeit von
Thomas Bliem

Betreut durch
Prof. Dr. C.-G. Schmidt
Mathematisches Institut II
Universität Karlsruhe (TH)

10. Januar 2005

Inhaltsverzeichnis

Einleitung

Der Ausgangspunkt dieser Untersuchung ist eine Folge von Distributionen auf $\mathbf{Z}_p$, die in drei verschiedenen Darstellungen auftritt: Als *Bernoullidistributionen* E_k werden die Glieder der Folge durch die Bernoullipolynome definiert. Als *Hurwitzdistributionen* H_k hängen sie mit speziellen Werten der Hurwitz'schen Zetafunktion zusammen. Als *Standarddistributionen* $L_{\{p\},k}$ erhält man sie als Fouriertransformierte spezieller Werte Dirichlet'scher L-Reihen. (In Satz 2.6 und Korollar 2.15 weise ich nach, dass dies tatsächlich drei verschiedene Ausprägungen der selben Sache sind.)

T. Kubota und H. W. Leopoldt schlossen die Untersuchungen dieser Folge von Distributionen mit ihrer 1964 erschienenen Arbeit [7] ab. Zusammenfassend weiß man Folgendes:

(i) Die Distributionen sind über die Gleichung $E_k(da) = a^{k-1}E_1(da)$ verbunden.

(ii) Sie nehmen nur rationale Werte an.

(iii) Ihre Werte gehorchen strengen Kongruenzbedingungen.

(iv) Diese erlauben es, die Distributionen so zu modifizieren, dass sie ganz bezüglich p werden.

(v) Mit ihrer Hilfe kann man eine p-adisch analytische Funktion konstruieren, die spezielle Werte Dirichlet'scher L-Reihen interpoliert.

Betrachtet man die Interpretation als $L_{\{p\},k}$ genauer, so erkennt man, dass die untersuchte Folge von Distributionen eng mit dem Körper $\mathbf{Q}$ der rationalen Zahlen und der Familie $(\mathbf{Q}(\mu_{p^n}))_{n\in\mathbf{N}}$ von Kreisteilungskörpern zusammenhängt. Es ergeben sich zwei Richtungen möglicher Verallgemeinerung, für die man ebenfalls das obige Programm (i) bis (v) durchführen möchte:

Einerseits kann man den Körper $\mathbf{Q}$ durch andere algebraische Zahlkörper ersetzen, die Familie von Erweiterungskörpern aber beibehalten (genauer: durch eine entsprechende Familie abelscher Erweiterungen ersetzen). Diese Verallgemeinerung gelang Ende der 1970er Jahre P. Deligne und A. Ribet [4], P. Cassou-Noguès [3] und D. Barsky [1].

Andererseits kann man am Grundkörper $\mathbf{Q}$ festhalten, jedoch den darüberliegenden Körperturm erweitern, so dass insbesondere auch über $\mathbf{Q}$ nichtabelsche Körper enthalten sind. Diesen Weg wollen wir hier beschreiten.

Danksagungen

Ich danke Prof. Dr. C.-G. Schmidt für viele interessante Gespräche über das Thema. Außerdem danke ich Dr. Stefan Kühnlein und Hendrik Kasten für einige Gespräche und nützliche Literaturhinweise.

Bezeichnungen

$\mathbf{N}$ bezeichne die Menge $\{1, 2, 3, \ldots\}$. In einer Summe $\sum_{\chi \,\mathrm{von}\, G}$ durchlaufe χ die irreduziblen Charaktere der Gruppe G. In einer Summe $\sum_{a \,\mathrm{rep.}\, G/H}$ durchlaufe a ein beliebiges Vertretersystem von G/H. Linksoperationen einer Gruppe werden gelegentlich in Potenzschreibweise notiert, in diesem Fall muss man $(a^\sigma)^\tau = a^{\tau\sigma}$ beachten. Mit *Charakteren* einer Gruppe sind stets effektive Charaktere gemeint, das heißt solche der Form $\chi = \mathrm{tr} \circ \rho$ für eine komplexe Darstellung ρ. *Virtuelle Charaktere* sind $\mathbf{Z}$-Linearkombinationen von Charakteren. Homomorphismen $G \to \mathbf{C}^*$ bezeichne ich stets explizit als *eindimensionale Charaktere*.

Kapitel 1

Einige Eigenschaften Artin'scher L-Funktionen

Die folgenden Überlegungen bilden den Kern des Beweises der Rationalität der Standarddistributionen (Satz 2.17). Sie sind in einem eigenen Kapitel zusammengefasst, da sie im Gegensatz zum Rest der Arbeit nicht die Sprache der Distributionen und Maße voraussetzen.

1.1 Grundlagen

Sei $L|K$ eine galoissche Erweiterung algebraischer Zahlkörper. Wir betrachten eine komplexe Darstellung $\rho : G(L|K) \to \mathrm{GL}_n(\mathbf{C})$ der Galoisgruppe. Sei $\chi := \mathrm{tr} \circ \rho$ der zugehörende Charakter, V der zugehörende $\mathbf{C}[G(L|K)]$-Modul. Sei S eine endliche Menge von Primidealen von K. Die Artin'sche L-Funktion zu dieser Darstellung ohne die zu Primidealen aus S gehörenden Eulerfaktoren bezeichnen wir je nach Situation mit

$$\mathcal{L}_S(L|K, \rho, s) = \mathcal{L}_S(L|K, \chi, s) = \mathcal{L}_S(L|K, V, s).$$

Ist $S = \emptyset$, so wird es häufig von der Notation ausgenommen,

$$\mathcal{L}(L|K, \rho, s) := \mathcal{L}_\emptyset(L|K, \rho, s) \text{ etc.}$$

Warnung. Im Gegensatz zur in manchen Büchern üblichen Schreibweise sind Eulerfaktoren zu unendlichen Primstellen (Gammafaktoren) stets ausgeschlossen, ohne dass die entsprechenden Primstellen in S auftauchen.

Die folgenden fundamentalen Eigenschaften Artin'scher L-Reihen zeigt Neukirch für $S = \emptyset$ in [12], Kap. VII, Sa. 10.4; der Beweis behandelt jedoch die einzelnen Eulerfaktoren getrennt, so dass er auch für $S \neq \emptyset$ gilt. Die Abbildung $\chi \mapsto \mathcal{L}_S(L|K, \chi, s)$ ist ein Homomorphismus der additiven Halbgruppe der Charaktere von $G(L|K)$ in die Multiplikativgruppe $\mathcal{M}(\mathbf{C})^*$ des

Körpers der meromorphen Funktionen auf $\mathbf{C}$. Man kann diesen kanonisch auf die Gruppe aller virtuellen Charaktere fortsetzen. Ist $L'|K$ eine weitere endliche galoissche Erweiterung mit $L \subseteq L'$, so induziert ρ eine Darstellung von $G(L'|K)$. Für die zugehörenden L-Funktionen gilt dann

$$\mathcal{L}_S(L'|K, \rho, s) = \mathcal{L}_S(L|K, \rho, s). \tag{1.1}$$

Man könnte daher auch den Körper L von der Notation ausnehmen und für eine Darstellung ρ der absoluten Galoisgruppe G_K, die über einen endlichen Quotienten faktorisiert, die L-Funktion $\mathcal{L}_S(K, \rho, s)$ definieren. Wir werden dennoch die traditionelle Bezeichnung bevorzugen und stets einen Körper L angeben, über dem sich die betrachtete Darstellung definieren lässt. Ebenso induziert für $L|M|K$ jeder Charakter ψ von $G(L|M)$ einen Charakter ψ_* von $G(L|K)$, und es gilt

$$\mathcal{L}_{\tilde{S}}(L|M, \psi, s) = \mathcal{L}_S(L|K, \psi_*, s), \tag{1.2}$$

für $\tilde{S} := \{\mathfrak{P} \text{ von } M : \mathfrak{P}|\mathfrak{p} \text{ für ein } \mathfrak{p} \in S\}$. Für den Charakter 1 zur trivialen Darstellung von $G(L|K)$ und $S = \emptyset$ erhält man gerade die Dedekind'sche Zetafunktion zum Körper K,

$$\mathcal{L}(L|K, 1, s) = \zeta_K(s).$$

1.2 Transformationsverhalten spezieller L-Werte unter $\mathrm{Aut}(\mathbf{C})$-Operation

Wir untersuchen in diesem Paragraphen, wie sich Körperautomorphismen von $\mathbf{C}$ auf spezielle Werte Artin'scher L-Reihen auswirken (siehe Satz 1.8). Wir betrachten dabei die Stellen $s = 1 - k$ für $k \in \mathbf{N}$. Betrachtet man insbesondere $s = 0$, so erhält man einen Spezialfall der Vermutung von Stark, die Tate in [15], ch. III, th. 1.2 zeigt. Die folgenden Überlegungen sollte man als Verallgemeinerungen dieses Satzes verstehen. Der Beweis ähnelt für ungerade k stark dem bei Tate vorgestellten, für gerade k muss man etwas anders vorgehen.

Sei zunächst G eine beliebige endliche Gruppe. Die Gruppe $\mathrm{Aut}(\mathbf{C})$ operiert von links auf der Menge der komplexwertigen Klassenfunktionen von G durch

$$\chi^\alpha := \alpha \circ \chi.$$

Lemma 1.1. *Die Operation von* $\mathrm{Aut}(\mathbf{C})$ *auf der Menge der Klassenfunktionen von G erfüllt:*

(i) Die Mengen der virtuellen Charaktere und der Charaktere sind invariant.

(ii) Für virtuelle Charaktere bleibt die Dimension $\chi(1)$ *erhalten.*

(iii) Für je zwei Klassenfunktionen χ und ψ gilt

$$(\chi + \psi)^\alpha = \chi^\alpha + \psi^\alpha.$$

(iv) Die Menge der irreduziblen Charaktere ist invariant.

Beweis. Wir betrachten die folgende Operation von $\mathrm{Aut}(\mathbf{C})$ auf komplexen G-Moduln: Sei V ein G-Modul und $\alpha \in \mathrm{Aut}(\mathbf{C})$. Dann sei $V^\alpha := V$ als Menge. Die Skalarmultiplikation sei jedoch durch

$$z \cdot_\alpha x := z^{\alpha^{-1}} x := \alpha^{-1}(z)x$$

gegeben. Gruppenelemente sollen auf V^α genauso wie auf V operieren, das heißt

$$\sigma \cdot_\alpha x := \sigma x.$$

Diese Operation ist linear, denn es gilt einerseits

$$\sigma \cdot_\alpha (x_1 + x_2) = \sigma(x_1 + x_2) = \sigma x_1 + \sigma x_2 = \sigma \cdot_\alpha x_1 + \sigma \cdot_\alpha x_1$$

für $\sigma \in G$ und $x_{1/2} \in V$, sowie andererseits

$$\sigma \cdot_\alpha (z \cdot_\alpha x) = \sigma(z^{\alpha^{-1}} x) = z^{\alpha^{-1}}(\sigma x) = z \cdot_\alpha (\sigma \cdot_\alpha x)$$

für $\sigma \in G,\ z \in \mathbf{C}$ und $x \in V$.

Sei nun $(e_1, \dots, e_n)$ eine Basis von V. Wir zeigen, dass (e_i) auch eine Basis von V^α ist: Sei $x \in V$ beliebig. Dann hat x eine Darstellung $x = \sum_i z_i e_i$ mit $z_i \in \mathbf{C}$. Also gilt

$$x = \sum_i z_i e_i = \sum_i (z_i^\alpha)^{\alpha^{-1}} e_i = \sum_i z_i^\alpha \cdot_\alpha e_i,$$

das heißt x ist auch in V^α als Linearkombination der e_i darstellbar. Damit ist (e_i) ein Erzeugendensystem von V^α. Seien nun andererseits $z_i \in \mathbf{C}$ mit $\sum_i z_i \cdot_\alpha e_i = 0$. Dann gilt

$$0 = \sum_i z_i \cdot_\alpha e_i = \sum_i z_i^{\alpha^{-1}} \cdot e_i.$$

Da (e_i) eine Basis von V ist, folgt $z_i^{\alpha^{-1}} = 0$ für alle i. Also ist auch auch $z_i = 0$ für alle i, und (e_i) ist eine Basis von V^α.

Sei (z_{ij}) die Matrix von $\sigma \in G$ bei Operation auf V. Für jedes i gilt also

$$\sigma \cdot_\alpha e_i = \sigma e_i = \sum_j z_{ij} e_j = \sum_j (z_{ij}^\alpha)^{\alpha^{-1}} e_j = \sum_j z_{ij}^\alpha \cdot_\alpha e_j.$$

Die Matrix von σ bei Operation auf V^α ist also (z_{ij}^α). Folglich gilt auch für die Spuren, dass $\mathrm{tr}_{V^\alpha} \sigma = (\mathrm{tr}_V \sigma)^\alpha$.

Die beschriebene Operation von $\mathrm{Aut}(\mathbf{C})$ auf G-Moduln induziert also die gewünschte Operation auf den Charakteren. Daraus folgt die erste Aussage. Die zweite und die dritte Aussage sind offensichtlich. Die vierte Aussage kann man wie folgt einsehen: Nach (i) ist die Menge der Charaktere invariant, nach (iii) die Teilmenge der reduziblen Charaktere. Also ist auch die Differenz dieser Mengen, die Menge der irreduziblen Charaktere, invariant. □

Sei nun H eine Untergruppe von G. Man kann jeder Klassenfunktion ψ auf H die induzierte Klassenfunktion ψ_* auf G wie folgt zuordnen: Zunächst setze man ψ auf G fort durch $\psi(\sigma) := 0$ für $\sigma \notin H$. Dann ist ψ_* durch

$$\psi_*(\sigma) = \frac{1}{|H|} \sum_{\tau \in G} \psi(\tau\sigma\tau^{-1})$$

für $\sigma \in G$ gegeben. Die Operation von $\mathrm{Aut}(\mathbf{C})$ auf der Menge der Klassenfunktionen ist mit der Induktion verträglich:

Lemma 1.2. *Sei H eine Untergruppe der endlichen Gruppe G. Dann gilt für jedes $\alpha \in \mathrm{Aut}(\mathbf{C})$ und jede Klassenfunktion ψ auf H:*

$$(\psi_*)^\alpha = (\psi^\alpha)_*.$$

Beweis. Mit der oben angegebenen expliziten Formel für induzierte Funktionen rechnet man direkt nach:

$$\begin{aligned}\psi_*(\sigma)^\alpha &= \left(\frac{1}{|H|} \sum_{\tau \in G} \psi(\tau\sigma\tau^{-1})\right)^\alpha \\ &= \frac{1}{|H|} \sum_{\tau \in G} \psi^\alpha(\tau\sigma\tau^{-1}) \\ &= (\psi^\alpha)_*(\sigma)\end{aligned}$$

für jedes $\sigma \in H$. □

Sei im Folgenden wieder $L|K$ eine galoissche Erweiterung algebraischer Zahlkörper, $G := G(L|K)$ und S eine endliche Menge von Primidealen von K. Für jeden G-Modul V und jedes $k \in \mathbf{N}$ bezeichne $r_{S,k}(V)$ die Nullstellenordnung der zugehörenden Artin'schen L-Funktion $\mathcal{L}_S(L|K, V, s)$ an der Stelle $s = 1 - k$. Für $S = \emptyset$ kürzen wir die Notation zu $r_k(V) := r_{\emptyset,k}(V)$ ab.

Für jede (endliche oder unendliche) Primstelle $\mathfrak{P}$ von L sei $\varphi_\mathfrak{P}$ ein zugehörender Frobeniusautomorphismus. Für $\mathfrak{P}|\infty$ ist $\varphi_\mathfrak{P}$ eindeutig bestimmt, da unendliche Primstellen stets unverzweigt sind. In diesem Fall sei $V^{\varphi_\mathfrak{P}} := \{x \in V : \rho(\varphi_\mathfrak{P})x = x\}$ sowie $V^{-\varphi_\mathfrak{P}} := \{x \in V : -\rho(\varphi_\mathfrak{P})x = x\}$. Der Vektorraum V zerlegt sich dann in eine direkte Summe $V = V^{\varphi_\mathfrak{P}} \oplus V^{-\varphi_\mathfrak{P}}$, siehe Neukirch, [12], Kap. VII, Beginn von § 12.

Lemma 1.3. *Zu jeder Primstelle $\mathfrak{p}$ von K wähle eine Fortsetzung $\mathfrak{P}|\mathfrak{p}$ von L. Die Nullstellenordnungen $r_{S,k}(V)$ erfüllen dann*

$$r_{S,k}(V) = \begin{cases} -\dim V^G + \sum_{\mathfrak{p}|\infty} \dim V^{\varphi_\mathfrak{P}} + \sum_{\mathfrak{p}\in S} \dim V^{G_\mathfrak{P}} & k = 1, \\ |\{\mathfrak{p} : \mathfrak{p} \textit{ komplex}\}| \cdot \dim V + \sum_{\mathfrak{p} \textit{ reell}} \dim V^{-\varphi_\mathfrak{P}} & k = 2, 4, 6, \ldots, \\ \sum_{\mathfrak{p}|\infty} \dim V^{\varphi_\mathfrak{P}} & k = 3, 5, 7, \ldots \end{cases}$$

Insbesondere ist $r_{S,k}(V)$ für $k \neq 1$ von S unabhängig. Außerdem ist $r_{S,k}(V)$ für alle $k \in \mathbf{N}$ nichtnegativ.

Beweis. Den Fall $k = 1$ zeigt Tate in [15], ch. I, pr. 3.4. Man beachte dabei: Die Menge S ausgeschlossener Eulerfaktoren taucht in Tates Formel nicht explizit auf, ist aber nach Vereinbarung 3.0 stets mitzudenken. Die unendlichen Primstellen werden nicht gesondert behandelt, da sie bei Tate stets in S enthalten sind.

Die übrigen Fälle ($k \geq 2$) berechnet man unter Verwendung der Funktionalgleichung für vollständige Artin'sche L-Reihen mit Berücksichtigung der Nullstellenordnungen fehlender Eulerfaktoren wie folgt:

Sei $\Gamma(s)$ die Gammafunktion,

$$L_\mathbf{C}(s) := 2(2\pi)^{-s}\Gamma(s) \quad \text{und} \quad L_\mathbf{R}(s) := \pi^{-s/2}\Gamma(s/2).$$

Für jedes Primideal $\mathfrak{p}$ von K bezeichne

$$\mathcal{L}_\mathfrak{p}(L|K, \chi, s) := \det(1 - \varphi_\mathfrak{P}(\mathfrak{N}\mathfrak{p})^{-s}|V^{I_\mathfrak{P}})^{-1}$$

den Eulerfaktor zu $\mathfrak{p}$. Für die unendlichen Primstellen $\mathfrak{p}$ seien die Eulerfaktoren durch

$$\mathcal{L}_\mathfrak{p}(L|K, \chi, s) := \begin{cases} L_\mathbf{C}(s)^{\dim V} & \mathfrak{p} \text{ komplex}, \\ L_\mathbf{R}(s)^{\dim V^{\varphi_\mathfrak{P}}} L_\mathbf{R}(s+1)^{\dim V^{-\varphi_\mathfrak{P}}} & \mathfrak{p} \text{ reell} \end{cases}$$

gegeben. Wir betrachten nun die *vollständige Artin'sche L-Reihe* zu V,

$$\Lambda(L|K, \chi, s) := c(\chi)^{s/2} \prod_{\mathfrak{p} \text{ Primstelle}} \mathcal{L}_\mathfrak{p}(L|K, \chi, s),$$

wobei $c(\chi) > 0$ eine geeignete Konstante ist. (Siehe Neukirch, [12], Kap. VII, Def. 12.2.) Die vollständige L-Reihe erfüllt die Funktionalgleichung

$$\Lambda(L|K, \chi, s) = W(\chi)\Lambda(L|K, \bar{\chi}, 1 - s)$$

mit einer Konstanten $W(\chi)$ vom Betrag 1 (Neukirch, [12], Kap. VII, Th. 12.6). Insbesondere erfüllen für alle $s_0 \in \mathbf{C}$ die Nullstellenordnungen in s_0 beziehungsweise $1 - s_0$, dass $v_{s_0}(\Lambda(L|K, \chi, s)) = v_{1-s_0}(\Lambda(L|K, \bar{\chi}, s))$. Setzt man hier konkret $s_0 = 1 - k$ für $k \geq 2$ ein, so erhält man

$$v_{1-k}(\Lambda(L|K, \chi, s)) = v_k(\Lambda(L|K, \bar{\chi}, s)) = 0.$$

Die zweite Gleichheit erhält man dabei wie folgt: Als konvergentes Produkt kann $\mathcal{L}(L|K, \bar{\chi}, s)$ keine Null- oder Polstellen in $\{\mathrm{Re}\, s > 1\}$ haben. Auch die verbliebenen endlich vielen Faktoren der vollständigen Artin'sche L-Reihe zu $\bar{\chi}$ haben dort keine Null- oder Polstellen, da die Gammafunktion keine Null- oder Polstellen in $\{\mathrm{Re}\, s > 0\}$ hat.

