Matrixgleichungen und Familien abelscher Varietäten in positiver Charakteristik

Ulrich Görtz

Ulrich Görtz
(Foto: Privat)

Der Bonner Zahlentheoretiker Ulrich Görtz hat gemeinsam mit Arthur Bartels (Münster) den von Kaven-Ehrenpreis für Mathematik erhalten. Der mit je 10 000 Euro dotierte Preis wurde am 15. September 2008 im Rahmen der Eröffnung der Jahrestagung der Deutschen Mathematiker-Vereinigung (DMV) in Erlangen verliehen. Der renommierte Preis wird von der von Kaven-Stiftung vergeben, die von der Deutschen Forschungsgemeinschaft (DFG) verwaltet wird.
Ulrich Görtz forscht auf dem Gebiet der arithmetischen algebraischen Geometrie. Nach seinem Diplom 1997 an der Universität Münster fertigte er eine Dissertation an der Universität Köln an und wurde dort im Jahr 2000 promoviert. Auslandsaufenthalte führten ihn an das Institut Henri Poincaré nach Paris, das Institute for Advanced Study in Princeton, das Fields Institute in Toronto sowie an die University of Chicago.
Ende 2006 habilitierte sich Dr. Görtz an der Universität Bonn und bewarb sich von dort aus im Jahr 2007 erfolgreich für ein Heisenberg-Stipendium der DFG, mit dem er nun am Mathematischen Institut der Bonner Uni tätig ist. Besonders angetan haben es dem in Münster geborenen Mathematiker algebraisch-geometrische Probleme, die ihren Ursprung im Langlands-Programm oder der Theorie der Shimura-Varietäten haben. Dabei gibt es Beziehungen zu mehreren Gebieten der Mathematik, neben der algebraischen Geometrie und Zahlentheorie insbesondere auch zur Darstellungstheorie. (DFG/Universität Bonn)

Im Folgenden stellt der Preisträger sein Arbeitsgebiet vor.

1 Einführung

Das Thema der arithmetischen Geometrie ist die Untersuchung von Polynomgleichungen, insbesondere in Hinsicht auf die geometrische Struktur ihrer Lösungsmengen. Speziell interessiert man sich – und so kommt die Arithmetik, die Zahlentheorie, ins Spiel – für Gleichungen mit ganzzahligen Koeffizienten und ganzzahlige Lösungen davon. Ein prominentes Beispiel ist die *Fermatsche Vermutung*, die besagt, dass die Gleichung $x^n + y^n = z^n$ keine Lösungen mit $x, y, z \in \mathbb{Z}$, $x, y, z \neq 0$, besitzt. Sie wurde bekanntermaßen vor einigen Jahren von Andrew Wiles gelöst, unter Zuhilfenahme schwieriger Methoden der arithmetischen Geometrie und aufbauend auf den Resultaten vieler anderer Mathematiker.

Ein wichtiger Bestandteil von Wiles' Beweis und allgemein der heutigen Zahlentheorie sind die elliptischen Kurven (siehe Beispiel 3). Der Name *elliptisch* beruht auf einem ziemlich indirekten Zusammenhang zu Ellipsen. Elliptische Funktionen und dann elliptische Kurven kommen zum Beispiel ins Spiel, wenn man den Umfang einer Ellipse berechnen will. Elliptische Kurven und ihre höherdimensionalen Analoga, die abelschen Varietäten, sind mindestens seit Riemanns Arbeit über die Theorie der abelschen Funktionen (1857), wenn auch damals natürlich in anderer Sprache, Gegenstand der algebraischen Geometrie und Zahlentheorie.

Erstaunlicherweise kann man die Menge aller elliptischen Kurven, oder allgemeiner aller abelschen Varietäten einer festen Dimension g (mit gewissen Zusatzstrukturen), wieder als ein geometrisches Objekt betrachten: man erhält eine Modulkurve oder allgemeiner einen Modulraum abelscher Varietäten, d. h. jeder Punkt in diesem Parameterraum entspricht einer elliptischen Kurve bzw. einer abelschen Varietät. Der Name „Modulraum" geht auf Riemann zurück. Er schreibt in loc. cit. in einem etwas anderen Kontext:

> Es hängt also [...] die [...] Klasse algebraischer Gleichungen von $3p - 3$ stetig veränderlichen Größen ab, welche die Moduln dieser Klasse genannt werden sollen.

In heutiger Sprechweise: Der Modulraum glatter projektiver Kurven vom Geschlecht $g \geq 2$ hat die Dimension $3g - 3$. Eine gut zugängliche Einführung über das Konzept des Modulraums oder Parameterraums hat Ben-Zvi [Be] geschrieben.

Das Thema des vorliegenden Artikels ist das Studium solcher Modulräume über Körpern positiver Charakteristik. Dort verhalten sich viele Dinge anders als über den komplexen Zahlen. Ein typisches Phänomen ist, dass die betrachteten Räume nicht glatt sind, sondern dass Singularitäten auftreten. Man spricht dann von einem Fall „schlechter Reduktion", und dieser Fall interessiert mich hier besonders.

Auch wenn man die Singularitäten zunächst als zusätzliche Schwierigkeit wahrnehmen wird, ist es dennoch sinn-

voll, diese Räume zu untersuchen, und neben interessanten Konsequenzen stößt man auf ganz konkrete und auch für sich genommen interessante Probleme, zum Beispiel im Bereich der kommutativen Algebra und elementaren algebraischen Geometrie, in der Theorie reduktiver algebraischer Gruppen und ihrer affinen Grassmannschen und affinen Flaggenvarietäten und über die Kombinatorik der zugrundeliegenden (affinen) Wurzelsysteme.

Eine wichtige Motivation für diese Untersuchungen ist das Langlands-Programm, ein wichtiges und ganz aktuelles Vermutungsgebäude der Zahlen- und Darstellungstheorie, das seit Ende der sechziger Jahre von Robert Langlands aufgebaut wurde und das, vereinfacht gesagt, präzise Vorhersagen über erstaunliche Zusammenhänge zwischen algebraischen und analytischen Objekten macht. Auf der algebraischen Seite treten beispielsweise Galois-Gruppen und ihre Darstellungen sowie algebraische Varietäten auf, auf der analytischen Seite sind typische Objekte algebraische Gruppen (etwa über $\mathbb{R}$, nichtarchimedischen lokalen Körpern oder dem Ring der Adele eines Zahlkörpers oder Funktionenkörpers) und ihre Darstellungen oder Modulformen oder allgemeiner automorphe Formen und automorphe Darstellungen.

