Über den Beweis der Fermat-Vermutung II

Autor(en): **Kramer, Jürg**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **53 (1998)**

PDF erstellt am: **21.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-3629

Elem. Math. 53 (1998) 45 – 60
0013-6018/98/020045-16 $ 1.50+0.20/0

Elemente der Mathematik

Über den Beweis der Fermat-Vermutung II

Jürg Kramer

Jürg Kramer studierte Mathematik und Physik an der Universität Basel; im Jahre 1985 promovierte er dort bei Martin Eichler über Modul- und Jacobiformen. Forschungsaufenthalte schlossen sich an: am Max-Planck-Institut für Mathematik in Bonn, an der Harvard University in Cambridge (MA) und am Mathematical Sciences Research Institute in Berkeley (CA). Dann wurde er Assistent von Gisbert Wüstholz an der Universität Wuppertal. Mit diesem kam er 1988 an die ETH in Zürich. Im Oktober 1994 trat er eine ordentliche Professur am Institut für Mathematik an der Humboldt-Universität in Berlin an, wo er einerseits seine Forschungsinteressen im Bereich der arithmetischen algebraischen Geometrie und der automorphen Formen weiterverfolgt und andererseits für die Lehrerausbildung in Mathematik verantwortlich ist. Seine Interessen ausserhalb der Mathematik erstrecken sich auf die Geschichte, insbesondere die Wissenschaftsgeschichte, und auf klassische und moderne Sprachen.

Der Beweis der Fermat-Vermutung durch Andrew Wiles und Richard Taylor ist zweifellos eine der ganz grossen Leistungen der Mathematik in diesem Jahrhundert. Zu Recht wurde denn auch die Lösung des alten Problems in weiten Kreisen als Sensation gefeiert. Für die Entwicklung der Mathematik dürften allerdings die hier neu eingeführten Methoden noch von grösserer Tragweite sein. Sie haben Wiles und Taylor erlaubt, sehr allgemeine und tiefliegende Sätze zu beweisen, aus denen sich als ganz spezielle Folgerung die Richtigkeit der Fermat-Vermutung ergab. Diese abstrakten Methoden und Sätze lassen sich nicht auf einfache Weise darstellen und erklären: die inhärente Komplexität der Sache macht dies schlicht unmöglich. Trotzdem ist es Jürg Kramer in einem ersten Artikel [El. Math. **50** (1995), 11–25] gelungen, die grundsätzliche Beweisstruktur (Zurückführung der Fermat-Vermutung auf die Vermutung von Shimura-Taniyama) übersichtlich darzustellen. Im vorliegenden Beitrag stellt er nun auf ähnliche Weise den von Wiles und Taylor erbrachten Beweis der Vermutung von Shimura-Taniyama vor. – Der Beitrag mag schwierigkeitsmässig an der oberen Grenze des für unsere Zeitschrift Vertretbaren liegen; wir haben uns trotzdem für eine Veröffentlichung entschieden: die *Elemente der Mathematik* wollen an dem epochalen Entwicklungsschritt der Mathematik nicht vorbeigehen, der mit den Arbeiten von Wiles und Taylor gemacht worden ist. *ust*

1 Einleitung

Diese Note ist eine Fortsetzung des Artikels [7]; dementsprechend werden die dort eingeführten Bezeichnungen verwendet. In der in [7] mit möglichst elementaren Mitteln gegebenen Übersicht über die Strategie des Beweises der Fermat-Vermutung stellte sich die Vermutung von Shimura und Taniyama im Spezialfall semistabiler elliptischer Kurven als die noch zu beweisende Schlüsselstelle heraus. Der vollständige Beweis dieser Vermutung gelang A. Wiles und R. Taylor im Herbst 1994 und wurde im Sommer 1995 in den beiden Arbeiten [23] und [21] publiziert. In diesem Artikel wird nun der Versuch unternommen, dem durch [7] neugierig gewordenen Leser eine Übersicht über den Beweis des Satzes von Wiles und Taylor anzubieten. Da dieser Artikel mathematisch etwas anspruchsvoller als der vorhergehende ist, wurde im sechsten Abschnitt ein Anhang über die ℓ-adischen Zahlen, die Gruppenstruktur einer elliptischen Kurve und die Hilbertsche Theorie Galoisscher Zahlkörper beigefügt. Wir hoffen, damit möglichst vielen, die sich durch die Note [7] angesprochen fühlten, einen Einblick in den Ideenreichtum und die Komplexität des Beweises des Schlüsselsatzes zum Beweis der Fermat-Vermutung zu ermöglichen. Dem interessierten Leser empfehlen wir auch die Lektüre der erst vor kurzem erschienenen, weitaus detaillierteren Abhandlungen [1], [3], [13], [15] und der beiden Originalartikel [23], [21], zu denen dieser Artikel eine gewisse Orientierungshilfe bieten könnte.

2 Galois-Darstellungen

Im folgenden soll also ein Überblick über den durch A. Wiles und R. Taylor in [23] und [21] dargestellten Beweis der Vermutung von Shimura und Taniyama (s. [7], Vermutung 4.5) für semistabile elliptische Kurven $E/\mathbb{Q}$ gegeben werden, d.h. über den Beweis des

2.1 Satz (Wiles, Taylor). *Jede semistabile elliptische Kurve $E/\mathbb{Q}$ ist modular zur Stufe $N = N_E$.*

2.2 Definition. Es sei $\overline{\mathbb{Q}}$ ein algebraischer Abschluss von $\mathbb{Q}$, $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ die absolute Galois-Gruppe und $\ell > 2$ eine Primzahl. Mit $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$ sei der Körper mit ℓ Elementen und mit $\mathbb{Z}_\ell$ der Ring der ganzen ℓ-adischen Zahlen (s. Anhang 6.1) bezeichnet. Wir betrachten dann zwei Typen von 2-dimensionalen Darstellungen von G:

(i) $\overline{\rho}_\ell : G \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$, *Galois-Darstellung in Charakteristik ℓ.*

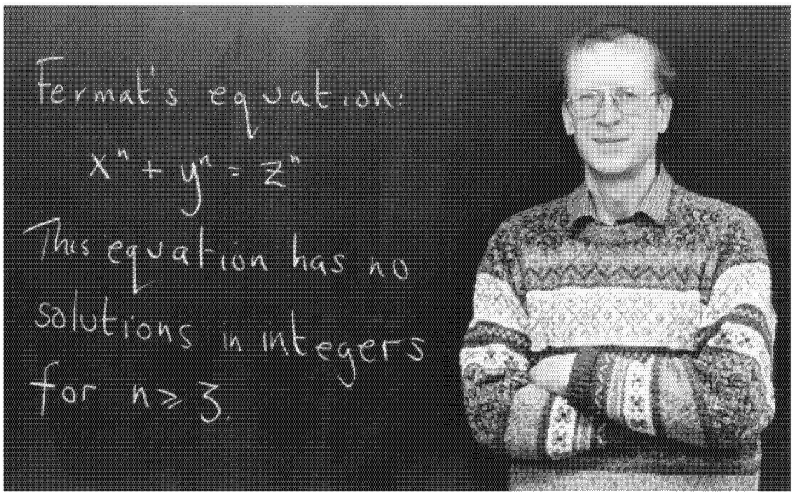
(ii) $\rho_\ell : G \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$, *$\ell$-adische Galois-Darstellung.*

2.3 Bemerkung. Da $\mathbb{Z}_\ell/(\ell) \cong \mathbb{F}_\ell$ gilt, erhalten wir durch Betrachtung einer gegebenen ℓ-adischen Galois-Darstellung ρ_ℓ modulo dem Hauptideal $(\ell) = \ell\mathbb{Z}_\ell$ eine Galois-Darstellung $\overline{\rho}_\ell$ in Charakteristik ℓ und damit das folgende, kommutative Diagramm:

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}) \\ & \searrow & \downarrow \mathrm{mod}\ (\ell) \\ & & \mathrm{GL}_2(\mathbb{F}_\ell) \end{array}$$

2.4 Beispiele (Elliptische Kurven). Es sei $E/\mathbb{Q}$ eine elliptische Kurve mit geometrischem Führer N_E. Wie im Anhang 6.2 ausgeführt ist, besitzt E die Struktur einer kommutativen Gruppe; dabei berechnen sich die Koordinaten der Summe $P+Q$ zweier Punkte $P, Q \in E$ durch rationale Funktionen mit rationalen Koeffizienten in den Koordinaten von P, Q. Daraus erkennen wir sofort, dass die absolute Galois-Gruppe G auf dem Kern $E[n] \subset E(\overline{\mathbb{Q}})$ des Homomorphismus $[n] : E \longrightarrow E$ (Multiplikation mit n) operiert. Aufgrund der Isomorphie $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ erhalten wir also die Galois-Darstellungen

$$\overline{\rho}_{E,n} : G \longrightarrow \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$



Andrew John Wiles vor der Wandtafel in seinem Büro an der Princeton University (Keystone/Charles Rex Arbogast/AP Photo).

