KÖNNEN ζ-FUNKTIONEN DIOPHANTISCHE GLEICHUNGEN LÖSEN?

EINE HINFÜHRUNG ZUR (NICHT-KOMMUTATIVEN) IWASAWA-THEORIE

OTMAR VENJAKOB

1. ζ-Funktionen und diophantische Gleichungen

1.1. **Dirichletsche L-Funktionen.** Als Leibniz 1673 die berühmte Formel

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \cdots = \frac{\pi}{4} \tag{1.1}$$

entdeckte, war er so begeistert, dass er seinen Beruf als Anwalt und Diplomat an den Nagel hängte, um sich ganz der Mathematik zu widmen. Tatsächlich ist diese Formel, die allerdings schon Gregory sowie dem indischen Mathematiker Madhava vor Leibniz bekannt war, ein Beispiel für die mysteriösen Eigenschaften von ζ- oder allgemeiner L-Funktionen, deren Faszination bis heute die Zahlentheorie durchdringt. Um dies zu erläutern, sei N eine natürliche Zahl und $(\mathbb{Z}/N\mathbb{Z})^\times$ die multiplikative Gruppe der Einheiten des Rings $\mathbb{Z}/N\mathbb{Z}$. Ein Homomorphismus abelscher Gruppen

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$$

in die Einheitengruppe der komplexen Zahlen heißt *Dirichlet Charakter* (modulo N). Wir setzen χ auf die Menge der natürlichen Zahlen fort, indem wir $\chi(n)$ den Wert $\chi(n \bmod N)$ zuordnen, falls n und N teilerfremd sind, und den Wert 0 sonst. Die *Dirichletsche L-Funktion bezüglich χ* ist dann definiert als

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

wobei s eine komplexe Variable mit Realteil $\Re(s) > 1$ ist. Diese Funktion besitzt eine meromorphe Fortsetzung auf die ganze komplexe Zahlenebene $\mathbb{C}$ und es gilt die Euleridentität

$$L(s, \chi) = \prod_p \frac{1}{1 - \chi(p)p^{-s}}.$$

Für den trivialen Charakter $\chi \equiv 1$ erhalten wir die *Riemannsche ζ-Funktion*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}, \tag{1.2}$$

während sich die Leibniz-Formel (1.1) nun als

$$L(1, \chi_1) = \frac{\pi}{4} \tag{1.3}$$

schreiben lässt, wenn der Charakter $\chi_1 : (\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\} \to \mathbb{C}^\times$ durch $\chi_1(\overline{1}) = 1$ und $\chi_1(\overline{3}) = -1$ definiert wird.

Date: February 15, 2007.

Dieser Artikel basiert in etwa auf der Antrittsvorlesung des Autors an der Rheinischen Friedrich-Wilhelms-Universität Bonn.

1.2. **Diophantische Gleichungen.** Ein, wenn nicht *das,* zentrale Problem der Zahlentheorie ist das Lösen diophantischer Gleichungen. Betrachten wir etwa für Primzahlen p und q die Gleichung

$$x^p - y^q = 1, \tag{1.4}$$

von der CATALAN 1844 vermutet hat, dass sie neben $3^2 - 2^3 = 1$ keine weitere Lösung in den ganzen Zahlen $\mathbb{Z}$ mit $x, y > 1$ hat. Diese Vermutung wurde 2002 von MIHĂILESCU bewiesen und ist mit der 1994 von WILES et al. bewiesenen Fermatschen Vermutung von 1665, nämlich dass die Gleichung

$$x^p + y^p = z^p \tag{1.5}$$

unter der Bedingung $xyz \neq 0$ für ungerades p keine Lösung über $\mathbb{Z}$ besitzt, zu vergleichen, wenngleich der Beweis letzterer Vermutung ungleich tiefliegender ist. Die Schwierigkeit dieser Gleichungen besteht darin, dass es sich jeweils um ein additives Problem handelt. Ließe es sich in ein multiplikatives Problem verwandeln, könnten wir uns vielleicht die eindeutige Primfaktorzerlegung ganzer Zahlen zunutze machen. Um dies zu ermöglichen, kann man die Gleichungen erst einmal über dem größeren Ring $\mathbb{Z}[\zeta_m]$ für eine geeignete m-te primitive Einheitswurzel ζ_m betrachten. Der Spezialfall

$$x^3 - y^2 = 1 \tag{1.6}$$

der Catalan-Gleichung (1.4) lässt sich zum Beispiel für $\zeta_4 = i$ mit $i^2 = -1$ über dem Ring $\mathbb{Z}[i]$ der Gaußschen Zahlen als

$$x^3 = (y + i)(y - i) \tag{1.7}$$

schreiben, während man über $\mathbb{Z}[\zeta_{p^n}]$ die Zerlegung

$$x^{p^n} + y^{p^n} = (x + y)(x + \zeta_{p^n} y)(x + \zeta_{p^n}^2 y) \cdot \ldots \cdot (x + \zeta_{p^n}^{p^n - 1} y) = z^{p^n} \tag{1.8}$$

erhält.

