Zahlentheorie und Geometrie vereint in der Serre-Vermutung

Gabor Wiese

15. Juni 2008

In den Jahren 2004-2007 wurde zur großen Überraschung der mathematischen Gemeinde (den Autor eingeschlossen) eines der großen Probleme der reinen Mathematik der Gegenwart gelöst: die 'Serre-Vermutung'. Sie stellt einen Zusammenhang zwischen scheinbar grundverschiedenen Objekten her, die unterschiedlichen Gebieten der Mathematik entstammen: der Zahlentheorie und der Geometrie.

Diese Vermutung geht auf den französischen Mathematiker Jean-Pierre Serre (geb. 1926, emeritierter Professor am Collège de France) zurück, der einer der besten und einflussreichsten Mathematiker seit der zweiten Hälfte des 20. Jahrhunderts ist und zum Beispiel als erster mit dem höchst renommierten Abel-Preis ausgezeichnet wurde. Eine erste Version seiner Vermutung formulierte er zu Beginn der 1970er Jahre: Sie postuliert einen qualitativen Zusammenhang zwischen Modulformen (Geometrie) und bestimmten Klassen von Zahlkörpern (Zahlentheorie). Beide Begriffe zu erklären, ist ein Hauptanliegen dieses Artikels. Ein quantitative Präzisierung der Vermutung folgte in einem Artikel im Jahre 1987.[1] Diese neue Formulierung stützte sich übrigens bereits zum Teil auf Computerberechnungen. Sie war unter anderem motiviert durch die so genannte Taniyama-Shimura-Weil-Vermutung und liefert sogar eine weit reichende Verallgemeinerung dieser. Es war nämlich vom Mathematiker Gerhard Frey, der damals Professor in Saarbrücken war, aber seit der Gründung am Essener Institut für Experimentelle Mathematik tätig ist, suggeriert worden, dass die Taniyama-Shimura-Weil-Vermutung den so genannten letzten Satz von Fermat (siehe Abbildung 2, nach Pierre de Fermat, ca. 1607-1665) zur Folge hat. Serre beweist in seiner Präzisierung, dass seine Vermutung den Satz von Fermat direkt impliziert. Es ist keine Übertreibung zu behaupten, dass die Herausforderung von Fermats Satz die Entwicklung der Zahlentheorie in den letzten mehr als 350 Jahren wesentlich vorangetrieben hat. [2]

Abbildung 1: J.-P. Serre im Gespräch mit J.-P. Wintenberger im Juli 2007

[1] Serre 1987.

[2] Für einen allgemein verständlichen Überblick siehe Aczel 1997 und Singh 2000.

Die Serre-Vermutung hat den Fortgang der Forschung in Zahlentheorie und Geometrie in den letzten Jahren stark beeinflusst und wird ihn noch weiter beeinflussen, denn ihr Beweis ist natürlich kein Schlussstein in diesem Gebiet. Es scheint vielmehr so, dass sie nur der erste Fall viel umfassenderer Zusammenhänge ist.

Es gab, gibt und wird noch viele Essener Aktivitäten auf dem Gebiet rund um die Serre-Vermutung geben: Gerhard Frey hat neben seinem bereits erwähnten bahnbrechenden Beitrag viele Studien durchgeführt und initiiert [3], Gebhard Böckle hat einen entscheidenden Beitrag zum Beweis der Serre-Vermutung geleistet, indem er bestimmte *Deformationsringe* beschrieben hat; hierauf können wir leider in diesem Text nicht näher eingehen. Auch der Autor forscht auf diesem Gebiet, vor allem im Fall von *Gewicht eins*, und konnte einige Beiträge leisten.[4]

Die Fermatsche Vermutung (Fermats letzter Satz) besagt, dass die Gleichung

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

für ganze Exponenten $n \geq 3$ keine Lösung in positiven natürlichen Zahlen a, b, c hat. Sie wurde 1994 von Andrew Wiles mit Methoden bewiesen, die im Beweis der Serre-Vermutung weit reichende Verallgemeinerungen erfahren haben.

Abbildung 2: Fermats letzter Satz

Die Leserin oder der Leser ist nun eingeladen zu einer Reise durch einen kleinen Teil der großen Welt der Mathematik. Ziel ist es, nicht nur Begriffe zu verwenden, sondern diese so gut es geht zu erklären. Die Darstellung ist natürlich vereinfacht, aber dennoch wird versucht, vom Essentiellen so viel wie möglich beizubehalten. Wer sich für das 'Wer, wann mit wem?' interessiert wird hier aber nicht fündig.[5]

1 Die Serre-Vermutung - ein Überblick

Abbildung 3: Erich Hecke

Die mathematischen Gebilde, die in der Serre-Vermutung Zahlentheorie und Geometrie verbinden, sind die *Modulformen*. Diesen widmen wir einen eigenen Abschnitt, in dem wir die verwendeten Begriffe erklären werden. Grob gesprochen sind Modulformen Funktionen, die der Geometrie entstammen und bestimmte Symmetrien erfüllen, die *Möbius-Symmetrien* nach August Ferdinand Möbius (1790-1868). In diesem Text betrachten wir nur Modulformen, die noch eine zweite Klasse von Symmetrien aufweisen, die *Hecke-Symmetrien*, nach Erich Hecke (1887-1947, Abbildung 3). Modulformen, die beiden Symmetrien besitzen, nennen wir *sehr symmetrische Modulformen* oder *Hecke-Eigenformen*.

Die zahlentheoretischen Objekte in der Serre-Vermutung sind *Zahlkörper*, genauer *ungerade* GL_2*-Zahlkörper*, und ihre *Arithmetik*. Was wir darunter verstehen, wird im folgenden Abschnitt geklärt. Zahlkörper sind wichtige Hilfsmittel der algebraischen Zahlentheorie.

[3] Siehe zum Beispiel Frey 1994.

[4] Siehe zum Beispiel Wiese 2004, 2007a, 2007b.

[5] Dafür siehe zum Beispiel die bereits erwähnten Bücher Aczel op. cit. und Singh op. cit.

Die erste Verbindung zwischen Modulformen und Zahlkörpern basiert auf Ideen von Sir Peter Swinnerton-Dyer (geb. 1927, Cambridge, England) und Serre und wurde in einem ersten Fall von Goro Shimura (geb. 1930, Princeton) und im Allgemeinen von Pierre Deligne (geb. 1944, Princeton) mit Methoden der *arithmetischen algebraischen Geometrie* bewiesen. Eine grobe Formulierung der Verbindung ist die folgende: *Jede sehr symmetrische Modulform enthält arithmetische Informationen zu bestimmten Zahlkörpern.* Um die Verbindung präzisieren zu können, erinnern wir an den Begriff einer *Primzahl*. Das ist eine natürliche Zahl größer als 1, die nur durch 1 und sich selbst teilbar ist, wie zum Beispiel 2, 3, 5, 7, 11, $\ldots$, $997, \ldots$. Die Präzisierung lautet wie folgt: *Jede sehr symmetrische Modulform enthält arithmetische Informationen zu je einem ungeraden* GL_2*-Zahlkörper pro Primzahl.*

Die Serre-Vermutung in ihrer ersten Formulierung aus den 1970ern ist die kühne Aussage, dass die Umkehrung hiervon auch gilt: *Die arithmetische Information zu jedem ungeraden* GL_2*-Zahlkörper steckt in einer sehr symmetrischen Modulform.* Mit anderen Worten: *Die Arithmetik der ungeraden* GL_2*-Zahlkörper wird vollständig durch sehr symmetrische Modulformen bestimmt.*

Dies ist eine Strukturaussage von großer Bedeutung, denn die Welt der Zahlkörper ist sehr mysteriös und im Allgemeinen schlecht vestanden. Hier wird also behauptet, dass einfache Funktionen, die der Geometrie und sogar dem 19. Jahrhundert entstammen, einen Teil der Welt der Zahlkörper beherrschen! Wie schon zu Anfang erwähnt, wissen wir seit kurzem, dass diese kühne Behauptung korrekt ist! Der Satz wurde bewiesen von Chandrashekhar Khare (Los Angeles) und Jean-Pierre Wintenberger (Straßburg), wobei Mark Kisin (Chicago) und Richard Taylor (Harvard) eine sehr große Rolle gespielt haben. Aber noch viel besser: Nicht nur wurde die erste Formulierung der Vermutung bewiesen, sondern auch die sehr präzise zweite Formulierung aus dem Jahre 1987.

Die Stärke der Serre-Vermutung zeigt sich darin, dass sie eine ganze Reihe berühmter Probleme auf einen Schlag löst, die wir leider aus Platzgründen hier nicht erklären können und nur schlagwortartig auflisten.