Speziell für $n = \ell$ ergibt sich somit eine Galois-Darstellung vom Typ (i)

$$\overline{\rho}_{E,\ell} : G \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell).$$

Durch Betrachtung des (projektiven) Systems $\{\overline{\rho}_{E,\ell}, \overline{\rho}_{E,\ell^2}, \overline{\rho}_{E,\ell^3}, \ldots\}$ von Galois-Darstellungen erhalten wir durch Übergang zum inversen Limes

$$\rho_{E,\ell} := \varprojlim_{\nu \to \infty} \overline{\rho}_{E,\ell^\nu}$$

eine Galois-Darstellung vom Typ (ii)

$$\rho_{E,\ell} : G \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Zur Beschreibung der Eigenschaften von $\overline{\rho}_{E,\ell}$ und $\rho_{E,\ell}$ ziehen wir Anhang 6.3 heran. Wir betrachten den Fixpunktkörper $K_{E,\ell}/\mathbb{Q}$ zum Kern $\ker\overline{\rho}_{E,\ell}$ von $\overline{\rho}_{E,\ell}$, d.h.

$$K_{E,\ell} = \overline{\mathbb{Q}}^{\ker\overline{\rho}_{E,\ell}} = \{\alpha \in \overline{\mathbb{Q}} \mid \sigma(\alpha) = \alpha \ \ \forall \sigma \in \ker\overline{\rho}_{E,\ell}\},$$

mit dem Ring der ganzen Zahlen $\mathbb{O}_{K_{E,\ell}}$. Man beweist nun, dass $\overline{\rho}_{E,\ell}$, resp. $\rho_{E,\ell}$, für alle Primzahlen p, $p \neq \ell$ und $p \nmid N_E$, unverzweigt ist; für diese Primzahlen besteht dann die Primidealzerlegung

$$p \cdot \mathbb{O}_{K_{E,\ell}} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$$

mit r Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Den Primidealen $\mathfrak{p}_j$ sind die Frobenius-Automorphismen $\mathrm{Frob}_{\mathfrak{p}_j} \in G$ $(j = 1, \ldots, r)$ zugeordnet, welche sämtlich zueinander konjugiert sind. Damit sind die *Spuren* $\mathrm{tr}\,\overline{\rho}_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}_j})$, resp. $\mathrm{tr}\,\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}_j})$, und die entsprechenden Determinanten eindeutig festgelegt, d.h. unabhängig von j. Wir schreiben deshalb $\mathrm{tr}\,\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)$, resp. $\mathrm{tr}\,\rho_{E,\ell}(\mathrm{Frob}_p)$, und $\det\overline{\rho}_{E,\ell}(\mathrm{Frob}_p)$, resp. $\det\rho_{E,\ell}(\mathrm{Frob}_p)$. Mit den Bezeichnungen von [7], Abschnitt 3.5, weist man nun folgende Eigenschaften für $\overline{\rho}_{E,\ell}$ nach:

$$\begin{aligned} \mathrm{tr}\,\overline{\rho}_{E,\ell}(\mathrm{Frob}_p) &\equiv b_p = p - N_p \mod \ell \quad && \forall p \neq \ell, p \nmid N_E, \\ \det\overline{\rho}_{E,\ell}(\mathrm{Frob}_p) &\equiv p \mod \ell && \forall p \neq \ell, p \nmid N_E. \end{aligned}$$

Entsprechend ergibt sich für $\rho_{E,\ell}$:

$$\begin{aligned} \mathrm{tr}\,\rho_{E,\ell}(\mathrm{Frob}_p) &= b_p = p - N_p \quad && \forall p \neq \ell, p \nmid N_E, \\ \det\rho_{E,\ell}(\mathrm{Frob}_p) &= p && \forall p \neq \ell, p \nmid N_E. \end{aligned}$$

2.5 Numerisches Beispiel. Wir betrachten die elliptische Kurve mit der minimalen Gleichung

$$E : Y^2 + Y = X^3 + X^2 - 9X - 15.$$

Für deren minimale Diskriminante $\Delta_E^{\min}$ und deren geometrischen Führer N_E berechnet man (s. auch [20], S. 82)

$$\Delta_E^{\min} = -19^3, N_E = 19.$$

Wir wählen jetzt $\ell = 3$. Mit Hilfe der Additionsformeln in Anhang 6.2 überprüft man leicht, dass der Kern $E[3]$ aus dem unendlich fernen Punkt O_E und den folgenden 8 Punkten besteht (bei diesen Rechnungen beachte man die Koordinatentransformation $X \mapsto X$, $Y \mapsto Y - 1/2$):

$$\begin{aligned} P_1 &= (5, 9) & P_2 &= (5, -10) \\ P_3 &= \left(-\frac{4}{3}, -\frac{1}{2} + \frac{19}{18}\sqrt{-3}\right) & P_4 &= \left(-\frac{4}{3}, -\frac{1}{2} - \frac{19}{18}\sqrt{-3}\right) \\ P_5 &= \left(-\frac{5}{2} + \frac{1}{2}\sqrt{-3}, \frac{3}{2} + \frac{1}{2}\sqrt{-3}\right) & P_6 &= \left(-\frac{5}{2} + \frac{1}{2}\sqrt{-3}, -\frac{5}{2} - \frac{1}{2}\sqrt{-3}\right) \\ P_7 &= \left(-\frac{5}{2} - \frac{1}{2}\sqrt{-3}, \frac{3}{2} - \frac{1}{2}\sqrt{-3}\right) & P_8 &= \left(-\frac{5}{2} - \frac{1}{2}\sqrt{-3}, -\frac{5}{2} + \frac{1}{2}\sqrt{-3}\right). \end{aligned}$$

Insbesondere stellt man fest, dass $E[3]$ die direkte Summe der durch P_1, resp. P_3, erzeugten zyklischen Untergruppen $\langle P_1 \rangle$, resp. $\langle P_3 \rangle$, der Ordnung 3 ist, d.h.

$$E[3] = \langle P_1 \rangle \oplus \langle P_3 \rangle \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Da nun $E[3] \subset E(K)$ mit $K := \mathbb{Q}(\sqrt{-3})$ gilt, faktorisiert die Galois-Darstellung $\overline{\rho}_{E,3} : G \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ über die Galois-Gruppe $\mathrm{Gal}(K/\mathbb{Q})$, d.h. $\overline{\rho}_{E,3}$ ist bestimmt durch die Wirkung von $\mathrm{Gal}(K/\mathbb{Q})$ auf $E[3]$. Beachten wir noch, dass die letztere Galois-Gruppe zyklisch von der Ordnung 2 ist, also

$$\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle = \{\mathrm{id}, \sigma\}$$

gilt, wobei σ der nicht-triviale Automorphismus von $\mathbb{Q}(\sqrt{-3})$ mit $\sigma(\sqrt{-3}) = -\sqrt{-3}$ ist, so ergibt sich

$$\overline{\rho}_{E,3}(\mathrm{id}) = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \quad , \quad \overline{\rho}_{E,3}(\sigma) = \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{2} \end{pmatrix}.$$

Wir berechnen schliesslich die Spuren und die Determinanten der Frobenius-Automorphismen Frob_p zu den Primzahlen $p \neq 3, 19$. Dazu stellen wir zunächst mit Hilfe des quadratischen Reziprozitätsgesetzes die Gleichheit der Legendre-Symbole

