Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

Elliptische Kurven

Vorlesung 28

Modularität bezüglich Kongruenzuntergruppen

Die in der letzten Vorlesung an Funktionen $f\colon \mathbb{H} \to \mathbb{C}$ formulierte Bedingungen bezüglich der vollen Modulgruppe $\mathrm{SL}_2(\mathbb{Z})$ kann man auch für Kongruenzuntergruppen Γ mit

$$\Gamma(N) \subseteq \Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$$

für ein gewisses N einschränken. Dies führt zu den folgenden Definitionen.

Definition 28.1. Es sei Γ eine Kongruenzuntergruppe und $k \in \mathbb{N}$. Eine meromorphe Funktion $f\colon \mathbb{H} \to \mathbb{C}$ auf der oberen Halbebene $\mathbb{H}$ heißt *Modulfunktion* bezüglich Γ vom Gewicht k, wenn

$$f(Mz) = (cz+d)^k f(z)$$

für alle

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

gilt und f meromorph im Unendlichen ist.

Definition 28.2. Es sei Γ eine Kongruenzuntergruppe und $k \in \mathbb{N}$. Eine holomorphe Funktion $f\colon \mathbb{H} \to \mathbb{C}$ auf der oberen Halbebene $\mathbb{H}$ heißt *Modulform* bezüglich Γ vom Gewicht k, wenn

$$f(Mz) = (cz+d)^k f(z)$$

für alle

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

gilt und f holomorph im Unendlichen ist.

Beachte, dass jede Kongruenzuntergruppe die Scherungsmatrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ enthält und damit die bezüglich Γ modularen Funktionen periodisch sind, also durch die Exponentialabbildung faktorisieren und somit die Konzepte meromorph und holomorph im Unendlichen definiert sind.

Bemerkung 28.3. Es sei $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ eine Kongruenzuntergruppe, die auf der oberen Halbebene $\mathbb{H}$ durch Modulsubstitution operiert. Dazu gehört die Quotientenabbildung

$$\pi_\Gamma\colon \mathbb{H} \longrightarrow \mathbb{H}/\Gamma =: Y_\Gamma,$$

bei der durch Γ ineinander überführbare Punkte miteinander identifiziert werden. Bei $\Gamma = \Gamma(N)$ und $\Gamma = \Gamma_0(N)$ finden sich Schreibweisen wie $Y(N)$ und $Y_0(N)$. Jede Γ-Modulform vom Gewicht 0 faktorisiert durch Y_Γ. Bei $\Gamma = \Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ ist

$$\mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \cong \mathbb{C}$$

und die Projektion stimmt mit der absoluten Invarianten j überein. Bei einer Untergruppenbeziehung $\Gamma \subseteq \Gamma'$ liegt eine nach Aufgabe 27.3 surjektive kanonische Abbildung

$$\mathbb{H}/\Gamma \longrightarrow \mathbb{H}/\Gamma'$$

vor. Wenn Γ ein Normalteiler in Γ' ist, so operiert nach Aufgabe 27.4 die endliche Restklassengruppe Γ'/Γ auf $\mathbb{H}/\Gamma$ mit dem Quotienten $\mathbb{H}/\Gamma'$. Bei $\Gamma = \Gamma(N)$ und $\Gamma' = \mathrm{SL}_2(\mathbb{Z})$ erhält man speziell, dass

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/(N))$$

auf $\mathbb{H}/\Gamma$ operiert mit dem Quotienten

$$\mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \cong \mathbb{C}.$$

Die Y_Γ sind riemannsche Flächen und die Quotientenabbildungen sind holomorph. Man kann sie durch die Hinzunahme von endlich vielen Punkten kompaktifizieren und erhält dadurch kompakte Riemannsche Flächen X_Γ, die Modulflächen heißen. Da kompakte Riemannschen Flächen den glatten projektiven Kurven über $\mathbb{C}$ entsprechen, spricht man auch von Modulkurven.

Bemerkung 28.4. Es gibt tiefliegende und vielfältige Beziehungen zwischen erstens elliptischen Kurven (über $\mathbb{C}$ und über $\mathbb{Q}$) zweitens Modulfunktionen und Modulformen, drittens Gittern in $\mathbb{C}$, viertens Modulgruppen und Kongruenzuntergruppen und fünftens Modulkurven, die man auseinanderhalten muss.