- Artin-Vermutung für GL_2. In umfangreichen Arbeiten wurde diese Vermutung in den 90er Jahren am Essener Institut für Experimentelle Mathematik in vielen, aber nur endlich vielen, Fällen überprüft.[6] Dass sie für unendlich viele Fälle richtig ist, wurde in einer ganzen Reihe von Arbeiten, initiiert von Richard Taylor, der auch ganz entscheidenden Anteil am Beweis der Taniyama-Shimura-Weil-Vermutung hatte, erst vor ein paar Jahren gezeigt. Dass sie in jedem Fall richtig ist, war nicht bekannt.

- Modulariät jeder abelschen Varietät vom GL_2-Typ (bisher nicht bekannt); diese ist eine Verallgemeinerung der

- Taniyama-Shimura-Weil-Vermutung; diese wurde 1994 von Andrew Wiles (Princeton) erstmals gelöst in einer Arbeit, die es auf die erste Seite der New York Times gebracht hat, denn sie impliziert

[6] Frey op. cit.

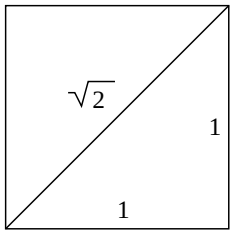


Abbildung 4: Quadrat und Diagonale

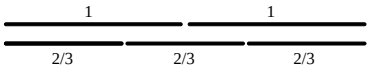


Abbildung 5: 1 und $\frac{2}{3}$ sind kommensurabel

- Fermats letzten Satz, den wir oben schon behandelt haben.

Der Autor dieses Artikels, der der Algorithmik sehr zugeneigt ist, wird nicht müde zu betonen, welche große Bedeutung die Serre-Vermutung für explizite Fragestellungen hat: Modulformen sind einfach berechenbar. Folglich sind mittels der Serre-Vermutung auch arithmetische Eigenschaften von ungeraden GL_2-Zahlkörpern einfach berechenbar!

Die Leserin oder der Leser wird die Begeisterung des Autors über diese große Entdeckung gespürt haben; sie wird geteilt von algebraischen Zahlentheoretikern weltweit. Auch wird die Leserin oder der Leser einen Eindruck von der strukturellen Bedeutung der Serre-Vermutung innerhalb der Zahlentheorie und der reinen Mathematik als solcher erhalten haben.

Nach diesem ersten Überblick beginnen wir nun die versprochene Reise durch die reine Mathematik, um uns ein genaueres Bild von der Serre-Vermutung zu verschaffen. Der erste und größte Teil ist der Welt der Zahlen gewidmet. Danach wenden wir uns der Geometrie, den verschiedenen Symmetrien und schließlich den Modulformen zu, bevor wir den Zusammenhang zwischen all diesen herstellen.

2 Zahlen

Algebraische Zahlen und Zahlkörper

Wir wollen und müssen unsere Geschichte früh beginnen. Weithin bekannt dürfte die Bestürzung der Pythagoräer sein, als sie feststellten, dass es Zahlen gibt, die keine Bruchzahlen sind. Genauer haben die Pythagoräer keine Zahlen sondern Längen bzw. Längenverhältnisse betrachtet und herausgefunden, dass die Diagonale im Quadrat inkommensurabel mit den Seiten ist: Egal, wie viele Stäbe der Länge der Diagonale man hintereinander legt, nie wird man auf ein Vielfaches der Länge einer Seite kommen (vgl. Abbildungen 4 und 5). Ist nämlich die Seitenlänge a, dann ist nach dem Satz von Pythagoras das Quadrat der Länge einer Diagonalen gleich $2a^2$. Folglich ist das Verhältnis von Diagonale zu Seite gleich $\sqrt{2}$. Wir, ein paar Jahrtausende später, wissen natürlich, dass $\sqrt{2}$ kein Bruch ist. Davon

kann man sich sehr einfach überzeugen und der Leser oder die Leserin ist eingeladen, die paar Zeilen in Abbildung 6 nachzuvollziehen.

Wir vollziehen jetzt den Schritt von den Bruchzahlen hin zu unserem ersten Beispiel eines Zahlkörpers, nämlich den, den die Mathematiker kurz mit $\mathbb{Q}(\sqrt{2})$ bezeichnen. Dabei handelt es sich um alle Zahlen der Form $\frac{p}{q} + \sqrt{2}\frac{r}{s}$. Diese haben die folgenden, ganz einfachen, aber kennzeichnenden Eigenschaften: Die Summe zweier solcher Zahlen ergibt wiederum eine, ebenso das Produkt; Addition und Multiplikation sind distributiv (siehe Abbildung 7).

Was ist also nun ein Zahl*körper*? Zum einen handelt es sich um einen Körper: Das ist eine Menge von Zahlen, die man addieren, subtrahieren, multiplizieren und dividieren kann, ohne die Menge zu verlassen, ganz wie in unserem Beispiel, wobei auch Assoziativität und Distributivität gelten sollen. Zum anderen wollen wir nur bestimmte Zahlen zulassen, zum Beispiel $\sqrt{2}$. Es ist wiederum eine ganz simple Eigenschaft, die man zu Grunde legt. In unserem Fall ist es die, dass $\sqrt{2}$ die Gleichung $x^2 - 2 = 0$ erfüllt (denn $(\sqrt{2})^2 - 2 = 2 - 2 = 0$).

Diesen Sachverhalt verallgemeinern wir jetzt wie folgt. Dabei halten wir uns vor Augen, dass es in der Zahlentheorie ja gerade um das Studium von Lösungen von Gleichungen mit ganzen Koeffizienten geht. Algebraische Zahlen bekommt man nun per Definition als Lösungen von Gleichungen mit ganzen Koeffizienten in einer Variablen. Genauer ist eine Zahl x eine *algebraische Zahl*, falls sie eine Gleichung (ein so genanntes *Polynom*)

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 = 0$$

erfüllt, wobei all die a_i ganze Zahlen sein sollen und jede natürliche Zahl als n erlaubt ist. Ein weiteres Beispiel ist der *goldene Schnitt* $\frac{1+\sqrt{5}}{2}$, der der Gleichung $x^2 - x - 1 = 0$ genügt (also $n = 2$ und $a_2 = 1$, $a_1 = -1$, $a_0 = -1$), wie man durch Einsetzen und Ausmultiplizieren nachprüft.

Wie passen die rationalen Zahlen in diesen Zusammenhang? Sie erfüllen gerade Gleichungen mit $n = 1$. Zum Beispiel ist ja für $x = \frac{2}{3}$, die Gleichung $3x - 2 = 0$ wahr. Die ganzen Zahlen sind hierbei gerade diejenigen, die eine Gleichung $x - a_0 = 0$ erfüllen; dann ist natürlich $x = a_0$ und $a_n = 1$. Es stellt sich heraus, dass dieses der Schlüssel für eine Verallgemeinerung des Begriffs der 'ganzen Zahl' auf Zahlkörper ist. Wir sagen, dass die Zahl x eine *ganze algebraische Zahl* ist, wenn in obiger Gleichung $a_n = 1$ gilt. Der goldene Schnitt und $\sqrt{2}$ sind somit sogar ganze algebraische Zahlen. Wir begegnen den algebraischen Zahlen im weiteren Verlauf als Koeffizienten von sehr symmetrischen Modulformen.

Nun können wir beschreiben, was ein Zahlkörper ist. Nach Definition ist dies ein Körper, der alle Potenzen einer algebraischen Zahl enthält und zudem auch alle Zahlen, die sich aus diesen durch beliebige Multiplikationen und Additionen mit Bruchzahlen ergeben.

Kummers Idealtheorie

Schon Euklid (365-300 v. Chr.) war bekannt, dass es unendlich viele Primzahlen gibt und dass sich jede positive natürliche Zahl auf eindeutige Weise (bis auf Umordnung) als Produkt von Primzahlen

Wir nehmen an, dass

$$\sqrt{2} = \frac{p}{q}$$

ein gekürzter Bruch ist. Dabei ist der Nenner q natürlich ungleich null. Nun quadrieren wir beide Seiten und erhalten die Gleichung

$$2 = \frac{p^2}{q^2}.$$

Wir multiplizieren beide Seiten mit q^2 und finden

$$2 \cdot q^2 = p^2.$$

Somit ist p^2 gerade. Dies ist aber nur möglich, wenn bereits p gerade war, denn das Quadrat einer ungeraden Zahl ist ungerade. Insbesondere ist nun p^2 durch 4 teilbar, also von der Form $p^2 = 4 \cdot r$. Unsere letzte Gleichung können wir jetzt so schreiben:

$$2 \cdot q^2 = 4 \cdot r.$$

Teilen wir beide Seiten durch 2, bekommen wir

$$q^2 = 2 \cdot r.$$

Hieraus folgt genau wie gerade, dass q gerade ist. Also sind sowohl p als auch q gerade. Der Bruch zu Beginn ist somit sowohl gekürzt (das hatten wir ja angenommen) als auch nicht gekürzt (Zähler und Nenner sind beide durch 2 teilbar). Das ist natürlich nicht möglich und stellt einen Widerspruch dar. Da alle gemachten Schritte richtig sind, muss die Annahme, dass wir $\sqrt{2}$ als gekürzten Bruch darstellen können, falsch sein. Hiermit haben wir bewiesen, dass $\sqrt{2}$ keine Bruchzahl ist.