Es gilt also mit $S_\infty := \{\mathfrak{p} \text{ von } K : \mathfrak{p}|\infty\}$:

$$\begin{aligned}
0 &= v_{1-k}(\Lambda(L|K, \chi, s)) \\
&= v_{1-k}\left(c(\chi)^{s/2} \cdot \mathcal{L}_S(L|K, \chi, s) \cdot \prod_{\mathfrak{p} \in S \cup S_\infty} \mathcal{L}_\mathfrak{p}(L|K, \chi, s) \right) \\
&= 0 + r_{S,k}(V) + \sum_{\mathfrak{p} \in S \cup S_\infty} v_{1-k}(\mathcal{L}_\mathfrak{p}(L|K, \chi, s)).
\end{aligned}$$

Nach $r_{S,k}(V)$ aufgelöst ergibt sich

$$r_{S,k}(V) = - \sum_{\mathfrak{p} \in S \cup S_\infty} v_{1-k}(\mathcal{L}_\mathfrak{p}(L|K, \chi, s)). \tag{1.3}$$

Das Problem ist also darauf reduziert, die Nullstellenordnung der auf der rechten Seite von (1.3) auftretenden Eulerfaktoren in $s = 1-k$ zu bestimmen.

Sei zunächst $\mathfrak{p} \in S$. Der Frobeniusautomorphismus $\varphi_\mathfrak{P}$ hat (als Element der endlichen Gruppe $G(L|K)$) endliche Ordnung, also sind alle Eigenwerte Einheitswurzeln. Insbesondere haben alle Eigenwerte den Betrag 1. Der zugehörende Eulerfaktor $\det(1 - \varphi_\mathfrak{P}(\mathfrak{N}\mathfrak{p})^{-s}|V^{I_\mathfrak{P}})^{-1}$ kann daher keine Polstelle für $s \in \mathbf{R} \setminus \{0\}$ haben, das heißt $v_{1-k}(\mathcal{L}_\mathfrak{p}(L|K, \chi, s)) = 0$.

Sei nun $\mathfrak{p}$ komplex. Es ist

$$\begin{aligned}
v_{1-k}(\mathcal{L}_\mathfrak{p}(L|K, \chi, s)) &= v_{1-k}(L_\mathbf{C}(s)^{\dim V}) \\
&= \dim V \cdot v_{1-k}(L_\mathbf{C}(s)) \\
&= \dim V \cdot v_{1-k}(2(2\pi)^{-s}\Gamma(s)) \\
&= -\dim V.
\end{aligned}$$

Sei schließlich $\mathfrak{p}$ reell. Es ist

$$\begin{aligned}
v_{1-k}(L_\mathbf{R}(s)) = v_{1-k}(\pi^{-s/2}\Gamma(s/2)) &= v_{1-k}(\Gamma(s/2)) = v_{(1-k)/2}(\Gamma(s)) \\
&= \begin{cases} -1 & (1-k)/2 \text{ ganz, d. h. } k \text{ ungerade,} \\ 0 & \text{sonst.} \end{cases}
\end{aligned}$$

Damit gilt

$$\begin{aligned}
v_{1-k}(\mathcal{L}_\mathfrak{p}(L|K, \chi, s)) &= v_{1-k}(L_\mathbf{R}(s)^{\dim V^{\varphi_\mathfrak{P}}} L_\mathbf{R}(s+1)^{\dim V^{-\varphi_\mathfrak{P}}}) \\
&= \dim V^{\varphi_\mathfrak{P}} \cdot v_{1-k}(L_\mathbf{R}(s)) + \dim V^{-\varphi_\mathfrak{P}} \cdot v_{1-k}(L_\mathbf{R}(s+1))
\end{aligned}$$

$$= \begin{cases} -\dim V^{\varphi_{\mathfrak{P}}} & k \text{ ungerade,} \\ -\dim V^{-\varphi_{\mathfrak{P}}} & k \text{ gerade.} \end{cases}$$

Einsetzen dieser Nullstellenordnungen in Formel (1.3) ergibt nun für gerade k

$$\begin{aligned} r_{S,k}(V) &= -\sum_{\mathfrak{p}\in S\cup S_\infty} v_{1-k}(\mathcal{L}_{\mathfrak{p}}(L|K,\chi,s)) \\ &= \sum_{\mathfrak{p}\text{ komplex}} \dim V + \sum_{\mathfrak{p}\text{ reell}} \dim V^{-\varphi_{\mathfrak{P}}} \\ &= |\{\mathfrak{p} : \mathfrak{p}\text{ komplex}\}| \cdot \dim V + \sum_{\mathfrak{p}\text{ reell}} \dim V^{-\varphi_{\mathfrak{P}}}. \end{aligned}$$

Für ungerade k ergibt sich entsprechend

$$\begin{aligned} r_{S,k}(V) &= -\sum_{\mathfrak{p}\in S\cup S_\infty} v_{1-k}(\mathcal{L}_{\mathfrak{p}}(L|K,\chi,s)) \\ &= \sum_{\mathfrak{p}\text{ komplex}} \dim V + \sum_{\mathfrak{p}\text{ reell}} \dim V^{\varphi_{\mathfrak{P}}} \\ &= \sum_{\mathfrak{p}|\infty} \dim V^{\varphi_{\mathfrak{P}}}. \end{aligned}$$

Der Übergang zur letzten Zeile ist dabei möglich, da für komplexe $\mathfrak{p}$ stets $\varphi_{\mathfrak{P}} = 1$ und daher $V^{\varphi_{\mathfrak{P}}} = V$ gilt. □

Lemma 1.4. *Die Zahlen $r_{S,k}$ sind invariant unter der Operation von* $\mathrm{Aut}(\mathbf{C})$*, das heißt für alle $\alpha \in \mathrm{Aut}(\mathbf{C})$, $k \in \mathbf{N}$ gilt*

$$r_{S,k}(V^\alpha) = r_{S,k}(V).$$

Beweis. Wegen der expliziten Formeln in Lemma 1.3 und da G auf V^α wie auf V operiert, reicht es zu zeigen, dass die Dimension jedes komplexen Vektorraums V invariant unter der Operation von $\mathrm{Aut}(\mathbf{C})$ ist, das heißt

$$\dim V = \dim V^\alpha$$

für alle $\alpha \in \mathrm{Aut}(\mathbf{C})$. Dies ist tatsächlich der Fall, da jede Basis von V auch eine Basis von V^α ist, wie wir im Beweis von Lemma 1.1 gesehen haben. □

Für einen Charakter χ von $G(L|K)$ bezeichne L_χ die minimale Erweiterung von K, über deren Galoisgruppe χ definiert ist, das heißt

$$L_\chi = L^{\ker \rho_\chi}.$$

Ein total imaginärer Zahlkörper heißt ein *CM-Körper*, wenn er eine quadratische Erweiterung eines total reellen Zahlkörpers ist. Ein Zahlkörper ist genau dann ein CM-Körper, wenn auf ihm die komplexe Konjugation einen eindeutigen, das heißt von der Einbettung in $\mathbf{C}$ unabhängigen, nichttrivialen Automorphismus definiert. (Siehe Lang, [8], ch. 1, § 2.)

Der Körper L_χ beeinflusst das Nullstellenverhalten von $\mathcal{L}(L|K, \chi, s)$ wie folgt:

Satz 1.5. *Sei χ ein Charakter von $G(L|K)$.*

(i) Enthält χ nicht den trivialen Charakter als Summanden und ist $r_{S,1}(\chi) = 0$, so ist K total reell und L_χ ein CM-Körper.

(ii) Ist $k \in \{3, 5, 7, \ldots\}$ und $r_{S,k}(\chi) = 0$, so ist K total reell und L_χ ein CM-Körper.

(iii) Für gerade k ist $r_{S,k}(\chi) = 0$ genau dann, wenn L_χ total reell ist.

Beweis. Wegen der Funktorialität der Artin'schen L-Reihen in Gleichung (1.1) hängt die Nullstellenordnung $r_{S,k}(\chi)$ nicht von L ab, sondern nur von χ als Charakter der absoluten Galoisgruppe G_K. Gleiches gilt für die minimale Erweiterung L_χ von K, über deren Galoisgruppe χ definiert ist. Man kann also annehmen, dass $L = L_\chi$, dass also die Darstellung injektiv ist.

Wir betrachten zunächst ungerade k. Nach der expliziten Berechnung der Nullstellenordnung in Lemma 1.3 folgt dann aus $r_{S,k}(\chi) = 0$, dass $V^{\varphi_\mathfrak{P}} = 0$ für alle $\mathfrak{p}|\infty$. Die Ordnung der Automorphismen $\varphi_\mathfrak{P}$ ist ein Teiler von 2. Die Jordan'sche Normalform von $\rho(\varphi_\mathfrak{P})$ kann daher auf der Hauptdiagonalen nur Einträge 1 und -1 enthalten, auf der Nebendiagonalen nur 0. Zusammen mit $V^{\varphi_\mathfrak{P}} = 0$ folgt $\rho(\varphi_\mathfrak{P}) = -1$ für alle $\mathfrak{p}$ und alle Wahlen der $\mathfrak{P}|\mathfrak{p}$. Da die Darstellung injektiv ist, folgt daraus, dass alle $\varphi_\mathfrak{P}$ gleich sind. Folglich ist K total reell und L ein CM-Körper.

Sei nun k gerade. Wegen Lemma 1.3 bedeutet dann $r_{S,k}(\chi) = 0$, dass es keine komplexen Primstellen gibt und dass $V^{-\varphi_\mathfrak{P}} = 0$ für alle reellen $\mathfrak{p}$. Daraus folgt wie oben, dass $-\rho(\varphi_\mathfrak{P}) = -1$, also $\rho(\varphi_\mathfrak{P}) = 1$, also $\varphi_\mathfrak{P} = 1$ für alle $\mathfrak{p}$ und $\mathfrak{P}$, dass also alle $\mathfrak{p}|\infty$ total zerlegt sind. Somit muss auch L total reell sein. Ist umgekehrt L total reell, so hat K keine komplexen Primstellen und die reellen $\mathfrak{p}$ sind in L total zerlegt, so dass $\varphi_\mathfrak{P} = 1$. Aus Lemma 1.3 liest man dann ab, dass $r_{S,k}(\chi) = 0$. □

Für den Beweis von Satz 1.8 benötigen wir die folgende Serre'sche Verfeinerung des Induktionssatzes von Brauer:

Lemma 1.6. *Sei G eine endliche Gruppe mit Zentrum Z und χ ein irreduzibler Charakter von G. Dann ist die Einschränkung von χ auf Z ein Vielfaches eines eindimensionalen Charakters $\psi : Z \to \mathbf{C}^*$, und χ hat eine Darstellung*

$$\chi = \sum_i n_i \chi_{i,*}.$$

Dabei sind die H_i Untergruppen von G und enthalten Z, die χ_i sind eindimensionale Charaktere von H_i, deren Einschränkung auf Z gerade ψ ist, und $n_i \in \mathbf{Z}$ sind ganze Zahlen.

Beweis. Siehe Tate, [15], ch. III, le. 1.3. □

Lemma 1.7. *Sei χ ein Charakter von $G(L|K)$ und $k \in \mathbf{N}$ mit $\mathcal{L}_S(L|K, \chi, 1-k) \neq 0$. Dann gibt es Zwischenkörper K_i von $L|K$, eindimensionale Charaktere χ_i von $G(L|K_i)$ und $n_i \in \mathbf{Z}$, für die gilt*

(i) $\chi = \sum_i n_i \chi_{i,*}$ *und*

(ii) $\mathcal{L}_{S_i}(L|K_i, \chi_i, 1-k) = \mathcal{L}_S(L|K, \chi_{i,*}, 1-k) \neq 0$

mit $S_i := \{\mathfrak{P}$ von $K_i : \mathfrak{P}|\mathfrak{p}$ für ein $\mathfrak{p} \in S\}$.

Beweis. Sei zunächst χ irreduzibel. Wenn χ eindimensional ist, ist nichts zu zeigen. Sei daher χ mehrdimensional, insbesondere $\chi \neq 1$. Wegen Gleichung (1.1) über die Unabhängigkeit Artin'scher L-Reihen vom Körper L kann man $L = L_\chi$ voraussetzen. Der erste Teil von (ii) ist einfach Gleichung (1.2) über Artin'sche L-Reihen zu induzierten Charakteren, gilt also viel allgemeiner.

Sei zunächst k gerade. Satz 1.5 besagt dann, dass L total reell ist. Nach dem (ursprünglichen) Induktionssatz von Brauer gibt es Zwischenkörper K_i von $L|K$, eindimensionale Charaktere χ_i von $G(L|K_i)$ und $n_i \in \mathbf{Z}$, für die (i) gilt. Da L total reell ist, haben nach Satz 1.5 auch die L-Reihen $\mathcal{L}_S(L|K, \chi_{i,*}, s)$ keine Nullstelle in $s = 1-k$. Damit ist der zweite Teil von (ii) gezeigt.

Sei nun k ungerade. Satz 1.5 besagt dann, dass K total reell und L ein CM-Körper ist. Sei Z das Zentrum vom $G(L|K)$. Gemäß Lemma 1.6 wählen wir Zwischenkörper K_i von $L|K$ mit $Z \subseteq G(L|K_i)$, eindimensionale Charaktere χ_i von $G(L|K_i)$ und $n_i \in \mathbf{Z}$. Diese erfüllen dann (i). Da L ein CM-Körper ist, stimmen alle $\varphi_\mathfrak{P}$ für $\mathfrak{P}|\infty$ überein. Sei τ dieser Automorphismus. Sei $j : L \to \mathbf{C}$ eine beliebige Einbettung. Damit ist τ durch $\tau(z) = j^{-1}(\overline{j(z)})$ gegeben. Für beliebige $\sigma \in G(L|K)$ gilt

$$\begin{aligned}(\sigma\tau\sigma^{-1})(z) &= \sigma j^{-1}(\overline{j(\sigma^{-1}z)})\\ &= (j\sigma^{-1})^{-1}(\overline{(j\sigma^{-1})(z)})\\ &= \tau(z),\end{aligned}$$

da auch $j\sigma^{-1}$ eine Einbettung von L in $\mathbf{C}$ ist. Also ist $\tau \in Z$. Sei $\psi : Z \to \mathbf{C}^*$ wie in Lemma 1.6. Im Beweis zu Satz 1.5 haben wir $\rho(\tau) = -1$ gesehen. Also gilt $\chi(\tau) = -\chi(1)$. Da $\chi = \chi(1)\psi$ auf Z folgt $\psi(\tau) = -1$. Wegen $\chi_i = \psi$ auf Z folgt also

$$\chi_i(\tau) = -1 \tag{1.4}$$

für alle i. Sei nun i fest, $\mathfrak{p}$ eine unendliche Primstelle von K_i und $\mathfrak{P}$ ihre Fortsetzung auf L. Dann ist der Frobeniusautomorphismus $\varphi_\mathfrak{P}$ zu $\mathfrak{P}$ durch

$\varphi_{\mathfrak{P}}(z) = \tilde{\jmath}^{-1}(\overline{\tilde{\jmath}(z)})$ für eine Einbettung $\tilde{\jmath} : L \to \mathbf{C}$ gegeben. Daher ist $\varphi_{\mathfrak{P}} = \tau$. Wegen (1.4) folgt also $\chi_i(\varphi_{\mathfrak{P}}) = -1$, also $V_i^{\varphi_{\mathfrak{P}}} = 0$. Nach Lemma 1.3 folgt $r_{S_i,k}(\chi_i) = 0$. Die L-Reihe $\mathcal{L}_{S_i}(L|K_i, \chi_i, s)$ hat also keine Nullstelle in $s = 1-k$. Damit ist (ii) auch für ungerade k gezeigt.

Abschließend behandeln wir den Fall reduzibler $\chi = \sum_j \chi^{(j)}$. Wir haben $\mathcal{L}_S(L|K, \chi, 1-k) \neq 0$ vorausgesetzt. Artin'sche L-Reihen können nach Lemma 1.3 keine Polstelle in $s = 1-k$ haben. Daher muss auch $\mathcal{L}_S(L|K, \chi^{(j)}, 1-k) \neq 0$ für alle j gelten. Nach dem bisher Gezeigten findet man also für jede irreduzible Komponente $\chi^{(j)}$ von χ eine Zerlegung $\chi^{(j)} = \sum_i n_i^{(j)} \chi_i^{(j)}$ mit (i) und (ii). Für χ ist dann

$$\chi = \sum_j \chi^{(j)} = \sum_j \sum_i n_i^{(j)} \chi_i^{(j)}$$

eine Zerlegung mit (i) und (ii). □

Satz 1.8. *Sei χ ein Charakter von $G(L|K)$. Dann gilt für alle $\alpha \in \mathrm{Aut}(\mathbf{C})$ und $k \in \mathbf{N}$:*

$$\mathcal{L}_S(L|K, \chi, 1-k)^\alpha = \mathcal{L}_S(L|K, \chi^\alpha, 1-k).$$

Beweis. Wenn der Satz für alle irreduziblen Charaktere gezeigt ist, folgt für beliebige $\chi = \sum_i \chi_i$, dass

$$\begin{aligned} \mathcal{L}_S(L|K, \chi, s)^\alpha &= \prod_i \mathcal{L}_S(L|K, \chi_i, s)^\alpha \\ &= \prod_i \mathcal{L}_S(L|K, \chi_i^\alpha, s) \\ &= \mathcal{L}_S(L|K, \chi^\alpha, s). \end{aligned}$$

Wir setzten daher ohne Einschränkung im Folgenden χ als irreduzibel voraus.

Sei zunächst χ eindimensional. Die Artin'sche L-Reihe $\mathcal{L}_S(L|K, \chi, 1-k)$ entspricht dann einer Hecke'schen L-Reihe,

$$\mathcal{L}_S(L|K, \chi, s) = L(\chi, s) = \sum_{(\mathfrak{a},\mathfrak{m})=1} \chi(\mathfrak{a})(\mathfrak{N}\mathfrak{a})^{-s}$$

für ein ganzes Ideal $\mathfrak{m}$ von K, wobei wir den χ entsprechenden Heckecharakter auf $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ ebenfalls mit χ bezeichnet haben. Diese Hecke'sche L-Reihe zerlegt sich weiter

$$\begin{aligned} \mathcal{L}_S(L|K, \chi, s) &= L(\chi, s) \\ &= \sum_{(\mathfrak{a},\mathfrak{m})=1} \chi(\mathfrak{a})(\mathfrak{N}\mathfrak{a})^{-s} \\ &= \sum_{\mathfrak{a}\,\text{rep.}\, J^{\mathfrak{m}}/P^{\mathfrak{m}}} \chi(\mathfrak{a}) \sum_{\substack{\mathfrak{b}\in\mathfrak{a}P^{\mathfrak{m}} \\ \mathfrak{b}\ \text{ganz}}} (\mathfrak{N}\mathfrak{b})^{-s} \qquad (1.5) \\ &= \sum_{\mathfrak{a}\,\text{rep.}\, J^{\mathfrak{m}}/P^{\mathfrak{m}}} \chi(\mathfrak{a}) H(s, \mathfrak{a}P^{\mathfrak{m}}) \end{aligned}$$

mit den *partiellen Zetafunktionen* $H(s, \mathfrak{a}P^{\mathfrak{m}}) := \sum_{\mathfrak{b}\in\mathfrak{a}P^{\mathfrak{m}},\ \mathfrak{b}\text{ ganz}} (\mathfrak{N}\mathfrak{b})^{-s}$. (Siehe auch Beispiel 2.7.)