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$$

fest. Ist also $p \equiv 1 \bmod 3$, so ist -3 ein quadratischer Rest $\bmod p$, und p lässt sich mit ganzen Zahlen ξ, η in der Form $\xi^2 + 3\eta^2$ darstellen. Daraus ergibt sich für das Hauptideal $p \cdot \mathbb{O}_K$ die Zerlegung

$$p \cdot \mathbb{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$$

mit zwei verschiedenen Primidealen $\mathfrak{p}_1, \mathfrak{p}_2$. Somit besteht für den Restklassengrad von p die Gleichung $f = 1$, also gilt $\mathrm{Frob}_p = \mathrm{id}$. Ist andererseits $p \equiv 2 \bmod 3$, so ist -3 ein quadratischer Nichtrest $\bmod p$, also ist das Hauptideal $p \cdot \mathbb{O}_K$ selbst ein Primideal mit $f = 2$. In diesem Fall gilt $\mathrm{Frob}_p = \sigma$. Insgesamt erhalten wir für Primzahlen $p \neq 3, 19$ die Kongruenzen

$$\begin{aligned} \mathrm{tr}\,\overline{\rho}_{E,3}(\mathrm{Frob}_p) &\equiv 2 \bmod 3, \quad p \equiv 1 \bmod 3, \\ \mathrm{tr}\,\overline{\rho}_{E,3}(\mathrm{Frob}_p) &\equiv 0 \bmod 3, \quad p \equiv 2 \bmod 3, \end{aligned}$$

und

$$\begin{aligned} \det\overline{\rho}_{E,3}(\mathrm{Frob}_p) &\equiv 1 \bmod 3, \quad p \equiv 1 \bmod 3, \\ \det\overline{\rho}_{E,3}(\mathrm{Frob}_p) &\equiv 2 \bmod 3, \quad p \equiv 2 \bmod 3. \end{aligned}$$

Wir bemerken abschliessend, dass die in diesem Beispiel konstruierte Galois-Darstellung $\overline{\rho}_{E,3}$ *nicht* irreduzibel ist.

3 Modulare Galois-Darstellungen

Einleitend bemerken wir, dass die in 2.2 gegebene Definition einer Galois-Darstellung in Charakteristik ℓ, bzw. einer ℓ-adischen Galois-Darstellung, dahingehend verallgemeinert werden kann, indem der Körper $\mathbb{F}_\ell$ durch eine endliche Erweiterung $k/\mathbb{F}_\ell$, bzw. der Ring $\mathbb{Z}_\ell$ durch eine endliche Erweiterung $\mathbb{O}/\mathbb{Z}_\ell$, ersetzt wird. Von dieser Verallgemeinerung werden wir in der folgenden Definition Gebrauch machen.

3.1 Definition. (i) Eine Galois-Darstellung $\overline{\rho}_\ell : G \longrightarrow \mathrm{GL}_2(k/\mathbb{F}_\ell)$ in Charakteristik ℓ heisst *modular zur Stufe* N, falls $0 \neq f \in S_2(\Gamma_0(N))$, $f(\tau) = q + \sum_{n=2}^{\infty} c_n q^n$, existiert, so dass

$$\begin{aligned} \operatorname{tr} \overline{\rho}_\ell(\mathrm{Frob}_p) &\equiv c_p \mod \ell \quad \forall p \neq \ell, p \nmid N, \\ \det \overline{\rho}_\ell(\mathrm{Frob}_p) &\equiv p \mod \ell \quad \forall p \neq \ell, p \nmid N \end{aligned}$$

gilt. Um die Abhängigkeit von der Spitzenform f hervorzuheben, schreiben wir $\overline{\rho}_{f,\ell}$ anstelle von $\overline{\rho}_\ell$.

(ii) Eine ℓ-adische Galois-Darstellung $\rho_\ell : G \longrightarrow \mathrm{GL}_2(\mathbb{O}/\mathbb{Z}_\ell)$ heisst *modular zur Stufe* N, falls $0 \neq f \in S_2(\Gamma_0(N))$, $f(\tau) = q + \sum_{n=2}^{\infty} c_n q^n$, existiert, so dass

$$\begin{aligned} \operatorname{tr} \rho_\ell(\mathrm{Frob}_p) &= c_p \quad \forall p \neq \ell, p \nmid N, \\ \det \rho_\ell(\mathrm{Frob}_p) &= p \quad \forall p \neq \ell, p \nmid N \end{aligned}$$

gilt. Um die Abhängigkeit von der Spitzenform f hervorzuheben, schreiben wir $\rho_{f,\ell}$ anstelle von ρ_ℓ.

3.2 Bemerkung. Um den Artikel möglichst einfach zu gestalten, werden wir im folgenden immer annehmen, dass die zu betrachtenden Spitzenformen *ganzzahlige* Fourierkoeffizienten besitzen. Damit brauchen wir dann auch keine echten Erweiterungen $k/\mathbb{F}_\ell$, bzw. $\mathbb{O}/\mathbb{Z}_\ell$, heranzuziehen. Wir betonen aber, dass man bei einer korrekten Behandlung des Gegenstandes nicht um diese Verallgemeinerung herumkommt.

3.3 Bemerkung. Ist die Galois-Darstellung $\overline{\rho}_\ell : G \longrightarrow \mathrm{GL}_2(k/\mathbb{F}_\ell)$ in Charakteristik ℓ modular im Sinne der vorhergehenden Definition, so ist die Stufe N nicht eindeutig bestimmt. In der Arbeit [17] hat J-P. Serre unter anderem eine Vorschrift zur Bestimmung der minimal möglichen Stufe $N(\overline{\rho}_\ell)$ vermutet. In der Folge sind viele Beiträge zu dieser Problemstellung entstanden; der entscheidende Durchbruch, welcher zur Bestätigung der Serre'schen Vermutungen führte, gelang K.A. Ribet mit der Arbeit [14].

3.4 Numerisches Beispiel. Wir betrachten die Galois-Darstellung $\overline{\rho}_{E,3} : G \longrightarrow \mathrm{GL}_2(\mathbb{F}_3)$ aus Beispiel 2.5. Für die Spuren der Frobenius-Automorphismen Frob_p hatten wir gefunden

$$\begin{aligned} \operatorname{tr} \overline{\rho}_{E,3}(\mathrm{Frob}_p) &\equiv 2 \mod 3, \quad p \equiv 1 \mod 3, \\ \operatorname{tr} \overline{\rho}_{E,3}(\mathrm{Frob}_p) &\equiv 0 \mod 3, \quad p \equiv 2 \mod 3. \end{aligned}$$

Andererseits berechnet man mit der in [7], Abschnitt 4, gegebenen Formel

$$\dim_{\mathbb{C}} S_2(\Gamma_0(19)) = 1.$$

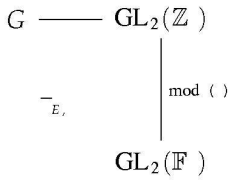
Die dadurch eindeutig festgelegte Spitzenform $0 \neq f \in S_2(\Gamma_0(19))$, $f(\tau) = q + \sum_{n=2}^{\infty} c_n q^n$, entnimmt man der Tabelle [20], S. 117; wir geben hier die Fourierkoeffizienten c_p zu den Primzahlen $p \neq 3, 19$, $p \leq 97$, wieder:

$$\begin{array}{llllll} c_2 = 0 & c_5 = 3 & c_7 = -1 & c_{11} = 3 & c_{13} = -4 & c_{17} = -3 \\ c_{23} = 0 & c_{29} = 6 & c_{31} = -4 & c_{37} = 2 & c_{41} = -6 & c_{43} = -1 \\ c_{47} = -3 & c_{53} = 12 & c_{59} = -6 & c_{61} = -1 & c_{67} = -4 & c_{71} = 6 \\ c_{73} = -7 & c_{79} = 8 & c_{83} = 12 & c_{89} = 12 & c_{97} = 8. & \end{array}$$

Ein Vergleich zeigt schliesslich, dass die Galois-Darstellung $\overline{\rho}_{E,3}$ in Charakteristik 3 modular zur Stufe $N = 19$ ist.