Abbildung 6: $\sqrt{2}$ ist kein Bruch

Die Summe zweier Zahlen aus $\mathbb{Q}(\sqrt{2})$ liegt in $\mathbb{Q}(\sqrt{2})$, z. B.

$$(\frac{1}{3}+\sqrt{2}\frac{1}{2})+(\frac{2}{3}+\sqrt{2}\frac{1}{3})=(\frac{1}{3}+\frac{2}{3})+\sqrt{2}(\frac{1}{2}+\frac{1}{3})=1+\sqrt{2}\frac{5}{6},$$

bzw. allgemeiner:

$$(\frac{p_1}{q_1}+\sqrt{2}\frac{r_1}{s_1})+(\frac{p_2}{q_2}+\sqrt{2}\frac{r_2}{s_2})=\frac{p_1q_2+p_2q_1}{q_1q_2}+\sqrt{2}\frac{r_1s_2+r_2s_1}{s_1s_2}.$$

Dieses gilt gleichermaßen für das Produkt (Ausmultiplizieren der Klammern):

$$\begin{aligned}(\frac{p_1}{q_1}+\sqrt{2}\frac{r_1}{s_1})\cdot(\frac{p_2}{q_2}+\sqrt{2}\frac{r_2}{s_2}) &= \frac{p_1}{q_1}\frac{p_2}{q_2}+\sqrt{2}\cdot\sqrt{2}\cdot\frac{r_1}{s_1}\frac{r_2}{s_2}+\sqrt{2}\frac{p_1}{q_1}\frac{r_2}{s_2}+\sqrt{2}\frac{r_1}{s_1}\frac{p_2}{q_2}\\ &= (\frac{p_1}{q_1}\frac{p_2}{q_2}+2\cdot\frac{r_1}{s_1}\frac{r_2}{s_2})+\sqrt{2}(\frac{p_1}{q_1}\frac{r_2}{s_2}+\frac{r_1}{s_1}\frac{p_2}{q_2}).\end{aligned}$$

Klammern manipuliert man genauso wie in den reellen Zahlen (Assoziativität und Distributivität).

Abbildung 7: Der Zahlkörper $\mathbb{Q}(\sqrt{2})$

schreiben lässt. Nun stellt sich natürlich die Frage, ob ähnliche Eigenschaften auch in Zahlkörpern erfüllt sind, genauer in den ganzen algebraischen Zahlen eines Zahlkörpers. Es stellt sich heraus, dass die naive Verallgemeinerung falsch ist. Jedoch hat Ernst Eduard Kummer (1810-1893), auch motiviert von der Herausforderung von Fermats letztem Satz, eine andere Verallgemeinerung gefunden, die für alle Zahlkörper gilt. Diese beschreiben wir nun.

In den ganzen algebraischen Zahlen eines Zahlkörpers kann man verschiedene Phänomene beobachten. Zum Beispiel kann es sein, dass sich eine Primzahl in dem Zahlkörper faktorisieren, also in das Produkt von zwei Zahlen (ungleich 1) zerlegen lässt. Des Weiteren kann im Allgemeinen nicht jede Zahl auf eindeutige Weise als Produkt von Zahlen geschrieben werden, die sich nicht weiter zerlegen lassen. Beispiele dieser Phänomene sind sehr einfach zu verstehen (siehe erster Teil der Abbildung 8).

Kummers große Einsicht war, von Zahlen zu bestimmten Mengen von Zahlen überzugehen, den *Idealen* (Kummer nannte diese 'ideale Zahlen'). Er hat ein Produkt von Idealen definiert und es ist ihm gelungen zu beweisen, dass sich jedes Ideal als eindeutiges Produkt von nicht weiter zerlegbaren Idealen schreiben lässt. Letztere nennt man *Primideale*, in Analogie zu den Primzahlen. Die in den gewöhnlichen ganzen Zahlen geltende eindeutige Zerlegung in Primzahlen wird also in Zahlkörpern ersetzt durch die eindeutige Zerlegung jedes Ideals in Primideale. Man kann jeder ganzen Zahl ein Ideal zuordnen, das dann *Hauptideal* heißt. Jedes Hauptideal lässt sich nach Kummers Satz in ein eindeutiges Produkt von Primidealen faktorisieren. Dieses führt uns zu für das Folgende wichtigen Begriffen: Zerlegung und Verzweigung. Eine Primzahl heißt *verzweigt*, wenn das Quadrat eines Primideals in der Faktorisierung des zur Primzahl gehörigen Hauptideals auftritt. Es ist ein klassischer Satz, dass für jeden Zahlkörper nur endlich viele Primzahlen verzweigt sind. Die verzweigten Primzahlen werden uns im Zusammenhang mit den Modulformen noch wieder begegnen. Eine Primzahl heißt *voll zerlegt*, wenn in der Faktorisierung des Hauptideals die maximal mögliche Anzahl von Primidea-

Die ganzen algebraischen Zahlen im Zahlkörper $\mathbb{Q}(\sqrt{-23})$ sind alle von der Form $a + b \cdot \frac{1+\sqrt{-23}}{2}$ mit (gewöhnlichen) ganzen Zahlen a, b; gerechnet wird ganz genauso wie für den Zahlkörper $\mathbb{Q}(\sqrt{2})$. Das erste Phänomen ist, dass sich einige Primzahlen zerlegen lassen. Hier ist ein Beispiel (wir benutzen die dritte binomische Formel):

$$\begin{aligned} 59 &= 36 + 23 = 36 - (-23) = 36 - (\sqrt{-23})^2 = (6 + \sqrt{-23}) \cdot (6 - \sqrt{-23}) \\ &= (5 + 2 \cdot \frac{1 + \sqrt{-23}}{2}) \cdot (7 - 2 \cdot \frac{1 + \sqrt{-23}}{2}) \end{aligned}$$

Das zweite Phänomen ist, dass die Faktorisierung nicht mehr eindeutig ist. Dazu betrachten wir folgendes Beispiel:

$$39 = 3 \cdot 13$$

und

$$39 = (4 + \sqrt{-23}) \cdot (4 - \sqrt{-23}) = (3 + 2 \cdot \frac{1 + \sqrt{-23}}{2}) \cdot (5 - 2 \cdot \frac{1 + \sqrt{-23}}{2}).$$

Man kann einfach nachrechnen, dass die Zahlen 3, 13, $3+2\cdot\frac{1+\sqrt{-23}}{2}$ und $5-2\cdot\frac{1+\sqrt{-23}}{2}$ sich jeweils nicht weiter zerlegen lassen. Somit ist also wirklich der klassische Satz, dass sich jede Zahl eindeutig als Produkt von Primzahlen schreiben lässt, in einem allgemeinen Zahlkörper nicht mehr wahr. Ein letztes Phänomen ist von sehr großer Bedeutung. Als Beispiel betrachten wir:

$$23 = -\big(1 - 2\frac{1 + \sqrt{-23}}{2}\big)^2.$$

Die Zahl 23 ist also, bis auf das Minuszeichen, ein Quadrat.
Beschreiben wir nun kurz einige Ideale in $\mathbb{Q}(\sqrt{-23})$. Das Hauptideal zu einer ganzen Zahl ist die Menge aller ihrer Vielfachen mit ganzen algebraischen Zahlen. Z. B. ist das Hauptideal von 3, bezeichnet mit (3), die Menge $3 \cdot (a + b \cdot \frac{1+\sqrt{-23}}{2})$ für alle gewöhnlichen ganzen Zahlen a und b. Allgemeiner ist ein Ideal eine Menge bestehend aus ganzen Zahlen des Zahlkörpers, so dass Summen zweier Elemente des Ideals wiederum im Ideal liegen und das Produkt eines beliebigen Elementes aus dem Ideal mit einer beliebigen ganzen algebraischen Zahl in $\mathbb{Q}(\sqrt{-23})$ auch wiederum im Ideal ist. Es stellt sich heraus, dass die eindeutigen Primidealzerlegungen der Hauptideale (3) und (13) wie folgt aussehen:

$$(3) = \mathfrak{P}_1\mathfrak{P}_2, \quad (13) = \mathfrak{P}_3\mathfrak{P}_4$$

mit bestimmten Primidealen $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{P}_3$ und $\mathfrak{P}_4$. Das heißt, dass 3 und 13 beide voll zerlegt sind. Das Hauptideal (39) ist dann von der Form

$$(39) = (3) \cdot (13) = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_4.$$

Außerdem ist

$$(23) = \mathfrak{Q}^2$$

mit $\mathfrak{Q}$ dem Hauptideal $(1 - 2\frac{1+\sqrt{-23}}{2})$. Somit ist 23 verzweigt.