Gleichung (1.5) ist zunächst nur für $\operatorname{Re} s > 1$ gültig. Da die äußeren Terme jedoch eine eindeutig bestimmte meromorphe Fortsetzung auf ganz $\mathbf{C}$ haben, stimmen sie auch dort überein. Die Werte der partiellen Zetafunktionen $H(s, \mathfrak{a}P^{\mathfrak{m}})$ an den Stellen $s = 1-k,\ k \in \mathbf{N}$ sind nach dem Satz von Siegel/Klingen rational (insbesondere endlich), siehe Neukirch, [12], Kap. VII, Ko. 9.9. Also gilt

$$\mathcal{L}_S(L|K, \chi, 1-k)^\alpha = \sum_{\mathfrak{a}\,\text{rep.}\ J^{\mathfrak{m}}/P^{\mathfrak{m}}} \chi(\mathfrak{a})^\alpha H(s, \mathfrak{a}P^{\mathfrak{m}}) = \mathcal{L}_S(L|K, \chi^\alpha, 1-k),$$

wie gewünscht.

Nun zum allgemeinen Fall: Sei χ ein beliebiger irreduzibler Charakter von $G(L|K)$. Im Beweis zu Lemma 1.1 haben wir gesehen, dass man den zu χ^α gehörenden $G(L|K)$-Modul V^α erhält, indem man die Operation von $G(L|K)$ auf V beibehält und V lediglich mit einer neuen komplexen Vektorraumstruktur versieht. Daraus folgt, dass $\ker\rho = \ker\rho^\alpha$, dass also $L_\chi = L_{\chi^\alpha}$. Wir können daher ohne Einschränkung annehmen, dass $L = L_\chi = L_{\chi^\alpha}$, dass also die Darstellungen ρ und ρ^α injektiv sind. Der Fall $\chi = 1$ wurde bereits im ersten Schritt behandelt. Wir schließen ihn daher im Folgenden aus, da er für $k = 1$ einer Sonderbehandlung bedürfte. Wegen Lemma 1.4 verschwindet mit der L-Funktion zu χ auch diejenige zu χ^α an der Stelle $s = 1-k$ und umgekehrt. Man kann also $r_{S,k}(\chi) = 0$ voraussetzen. Unser Ziel ist es, den allgemeinen Fall durch Brauerinduktion auf den bereits behandelten Fall eindimensionaler Charaktere zurückzuführen.

Gemäß Lemma 1.7 wählen wir Zwischenkörper K_i von $L|K$, eindimensionale Charaktere χ_i von $G(L|K_i)$ und $n_i \in \mathbf{Z}$ so, dass $\chi = \sum_i n_i \chi_{i,*}$ und dass die L-Reihen zu den χ_i keine Nullstellen in $s = 1-k$ haben. Für eindimensionale Charaktere haben wir die gewünschte Transformationsformel schon gezeigt. Wir können daher direkt nachrechnen:

$$\begin{aligned}
\mathcal{L}_S(L|K, \chi, 1-k)^\alpha &= \mathcal{L}_S(L|K, \sum_i n_i\chi_{i,*}, 1-k)^\alpha \\
&= \Big(\prod_i \mathcal{L}_S(L|K, \chi_{i,*}, 1-k)^{n_i}\Big)^\alpha && \text{da keine Nullst.} \\
&= \Big(\prod_i \mathcal{L}_{S_i}(L|K_i, \chi_i, 1-k)^{n_i}\Big)^\alpha && \text{nach (1.2)} \\
&= \prod_i \big(\mathcal{L}_{S_i}(L|K_i, \chi_i, 1-k)^\alpha\big)^{n_i} \\
&= \prod_i \mathcal{L}_{S_i}(L|K_i, \chi_i^\alpha, 1-k)^{n_i} && \text{da } \chi_i \text{ eindim.} \\
&= \prod_i \mathcal{L}_S(L|K, (\chi_i^\alpha)_*, 1-k)^{n_i} && \text{nach (1.2)}
\end{aligned}$$

$$
\begin{aligned}
&= \prod_i \mathcal{L}_S(L|K, (\chi_{i,*})^\alpha, 1-k)^{n_i} \qquad \text{nach Le. 1.2} \\
&= \mathcal{L}_S(L|K, \sum_i n_i (\chi_{i,*})^\alpha, 1-k) \\
&= \mathcal{L}_S(L|K, \left(\sum_i n_i \chi_{i,*}\right)^\alpha, 1-k) \\
&= \mathcal{L}_S(L|K, \chi^\alpha, 1-k).
\end{aligned}
$$

□

Kapitel 2

Galoisdistributionen

2.1 Einführung

Definition. Sei $X = \varprojlim X_i$ $(i \in I)$ ein proendlicher topologischer Raum und A eine abelsche Gruppe. Eine Abbildung $F : \bigcup_i X_i \to A$ heißt eine **Distribution** auf X mit Werten in A, falls für alle $i, j \in I$, $i \leq j$ und $x \in X_i$ die Distributionsrelation

$$F(x) = \sum_{\substack{y \in X_j \\ y \mapsto x}} F(y) \tag{2.1}$$

erfüllt ist. Die abelsche Gruppe der Distributionen auf X mit Werten in A bezeichnen wir mit $\mathrm{Dist}(X, A)$.

Bemerkung. Die Distributionsrelation (2.1) besagt, dass

$$\mathrm{Dist}(X, A) = \varprojlim \mathrm{Abb}(X_i, A),$$

wenn die Abbildungen φ_{ij} im projektiven System $\big(\mathrm{Abb}(X_i, A)\big)_{i \in I}$ als

$$(\varphi_{ij} F)(x) := \sum_{y \mapsto x} F(y)$$

gewählt werden.

Beispiel 2.1. Für $N, a \in \mathbf{N}$ sei

$$H(s, a \bmod N) := \sum_{\substack{n \geq 1 \\ n \equiv a \ (N)}} n^{-s}.$$

Dann ist $(a \bmod N) \mapsto H(s, a \bmod N)$ eine Distribution auf $\hat{\mathbf{Z}} = \varprojlim \mathbf{Z}/N\mathbf{Z}$ mit Werten im komplexen Vektorraum der formalen Dirichletreihen in einer Variablen s. Die Dirichletreihen $H(s, a \bmod N)$ konvergieren für $\mathrm{Re}\, s > 1$

und haben meromorphe Fortsetzungen auf $\mathbf{C}$ mit einzigem Pol in $s = 1$ (siehe Washington, [16], ch. 4, Absatz über die Hurwitz'sche Zetafunktion). Wir können die Distribution also auch mit Werten im Körper $\mathcal{M}(\mathbf{C})$ der meromorphen Funktionen auf $\mathbf{C}$ betrachten.

Beispiel 2.2. Sei $B_k(x)$ das k-te Bernoullipolynom, gegeben durch die Taylorentwicklung

$$\frac{ze^{xz}}{e^z - 1} = \sum_{k=0}^{\infty} B_k(x) \frac{z^k}{k!}.$$

Für $x \in \mathbf{R}$ bezeichne $\langle x \rangle$ das Element in $x + \mathbf{Z}$ mit $0 < \langle x \rangle \leq 1$. Dann definiert

$$E_k(a \bmod N) := N^{k-1} \frac{B_k(\langle a/N \rangle)}{k}$$

eine Distribution E_k auf $\hat{\mathbf{Z}}$ mit Werten in $\mathbf{Q}$. (Das zeigt etwa Lang in [9], ch. 2, § 2.) E_k heißt die k-te **Bernoullidistribution**.

Warnung. Die übliche Definition von $\langle x \rangle$ behandelt die Grenzfälle genau umgekehrt. Unsere Definition ist jedoch in diesem Kontext nützlicher, da nur mit ihr Satz 2.6 auch für $k = 1$ gilt.

Lemma 2.3. *Sei F eine Distribution auf X mit Werten in A und $\varphi : A \to B$ ein Homomorphismus abelscher Gruppen. Dann ist $\varphi \circ F$ eine Distribution auf X mit Werten in B.*

Beweis. Klar. □

Beispiel 2.4. Sei $s_0 \in \mathbf{C},\ s_0 \neq 1$. Mit H wie in Beispiel 2.1 definiert dann

$$(a \bmod m) \mapsto H(s_0, a \bmod m)$$

eine Distribution auf $\hat{\mathbf{Z}}$ mit Werten in $\mathbf{C}$. Der Homomorphismus φ ist in diesem Fall die Auswertung an s_0. Die auf diese Weise für $s_0 = 1 - k,\ k \in \mathbf{N}$ erhaltene Distribution nennt man die k-te **Hurwitzdistribution** H_k.

Modulwertige Distributionen kann man zur Integration lokal konstanter Funktionen benutzen: Sei $X = \varprojlim X_i$ weiterhin ein proendlicher topologischer Raum, R ein kommutativer Ring und M ein R-Modul. Für $i \in I$ sei $\pi_i : X \to X_i$ die kanonische Projektion. Für $y \in X_i$ ist dann $\pi_i^{-1}(\{y\})$ eine offene, abgeschlossene Teilmenge von X.

Eine Funktion $f : X \to R$ heißt **über X_i faktorisierend**, falls es eine Abbildung $\tilde{f} : X_i \to R$ mit $f = \tilde{f} \circ \pi_i$ gibt. Wir nennen $f : X \to R$ **über ein X_i faktorisierend**, falls f über X_i faktorisiert für ein $i \in I$. Es bezeichne $\mathcal{S}(X, R)$ den R-Modul aller Funktionen, die über ein X_i faktorisieren. Dies sind genau die lokal konstanten Funktionen.

Definition. Sei F eine Distribution auf X mit Werten in M, $f \in \mathcal{S}(X, R)$. Dann heißt

$$\int_X f(y)F(dy) := \sum_{y \in X_i} \tilde{f}(y)F(y)$$

das **Integral** von f über X bezüglich F, wobei i so groß gewählt sei, dass f über X_i faktorisiert.

Für Mengen $A \subseteq B$ bezeichnet $1_A : B \to \{0, 1\}$ die charakteristische Funktion von A.

Satz 2.5. *Die R-Moduln* $\mathrm{Dist}(X, M)$ *und* $\mathrm{Hom}_R(\mathcal{S}(X, R), M)$ *sind kanonisch isomorph. Dabei entspricht die Distribution F dem Homomorphismus Φ mit*

$$\Phi(f) = \int_X f(y)F(dy).$$

Umgekehrt entspricht einem Homomorphismus Φ die Distribution F mit

$$F(y) := \Phi(1_{\pi_i^{-1}(\{y\})})$$

für $y \in X_i$.

Beweis. Wir zeigen, dass die Verkettung der angegebenen Abbildungen in beiden Reihenfolgen die Identität ergibt. Sei dazu zunächst $F \in \mathrm{Dist}(X, M)$. Sei Φ der Homomorphismus mit $\Phi(f) = \int_X f(y)F(dy)$. Dann gilt für jedes $i \in I$ und $y \in X_i$:

$$\begin{aligned}
\Phi(1_{\pi_i^{-1}(\{y\})}) &= \int_X 1_{\pi_i^{-1}(\{y\})}(z)F(dz) \\
&= \sum_{z \in X_i} \tilde{1}_{\pi_i^{-1}(\{y\})}(z)F(z) \\
&= \sum_{z \in X_i} 1_{\{y\}}(z)F(z) \\
&= F(y).
\end{aligned}$$

Sei andererseits $\Phi \in \mathrm{Hom}_R(\mathcal{S}(X, R), M)$. Sei F die Distribution mit $F(y) := \Phi(1_{\pi_i^{-1}(\{y\})})$ für $y \in X_i$. Dann gilt für jedes $i \in I$ und jedes $f \in \mathcal{S}(X, R)$, das über X_i faktorisiert:

$$\begin{aligned}
\int_X f(y)F(dy) &= \sum_{y \in X_i} \tilde{f}(y)F(y) \\
&= \sum_{y \in X_i} \tilde{f}(y)\Phi(1_{\pi_i^{-1}(\{y\})}) \\
&= \Phi\left(\sum_{y \in X_i} \tilde{f}(y)1_{\pi_i^{-1}(\{y\})}\right)
\end{aligned}$$

$$= \Phi(f).$$

□

Wir werden gelegentlich die beiden Seiten der obigen Isomorphie identifizieren und setzen daher

$$F(f) := \int_X f(y)F(dy).$$

Bemerkung. Satz 2.5 bereinigt eine Ungenauigkeit in der Definition des Begriffs der Distribution: Man spricht von Distributionen auf dem proendlichen topologischen Raum X. Die Definition hängt jedoch von der gewählten Darstellung $X = \varprojlim X_i$ ab. Genauer müsste man also von Distributionen des projektiven Systems (X_i) sprechen. Sei A eine abelsche Gruppe. Nach Satz 2.5 (für $R = \mathbf{Z},\ M = A$) ist nun die Gruppe $\mathrm{Dist}(X, A)$ kanonisch zu $\mathrm{Hom}_{\mathbf{Z}}(\mathcal{S}(X, \mathbf{Z}), A)$ isomorph. $\mathrm{Dist}(X, A)$ ist also tatsächlich eine Invariante des topologischen Raumes X.

2.2 Bernoulli- und Hurwitzdistributionen

Dieser Abschnitt stellt einige Eigenschaften der Bernoullidistributionen E_k aus Beispiel 2.2 und der Hurwitzdistributionen H_k aus Beispiel 2.4 zusammen.

Satz 2.6. *Für alle $k \in \mathbf{N}$ gilt*

$$H_k = -E_k,$$

das heißt die Bernoulli- und Hurwitzdistributionen stimmen bis auf das Vorzeichen überein. Insbesondere hat auch H_k Werte in $\mathbf{Q}$.

Beweis. Für $0 < x \leq 1$ bezeichne $\zeta(s, x) := \sum_{i=0}^{\infty}(x + i)^{-s}$ die (meromorph auf $\mathbf{C}$ fortgesetzte) Hurwitz'sche Zetafunktion. Für $N \in \mathbf{N},\ 1 \leq a \leq N$ gilt

$$\begin{aligned} H(s, a \bmod N) &= \sum_{k=0}^{\infty}(a + kN)^{-s} \\ &= N^{-s}\sum_{k=0}^{\infty}(a/N + k)^{-s} \\ &= N^{-s}\zeta(s, a/N) \end{aligned}$$

Die obige Rechnung ist zunächst nur für $\mathrm{Re}\, s > 1$ gültig. Da die äußeren Terme jedoch eine eindeutig bestimmte meromorphe Fortsetzung auf ganz $\mathbf{C}$ haben, stimmen diese auch dort überein. Nach Washington, [16], th. 4.2, ist $\zeta(1 - k, x) = -B_k(x)/k$ für $0 < x \leq 1$, insgesamt also

$$H_k(a \bmod N) = H(1 - k, a \bmod N)$$

$$\begin{aligned} &= N^{k-1}\zeta(1-k, a/N) \\ &= -N^{k-1}B_k(a/N)/k \\ &= -E_k(a \bmod N). \end{aligned}$$

Die Tatsache, dass wir a als Vertreter in $\{1, \ldots, N\}$ gewählt haben, entspricht dabei der Bedingung $0 < \langle x \rangle \leq 1$, vergleiche die Warnung auf Seite 20. □

Beispiel 2.7. Die Hurwitzdistributionen aus Beispiel 2.1 und 2.4 kann man durch Einschränkung auch als Distributionen auf $\mathbf{Z}_p$ und $\mathbf{Z}_p^*$ für jede Primzahl p betrachten. Die auf $\mathbf{Z}_p^*$ definierte Version erlaubt die folgende Verallgemeinerung: Sei K ein algebraischer Zahlkörper. Für ein Ideal $\mathfrak{m}$ von K bezeichne $J^{\mathfrak{m}}$ die Gruppe der zu $\mathfrak{m}$ teilerfremden Ideale von K und $P^{\mathfrak{m}}$ die Untergruppe der Hauptideale, die durch ein total positives Element erzeugt werden, das in der Klasse von 1 modulo $\mathfrak{m}$ liegt. (Somit gilt laut Klassenkörpertheorie $G(K^{\mathfrak{m}}|K) = J^{\mathfrak{m}}/P^{\mathfrak{m}}$, wobei $K^{\mathfrak{m}}$ den Strahlklassenkörper zu $\mathfrak{m}$ bezeichnet. Im projektiven Limes ergibt sich $G_K^{ab} = \varprojlim J^{\mathfrak{m}}/P^{\mathfrak{m}}$.) Für jedes zu $\mathfrak{m}$ teilerfremde Ideal $\mathfrak{a}$ von K sei

$$H(s, \mathfrak{a}P^{\mathfrak{m}}) := \sum_{\substack{\mathfrak{b} \in \mathfrak{a}P^{\mathfrak{m}} \\ \mathfrak{b} \text{ ganz}}} (\mathfrak{N}\mathfrak{b})^{-s}$$

die **partielle Zetafunktion** zu $\mathfrak{a}$, die bereits im Beweis zu Satz 1.8 verwendet wurde. Sei nun $\mathfrak{p}$ ein festes Primideal von K und $K^{\mathfrak{p}^\infty} := \bigcup_{n \in \mathbf{N}} K^{\mathfrak{p}^n}$ die Vereinigung aller Strahlklassenkörper zu $\mathfrak{p}$-Potenzen. Wenn wir $\mathfrak{m}$ der Form $\mathfrak{m} = \mathfrak{p}^n$ betrachten, erhalten wir eine Distribution auf $\varprojlim J^{\mathfrak{p}}/P^{\mathfrak{p}^n} = \varprojlim J^{\mathfrak{p}^n}/P^{\mathfrak{p}^n} = G(K^{\mathfrak{p}^\infty}|K)$ mit Werten im Vektorraum der formalen Dirichletreihen in s bzw. (nach Fortsetzung) im Körper der meromorphen Funktionen auf $\mathbf{C}$. Diese Funktionen haben an den Stellen $s = 1-k$ für $k \in \mathbf{N}$ keine Pole (sondern nehmen nach dem unten zitierten Satz von Siegel/Klingen dort sogar rationale Werte an). Mit dem Lemma 2.3 erhalten wir also für $k \in \mathbf{N}$ wieder Distributionen H_k^K mit Werten in $\mathbf{C}$ durch

$$H_k^K(\mathfrak{a}P^{\mathfrak{p}^n}) := H(1-k, \mathfrak{a}P^{\mathfrak{p}^n}).$$

Diese werden wir ebenfalls als **Hurwitzdistributionen** bezeichnen.

Warnung. Die Wahl eines festen Primideals $\mathfrak{p}$ erscheint auf den ersten Blick überflüssig: Für jede Klasse $\mathfrak{a}P^{\mathfrak{m}} \in J^{\mathfrak{m}}/P^{\mathfrak{m}}$ kann man $H(s, \mathfrak{a}P^{\mathfrak{m}})$ definieren. Allerdings erfüllen diese Funktionen nicht mehr die Distributionsrelation (2.1), so dass man keine Distribution auf $\varprojlim J^{\mathfrak{m}}/P^{\mathfrak{m}} = G_K^{ab}$ erhält. Dies liegt am Fehlen von Eulerfaktoren bei Hecke'schen L-Reihen zu nichtprimitiven Charakteren. Durch Verwendung Artin'scher L-Reihen kann man diesen Mangel beheben (siehe Abschnitt 2.5).

