kleine AG 'Algebraische Geometrie und Zahlentheorie'
am 29.10.2005 in Bonn

Modulare Elliptische Kurven

Sei E eine über dem Körper $\mathbb{Q}$ definierte elliptische Kurve, gegeben durch eine Weierstrass-Gleichung

$$y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Q},\ \Delta := 4a^3 + 27b^3 \neq 0.$$

Zu E assoziiert man eine L-function

$$L(E/\mathbb{Q}, s) \ = \prod_p L(E/\mathbb{Q}_p, s) \ = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

wobei a_n ganze Zahlen sind. Der Euler-Faktor $L(E/\mathbb{Q}_p, s)$ ist definiert in Abhängigkeit von der Reduktion von E modulo p. Wenn E bei p gute Reduktion hat (also z.B. wenn p nicht im Nenner von a, b auftritt und $\Delta \not\equiv 0 \pmod{p}$), so definiert man

$$L(E/\mathbb{Q}_p, s) := \frac{1}{1 - a_p p^{-s} + p^{1-2s}}, \qquad a_p := p + 1 - |E(\mathbb{F}_p)|.$$

Die elliptische Kurve E heisst *modular*, wenn die Folge ganzer Zahlen a_n die Fourier-Koeffizienten einer normierten Spitzenform vom Gewicht zwei sind,

$$f(\tau) \ = \sum_{n=0}^{\infty} a_n e^{2\pi i n \tau}, \qquad (a_0 = 1)$$

welche simultane Eigenform für alle Heckeoperatoren ist.

Die berühmte Vermutung von Taniyama-Weil besagt, daß jede elliptische Kurve über $\mathbb{Q}$ modular ist. Sie ist mittlerweile in vollständiger Allgemeinheit bewiesen, durch Arbeiten von Wiles, Taylor-Wiles und Breuil-Conrad-Diamond-Taylor. Nach Argumenten von Frey, Serre und Ribet kann man mit diesen Ergebnissen den Satz von Fermat beweisen.

Ziel der AG wird aber eher sein, die *Aussage* der Taniyama-Weil-Vermutung zu verstehen, insbesondere die Äquivalenz der verschiedenen Definitionen von Modularität.

Für alle Vorträge sind 50 min. vorgesehen, und alle im Programm erwähnten Punkte sollten angesprochen werden. Im Zweifelsfall kann man immer auf Beweise verzichten. Für die ersten beiden Vorträge benötigt man nur Grundkenntnisse über algebraische Kurven und Riemannsche Flächen. Im 3. und 4. kommt noch etwas algebraische Zahlentheorie hinzu. Der 5. Vortrag ist eher was für Kenner der Materie.

Das Programm besteht i.W. aus einer Auswahl aus dem Artikel von Darmon, Diamond und Taylor [3]. Es wird aber oft nötig sein, auf die dort angegeben

Quellen zurückzugreifen. An vielen Stellen kann man sich auch gleich ganz nach einer anderen Quelle richten, z.B. [6], [4] oder [2].

1. Vortrag: Modulkurven und Modulformen

Es geht im Wesentlichen um den Inhalt von [3], §1.2-1.3: Definition und wesentliche Eigenschaften von Modulkurven und -formen und Hecke-Operatoren. Wichtig ist folgendes:

- Spitzenformen vom Gewicht zwei sind holomorphe Differentialformen auf Modulkurven.
- Definition der Hecke-Operatoren auf zwei Weisen: explizit anhand der Fourier-Entwicklung und konzeptuell als Korrespondenz zwischen Modulkurven.
- Eigenformen und 'Multiplizität-Eins'.
- Atkin-Lehner-Theorie: Neuformen und die Struktur der Hecke-Algebra $\mathbb{T}$, insbesondere Theorem 1.22.

Weglassen sollte man die Interpretation von Modulkurven als Modulräume von elliptischen Kurven (wird im 4. Vortrag behandelt).

2. Vortrag: Die Shimura-Konstruktion

Ziel des Vortrags ist, eine Konstruktion von Shimura zu erklären, die zu einer Hecke-Eigenform f vom Gewicht zwei eine über $\mathbb{Q}$ definierte abelsche Varietät A_f assoziiert. Hat f rationale Koeffizienten so ist A_f eine elliptische Kurve. Mithilfe dieser Konstruktion kann man dann eine geometrische Version der Taniyama-Weil-Vermutung formulieren: jede elliptische Kurve über $\mathbb{Q}$ ist isogen zu A_f, für eine geeignete Eigenform f.

Die Referenz ist [3], §1.5-1.7. Im Einzelnen:

- Analytische Beschreibung der Jacobischen von Modulkurven durch die Abel-Jacobi-Abbildung, wie in [3], p. 27f.
- Die Modulkurven $X_0(N)$, $X_1(N)$ und ihre Hecke-Korrespondenzen sind über $\mathbb{Q}$ definiert (ohne Begründung).
- Ganzzahlige Modulformen und das q-Entwicklungsprinzip (Thm 1.31, Prop. 1.32, Thm. 1.33).
- Die Shimura-Konstruktion: Def. 1.44, Lemma 1.46, Prop. 1.49.
- Geometrische Definition von Modularität: Prop. 1.53 (Beweis bis auf die Implikation $(a) \Rightarrow (b)$), Conj. 1.54 (Satz von BCDT).