3.5 Bemerkung. (a) Es sei $E/\mathbb{Q}$ eine elliptische Kurve mit geometrischem Führer N_E. Falls die Kurve $E/\mathbb{Q}$ modular zur Stufe $N = N_E$ ist (s. [7], Abschnitt 4.3), so folgt unmittelbar, dass die in Beispiel 2.4 konstruierten Galois-Darstellungen $\overline{\rho}_{E,\ell}$ und $\rho_{E,\ell}$ für *jede Primzahl* ℓ im Sinne der Definition 3.1 modular zur Stufe N sind. Umgekehrt geht aus einem Satz von G. Faltings (s. [2]) hervor, dass die Modularität von $\rho_{E,\ell}$ für *eine Primzahl* ℓ die Modularität von $E/\mathbb{Q}$ zur Stufe $N = N_E$ zur Folge hat.

(b) Das eben erwähnte Resultat von G. Faltings liefert folgende Strategie zum Beweis des Satzes von Wiles und Taylor: Für eine semistabile elliptische Kurve $E/\mathbb{Q}$ gilt es eine Primzahl ℓ zu finden, für welche die ℓ-adische Galois-Darstellung $\rho_{E,\ell}$ modular ist. Diese Primzahl findet man, indem man zuerst eine Primzahl ℓ sucht, für welche die Galois-Darstellung $\overline{\rho}_{E,\ell}$ in Charakteristik ℓ modular ist. Dies ist relativ einfach; wir werden in Abschnitt 5 darauf zurückkommen. Weiter gilt es dann für sämtliche Hochhebungen ('Deformationen') dieser Galois-Darstellung $\overline{\rho}_{E,\ell}$ zu ℓ-adischen Galois-Darstellungen $\rho_\ell : G \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$, für welche definitionsgemäss das kommutative Diagramm



besteht, unter Verwendung der Modularität von $\overline{\rho}_{E,\ell}$ die Modularität von ρ_ℓ nachzuweisen. Dies ist schwierig; wir werden in Abschnitt 4 darauf eingehen. Zusammengenommen ergibt sich dann insbesondere die gewünschte Modularität von $\rho_{E,\ell}$ und damit der Beweis des Satzes 2.1.

3.6 Hecke-Algebra. Auf $S_2(\Gamma_0(N))$ wirken gewisse Operatoren, die sogenannten *Hecke-Operatoren* T_p $(p \nmid N)$ und U_p $(p|N)$. Ihre Wirkung auf eine Spitzenform $f(\tau) = q + \sum_{n=2}^{\infty} c_n q^n$ ist wie folgt gegeben

$$(T_p f)(\tau) = \sum_{n=1}^{\infty} (c_{np} + p \cdot c_{n/p}) q^n \quad (p \nmid N),$$

$$(U_p f)(\tau) = \sum_{n=1}^{\infty} c_{np} q^n \qquad\qquad (p|N);$$

hierbei ist $c_{n/p} = 0$ zu setzen, falls $n/p \notin \mathbb{Z}$ gilt. Die Hecke-Operatoren erzeugen eine kommutative $\mathbb{Z}$-Algebra, die sogenannte *Hecke-Algebra* $\mathbb{T}(N)$. Es zeigt sich, dass die Hecke-Operatoren T_p $(p \nmid N)$ bezüglich eines gewissen Skalarprodukts auf $S_2(\Gamma_0(N))$, des sogenannten Petersson-Skalarprodukts, selbstadjungiert sind. Aufgrund der Kommutativität von $\mathbb{T}(N)$ existiert somit eine Basis von $S_2(\Gamma_0(N))$, welche aus *simultanen* Eigenfunktionen bezüglich der Hecke-Operatoren T_p $(p \nmid N)$ besteht. Ist f eine solche Eigenfunktion, welche zudem Eigenfunktion der Hecke-Operatoren U_p $(p|N)$ ist, so wird

f primitive Eigenform oder kurz *Neuform* genannt. Für eine Neuform f bestehen also die Beziehungen

$$T_p f = c_p \cdot f \ \ (p \nmid N), \ \ U_p f = c_p \cdot f \ \ (p|N),$$

wobei c_p gerade der p-te Fourierkoeffizient von f ist, und die Zuordnungen

$$T_p \mapsto c_p \ \ (p \nmid N), \ \ U_p \mapsto c_p \ \ (p|N)$$

definieren einen Algebrenhomomorphismus ψ_f von $\mathbb{T}(N)$ nach (einer Erweiterung von) $\mathbb{Z}_\ell$. Umgekehrt definiert ein Algebrenhomomorphismus ψ von $\mathbb{T}(N)$ nach $\mathbb{Z}_\ell$ eine eindeutig bestimmte Neuform $f \in S_2(\Gamma_0(N))$, $f(\tau) = q + \sum_{n=2}^{\infty} c_n q^n$, mit der Eigenschaft

$$c_p = \psi(T_p) \ \ (p \nmid N), \ \ c_p = \psi(U_p) \ \ (p|N);$$

es sei darauf hingewiesen, dass die vorhergehende Aussage richtig bleibt, wenn ψ nur für fast alle Erzeugenden von $\mathbb{T}(N)$ erklärt ist.

3.7 Bemerkung. Spitzenformen zu modularen elliptischen Kurven der Stufe N bzw. zu modularen Galois-Darstellungen der Stufe N sind Neuformen zur Hecke-Algebra $\mathbb{T}(N)$. Ist umgekehrt $f \in S_2(\Gamma_0(N))$ eine Neuform zur Hecke-Algebra $\mathbb{T}(N)$, so lassen sich mit Hilfe der Theorie von Eichler-Shimura (s. [18], Section 7.6) Galois-Darstellungen $\overline{\rho}_\ell$, bzw. ρ_ℓ, konstruieren, welche modular zur Stufe N sind.

4 Deformationen von Galois-Darstellungen

4.1. In diesem Abschnitt fixieren wir eine endliche Menge Σ von Primzahlen mit $\ell \in \Sigma$ und eine *(absolut) irreduzible* Galois-Darstellung $\overline{\rho}_\ell : G \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ in Charakteristik ℓ, welche für alle $p \notin \Sigma$ unverzweigt ist (s. Anhang 6.3) und für $p \in \Sigma$ ein gewisses Verhalten hat, auf das wir hier nicht näher eingehen können. Unter Verwendung der von B. Mazur entwickelten Methoden beweist man dann den folgenden Satz (s. [12], Section 1.2 und [23], Chapter 1, Section 1).

4.2 Satz. *Mit den vorhergehenden Bezeichnungen gilt: Es existiert eine lokale, vollständige $\mathbb{Z}_\ell$-Algebra $\mathcal{R}$ (mit maximalem Ideal $\mathfrak{m}_\mathcal{R}$ und Restklassenkörper $\mathcal{R}/\mathfrak{m}_\mathcal{R} \cong \mathbb{F}_\ell$) und eine universelle Galois-Darstellung $\rho_\mathcal{R} : G \longrightarrow \mathrm{GL}_2(\mathcal{R})$ mit den folgenden Eigenschaften:*

(1) $\rho_\mathcal{R} \bmod \mathfrak{m}_\mathcal{R} \cong \overline{\rho}_\ell$.

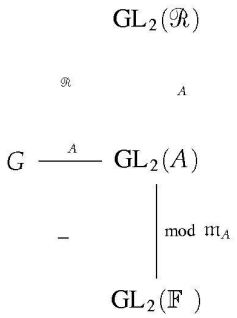
(2) *$\rho_\mathcal{R}$ ist unverzweigt für alle $p \notin \Sigma$.*

(3) $\det \rho_\mathcal{R}(\mathrm{Frob}_p) = p$ *für alle $p \notin \Sigma$.*

(4) *$\rho_\mathcal{R}$ hat ein gewisses Verhalten für die Primzahlen $p \in \Sigma$, auf das hier nicht näher eingegangen werden soll.*

(5) *Jede andere Galois-Darstellung $\rho_A : G \longrightarrow \mathrm{GL}_2(A)$ (hierbei bedeute A eine lokale, vollständige $\mathbb{Z}_\ell$-Algebra mit maximalem Ideal $\mathfrak{m}_A$ und Restklassenkörper $A/\mathfrak{m}_A \cong \mathbb{F}_\ell$) mit den Eigenschaften (1)–(4) definiert einen eindeutig bestimmten*

Algebrenhomomorphismus $\varphi_A : \mathcal{R} \longrightarrow A$ *mit* $\rho_A = \varphi_A \circ \rho_{\mathcal{R}}$*; d.h. es besteht das folgende, kommutative Diagramm:*