Nun stellt sich leider heraus, dass $\mathbb{Z}[\zeta_m]$ im allgemeinen kein faktorieller Ring ist, d.h. keine eindeutige Primfaktorzerlegung besitzt. KUMMER hatte deshalb die Idee, Zahlen durch "ideale Zahlen" zu ersetzen: Die eindeutige Zerlegung in Primzahlen wird dann zur eindeutigen Zerlegung von *Idealen* $0 \neq \mathfrak{a} \subseteq \mathbb{Z}[\zeta_m]$ in *Primideale* $\mathfrak{P}_i \neq 0$

$$\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{P}_i^{n_i} \tag{1.9}$$

mit natürlichen Zahlen $n_i \geq 0$. Dabei ist ein Ideal $\mathfrak{a}$ von $\mathbb{Z}[\zeta_m]$ nichts anderes als ein $\mathbb{Z}[\zeta_m]$-Untermodul des Ringes $\mathbb{Z}[\zeta_m]$ selbst, d.h. eine Untergruppe, die zusätzlich unter der Multiplikation mit Elementen des Ringes abgeschlossen ist. Das Produkt $\mathfrak{ab}$ von Idealen $\mathfrak{a}$ und $\mathfrak{b}$ ist definiert als das kleinste Ideal, welches alle Produkte der Form ab von Elementen $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ enthält. Ein Primideal $\mathfrak{p}$ ist schließlich ein Ideal, welches die folgende Eigenschaft besitzt: Umfasst $\mathfrak{p}$ das Produkt $\mathfrak{ab}$, so umfasst $\mathfrak{p}$ bereits einen der Faktoren $\mathfrak{a}$ oder $\mathfrak{b}$. In einem faktoriellen Ring sind alle Ideale $\mathfrak{a}$ Hauptideale, d.h. werden von bereits einem Element a erzeugt

$$\mathfrak{a} = (a).$$

Die Primideale $\mathfrak{p} \neq 0$ entsprechen gerade den Hauptidealen (p), die von einem Primelement p erzeugt werden, und die Relation "$\mathfrak{p}$ umfasst $\mathfrak{a}$" entspricht der herkömmlichen Teilbarkeitsrelation "p teilt a." Das Inverse $\mathfrak{a}^{-1}$ eines Ideals $\mathfrak{a}$ ist definiert als das *gebrochene Ideal*, d.h. der (endlich erzeugte) $\mathbb{Z}[\zeta_m]$-Untermodul von $\mathbb{Q}(\zeta_m)$, bestehend aus allen Elementen x, für die $x \cdot \mathfrak{a} \subseteq \mathbb{Z}[\zeta_m]$ bzw. so dass $\mathfrak{a}^{-1}\mathfrak{a} = \mathbb{Z}[\zeta_m]$ gilt. Lässt man für die Exponenten n_i in (1.9) alle ganzen Zahlen zu, erhält man bezüglich der oben definierten Multiplikation die (abelsche)

Gruppe der gebrochenen Ideale $I(\mathbb{Z}[\zeta_m])$ mit neutralem Element $\mathbb{Z}[\zeta_m]$. Die Idealklassengruppe, d.h. der Quotient

$$Cl(\mathbb{Q}(\zeta_m)) := I(\mathbb{Z}[\zeta_m])/H(\mathbb{Z}[\zeta_m]) \cong Pic(\mathbb{Z}[\zeta_m])^1$$

von $I(\mathbb{Z}[\zeta_m])$ nach der Untergruppe der (gebrochenen) Hauptideale $H(\mathbb{Z}[\zeta_m])$, misst die Abweichung von $\mathbb{Z}[\zeta_m]$, faktoriell zu sein, und ist eine der bedeutendsten arithmetischen Invarianten eines Zahlkörpers; ein grundlegendes Theorem der Zahlentheorie garantiert die Endlichkeit von $Cl(\mathbb{Q}(\zeta_m))$ und wir schreiben $h_{\mathbb{Q}(\zeta_m)} := \#Cl(\mathbb{Q}(\zeta_m))$ für die *Klassenzahl* von $\mathbb{Q}(\zeta_m)$. Nach der globalen Klassenkörpertheorie besitzt die Idealklassengruppe eine weitere bedeutende Interpretation: Sie ist die Galoisgruppe $G(L_m/K_m) = Cl(K_m)$ der maximalen abelschen unverzweigten Erweiterung L_m von $K_m := \mathbb{Q}(\zeta_m)$.