Satz 2.8 (Siegel, Klingen). *Die Hurwitzdistributionen zu jedem algebraischen Zahlkörper K haben Werte in $\mathbf{Q}$, das heißt*

$$H_k^K \in \mathrm{Dist}(\varprojlim J^{\mathfrak{p}}/P^{\mathfrak{p}^n}, \mathbf{Q}).$$

Beweis. Siehe zum Beispiel Neukirch, [12], Kap. VII, Ko. 9.9. □

2.3 Die Algebra der Distributionen

Sei $G = \varprojlim G_i$ $(i \in I)$ eine proendliche Gruppe und A ein Ring. Die abelsche Gruppe $\mathrm{Dist}(G, A)$ wird dann ein A-Modul, indem A werteweise auf den Distributionen operiert.

Definition. Wir definieren das **Faltungsprodukt** auf $\mathrm{Dist}(G, A)$ durch

$$(F * G)(c) := \sum_{ab=c} F(a)G(b)$$

für $c \in G_i$, wobei (a, b) die Paare von Elementen von G_i durchläuft, die $ab = c$ erfüllen. $\mathrm{Dist}(G, A)$ ist damit eine A-Algebra.

Definition. Für eine proendliche Gruppe $G = \varprojlim G_i$ $(i \in I)$ und einen Ring A sei

$$A[[G]] := \varprojlim A[G_i]$$

der **vollständige Gruppenring** von G mit Koeffizienten in A.

Satz 2.9. *Die A-Algebren* $\mathrm{Dist}(G, A)$ *und* $A[[G]]$ *sind kanonisch isomorph.*

Beweis. Wegen der Isomorphie $\mathrm{Dist}(G, A) = \varprojlim \mathrm{Abb}(G_i, A)$ aus der Bemerkung auf Seite 19 sind die beiden Objekte sicher als abelsche Gruppen und A-Moduln isomorph. Man muss sich also nur noch von der Übereinstimmung der Produkte überzeugen. Tatsächlich ist das Produkt in den Gruppenringen $A[G_i]$ genau wie das Faltungsprodukt definiert. □

Definition. Für ein Element $\theta = \sum c_\sigma \cdot \sigma$ in einem beliebigen Gruppenring heiße $\bar{\theta} := \sum c_\sigma \cdot \sigma^{-1}$ das zu θ **opposite Element**.

Beispiel 2.10. Sei $F \in \mathrm{Dist}(\mathbf{Z}_p^*, \mathbf{Q})$ die Einschränkung der ersten Bernoullidistribution E_1 auf $\mathbf{Z}_p^* = G(\mathbf{Q}(\mu_{p^\infty})|\mathbf{Q}) = \varprojlim G(\mathbf{Q}(\mu_{p^n})|\mathbf{Q})$. Für $a \in (\mathbf{Z}/p^n\mathbf{Z})^*$ sei $\sigma_a \in G(\mathbf{Q}(\mu_{p^n})|\mathbf{Q})$ der Automorphismus, der auf p^n-ten Einheitswurzeln durch $\zeta^{\sigma_a} = \zeta^a$ operiert. Wegen $B_1(x) = x - 1/2$ entspricht F als Element von $\mathbf{Q}[[G(\mathbf{Q}(\mu_{p^\infty})|\mathbf{Q})]]$ der Familie $(\bar{\theta}(p^n))_{n\in\mathbf{N}}$ mit

$$\bar{\theta}(p^n) = \sum_{\substack{a=1,\ldots,p^n-1 \\ (a,p)=1}} B_1(a/p^n) \cdot \sigma_a$$

$$= \sum_{\substack{a=1,\dots,p^n-1\\(a,p)=1}} \left(\frac{a}{p^n} - \frac{1}{2}\right) \cdot \sigma_a.$$

Man erhält also durch $\bar{\theta}(p^n)$ opposite Stickelbergerelemente. Allgemein erhält man durch Betrachten von E_k ($k \in \mathbf{N}$) die oppositen k-ten Stickelbergerelemente $\theta_k(p^n)$ aus Lang, [9], ch. 2, § 3.

(Lieber würde man statt p^n wirklich alle N betrachten. Das geht aus den in der Warnung zu Beispiel 2.7 angegebenen Gründen nicht: Die Einschränkung von E_1 auf $\hat{\mathbf{Z}}^*$ ist keine Distribution.)

2.4 Klassendistributionen und die skalare Fouriertransformation

Auf proendlichen Gruppen erhält man Distributionen als Fouriertransformierte von Charakterfunktionen (siehe Satz 2.12). Um dies zu zeigen benötigen wir zunächst die folgende Orthogonalitätsrelation:

Lemma 2.11. *Sei G eine endliche Gruppe, H normal in G, außerdem χ ein irreduzibler Charakter und c ein Element von G. Dann gilt*

$$\sum_{\substack{\tilde{c}\in G\\ \tilde{c}H=cH}} \chi(\tilde{c}) = \begin{cases} |H| \cdot \chi(\tilde{c}) & \textit{falls } \rho_\chi \textit{ über } G/H \textit{ faktorisiert,} \\ 0 & \textit{sonst,} \end{cases}$$

wobei ρ_χ eine zu χ gehörende Darstellung bezeichne.

Beweis. Der erste Fall ist offensichtlich. Im zweiten Fall gilt für alle irreduziblen Charaktere χ', für die $\rho_{\chi'}$ über G/H faktorisiert, dass $\chi \neq \chi'$. Also folgt aus den Orthogonalitätsrelationen

$$(\chi, \chi')_G := \frac{1}{|G|} \sum_{a\in G} \chi(a)\bar{\chi}'(a) = 0.$$

Sei $f : G/H \to \mathbf{C}$ gegeben durch

$$f(aH) := \sum_{b\in H} \chi(ab).$$

f ist eine Klassenfunktion auf G/H, denn

$$\begin{aligned} f(xax^{-1}H) &= \sum_{b\in H} \chi(xax^{-1}b) \\ &= \sum_{b\in H} \chi(xax^{-1}xbx^{-1}) \end{aligned}$$

$$\begin{aligned} &= \sum_{b\in H} \chi(xabx^{-1}) \\ &= \sum_{b\in H} \chi(ab). \end{aligned}$$

Für jeden irreduziblen Charakter χ' von G/H gilt

$$\begin{aligned} (f,\chi')_{G/H} &= \frac{1}{(G:H)} \sum_{a \bmod H} f(a)\bar{\chi}'(a) \\ &= \frac{1}{(G:H)} \sum_{a \bmod H} \sum_{b\in H} \chi(ab)\bar{\chi}'(ab) \\ &= \text{konst.} \cdot (\chi,\chi')_G \\ &= 0. \end{aligned}$$

Da die χ' eine Orthonormalbasis des Raumes der komplexwertigen Klassenfunktionen auf G/H bilden, folgt $f = 0$. $\square$

Sei $G = \varprojlim G_i$ $(i \in I)$ eine proendliche Gruppe und V ein komplexer Vektorraum.

Definition. Eine **Charakterfunktion** von G mit Werten in V ist eine Abbildung, die jedem irreduziblen Charakter von G, der über ein G_i faktorisiert, ein Element aus V zuordnet. $\mathrm{ChFct}(G,V)$ bezeichne den komplexen Vektorraum der Charakterfunktionen von G mit Werten in V.

Eine Distribution F auf einer proendlichen Gruppe G mit Werten in V heißt eine **Klassendistribution**, falls sie auf jeder Konjugationsklasse jedes endlichen Quotienten G_i konstant ist. $\mathrm{ClDist}(G,V)$ bezeichne die Menge der Klassendistributionen auf G mit Werten in V.

Satz 2.12. *Die Vektorräume* $\mathrm{ClDist}(G,V)$ *und* $\mathrm{ChFct}(G,V)$ *sind kanonisch isomorph. Dabei entspricht einer Distribution F die Charakterfunktion Φ mit*

$$\Phi(\chi) = \int_G \chi(\sigma)F(d\sigma).$$

Umgekehrt entspricht einer Charakterfunktion Φ die Distribution F mit

$$F(\sigma) = \frac{1}{|G_i|} \sum_{\chi\,von\,G_i} \Phi(\chi)\cdot\bar{\chi}(\sigma)$$

für $\sigma \in G_i$.

Beweis. Der entscheidende Punkt ist, einzusehen, dass die Zuordnung $\Phi \mapsto F$ tatsächlich stets eine Distribution liefert. Man muss dazu die Distributionsrelation (2.1) verifizieren. Sei also $i \le j$, $\sigma \in G_i$. Dann gilt

$$\sum_{\substack{\tau\in G_j \\ \tau\mapsto\sigma}} F(\tau) = \frac{1}{|G_j|} \sum_{\chi\,\mathrm{von}\,G_j} \Phi(\chi) \sum_{\tau} \bar{\chi}(\tau)$$

$$
\begin{aligned}
&= \frac{1}{|G_i|} \sum_{\chi \,\mathrm{von}\, G_i} \Phi(\chi)\bar{\chi}(\sigma) \\
&= F(\sigma),
\end{aligned}
$$

wobei der Übergang zur zweiten Zeile dadurch gerechtfertigt ist, dass $\sum_\tau \bar{\chi}(\tau)$ laut Lemma 2.11 gerade 0 bzw. $\frac{|G_j|}{|G_i|}\bar{\chi}(\sigma)$ ist. F ist als Linearkombination von Charakteren definiert. Also ist F auch konstant auf Konjugationsklassen, also eine Klassendistribution.

Dass die beiden Abbildungen invers zueinander sind, kann man nun unmittelbar mit Hilfe der Orthogonalitätsrelationen für Charaktere wie folgt nachrechnen: Sei zunächst Φ eine beliebige Charakterfunktion und F die dazu wie im Satz definierte Distribution. Dann gilt für jeden Charakter χ, der über G_i faktorisiert:

$$
\begin{aligned}
\int_G \chi(\sigma) F(d\sigma) &= \sum_{\sigma \in G_i} \chi(\sigma) F(\sigma) \\
&= \sum_{\sigma \in G_i} \chi(\sigma) \frac{1}{|G_i|} \sum_{\psi \,\mathrm{von}\, G_i} \Phi(\psi)\bar{\psi}(\sigma) \\
&= \sum_{\psi \,\mathrm{von}\, G_i} \Phi(\psi) \frac{1}{|G_i|} \sum_{\sigma \in G_i} \chi(\sigma)\bar{\psi}(\sigma) \\
&= \sum_{\psi \,\mathrm{von}\, G_i} \Phi(\psi)(\chi, \psi) \\
&= \Phi(\chi).
\end{aligned}
$$

Sei nun umgekehrt F eine beliebige Klassendistribution und Φ die dazu wie im Satz definierte Charakterfunktion. Dann gilt für $\sigma \in G_i$:

$$
\begin{aligned}
\frac{1}{|G_i|} \sum_{\chi \,\mathrm{von}\, G_i} \Phi(\chi)\bar{\chi}(\sigma) &= \frac{1}{|G_i|} \sum_{\chi \,\mathrm{von}\, G_i} \int_G \chi(\tau) F(d\tau) \bar{\chi}(\sigma) \\
&= \frac{1}{|G_i|} \sum_{\chi \,\mathrm{von}\, G_i} \sum_{\tau \in G_i} \chi(\tau) F(\tau) \bar{\chi}(\sigma) \\
&= \sum_{\chi \,\mathrm{von}\, G_i} \frac{1}{|G_i|} \left(\sum_{\tau \in G_i} F(\tau)\chi(\tau) \right) \bar{\chi}(\sigma) \\
&= \sum_{\chi \,\mathrm{von}\, G_i} (F|_{G_i}, \bar{\chi}) \bar{\chi}(\sigma) \\
&= \sum_{\chi \,\mathrm{von}\, G_i} (F|_{G_i}, \chi) \chi(\sigma) \\
&= \left(\sum_{\chi \,\mathrm{von}\, G_i} (F|_{G_i}, \chi)\chi \right) (\sigma)
\end{aligned}
$$

$$= F(\sigma).$$

□

Wir werden aufgrund von Satz 2.12 Distributionen und zugehörende Charakterfunktionen gelegentlich identifizieren und mit dem gleichen Buchstaben bezeichnen.

Die durch Satz 2.12 erhaltenen Distributionen sind konstant auf jeder Konjugationsklasse jedes endlichen Quotienten der zugrundeliegenden proendlichen Gruppe. Es ist daher gelegentlich handlicher, direkt zu Distributionen auf einem geeigneten Klassenraum überzugehen. Dies ist wie folgt möglich:

Satz 2.13. *Sei $G = \varprojlim G_i$ $(i \in I)$ eine proendliche Gruppe. Für jeden endlichen Quotienten G_i bezeichne $\mathrm{Cl}(G_i)$ die Menge der Konjugationsklassen. F sei eine Distribution auf G, die auf jedem Element jedes $\mathrm{Cl}(G_i)$ konstant ist. Für $c \in \mathrm{Cl}(G_i)$, $\sigma \in c$ sei*

$$\underline{F}(c) := |c|\, F(\sigma) = \sum_{\tau \in c} F(\tau).$$

Dies definiert eine Distribution $\underline{F}$ auf dem proendlichen topologischen Raum $\mathrm{Cl}(G) := \varprojlim \mathrm{Cl}(G_i)$.

Beweis. Der projektive Limes $\varprojlim \mathrm{Cl}(G_i)$ ist wohldefiniert, da konjugierte Elemente in einem endlichen Quotienten G_j auf im kleineren Quotienten G_i $(i \leq j)$ konjugierte Elemente abgebildet werden. Man muss also nur noch die Distributionsrelation (2.1) nachrechnen. Sei dazu $i \leq j$, $c \in \mathrm{Cl}(G_i)$. Dann gilt

$$\begin{aligned}
\underline{F}(c) &= \sum_{\tau \in c} F(\tau) \\
&= \sum_{\tau \in c} \sum_{\tilde{\tau} \mapsto \tau} F(\tilde{\tau}) \\
&= \sum_{\tilde{c} \mapsto c} \sum_{\tilde{\tau} \in \tilde{c}} F(\tilde{\tau}) \\
&= \sum_{\tilde{c} \mapsto c} \underline{F}(\tilde{c}),
\end{aligned}$$

wobei der Übergang zur dritten Zeile aus dem folgenden Grund gerechtfertigt ist: Im ersten Fall wird über $\{\tilde{\tau} \in G_j : \varphi_{ij}(\tilde{\tau}) \sim \sigma\}$ summiert, im zweiten Fall über $\{\tilde{\tau} \in G_j : \tilde{\tau} \sim \tilde{\tau}' \text{ und } \varphi_{ij}(\tilde{\tau}') \sim \sigma \text{ für ein } \tilde{\tau}' \in G_j\}$. Tatsächlich sind diese beiden Mengen gleich. □

2.5 Die Standarddistributionen

Satz 2.12 erlaubt es, Charakterfunktionen in Distributionen umzuwandeln. Das nutzen wir für die folgende Konstruktion aus.

Sei K ein algebraischer Zahlkörper, G_K die absolute Galoisgruppe von K und S eine endliche Menge von Primidealen von K. Für jeden Charakter χ jedes endlichen Quotienten $G(L|K)$ bezeichne $\mathcal{L}_S(L|K, \rho_\chi, s)$ die zugehörende Artin'sche L-Reihe ohne die zu Primidealen aus S gehörenden Eulerfaktoren. Für $L|K$ endlich galoissch und $\sigma \in G(L|K)$ sei

$$L_S(s, \sigma) := \frac{1}{|G(L|K)|} \sum_{\chi \text{ von } G(L|K)} \mathcal{L}_S(L|K, \rho_\chi, s) \cdot \bar{\chi}(\sigma)$$

die **partielle Zetafunktion** zu σ. Dann ist $\sigma \mapsto L_S(s, \sigma)$ gemäß Satz 2.12 eine Distribution auf G_K mit Werten in $\mathcal{M}(\mathbf{C})$. Die Bezeichnung als „partielle Zetafunktion“ ist dadurch gerechtfertigt, dass $L_S(s, 1) = \zeta_{K,S}(s)$ für den trivialen Automorphismus $1 \in G_{\mathbf{Q}}$, wobei $\zeta_{K,S}(s)$ die Dedekind'sche Zetafunktion zu K ohne die zu Primidealen aus S gehörenden Eulerfaktoren bezeichnet. Die Distributionsrelation (2.1) besagt damit, dass man für jede endliche Galoiserweiterung $L|K$ eine additive Zerlegung

$$\zeta_{K,S}(s) = \sum_{\sigma \in G(L|K)} L_S(s, \sigma)$$

der Dedekind'schen Zetafunktion erhält.

Wie in Beispiel 2.4 kann man auch die partiellen Zetafunktionen an einer Stelle s_0 auswerten, an der keine von ihnen einen Pol hat. Man erhält so eine Distribution $\sigma \mapsto L_S(s_0, \sigma)$ mit Werten in $\mathbf{C}$. Nach Lemma 1.3 haben Artin'sche L-Reihen keine Pole in $s = 1 - k$. Also können auch partielle Zetafunktionen dort keine Pole haben. Die obige Konstruktion ist also für $s_0 = 1 - k$ möglich.

Definition. Wir bezeichnen die so erhaltene Distribution mit $L^K_{S,k}$, das heißt

$$L^K_{S,k}(\sigma) = L_S(1 - k, \sigma).$$

$L^K_{S,k}$ heißt die k-te **Standarddistribution** zu S auf G_K. Für $K = \mathbf{Q}$ schreiben wir kurz $L_{S,k} := L^{\mathbf{Q}}_{S,k}$.

Satz 2.12 besagt also in diesem Fall, dass

$$\mathcal{L}_S(L|K, \chi, 1 - k) = \int_{G_K} \chi(\sigma) L^K_{S,k}(d\sigma) \tag{2.2}$$

für alle irreduziblen Charaktere χ jedes endlichen Quotienten von G_K.

Warnung. Gleichung (2.2) wird falsch, wenn man die Voraussetzung der Irreduzibilität von χ fallen lässt: Das sieht man schon daran, dass sich die linke Seite bei Addition von Charakteren multiplikativ verhält, die rechte Seite aber additiv.