4.3. Zur Formulierung des nächsten Satzes bezeichne M das Produkt aller Primzahlen $p \in \Sigma$ mit gewissen nichtnegativen Exponenten, welche durch das Verhalten von $\overline{\rho}_\ell$ an den Stellen $p \in \Sigma$ bestimmt werden; wir können hier nicht näher darauf eingehen. Weiter setzen wir voraus, dass die (absolut) irreduzible Galois-Darstellung $\overline{\rho}_\ell : G \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ in Charakteristik ℓ *modular* zur Stufe M ist, d.h. es gilt $\overline{\rho}_\ell = \overline{\rho}_{f,\ell}$, wobei $f \in S_2(\Gamma_0(M))$, $f(\tau) = q + \sum_{n=2}^{\infty} c_n q^n$, die entsprechende Neuform ist. Wir bemerken, dass das Beispiel 3.4 in diesem Zusammenhang nicht herangezogen werden kann, da die Galois-Darstellung von 3.4 nicht irreduzibel ist. Das zu formulierende, wichtige Ergebnis von A. Wiles ist nun ein Analogon zu Satz 4.2, in dem diejenigen Hochhebungen der Galois-Darstellung $\overline{\rho}_{f,\ell}$ zu ℓ-adischen Galois-Darstellungen charakterisiert werden, welche *modular* sind. Dazu wird mit Hilfe der Hecke-Algebra $\mathbb{T}(M)$ eine 'universelle' Hecke-Algebra konstruiert, welche durch den nachfolgenden Satz beschrieben wird (s. [23], Chapter 2, Section 3).

4.4 Satz. *Mit den vorhergehenden Bezeichnungen gilt: Es existiert eine lokale, vollständige* $\mathbb{Z}_\ell$*-Algebra* $\mathcal{T}$ *(mit maximalem Ideal* $\mathfrak{m}_{\mathcal{T}}$ *und Restklassenkörper* $\mathcal{T}/\mathfrak{m}_{\mathcal{T}} \cong \mathbb{F}_\ell$*) und eine universelle Galois-Darstellung* $\rho_{\mathcal{T}} : G \longrightarrow \mathrm{GL}_2(\mathcal{T})$ *mit den folgenden Eigenschaften:*

(1) *Es existiert ein maximales Ideal* $\mathfrak{m} \subset \mathbb{T}(M)$ *derart, dass* $\mathcal{T}$ *die Vervollständigung der Lokalisierung* $\mathbb{T}(M)_{\mathfrak{m}}$ *von* $\mathbb{T}(M)$ *an* $\mathfrak{m}$ *ist.*

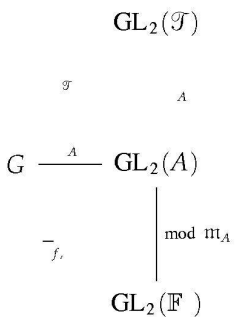
(2) $\rho_{\mathcal{T}} \bmod \mathfrak{m}_{\mathcal{T}} \cong \overline{\rho}_{f,\ell}$.

(3) $\rho_{\mathcal{T}}$ *ist unverzweigt für alle* $p \notin \Sigma$*, und es gilt* $\operatorname{tr} \rho_{\mathcal{T}}(\mathrm{Frob}_p) = T_p$ *für alle* $p \notin \Sigma$ *(hierbei wurde für das natürliche Bild von* $T_p \in \mathbb{T}(M)$ *in* $\mathcal{T}$ *wieder* T_p *geschrieben).*

(4) $\det \rho_{\mathcal{T}}(\mathrm{Frob}_p) = p$ *für alle* $p \notin \Sigma$.

(5) *Jede andere modulare Galois-Darstellung* $\rho_A : G \longrightarrow \mathrm{GL}_2(A)$ *(hierbei bedeute* A *eine lokale, vollständige* $\mathbb{Z}_\ell$*-Algebra mit maximalem Ideal* $\mathfrak{m}_A$ *und Restklassenkörper* $A/\mathfrak{m}_A \cong \mathbb{F}_\ell$*) mit den Eigenschaften* (2)–(4) *definiert einen eindeutig*

bestimmten Algebrenhomomorphismus $\psi_A : \mathcal{T} \longrightarrow A$ *mit* $\rho_A = \psi_A \circ \rho_{\mathcal{T}}$*; d.h. es besteht das folgende, kommutative Diagramm:*



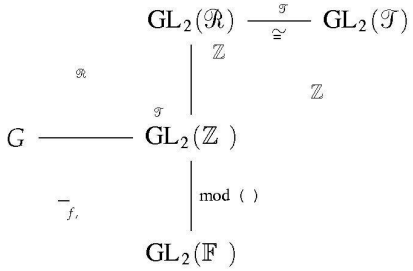
4.5 Bemerkung. (a) Eine Analyse der Konstruktion der Algebra $\mathcal{T}$, insbesondere Satz 4.4 (1), zeigt, dass die (natürlichen Bilder der) Hecke-Operatoren T_p, $p \notin \Sigma$, die Algebra $\mathcal{T}$ erzeugen.

(b) Aufgrund von Satz 4.2 (5) (mit $A = \mathcal{T}$) existiert ein eindeutig bestimmter Algebrenhomomorphismus $\varphi_{\mathcal{T}} : \mathcal{R} \longrightarrow \mathcal{T}$ mit der Eigenschaft $\rho_{\mathcal{T}} = \varphi_{\mathcal{T}} \circ \rho_{\mathcal{R}}$. Zusammen mit der Eigenschaft (3) von $\rho_{\mathcal{T}}$ führt dies für alle $p \notin \Sigma$ zu der Beziehung

$$\varphi_{\mathcal{T}}(\operatorname{tr} \rho_{\mathcal{R}}(\mathrm{Frob}_p)) = \operatorname{tr} \rho_{\mathcal{T}}(\mathrm{Frob}_p) = T_p.$$

Da nun die Hecke-Operatoren T_p, $p \notin \Sigma$, nach (a) die Algebra $\mathcal{T}$ erzeugen, ergibt sich sofort die Surjektivität von $\varphi_{\mathcal{T}}$.

(c) Wir zeigen nun unter der Annahme der *Injektivität* von $\varphi_{\mathcal{T}}$, d.h. der *Isomorphie* von $\varphi_{\mathcal{T}}$, wiederum unter Verwendung der Sätze 4.2 und 4.4, dass jede ℓ-adische Galois-Darstellung $\rho_\ell : G \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ mit der Eigenschaft $\rho_\ell \bmod (\ell) \cong \overline{\rho}_{f,\ell}$ *modular* zur Stufe M ist: Zunächst beachten wir dazu das kommutative Diagramm



Nach der Bemerkung am Ende des Abschnitts 3.6 existiert dann zum Algebrenhomomorphismus $\psi_{\mathbb{Z}_\ell} : \mathcal{T} \longrightarrow \mathbb{Z}_\ell$ eine eindeutig bestimmte Neuform $g \in S_2(\Gamma_0(M))$, $g(\tau) = q + \sum_{n=2}^{\infty} d_n q^n$, so dass für alle Primzahlen $p \notin \Sigma$ die Gleichung

$$d_p = \psi_{\mathbb{Z}_\ell}(T_p)$$

gilt. Mit Hilfe des vorhergehenden Diagramm berechnet man schliesslich für diese Primzahlen p

$$\begin{aligned}\operatorname{tr}\rho_\ell(\mathrm{Frob}_p) &= \operatorname{tr}\left((\varphi_{\mathbb{Z}_\ell}\circ\rho_{\mathcal{R}})(\mathrm{Frob}_p)\right)\\ &= \varphi_{\mathbb{Z}_\ell}\left(\operatorname{tr}\rho_{\mathcal{R}}(\mathrm{Frob}_p)\right) = \varphi_{\mathbb{Z}_\ell}\left(\operatorname{tr}((\varphi_{\mathcal{T}}^{-1}\circ\rho_{\mathcal{T}})(\mathrm{Frob}_p))\right)\\ &= (\varphi_{\mathbb{Z}_\ell}\circ\varphi_{\mathcal{T}}^{-1})\left(\operatorname{tr}\rho_{\mathcal{T}}(\mathrm{Frob}_p)\right) = \psi_{\mathbb{Z}_\ell}(T_p) = d_p.\end{aligned}$$

Daraus folgt, wie behauptet, dass die ℓ-adische Galois-Darstellung $\rho_\ell : G \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ modular zur Stufe M ist. Es ist zu beachten, dass die beiden Neuformen f, g im allgemeinen verschieden sind, deren Fourierkoeffizienten aber für alle $p \notin \Sigma$ den Kongruenzen $c_p \equiv d_p \bmod \ell$ genügen.