1.3. **Die analytische Klassenzahlformel.** Es ist nun gewissermaßen ein Wunder, dass die Dirichletsche L-Funktion $L(s, \chi_1)$ die Arithmetik in $\mathbb{Z}[i]$ kennt, und daher "weiß", dass die Gleichung (1.6) über $\mathbb{Z}[i]$ und daher erst recht über $\mathbb{Z}$ keine Lösung besitzt: Zuerst bemerken wir, dass wegen des kanonischen Isomorphismus aus der Galoistheorie der Kreisteilungskörper

$$G(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow[\cong]{\kappa_N} (\mathbb{Z}/N\mathbb{Z})^\times \tag{1.10}$$

mit $g(\zeta_N) = \zeta_N^{\kappa_N(g)}$ für alle $g \in G(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ der Charakter χ als ein Charakter der Galoisgruppe aufgefasst werden sollte und somit (für $N = 4$) klar ist, dass $L(s, \chi_1)$ eine (analytische) Invariante von $\mathbb{Q}(i)$ ist. Die *analytische Klassenzahlformel* für imaginär quadratische Zahlkörper liest sich nun als

$$h_{\mathbb{Q}(i)} = \frac{\#\mu(\mathbb{Q}(i))\sqrt{N}}{2\pi} L(1, \chi_1) = \frac{4 \cdot 2}{2\pi} L(1, \chi_1) = \frac{4}{\pi} L(1, \chi_1) = 1$$

mit der Leibniz Formel (1.3) für die letzte Umformung, d.h. der Ring $\mathbb{Z}[i]$ ist faktoriell.
Nun sieht man aber leicht, dass unter der Annahme einer nicht-trivialen Lösung $(x, y) \in (\mathbb{Z}[i])^2$ der Gleichung (1.7) die Faktoren $y+i$ und $y-i$ teilerfremd sind, d.h. wir erhalten eine Darstellung von $y + i$ als 3-te Potenz $y + i = (a + bi)^3$ für $a, b \in \mathbb{Z}$ geeignet[2]. Die Zerlegung dieser Gleichung in Real- und Imaginärteil liefert dann den Widerspruch $y = 0$.

Für Primzahlen p, die die Klassenzahl $h_{\mathbb{Q}(\zeta_p)}$ nicht teilen, zeigt man ganz ähnlich, dass die entsprechende Fermat-Gleichung (1.5) keine nicht-triviale Lösung besitzt. Solche Primzahlen heißen *regulär* und KUMMER hat erkannt, dass die Riemannsche ζ-Funktion "weiß", wann dies der Fall ist: nämlich genau dann, wenn die Zähler der Werte $\zeta(-1), \zeta(-3), \zeta(-5), \ldots, \zeta(4-p)$ nicht durch p teilbar sind. Dabei ist die *Rationalität* dieser Zahlen ein weiteres erstaunliches Phänomen; sie war bereits Euler bekannt. Den ersten nicht-trivialen Zähler erhält man mit der Primzahl 691 für $\zeta(-11)$, die erste irreguläre Primzahl ist allerdings schon $p = 37$. Auch dieses Kummer-Kriterium ist letztlich eine Folge der analytischen Klassenzahlformel sowie gewisser, ebenfalls von Kummer entdeckter p-adischer Kongruenzen zwischen bestimmten Werten von L-Funktionen.
Auch wenn sich natürlich mit obigen Überlegungen weder der allgemeine Fall der Catalan- noch der Fermat-Vermutung beweisen lässt, waren sie historisch ein wichtiger Schritt in der Entwicklung der modernen Zahlentheorie. Insbesondere bilden diese Beobachtungen den *Ausgangspunkt*

[1] Die Gruppe der Isomorphieklassen von Geradenbündeln auf der Kurve $\mathrm{Spec}(\mathbb{Z}[\zeta_m])$ bzw. von lokal-freien $\mathbb{Z}[\zeta_m]$-Moduln vom Rang 1.

[2] Zuerst stellt man fest, dass x kongruent 1 modulo 4, also ungerade ist. Da der größte gemeinsame Teiler d von $y+i$ und $y-i$ wegen (1.7) die Zahl x teilt, ist er "ungerade". Andererseits teilt d auch $2 = -i\{(y+i)-(y-i)\}$, ist also "gerade", Widerspruch! Ferner ist zu beachten, dass die Einheiten von $\mathbb{Z}[i]$ genau aus $\{\pm 1, \pm i\}$ bestehen und allesamt dritte Potenzen in $\mathbb{Z}[i]$ sind.