Die Funktionen $L_S(s,\sigma)$ hängen mit den Funktionen $H(s, a \bmod m)$ aus Beispiel 2.1 wie folgt zusammen:

Satz 2.14. *Sei p eine Primzahl, $n \in \mathbf{N}$. $\sigma \in G(\mathbf{Q}(\mu_{p^n})|\mathbf{Q})$ operiere auf p^n-ten Einheitswurzeln durch $\zeta^\sigma = \zeta^a$ für $a \in (\mathbf{Z}/p^n\mathbf{Z})^*$. Dann gilt (mit $S = \emptyset$)*

$$L_\emptyset(s,\sigma) = H(s, a \bmod p^n) + \frac{1}{(p-1)p^{n-1}} H(s, p \bmod p).$$

Beweis. Sei $G = G(\mathbf{Q}(\mu_{p^n})|\mathbf{Q})$. Für jeden Charakter χ von G bezeichne χ ebenfalls den zugehörenden *primitiven* Dirichletcharakter. Für $s \in \mathbf{C}$ mit $\operatorname{Re} s > 1$ gilt dann

$$\begin{aligned}
|G| \cdot L(s,\sigma) &= \sum_{\chi \in \hat{G}} \mathcal{L}(\mathbf{Q}(\mu_{p^n})|\mathbf{Q}, \chi, s) \cdot \bar{\chi}(\sigma) \\
&= \sum_{\chi \in \hat{G}} \sum_{m=1}^{\infty} \chi(m) m^{-s} \chi(a^{-1}) \\
&= \sum_{\chi \in \hat{G}} \sum_{m=1}^{\infty} \chi(a^{-1}m) m^{-s} \\
&= \sum_{m=1}^{\infty} \left(\sum_{\chi \in \hat{G}} \chi(a^{-1}m) \right) m^{-s}.
\end{aligned}$$

Wegen

$$\sum_{\chi \in \hat{G}} \chi(a^{-1}m) = \begin{cases} 0, & \text{falls } a^{-1}m \not\equiv 1 \ (p^n) \text{ und } p \nmid m, \\ |G|, & \text{falls } a^{-1}m \equiv 1 \ (p^n), \text{ sowie} \\ 1, & \text{falls } p \mid m \text{ (beachte } \chi = 1) \end{cases}$$

folgt

$$|G| \cdot L(s,\sigma) = |G| \cdot \left(\sum_{m \equiv a \ (p^n)} m^{-s} + \frac{1}{|G|} \sum_{p|m} m^{-s} \right)$$

und damit die Behauptung. $\square$

Korollar 2.15. *Sei p eine Primzahl, $n \in \mathbf{N}$. $\sigma \in G(\mathbf{Q}(\mu_{p^n})|\mathbf{Q})$ operiere auf p^n-ten Einheitswurzeln durch $\zeta^\sigma = \zeta^a$ für $a \in (\mathbf{Z}/p^n\mathbf{Z})^*$. Dann gilt (mit $S = \{p\}$)*

$$L_{\{p\}}(s,\sigma) = H(s, a \bmod p^n).$$

Beweis. Da $H(s, p \bmod p) = p^{-s}\zeta(s)$ folgt aus Satz 2.14:

$$
\begin{aligned}
H(s, a \bmod p^n) &= L(s,\sigma) - \frac{1}{|G|} p^{-s}\zeta(s) \\
&= L(s,\sigma) - \frac{1}{|G|}\big(1 - (1-p^{-s})\big)\,\zeta(s) \\
&= L(s,\sigma) - \frac{1}{|G|}\big(\zeta(s) - (1-p^{-s})\zeta(s)\big) \\
&= \frac{1}{|G|}\left(\sum_{\chi \text{ von } G} \mathcal{L}(\mathbf{Q}(\mu_{p^n})|\mathbf{Q},\chi,s)\bar{\chi}(\sigma) - \zeta(s) + (1-p^{-s})\zeta(s)\right).
\end{aligned}
$$

In der Summe über alle χ wird also der Summand zum trivialen Charakter $\chi = 1$ durch den entsprechenden Summanden ersetzt, bei dem der p-Eulerfaktor entfernt wurde. Da $\chi(p) = 0$ für alle $\chi \neq 1$ können wir schreiben

$$
\begin{aligned}
H(s, a \bmod p^n) &= \frac{1}{|G|}\left(\sum_{\chi \text{ von } G} (1-\chi(p)p^{-s})\mathcal{L}(\mathbf{Q}(\mu_{p^n})|\mathbf{Q},\chi,s)\bar{\chi}(\sigma)\right) \\
&= \frac{1}{|G|}\left(\sum_{\chi \text{ von } G} \mathcal{L}_{\{p\}}(\mathbf{Q}(\mu_{p^n})|\mathbf{Q},\chi,s)\bar{\chi}(\sigma)\right) \\
&= L_{\{p\}}(s,\sigma)
\end{aligned}
$$

und erhalten das Korollar. □

Der Zusammenhang zwischen den Hurwitzdistributionen und den Standarddistributionen zeigt sich auch über anderen Grundkörpern als $\mathbf{Q}$. In diesem Fall zeigen wir der Einfachheit halber direkt die Korollar 2.15 entsprechende Version, die ohnehin die natürlichere ist.

Satz 2.16. *Sei K ein algebraischer Zahlkörper, $\mathfrak{p}$ ein Primideal von K und $n \in \mathbf{N}$. Sei $\mathfrak{m} := \mathfrak{p}^n$ und $L := K^{\mathfrak{m}}$ der Strahlklassenkörper zu $\mathfrak{m}$. Sei $\mathfrak{a}$ ein ganzes, zu $\mathfrak{p}$ teilerfremdes Ideal von K, sowie $\sigma := (\mathfrak{a}, L|K) \in G(L|K)$ der ihm über das Artinsymbol zugeordnete Automorphismus. Dann gilt*

$$L_{\{\mathfrak{p}\}}(s,\sigma) = H(s, \mathfrak{a}P^{\mathfrak{m}}).$$

Beweis. Sei $G := G(L|K)$. Für einen Charakter χ von G bezeichne χ ebenfalls den (nicht notwendig primitiven) zugehörenden Heckecharakter auf der Strahlklassengruppe $J^{\mathfrak{m}}/P^{\mathfrak{m}}$. Damit gilt $\mathcal{L}_{\{\mathfrak{p}\}}(L|K,\chi,s) = L(\chi,s)$ für jedes χ, wobei $L(\chi,s)$ die Hecke'sche L-Reihe bezeichnet. Es gilt:

$$|G|\, L_{\{\mathfrak{p}\}}(s,\sigma) = \sum_{\chi \text{ von } G} \mathcal{L}_{\{\mathfrak{p}\}}(L|K,\chi,s)\bar{\chi}(\sigma)$$

$$\begin{aligned}
&= \sum_{\chi} L(\chi, s)\chi(\sigma^{-1}) \\
&= \sum_{\chi} \sum_{(\mathfrak{b},\mathfrak{p})=1} \chi(\mathfrak{b})(\mathfrak{N}\mathfrak{b})^{-s}\chi(\mathfrak{a}^{-1}) \\
&= \sum_{(\mathfrak{b},\mathfrak{p})=1} \left(\sum_{\chi} \chi(\mathfrak{b}\mathfrak{a}^{-1})\right)(\mathfrak{N}\mathfrak{b})^{-s}.
\end{aligned}$$

Da

$$\sum_{\chi} \chi(\mathfrak{b}\mathfrak{a}^{-1}) = \begin{cases} |G| & \mathfrak{b}\mathfrak{a}^{-1} = 1 \text{ in } J^{\mathfrak{m}}/P^{\mathfrak{m}}, \\ 0 & \text{sonst} \end{cases}$$

ist also

$$|G|\, L_{\{\mathfrak{p}\}}(s,\sigma) = |G| \sum_{\substack{\mathfrak{b}\in\mathfrak{a}P^{\mathfrak{m}} \\ \mathfrak{b} \text{ ganz}}} (\mathfrak{N}\mathfrak{b})^{-s} = |G|\, H(s, \mathfrak{a}P^{\mathfrak{m}}),$$

und die Behauptung folgt. □

2.6 Rationalität der Standarddistributionen

Satz 2.17. *Sei $L|K$ eine endliche galoissche Erweiterung algebraischer Zahlkörper, $\sigma \in G(L|K)$ und S eine beliebige endliche Menge von Primidealen in K. Dann gilt*

$$L_S(1-k,\sigma) \in \mathbf{Q}$$

für die partielle Zetafunktion $L_S(s,\sigma)$ aus Abschnitt 2.5 und jedes $k \in \mathbf{N}$. Mit anderen Worten hat also die Standarddistribution $L^K_{S,k}$ auf G_K Werte in $\mathbf{Q}$.

Beweis. Sei $\alpha \in \mathrm{Aut}(\mathbf{C})$ beliebig. Dann gilt nach Satz 1.8

$$\begin{aligned}
L_S(1-k,\sigma)^\alpha &= \left(\frac{1}{|G|} \sum_{\chi \text{ von } G} \mathcal{L}_S(L|K,\chi,1-k)\bar{\chi}(\sigma)\right)^\alpha \\
&= \frac{1}{|G|} \sum_{\chi \text{ von } G} \mathcal{L}_S(L|K,\chi,1-k)^\alpha \bar{\chi}^\alpha(\sigma) \\
&= \frac{1}{|G|} \sum_{\chi \text{ von } G} \mathcal{L}_S(L|K,\chi^\alpha,1-k)\chi^\alpha(\sigma^{-1}) \\
&= \frac{1}{|G|} \sum_{\chi \text{ von } G} \mathcal{L}_S(L|K,\chi,1-k)\chi(\sigma^{-1}) \\
&= \frac{1}{|G|} \sum_{\chi \text{ von } G} \mathcal{L}_S(L|K,\chi,1-k)\bar{\chi}(\sigma) \\
&= L_S(1-k,\sigma).
\end{aligned}$$

$L_S(1-k,\sigma)$ ist also invariant unter $\mathrm{Aut}(\mathbf{C})$ und damit rational. □

Kapitel 3

Distributionen auf $\mathrm{GL}_2(\mathbf{Z}_p)$

Bisher haben wir Standarddistributionen auf $G_{\mathbf{Q}}$ betrachtet. Die zugehörende Familie von Körpererweiterungen von $\mathbf{Q}$ ist die Familie *aller* algebraischen Erweiterungen. Im abelschen Fall entspricht dies der Untersuchung der Bernoullidistributionen auf $\hat{\mathbf{Z}}$, das heißt bezüglich der Familie *aller* abelscher Erweiterungen von $\mathbf{Q}$. Schon im abelschen Fall erhält man jedoch viele Ergebnisse nur für die Einschränkung der Distributionen auf $\mathbf{Z}_p$, das heißt für die Familie der p^n-ten Kreisteilungskörper über $\mathbf{Q}$. Das Ziel dieses Kapitels ist es, eine entsprechende Familie nichtabelscher Erweiterungen von $\mathbf{Q}$ zu untersuchen und so weitere Erkenntnisse über die Standarddistributionen zu erhalten.

3.1 Einführung

Sei E eine über $\mathbf{Q}$ definierte elliptische Kurve und p eine Primzahl. Der $(\mathbf{Z}/p^n\mathbf{Z})$-Modul der p^n-ten Teilungspunkte von E über $\bar{\mathbf{Q}}$ wird mit $E[p^n]$ bezeichnet. $\mathbf{Q}(E[p^n])$ bezeichne den kleinsten Erweiterungskörper von $\mathbf{Q}$, über dem alle p^n-ten Teilungspunkte definiert sind. Wir setzen im Folgenden voraus, dass die natürliche Galoisdarstellung

$$G(\mathbf{Q}(E[p^n])|\mathbf{Q}) \to \mathrm{Aut}(E[p^n])$$

für alle n surjektiv ist. (Wie Serre in [13] gezeigt hat, ist dies der Normalfall.) Wir wählen eine feste Basis von $E[p^n]$ und können damit identifizieren: $E[p^n] = (\mathbf{Z}/p^n\mathbf{Z})^2,\ \mathrm{Aut}(E[p^n]) = \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$. Im projektiven Limes ergibt sich für $\mathbf{Q}(E[p^\infty]) := \bigcup \mathbf{Q}(E[p^n])$

$$G(\mathbf{Q}(E[p^\infty])|\mathbf{Q}) = \mathrm{Aut}(T_p(E)) = \mathrm{GL}_2(\mathbf{Z}_p),$$

wobei $T_p(E) := \varprojlim E[p^n]$ den Tatemodul bezeichnet.

Sei $L_{\{p\},k}$ die Einschränkung der k-ten Standarddistribution aus Abschnitt 2.5 auf $G(\mathbf{Q}(E[p^\infty])|\mathbf{Q}) = \mathrm{GL}_2(\mathbf{Z}_p)$. Diese Distribution wird im Folgenden untersucht.

3.2 Folgerungen aus der Distributionsrelation

Die Standarddistributionen sind auf ganz $G_{\mathbf{Q}}$ definiert. Wir betrachten hier die Einschränkung auf $G(\mathbf{Q}(E[p^\infty])|\mathbf{Q})$, was dem Körperturm $(\mathbf{Q}(E[p^n]))_{n\in\mathbf{N}}$ der p^n-ten Teilungspunkte von E entspricht. Durch Vergleich mit anderen Körpertürmen liefert (2.1) jeweils Relationen der Werte der Distribution. Wir werden hier den klassischen Turm der p^n-ten Kreisteilungskörper zum Vergleich heranziehen.

Satz 3.1. *Das Diagramm*

$$\begin{array}{ccc} \mathrm{Aut}(E[p^n]) & \xrightarrow{\det} & (\mathbf{Z}/p^n\mathbf{Z})^* \\ \| & & \| \\ G(\mathbf{Q}(E[p^n])|Q) & \longrightarrow & G(\mathbf{Q}(\mu_{p^n})|\mathbf{Q}) \end{array}$$

ist kommutativ.

Beweis. Der untere Homomorphismus ist wohldefiniert, das heißt $\mu_{p^n} \subseteq \mathbf{Q}(E[p^n])$ laut Silverman, [14], ch. III, co. 8.1.1. Sei

$$(\ ,\ ) : E[p^n] \times E[p^n] \to \mu_{p^n}$$

die Weilpaarung und $\{S, T\}$ eine Basis von $E[p^n]$. Dann ist $\zeta := (S, T)$ eine primitive p^n-te Einheitswurzel. Sei $\sigma \in G(\mathbf{Q}(E[p^n])|\mathbf{Q})$. Dann gibt es eindeutig bestimmte $a, b, c, d \in \mathbf{Z}/p^n\mathbf{Z}$ mit

$$S^\sigma = [a]S + [c]T, \quad T^\sigma = [b]S + [d]T.$$

Es folgt

$$\begin{aligned} \zeta^\sigma &= (S, T)^\sigma \\ &= (S^\sigma, T^\sigma) \\ &= ([a]S + [c]T, [b]S + [d]T) \\ &= (S, S)^{ab} \cdot (S, T)^{ad} \cdot (T, S)^{bc} \cdot (T, T)^{cd} \\ &= (S, T)^{ad-bc} \\ &= \zeta^{ad-bc} \end{aligned}$$

und damit die Behauptung. □

Korollar 3.2. *Sei $a \in (\mathbf{Z}/p^n\mathbf{Z})^*$ und $k \in \mathbf{N}$. Dann gilt*

$$\sum_{\substack{c\in\mathrm{Aut}(E[p^n]) \\ \det c = a}} L_{\{p\}}(1-k, c) = -p^{(k-1)n} \frac{B_k(\langle a/p^n \rangle)}{k}.$$

Beweis. Sei $\sigma \in G(\mathbf{Q}(\mu_{p^n})|\mathbf{Q})$ der Automorphismus mit $\zeta^\sigma = \zeta^a$ für $\zeta \in \mu_{p^n}$. Dann gilt nach Anwendung von Satz 3.1, (2.1), Korollar 2.15 und Satz 2.6 (in dieser Reihenfolge)

$$\begin{aligned}\sum_{\substack{c \in \mathrm{Aut}(E[p^n]) \\ \det c = a}} L_{\{p\}}(1-k, c) &= \sum_{\substack{\tau \in G(\mathbf{Q}(E[p^n])|\mathbf{Q}) \\ \tau|_{\mathbf{Q}(\mu_{p^n})} = \sigma}} L_{\{p\}}(1-k, \tau) \\ &= L_{\{p\}}(1-k, \sigma) \\ &= H(1-k, a \bmod p^n) \\ &= -p^{(k-1)n} \frac{B_k(\langle a/p^n \rangle)}{k},\end{aligned}$$

womit das Korollar gezeigt ist. □

3.3 Distributionen und die matrixwertige Fouriertransformation

In Satz 2.12 haben wir gesehen, dass für jede proendliche Gruppe G der Vektorraum der komplexwertigen Klassendistributionen auf G kanonisch zum Vektorraum aller komplexwertigen Charakterfunktionen von G isomorph ist,

$$\mathrm{ClDist}(G, \mathbf{C}) = \mathrm{ChFct}(G, \mathbf{C}).$$

Dies folgt durch Übergang zum projektiven Limes daraus, dass für jede endliche Gruppe die Charaktere eine Basis des Raumes aller komplexwertiger Klassenfunktionen auf G bilden. Wir werden nun eine Version der Fouriertransformation kennenlernen, mit deren Hilfe man auch Funktionen erhalten kann, die *nicht* konstant auf den Konjugationsklassen sind. Ihre Anwendung findet diese Theorie im Beweis von Lemma 3.13.

Sei G zunächst eine *endliche* Gruppe und K ein algebraisch abgeschlossener Körper der Charakteristik 0. Wir verwenden die folgenden Bezeichnungen:

Definition. $\mathrm{Fct}(G)$ sei der Vektorraum der Abbildungen von G nach K. Elemente von $\mathrm{Fct}(G)$ werden **Funktionen** auf G genannt.

$\mathrm{ClFct}(G)$ sei der Vektorraum derjenigen Funktionen auf G, die auf Konjugationsklassen konstant sind. Elemente von $\mathrm{ClFct}(G)$ werden **Klassenfunktionen** auf G genannt.

$\mathrm{ChFct}(G)$ sei der Vektorraum der Abbildungen, die jedem irreduziblen Charakter von G ein Element von K zuordnen. Elemente von $\mathrm{ChFct}(G)$ werden **Charakterfunktionen** von G genannt.

$\mathrm{MChFct}(G)$ sei der Vektorraum der Abbildungen, die jedem irreduziblen Charakter χ von G einen K-Endomorphismus des Darstellungsraumes V_χ zuordnen. Elemente von $\mathrm{MChFct}(G)$ werden **matrixwertige Charakterfunktionen** von G genannt.

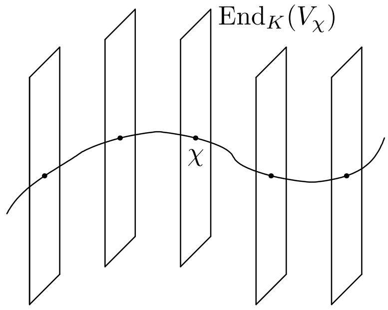

Abbildung 3.1: Veranschaulichung von $\mathrm{MChFct}(G)$.

Man sollte sich Elemente von $\mathrm{MChFct}(G)$ wie Schnitte in ein Vektorraumbündel vorstellen, siehe Abbildung 3.1. Wir haben nun die folgenden Lemmata über verschiedene Versionen der Fouriertransformation:

Lemma 3.3. *Die Abbildung* $\mathrm{SFT} : \mathrm{ClFct}(G) \to \mathrm{ChFct}(G)$*, gegeben durch*

$$(\mathrm{SFT}\, f)(\chi) := \sum_{\sigma \in G} f(\sigma)\chi(\sigma),$$

ist ein Vektorraumisomorphismus. Die Umkehrabbildung ist durch

$$(\mathrm{SFT}^{-1}\, F)(\sigma) = \frac{1}{|G|} \sum_{\chi \, von \, G} F(\chi)\chi(\sigma^{-1})$$

gegeben.