4.6 Hauptsatz. *Mit den Bezeichnungen von Satz 4.2 und den Voraussetzungen von Satz 4.4 folgt, dass der surjektive Algebrenhomomorphismus $\varphi_{\mathcal{T}} : \mathcal{R} \longrightarrow \mathcal{T}$ injektiv, d.h. ein Isomorphismus ist.*

Der *Beweis* soll in fünf Schritten kurz skizziert werden; bei jedem Schritt verweisen wir den interessierten Leser für weitere Einzelheiten auf die entsprechenden Seiten in [23] und [21]:

Schritt 1. Die Zuordnung $T_p \mapsto c_p$ (hierbei ist c_p der p-te Fourierkoeffizient von f) definiert einen Algebrenhomomorphismus $\pi : \mathcal{T} \longrightarrow \mathbb{Z}_\ell$. Damit setze man $\mathfrak{p}_{\mathcal{T}} := \ker\pi$ und $\mathfrak{p}_{\mathcal{R}} := \ker(\pi\circ\varphi_{\mathcal{T}}) = \varphi_{\mathcal{T}}^{-1}(\mathfrak{p}_{\mathcal{T}})$. Aus einem Resultat von B. Mazur (s. [11], Sections II.15–II.17) folgt weiter, dass $\mathcal{T}$ eine Gorenstein-Algebra ist, d.h. es gilt $\mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{T}, \mathbb{Z}_\ell) \cong \mathcal{T}$. Es bezeichne dann $\pi' \in \mathcal{T}$ das Bild von $\pi \in \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathcal{T}, \mathbb{Z}_\ell)$ unter diesem Isomorphismus, und man setze $\eta := \pi(\pi') \in \mathbb{Z}_\ell$. Mit diesen Bezeichnungen beweist man die Ungleichungen

$$\#\mathfrak{p}_{\mathcal{R}}/\mathfrak{p}_{\mathcal{R}}^2 \geq \#\mathfrak{p}_{\mathcal{T}}/\mathfrak{p}_{\mathcal{T}}^2 \geq \#\mathbb{Z}_\ell/(\eta).$$

Dies ist relativ einfach und findet sich in [23], S. 515.

Schritt 2. Die Komposition der Galois-Darstellung $\overline{\rho}_{f,\ell} : G \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ mit der adjungierten Darstellung $\mathrm{Ad} : \mathrm{GL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{Aut}(\mathrm{M}_2(\mathbb{F}_\ell))$ induziert die Darstellung

$$\mathrm{Ad}\,\overline{\rho}_{f,\ell} : G \longrightarrow \mathrm{Aut}(V_\ell)$$

mit $V_\ell := \mathrm{M}_2(\mathbb{F}_\ell)$. Damit stellt man fest, dass der Tangentialraum $\mathrm{Hom}\left(\mathfrak{m}_{\mathcal{R}}/(\mathfrak{m}_{\mathcal{R}}^2, \ell), \mathbb{F}_\ell\right)$ von $\mathrm{Spec}\,\mathcal{R}/(\ell)$, d.h. der speziellen Faser von $\mathrm{Spec}\,\mathcal{R}$ über $\mathrm{Spec}\,\mathbb{Z}_\ell$, der Bijektion

$$\mathrm{Hom}\left(\mathfrak{m}_{\mathcal{R}}/(\mathfrak{m}_{\mathcal{R}}^2, \ell), \mathbb{F}_\ell\right) \cong H^1_{Sel}(G, V_\ell)$$

genügt, wo $H^1_{Sel}(G, V_\ell)$ eine gewisse Untergruppe der Galois-Kohomologiegruppe $H^1(G, V_\ell)$ ist, welche durch lokale Bedingungen an den Primstellen $p \in \Sigma$ erklärt ist (s. [23], S. 460f.); $H^1_{Sel}(G, V_\ell)$ heisst *Selmer-Gruppe*. Allgemeiner lassen sich für jedes $\nu = 1, 2, 3, \ldots$ Selmer-Gruppen $H^1_{Sel}(G, V_{\ell^\nu})$ definieren, wo $V_{\ell^\nu} := \mathrm{M}_2(\mathbb{Z}/\ell^\nu\mathbb{Z})$ ist; damit setzt man

$$H^1_{Sel}(G, V) := \bigcup_{\nu=1}^{\infty} H^1_{Sel}(G, V_{\ell^\nu}).$$

Die obige Bijektion führt dann zu der Gleichheit

$$\#\mathfrak{p}_{\mathcal{R}}/\mathfrak{p}_{\mathcal{R}}^2 = \#H^1_{Sel}(G,V).$$

Die Einzelheiten hierzu finden sich in [23], Proposition 1.2, S. 464f.

Schritt 3. Die lokale, vollständige $\mathbb{Z}_\ell$-Algebra $\mathcal{T}$ lässt sich in der Form

$$\mathcal{T} = \mathbb{Z}_\ell[[X_1,\ldots,X_r]]/I$$

darstellen, wobei $X_1,\ldots,X_r$ Unbestimmte und I ein Ideal des Potenzreihenrings $\mathbb{Z}_\ell[[X_1,\ldots,X_r]]$ ist. Man beweist nun, dass das Ideal I durch $(r-\dim\mathcal{T})$ Elemente erzeugt wird, d.h. dass die Algebra $\mathcal{T}$ ein vollständiger Durchschnitt ist. Man erhält dieses wichtige Ergebnis, indem man anstelle der 'universellen' Hecke-Algebra $\mathcal{T}$ zur Stufe M eine unendliche Folge von analog konstruierten 'universellen' Hecke-Algebren $\mathcal{T}_n$ $(n=1,2,3,\ldots)$, im wesentlichen zu den Stufen $M\cdot q_1\cdot\ldots\cdot q_r$, betrachtet, wobei $q_1,\ldots,q_r$ Primzahlen sind, welche $q_j\equiv 1 \bmod \ell^n$ erfüllen und weiteren technischen Bedingungen genügen. Für $n\gg 0$ ergibt sich dann, dass die Algebra $\mathcal{T}_n$ ein vollständiger Durchschnitt ist, und mit dem Kriterium von E. Kunz (s. [8], Section 2) folgt damit, dass $\mathcal{T}$ ein vollständiger Durchschnitt ist. Die Einzelheiten hierzu finden sich in der Arbeit [21].

Schritt 4. Die vollständige Durchschnitt-Eigenschaft der Algebra $\mathcal{T}$ führt mit etwas Kommutativer Algebra unmittelbar zur Gleichung

$$\#\mathfrak{p}_{\mathcal{T}}/\mathfrak{p}_{\mathcal{T}}^2 = \#\mathbb{Z}_\ell/(\eta).$$

Dies findet sich in [23], Appendix, Proposition 2. Eine weitere Konsequenz der vollständigen Durchschnitt-Eigenschaft der Algebra $\mathcal{T}$ ist die Ungleichung

$$\#H^1_{Sel}(G,V) \le \#\mathfrak{p}_{\mathcal{T}}/\mathfrak{p}_{\mathcal{T}}^2.$$

Dies ist der Inhalt von [23], Chapter 3.

Schritt 5. Fasst man jetzt die Resultate der Schritte 1, 2 und 4 zusammen, so hat man die Gleichheiten

$$\#H^1_{Sel}(G,V) = \#\mathfrak{p}_{\mathcal{R}}/\mathfrak{p}_{\mathcal{R}}^2 = \#\mathfrak{p}_{\mathcal{T}}/\mathfrak{p}_{\mathcal{T}}^2 = \#\mathbb{Z}_\ell/(\eta).$$

Die mittlere Gleichheit und die vollständige Durchschnitt-Eigenschaft der Algebra $\mathcal{T}$ führen schliesslich zur behaupteten Isomorphie $\mathcal{R}\cong\mathcal{T}$. Dies findet sich in [23], Appendix, Proposition 1. □

5 Das Ende des Beweises

5.1. In diesem Abschnitt soll der Beweis des Satzes 2.1 abgeschlossen werden. Es sei also $E/\mathbb{Q}$ eine semistabile elliptische Kurve mit geometrischem Führer N_E. Wir haben zu zeigen, dass E modular zur Stufe $N = N_E$ ist. Dazu betrachten wir die Galois-Darstellung $\overline{\rho}_{E,3}$ in Charakteristik 3, wählen Σ als die Menge aller Primteiler von N_E zusammen mit $\ell = 3$ und definieren M wie in Abschnitt 4.3. Es werden nun drei Fälle unterschieden. Den interessierten Leser verweisen wir für weitere Einzelheiten auf die Seiten 541–544 in [23].