der klassischen Iwasawa-Theorie, die sich um ein tieferes Verständnis dieser Beziehung zwischen speziellen Werten komplexer L-Funktionen und Idealklassengruppen oder allgemeineren kohomologischen Invarianten von Zahlkörpern via p-adische L-Funktionen bemüht. Bevor wir darauf näher eingehen, soll im nächsten Abschnitt zur Motivation kurz der Funktionenkörperfall beschrieben werden. Dabei lassen wir uns wie IWASAWA von der bestechenden *Analogie zwischen Zahlkörpern,* d.h. den endlichen Erweiterungen von $\mathbb{Q}$, *und den Funktionenkörpern* $K(C)$ von Kurven C über dem endlichem Körper $\mathbb{F}_l$, d.h. den endlichen Erweiterungen des rationalen Funktionenkörpers $\mathbb{F}_l(X) = K(\mathbb{P}^1_{\mathbb{F}_l})$ in einer Variablen, leiten und versuchen anschließend, die geometrische Intuition, die wir uns im Falle der Kurven zunutze machen, auf den Zahlkörperfall zu übertragen.

2. Die Zetafunktion von Kurven über endlichen Körpern

Sei also C eine glatte, projektive Kurve über dem endlichem Körper $\mathbb{F}_l$, d.h. eine singularitätenfreie Kurve, die sich als abgeschlossener Teil in einen projektiven Raum $\mathbb{P}^n_{\mathbb{F}_l}$ einbetten lässt. Wir fixieren eine solche Einbettung und reden dann von den Koordinaten der Punkte $C(\overline{\mathbb{F}_l}) \subseteq \mathbb{P}^n_{\mathbb{F}_l}(\overline{\mathbb{F}_l})$ von C, wobei $\overline{\mathbb{F}_l}$ einen algebraischen Abschluss von $\mathbb{F}_l$ bezeichne. Mit

$$N_r := \#C(\mathbb{F}_{l^r})$$

werde die Anzahl der (endlich vielen) Punkte von C mit Koordinaten in dem Körper $\mathbb{F}_{l^r}$ mit l^r Elementen bezeichnet. Diese Menge besteht also gerade aus den Fixpunkten des (geometrischen) Frobeniusisomorphismus ϕ^r, der jede Koordinate x_i auf $x_i^{l^r}$ abbildet. Die Idee, eine geeignete Kohomologietheorie $\mathbb{H}^\bullet(C)$ mit Koeffizienten in Charakteristik 0 zu konstruieren, so dass man die Anzahl der Fixpunkte durch eine Lefschetz-Spur-Formel bestimmen kann, geht auf GROTHENDIECK zurück und wurde von DELIGNE ausgeführt:

$$N_r = \sum_{n=0}^{2} (-1)^n \mathrm{Tr}(\phi^r | \mathbb{H}^n(C)). \tag{2.11}$$

Dabei handelt es sich um die sogenannte étale Kohomologie von $\overline{C} := C \times_{\mathbb{F}_l} \overline{\mathbb{F}_l}$, d.h. von C nach Konstantenerweiterung nach $\overline{\mathbb{F}_l}$. Es sei an dieser Stelle daran erinnert, dass $\overline{\mathbb{F}_l} = \mathbb{F}_l(\mu)$ durch Adjunktion aller (prim zu p) Einheitswurzeln entsteht. Den nicht-trivialen Primidealen im Zahlkörperfall entsprechen nun die *abgeschlossenen Punkte* $|C|$ von C. Beim Übergang zu $\overline{C}$ "zerlegt" sich $x \in |C|$ in $\mathrm{Grad}(x)$ viele Punkte in $|\overline{C}| = C(\overline{\mathbb{F}_l})$, deren sämtliche Koordinaten bereits in $k(x)$, dem Restklassenkörper von x liegen; überdies ist $k(x)$ minimal mit dieser Eigenschaft und hat den Körpergrad $\mathrm{Grad}(x)$ über $\mathbb{F}_l$.

Die ζ-Funktion von C, die die Fixpunktanzahlen N_r codiert, ist definiert als

$$\zeta_C(s) = \prod_{x \in |C|} \frac{1}{1 - (\#k(x))^{-s}} = \exp(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}) \tag{2.12}$$

für $s \in \mathbb{C}$ mit $\Re(s) > 1$ und $t = l^{-s}$ (vgl. das Eulerprodukt mit dem in (1.2)); der zweite Ausdruck folgt aus dem ersten mittels der Identität

$$-\ln(1-T) = \sum_{r=1}^{\infty} \frac{T^r}{r} \tag{2.13}$$

und den Formeln $\#k(x) = l^{\mathrm{Grad}(x)}$ und $N_r = \sum_{x \in |C|, \mathrm{Grad}(x) | r} \mathrm{Grad}(x)$. In dem einfachen Beispiel $C = \mathbb{P}^1_{\mathbb{F}_l}$ ist die Anzahl

$$\#N_r = \#\mathbb{P}^1(\mathbb{F}_{l^r}) = \#\mathbb{A}^1(\mathbb{F}_{l^r}) + 1 = l^r + 1$$

um 1 größer ist als die entsprechende Anzahl für den affinen Raum $\mathbb{A}^1$. Aufgrund der Identität (2.13) erhalten wir daher aus der zweiten Formel in der Definition (2.12)

$$\zeta_{\mathbb{P}^1_{\mathbb{F}_l}}(s) = \frac{1}{(1-t)(1-lt)}$$

eine Darstellung als rationale Funktion in t.