Etwas konkreter besagt die Langlands-Korrespondenz im Fall eines endlichen Erweiterungskörpers K des Körpers der p-adischen Zahlen $\mathbb{Q}_p$, dass eine Bijektion besteht zwischen gewissen n-dimensionalen Darstellungen der Weil-Gruppe von K (einer Untergruppe der absoluten Galois-Gruppe $\mathrm{Gal}(\overline{K}/K)$) und gewissen Darstellungen der p-adischen Gruppe $GL_n(K)$. Im Fall $n = 1$ ist dies eine direkte Konsequenz aus der Klassenkörpertheorie für K. Der allgemeine Fall wurde vor einigen Jahren von Harris und Taylor bewiesen, die die Korrespondenz realisieren durch die simultane Operation der beiden relevanten Gruppen auf der Kohomologie von Modulräumen abelscher Varietäten. Hier ist besonders ein gutes Verständnis der Fälle schlechter Reduktion unabdingbar.

Eine andere wichtige Facette ist die Vermutung, dass sich Zeta-Funktion algebraischer Varietäten ausdrücken lassen in Termen von Zeta-Funktionen automorpher Darstellungen. So fügt sich auch die von Wiles, Taylor und anderen bewiesene Taniyama-Shimura-Weil-Vermutung, dass jede elliptische Kurve über den rationalen Zahlen modular ist, ins Langlands-Programm ein. In diesem Fall sind die algebraischen bzw. analytischen Objekte die elliptischen Kurven bzw. die „zugehörigen" Modulformen. Die Zeta-Funktion der hier betrachteten Modulräume, sogenannter Shimura-Varietäten, durch automorphe L-Funktionen darzustellen, bleibt in den meisten Fällen eine spannende offene Frage.

Was diese äußerst abstrakte Mathematik besonders reizvoll macht, ist, dass der aufwendige technische Apparat der algebraischen Geometrie genutzt werden kann, um elementare (und doch tiefliegende) Probleme der Zahlentheorie zu lösen (siehe auch Abschnitt 3.3 über Delignes Beweis der Ramanujan-Vermutung), und dass man auf sehr zugängliche und dennoch fesselnde Probleme trifft – zum Beispiel im Bereich der kommutativen Algebra auf gewisse Matrixgleichungen. Davon handelt der nächste Abschnitt.

2 Matrixgleichungen

2.1 (2×2)-*Matrizen vom Quadrat* 0

Wir beginnen ganz elementar (und werden im Abschnitt 4.1 den Zusammenhang zu Modulräumen abelscher Varietäten herstellen). Sei k ein Körper und $M_{r\times n}(k)$ der Raum der $(r \times n)$-Matrizen über k. Sei

$$X = X(k) = \{A \in M_{2\times 2}(k);\ A^2 = 0\}.$$

Wir verstehen X als die Lösungsmenge eines polynomialen Gleichungssystems in vier Unbestimmten: Schreiben wir

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

so ist

$$\begin{aligned} X(k) = \{&(a,b,c,d) \in k^4; \\ &a^2 + bc = b(a+d) = c(a+d) = d^2 + bc = 0\}. \end{aligned}$$

Dieses Objekt kann man nun mit den Methoden der algebraischen Geometrie (bzw. der kommutativen Algebra studieren). Wir wollen eine einfache Fragestellung konkretisieren. Was ist die Menge $I(X)$ aller Polynome in $k[a,b,c,d]$, die auf X verschwinden? Offenbar ist diese Menge ein Ideal, und sie enthält das Ideal

$$I = (a^2 + bc, b(a+d), c(a+d), d^2 + bc).$$

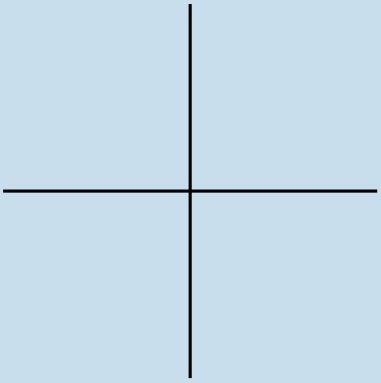
Allerdings ist $I(X)$ größer als I. Verstehen wir die Punkte von k^4 wieder als Matrizen, so sind die Punkte von X gerade die nilpotenten Matrizen. Wir sehen, dass die Spur $a + d$ und die Determinante $ad - bc$ ebenfalls auf X verschwinden, und eine leichte Rechnung zeigt, dass $I(X) = (a+d, ad-bc) \supsetneq I$. Wir nennen ein System von Gleichungen

$$f_1 = \cdots = f_r = 0, \quad f_i \in k[T_1, \ldots, T_n],$$

reduziert, wenn das Ideal $I = (f_1, \ldots, f_r)$ alle Polynome umfasst, die auf der gemeinsamen Nullstellenmenge V der f_i verschwinden. Eine äquivalente Charakterisierung ist, dass der *affine Koordinatenring* $\Gamma(V) := k[T_1, \ldots, T_n]/I$ reduziert ist, d. h. keine nilpotenten Elemente besitzt. Das Gleichungssystem

$$a^2 + bc = b(a+d) = c(a+d) = d^2 + bc = 0,$$

das wir für die Definition von X verwendet haben, ist also nicht reduziert.



Die Lösungsmenge $Z_{1,2}(k)$

Beispiel 1. Der Fall $r = 1$, $n = 2$ ist der einfachste Fall dieser Singularitäten. Die Gleichung ist dann einfach $XY = 0$ (in der X, Y-Ebene), ihre Lösungsmenge das Achsenkreuz in der Ebene.