Die nötige Rechnung haben wir im Wesentlichen bereits im Beweis zu Satz 2.12 nachvollzogen. Allerdings soll hier nicht mehr $K = \mathbf{C}$ vorausgesetzt werden und die Bezeichnungen haben sich geändert. Daher hier ein Beweis:

Beweis. Der Vektorraum $\mathrm{ClFct}(G)$ ist mit der Bilinearform $\langle\ ,\ \rangle$ versehen, wobei

$$\langle \varphi, \psi \rangle := \frac{1}{|G|} \sum_{\sigma \in G} \varphi(\sigma)\psi(\sigma^{-1}).$$

Nach Lang, [10], ch. XVIII, th. 5.1 bilden die irreduziblen Charaktere eine Orthonormalbasis von $\mathrm{ClFct}(G)$ bezüglich dieser Bilinearform. Insbesondere haben die beiden Vektorräume $\mathrm{ClFct}(G)$ und $\mathrm{ChFct}(G)$ die gleiche endliche Dimension. Es reicht daher, zum Beispiel $\mathrm{SFT} \circ \mathrm{SFT}^{-1} = 1$ nachzurechnen. Tatsächlich gilt für $F \in \mathrm{ChFct}(G)$ und jeden irreduziblen Charakter χ von G:

$$(\mathrm{SFT}\,\mathrm{SFT}^{-1}\, F)(\chi) = \sum_{\sigma \in G} (\mathrm{SFT}^{-1}\, F)(\sigma)\chi(\sigma)$$

$$
\begin{aligned}
&= \sum_{\sigma\in G} \frac{1}{|G|} \sum_{\psi \,\mathrm{von}\, G} F(\psi)\psi(\sigma^{-1})\chi(\sigma) \\
&= \sum_{\psi \,\mathrm{von}\, G} F(\psi) \frac{1}{|G|} \sum_{\sigma\in G} \psi(\sigma^{-1})\chi(\sigma).
\end{aligned}
$$

Da

$$
\frac{1}{|G|} \sum_{\sigma\in G} \psi(\sigma^{-1})\chi(\sigma) = \langle \chi, \psi \rangle = \begin{cases} 1 & \psi = \chi, \\ 0 & \psi \neq \chi \end{cases}
$$

ist also wie gewünscht $(\mathrm{SFT}\,\mathrm{SFT}^{-1} F)(\chi) = F(\chi)$. □

Lemma 3.4. *Die Abbildung* $\mathrm{MFT} : \mathrm{Fct}(G) \to \mathrm{MChFct}(G)$*, gegeben durch*

$$
(\mathrm{MFT}\, f)(\chi) := \sum_{\sigma\in G} f(\sigma)\rho_\chi(\sigma),
$$

ist ein Vektorraumisomorphismus. Die Umkehrabbildung ist durch

$$
(\mathrm{MFT}^{-1} F)(\sigma) = \frac{1}{|G|} \sum_{\chi \,\mathit{von}\, G} \chi(1) \operatorname{tr}\left(\rho_\chi(\sigma^{-1}) F(\chi)\right)
$$

gegeben.

Beweis. Diese Aussage steht i. W. bei Fulton/Harris, [5], allerdings nur als Übung (ex. 3.32) und nur für $K = \mathbf{C}$. Daher hier der Nachweis: Die Vektorräume $\mathrm{Fct}(G)$ und $\mathrm{MChFct}(G)$ haben die gleiche endliche Dimension. ($|G| = \sum_\chi \chi(1)^2$, siehe Lang, [10], ch. XVIII, Formel vor pr. 4.2.) Also reicht es, zum Beispiel $\mathrm{MFT}^{-1} \circ \mathrm{MFT} = 1$ nachzurechnen. Tatsächlich gilt für alle $f \in \mathrm{Fct}(G)$ und $\sigma \in G$

$$
\begin{aligned}
(\mathrm{MFT}^{-1}\,\mathrm{MFT}\, f)(\sigma) &= \frac{1}{|G|} \sum_{\chi \,\mathrm{von}\, G} \chi(1) \operatorname{tr}\left(\rho_\chi(\sigma^{-1})(\mathrm{MFT}\, f)(\chi)\right) \\
&= \frac{1}{|G|} \sum_{\chi \,\mathrm{von}\, G} \chi(1) \operatorname{tr}\left(\rho_\chi(\sigma^{-1}) \sum_{\tau} f(\tau)\rho_\chi(\tau)\right) \\
&= \frac{1}{|G|} \sum_{\tau\in G} f(\tau) \sum_{\chi \,\mathrm{von}\, G} \chi(1) \operatorname{tr}\left(\rho_\chi(\sigma^{-1}\tau)\right) \\
&= \frac{1}{|G|} \sum_{\tau\in G} f(\tau) \sum_{\chi \,\mathrm{von}\, G} \chi(1)\chi(\sigma^{-1}\tau) \\
&= f(\sigma).
\end{aligned}
$$

Der Übergang zur letzten Zeile ist dabei aus den folgenden Gründen möglich: Nach Lang, [10], ch. XVIII, pr. 4.3 und der vorausgehenden Formel ist

$$
\sum_{\chi \,\mathrm{von}\, G} \chi(1)\chi(\sigma) = \begin{cases} |G| & \sigma = 1, \\ 0 & \sigma \neq 1. \end{cases}
$$

Also folgt

$$\sum_{\chi \text{ von } G} \chi(1)\chi(\sigma^{-1}\tau) = \begin{cases} |G| & \sigma = \tau, \\ 0 & \sigma \neq \tau \end{cases}$$

und in unserer Rechnung bleibt nur der Summand mit $\tau = \sigma$ übrig. □

MFT ist auch ein Isomorphismus von K-Algebren, wenn man $\mathrm{Fct}(G)$ mit dem Faltungsprodukt versieht.

Der folgende Satz beschreibt, wie die beiden Versionen SFT und MFT der Fouriertransformation zusammenhängen. Die kanonische Einbettung $K \to \mathrm{End}_K(V)$, die Skalare mit der zugehörigen Diagonalmatrix identifiziert, wird zur Vereinfachung der Notation ohne besondere Bezeichnung implizit verwendet.

Satz 3.5. *Sei* $I : \mathrm{ChFct}(G) \to \mathrm{MChFct}(G)$ *die durch*

$$(If)(\chi) := \frac{1}{\chi(1)} f(\chi)$$

gegebene Einbettung. Dann ist das Diagramm

$$\begin{tikzcd} \mathrm{Fct}(G) \arrow[r, "\mathrm{MFT}"] & \mathrm{MChFct}(G) \\ \mathrm{ClFct}(G) \arrow[r, "\mathrm{SFT}"] \arrow[u] & \mathrm{ChFct}(G) \arrow[u, "I"'] \end{tikzcd}$$

kommutativ.

Beweis. Sei $f \in \mathrm{ClFct}(G)$. Dann gilt einerseits

$$(\mathrm{SFT}\, f)(\chi) = \sum_{\sigma \in G} f(\sigma) \operatorname{tr} \rho_\chi(\sigma) = \operatorname{tr}\left(\sum_{\sigma \in G} f(\sigma)\rho_\chi(\sigma) \right),$$

andererseits

$$(\mathrm{MFT}\, f)(\chi) = \sum_{\sigma \in G} f(\sigma)\rho_\chi(\sigma).$$

$(\mathrm{MFT}\, f)(\chi)$ ist für $f \in \mathrm{ClFct}(G)$ sogar ein G-Endomorphismus, denn für $\tau \in G$ gilt

$$\begin{aligned} \rho_\chi(\tau) \cdot (\mathrm{MFT}\, f)(\chi) \cdot \rho_\chi(\tau^{-1}) &= \rho_\chi(\tau) \left(\sum_{\sigma \in G} f(\sigma)\rho_\chi(\sigma) \right) \rho_\chi(\tau^{-1}) \\ &= \sum_{\sigma \in G} f(\sigma)\rho_\chi(\tau\sigma\tau^{-1}) \\ &= \sum_{\sigma \in G} f(\tau^{-1}\sigma\tau)\rho_\chi(\sigma) \end{aligned}$$

$$= \sum_{\sigma \in G} f(\sigma) \rho_\chi(\sigma)$$
$$= (\mathrm{MFT}\, f)(\chi).$$

Nach Schurs Lemma ist daher $(\mathrm{MFT}\, f)(\chi)$ ein Skalar. Die Abbildung $z \mapsto \chi(1)^{-1} z$ ist der einzige Schnitt von tr, in dessen Bild nur Skalare liegen. $\square$

Vermutung 3.6. Für proendliche Gruppen G induziert MFT in Analogie zu Satz 2.12 einen Isomorphismus

$$\mathrm{Dist}(G, K) \to \mathrm{MChFct}(G),$$

wobei ein Element von $\mathrm{MChFct}(G)$ jedem Charakter von G, der über ein G_i faktorisiert, einen G-Endomorphismus des zugehörenden Darstellungsraumes zuordnet.

3.4 Maße auf proendlichen Räumen

Sei X ein proendlicher topologischer Raum und R ein kommutativer Ring. In Satz 2.5 haben wir einen kanonischen Isomorphismus zwischen den R-Moduln $\mathrm{Dist}(X, R)$ und $\mathrm{Hom}_R(\mathcal{S}(X, R), R) =: \mathcal{S}(X, R)'$ konstruiert. Gegeben ist dieser Isomorphismus durch das Integral $\int_X f(y)\mu(dy)$ für $\mu \in \mathrm{Dist}(X, R)$ und $f \in S(X, R)$.

Sei nun $R = \mathcal{O}$ der Bewertungsring eines vollständig nichtarchimedisch bewerteten Körpers. Wir setzten in diesem Fall $\mathrm{Meas}(X, \mathcal{O}) := \mathrm{Dist}(X, \mathcal{O})$ und nennen die Elemente von $\mathrm{Meas}(X, \mathcal{O})$ **Maße** auf X mit Werten in $\mathcal{O}$.

Satz 3.7. *Für jedes Maß $\mu \in$ Meas$(X, \mathcal{O})$ ist das zugehörige Funktional $f \mapsto \int f(y)\mu(dy)$ stetig auf $C(X, \mathcal{O})$ fortsetzbar. Wir erhalten also einen Isomorphismus zwischen* $\mathrm{Meas}(X, \mathcal{O})$ *und dem Raum $C(X, \mathcal{O})'$ der stetigen Funktionale auf $C(X, \mathcal{O})$.*

Ähnliche Versionen dieses Satzes findet man bei Hida ([6], § 4.3, pr. 2) und bei Mazur/Swinnerton-Dyer ([11], § 7.1, pr.).

Beweis. Sei $\mu \in \mathrm{Meas}(X, \mathcal{O})$ ein Maß und $\Phi : \mathcal{S}(X, \mathcal{O}) \to \mathcal{O}$ das zugehörige Funktional. Wir versehen $C(X, \mathcal{O})$ mit der Supremumsnorm $\|f\|_\infty := \sup\{f(y) : y \in X\}$. Damit wird $C(X, \mathcal{O})$ ein $\mathcal{O}$-Banachmodul.

Für $y \in X_i$ und i beliebig ist $|\mu(y)| \leq 1$. Für $f \in \mathcal{S}(X, \mathcal{O})$ ist daher $|\Phi(f)| \leq \|f\|_\infty$, das heißt der Operator Φ ist beschränkt (durch 1), also stetig. Φ lässt sich daher eindeutig zu einem stetigen Funktional auf $C(X, \mathcal{O}) = \overline{\mathcal{S}(X, \mathcal{O})}$ fortsetzen. $\square$

Lemma 3.8. *Seien X und Y proendliche topologische Räume, $\varphi : X \to Y$ stetig und $\mu \in$ Meas$(X, \mathcal{O})$ ein Maß auf X. Für $f \in C(Y, \mathcal{O})$ sei $\varphi^* f :=$*

$f \circ \varphi \in C(X, \mathcal{O})$. Dann gibt es ein genau ein Maß $\varphi_* \mu \in \operatorname{Meas}(Y, \mathcal{O})$ auf Y mit der Eigenschaft

$$\int_X (\varphi^* f)(x)\mu(dx) = \int_Y f(y)(\varphi_*\mu)(dy)$$

für alle $f \in C(Y, R)$.

Tatsächlich könnte man $\varphi_*\mu$ explizit angeben, wir haben jedoch keine Verwendung für eine solche Formel.

Beweis. Die linke Seite der Gleichung definiert ein stetiges Funktional auf $C(Y, \mathcal{O})$. Da $C(X, \mathcal{O})' \cong \operatorname{Meas}(X, \mathcal{O})$ wird dieses durch genau ein Maß $\varphi_*\mu$ dargestellt. □

3.5 Eine Konstruktion p-adischer L-Funktionen zu Maßen auf $\mathrm{GL}_2(\mathbf{Z}_p)$

Diese Konstruktion folgt der bei Lang, [9], ch. 4, § 3, vorgestellten. Rufen wir uns zunächst den klassischen Fall in Erinnerung: Die Bernoullidistributionen E_k sind Distributionen auf $\mathbf{Z}_p$ mit Werten in $\mathbf{Q}$. Wählt man $c \in \mathbf{Z}_p^*$ und definiert $E_{k,c}(da) := E_k(da) - c^k E_k(c^{-1}da)$, so haben die Distributionen $E_{k,c}$ Werte in $\mathbf{Z}_p$, sind also Maße. Die Maße $E_{k,c}$ hängen über $E_{k,c}(da) = a^{k-1}E_{1,c}(c^{-1}da)$ zusammen.

Der analoge Sachverhalt für die Standarddistributionen $L_{\{p\},k}$ auf $\mathrm{GL}_2(\mathbf{Z}_p)$ wäre der folgende: Sei $c \in \mathbf{Z}_p^*$. Wir fassen c als Element von $\mathrm{GL}_2(\mathbf{Z}_p)$ auf, so dass $\det c = c^2$. Sei $L_{\{p\},k,c}$ die durch

$$L_{\{p\},k,c}(d\sigma) := L_{\{p\},k}(d\sigma) - (\det c)^k L_{\{p\},k}(c^{-1}d\sigma)$$

gegebene Distribution auf $\mathrm{GL}_2(\mathbf{Z}_p)$ mit Werten in $\mathbf{Q}_p$.

Vermutung 3.9. Die so definierten Distributionen $L_{\{p\},k,c}$ haben Werte in $\mathbf{Z}_p$ für alle k, sind also Maße. Diese Maße hängen über $L_{\{p\},k,c}(d\sigma) = (\det \sigma)^{k-1} L_{\{p\},1,c}(d\sigma)$ zusammen.

Wir betrachten nun allgemein Distributionen mit diesen Eigenschaften. Sei $(F_k)_{k\in\mathbf{N}}$ eine Folge von Klassendistributionen auf $\mathrm{GL}_2(\mathbf{Z}_p)$ mit Werten in $\mathbf{Q}_p$. Für $c \in \mathbf{Z}_p^*$ und $k \in \mathbf{N}$ setze

$$F_{k,c}(d\sigma) := F_k(d\sigma) - (\det c)^k F_k(c^{-1}d\sigma).$$

Die Distributionen F_k sollen nun die folgenden Axiome erfüllen:

A1. Für alle $c \in \mathbf{Z}_p^*$ und $k \in \mathbf{N}$ hat $F_{k,c}$ Werte in $\mathbf{Z}_p$, ist also ein Maß.

A2. $F_{k,c}(d\sigma) = (\det \sigma)^{k-1} F_{1,c}(d\sigma)$ für alle $c \in \mathbf{Z}_p^*$ und $k \in \mathbf{N}$.

Diese Axiome erlauben es, eine p-adische L-Funktion zu konstruieren, siehe Satz 3.11. Zunächst ist dazu jedoch etwas Vorarbeit nötig.

Für $a \in \mathbf{Z}_p^*$ schreiben wir

$$a = \langle a \rangle \cdot \omega(a)$$

mit einer $(p-1)$-ten Einheitswurzel $\omega(a)$. Damit ist ω der Teichmüllercharakter und $\langle a \rangle \in 1 + p\mathbf{Z}_p$. Für $\sigma \in \mathrm{GL}_2(\mathbf{Z}_p)$ sei $\tilde{\omega}(\sigma) := \omega(\det \sigma)$. Damit ist $\tilde{\omega}$ ein eindimensionaler Charakter auf $\mathrm{GL}_2(\mathbf{Z}_p)$.

Definition. Eine Funktion $f : \mathbf{Z}_p \to \mathbf{C}_p$ heißt **p-adisch analytisch** auf $\mathbf{Z}_p$, falls sie um 0 in eine auf ganz $\mathbf{Z}_p$ konvergente Potenzreihe mit Koeffizienten in $\mathbf{C}_p$ entwickelt werden kann. Eine Funktion $g : B \to \mathbf{Z}_p$ heißt **p-adisch meromorph** auf $\mathbf{Z}_p$, falls es p-adisch analytische Funktionen p und q gibt mit $q \neq 0,\ B = \mathbf{Z}_p \setminus q^{-1}(\{0\})$ und $g = p/q$ auf B.

Lemma 3.10. *Sei $\mathcal{O}$ der Bewertungsring von $\mathbf{C}_p$ und $\mu \in \mathrm{Meas}(\mathrm{GL}_2(\mathbf{Z}_p), \mathcal{O})$ ein Maß. Dann ist*

$$\int_{\mathrm{GL}_2(\mathbf{Z}_p)} \langle \det \sigma \rangle^s \mu(d\sigma)$$

als Funktion von s p-adisch analytisch auf $\mathbf{Z}_p$.

Beweis. Nach Lemma 3.8 ist

$$\int_{\mathrm{GL}_2(\mathbf{Z}_p)} \langle \det \sigma \rangle^s \mu(d\sigma) = \int_{\mathbf{Z}_p^*} \langle a \rangle^s (\det_* \mu)(da)$$

für ein Maß $\det_* \mu \in \mathrm{Meas}(\mathbf{Z}_p^*, \mathcal{O})$. Die rechte Seite dieser Gleichung ist p-adisch analytisch nach Lang, [9], ch. 4, le. nach th. 3.1. □

Wir wählen nun feste Einbettungen $\bar{\mathbf{Q}} \to \mathbf{C}$ und $\bar{\mathbf{Q}} \to \bar{\mathbf{Q}}_p \subseteq \mathbf{C}_p$. Damit können wir Charaktere sowohl komplex als auch p-adisch auffassen.

Satz 3.11. *Seien $F_k \in \mathrm{Dist}(\mathrm{GL}_2(\mathbf{Z}_p), \mathbf{Q}_p)$ Distributionen, die die Axiome* A1 *und* A2 *erfüllen. Zu jedem irreduziblen Charakter χ jedes endlichen Quotienten von $\mathrm{GL}_2(\mathbf{Z}_p)$ gibt es dann genau eine p-adisch meromorphe Funktion $L_p(\chi, s)$ auf $\mathbf{Z}_p$, mit der*

$$L_p(\chi, 1-k) = \int_{\mathrm{GL}_2(\mathbf{Z}_p)} (\chi\tilde{\omega}^{-k})(\sigma) F_k(d\sigma) \tag{3.1}$$

für alle $k \in \mathbf{N}$ gilt.

Für den angestrebten Fall $F_k = L_{\{p\},k}$ gilt dabei nach (2.2)

$$\int_{\mathrm{GL}_2(\mathbf{Z}_p)} (\chi\tilde{\omega}^{-k})(\sigma) F_k(d\sigma) = \mathcal{L}_{\{p\}}(K|\mathbf{Q}, \chi\tilde{\omega}^{-k}, 1-k).$$

Falls Vermutung 3.9 zutrifft, erhalten wir also mit Satz 3.11 eine Interpolation spezieller Werte Artin'scher L-Reihen,

$$L_p(1-k,\chi) = \mathcal{L}_{\{p\}}(K|\mathbf{Q}, \chi\tilde{\omega}^{-k}, 1-k).$$

Im Lichte der Warnung in § 2.5 (siehe Seite 30) sollte man dabei beachten, dass mit χ stets auch $\chi\tilde{\omega}^{-k}$ irreduzibel ist, da $\tilde{\omega}$ ein eindimensionaler Charakter ist.

Beweis. Gleichung (3.1) legt die Werte von $L_p(\chi, 1-k)$ auf $\{1-k : k \in \mathbf{N}\}$ fest. Da diese Menge dicht in $\mathbf{Z}_p$ liegt, ist die postulierte Funktion eindeutig bestimmt. Ihre Existenz wird durch die folgende Konstruktion sichergestellt:

Sei $c \in \mathbf{Z}_p^*$ so, dass $\langle \det c\rangle$ keine Einheitswurzel ist. Sei f die durch

$$f(s) := \int_{\mathrm{GL}_2(\mathbf{Z}_p)} \langle \det \sigma\rangle^{1-s} \chi(\sigma) \det(\sigma)^{-1} F_{1,c}(d\sigma)$$

auf $\mathbf{Z}_p$ erklärte Funktion. Wir zeigen, dass die durch

$$L_p(\chi, s) := \left(1 - \frac{\chi(c)\langle \det c\rangle^{1-s}}{\chi(1)}\right)^{-1} f(s) \tag{3.2}$$

gegebene Funktion das Verlangte leistet. (Da wir die Eindeutigkeit bereits eingesehen haben, ist diese Funktion dann insbesondere unabhängig von c.)