Benutzt man allgemeiner für eine beliebige Kurve C die Spurformel (2.11) sowie die Identität $\ln(\det(1-\phi t|\mathbb{H}^n)^{-1}) = \sum_{n=1}^{\infty} \mathrm{Tr}(\phi^n|\mathbb{H}^n))\frac{t^n}{n})$ erhält man nicht nur die Rationalität von

$$\zeta_C(s) = \prod_{n=0}^{2} \det(1-\phi t|\mathbb{H}^n(C))^{(-1)^{n+1}} = \frac{\det(1-\phi t|\text{“}Pic^0(\overline{C})\text{”})}{(1-t)(1-lt)} \ \in \ \mathbb{Q}(t),$$

sondern eine Darstellung als alternierendes Produkt von charakteristischen Polynomen der Operation von ϕ auf den Kohomologiegruppen. Diese kann man explizit bestimmen und der entscheidende Beitrag $\frac{\zeta_C}{\zeta_{\mathbb{P}^1_{\mathbb{F}_l}}}$, nämlich im Grad 1, ist durch die Jacobische J_C von C gegeben, deren abgeschlossenen Punkte $J_C(\overline{\mathbb{F}_l})$ mit der Picard-Gruppe $Pic^0(\overline{C})$ der Geradenbündel vom Grad 0 identifiziert werden können, also das Analogon der Idealklassengruppe im Zahlkörperfall bilden. Insbesondere hat ζ_C Pole genau in $s = 0, 1$ und jede Nullstelle α erfüllt die “Riemannsche Vermutung” $|\alpha| = l^{\frac{1}{2}}$ bezüglich des komplexen Absolutbetrages (für jede Einbettung nach $\mathbb{C}$), d.h. $\Re(s) = \frac{1}{2}$. Diese Ergebnisse erzielte Weil 1948 für Kurven, für höher-dimensionale Varietäten wurden diese als *Weil-Vermutung* bekannten Aussagen von Deligne bewiesen.

Wie oben bereits erwähnt hat die Analogie zwischen Funktionenkörpern und Zahlkörpern immer wieder Anstöße für die Zahlentheorie gegeben. Auch Iwasawa hat sich von der Geometrie inspirieren lassen und sich gefragt, ob es auch für die Riemannsche ζ-Funktion solch eine einfache geschlossene Darstellung gibt. Für eine *p-adische Version* der Riemannschen ζ-Funktion trifft dies tatsächlich zu, wie wir im Folgenden beschreiben wollen.

3. Die p-adische ζ-Funktion und die Hauptvermutung von Iwasawa

Wir haben im Funktionenkörperfall Einheitswurzeln adjungiert, um uns in eine “geometrische Situation” zu bringen, in der der Frobeniusautomorphismus operiert. Ganz analog betrachten wir nun für eine ungerade Primzahl p den Körperturm

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_p) \subseteq \ldots \subseteq F_n := \mathbb{Q}(\zeta_{p^n}) \subseteq F_{n+1} := \mathbb{Q}(\zeta_{p^{n+1}}) \subseteq \ldots \subseteq F_\infty := \bigcup_{n\geq 0} F_n.$$

Wir schreiben $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ für den Ring der p-adischen ganzen Zahlen, d.h. der (formalen) Reihen $\sum_{n=0}^{\infty} a_n p^n$ mit $0 \leq a_i < p$, und $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$ für seinen Quotientenkörper. Dann gilt $\mathbb{Z}_p^\times = \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times$ und die Isomorphismen (1.10) für $N = p^n$, $n \geq 0$, induzieren einen Isomorphismus

$$\kappa : G := G(F_\infty/\mathbb{Q}) \xrightarrow{\cong} \mathbb{Z}_p^\times = \mu_{p-1} \times (1+p\mathbb{Z}_p)\big(\cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p\big),$$

der durch die Bedingung $g(\zeta_{p^n}) = \zeta_{p^n}^{\kappa(g)}$ für alle $g \in G$ und alle $n \geq 0$ eindeutig bestimmt ist und als der *(p-)zyklotomische Charakter* bezeichnet wird, wobei μ_{p-1} die Gruppe der $(p-1)$ten Einheitswurzeln bezeichnet. Die Torsionsuntergruppe Δ von G kann mit $G(F_1/\mathbb{Q})$ identifiziert werden und das Einschränken von κ auf Δ liefert den Teichmüller-Charakter $\omega := \kappa_{|\Delta} : \Delta \cong \mu_{p-1} \subseteq \mathbb{C}^\times$, der in natürlicher Weise via (1.10) als Dirichlet-Charakter aufgefasst werden kann.