2.2 *Zirkuläre Komplexe*

Betrachten wir nun ein komplizierteres Gleichungssystem, das wieder durch Matrizengleichungen gegeben ist. Wir fixieren natürliche Zahlen r und n und setzen

$$Z_{r,n}(k) = \{(M_1, \dots, M_n) \in (M_{r\times r}(k))^n; \\ M_1 \cdots M_n = M_2 \cdots M_n M_1 = \cdots \\ = M_n M_1 \cdots M_{n-1} = 0\}.$$

Ähnlich wie oben ist $Z_{r,n}(k) \subseteq k^{r^2 n}$ die Lösungsmenge eines Systems von Polynomgleichungen, das wir mit $Z_{r,n}$ bezeichnen.

Für $r = 1$ handelt es sich hier um (1×1)-Matrizen, also einfach um Unbestimmte. Diese vertauschen miteinander, so dass man es nur noch mit der einen Gleichung $M_1 \cdots M_n = 0$ zu tun hat. Dieses Gleichungssystem ist offensichtlich reduziert. Für $n = 2$ wurde die Reduziertheit von E. Strickland 1982 gezeigt. Diesen Fall nennt man auch die *Varietät der zirkulären Komplexe*; er wurde auch von anderen studiert. Für größeres n werden die Gleichungen extrem kompliziert. Schon im Fall $r = 3$, $n = 3$ reichen die 16 GB Arbeitsspeicher in dem mir zur Verfügung stehenden Rechner nicht aus, um die Reduziertheit mit einem der gängigen Computeralgebra-Programme zu überprüfen.

Theorem 1. *Das Gleichungssystem $Z_{r,n}$ ist reduziert.*

Das Theorem folgt aus den Ergebnissen von [GI], siehe insbesondere den dortigen Abschnitt 4.4.5. Zum Beweis des Theorems bettet man $Z_{r,n}$ ein in eine „affine Flaggenvarietät“ und zeigt, dass man $Z_{r,n}$ mit einer offenen Teilmenge eines Durchschnitts von Schubertvarietäten identifizieren kann. Solche Durchschnitte sind, wie im endlich-dimensionalen Fall, stets reduziert. Gleichzeitig erhält man so eine viel genauere Beschreibung der lokalen Struktur von $Z_{r,n}$. Es ist erstaunlich, dass man für den Beweis dieser elementaren Tatsachen relativ neue, unendlich-dimensionale Objekte der algebraischen Geometrie verwendet. Ein „direkter“ Beweis für die Reduziertheit ist mir nicht bekannt. Ähnliche Matrixgleichungen sind schon vor Jahrzehnten von vielen verschiedenen Autoren betrachtet worden, neben Strickland zum Beispiel von de Concini, aber auch in jüngerer Zeit, zum Beispiel von Faltings [F].

3 Modulkurven

3.1 *Modulkurven über den komplexen Zahlen*

Die Gruppe $SL_2(\mathbb{Z})$ aller ganzzahligen (2×2)-Matrizen mit Determinante 1 operiert auf der oberen Halbebene $\mathbb{H} = \{z \in \mathbb{C};\ \mathrm{Im}\, z > 0\}$ durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

Im Folgenden werden wir in der Regel die Einschränkung dieser Operation auf Untergruppen der Form

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z});\ c \equiv 0 (\mathrm{mod}\ N) \right\}$$

betrachten. Die Quotienten $Y(\mathbb{C}) := SL_2(\mathbb{Z})\backslash\mathbb{H}$, $Y_0(N)(\mathbb{C}) := \Gamma_0(N)\backslash\mathbb{H}$ tragen in natürlicher Weise die Struktur einer Riemannschen Fläche.

Die $Y_0(N)$ können (anders als etwa $\mathbb{H}$) durch Hinzunahme endlich vieler Punkte kompaktifiziert werden. Alle kompakten Riemannschen Flächen sind algebraisierbar, d. h. sie lassen sich als Nullstellenmengen von Polynomen beschreiben, und dasselbe gilt dann auch für die offenen Teile $Y_0(N)$. Die Kurven Y und $Y_0(N)$ (bzw. ihre Kompaktifizierungen) sind Beispiele von *Modulkurven*. Siehe zum Beispiel [Sh], [DS].

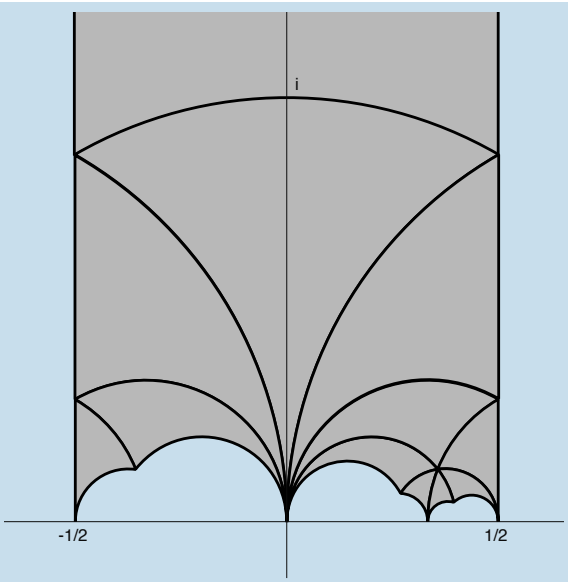
Um das Konzept der Modulkurve über beliebigen Körpern betrachten zu können, nutzen wir eine andere Beschreibung, die gleichzeitig die Wahl des Namens Modulkurve erklärt. Und zwar haben wir Bijektionen

$$SL_2(\mathbb{Z})\backslash\mathbb{H} \longrightarrow \{\Lambda \subset \mathbb{C} \text{ Gitter}\}/\mathbb{C}^\times \\ \to \{E \text{ kompakte Riem. Fläche vom Geschlecht } 1\}/\cong .$$

Hier verstehen wir unter einem Gitter in $\mathbb{C}$ einen freien $\mathbb{Z}$-Untermodul vom Rang 2, der über $\mathbb{R}$ den $\mathbb{R}$-Vektorraum $\mathbb{C}$ erzeugt. Die multiplikative Gruppe $\mathbb{C}^\times$ operiert durch Multiplikation; mit anderen Worten betrachten wir die Gitter nur bis auf Homothetie. Die Abbildungen sind gegeben durch

$$z \mapsto \mathbb{Z} \oplus z\mathbb{Z}, \quad \Lambda \mapsto \mathbb{C}/\Lambda.$$