Es ist

$$f(s) = \int_{\mathrm{GL}_2(\mathbf{Z}_p)} \langle \det \sigma\rangle^{1-s} \mu(d\sigma)$$

für das Maß $\mu(d\sigma) := \chi(\sigma)\det(\sigma)^{-1} F_{1,c}(d\sigma)$ auf $\mathrm{GL}_2(\mathbf{Z}_p)$. Nach Lemma 3.10 ist f also p-adisch analytisch auf $\mathbf{Z}_p$. Der Nenner $1 - \chi(c)\langle \det c\rangle^{1-s}/\chi(1)$ ist ebenfalls p-adisch analytisch auf $\mathbf{Z}_p$ und nicht die Nullfunktion. Damit ist die durch (3.2) gegebene Funktion p-adisch meromorph. Es bleibt also zu zeigen, dass sie tatsächlich (3.1) erfüllt. Direktes Nachrechnen ergibt

$$\begin{aligned}
f(1-k) &= \int \langle \det \sigma\rangle^{k} \chi(\sigma)(\det\sigma)^{-1} F_{1,c}(d\sigma) \\
&= \int \langle \det \sigma\rangle^{k-1} \chi(\sigma)\tilde{\omega}(\sigma)^{-1} F_{1,c}(d\sigma) \\
&= \int (\det \sigma)^{k-1} (\chi\tilde{\omega}^{-k})(\sigma) F_{1,c}(d\sigma) \\
&= \int (\chi\tilde{\omega}^{-k})(\sigma) F_{k,c}(d\sigma) \\
&= \left(1 - \frac{(\chi\tilde{\omega}^{-k})(c)(\det c)^{k}}{\chi(1)}\right) \int (\chi\tilde{\omega}^{-k})(\sigma) F_k(d\sigma) \\
&= \left(1 - \frac{\chi(c)\langle \det c\rangle^{k}}{\chi(1)}\right) \int (\chi\tilde{\omega}^{-k})(\sigma) F_k(d\sigma).
\end{aligned}$$

Der Übergang zur zweitletzten Zeile wird dabei durch Lemma 3.13 gerechtfertigt, das wir auf den Charakter $\chi\tilde{\omega}^{-k}$ (statt χ) anwenden.

Die Darstellung ρ faktorisiert nach Voraussetzung über eine endliche Gruppe $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$. Das Element c liegt im Zentrum von $\mathrm{GL}_2(\mathbf{Z}_p)$, also liegt sein Bild im Zentrum von $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$. Nach Schurs Lemma ist also $\rho(c)$ eine skalare Matrix α mit einer Einheitswurzel α. Es gilt $\chi(c) = \operatorname{tr}\rho(c) = \chi(1)\alpha$, also ist $\alpha = \chi(c)/\chi(1)$. Nach Wahl von c ist aber $\langle\det c\rangle$ keine Einheitszurzel. Also ist auch $\langle\det c\rangle^k$ keine Einheitswurzel für $k \in \mathbf{N}$. Insgesamt folgt $\chi(c)\langle\det c\rangle^k/\chi(1) \neq 1$ für alle $k \in \mathbf{N}$. Daher verschwindet der Faktor $1 - \chi(c)\langle\det c\rangle^k/\chi(1)$ für kein $k \in \mathbf{N}$. Man kann ihn also herausdividieren und erhält (3.1). □

Zum Beweis von Lemma 3.13 muss man matrixwertige lokal konstante Funktionen integrieren. Diese Integrale sind komponentenweise erklärt. Sie erfüllen die folgende Rechenregel:

Lemma 3.12. *Sei X ein proendlicher topologischer Raum, R ein kommutativer Ring, $A \in M_n(R)$ eine konstante Matrix, $B \in \mathcal{S}(X, M_n(R))$ eine lokal konstante, matrixwertige Funktion und $\mu \in \mathrm{Dist}(X, R)$ eine Distribution. Dann gilt*

$$\int AB(\sigma)\mu(d\sigma) = A\int B(\sigma)\mu(d\sigma).$$

Beweis. Tiefgestellte Indizes ij bezeichnen die (i,j)-te Komponente einer Matrix. Dann kann man komponentenweise nachrechnen

$$\begin{aligned}\left(\int AB(\sigma)\mu(d\sigma)\right)_{ij} &= \int \big(AB(\sigma)\big)_{ij}\mu(d\sigma)\\ &= \int\left(\sum_k A_{ik}B(\sigma)_{kj}\right)\mu(d\sigma)\\ &= \sum_k A_{ik}\int B(\sigma)_{kj}\mu(d\sigma)\\ &= \sum_k A_{ik}\left(\int B(\sigma)\mu(d\sigma)\right)_{kj}\\ &= \left(A\int B(\sigma)\mu(d\sigma)\right)_{ij},\end{aligned}$$

so dass die beiden Seiten der behaupteten Gleichung übereinstimmen. □

Lemma 3.13. *Für jeden irreduziblen Charakter χ jedes endlichen Quotienten von $\mathrm{GL}_2(\mathbf{Z}_p)$ gilt*

$$\int \chi(\sigma)F_{k,c}(d\sigma) = \left(1 - \frac{\chi(c)(\det c)^k}{\chi(1)}\right)\int \chi(\sigma)F_k(d\sigma).$$

Vergleiche für den klassischen Fall Lang, [9], ch. 2, th. 2.4.

Beweis. Sei ρ die zu χ gehörende Darstellung. Es gilt:

$$\begin{aligned}\int \rho(\sigma) F_{k,c}(d\sigma) &= \int \rho(\sigma) F_k(d\sigma) - (\det c)^k \int \rho(\sigma) F_k(c^{-1} d\sigma) \\ &= \int \rho(\sigma) F_k(d\sigma) - (\det c)^k \int \rho(c\sigma) F_k(d\sigma) \\ &= \int \rho(\sigma) F_k(d\sigma) - (\det c)^k \rho(c) \int \rho(\sigma) F_k(d\sigma).\end{aligned}$$

Dabei ist der Übergang zur letzten Zeile der Schritt, der den Übergang von Charakteren zu Darstellungen notwendig macht: Beim Betrachten nichtabelscher Charaktere könnte man c nicht aus dem Integral herausziehen. Für Darstellungen ermöglicht jedoch Lemma 3.12 diesen Schritt. Wir haben also

$$\int \rho(\sigma) F_{k,c}(d\sigma) = \Big(1 - (\det c)^k \rho(c)\Big) \int \rho(\sigma) F_k(d\sigma). \tag{3.3}$$

Wir betrachten nun die einzelnen Terme von (3.3). Die Darstellung ρ faktorisiert über einen endlichen Quotienten G von $\mathrm{GL}_2(\mathbf{Z}_p)$. Es ist also

$$\int \rho(\sigma) F_k(d\sigma) = \sum_{\sigma \in G} \rho(\sigma) F_k(\sigma) = (\mathrm{MFT}\, F_k|_G)(\chi).$$

F_k ist eine Klassendistribution, also folgt aus Satz 3.5, dass

$$\begin{aligned}(\mathrm{MFT}\, F_k|_G)(\chi) &= (I\, \mathrm{SFT}\, F_k|_G)(\chi) \\ &= \frac{1}{\chi(1)} \sum_{\sigma \in G} \chi(\sigma) F_k(\sigma) \\ &= \frac{1}{\chi(1)} \int \chi(\sigma) F_k(d\sigma).\end{aligned}$$

Dabei sind Skalare wieder kanonisch mit der entsprechenden Diagonalmatrix identifiziert. Insgesamt haben wir also gesehen, dass

$$\int \rho(\sigma) F_k(d\sigma) = \frac{1}{\chi(1)} \int \chi(\sigma) F_k(d\sigma).$$

Insbesondere ist also der letzte Term $\int \rho(\sigma) F_k(d\sigma)$ von (3.3) eine skalare Matrix. Da c in $\mathbf{Z}_p^*$, also im Zentrum von $\mathrm{GL}_2(\mathbf{Z}_p)$ liegt, ist auch $F_{k,c}$ eine Klassendistribution. Mit der gleichen Argumentation wie eben folgt

$$\int \rho(\sigma) F_{k,c}(d\sigma) = \frac{1}{\chi(1)} \int \chi(\sigma) F_{k,c}(d\sigma).$$

Damit ist also auch der erste Term $\int \rho(\sigma)F_{k,c}(d\sigma)$ von (3.3) eine skalare Matrix. Folglich muss auch der verbliebene Term $1-(\det c)^k\rho(c)$ eine skalare Matrix sein, also

$$1-(\det c)^k\rho(c) = 1-\frac{(\det c)^k\chi(c)}{\chi(1)}.$$

Die Gleichung (3.3) wird damit zu

$$\frac{1}{\chi(1)}\int \chi(\sigma)F_{k,c}(d\sigma) = \left(1-\frac{(\det c)^k\chi(c)}{\chi(1)}\right)\cdot\frac{1}{\chi(1)}\int \chi(\sigma)F_k(d\sigma).$$

Durchmultiplizieren dieser Gleichung mit $\chi(1)$ liefert das Lemma. □

3.6 Mehrdimensionale abelsche Fouriertransformation

Die Motivation für die Untersuchungen dieses Paragraphen ist die folgende: Das natürliche Objekt der Untersuchung im abelschen Fall sind die Distributionen $L_{\{p\},k}$ auf $G(\mathbf{Q}(\mu_{p^\infty})|\mathbf{Q}) = \mathbf{Z}_p^*$. Jedoch ist es oft handlicher, diese Distribution auf $\mathbf{Z}_p$ fortgesetzt zu betrachten: Entweder setzt man einfach durch 0 fort, oder man verwendet die Hurwitzdistributionen H_k bzw. die Bernoullidistributionen E_k.

Warnung. $\mathbf{Z}_p$ und $\mathbf{Z}_p^*$ hängen auf zwei Arten zusammen: Erstens ist $\mathbf{Z}_p$ ein Faktor und Quotient von $\mathbf{Z}_p^*$ und korrespondiert so zu einer Pro-p-Teilerweiterung $\mathbf{Q}^\infty$ von $\mathbf{Q}(\mu_{p^\infty})|\mathbf{Q}$. Zweitens ist $\mathbf{Z}_p^*$ als Teilmenge in $\mathbf{Z}_p$ enthalten. Dieser zweite Zusammenhang wird hier angesprochen. Insbesondere sollte man die klassischen Bernoullidistributionen *nicht* als zu $\mathbf{Q}^\infty$, sondern als zu $\mathbf{Q}(\mu_{p^\infty})$ gehörend betrachten.

Man kann nun auch die Standarddistributionen $L_{\{p\},k}$ auf $M_2(\mathbf{Z}_p) := \mathbf{Z}_p^{(2,2)} = \mathbf{Z}_p^4$ fortsetzen, und sie eventuell so einfacher beschreiben. Wir entwickeln daher zunächst allgemein die mehrdimensionale abelsche Fourieranalysis (in Dimension d, angestrebt ist der Fall $d=4$). Klassische Vorlagen sind für den eindimensionalen, p-adischen Fall Lang, [9], ch. 4, §§ 1 u. 2, sowie für den mehrdimensionalen, archimedischen Fall Bauer, [2], §§ 22 u. 25.

Sei $d \in \mathbf{N}$ und $\mathcal{O}$ der Bewertungsring von $\mathbf{C}_p$. Sei $\mathfrak{m}$ das maximale Ideal von $\mathcal{O}$.

Definition. Sei $\mu \in \mathrm{Meas}(\mathbf{Z}_p^d, \mathcal{O})$. Dann heißt die Funktion $\Phi : (1+\mathfrak{m})^d \to \mathcal{O}$, gegeben durch

$$\Phi(t) := \int_{\mathbf{Z}_p^d} t^y \mu(dy), \quad \text{wobei } t^y := \prod_{i=1}^d t_i^{y_i},$$

die **charakteristische Funktion** von μ.

Satz 3.14. *Für* $k \in \mathbf{N}_0^d$ *sei*

$$a_k(\mu) := \int_{\mathbf{Z}_p^d} \binom{y}{k} \mu(dy), \quad \textit{wobei } \binom{y}{k} := \prod_{i=1}^{d} \binom{y_i}{k_i}.$$

Dann gilt

$$\Phi(t) = \sum_{k \in \mathbf{N}_0^d} a_k(\mu)(t-1)^k, \quad \textit{wobei } (t-1)^k := \prod_{i=1}^{n} (t_i - 1)^{k_i}.$$

Insbesondere ist Φ *analytisch auf* $(1+\mathfrak{m})^d$.

Beweis. Setze $x_i := t_i - 1$. Dann gilt

$$\begin{aligned}
\Phi(t) &= \int_{\mathbf{Z}_p^d} \prod_{i=1}^{d} t_i^{y_i} \mu(dy) \\
&= \int_{\mathbf{Z}_p^d} \prod_{i=1}^{d} (1+x_i)^{y_i} \mu(dy) \\
&= \int_{\mathbf{Z}_p^d} \prod_{i=1}^{d} \left(\sum_{k=0}^{\infty} \binom{y_i}{k} x_i^k \right) \mu(dy) \\
&= \int_{\mathbf{Z}_p^d} \sum_{k \in \mathbf{N}_0^d} \prod_{i=1}^{d} \binom{y_i}{k_i} x^k \mu(dy) \\
&= \sum_{k \in \mathbf{N}_0^d} a_k(\mu) x^k
\end{aligned}$$

und damit die Behauptung. □

Wendet man Satz 3.14 für $t = 1 := (1, \ldots, 1)$ an, so ergibt sich

$$\int_{\mathbf{Z}_p^d} \mu(dy) = \Phi(1). \tag{3.4}$$

Satz 3.15. *Sei* $t_0 \in (1+\mathfrak{m})^d$. *Die charakteristische Funktion von* $\tilde{\mu}(dy) := t_0^y \mu(dy)$ *ist dann*

$$\tilde{\Phi}(t) = \Phi(t_0 \cdot t),$$

wobei $t_0 \cdot t$ *durch* $(t_0 \cdot t)_i = t_{0,i} t_i$ *gegeben sei.*

Beweis. Für $t \in (1+\mathfrak{m})^d$ gilt

$$\tilde{\Phi}(t) = \int_{\mathbf{Z}_p^d} t^y \tilde{\mu}(dy)$$

$$
\begin{aligned}
&= \int_{\mathbf{Z}_p^d} t^y t_0^y \mu(dy) \\
&= \int_{\mathbf{Z}_p^d} (t_0 \cdot t)^y \mu(dy) \\
&= \Phi(t_0 \cdot t).
\end{aligned}
$$

□

Sei f eine Funktion auf $\mathbf{Z}_p^d$, die über $(\mathbf{Z}/p^n\mathbf{Z})^d$ faktorisiert. Für $\zeta \in \mu_{p^n}^d$ sei

$$\hat{f}(\zeta) := \frac{1}{p^{nd}} \sum_{y \in (\mathbf{Z}/p^n\mathbf{Z})^d} f(y)\zeta^{-y}.$$

Dann gilt

$$f(y) = \sum_{\zeta \in \mu_{p^n}^d} \hat{f}(\zeta)\zeta^y, \tag{3.5}$$

denn

$$
\begin{aligned}
p^{nd} \sum_{\zeta \in \mu_{p^n}^d} \hat{f}(\zeta)\zeta^y &= \sum_{\zeta \in \mu_{p^n}^d} \left(\sum_{\tilde{y} \in (\mathbf{Z}/p^n\mathbf{Z})^d} f(\tilde{y})\zeta^{-\tilde{y}} \right) \zeta^y \\
&= \sum_{\tilde{y} \in (\mathbf{Z}/p^n\mathbf{Z})^d} f(\tilde{y}) \sum_{\zeta \in \mu_{p^n}^d} \zeta^{y-\tilde{y}} \\
&= p^{nd} f(y).
\end{aligned}
$$

Satz 3.16. *Die charakteristische Funktion von $\tilde{\mu}(dy) := f(y)\mu(dy)$ ist*

$$\tilde{\Phi}(t) = \sum_{\zeta \in \mu_{p^n}^d} \hat{f}(\zeta)\Phi(\zeta \cdot t).$$

Beweis. Für $t \in (1 + \mathfrak{m})^d$ gilt

$$
\begin{aligned}
\tilde{\Phi}(t) &= \int_{\mathbf{Z}_p^d} t^y f(y)\mu(dy) \\
&= \int_{\mathbf{Z}_p^d} t^y \left(\sum_{\zeta \in \mu_{p^n}^d} \hat{f}(\zeta)\zeta^y \right) \mu(dy) \\
&= \sum_{\zeta \in \mu_{p^n}^d} \hat{f}(\zeta) \int_{\mathbf{Z}_p^d} (t \cdot \zeta)^y \mu(dy) \\
&= \sum_{\zeta \in \mu_{p^n}^d} \hat{f}(\zeta)\Phi(\zeta \cdot t).
\end{aligned}
$$

□

Sei $d = 4$. Wir identifizieren $\mathbf{Z}_p^4$ mit $M_2(\mathbf{Z}_p)$ durch $(y_1, y_2, y_3, y_4) \mapsto \left(\begin{smallmatrix} y_1 & y_2 \\ y_3 & y_4 \end{smallmatrix}\right)$. Sei ξ eine primitive p-te Einheitswurzel. Wir identifizieren $M_2(\mathbf{F}_p)$ mit μ_p^4 durch $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \mapsto (\xi^\alpha, \xi^\beta, \xi^\gamma, \xi^\delta)$. Ein Einheitswurzelvektor $\zeta \in \mu_p^4 \setminus \{1\}$ heißt **regulär** bzw. **singulär**, falls die entsprechende Matrix diese Eigenschaft hat. Der Einheitswurzelvektor $\zeta = 1 = (1, 1, 1, 1)$ entspricht der Nullmatrix, soll aber weder als singulär noch als regulär gelten. Diese Klassifikation ist unabhängig von der Wahl von ξ.

Das folgende Lemma stellen wir für den Beweis von Satz 3.18 bereit:

Lemma 3.17. *Durchläuft (a, b) die Menge $\mathbf{F}_p \times \mathbf{F}_p$, so nimmt $a \cdot b$ den Wert 0 genau $(2p - 1)$-mal an, jeden anderen Wert genau $(p - 1)$-mal.*

Beweis. Klar. □

Satz 3.18. *Die charakteristische Funktion von $\tilde{\mu}(d\sigma) := 1_{\mathrm{GL}_2(\mathbf{Z}_p)}(\sigma)\mu(d\sigma)$ ist dann*

$$\tilde{\Phi}(t) = (U\Phi)(t) := \frac{(p+1)(p-1)^2}{p^3}\Phi(t) + \frac{1-p}{p^3} \sum_{\substack{\zeta \in \mu_p^4 \\ \zeta \text{ sing.}}} \Phi(\zeta \cdot t) + \frac{1}{p^3} \sum_{\substack{\zeta \in \mu_p^4 \\ \zeta \text{ reg.}}} \Phi(\zeta \cdot t).$$

Beweis. Sei $\zeta \in \mu_p^4$ mit $\zeta \neq 1$. Zu ζ betrachten wir wie oben $\alpha, \beta, \gamma, \delta \in \mathbf{F}_p$ mit $\zeta_1 = \xi^\alpha$, $\zeta_2 = \xi^\beta$, $\zeta_3 = \xi^\gamma$ und $\zeta_4 = \xi^\delta$ für eine feste, primitive p-te Einheitswurzel ξ. Sei $L_\zeta : M_2(\mathbf{F}_p) \to \mathbf{F}_p$ die durch

$$L_\zeta \begin{pmatrix} a & b \\ c & d \end{pmatrix} := \alpha a + \beta b + \gamma c + \delta d$$

gegebene Linearform. Hiermit definieren wir

$$\lambda(\zeta) := \left|\{y \in M_2(\mathbf{F}_p) : L_\zeta(y) = \det y = 0\}\right|.$$

Die Zahl λ hängt nun wie folgt von ζ ab:

$$\lambda(\zeta) = \begin{cases} p(2p-1) & \zeta \text{ singulär}, \\ p^2 & \zeta \text{ regulär}. \end{cases} \tag{3.6}$$

Man sieht das durch die folgende Fallunterscheidung ein: ζ heißt *vom Typ* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, falls $\alpha, \beta \neq 0$ und $\gamma = \delta = 0$. Analog sind weitere Typen für jede (2×2)-Matrix mit Koeffizienten aus $\{0, 1\}$ definiert.