(1) Ein Gitter definiert einen komplexen Torus und damit wegen Satz 12.13 eine elliptische Kurve über $\mathbb{C}$.
(2) Eine Modulfunktion ist auf der oberen Halbebene definiert. Da ein Gitter aber nach Lemma 9.5 zu einem Gitter der Form $\langle 1, \tau \rangle$ mit $\tau \in \mathbb{H}$ streckungsäquivalent ist, kann man eine Modulfunktion auch so auffassen, dass sie einem Gitter einen Wert zuweist. Eine Modulfunktion mit Gewicht 0 ist invariant unter der Operation der vollen Modulgruppe, daher kann man eine solche Funktion auffassen als eine Funktion auf der Quotientenmenge aller Gitter modulo der Äquivalenzrelation der Streckungsäquivalenz. Wegen Satz 10.8 kann man eine solche Funktion als eine Zuordnung auffassen, die jedem komplexen eindimensionalen Torus eine Zahl zuordnet. Das Hauptergebnis ist hier, dass die j-Invariante eine Modulfunktion vom Gewicht 0 ist (die Invarianz bei Streckung ist Lemma 12.7 (4)) und jede Modulfunktion vom Gewicht 0 eine rationale Funktion in j ist. Dies rechtfertigt auch die Bezeichnung absolute Invariante.

(3) Die Eisenstein-Reihen zum Gewicht k (mit $k \geq 3$) sind Modulformen vom Gewicht k. Sie ordnen einem Gitter bzw. einem Element $\tau \in \mathbb{H}$ eine für das Gitter charakteristische Zahl zu, wobei das Transformationsverhalten beim Übergang zu einem streckungsäquivalenten Gitter übersichtlich und eben durch das Gewicht beschrieben wird, siehe Lemma 12.2 (4) und Lemma 27.7. Die Werte der verschiedenen Eisenstein-Reihen an einem festen Gitter Λ legen nach Lemma 12.10 im Wesentlichen die Weierstraßsche $\wp$-Funktion $\wp$ zum Gitter fest, mit der die algebraische Realisierung als elliptische Kurve des komplexen Torus zu Λ gewonnen wird. Die Gleichung der Kurve kann man direkt mit G_4 und G_6 angeben, siehe Satz 12.11.

(4) Eine Kongruenzuntergruppe Γ definiert einen Quotienten $\mathbb{H}/\Gamma$. Bei der vollen Modulgruppe entsteht bei diesem Prozess die komplexe Ebene, mit der absoluten Invariante als Abbildung dazwischen, und die Punkte repräsentieren eindeutig die elliptischen Kurven. Bei einer Kongruenzuntergruppe repräsentieren die Punkte des Quotienten eine elliptische Kurve zusammen mit einer zusätzlichen Dekorierung, beispielsweise einer N-Torsionsbasis (siehe Lemma 27.12) oder einem festen Punkt auf der elliptischen Kurve von einer gewissen festen Ordnung. In einer solchen Situation kann dem Quotienten die Struktur einer riemannschen Fläche gegeben werden. Diese kann man durch Hinzunahme von endlich vielen Punkten kompaktifizieren und es entsteht eine kompakte riemannsche Fläche, eine sogenannte *Modulkurve* oder *Modulfläche*. Diese ist manchmal selbst eine elliptische Kurve, manchmal nicht. Ferner kann es von einer solchen Modulkurve nichtkonstante holomorphe bzw. algebraische Abbildungen auf eine elliptische Kurve geben.

(5) Eine Modulform zu einer Kongruenzuntergruppe besitzt, aufgefasst als holomorphe Funktion auf der offenen Einheitskreisscheibe, eine Potenzreihenentwicklung im Nullpunkt. Deren Koeffizienten kann man mit den Koeffizienten der L-Reihe einer elliptischen Kurve über $\mathbb{Q}$ in Beziehung setzen.