Wir können also den Quotienten $SL_2(\mathbb{Z})\backslash\mathbb{H}$ als Parameterraum oder *Modulraum* der kompakten Riemannschen Flächen vom Geschlecht 1 betrachten. Nun können wir kompakte Riemannsche Flächen auch als algebraische Kurven (über $\mathbb{C}$) auffassen – im konkreten Fall



Beispiel 2. Ein Fundamentalbereich der Operation von $\Gamma_0(6)$ auf $\mathbb{H}$. Die einzelnen „Dreiecke" sind Fundamentalbereiche der Gruppe $SL_2(\mathbb{Z})$. Durch geeignete Identifizierung der Ränder erhält man die Modulkurve $Y_0(N)$ (zumindest als topologischen Raum). Man sieht auch, dass diese nicht kompakt ist; es fehlen die endlich vielen *Spitzen* auf $\mathbb{R}$ (und im Unendlichen), die im Abschluss liegen. Die Abbildung wurde angefertigt mit Hilfe eines Programms von H. Verrill, www.math.lsu.edu/~verrill/fundomain/fundomain.c.

erhält man mit Hilfe der Weierstraßschen $\wp$-Funktion eine abgeschlossene Einbettung von $\mathbb{C}/\Lambda$ in die projektive Ebene $\mathbb{P}^2(\mathbb{C})$, durch die unsere Riemannsche Fläche mit der Nullstellenmenge einer kubischen Gleichung identifiziert wird. An der Beschreibung als Quotient $\mathbb{C}/\Lambda$ sehen wir, dass alle kompakten Riemannschen Flächen vom Geschlecht 1 mit einer Gruppenstruktur versehen werden können (so dass Verknüpfung und Inverses holomorphe Abbildungen sind). Damit erhalten wir die Beschreibung

$$SL_2(\mathbb{Z})\backslash\mathbb{H} = \{E \text{ vollst. alg. Kurve mit Gruppenstruktur}\}/\cong .$$

Vollständige algebraische Kurven mit Gruppenstruktur werden auch als *elliptische Kurven* bezeichnet.

In ähnlicher Weise haben wir

$$\Gamma_0(N)\backslash\mathbb{H} \longrightarrow \{(E,E',\varphi); E,E' \text{ ell. Kurven}/\mathbb{C}, \varphi\colon E \to E' \text{ Isogenie mit zyklischem Kern der Ordnung } N\}.$$

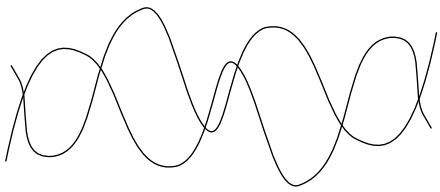
Hier verstehen wir unter einer *Isogenie* einen surjektiven Morphismus, der die Gruppenstruktur erhält.

3.2 Modulkurven über beliebigen Körpern

Der Begriff der elliptischen Kurve in der Formulierung „vollständige algebraische Kurve mit Gruppenstruktur" ergibt über beliebigen Grundkörpern Sinn, und man kann auch in der allgemeinen Situation zeigen, dass die Menge der Isomorphieklassen elliptischer Kurven die Struktur einer algebraischen Kurve trägt. Wir fixieren eine Primzahl p und wählen nun als Grundkörper $k = \overline{\mathbb{F}_p}$ einen algebraischen Abschluss des Körpers $\mathbb{F}_p$. Ähnliches gilt für die $\Gamma_0(N)$-Variante; die so erhaltene Kurve bezeichnen wir mit $Y_0(N)$. (Wir fixieren hier zusätzlich eine geeignete „Niveau-Struktur außerhalb von p", die aber für das Weitere nebensächlich ist und die wir deshalb nicht weiter erwähnen.)

Theorem 2. *Sei N teilerfremd zu p.*

1. (Igusa 1959) *Die Kurve $Y_0(N)$ über k ist glatt.*
2. (Deligne-Rapoport 1973) *Die Kurve $Y_0(pN)$ über k besteht aus zwei Kopien der Kurve $Y_0(N)$, die sich in endlich vielen Punkten transversal schneiden.*



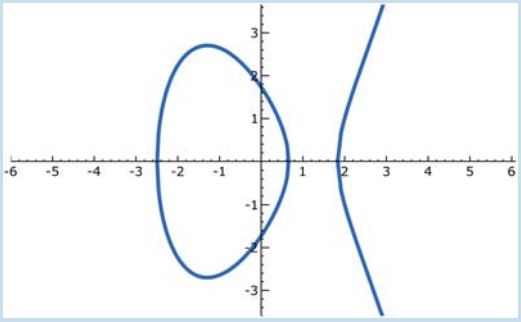
Eine schematische Darstellung der Modulkurve $Y_0(pN)$ über $\overline{\mathbb{F}_p}$.

Jeder Punkt dieser Kurve entspricht also einer Isogenie $E \to E'$ mit zyklischem Kern der Ordnung p. (Der Kern, und der Begriff der Ordnung, sind hier im Sinne endlicher Gruppenschemata zu verstehen.) Die Schnittpunkte entsprechen gerade den Isogenien von *supersingulären* elliptischen Kurven, also solchen mit der Eigenschaft, dass der Kern der Multiplikation mit p auf E (und äquivalent auf E') topologisch aus nur einem einzigen Punkt besteht. Die andere Möglichkeit ist die, dass er als abstrakte Gruppe isomorph ist zu $\mathbb{Z}/p\mathbb{Z}$; man nennt die elliptische Kurve dann *gewöhnlich*. Man vergleiche die Situation über $\mathbb{C}$, wo jede elliptische Kurve die Form $\mathbb{C}/\Lambda$ hat und der Kern der Multiplikation mit N folglich isomorph ist zu $(\mathbb{Z}/N\mathbb{Z})^2$. Siehe Beispiel 3 für eine äquivalente Charakterisierung.