1. Fall: ζ ist vom Typ $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, also singulär. In diesem Fall gilt $\lambda(\zeta) = \left|\left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : ad - bc = 0,\ a = 0\right\}\right|$. Man kann also d beliebig wählen (p Möglichkeiten). Wegen der Bedingung $bc = 0$ gibt es nach Lemma 3.17 genau $2p - 1$ Möglichkeiten für die Wahl von b und c. Insgesamt ist also $\lambda(\zeta) = p(2p - 1)$.

2. Fall: ζ ist vom Typ $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, also regulär. In diesem Fall gilt $\lambda(\zeta) = \left|\left\{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) : ad-bc=0,\ \alpha a+\delta d=0\right\}\right|$. Falls $a=0$, so ist auch $d, ad, bc = 0$, und wegen Lemma 3.17 ergeben sich genau $2p-1$ Möglichkeiten für die Wahl von b und c. Falls $a \neq 0$, so ist sind auch $d, ad, bc \neq 0$, und wegen des gleichen Lemmas ergeben sich für jede der $p-1$ möglichen Werte von a wieder $p-1$ Möglichkeiten für b und c. Insgesamt ist also $\lambda(\zeta) = 2p-1+(p-1)^2 = p^2$.

3. Fall: ζ ist vom Typ $\left(\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right)$, also singulär. In diesem Fall gilt $\lambda(\zeta) = \left|\left\{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) : ad-bc=0,\ \alpha a+\beta b=0\right\}\right|$. Falls $a=0$, so ist auch $b=0$ und c und d können frei gewählt werden, so dass es p^2 Möglichkeiten gibt. Falls $a \neq 0$, so ist auch $b \neq 0$ eindeutig durch a bestimmt, und man kann einen der Werte c und d frei wählen, während der andere durch die Determinantenbedingung bestimmt ist, so dass sich für jede der $p-1$ möglichen Wahlen von a weitere p Möglichkeiten ergeben. Insgesamt ist also $\lambda(\zeta) = p^2+(p-1)p = p(2p-1)$.

4. Fall: ζ ist vom Typ $\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$, also regulär. In diesem Fall gilt $\lambda(\zeta) = \left|\left\{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) : ad-bc=0,\ \alpha a+\beta b+\gamma c=0\right\}\right|$. Durch Auflösen der zweiten Gleichung nach c erhalten wir $c = -\frac{\alpha}{\gamma}a - \frac{\beta}{\gamma}b$. Einsetzen in die erste Gleichung liefert $ad+\frac{\alpha}{\gamma}ab+\frac{\beta}{\gamma}b^2=0$, bzw. äquivalent $a\left(d+\frac{\alpha}{\gamma}b\right) = -\frac{\beta}{\gamma}b^2$. Nach Lemma 3.17 gibt es für $b=0$ also genau $2p-1$ Möglichkeiten zur Wahl von a und d. Für jede der $p-1$ möglichen Wahlen von $b \neq 0$ gibt es nach dem gleichen Lemma $p-1$ gültige Wahlen für a und d. Der Wert von c ist jeweils eindeutig bestimmt, so dass sich insgesamt $\lambda(\zeta) = 2p-1+(p-1)^2 = p^2$ ergibt.

5. Fall: ζ ist vom Typ $\left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right)$. In diesem Fall kann ζ sowohl regulär als auch singulär sein. Wir betrachten eine weitere Symmetrie: $\mathrm{GL}_2(\mathbf{F}_p)$ operiert linear auf $M_2(\mathbf{F}_p)$ durch Linksmultiplikation, und diese Operation lässt $\mathrm{GL}_2(\mathbf{F}_p) \subseteq M_2(\mathbf{F}_p)$ invariant. Ist $\tilde{\zeta}$ der Vektor von Einheitswurzeln mit $L_{\tilde{\zeta}} = L_\zeta \circ \left(\begin{smallmatrix}x&y\\z&u\end{smallmatrix}\right)$ für $\left(\begin{smallmatrix}x&y\\z&u\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_p)$, so gilt daher $\lambda(\zeta) = \lambda(\tilde{\zeta})$. Es gilt

$$\begin{aligned}
L_{\tilde{\zeta}}\begin{pmatrix}a & b\\ c & c\end{pmatrix} &= L_\zeta \begin{pmatrix}x & y\\ z & u\end{pmatrix}\begin{pmatrix}a & b\\ c & c\end{pmatrix}\\
&= L_\zeta \begin{pmatrix}xa+yc & xb+yd\\ za+uc & zb+ud\end{pmatrix}\\
&= (\alpha x+\gamma z)a + (\beta x+\delta z)b\\
&\qquad + (\alpha y+\gamma u)c + (\beta y+\delta u)d,
\end{aligned}$$

so dass L_ζ also zur Matrix

$$\begin{pmatrix}\alpha x+\gamma z & \beta x+\delta z\\ \alpha y+\gamma u & \beta y+\delta u\end{pmatrix}$$

gehört. Seien nun $\alpha, \beta, \gamma, \delta \neq 0$. Wir werden x, y, z und u so wählen, dass $\tilde{\zeta}$ vom Typ $\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$ oder $\left(\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right)$ ist: Wähle $(y,u) \perp (\beta, \delta)$, so dass $\beta y+\delta u = 0$. Man kann dann x und z so wählen, dass $\alpha x+\gamma z \neq 0$ und $\beta x+\delta z \neq 0$. Es ist dann

$$\alpha y + \gamma u = 0 \quad \text{genau dann, wenn} \quad (\alpha, \gamma) \parallel (\beta, \delta),$$

und wir haben den Fall auf den 3. und 4. Fall zurückgeführt.

Alle übrigen Typen von Einheitswurzelvektoren erhält man aus den behandelten durch Symmetrie. Damit ist (3.6) gezeigt.

Wir definieren

$$\nu(\zeta) := |\{y \in \mathrm{GL}_2(\mathbf{F}_p) : L_\zeta(y) = 0\}| \,.$$

$M_2(\mathbf{F}_p)$ zerlegt sich disjunkt in $M_2(\mathbf{F}_p) = \mathrm{GL}_2(\mathbf{F}_p) \cup \{y \in M_2(\mathbf{F}_p) : \det y = 0\}$ und L_ζ hat in $M_2(\mathbf{F}_p)$ genau p^3 Nullstellen. (Dazu haben wir $\zeta \neq 1$ vorausgesetzt.) Also folgt aus (3.6)

$$\nu(\zeta) = p^3 - \lambda(\zeta) = \begin{cases} p(p-1)^2 & \zeta \text{ singulär,} \\ p^2(p-1) & \zeta \text{ regulär.} \end{cases} \tag{3.7}$$

Sei nun $f = 1_{\mathrm{GL}_2(F_p)}$. Aus $\nu(\zeta)$ kann man wie folgt $\hat{f}(\zeta)$ berechnen: Mit $y = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ gilt

$$\begin{aligned} \hat{f}(\zeta) &= \frac{1}{p^4} \sum_{y \in M_2(\mathbf{F}_p)} f(y) \zeta^y \\ &= \frac{1}{p^4} \sum_{y \in \mathrm{GL}_2(\mathbf{F}_p)} \zeta_1^a \zeta_2^b \zeta_3^c \zeta_3^d \\ &= \frac{1}{p^4} \sum_{y \in \mathrm{GL}_2(\mathbf{F}_p)} \xi^{\alpha a + \beta b + \gamma c + \delta d} \\ &= \frac{1}{p^4} \sum_{y \in \mathrm{GL}_2(\mathbf{F}_p)} \xi^{L_\zeta(y)}. \end{aligned}$$

In der letzten Summe liefert jedes y mit $L_\zeta(y) = 0$ einen Summanden 1. $\mathbf{F}_p^*$ operiert auf $\mathrm{GL}_2(\mathbf{F}_p)$ durch Multiplikation. Jede Bahn eines y mit $L_\zeta(y) \neq 0$ liefert einen Summanden -1. Also gilt

$$\begin{aligned} \hat{f}(\zeta) &= \frac{1}{p^4} \left(\nu(\zeta) - \frac{|\mathrm{GL}_2(\mathbf{F}_p)| - \nu(\zeta)}{p-1} \right) \\ &= \frac{1}{p^4} \left(\nu(\zeta) - p(p+1)(p-1) + \frac{\nu(\zeta)}{p-1} \right) \\ &= \frac{\nu(\zeta) - (p+1)(p-1)^2}{p^3(p-1)}. \end{aligned}$$

Aus (3.7) errechnet man dann

$$\hat{f}(\zeta) = \begin{cases} \frac{1-p}{p^3} & \zeta \text{ singulär,} \\ \frac{1}{p^3} & \zeta \text{ regulär.} \end{cases}$$

Für $\zeta = 1$ sieht man direkt, dass

$$\hat{f}(1) = \frac{1}{p^4}\,|\mathrm{GL}_2(\mathbf{F}_p)| = \frac{p(p+1)(p-1)^2}{p^4} = \frac{(p+1)(p-1)^2}{p^3}.$$

Damit ergibt Satz 3.16 das gewünschte Ergebnis:

$$\begin{aligned}\tilde{\Phi}(t) &= \sum_{\zeta\in\mu_p^4} \hat{f}(\zeta)\Phi(\zeta\cdot t)\\ &= \hat{f}(1)\Phi(t) + \sum_{\zeta \text{ sing.}} \hat{f}(\zeta)\Phi(\zeta\cdot t) + \sum_{\zeta \text{ reg.}} \hat{f}(\zeta)\Phi(\zeta\cdot t)\\ &= \frac{(p+1)(p-1)^2}{p^3}\Phi(t) + \frac{1-p}{p^3}\sum_{\zeta \text{ sing.}} \Phi(\zeta\cdot t) + \frac{1}{p^3}\sum_{\zeta \text{ reg.}} \Phi(\zeta\cdot t).\end{aligned}$$

□

Sei nun wieder $d \in \mathbf{N}$ beliebig.

Definition. Sei $k \in \mathbf{N}_0^d$. Dann heißt

$$M_k(\mu) := \int_{\mathbf{Z}_p^d} y^k \mu(dy)$$

das k-te **Moment** von μ. Wir definieren außerdem den Differentialoperator

$$D_k := \prod_{i=1}^{d} \left(t_i \frac{\partial}{\partial t_i}\right)^{k_i}.$$

Satz 3.19. *Sei $k \in \mathbf{N}_0^d$. Die charakteristische Funktion von $y^k\mu(dy)$ ist dann $D_k\Phi$. Insbesondere ist*

$$M_k(\mu) = (D_k\Phi)(1).$$

Beweis. Man muss o. B. d. A. nur den Fall $k = (1, 0, \dots, 0)$ betrachten, der Rest folgt dann aus Symmetriegründen und mit Induktion. Wir möchten eine p-adische Version der Leibnitzformel über Differenziation unter dem Integral verwenden. Um den Gedankengang nicht zu unterbrechen, wird diese unten als Satz 3.21 nachgereicht. Hier nur ihre Anwendung: Seien $t_2, \dots t_d \in 1 + \mathfrak{m}$ fest. Sei $f : (1 + \mathfrak{m}) \times \mathbf{Z}_p^d \to \mathcal{O}$ die durch

$$f(t_1, y) := t^y = t_1^{y_1} \prod_{i=2}^{d} t_i^{y_i}$$

gegebene Funktion. Dann gilt für $t_1 \in 1 + \mathfrak{m}$ und $y \in Z_p^d$:

$$f(t_1, y) = t_1^{y_1} \prod_{i=2}^{d} t_i^{y_i}$$

$$
\begin{aligned}
&= \left(\sum_{k=0}^{\infty} \binom{y_1}{k} (t_1 - 1)^k \right) \prod_{i=2}^{d} t_i^{y_i} \\
&= \sum_{k=0}^{\infty} \left(\binom{y_1}{k} \prod_{i=2}^{d} t_i^{y_i} \right) (t_1 - 1)^k \\
&= \sum_{k=0}^{\infty} f_k(y)(t_1 - 1)^k
\end{aligned}
$$

mit $f_k \in C(\mathbf{Z}_p^d, \mathcal{O})$ gegeben durch $f_k(y) := \binom{y_1}{k} \prod_{i=2}^{d} t_i^{y_i}$. Die Funktion f wird also durch eine Potenzreihe aus $C(\mathbf{Z}_p^d, \mathcal{O})[[t_1 - 1]]$ dargestellt. Damit ist Satz 3.21 für t^y anwendbar. Für $t \in 1 + \mathfrak{m}$ gilt also

$$
\begin{aligned}
(D_k \Phi)(t) &= t_1 \frac{\partial}{\partial t_1} \int_{\mathbf{Z}_p^d} t^y \mu(dy) \\
&= \int_{\mathbf{Z}_p^d} t_1 \frac{\partial}{\partial t_1} \prod_{i=1}^{d} t_i^{y_i} \mu(dy) \\
&= \int_{\mathbf{Z}_p^d} t_1 y_1 t_1^{y_1 - 1} \prod_{i=2}^{d} t_i^{y_i} \mu(dy) \\
&= \int_{\mathbf{Z}_p^d} t^y y_1 \mu(dy).
\end{aligned}
$$

Die Leibnitzformel wurde dabei beim Übergang zur zweiten Zeile angewendet. □

Beispiel 3.20. Im Folgenden eine Anwendung, um die Bedeutung dieser Theorie zu illustrieren: Sei μ ein Maß auf $M_2(\mathbf{Z}_p)$, zum Beispiel ein durch 0 fortgesetztes Maß auf $\mathrm{GL}_2(\mathbf{Z}_p)$. Dann gilt

$$
(\det y)\mu(dy) = y_1 y_4 \mu(dy) - y_2 y_3 \mu(dy),
$$

also ist die charakteristische Funktion von $\tilde{\mu} := (\det y)\mu(dy)$ durch

$$
\begin{aligned}
\tilde{\Phi}(t) &= (D_{(1,0,0,1)}\Phi)(t) - (D_{(0,1,1,0)}\Phi)(t) \\
&= \left(t_1 t_4 \frac{\partial^2}{\partial t_1 \partial t_4} - t_2 t_3 \frac{\partial^2}{\partial t_2 \partial t_3} \right) \Phi(t)
\end{aligned}
$$

gegeben. Betrachtet man zum Beispiel $\mu = L_{\{p\},1,c}$ und ist Vermutung 3.9 zutreffend, so kann man aus der charakteristischen Funktion von $L_{\{p\},1,c}$ diejenigen sämtlicher $L_{\{p\},k,c}$ $(k \in \mathbf{N})$ gewinnen.

Wir zeigen nun die im Beweis zu Satz 3.19 angekündigte Version der Leibnitzformel über Differenziation unter dem Integral. Zur Vereinfachung der Notation betrachten wir hier Funktionen auf $\mathfrak{m}$ anstatt auf $1 + \mathfrak{m}$.

Sei $\mathcal{O}$ der Bewertungsring eines vollständig nichtarchimedisch bewerteten Körpers, X ein proendlicher topologischer Raum und $\mu \in \operatorname{Meas}(X, \mathcal{O})$ ein Maß. Sei $f \in C(X, \mathcal{O})[[t]]$ eine Potenzreihe mit Koeffizienten in $C(X, \mathcal{O})$. Der $\mathcal{O}$-Modul $C(X, \mathcal{O})$ wird ein Banachmodul, wenn man ihn mit der Supremumsnorm $\| \|_\infty$ versieht. Die Potenzreihe f ist konvergent auf $\mathfrak{m}$, stellt also eine Funktion $f : \mathfrak{m} \to C(X, \mathcal{O})$ dar. Eine Funktion, die auf diese Weise entsteht, nennen wir *analytisch*.

Satz 3.21. *Sei $f : \mathfrak{m} \to C(X, \mathcal{O})$ eine analytische Funktion. Dann ist $\int_X f(t, y)\mu(dy)$ nach t differenzierbar und erfüllt*

$$\frac{\partial}{\partial t} \int_X f(t, y)\mu(dy) = \int_X \frac{\partial}{\partial t} f(t, y)\mu(dy). \tag{3.8}$$

Beweis. Sei f durch die Potenzreihe $f = \sum t^i f_i$ mit $f_i \in C(X, \mathcal{O})$ dargestellt. Sei $t_0 \in \mathfrak{m}$ beliebig. Dann gilt:

$$\int \frac{\partial}{\partial t} f(t, y)\bigg|_{t=t_0} \mu(dy) = \int \left(\sum_{i=1}^{\infty} i t_0^{i-1} f_i(y) \right) \mu(dy).$$

Da das Integral linear und stetig auf $C(X, \mathcal{O})$ ist, ist dies

$$\cdots = \sum_{i=1}^{\infty} i t_0^{i-1} \int f_i(y)\mu(dy) = \frac{\partial}{\partial t} \sum_{i=0}^{\infty} t^i \int f_i(y)\mu(dy)\bigg|_{t=t_0}.$$

Wiederum wegen der Linearität und Stetigkeit des Integrals können wir weiterrechnen

$$\cdots = \frac{\partial}{\partial t} \int \left(\sum_{i=0}^{\infty} t^i f_i(y) \right) \mu(dy)\bigg|_{t=t_0} = \frac{\partial}{\partial t} \int f(t, y)\mu(dy)\bigg|_{t=t_0}.$$

□

Literaturverzeichnis

[1] D. Barsky. Fonctions zêta p-adiques d'une classe de rayon des corps de nombres totalement réels. *Groupe d'étude d'analyse ultramétrique* **5** (1977/1978), 16-01–16-36.

[2] H. Bauer. *Wahrscheinlichkeitstheorie.* 5. Aufl., de Gruyter, 2002.

[3] P. Cassou-Noguès. Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. *Inventiones math.* **51** (1979), 29–59.

[4] P. Deligne, K. A. Ribet. Values of abelian L-functions at negative integers over totally real fields. *Inventiones math.* **59** (1980), 227–286.

[5] W. Fulton, J. Harris. *Representation theory: a first course.* Graduate texts in mathematics, Nr. 129. Springer, 1991.

[6] H. Hida. *Elementary theory of L-functions and Eisenstein series.* London Mathematical Society student texts, Nr. 26. Cambridge University Press, 1993.

[7] T. Kubota, H. W. Leopoldt. Eine p-adische Theorie der Zetawerte. *J. reine angew. Math.* **214/215** (1964), 328–339.

[8] S. Lang. *Complex multiplication.* Grundlehren der mathematischen Wissenschaften, Nr. 255. Springer, 1983.

[9] ______. *Cyclotomic fields I and II.* Graduate texts in mathematics, Nr. 121. Springer, 1990.

[10] ______. *Algebra.* 3rd ed., Addison-Wesley, 1993.

[11] B. Mazur, P. Swinnerton-Dyer. Arithmetic of Weil curves. *Inventiones math.* **25** (1974), 1–61.

[12] J. Neukirch. *Algebraische Zahlentheorie.* Springer, 1992.

[13] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones math.* **15** (1972), 259–331.

[14] J. H. Silverman. *The arithmetic of elliptic curves.* Graduate texts in mathematics, Nr. 106. Springer, 1986.

[15] J. Tate. *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$.* Progress in mathematics, Nr. 47. Birkhäuser, 1984.

[16] L. C. Washington. *Introduction to cyclotomic fields.* Graduate texts in mathematics, Nr. 83. Springer, 1982.

Erklärung

Ich habe diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet.

Karlsruhe, 10. Januar 2005

Thomas Bliem