Abbildung 8: Phänomene im Zahlkörper $\mathbb{Q}(\sqrt{-23})$.

len auftritt (für diejenigen, die es genau wissen wollen: so viele wie der Grad des Zahlkörpers). Ein Beispiel ist in Abbildung 8 diskutiert. Nach einem berühmten Satz von Nikolai Grigorjewitsch Tschebotarjow (1894-1947) bestimmt die Menge der voll zerlegten Primzahlen den Zahlkörper eindeutig. Schließen wir diesen Abschnitt mit der Bemerkung, dass man die Eigenschaften der Primideale, also zum Beispiel Zerlegung und Verzweigung, häufig unter dem Begriff *Arithmetik* zusammenfasst.

Endliche Körper

Hier möchten wir jetzt auf eine ganz andere Klasse von Zahlen und Körpern eingehen, nämlich die endlichen. Der Hauptsatz über endliche Körper besagt, dass die Anzahl der Elemente jedes endlichen Körpers eine Primzahlpotenz ist, also von der Form p^r mit p einer Primzahl und r einer positiven natürlichen Zahl. Umgekehrt gibt es für jede Primzahlpotenz einen endlichen Körper mit der gegebenen Anzahl an Elementen. Er sei mit $\mathrm{GF}(p^r)$ bezeichnet.

Die einfachsten endlichen Körper sind diejenigen, deren Anzahl an Elementen eine Primzahl ist, z. B. $p = 5$ (also $r = 1$). Diese erhält man direkt als 'Rechnen mit Resten'. Die Elemente dieser Körper werden repräsentiert durch die Zahlen 0, 1, $\ldots$, $p-1$, in unserem Beispiel also 0 bis 4. Man addiert zwei solche Elemente, z. B. 2 und 4, indem man die gewöhnliche Summe bildet, also 6, und dann den Rest beim Teilen durch p ausrechnet; dieser ist dann die Summe der beiden Elemente in $\mathrm{GF}(p)$. In unserem Beispiel wäre also $2+4 = 1$ in $\mathrm{GF}(5)$. Ganz genauso verfährt man mit Produkten. Wir bilden das Produkt von 2 und 4 zunächst in den natürlichen Zahlen, also 8; der Rest bei Division durch 5 ist 3; dieses ist das Produkt von 2 und 4 im endlichen Körper $\mathrm{GF}(5)$.

Endliche Körper spielen in diesem Artikel zwei wichtige Rollen. Zum einen benötigen wir sie zur Definition von GL_2-Zahlkörpern. Zum anderen kann man von Zahlkörpern zu endlichen Körpern übergehen und zwar für jedes Primideal des Zahlkörpers.

Reelle Zahlen und unendliche Reihen

Nach der Betrachtung der Zahlen in endlichen Körpern wollen wir uns nun den reellen Zahlen zuwenden. Die reellen Zahlen sind die Zahlen, die wir im Alltag verwenden. Diese stellen wir zumeist in Dezimalschreibweise dar: $23,05$ oder $1,979$ oder $\sqrt{2} = 1,414213562373\ldots$. Was meinen wir mit $1,979$? Natürlich: $1 + \frac{9}{10} + \frac{7}{100} + \frac{9}{1000}$. Eine allgemeine reelle Zahl hat ja eine unendlich lange Dezimalschreibweise, wir haben es somit mit unendlich langen Summen zu tun, solche nennen wir Reihen. Wir können zum Beispiel jede reelle Zahl größer gleich 0 und kleiner als 1 schreiben als

$$0, z_1 z_2 z_3 \cdots = \frac{z_1}{10} + \frac{z_2}{10^2} + \frac{z_3}{10^3} + \cdots = \sum_{i=1}^{\infty} \frac{z_i}{10^i},$$

wobei die Ziffern z_i ganze Zahlen zwischen 0 und 9 sind. Der Ausdruck $\sum_{i=1}^{\infty} \frac{z_i}{10^i}$ bedeutet dann genau das, was davor steht, nämlich, dass man all die Brüche $\frac{z_i}{10^i}$ (für $i = 1, 2, 3, \ldots$, also unendlich viele) aufsummiert.

Die harmonische Reihe ist definiert als

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n}.$$

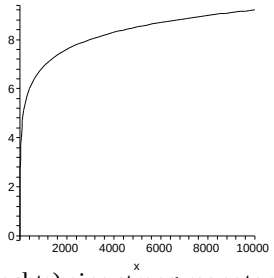
Diese divergiert. Aber langsam! Die Leserin oder der Leser ist eingeladen, sich mit dem Taschenrechner oder dem Computer einen Eindruck von der Langsamkeit des Wachstums zu verschaffen.

Um einzusehen, dass die Reihe divergiert, kann man die Summe mit dem Integral $\int_1^\infty \frac{1}{x} dx$ vergleichen:

$$\int_1^N \frac{1}{x} dx \leq \sum_{n=1}^{N} \frac{1}{n}.$$

Rechnet man das Integral aus, erhält man

$$\log(N) \leq \sum_{n=1}^{N} \frac{1}{n}.$$



Da der natürliche Logarithmus $\log$ (siehe Abbildung rechts) eine streng monoton steigende Funktion ist, folgt, dass die harmonische Reihe divergiert.

Abbildung 10: Die harmonische Reihe

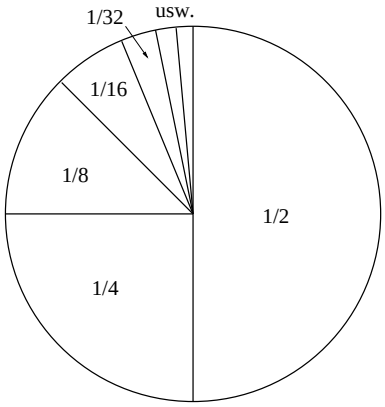


Abbildung 9: Kuchen als Illustration von $\sum_{n=1}^{\infty} \frac{1}{2^n} = 1$

Betrachten wir als anderes Beispiel die Reihe

$$\sum_{n=1}^{\infty} \frac{1}{2^n} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \ldots.$$

Man kann sie als 'Null Komma Periode 1' im Binärsystem lesen. Erinnern wir uns, dass 'Null Komma Periode 9' im Dezimalsystem gleich 1 ist, so können wir in Analogie hoffen, dass obige Reihe den Wert 1 hat. Das ist in der Tat so, und man kann sich dieses ganz einfach am Bild des Kuchens klar machen (Abbildung 9). Das erste Stück gibt einen halben Kuchen, die ersten beiden einen drei Viertel Kuchen, die ersten drei einen sieben Achtel Kuchen, bzw. allgemeiner die ersten N einen $\frac{2^N-1}{2^N}$-tel Kuchen. Man sieht sofort, dass das fehlende Stück mit jedem Schnitt immer kleiner wird: Seine Größe kommt der 0 beliebig nah (man sagt, sie konvergiert gegen 0) und somit nimmt die Reihe den Wert 1 an.

Der Leser oder die Leserin sei gewarnt, dass nicht jede unendliche Reihe *konvergiert*, also einen wohl definierten Wert hat: Das unendlich oft Aufaddieren der 1 (also $\sum_{n=1}^{\infty} 1$) ergibt natürlich keine wohl definierte Zahl; man sagt, dass die Reihe *divergiert*. Ein etwas ausgefalleneres Beispiel einer divergenten Reihe findet sich in Abbildung 10. Euler hat übrigens bewiesen, dass die Reihe $\sum_{n=1}^{\infty} \frac{1}{n^2}$ den Wert $\frac{\pi^2}{6}$ hat.