3.3 Die Ramanujan-Vermutung

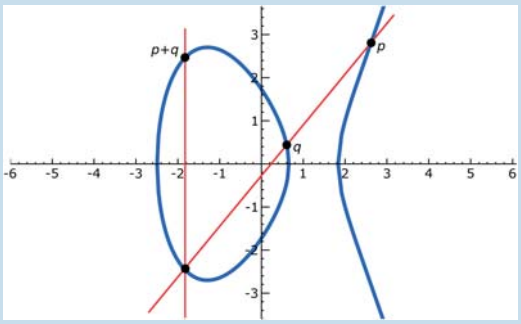
Eine zeitgemäße Begründung, warum man sich für diese Modulräume interessiert, ist das oben erwähnte Langlands-Programm. An dieser Stelle gehen wir darauf aber nicht näher ein, sondern erwähnen eine ältere, aber leichter zugängliche und frappierende Anwendung, nämlich Delignes Ende der 1960er Jahre erbrachten Beweis [D], dass die Ramanujan-Vermutung aus den Weil-Vermutungen folgt. Kurz vorher hatten Kuga und Shimura einen solchen Reduktionsschritt im Fall gewisser kompakter Quotienten von $\mathbb{H}$ durchgeführt. Ganz im Einklang mit dem Langlands-Programm zeigt sich hier

Beispiel 3. Die Gleichung $E : y^2 - x^3 + 5x - 3 = 0$ beschreibt eine elliptische Kurve.



Die Lösungsmenge der Gleichung E über den reellen Zahlen

Eine interessante Eigenschaft elliptischer Kurven ist, dass man zu zwei gegebenen Lösungen der Gleichung immer eine dritte produzieren kann: Man kann zwei Punkte „miteinander verknüpfen", genau wie man zwei Zahlen addieren kann und so eine dritte erhält. In der Tat kann man diese Prozedur so durchführen, dass die üblichen Rechenregeln erfüllt sind; die Punkte der elliptischen Kurve bilden eine kommutative Gruppe. Geometrisch wird die „Addition" von Punkten in der zweiten Abbildung veranschaulicht: Gegeben eine Gerade, die die elliptische Kurve in genau drei Punkten schneidet, so ist die Summe von zweien dieser Punkte gerade das Spiegelbild bezüglich der x-Achse des dritten Punktes.



Das Gruppengesetz auf der elliptischen Kurve E

Um die Gruppenverknüpfung vollständig zu beschreiben, muss man noch ein kleines bisschen mehr sagen, und außerdem der hier gezeigten Lösungsmenge noch einen zusätzlichen Punkt „im Unendlichen" hinzufügen. Dieser Punkt ist gerade das neutrale Element. Aus zahlentheoretischer Sicht ist dieses Gruppengesetz auch deswegen interessant, weil man dabei aus Punkten mit rationalen Zahlen als Koeffizienten durch Addition wieder einen Punkt mit rationalen Koeffizienten bekommt.
Dieselbe Gleichung können wir auch über endlichen Körpern betrachten. Sei $\mathbb{F}_p$ der Körper mit p Elementen (p eine Primzahl). Dann definiert die obige Gleichung eine elliptische Kurve, sofern $p \neq 2$ und $p \neq 257$.

Die Kurve E, verstanden als elliptische Kurve über dem endlichen Körper $\mathbb{F}_p$, ist genau dann supersingulär, wenn p die Anzahl der Lösungen der (affinen) Gleichung für E über $\mathbb{F}_p$ teilt, oder elementar ausgedrückt:

$$p \mid \#\{(x,y) \in \{0,\dots,p-1\}^2; \\ y^2 - x^3 + 5x - 3 \equiv 0 \mod p\}.$$

Man rechnet so zum Beispiel leicht nach, dass unsere elliptische Kurve über $\mathbb{F}_3$ supersingulär ist, über $\mathbb{F}_5$ jedoch nicht.
Die zahlentheoretische Eigenschaft der „Modularität", die nach dem Satz von Wiles jede elliptische Kurve über $\mathbb{Q}$ hat, beschreibt eine überraschende Verbindung zwischen den Anzahlen der Punkte von E über verschiedenen endlichen Körpern. Um diese Beziehungen genauer auszudrücken, fassen wir die Anzahlen in die Reihe

$$f(z) = \sum_{n \geq 1} a_n e^{2\pi i n z}$$

zusammen (wobei a_p bis auf einen Korrekturterm die Anzahl der Punkte von E über $\mathbb{F}_p$ bezeichnet, und die anderen Koeffizienten aus den a_p rekonstruiert werden können). Dann ist f eine Modulform, also eine komplex differenzierbare Funktion $\mathbb{H} \to \mathbb{C}$, die sich unter der Operation einer großen Untergruppe von $SL_2(\mathbb{Z})$ in besonders einfacher Weise transformiert. Ein Beispiel einer solchen Modulform ist die unten betrachtete Funktion Δ.
Elliptische Kurven haben sich auch in der Kryptographie und bei der Suche nach Algorithmen zur Faktorisierung großer Zahlen als sehr nützlich erwiesen. Wer neugierig geworden ist, erfährt mehr über elliptische Kurven zum Beispiel in dem Buch [ST] von Silverman und Tate und (zur Anwendung in der Verschlüsselungstheorie) im Buch [W] von Werner.

eine tiefe Verbindung zwischen Zahlentheorie, algebraischer Geometrie und Analysis; Verallgemeinerungen der Ramanujan-Vermutung sind nach wie vor von großem Forschungsinteresse. Wir definieren

$$D(q) = q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n$$

und betrachten diesen Ausdruck zunächst als formale Potenzreihe in q mit ganzzahligen Koeffizienten. Die $\tau(n)$ sind also definiert als diejenigen ganzen Zahlen, die durch Ausmultiplizieren des Produktes entstehen.

Vermutung 1 (Ramanujan, 1916). *Für jede Primzahl p gilt*

$$|\tau(p)| \leq 2p^{11/2}.$$

Diese Vermutung beschreibt eine erstaunliche und tiefliegende Eigenschaft dieser Koeffizienten. Um Deligne Beweisidee zu skizzieren, beginnen wir mit der Bemerkung, dass $D(q)$ gerade die Fourier-Entwicklung

„der“ Spitzenform $\Delta\colon \mathbb{H} \to \mathbb{C}$ vom Gewicht 12 ist, d. h. $\Delta(z) := D(e^{2\pi i z})$ ist eine holomorphe Funktion $\mathbb{H} \to \mathbb{C}$, und

$$\Delta\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z\right) = (cz+d)^{12}\Delta(z)$$
$$\forall z \in \mathbb{H}, \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Die Funktion Δ transformiert sich also unter der Wirkung der $SL_2(\mathbb{Z})$ in sehr einfacher Weise, und wir können uns Δ daher fast als eine Funktion auf dem Quotienten $SL_2(\mathbb{Z})\backslash\mathbb{H}$ vorstellen. (Korrekter wäre es zu sagen, dass Δ ein Schnitt eines gewissen Geradenbündels auf $SL_2(\mathbb{Z})\backslash\mathbb{H}$ ist.)