Die Untergruppe $\Gamma := G(F_\infty/F_1)$ ist isomorph zu $\mathbb{Z}_p$ und wir bezeichnen mit γ einen topologischen Erzeuger; dieser wird die Rolle von ϕ aus dem Funktionenkörperfall übernehmen. Das zentrale Bindeglied zwischen L-Funktion und Idealklassengruppe stellt die *Iwasawa-Algebra*

$$\Lambda(G) := \varprojlim_n \mathbb{Z}_p[G/\Gamma^{p^n}] \cong \mathbb{Z}_p[\Delta][[T]]$$

dar, wobei die Identifikation mit dem Potenzreihenring via $T := \gamma - 1$ von der Wahl von γ abhängt. Hier bezeichnet $\mathbb{Z}_p[U]$ für eine beliebige Gruppe U die Gruppenalgebra von U mit Koeffizienten in $\mathbb{Z}_p$ und Γ^{p^n} ist die eindeutige Untergruppe von Γ mit Index $(\Gamma : \Gamma^{p^n}) = p^n$.

3.1. **Die *analytische* p-adische ζ-Funktion.** Der Teichmüller-Charakter ω induziert ein (primitives, vollständiges) System von Idempotenten

$$e_{\omega^i} := \frac{1}{p-1} \sum_{\delta \in \Delta} \omega^i(\delta)\delta^{-1} \in \mathbb{Z}_p[\Delta] \subseteq \Lambda(G), \quad 1 \leq i \leq p-1,$$

von $\Lambda(G)$, so dass sich für den maximalen Quotientenring $Q(G)$ von $\Lambda(G)$ die folgende Zerlegung in ein Produkt von Ringen jeweils isomorph zum Quotientenkörper $Q(\mathbb{Z}_p[[T]])$ von $\mathbb{Z}_p[[T]]$ ergibt:

$$Q(G) \cong \prod_{i=1}^{p-1} Q(\mathbb{Z}_p[[T]])e_{\omega^i}.$$

Die Elemente von $Q(G)$, d.h. Elemente der Form $Z = \sum_{i=1}^{p-1} Z_i(T)e_{\omega^i}$ lassen sich als Funktionen auf $\mathbb{Z}_p$ auffassen, die für $n \in \mathbb{N}$ durch

$$Z(n) := Z_{i(n)}(\kappa(\gamma)^n - 1) \in \mathbb{Q}_p \cup \{\infty\}$$

gegeben sind, wenn $1 \leq i(n) \leq p-1$ die eindeutige Zahl mit $i(n) \equiv n \bmod (p-1)$ bezeichnet. Dabei sind die einzelnen "Zweige" $Z_i(\kappa(\gamma)^s - 1)$ meromorphe Funktionen in $s \in \mathbb{Z}_p$.

Kubota, Leopoldt und Iwasawa zeigen nun, dass es eine eindeutige *p-adische ζ-Funktion* $\zeta_p \in Q(G)$ gibt, derart dass für negative ganze Zahlen k

$$\zeta_p(k) = (1 - p^{-k})\zeta(k)$$

gilt, d.h. dass ζ_p - bis auf den Eulerfaktor bei p - die Riemannsche ζ-Funktion p-adisch interpoliert. Der Index p soll hier also in suggestiver Form den Übergang der Funktion ζ zu seinem p-adischen Analogon ζ_p andeuten. Auch wenn das Symbol ζ_p andererseits bereits eine p-te primitive Einheitswurzel bezeichnet, dürfte die jeweils aktuelle Bedeutung stets aus dem Zusammenhang ersichtlich sein. Genauer ist die i-te Komponente $\zeta_{p,i}(\kappa(\gamma)^s - 1)$ gerade die *p-adische L-Funktion* $L_p(s, \omega^{1-i})$ zum Dirichlet-Charakter ω^{1-i}, die der Interpolationseigenschaft

$$L_p(k, \omega^{1-i}) = (1 - \omega^{1-i}(p)p^{-k})L(k, \omega^{1-i})$$

für negative ganze Zahlen k mit $k \equiv 1 \bmod (p-1)$ genügt. Insbesondere verschwindet für gerades i aufgrund trivialer Nullstellen der L-Funktionen die Komponente $\zeta_{p,i}$ bzw. die p-adische L-Funktion $L_p(s, \omega^{1-i})$ identisch.