Es gibt, wie wir ja wissen, unendlich viele natürliche Zahlen $1, 2, 3, \ldots$ und auch unendlich viele

Wir nehmen an, dass wir die reellen Zahlen zwischen 0 und 1 aufzählen können. Diese Annahme wollen wir zum Widerspruch führen, was dann beweist, dass die reellen Zahlen überabzählbar sind. Schreiben wir die angenommene Aufzählung (in Dezimalschreibweise) auf:

1.	$0,\, z_{1,1}\, z_{1,2}\, z_{1,3}\, z_{1,4}\, z_{1,5}\, z_{1,6}\, z_{1,7}\, z_{1,8}\, \ldots$
2.	$0,\, z_{2,1}\, z_{2,2}\, z_{2,3}\, z_{2,4}\, z_{2,5}\, z_{2,6}\, z_{2,7}\, z_{2,8}\, \ldots$
3.	$0,\, z_{3,1}\, z_{3,2}\, z_{3,3}\, z_{3,4}\, z_{3,5}\, z_{3,6}\, z_{3,7}\, z_{3,8}\, \ldots$
4.	$0,\, z_{4,1}\, z_{4,2}\, z_{4,3}\, z_{4,4}\, z_{4,5}\, z_{4,6}\, z_{4,7}\, z_{4,8}\, \ldots$
5.	$0,\, z_{5,1}\, z_{5,2}\, z_{5,3}\, z_{5,4}\, z_{5,5}\, z_{5,6}\, z_{5,7}\, z_{5,8}\, \ldots$
6.	$0,\, z_{6,1}\, z_{6,2}\, z_{6,3}\, z_{6,4}\, z_{6,5}\, z_{6,6}\, z_{6,7}\, z_{6,8}\, \ldots$
7.	$0,\, z_{7,1}\, z_{7,2}\, z_{7,3}\, z_{7,4}\, z_{7,5}\, z_{7,6}\, z_{7,7}\, z_{7,8}\, \ldots$
8.	$0,\, z_{8,1}\, z_{8,2}\, z_{8,3}\, z_{8,4}\, z_{8,5}\, z_{8,6}\, z_{8,7}\, z_{8,8}\, \ldots$
$\ldots$	$\ldots$

Dabei sind die $z_{i,j}$ Ziffern zwischen 0 und 9. Wir dürfen annehmen, dass $z_{1,1}$ gleich 0 ist. Wir bilden nun eine reelle Zahl, die nicht in der obigen Aufzählung enthalten ist. Für jede natürliche Zahl i sei dazu $\bar{z}_i$ die eindeutig bestimmte Zahl zwischen 0 und 9, so dass $\bar{z}_i - z_{i,i} - 2$ durch 10 teilbar ist. Drei Beispiele: Ist $z_{i,i} = 0$, dann ist $\bar{z}_i = 2$; ist $z_{i,i} = 1$, dann ist $\bar{z}_i = 3$; ist $z_{i,i} = 9$, dann ist $\bar{z}_i = 1$. Wir betrachten nun die reelle Zahl in Dezimalschreibweise

$$0,\, \bar{z}_1\, \bar{z}_2\, \bar{z}_3\, \bar{z}_4\, \bar{z}_5\, \bar{z}_6\, \bar{z}_7\, \bar{z}_8\, \ldots.$$

Sie ist zwischen 0 und 1 (die Neuner-Periode kann sie wegen $z_{1,1} = 0$ nicht sein). Die Zahl ist ganz offensichtlich verschieden von allen aufgelisteten Zahlen, denn für jede natürliche Zahl i unterscheidet sie sich von der i-ten Zahl in unserer Auflistung, nämlich an der i-ten Stelle. Wir haben also eine reelle Zahl gefunden, die noch nicht in der Aufzählung enthalten war. Das ist der gesuchte Widerspruch, denn wir haben ja angenommen, alle aufgelistet zu haben.

Abbildung 11: Die reellen Zahlen sind überabzählbar.

reelle Zahlen. Es war eine geniale Einsicht von Georg Cantor (1845-1918), dass es trotzdem mehr reelle als natürliche Zahlen gibt. Die natürlichen Zahlen sind ja die 'Zählzahlen'. Damit, dass es mehr reelle als natürliche Zahlen gibt, meinen wir, dass es unmöglich ist, die reellen Zahlen zu zählen. Wir sprechen davon, dass die Menge der reellen Zahlen *überabzählbar* ist. In Abbildung 11 haben wir Cantors ganz simple Beweisidee wiedergegeben. Die Menge der algebraischen Zahlen hingegen kann man abzählen. Es ist eine ganz hübsche Aufgabe, dieses zu beweisen. Dazu sollte man benutzen, dass man die definierenden Gleichungen, die Polynome, auflisten kann und jede solche Gleichung höchstens so viele Lösungen hat wie ihr Grad (das ist das n) angibt. Die Konsequenz ist, dass es viel mehr reelle Zahlen als algebraische gibt. Somit ist die Eigenschaft, eine algebraische Zahl zu sein, etwas ganz Besonderes. Das berühmteste Beispiel einer reellen Zahl, die nicht algebraisch ist, ist die Kreiszahl π. Die nicht-Algebraiziät wurde erst im Jahre 1882 bewiesen.

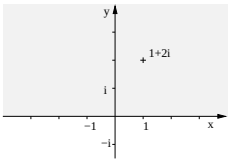


Abbildung 12: Obere Halbebene

Komplexe Zahlen

Komplexe Zahlen sind daraus entstanden, dass man gerne hätte, dass eine quadratische Gleichung $x^2+a\cdot x+b=0$ stets zwei Lösungen hat, die man eventuell mit Vielfachheiten zählen muss. Erinnern wir uns, dass zum Beispiel $x^2-1=0$ die Lösungen 1 und -1 hat. Die Gleichung $x^2+2x+1=(x+1)^2=0$ hat die Lösung -1 mit Vielfachheit 2. Die Lösungen von $x^2-2=0$ sind $\sqrt{2}$ und $-\sqrt{2}$. Wie sieht es mit $x^2+1=0$ aus? Da das Quadrat jeder reellen Zahl nicht negativ ist, kann diese Gleichung keine Nullstelle in den reellen Zahlen haben. Da es sich als sehr praktisch herausstellt, wenn jede quadratische Gleichung zwei Lösungen (mit Vielfachheiten) hat, führt man nun die Zahl $i=\sqrt{-1}$ *formal* ein; es ist keine reelle Zahl, es ist lediglich eine Zahl, deren Quadrat gleich -1 ist. Nun erhalten wir, dass $x^2+1=0$ die Lösungen i und $-i$ hat. Eine *komplexe Zahl* ist dann definiert als eine Zahl der Form $x+i\cdot y$ mit reellen Zahlen x und y.

In den komplexen Zahlen hat nun jede quadratische Gleichung zwei Lösungen (mit Vielfachheiten). Zum Beispiel sind die Lösungen von $x^2+23=0$ gleich $\sqrt{-23}=\sqrt{-1}\cdot\sqrt{23}=i\cdot\sqrt{23}$ und $-i\cdot\sqrt{23}$. Der so genannte *Hauptsatz der Algebra* besagt nun, dass jede Gleichung n-ten Grades genau n Lösungen (mit Vielfachheiten) in den komplexen Zahlen hat.

3 Geometrie

Komplexe Geometrie

Schließen wir für unsere geometrischen Betrachtungen direkt an die komplexen Zahlen an. Alle sind von der Form $x+i\cdot y$ mit reellen Zahlen x,y. Wir können x und y als kartesische Koordinaten ansehen und die komplexen Zahlen mit der Ebene identifizieren. Dieses ist bereits ein komplex geometrisches Objekt, in gewissem Sinne das einfachste.

Für die Theorie der Modulformen benötigen wir nur einen Teil hiervon, nämlich die *obere Halbebene*. Diese ist genauso definiert, wie der Name es suggeriert, nämlich als der Teil der Ebene, der oberhalb der x-Achse liegt. In der Sprache der komplexen Zahlen besteht die obere Halbebene also genau aus den komplexen Zahlen $x+i\cdot y$ mit $y>0$ (siehe Abbildung 12).

Um eine Idee von allgemeineren komplex geometrischen Objekten zu bekommen, betrachtet man am besten zunächst den Zusammenhang zwischen Erdkugel und Weltatlas. Die Erde ist eine Kugel und ihre Oberfläche 'passt' nicht als Ganzes in ein Buch. Wenn wir uns allerdings auf kleine Ausschnitte (zum Beispiel die Stadt Essen) beschränken, dann merken wir gar nicht, dass wir auf einer

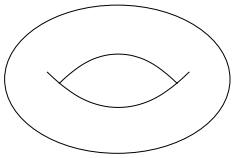


Abbildung 13: Torus

Kugel stehen und wir können den Stadtplan als etwas 'Plattes' auffassen, das dann wohl in ein Buch passt. Wenn wir nun so viele kleine Pläne in unseren Atlas aufnehmen, dass jeder Punkt der Erde in mindestens einem Plan liegt, dann haben wir die Oberfläche der Erde vollständig beschrieben. Genauso geht man vor bei den *Riemannschen Flächen*. Es sind dies geometrische Objekte (wie zum Beispiel die Kugeloberfläche), die im Kleinen so aussehen wie die komplexe Ebene, die man also mit Hilfe eines Atlas beschreiben kann. Betrachtet man nur die so genannten kompakten Riemannschen Flächen, dann kann man sie (bis auf glatte Transformationen) durch die Anzahl ihrer Löcher eindeutig charakterisieren: die Kugel hat kein Loch, der Fahrradreifen (Torus) aus Abbildung 13 hat ein Loch etc.

Die Riemannschen Flächen haben übrigens ihren Eingang in die große Weltliteratur gefunden: 'Near Shepherd's Bush two thousand Beta-Minus mixed doubles were playing Riemann-surface tennis.'[7] 'The nearest Riemann-surfaces were at Guildford.'[8]

Modulformen kann man als bestimmte Funktionen (Differentialformen) auf bestimmten Riemannschen Flächen ansehen. Damit sind Modulformen in der Geometrie verwurzelt. Wie viele essentiell verschiedene Modulformen (eines bestimmten Typs) es zu einer gegebenen Riemannschen Fläche gibt, kann man übrigens ganz einfach an der Anzahl der Löcher ablesen.