Diese Verbindung zu den Modulkurven kann man nutzen, um die Zahlen $\tau(n)$ noch anders zu beschreiben. Wir betrachten dazu die sogenannte *Hecke-Korrespondenz*

$$Y \xleftarrow{p_1} Y_0(p) \xrightarrow{p_2} Y,$$

wobei der Pfeil nach links durch $(E \to E') \mapsto E$, der nach rechts durch die Vorschrift $(E \to E') \mapsto E'$ gegeben sei. Damit können wir Funktionen auf Y transformieren, d. h. wir erhalten aus einer Funktion f eine neue Funktion

$$T_p(f)\colon z \mapsto \sum_{x \in p_2^{-1}(z)} f(p_1(x)).$$

Diesen *Hecke-Operator* kann man in ähnlicher Weise auch auf Δ anwenden, und es war bereits 1937 Hecke bekannt, dass Δ eine Eigenfunktion von T_p mit Eigenwert $\tau(p)$ ist. Das zeigt bereits, dass die τ-Funktion multiplikativ ist (d. h. $\tau(mn) = \tau(m)\tau(n)$ für teilerfremde m, n), was auch von Ramanujan vermutet und von Mordell bewiesen worden war.

Man kann die $\tau(p)$ als Eigenwert des Hecke-Operators auf der Kohomologie der Modulkurve realisieren, die man aufgrund von Basiswechselsätzen statt in Charakteristik 0 auch in Charakteristik p ausrechnen kann. Dann zerfällt die Kurve $Y_0(p)$ wie oben beschrieben in zwei Komponenten, und dieses gute Verständnis der geometrischen Seite erweist sich als Schlüssel zum weiteren Beweis. Der Satz von Eichler-Shimura besagt, dass sich der Hecke-Operator entsprechend in eine Summe $T_p = F + p^{-1}F$ zerlegt. Hier bezeichnet F den Frobenius-Automorphismus (einer geeigneten Kohomologiegruppe). Damit lässt sich die Frage nach den Eigenwerten von T_p und insbesondere die Ramanujan-Vermutung zurückführen auf das Studium der Eigenwerte des Frobenius-Operators. Über diese liefern die Weil-Vermutungen, die in den 1970er Jahren ebenfalls von Deligne bewiesen wurden, genaue Informationen, und der Beweis der Ramanujan-Vermutung ist damit vollständig.

4 Modulräume abelscher Varietäten

Nun betrachten wir höherdimensionale Analoga elliptischer Kurven, sogenannte *abelsche Varietäten*, und ihre Modulräume. Unter einer abelschen Varietät verstehen wir eine vollständige Varietät mit Gruppenstruktur; wie der Name andeutet, ist eine solche Gruppenstruktur notwendigerweise kommutativ.

Über den komplexen Zahlen hat jede abelsche Varietät die Form $\mathbb{C}^g/\Lambda$, $\Lambda \subset \mathbb{C}^g$ ein Gitter; allerdings sind, falls $g > 1$, nicht alle dieser Quotienten algebraisierbar. Das prominenteste Beispiel eines Parameterraums abelscher Varietäten ist die Siegelsche Modulvarietät, die sich über $\mathbb{C}$ ganz ähnlich wie die Modulkurven als Quotient des Siegelschen Halbraumes $\mathbb{H}_g$ aller symmetrischen $(g \times g)$-Matrizen über $\mathbb{C}$ mit positiv definitem Imaginärteil nach der Operation der Gruppe $Sp_{2g}(\mathbb{Z})$ beschreiben lässt.

Über anderen Grundkörpern lassen sich die abelschen Varietäten nicht so einfach beschreiben. Man kann aber wieder zeigen, dass die Menge der abelschen Varietäten (mit gewissen Zusatzstrukturen) die Struktur einer algebraischen Varietät trägt. In positiver Charakteristik kann man sich zudem zusätzliche Methoden, insbesondere die von der Frobenius-Abbildung induzierten Homomorphismen, zunutze machen.

4.1 *Modulräume abelscher Varietäten und Matrixgleichungen*

Einen Bezug zu den im ersten Abschnitt diskutierten Matrixgleichungen kann man am einfachsten für den folgenden Modulraum herstellen:

Seien $0 < r < n$ natürliche Zahlen, und $K/\mathbb{Q}$ eine imaginär-quadratische Körpererweiterung, in der die Primzahl p zerfällt als Produkt zweier Primideale $\mathfrak{p}_0$, $\mathfrak{p}_1$. Wir betrachten den Modulraum $\mathcal{A}_{r,n}$ aller Tupel

$$A_0 \to A_1 \to \cdots \to A_{n-1} \to A_0,$$

wobei die A_i abelsche Varietäten der Dimension n sind, die eine Operation des Rings $\mathcal{O}_K$ der ganzen Zahlen von K tragen, und die Morphismen $A_i \to A_{i+1}$ Isogenien sind, deren Kerne zyklisch von Ordnung p sind, und die verträglich mit der $\mathcal{O}_K$-Wirkung sind. Wir verlangen ferner, dass die Verkettungen $A_0 \to A_0$ und $A_i \to A_0 \to A_i$ $(i > 0)$ jeweils durch die Multiplikation mit p gegeben sind. Zu diesem Datum gehöre auch eine geeignete Polarisierung der A_i, die wir im Weiteren ignorieren.

Wir betrachten das Modulproblem über dem Körper $k = \overline{\mathbb{F}_p}$, einem algebraischen Abschluss des endlichen Körpers $\mathbb{F}_p$. Da p in K zerfällt, zerlegt sich $\mathcal{O}_K \otimes_{\mathbb{Z}_p} k \cong k \times k$ entsprechend. Die $\mathcal{O}_K$-Operation auf den A_i hat also zur Folge, dass die Tangentialräume (im neutralen Element) in eine direkte Summe $T_e A_i = T_i^0 \oplus T_i^1$ zerfallen, und wir fordern, dass alle T_i^0 die Dimension r (und folglich alle T_i^1 die Dimension $n - r$) haben.