5.2. Zuerst nehmen wir an, dass die Galois-Darstellung $\overline{\rho}_{E,3}$ irreduzibel ist. Aufgrund dieser Annahme, der Wahl von Σ und der Semistabilität von E zeigt sich, dass die Voraussetzungen 4.1 von Satz 4.2 erfüllt sind. Weiter zeigt man mit Hilfe eines Resultats von R.P. Langlands (s. [10]) und einer Ergänzung dazu von J. Tunnell (s. [22]), dass $\overline{\rho}_{E,3}$ modular zur Stufe M ist. Somit gilt $\overline{\rho}_{E,3} = \overline{\rho}_{f,3}$ mit einer Neuform $f \in S_2(\Gamma_0(M))$. Damit sind jetzt auch die Voraussetzungen 4.3 von Satz 4.4 erfüllt. Eine Anwendung des Hauptsatzes 4.6 zusammen mit der Bemerkung 4.5(c) beweist dann die Modularität der 3-adischen Galois-Darstellung $\rho_{E,3}$ und somit die Modularität von E zur Stufe M; daraus ergibt sich schliesslich auch die Modularität von E zur Stufe $N = N_E$.

5.3. Als nächstes nehmen wir an, dass die Galois-Darstellung $\overline{\rho}_{E,3}$ reduzibel, aber $\overline{\rho}_{E,5}$ irreduzibel ist. Unter dieser Voraussetzung konstruiert man eine semistabile elliptische Kurve $E'/\mathbb{Q}$, welche die beiden folgenden Eigenschaften hat:

(i) Die Galois-Darstellung $\overline{\rho}_{E',3}$ ist irreduzibel.

(ii) Es besteht ein G-äquivarianter Isomorphismus $E'[5] \cong E[5]$, d.h. die Galois-Darstellungen $\overline{\rho}_{E',5}$ und $\overline{\rho}_{E,5}$ sind isomorph.

Wegen (i) lassen sich die in 5.2 durchgeführten Überlegungen auf die elliptische Kurve $E'/\mathbb{Q}$ anwenden. Damit ergibt sich die Modularität der 3-adischen Galois-Darstellung $\rho_{E',3}$, also mit dem Satz von Faltings auch die Modularität der 5-adischen Galois-Darstellung $\rho_{E',5}$, insbesondere also auch die Modularität von $\overline{\rho}_{E',5}$. Aufgrund der Isomorphie (ii) folgt dann die Modularität der Galois-Darstellung $\overline{\rho}_{E,5}$. Nun folgert man wie in 5.2 die Modularität der 5-adischen Galois-Darstellung $\rho_{E,5}$ und somit die Modularität von E zur Stufe $N = N_E$.

5.4. Es bleibt schliesslich der Fall, dass sowohl $\overline{\rho}_{E,3}$ als auch $\overline{\rho}_{E,5}$ reduzibel sind. Unter dieser Voraussetzung überlegt man sich, dass dann die Semistabilität von $E/\mathbb{Q}$ verletzt ist, d.h. dieser Fall braucht nicht behandelt zu werden. Trotzdem bemerken wir, dass sich in diesem Fall die elliptische Kurve ebenfalls als modular zur Stufe $N = N_E$ herausstellt. □

Anhang

6.1 ℓ-adische Zahlen. Es sei ℓ eine Primzahl. Für jedes $\nu = 1, 2, 3, \ldots$ betrachte man die Restklassenringe $\mathbb{Z}/\ell^\nu\mathbb{Z}$; mit Hilfe der Zuordnung

$$a \bmod \ell^\nu \mapsto a \bmod \ell^{\nu-1}$$

erhält man Ringhomomorphismen

$$\varphi_\nu : \mathbb{Z}/\ell^\nu\mathbb{Z} \longrightarrow \mathbb{Z}/\ell^{\nu-1}\mathbb{Z}.$$

Die *ganzen ℓ-adischen Zahlen* $\mathbb{Z}_\ell$ sind nun definiert als die Menge aller Tupel $(\ldots, a_\nu, \ldots, a_1)$ mit $a_\nu \in \mathbb{Z}/\ell^\nu\mathbb{Z}$ $(\nu = 1, 2, 3, \ldots)$ und $\varphi_\nu(a_\nu) = a_{\nu-1}$ für alle $\nu = 2, 3, 4, \ldots$. Man sagt, $\mathbb{Z}_\ell$ sei der *inverse Limes* des (projektiven) Systems $\{\mathbb{Z}/\ell^\nu\mathbb{Z}\}_{\nu=1}^{\infty}$, und schreibt

$$\mathbb{Z}_\ell = \varprojlim_{\nu\to\infty} \mathbb{Z}/\ell^\nu\mathbb{Z}.$$

Es zeigt sich, dass $\mathbb{Z}_\ell$ ein Integritätsbereich ist und dass die Isomorphie $\mathbb{Z}_\ell/\ell\,\mathbb{Z}_\ell \cong \mathbb{F}_\ell$ besteht. Indem man einer ganzen Zahl $a \in \mathbb{Z}$ das Tupel $(\ldots, a \bmod \ell^\nu, \ldots, a \bmod \ell)$ zuordnet, erhält man eine Einbettung der ganzen Zahlen $\mathbb{Z}$ in die ganzen ℓ-adischen Zahlen $\mathbb{Z}_\ell$. Der Quotientenkörper von $\mathbb{Z}_\ell$ ist der Körper der *ℓ-adischen Zahlen* $\mathbb{Q}_\ell$, welcher folgende weitere Charakterisierung hat: Ist $a \in \mathbb{Q}$, so können wir mit eindeutig bestimmtem $\alpha \in \mathbb{Z}$, $a = \ell^\alpha \cdot a'$ schreiben, wobei a' eine rationale Zahl ist, deren Zähler und Nenner nicht durch ℓ teilbar sind. Die *ℓ-adische Norm* $\|a\|_\ell$ von a ist dann gegeben durch

$$\|a\|_\ell := e^{-\alpha}.$$

Man beweist, dass der Körper $\mathbb{Q}_\ell$ die Vervollständigung von $\mathbb{Q}$ bezüglich der ℓ-adischen Norm ist.

Eine ausgezeichnete und ausführlichere Behandlung der ℓ-adischen Zahlen findet sich in [16], Chapter II.

6.2 Die Gruppenstruktur einer elliptischen Kurve. Eine elliptische Kurve $E/\mathbb{Q}$ sei vorgelegt (s. [7], Abschnitt 3); der Einfachheit halber sei hier angenommen, dass E durch eine Gleichung der Form

$$E : Y^2 = X^3 + a_2X^2 + a_4X + a_6$$

mit $a_2, a_4, a_6 \in \mathbb{Q}$ gegeben ist. Sind P, Q zwei Punkte auf E, so kann diesen wie folgt ein dritter Punkt $R \in E$ zugeordnet werden: Man legt zunächst die Verbindungsgerade L durch P, Q; ist $P = Q$, so wählt man für L die Tangente an P. Da die Kurve E vom Grad 3 ist, schneidet L die Kurve E in genau einem weiteren Punkt $R' \in E$; indem man R' an der X-Achse spiegelt, erhält man den gewünschten Punkt $R \in E$. Man setzt nun $P + Q := R$ und überzeugt sich, dass damit E zu einer *kommutativen Gruppe* wird. Der unendlich ferne Punkt $O_E \in E$ übernimmt dabei die Rolle des neutralen Elements. Ist $P = (x_P, y_P), Q = (x_Q, y_Q)$ und $x_P \neq x_Q$, so sind die Koordinaten (x_R, y_R) von R gegeben durch die Formeln