Der Modularitätsatz

Eine über $\mathbb{Q}$ definierte elliptische Kurve besitzt eine L-Reihe, die man als eine Dirichletreihe $\sum_{n\in\mathbb{N}_+} a_n n^{-s}$ schreiben kann. Aus den Koeffizienten a_n kann man andere Objekte bilden, insbesondere andere Reihen. Hier interessieren wir uns für die Reihe

$$g(z) := \sum_{n\in\mathbb{N}_+} a_n e^{2\pi \mathrm{i} n z}.$$

Es handelt sich um eine Fourierreihe, die man oft auch als Potenzreihe

$$\sum_{n\in\mathbb{N}_+} a_n q^n$$

schreibt, dabei gilt also $q = e^{2\pi \mathrm{i} z}$, es liegt eine Potenzreihe in $e^{2\pi \mathrm{i} z}$ vor. Es liegt die Zusammensetzung

$$\mathbb{C} \stackrel{z \mapsto e^{2\pi \mathrm{i} z}}{\longrightarrow} \mathbb{C} \stackrel{q \mapsto \sum a_n q^n}{\longrightarrow} \mathbb{C}$$

bzw.

$$\mathbb{H} \stackrel{z \mapsto e^{2\pi \mathrm{i} z}}{\longrightarrow} U(0,1) \stackrel{q \mapsto \sum a_n q^n}{\longrightarrow} \mathbb{C}$$

vor, für die Konvergenz auf der offenen Einheitskreisscheibe siehe Aufgabe 27.6. Man kann sich nun fragen, ob sich Gesetzmäßigkeiten der L-Reihe, die ja strukturelle Eigenschaften der elliptischen Kurve zusammenfasst, in Gesetzmäßigkeiten von $g(z)$ niederschlagen bzw. dort erst sichtbar bzw. sinnvoll formulierbar werden. Es gilt nun in der Tat der folgende *Modularitätssatz*, vormals die Vermutung von Taniyama-Shimura, der in einem wichtigen Spezialfall zuerst von Wiles und dann vollständig von Breuil, Conrad, Diamond, Taylor bewiesen wurde. Er kann auf recht unterschiedliche Weise formuliert werden, wir erwähnen eine Version, die ohne großen begrifflichen Aufwand direkt die Koeffizienten der L-Reihe ins Visier nimmt. Der Beweis geht deutlich über eine Einführung in elliptische Kurven hinaus.

Satz 28.5. *Es sei E eine elliptische Kurve über $\mathbb{Q}$ und sei*

$$L(E,s) = \sum_{n \in \mathbb{N}_+} a_n n^{-s}$$

die zugehörige L-Reihe. Dann gibt es eine natürliche Zahl N derart, dass die Funktion

$$g(z) := \sum_{n \in \mathbb{N}_+} a_n e^{2\pi \mathrm{i} n z}$$

eine Modulform bezüglich $\Gamma_0(N)$ vom Gewicht 2 ist. Das bedeutet, dass g die funktionale Identität

$$g(Mz) = (cz+d)^2 g(z)$$

für jedes $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ erfüllt.

Da die Reihe $\sum_{n \in \mathbb{N}_+} a_n q^n$ auf dem offenen Ball definiert ist, liegt für die zugehörige Abbildung auf $\mathbb{H}$ Holomorphie im Unendlichen mit dem Wert 0 vor. Die Hauptaussage ist also die Verträglichkeit mit der Operation der Kongruenzuntergruppe, die eine zusätzliche Gesetzmäßigkeit zwischen den Koeffizienten a_n und damit zwischen den verschiedenen Reduktionen der elliptischen Kurve ausdrückt.

Eine weitere Formulierung des Modularitätssatzes ist, dass es eine nichtkonstante holomorphe (oder algebraische) Abbildung

$$X_0(N) \longrightarrow E$$

gibt, wobei $X_0(N)$ die Modulkurve zur Kongruenzuntergruppe $\Gamma_0(N)$ bezeichnet.

Nach Satz 18.15 liefert eine über $\mathbb{Q}$ definierte elliptische Kurve E zu jeder Primzahl ℓ eine Darstellung der absoluten Galoisgruppe von $\mathbb{Q}$ in den ℓ-adischen Tate-Module

$$T_\ell(E) \cong \hat{\mathbb{Z}}_\ell \times \hat{\mathbb{Z}}_\ell,$$

also einen Gruppenhomomorphismus

$$G_{\overline{\mathbb{Q}}|\mathbb{Q}} \longrightarrow \operatorname{Aut} T_\ell(E) \cong \mathrm{GL}_2\Big(\hat{\mathbb{Z}}_\ell\Big).$$

Ebenso definiert eine Modulform eine solche Darstellung. Im Beweis werden letztlich solche Darstellungen miteinander verglichen.