Dieser Modulraum gehört im Sinne der Theorie der Shimura-Varietäten zur Gruppe der unitären Ähnlichkeiten der Signatur $(r, n-r)$. An der Primstelle p haben wir es (wie im $\Gamma_0(p)$-Fall der oben betrachteten Modulkurve) mit einer Niveaustruktur vom Iwahori-Typ zu tun.

Nun stellen wir die Verbindung zu den Matrixgleichungen $Z_{r,n}$ her. Aus einer Kette $(A_i)_i \in \mathcal{A}_{r,n}(k)$ abelscher Varietäten über k erhalten wir eine Kette von Abbildungen

$$T_0^0 \to T_1^0 \to \cdots T_{n-1}^0 \to T_0^0$$

von r-dimensionalen k-Vektorräumen, derart dass alle Verkettungen $T_i^0 \to T_i^0$ die Multiplikation mit p sind. Nun ist $p = 0$ in k, also sind diese Verkettungen alle die Nullabbildung, und wählen wir Basen der T_i^0, so erhalten wir ein Element von $Z_{r,n}(k)$. Man kann dann beweisen, dass der oben definierte Modulraum „die gleichen Singularitäten" hat wie (ein offener Teil von) $Z_{r,n}$; insbesondere ist er nach Theorem 1 reduziert, und es folgt auch, dass seine irreduziblen Komponenten normal sind. (Eine präzise Beschreibung des Zusammenhangs ist, dass man einen *glatten* Morphismus von $\mathcal{A}_{r,n}$ in den Stack-Quotienten $[(GL_r)^n \backslash Z_{r,n}]$ hat.) Diese Aussagen über die Struktur des Modulraums liefern

Theorem 3. *1. Der Raum $\mathcal{A}_{r,n}$ über $\mathbb{F}_p$ ist reduziert, alle irreduziblen Komponenten sind normale Varietäten.*
2. Das obige Modulproblem, über dem Ring $\mathbb{Z}_p$ der p-adischen Zahlen betrachtet, definiert ein flaches *Modell der entsprechenden Shimura-Varietät.*

Die Flachheitseigenschaft besagt, dass hier überhaupt ein sinnvolles Modell vorliegt, in dem Sinne, dass die spezielle Faser (über $\mathbb{F}_p$) in stetiger Weise zu der allgemeinen Faser passt. Die genaueren Aussagen im ersten Punkt, und speziell die Reduziertheit, sind zum Beispiel auch in den kürzlich vorgelegten Arbeiten [S] von Stroh über eine Kompaktifizierung dieser Räume wichtig.

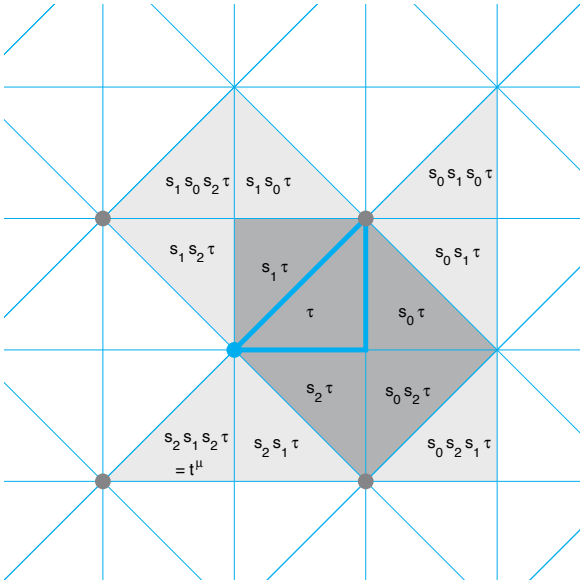
Ist $n = 2$, $r = 1$, so sind wir in der Situation der Modulkurve $Y_0(p)$ und von Beispiel 1. Wir sehen an den Abbildungen 1 und 2, dass tatsächlich der Raum $Z_{1,2}(k)$ die „gleichen" Singularitäten hat wie die Modulkurve: Abgesehen von den glatten Punkten gibt es Punkte, in denen sich zwei glatte Kurven transversal schneiden.

4.2 *Der supersinguläre Ort im Siegel-Fall*

Zum Abschluss kommen wir noch einmal auf den oben erwähnten Siegel-Fall zu sprechen; wir statten ihn jetzt aber mit Niveau-Struktur vom Iwahori-Typ aus. Bei der Beschreibung als Parameterraum äußert sich das so, dass wir ähnlich wie bei der Definition von $\mathcal{A}_{r,n}$ statt einzelner abelscher Varietäten nun Ketten

$$A_0 \to A_1 \to \cdots \to A_n$$

betrachten, wo alle A_i abelsche Varietäten der Dimension n und die Morphismen wie oben Isogenien der Ordnung p sind. Wir betrachten hier aber keine zusätzliche



Die zulässige Menge für GSp_4 besteht aus den 13 grau gefärbten Alkoven. In diesem Fall ist der supersinguläre Ort eine Vereinigung von KR-Strata, und zwar von denjenigen, die zu dunkelgrau wiedergegebenen Alkoven gehören.

Operation auf den abelschen Varietäten, sondern fordern, dass A_0 und A_n mit prinzipalen Polarisierungen λ_0, λ_n versehen sind, derart dass der Pull-back von λ_n nach A_0 gerade $p\lambda_0$ ist. Die lokale Struktur dieses Raumes kann man ähnlich wie oben mit gewissen Matrixgleichungen in Beziehung setzen, und man erhält ganz analoge Aussagen zu denen von Theorem 3; siehe [G2].