Arithmetische algebraische Geometrie

Viele geometrische Objekte, zum Beispiel alle (kompakten) Riemannschen Flächen, die ja zunächst komplex geometrischer Natur sind, haben eine Struktur über einem Zahlkörper, was wir sofort erklären. Der Ansatz der *arithmetischen algebraischen Geometrie*, vorangetrieben vor allem von Alexander Grothendieck (geb. 1928), ist, Zahlentheorie und Geometrie zu verbinden, indem man Geometrie über Zahlkörpern studiert und viele klassische geometrische Sätze auch über Zahlkörpern beweist.

Betrachten wir ein ganz einfaches, aber doch schon interessantes Beispiel, den Kreis vom Radius 1 (Abbildung 14). Er besteht aus allen Punkten, deren Abstand vom Nullpunkt gleich 1 ist, deren Koordinaten (x, y) also $x^2 + y^2 = 1$ erfüllen. Mit anderen Worten besteht der reelle Einheitskreis aus den reellen Lösungen (x, y) der Gleichung $x^2 + y^2 - 1 = 0$. Man bemerke, dass in dieser Gleichung nur noch ganze Zahlen vorkommen, alles genuin reelle ist verschwunden! Nun kann man sich natürlich fragen, welche Bruchzahlen diese Gleichung erfüllen, und allgemeiner noch, welche Zahlen eines vorgegebenen Zahlkörpers dieses auch tun. Damit ist man wieder bei einer ganz offenbar

[7] Huxley, Chapter 4
[8] ibid., Chapter 18

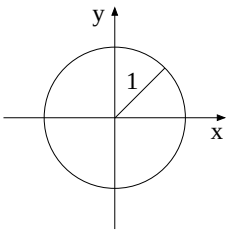


Abbildung 14: Einheitskreis

zahlentheoretischen Fragestellung, nämlich, Zahlen zu untersuchen, die einer gegebenen Gleichung genügen. Bleiben wir kurz beim Einheitskreis und den Bruchzahlen. Erfüllen Bruchzahlen $x = \frac{a}{c}$ und $y = \frac{b}{c}$ (wir haben sie auf den kleinsten gemeinsamen Nenner gebracht) die Gleichung, so erhalten wir nach Durchmultiplizieren mit c:

$$a^2 + b^2 = c^2,$$

also ein Pythagoräisches Zahlentripel. Übrigens stammt jedes teilerfremde Pythagoräische Zahlentripel genau von einem rationalen Punkt auf dem Kreis. Hier ist ein ganz konkretes Beispiel: $x = \frac{3}{5}$ und $y = \frac{4}{5}$ beschreiben einen rationalen Punkt auf dem Einheitskreis, der vom Zahlentripel $3^2 + 4^2 = 5^2$ herkommt. Den letzten Satz von Fermat kann man auch so umformulieren: Die Kurve, die durch die Lösungen von $x^n + y^n - 1 = 0$ (für jedes $n \geq 3$) gegeben ist, besitzt keine Punkte, deren Koordinaten Bruchzahlen ungleich null sind.

Dass ein geometrisches Objekt, zum Beispiel eine Riemannsche Fläche, eine Struktur über einem Zahlkörper hat, bedeutet nun genau das, was wir am Beispiel des Einheitskreises gesehen haben: Die Punkte sind gerade die Lösungen von unter Umständen mehreren Gleichungen mit Einträgen im Zahlkörper (im Beispiel $x^2 + y^2 - 1 = 0$; der Zahlkörper ist der der Bruchzahlen).

4 Symmetrien

Geometrische Symmetrien

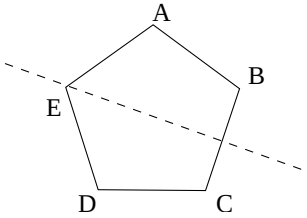


Abbildung 15: Fünfeck

Eine sehr wichtige Methode zur Untersuchung von geometrischen Objekten ist die Betrachtung ihrer *Symmetrien*. Ebene Symmetrien sind abstandserhaltende Transformationen, die das Objekt in sich selbst überführen. Als Beispiel betrachten wir das regelmäßige Fünfeck (Abbildung 15). Welche Symmetrien gibt es? Es sind dies die Drehungen um $n \cdot 72$ Grad mit $n \in \{0, 1, 2, 3, 4\}$ und die Spiegelungen an den Achsen, die durch einen Eckpunkt gehen und senkrecht auf der gegenüber dem Eckpunkt liegenden Seite stehen. Insgesamt gibt es also 10 solche Transformationen. Das Hintereinanderausführen von zwei solchen liefert eine dritte. Außerdem kann man die Transformationen wieder rückgängig machen (die Rotation um $n \cdot 72$

Die Modulgruppe, bezeichnet mit $\mathrm{SL}_2(\mathbb{Z})$, ist die Menge aller 2×2-Matrizen (d. h. Zahlenviertupel) $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ mit ganzen Zahlen als Einträgen (zum Beispiel $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$), so dass die *Determinante*, das ist die Zahl $ad - bc$, gleich 1 ist.
Man multipliziert zwei Matrizen wie folgt:

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) = \left(\begin{smallmatrix} ar+bt & as+bu \\ cr+dt & cs+du \end{smallmatrix}\right).$$

Ferner gelten

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$$

und

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

Diese Eigenschaften, zusammen mit den üblichen Klammerregeln (Assoziativität), fasst man unter dem Namen *Gruppe* zusammen.

Abbildung 16: Die Modulgruppe

Grad durch Rotation um $(5 - n) \cdot 72$ Grad, und die Spiegelung durch nochmaliges Ausführen). Man sagt, dass die Symmetrien eine *Gruppe* bilden.

Für Modulformen sind die *Möbius-Symmetrien* der oberen Halbebene von grundlegender Bedeutung. Sie sind ganz einfach definiert. Ist $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ ein Element der Modulgruppe (siehe Abbildung 16), dann ordnet man ihm die Möbius-Symmetrie zu, die den Punkt z der oberen Halbebene auf den Punkt $\frac{az+b}{cz+d}$ schickt. Betrachten wir zwei Beispiele. Die Symmetrie zum Element $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ ergibt sich als 'z geht auf $z + 1$', es handelt sich also um die Verschiebung um 1. Das Element $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ ergibt die Abbildung, die z auf $-\frac{1}{z}$ schickt.

Alle Symmetrien der Modulgruppe kann man durch einen Kunstgriff auch in einem geometrischen Objekt fassen, dem Quotienten bzw. der *Modulkurve* (der Stufe 1). Dieses ist eine Riemannsche Fläche.

Symmetrien von Zahlkörpern

Die Betrachtung von Symmetrien von Körpern geht zurück auf Evariste Galois (1811-1832). Eine Galois-Symmetrie ist eine Abbildung des Körpers in sich selbst, die die Addition und die Multiplikation respektiert (d.h. ist ϕ die Abbildung und sind a, b Elemente des Körpers, dann gelten $\phi(a + b) = \phi(a) + \phi(b)$ und $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$). Der Zahlkörper $\mathbb{Q}(\sqrt{2})$ hat zum Beispiel neben der Identität noch die Galois-Symmetrie, die dadurch charakterisiert ist, dass sie $\sqrt{2}$ auf $-\sqrt{2}$ schickt. Es gibt übrigens Zahlkörper, deren Gruppe von Galois-Symmetrien denselben Gesetzen folgt wie die Symmetriegruppe des Fünfecks. Z. B. ist dies der Fall bei dem Körper, den man erhält, indem

man zu den Bruchzahlen noch alle Lösungen der Gleichung $x^5 - 2x^4 + 2x^3 - x^2 + 1 = 0$ hinzufügt und alle Zahlen, die man aus diesen durch Multiplikation und Addition erhält.

Betrachten wir nun einen Zahlkörper (technische Voraussetzung: galoissch). Für jede unverzweigte Primzahl p gibt es eine Galois-Symmetrie, die *p-Frobenius-Symmetrie*, nach Ferdinand Georg Frobenius (1849-1917). Nun ist es aber so, dass ein Zahlkörper stets nur endlich viele verschiedene Galois-Symmetrien hat. Es ist von großem Interesse zu wissen, welche Galois-Symmetrie nun zur p-Frobenius-Symmetrie für eine gegebene Primzahl p gehört. Denn daraus kann man zum Beispiel ablesen, wieviele Primideale in der Faktorisierung des zu p gehörigen Hauptideals liegen. Die p-Frobenius-Symmetrien speichern also die Arithmetik des Zahlkörpers.