3. Vortrag: Die Galois-Darstellung einer elliptischen Kurve

Ist $E/\mathbb{Q}$ eine elliptische Kurve, so erhält man für jede Primzahl ℓ eine ℓ-adische Galois-Darstellung

$$\rho_E : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Zu dieser Galois-Darstellung assoziiert man eine natürliche Zahl $N(E)$, den *Führer* von E, und eine L-Funktion $L(E/\mathbb{Q}, s)$. Dazu sollte folgendes gesagt werden (siehe [3], §1.1 und §2.1-2.2).

- Allgemeine Definition von ℓ-adischen und mod-ℓ-Galois-Darstellungen.
- Definition des Führers von ρ und $\bar{\rho}$.
- Definition der L-Funktion von ρ.
- Beispiel: $\rho(E)$ und $\bar{\rho}(E)$. Für alle Primzahlen p, bei denen E gute Reduktion hat, gilt für den Koeffizienten a_p von $L(E/\mathbb{Q}, s)$ die Formel $a_p = p + 1 - |E(\mathbb{F}_p)|$ und die Ungleichung $|a_p| \leq \sqrt{p}$. Der Führer $N(E)$ ist bestimmt durch die schlechte Reduktion von E.
- Analytische Definition der Modularität: E ist modular, wenn $L(E/\mathbb{Q}, s) = L(f, s)$ für eine Eigenform f (es ist zunächst nicht klar, ob diese Definition etwas mit der geometrischen Definition vom 2. Vortrag zu tun hat).

4. Vortrag: Modulare Galois-Darstellungen und die Eichler-Shimura-Relation

Zu jeder Eigenform f kann man mithilfe der Shimura-Konstruktion eine 2-dimensionale ℓ-adische Galoisdarstellung $\rho(f)$ assoziieren. Man erhält so eine arithmetische Definition von Modularität: eine elliptische Kurve $E/\mathbb{Q}$ ist modular, wenn ihre ℓ-adische Galois-Darstellung isomorph ist zu $\rho(f)$, für eine geeignete Eigenform f. Das Ziel des Vortrages ist, die wesentlichen Eigenschaften von $\rho(f)$ zu bestimmen und so die Äquivalenz der verschiedenen Definitionen von Modularität zu beweisen. Hierbei spielt die Eichler-Shimura-Relation eine überragende Rolle. Im Einzelnen:

- Die Modulinterpretation von $X_0(N)$ und $X_1(N)$, Modelle über $\mathbb{Q}$ und $\mathbb{Z}$. Siehe [3], p.24f, Rem. 1.10 und 1.11, p.35-37.
- Die Eichler-Shimura-Relation: [3], Thm. 1.29.
- Definition und Eigenschaften von $\rho(f)$ und $\bar{\rho}(f)$: [3], §3.1. Von Thm. 3.1 nur (a), (b) und (d), letzteres ohne Beweis; den Abschnitt über Artin-Darstellungen weglassen.
- Arithmetische Definition von Modularität: [3], Proposition 3.20. Stelle auch eine Verbindung zu der analytischen Definition im 3. Vortrag her.

5. Vortrag: Eigenschaften von $\rho(f)$ für $p|N$ und Niveau-Verminderung

Im letzten Vortrag sollen zum einen die Eigenschaften der Galois-Darstellung $\rho(f)$ an den Primstellen, die das Niveau teilen, diskutiert werden ([3], Thm. 3.1 (c)-(f)), zum anderen der Beweis der Implikation $(a) \Rightarrow (b)$ von [3], Proposition 1.53 skizziert werden. Für beide Punkte benötigt man einen etwas höheren Standpunkt als in den vorhergehenden Vorträgen, insbesondere den Zusammenhang zwischen Modulformen und automorphen Darstellungen. Als Quelle empfehle ich [5] und [1], aber es kann gut sein dass es noch bessere gibt.

References

[1] Henri Carayol. Sur les représentations galoisiennes modulo l attachées aux formes modulaires. *Duke Math. J.*, 59(3):785–801, 1989.

[2] Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors. *Modular forms and Fermat's last theorem*. Springer-Verlag, 1997. Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995.

[3] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Current developments in mathematics, 1995 (Cambridge, MA)*, pages 1–154. Internat. Press, 1994.

[4] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, 2005.

[5] B. Edixhoven. Modular Forms, Galois representations and local Langlands. www.crm.es/Publications/Quaderns/Quadern20-2.pdf.

[6] Serge Lang. *Introduction to modular forms*, volume 222 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, 1995.