Wir wollen zum Schluss die globale Struktur des supersingulären Ortes diskutieren. Der supersinguläre Ort S ist der abgeschlossene Ort derjenigen Ketten, in denen A_0 (oder äquivalent alle A_i) supersingulär sind. Dabei heißt eine abelsche Varietät A *supersingulär*, wenn es eine Isogenie von einem Produkt supersingulärer elliptischer Kurven auf A gibt. Die geometrische Gestalt des supersingulären Ortes und besonders seine Kohomologie sind von großem Interesse. Es ist ein typisches Phänomen, dass man die Kohomologie der gesamten speziellen Faser durch einen Induktionsprozess aus der des supersingulären Ortes erhält; dieses Prinzip ist im Beweis der lokalen Langlands-Korrespondenz für GL_n von Harris und Taylor bedeutsam, und ganz besonders auch in den neueren Arbeiten [B] von Boyer, der die Ergebnisse von Harris und Taylor zur lokalen Langlands-Korrespondenz weiter verfeinert.

In der Arbeit [GY] zeigen C.-F. Yu und der Autor:

Theorem 4. *1. Sei n gerade. Dann ist $\dim S = \frac{n^2}{2}$. Die irreduziblen Komponenten der maximalen Dimension $n^2/2$ von S sind isomorph zur Flaggenvarietät der Gruppe $Sp_n \times Sp_n$.*

2. *Sei n ungerade. Dann ist $\frac{n^2-n}{2} \leq \dim S \leq \frac{n^2-1}{2}$, und S besitzt irreduzible Komponenten, die isomorph sind zur Flaggenvarietät der Gruppe SL_n.*

Dieses Theorem beruht auf einer Untersuchung der sogenannten Kottwitz-Rapoport-Stratifizierung des Siegel-Raums (über $\mathbb{F}_p$), die man sich als Stratifizierung bezüglich der Singularitäten dieses Raums vorstellen sollte. Durch die Beschreibung der Singularitäten durch Matrixgleichungen lässt sich ein Bezug zur affinen Flaggenvarietät herstellen. Die Strata werden dann durch eine endliche Teilmenge der Menge aller Alkoven im Standardapartment der Gruppe Sp_{2n} beschrieben, siehe Abbildung 5 für den Fall $n = 2$.

Die Abschlussrelationen zwischen den Strata sind durch die Bruhat-Ordnung gegeben. Man erhält so eine sehr explizite kombinatorische Beschreibung dieser Situation, die allerdings gleichzeitig hochkompliziert ist. Zum Beispiel gibt es für $n = 6$ bereits 75973 Strata. Um die komplexe Kombinatorik in den Griff zu bekommen, sind oft Computer-Experimente hilfreich.

Diejenigen Strata, die ganz in S enthalten sind, können nicht nur lokal, sondern insgesamt ganz konkret beschrieben werden: Es handelt sich um disjunkte Vereinigungen Deligne-Lusztig-Varietäten (zu verschiedenen algebraischen Gruppen über $\mathbb{F}_p$). Mit Blick auf die enge Verbindung zwischen Deligne-Lusztig-Varietäten und der Darstellungstheorie endlicher Gruppen vom Lie-Typ ist zu hoffen, dass sich dieser Zusammenhang auch im Sinne des Langlands-Programms nutzen lässt, um die Kohomologie von S in darstellungstheoretischer Weise zu beschreiben.

Der supersinguläre Ort ist das eindeutig bestimmte abgeschlossene Stratum der „Newton-Stratifizierung". Die Frage, welche Newton-Strata welche KR-Strata schneiden (und in welcher Dimension), führt auf den Begriff der *affinen Deligne-Lusztig-Varietät* – das Analogon einer Deligne-Lusztig-Varietät im Kontext eines affinen Wurzelsystems. Dementsprechend sind affine Deligne-Lusztig-Varietäten Unterschemata von affinen Grassmannschen beziehungsweise affinen Flaggenvarietäten. Siehe [GHKR].

Wer sich mit diesen Themen eingehender befassen möchte, dem seien auch die Übersichtsartikel [Ha] von Haines und [R] von Rapoport ans Herz gelegt.

Ich danke Martin Kreidl und Michael Rapoport für ihre Bemerkungen zu diesem Artikel.

Literatur

[Be] D. Ben-Zvi, *Moduli spaces*, Ch. IV.8 in Princeton Companion to Mathematics, Princeton Univ. Press 2008.

[B] P. Boyer, *Monodromie du faisceau pervers des cycles évanescents de quelques variétés de Shimura simples*, Preprint; *Cohomologie des systèmes locaux de Harris-Taylor et applications*, Preprint.

[D] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Sém. Bourbaki **11** (1968-69), Exp. 355.

[DS] F. Diamond, J. Shurman, *A first course in modular forms*, Springer Graduate Texts in Math. 228, 2005.

[F] G. Faltings, *Explicit resolution of local singularities of moduli-spaces*, J. Reine Angew. Math. **483** (1997), 183–196.

[G1] U. Görtz, *On the flatness of local models for certain Shimura varieties of PEL-type*, Math. Ann. **321** (2001), 689–727.

[G2] U. Görtz, *On the flatness of local models for the symplectic group*, Adv. Math. **176** (2003), 89–115.

[GHKR] U. Görtz, T. Haines, R. Kottwitz, D. Reuman, *Dimensions of some affine Deligne-Lusztig varieties*; Ann. sci. de l'E. N. S. 4^{e} série, t. 39 (2006), 467–511.

[GY] U. Görtz, C.-F. Yu, *The supersingular locus in Siegel modular varieties with Iwahori level structure*, arXiv:0807.1229

[Ha] T. Haines, *Introduction to Shimura varieties with bad reduction of parahoric type*, in: Harmonic analysis, the trace formula, and Shimura varieties, Clay Math. Proc. **4** (2005), 583–642.

[R] M. Rapoport, *A guide to the reduction modulo p of Shimura varieties*; Astérisque 298 (2005), 271–318.

[Sh] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Forms*, Princeton Univ. Press 1971.

[ST] J. Silverman, J. Tate, *Rational points on elliptic curves*, Springer UTM, 1992.

[S] B. Stroh, *Compactification de variétés de Siegel aux places de mauvaise réduction*, arXiv:0810.0117; *Compactification minimale et mauvaise réduction*, arXiv:0811.1484.

[W] A. Werner, *Elliptische Kurven in der Kryptographie*, Springer 2002.

Dr. Ulrich Görtz, Mathematisches Institut der Universität Bonn, Beringstraße 1, 53115 Bonn. ugoertz@math.uni-bonn.de