3.2. **Die *algebraische* p-adische ζ-Funktion und die Hauptvermutung.** Während in der geometrischen Situation der Frobenius auf $Pic^0(\overline{C})$ operiert, erhalten wir nun eine Operation von γ auf dem Analogon

$$X := \varprojlim_n Cl(F_n)(p) \cong G(L_\infty/F_\infty),$$

wobei nach globaler Klassenkörpertheorie L_∞ die maximal unverzweigte abelsche pro-p-Erweiterung von F_∞ ist. Der Tatsache entsprechend, dass die geraden Komponenten von ζ_p identisch verschwinden, müssen wir von X zu der Untergruppe $X^-(= \bigoplus_{i \text{ ungerade}} e_i X)$ übergehen, auf

der die komplexe Konjugation, d.h. das eindeutig bestimmte Element in Δ der Ordnung 2, mit dem Eigenwert -1 operiert. Es ist bekannt, dass $X^- \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ ein endlich dimensionaler $\mathbb{Q}_p$-Vektorraum ist. Ferner bezeichne

$$\mathbb{Q}_p(1) := (\varprojlim_n \mu_{p^n}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

den Tate-Modul, d.h. den 1-dimensionalen $\mathbb{Q}_p$-Vektorraum, auf dem G und daher Δ und γ mittels des zyklotomischen Charakters κ operiert. Für einen endlich dimensionalen $\mathbb{Q}_p$-Vektorraum M, auf dem γ und Δ von einander unabhängig operieren, bezeichnen wir mit

$$\det(1-\gamma T|M) \in \mathbb{Q}_p[\Delta][T] \cong \prod_{i=1}^{p-1} \mathbb{Q}_p[T]e_{\omega^i}$$

das charakteristische Polynom mit Koeffizienten in $\mathbb{Q}_p[\Delta]$, dessen i-te Komponente bezüglich der Wedderburn-Zerlegung das Polynom $\det(1-\gamma T|e_{\omega^i}M) \in \mathbb{Q}_p[T]$ darstellt. Schließlich schreiben wir $a \approx b$ für $a, b \in Q(G)^\times$, wenn a und b bis auf eine Einheit in $\Lambda(G)$ übereinstimmen. Damit lässt sich die von Mazur und Wiles 1986 bewiesene **Hauptvermutung der Iwasawa-Theorie** wie folgt formulieren:

$$\zeta_p \approx \frac{\det(1-\gamma T|X^- \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)}{\det(1-\gamma T|\mathbb{Q}_p(1))} = \prod \det(1-\gamma T|\mathbb{H}^i)^{(-1)^{i+1}}$$

für gewisse Galois- bzw. étale Kohomologiegruppen $\mathbb{H}^i$. Damit kann auch die p-adische ζ-Funktion im wesentlichen durch eine Art *Spurformel* beschrieben werden. Der Ausdruck auf der rechten Seite wird auch als die *algebraische* p-adische ζ-Funktion bezeichnet und die Hauptvermutung besagt dann, dass die analytische und algebraische p-adische ζ-Funktion im wesentlichen übereinstimmen. Dieses Theorem manifestiert einen tiefliegenden Zusammenhang zwischen einem p-adisch *analytischen* Objekt, nämlich ζ_p, und der rein *algebraisch* definierten Invariante X, beides Abbildungen oder "Schatten" der multiplikativen Gruppe $\mathbb{G}_m$, deren Torsionsuntergruppe gerade aus den Einheitswurzeln besteht und deren p-adischer Tate-Modul $\mathbb{Q}_p(1)$ gerade die Koeffizienten der obigen Kohomologie-Theorie liefert. Die Hauptvermutung manifestiert mit anderen Worten die Tatsache, dass sich die analytische Klassenzahlformel gut in p-adischen Familien ausdehnt.

4. Nicht-kommutative Iwasawa-Theorie

Anstelle der multiplikativen Gruppe $\mathbb{G}_m$ kann man zum Beispiel auch zu einer elliptischen Kurve E über $\mathbb{Q}$ oder allgemeiner zu einer p-adischer Darstellung $\rho : G_{\mathbb{Q}} \to GL(V)$ übergehen und sich fragen, was eine analoge Iwasawa-Theorie bedeuten soll. Hier ist V ein endlich dimensionaler $\mathbb{Q}_p$-Vektorraum, und zwar $\mathbb{Q}_p(1)$ im Falle von $\mathbb{G}_m$ und der Tate-Modul $V_p(E) = \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, E(\bar{\mathbb{Q}}))$ im Falle von E.
Hierbei sind zwei Rollen zu unterscheiden: Zum einen kann man diese Objekte über demselben (zyklotomischen) Körperturm studieren, indem man diese Darstellungen als neue Koeffizienten in die Galoiskohomologie einsetzt, zum anderen kann man den zyklotomischen Körperturm durch die p-adische Lie-Erweiterung ersetzen, die durch ρ definiert wird: K_∞ ist der Fixkörper von $\overline{\mathbb{Q}}$ unter $\ker(\rho)$, und schließlich lassen sich beide Modifikationen kombinieren.
Während für den ersten Fall eine Beschreibung - zumindest vermutungsweise - von Perrin-Riou, Greenberg, Colmez et al. schon seit langem bekannt war, führt der zweite Fall schon auf Probleme bei der Formulierung einer Hauptvermutung, da nun die Iwasawa-Algebra von