Eine wichtige Folgerung aus dem Modularitätsatz ist der folgende Satz, vormals eine Vermutung von Hasse-Weil.

Satz 28.6. *Zu einer elliptischen Kurve über $\mathbb{Q}$ besitzt die zugehörige L-Reihe*

$$L(E,s) = \sum_{n\in\mathbb{N}_+} a_n n^{-s}$$

eine analytische Fortsetzung auf $\mathbb{C}$.

Dies sichert, dass in der Vermutung von Birch und Swinnerton-Dyer die L-Reihe in $s = 1$ eine sinnvolle Fortsetzung besitzt und der analytische Rang dort überhaupt wohldefiniert ist.

Der Satz von Wiles

Die Vermutung von Taniyama-Shimura, die selbst von ca. 1955 stammt, erfuhr um 1986 ein vertieftes Interesse, als sich eine Beziehung zur Vermutung von Fermat ergab. Diese besagt, dass es zu einem Exponenten $n \geq 3$ keine nichtriviale ganzzahlige Lösung (a,b,c) der Gleichung

$$a^n + b^n = c^n$$

gibt. Für eine Vielzahl von Exponenten war dies zuvor mit unterschiedlichen Methoden, hauptsächlich aus der algebraischen Zahlentheorie, bewiesen worden, aber eben nicht für alle. Diese Vermutung wurde häufig als das bekannteste offene mathematische Problem genannt. Für $n = 3$ geht es um die Frage, ob die elliptische Kurve $x^n + y^n = z^n$ ganzzahlige Lösungen besitzt. Es wurde schon von Euler gezeigt, dass es solche Punkte nicht gibt. Die neue Entwicklung war nun, dass das Problem von Fermat für jeden Exponenten n etwas mit einer elliptischen Kurve zu tun hat. Dazu geht man von einer potentiellen nichttrivialen ganzzahligen Lösung (deren Existenz man letztlich widerlegen möchte)

$$a^n + b^n = c^n$$

aus und betrachtet dazu die Weierstraß-Gleichung

$$y^2 = x(x-a^n)(x-b^n).$$

Wegen der Nichttrivialität der Lösung liegt eine über $\mathbb{Q}$ definierte elliptische Kurve vor, die sogenannte *Frey-Kurve* (oder Frey-Hellegouarch-Kurve). Das c kommt nicht explizit in der Gleichung vor, ist aber natürlich durch a und b jederzeit präsent. Frey äußerte die Vermutung, dass eine solche Kurve ein Gegenbeispiel zur Vermutung von Taniyama-Shimura sein könnte, bzw., dass wenn die Vermutung von Taniyama-Shimura stimmt, dass es dann eine solche Kurve nicht geben kann und dass damit der große Fermat gelten müsse. Diese Beziehung zwischen Taniyama-Shimura und großem Fermat wurde dann von Serre und Ribet bewiesen. Ab 1990 war also klar: Wenn man zeigen kann, dass jede elliptische Kurve über $\mathbb{Q}$ modular ist, dann folgt der Große Fermat. Mitte der Neunziger gelang es nun Wiles, zwar nicht die volle Vermutung von Taniyama-Shimura zu beweisen, aber immerhin für eine große Klasse von elliptischen Kurven, die die Frey-Kurven miteinschließen, nämlich für die sogenannten semistabilen elliptischen Kurven. Das sind diejenigen elliptischen Kurven, bei denen für keine Primzahl additive Reduktion auftritt. Auf diesem Weg ergibt sich.

Satz 28.7. *Die diophantische Gleichung*

$$a^n + b^n = c^n$$

besitzt für kein $n \geq 3$ eine ganzzahlige nichttriviale Lösung.

Die volle Vermutung von Taniyama-Shimura wurde gegen 2000 aufbauend auf Wiles Arbeiten von Breuil, Conrad, Diamond, Taylor bewiesen.

Abbildungsverzeichnis