Für den Fortgang dieses Artikels spielen Zahlkörper, deren Galois-Symmetriegruppen in einer gewissen großen Familie von Gruppen liegen, die Hauptrolle. Diese Zahlkörper bezeichnen wir als GL_2*-Zahlkörper*. Sie sind dadurch ausgezeichnet, dass ihre Galois-Symmetriegruppe aus Elementen der Matrix-Gruppe GL_2 über einem endlichen Körper $\mathrm{GF}(p^r)$ besteht. Diese Matrix-Gruppe ist ganz genauso definiert wie die Modulgruppe aus Abbildung 16, mit dem einzigen Unterschied, dass die Einträge in den Matrizen (den Viertupeln) jetzt aus dem endlichen Körper $\mathrm{GF}(p^r)$ sind und die Determinante jetzt auch jede Zahl ungleich null sein darf.

Es gilt noch viel mehr: Die Galois-Symmetrien eines Zahlkörpers geben auch Symmetrien auf den Punkten von geometrischen Objekten mit einer Struktur über diesem Zahlkörper. Diese Symmetrien sind ganz anderer Natur als die geometrischen Symmetrien, die wir eben behandelt haben. Ganz allgemein gilt: Lässt eine Galois-Symmetrie eines Zahlkörpers die Einträge (Koeffizienten) der definierenden Gleichungen fest, so schickt sie eine Lösung der Gleichungen wiederum auf eine Lösung. Dieses machen wir uns wiederum am Beispiel des Einheitskreises und des Zahlkörpers $\mathbb{Q}(\sqrt{2})$ klar. Ein Punkt des Einheitskreises ist $(x, y) = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$, da ja $x^2 + y^2 = (\frac{1}{\sqrt{2}})^2 + (\frac{1}{\sqrt{2}})^2 = \frac{1}{2} + \frac{1}{2} = 1$ gilt. Die nicht triviale Galois-Symmetrie, die wir oben beschrieben haben, gibt uns einen neuen Punkt auf dem Kreis, nämlich $(\frac{1}{-\sqrt{2}}, \frac{1}{-\sqrt{2}})$, was man wie gerade nachprüft. Diese Symmetrie sieht vielleicht auf den ersten Blick wie die Spiegelung am Mittelpunkt aus, ist es aber nicht, denn zum Beispiel wird der oben betrachtete Punkt $(\frac{3}{5}, \frac{4}{5})$ festgelassen. Vielmehr kann man aufgrund der Galois-Symmetrien Punkte unterscheiden, deren Koordinaten in verschiedenen Zahlkörpern liegen.

5 Modulformen

Nun wollen wir genauer auf Modulformen eingehen. Modulformen sind Abbildungen von der oberen Halbebene in die komplexen Zahlen, die durch unendliche Reihen gegeben sind. Eine Modulform f ordnet jedem Punkt z aus der oberen Halbebene aufgrund einer bestimmten Regel einen Punkt $f(z)$ in den komplexen Zahlen zu. Die Regel ist stets von der Art

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$$

mit komplexen Zahlen a_n. Dabei ist e die Eulersche Zahl (ungefähr $2,71828$), also die Zahl, bei der der natürliche Logarithmus, den wir schon gesehen haben, den Wert 1 annimmt. Unendlichen

$$\begin{aligned} f(z) =& q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + q^{25} + q^{26} + q^{27} \\ & - q^{29} - q^{31} + q^{39} - q^{41} - q^{46} - q^{47} + q^{48} + q^{49} - q^{50} - q^{54} \\ & + q^{58} + 2 \cdot q^{59} + q^{62} + q^{64} - q^{69} - q^{71} - q^{73} - q^{75} - q^{78} - q^{81} \\ & + q^{82} + q^{87} + q^{93} + q^{94} - q^{98} + 2 \cdot q^{101} - q^{104} - 2 \cdot q^{118} + q^{121} \\ & + q^{123} - q^{127} - q^{128} - q^{131} + q^{138} - q^{139} + q^{141} + q^{142} + q^{146} \\ & - q^{147} + q^{150} - q^{151} + q^{162} - q^{163} + 2 \cdot q^{167} + 2 \cdot q^{173} - q^{174} \\ & - 2 \cdot q^{177} - q^{179} + q^{184} - q^{186} - q^{192} - q^{193} - q^{197} + \dots \end{aligned}$$

Die drei Punkte bedeuten, dass die Funktion noch unendlich weiter geht. Es gibt aber kein offensichtliches Bildungsgesetz, wie man es vielleicht aus (mathematisch unhaltbaren) Intelligenztests kennt. In obiger Formel steht q für die Funktion $q = q(z) = e^{2\pi iz}$ in der Variable z.

Abbildung 17: Sehr symmetrische Modulform von Stufe 23 und Gewicht 1

Eine Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in der Modulgruppe ist von *Stufe* N, wenn c durch N teilbar ist. Eine Funktion $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi inz}$ ist eine *Modulform* von *Stufe* N und *Gewicht* k, wenn für jede Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ von Stufe N

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$$

gilt und die technische Bedingung 'Holomorphizität in den Spitzen' erfüllt ist. Man bemerke die Möbius-Symmetrie in der Gleichung!

Abbildung 18: Modulformen

Reihen sind wir auch bereits vorne begegnet; hier sind die a_n so gewählt, dass die Reihen konvergieren und eine komplexe Zahl $f(z)$ definieren. Ein Beispiel mit sehr kleinen Koeffizienten findet sich in Abbildung 17.

Dieses alleine macht aber keine Modulform aus, sondern wir haben nur eine *Fourier-Reihe* beschrieben, nach Jean Baptiste Joseph Fourier (1768-1830). Das Besondere an Modulformen ist, dass sie ein spezielles Verhalten bezüglich bestimmter Möbius-Symmetrien aufweisen. Jede Modulform hat eine *Stufe* N und ein *Gewicht* k; beides sind positive natürliche Zahlen. Bezüglich jeder Möbius-Symmetrie von so genannter Stufe N verlangt man von einer Modulform nun, dass sie eine Symmetrie mit Gewicht k hat (siehe Abbildung 18 für genauere Aussagen). Es sei noch einmal darauf hingewiesen, dass man Modulformen auch als Funktionen auf bestimmten Riemannschen Flächen, nämlich den Modulkurven (passender Stufe), betrachten kann. Das ist technisch schwieriger, aber der große Vorteil ist, dass die Geometrie deutlicher zum Vorschein kommt.

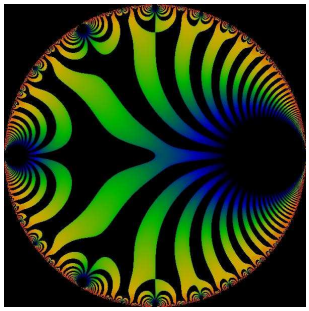


Abbildung 19: Delta-Funktion (Realteil)

Modulformen spielen seit ihrer Einführung im 19. Jahrhundert eine zentrale Rolle in der Zahlentheorie. Zu Anfang wurden sie mit Hilfe der Funktionentheorie untersucht. Es wurde früh festgestellt, dass die zugehörigen Fourierkoeffizienten, das sind die a_n, häufig interessante zahlentheoretische Bedeutungen haben. So gibt es z. B. eine Modulform, deren n-ter Fourierkoeffizient angibt, wie oft die natürliche Zahl n als Summe von 4 Quadraten dargestellt werden kann. Man kann Modulformen auch in einem Bild sichtbar machen; dabei ersetzt man die obere Halbebene durch die Einheitskreisscheibe. In Abbildung 19 findet sich die vielleicht berühmteste aller Modulformen, die Ramanujansche Delta-Funktion, nach Srinivasa Ramanujan (1887-1920). Die Möbius-Symmetrien treten im Bild sehr deutlich hervor.

Für unsere Betrachtungen stellen sich diejenigen Modulformen als besonders zugänglich heraus, die noch zusätzliche Symmetrien erfüllen. Diese zusätzlichen Symmetrien, die *Hecke-Symmetrien*, kann man auf verschiedene Arten sehen. Zum einen kann man Hecke-Symmetrien auf dem Raum der Modulformen durch Formeln in den Koeffizienten a_n definieren. Zu jeder natürlichen Zahl m gibt es eine Hecke-Symmetrie (siehe Abbildung 20). Ein viel konzeptionellerer Standpunkt ist allerdings wiederum geometrischer Natur: Hecke-Symmetrien lassen sich als Symmetrien (genauer Korrespondenzen) der Modulkurven verstehen.

Wir nennen Modulformen, die auch den Hecke-Symmetrien genügen, *sehr symmetrische Modulformen* oder *Hecke-Eigenformen*. Für sie gilt das wichtige Resultat, dass die a_n in der unendlichen Reihe ganze algebraische Zahlen sind und nicht 'nur' komplexe. Noch stärker gilt, dass man, wenn man alle möglichen Summen und Produkte aller Bruchzahlen und aller a_2, a_3, a_4 etc. bildet, einen Zahlkörper, den *Koeffizientenkörper* der Modulform, erhält.