$$x_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q - a_2,$$

$$y_R = \left(\frac{y_Q - y_P}{x_Q - x_P}\right) \cdot (x_P - x_R) - y_P.$$

Im Fall $x_P = x_Q$ hat man $P = \mp Q$; im ersteren Fall ergibt sich $R = P - P = O_E$; im letzteren folgt $R = P + P$ mit den Koordinaten

$$x_R = \frac{x_P^4 - 2a_4x_P^2 - 8a_6x_P + a_4^2 - 4a_2a_6}{4y_P^2},$$

$$y_R = \frac{x_P^3 - 3x_P^2x_R - 2a_2x_Px_R - a_4(x_P + x_R) - 2a_6}{2y_P}.$$

Ist $n \in \mathbb{Z}$, so bezeichne man mit $[n] : E \longrightarrow E$ den Morphismus 'Multiplikation mit n'; dieser ist also gegeben durch

$$[n](P) = P + \cdots + P \quad (n\text{–mal}).$$

Im Spezialfall $n = 2$ erhält man die Koordinaten von $[2](P) = P + P$ gerade mit Hilfe der vorhergehenden Formeln. Im allgemeinen beweist man, dass $E[n] := \ker[n]$ als $\mathbb{Z}$-Modul isomorph zu $(\mathbb{Z}/n\mathbb{Z})^2$ ist.

Wie bereits in [7] seien zu diesem Themenkomplex wieder die Lehrbücher [5], [6] und [19] empfohlen.

6.3 Der Frobenius-Automorphismus. Es sei $K/\mathbb{Q}$ eine endliche Galois-Erweiterung und $\mathbb{O}_K \subset K$ der Ring der ganzen Zahlen von K. Ist dann p eine Primzahl, so ist das Ideal $p \cdot \mathbb{O}_K$ im allgemeinen kein Primideal, aber es lässt sich (bis auf die Reihenfolge) in eindeutiger Weise als Potenzprodukt von r Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ schreiben, nämlich

$$p \cdot \mathbb{O}_K = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r)^e.$$

Die natürliche Zahl e heisst der *Verzweigungsindex* von p; die Primzahl p heisst *unverzweigt* in $\mathbb{O}_K$, falls $e = 1$ ist, andernfalls heisst p *verzweigt* in $\mathbb{O}_K$. Die Galois-Gruppen $D_j := \mathrm{Gal}(\mathbb{O}_K/\mathfrak{p}_j \,/\, \mathbb{F}_p)$ der endlichen Galois-Erweiterungen $\mathbb{O}_K/\mathfrak{p}_j$ von $\mathbb{F}_p$ haben unabhängig von j alle dieselbe Ordnung f, der *Restklassengrad* von p; mit diesen Bezeichnungen besteht übrigens die Formel

$$e \cdot f \cdot r = [K : \mathbb{Q}].$$

Die Galois-Gruppen D_j sind zyklisch und werden durch die Substitutionen $\alpha \mapsto \alpha^p$ ($\alpha \in \mathbb{O}_K/\mathfrak{p}_j$) erzeugt, welche durch $\mathrm{Frob}_{\mathfrak{p}_j}$ ($j = 1, \ldots, r$) bezeichnet und *Frobenius-Automorphismen* genannt werden. Im unverzweigten Fall lassen sich die Galois-Gruppen D_j in die absolute Galois-Gruppe G einbetten; sie werden dann *Zerlegungsgruppen* von $\mathfrak{p}_j$ genannt. Mit $\mathrm{Frob}_{\mathfrak{p}_j}$ ($j = 1, \ldots, r$) erhält man somit r ausgezeichnete Elemente von G, welche sich sämtlich als zueinander konjugiert herausstellen.

Es sei schliesslich $\rho : G \longrightarrow \mathrm{GL}_2(R)$ ($R = \mathbb{F}_\ell, \mathbb{Z}_\ell$) eine Galois-Darstellung, d.h. ein in der Krull-Topologie stetiger Gruppenhomomorphismus. Dann betrachten wir speziell den (galoisschen) Fixpunktkörper $K/\mathbb{Q}$ zum Kern $\ker\rho$ von ρ, d.h.

$$K = \overline{\mathbb{Q}}^{\ker\rho} = \{\alpha \in \overline{\mathbb{Q}} \,|\, \sigma(\alpha) = \alpha \;\; \forall \sigma \in \ker\rho\},$$

mit dem Ring der ganzen Zahlen $\mathbb{O}_K$. Die Galois-Darstellung ρ heisst dann *unverzweigt* (resp. *verzweigt*) für die Primzahl p, falls p unverzweigt (resp. verzweigt) in $\mathbb{O}_K$ ist.

Weitere Einzelheiten zu diesem Themenkomplex sind in den Lehrbüchern [4], I. Teil, und [9], Chapter I, zu finden.

Literatur

[1] *H. Darmon, F. Diamond, R. Taylor*, Fermat's last theorem, in 'Current Developments in Mathematics', ed. by R. Bott et al. International Press, Cambridge, Massachusetts 1995.

[2] *G. Faltings*, Endlichkeitssätze für abelsche Varietäten. Invent. Math. **73** (1983), 349–366.

[3] *G. Faltings*, Der Beweis der Fermat-Vermutung durch R. Taylor und A. Wiles. DMV-Mitteilungen **2** (1995), 6–8.

[4] *H. Hasse*, Vorlesungen über Klassenkörpertheorie. Physica-Verlag, Würzburg 1967.

[5] *D. Husemöller*, Elliptic curves. Graduate Texts in Math. **111**, Springer-Verlag, Berlin-Heidelberg-New York 1987.

[6] *A.W. Knapp*, Elliptic curves. Math. Notes **40**, Princeton University Press, Princeton, New Jersey 1992.

[7] *J. Kramer*, Über die Fermat-Vermutung. El. Math. **50** (1995), 11–25.

[8] *E. Kunz*, Almost complete intersections are not Gorenstein. J. of Alg. **28** (1974), 111–115.

[9] *S. Lang*, Algebraic number theory. Addison-Wesley Publishing Company, Reading Massachusetts 1970.

[10] *R.P. Langlands*, Base change for GL(2). Ann. of Math. Studies **96**, Princeton University Press, Princeton, New Jersey 1980.

[11] *B. Mazur*, Modular curves and the Eisenstein ideal. Publ. Math. IHES **47** (1977), 33–186.

[12] *B. Mazur*, Deforming Galois representations, in 'Galois groups over $\mathbb{Q}$'. Springer-Verlag, New York-Berlin-Heidelberg-London-Paris-Tokyo-Hong Kong 1989.

[13] *V.K. Murty (ed.)*, Seminar on Fermat's last theorem. CMS Conf. Proc. **17**, Amer. Math. Soc., Providence, Rhode Island 1995.

[14] *K.A. Ribet*, On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. Invent. Math. **100** (1990), 431–476.

[15] *K.A. Ribet*, Galois representations and modular forms. Bull. Amer. Math. Soc. (N.S.) **32** (1995), 375–402.

[16] *J-P. Serre*, A course in arithmetic. Graduate Texts in Math. **7**, Springer-Verlag, New York-Heidelberg-Berlin 1973.

[17] *J-P. Serre*, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J. **54** (1987), 179–230.

[18] *G. Shimura*, Introduction to the arithmetic theory of automorphic forms. Princeton University Press, Princeton, New Jersey 1971.

[19] *J.H. Silverman*, The arithmetic of elliptic curves. Graduate Texts in Math. **106**, Springer-Verlag, Berlin-Heidelberg-New York-Tokyo 1986.

[20] *H.P.F. Swinnerton-Dyer*, Numerical tables on elliptic curves, in 'Modular functions of one variable IV', ed. by W. Kuyk et al. Lecture Notes in Math. **476** (1975), 75–144.

[21] *R. Taylor, A. Wiles*, Ring theoretic properties of certain Hecke algebras. Ann. Math. **141** (1995), 553–572.

[22] *J. Tunnell*, Artin's conjecture for representations of octahedral type. Bull. Amer. Math. Soc. (N.S.) **5** (1981), 173–175.

[23] *A. Wiles*, Modular elliptic curves and Fermat's Last Theorem. Ann. Math. **141** (1995), 443–551.

Jürg Kramer
Institut für Mathematik
Humboldt-Universität zu Berlin
Unter den Linden 6
D-10099 Berlin