$\mathcal{G} := G(K_\infty/\mathbb{Q})$ im allgemeinen nicht-kommutativ ist, die Methoden der kommutativen Algebra also nicht greifen, und daher nicht ohne weiteres klar ist, welcher Art Objekte die algebraische und analytische p-adische L-Funktion sein sollen. Schließlich konnte dieses Problem mit Methoden der algebraischen K-Theorie durch Arbeiten von Burns, Flach, Huber, Kings, Fukaya, Kato, Coates, Sujatha und dem Autor teilweise gelöst werden, siehe die Übersichtsartikel [2, 1][3]. An dieser Stelle sei nur noch erwähnt, dass der analytischen Klassenzahlformel im Fall von $\mathbb{G}_m$ die Birch und Swinnerton-Dyer Vermutung im Falle einer elliptischen Kurve E und die Tamagawa-Zahl Vermutung von Bloch und Kato im allgemeinen Fall entspricht.
Völlig rätselhaft ist allerdings bis heute die Existenz der analytischen p-adischen L-Funktion. Betrachten wir dazu abschließend die einfachste Situation einer p-adischen Lie-Erweiterung der Dimension zwei und fragen uns, was die Existenz dieser Funktion konkret zu bedeuten hat: K_∞ enthalte F_∞, sei ein CM-Körper und die Galoisgruppe $\mathcal{G} = G(K_\infty/\mathbb{Q})$ sei isomorph zu einem semidirekten Produkt der Form $\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times$. Ferner setzen wir $H := G(K_\infty/F_\infty) \cong \mathbb{Z}_p$. Dann gibt es einen endlich erzeugten $\Lambda(\mathcal{G})$-Modul $X(K_\infty)$ definiert über K_∞ analog zu dem $\Lambda(G)$-Modul X über F_∞. Burns, Schneider und der Autor haben gezeigt, dass jeder Lift $\widetilde{\gamma}$ von $\gamma \in G$ nach $\mathcal{G}$ über die Vorschrift $x \otimes y \mapsto x \otimes y - x\widetilde{\gamma}^{-1} \otimes \widetilde{\gamma} y$ einen $\Lambda(\mathcal{G})$-Homomorphismus

$$\Lambda(\mathcal{G}) \otimes_{\Lambda(H)} X(K_\infty) \xrightarrow{\text{“}1-\gamma\text{”}} \Lambda(\mathcal{G}) \otimes_{\Lambda(H)} X(K_\infty)$$

induziert, der aufgefasst in einer geeigneten K-Gruppe als das “charakteristische Polynom der Operation von γ auf $X(K_\infty)$” angesehen werden kann und die *nicht-kommutative* algebraische p-adische L-Funktion von $\mathbb{G}_m$ über K_∞ definiert, die also wiederum die Form einer *Spurformel* hat. Nach Berechnungen dieser K-Gruppe durch Kato ist die Existenz der analytischen p-adischen L-Funktion äquivalent dazu, dass die herkömmlichen p-adischen L-Funktionen $L_p(s, \chi)$ aus der zyklotomischen Theorie für gewisse Charaktere χ von H (komplizierte) völlig *neuartige Kongruenzen* eingehen. Die Gültigkeit einer entsprechenden *nicht-kommutativen* Hauptvermutung ist dann äquivalent zu der Gültigkeit der klassischen (abelschen) Hauptvermutung für all diese Charaktere (über variierenden total reellen Zahlkörpern innerhalb F_∞).

References

1. O. Venjakob, *From the Birch and Swinnerton-Dyer Conjecture over the Equivariant Tamagawa Number Conjecture to non-commutative Iwasawa theory*, to appear in ‘L-functions and Galois representations’, Proceedings of the 2004 Durham Symposium, C.U.P. 4
2. ———, *From classical to non-commutative Iwasawa theory - an introduction to the GL_2 main conjecture*, 4ECM Stockholm 2004, EMS, 2005. 4, 3

Universität Bonn, Mathematisches Institut, Beringstr. 1, 53115 Bonn.

E-mail address: venjakob@math.uni-bonn.de

URL: http://www.math.uni-bonn.de/people/venjakob

[3] In [2] hat sich ein fataler Fehler eingeschlichen: In der Formulierung der “Main Conjecture” ist X^+ durch X^- zu ersetzen!