6 Zusammenhang von Zahlentheorie und Geometrie

Symmetrien als Schlüssel

Kommen wir nun zum eigentlichen Gegenstand dieses Artikels, dem Zusammenhang zwischen Geometrie und Zahlentheorie, der durch Modulformen beschrieben wird, also dem Gegenstand der Serre-Vermutung. Dieser Zusammenhang beruht auf all den Symmetrien, die wir beschrieben haben.

Wir beschreiben die Hecke-Symmetrie (den *Hecke-Operator*) T_p für eine Primzahl p. Sei

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$$

eine Modulform von Gewicht k. Dann gibt es eine Modulform

$$T_p f(z) = \sum_{r=0}^{\infty} b_r e^{2\pi i r z}.$$

Dabei gilt: Falls p die Zahl r teilt, dann ist

$$b_r = a_{rp} + p^{k-1} a_{r/p}.$$

Falls nicht, dann ist

$$b_r = a_{rp}.$$

Die Symmetrien T_m für natürliche Zahlen m berechnen sich mit Hilfe einfacher Formeln aus den T_p.

Abbildung 20: Hecke-Symmetrien

Die Möbius-Symmetrien bewirken zunächst, wie oben schon herausgestellt, dass man eine gegebene Modulform als eine Funktion (Differentialform) auf einer (kompakten) Riemannschen Fläche, der Modulkurve (passender Stufe), betrachten kann. Diese kann, genauso wie der Einheitskreis, als Lösungsmenge von Gleichungen beschrieben werden, deren Einträge ganze Zahlen sind. Damit kommt eine Modulform also von einem geometrischen Objekt mit einer Struktur über dem einfachsten Zahlkörper, den Bruchzahlen. Somit ergibt jede Galois-Symmetrie eines Zahlkörpers auch eine Symmetrie der Modulkurve, wie vorne erklärt wurde.

Der Zusammenhang zwischen Zahlentheorie und Geometrie, der auf Modulformen beruht, ist aber qualitativ noch viel weiter gehender Natur. Er beruht nämlich neben dem gerade Beschriebenen ganz entscheidend auf den zusätzlichen Symmetrien, den Hecke-Symmetrien, die eine sehr symmetrische Modulform erfüllt.

Eine sehr symmetrische Modulform weist also Hecke-Symmetrien und Galois-Symmetrien auf. Erstere sind geometrischer, letztere zahlentheoretischer Natur. Der Zusammenhang zwischen Geometrie und Zahlentheorie ergibt sich aus diesen, denn sie hängen eng zusammen: Die Hecke-Symmetrie T_p für eine Primzahl p bestimmt nämlich die Galois-Symmetrie, die von der p-Frobenius-Symmetrie kommt!

p	Koeff.	Bedeutung
2	-1	$1^2+23=24=2\cdot 12$
3	-1	$1^2+23=24=3\cdot 8$
5	0	5 teilt nie n^2+23
7	0	7 teilt nie n^2+23
11	0	11 teilt nie n^2+23
13	-1	$4^2+23=39=13\cdot 3$
$\dots$	$\dots$	$\dots$
997	2	$164^2+23=997\cdot 27$
1009	0	1009 teilt nie n^2+23
$\dots$	$\dots$	$\dots$

Der Leser/die Leserin ist eingeladen, weitere Beispiele dieses interessanten Zusammenhangs zu überprüfen. Man kann übrigens eine noch genauere Beschreibung geben (für Kenner): Der Koeffizient bei p ist 2, wenn p in $\mathbb{Q}(\sqrt{-23})$ in zwei Hauptideale zerfällt; er ist -1, wenn p in zwei nicht-Hauptideale zerfällt; er ist 0, wenn es nur ein Ideal über p gibt.

Abbildung 21: Modulform von Stufe 23 und Gewicht 1 - Diskussion

Ein kleines Beispiel

Hier sei ein erstes ganz einfaches Beispiel des Zusammenhangs zwischen Zahlentheorie und Geometrie mittels Modulformen angeführt. Es ist so einfach, dass nicht alle Phänomene sichtbar werden, aber es gibt doch eine Idee von der Art zahlentheoretischer Information, die in jeder sehr symmetrischen Modulform gespeichert ist. Wie wir unten beschreiben werden, handelt die zahlentheoretische Aussage in voller Allgemeinheit von Zahlkörpern, deren Benutzung wir aber für das erste kleine Beispiel zunächst vermeiden können. Wir betrachten die sehr symmetrische Modulform aus Abbildung 17. Ihre Fourierkoeffizienten sind stets 0, ± 1 oder ± 2. Schaut man genauer hin, sieht man, dass die Koeffizienten a_p (also die Zahl vor q^p) für jede Primzahl p (mit der einzigen Ausnahme 23) stets 0, -1 oder 2 sind.

Eine vereinfachte Form des Zusammenhangs zwischen Geometrie und Zahlentheorie besagt das Folgende: Ist der Koeffizient a_p für eine Primzahl $p \neq 23$ gleich -1 oder gleich 2, dann gibt es eine natürliche Zahl n, so dass n^2+23 durch p teilbar ist. Ist der Koeffizient gleich 0, dann gibt es kein solches n. Siehe Abbildung 21 für ein paar Beispiele. Selbst in diesem kleinen Beispiel sehen wir, welche überhaupt nicht offensichtliche Information in einer Modulform kodiert ist.

Man kann und sollte sich natürlich fragen, ob einem diese Information in der Modulform überhaupt etwas nützt. Ob es für eine gegebene Primzahl p nun ein solches n gibt oder nicht, kann man ja bestimmt auch anders ausrechnen. In der Tat, denn wie der vorgebildete Leser bzw. die vorgebildete Leserin vielleicht weiß, war bereits Carl Friedrich Gauß (1777-1855) klar, wie man eine solche Frage sehr schnell löst, nämlich mittels des Gauß'schen Reziprozitätsgesetzes. Die genauere Erklärung der

Koeffizienten vom Ende von Abbildung 21 ist übrigens schon wesentlich schwerer: Für Kenner: Man muss in der Klassengruppe des Zahlkörpers in Abbildung 8 rechnen und der der Modulform zugeordnete Zahlkörper ist ein Teilkörper des Hilbertschen Klassenkörpers des quadratischen Zahlkörpers.

Aber: In den allermeisten anderen Fällen, die nicht so klein sind wie das gerade behandelte Beispiel, hat man keine andere Möglichkeit, irgendeine Information über die zur Modulform gehörigen Zahlkörper zu erlangen. Denn es ist sehr schwer, den zugehörigen Zahlkörper auszurechnen, also eine definierende Gleichung anzugeben. Ein entsprechender Algorithmus wurde erst in den letzten Jahren, hauptsächlich von Bas Edixhoven (Leiden), entwickelt. Aber selbst mit diesem Algorithmus erhält man nur in wenigen 'kleinen' Fällen wirklich den Zahlkörper, denn die Berechnung würde häufig Jahrhunderte oder gar weit über die Lebensdauer des Universums hinausreichen, abgesehen davon, dass mehr Speicher notwendig wäre als es Atome im Universum gibt. Von der Modulform kann man aber trotzdem meist die ersten Koeffizienten berechnen. Die zugehörigen Zahlkörper werden beliebig groß: Gibt man eine beliebige Schranke vor, dann kann man eine Modulform mit zugehörigem Zahlkörper finden, dessen Grad größer als die Schranke ist. Zum Beispiel findet man schon in Stufe 3313 (siehe unten; das ist übrigens eine sehr kleine Zahl!) eine Modulform mit Zahlkörper vom Grad mindestens $49252507745493099015348800125179517256349674088081808334935366755307152214369811852433228126288827677971126146826 24$ (für Kenner, die Zerlegungsgruppe von 2 ist SL_2 von $\mathrm{GF}(2^{127})$; die Elementanzahl dieser Gruppe ist obige Zahl). Die Modulform gibt aber Informationen über Zahlkörper preis, derer man sonst nie habhaft werden könnte.

GL_2-Zahlkörper zu einer sehr symmetrischen Modulform

Wir beschreiben jetzt genauer den Zusammenhang zwischen Geometrie und Zahlentheorie, der von einer sehr symmetrischen Modulform $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ von Stufe N und Gewicht k herkommt. Zunächst dürfen wir ein beliebiges Primideal im Koeffizientenkörper von f wählen. Wie wir wissen, kann man jede ganze algebraische Zahl im Koeffizientenkörper mittels des Primideals in einen endlichen Körper $\mathrm{GF}(q)$ (mit q einer Primzahlpotenz) abbilden, was wir im Folgenden auch tun werden.

Die Hauptaussage ist nun, dass es zur Modulform f und dem gewählten Primideal einen Zahlkörper K gibt, dessen Galois-Symmetriegruppe aus Matrizen in der Matrix-Gruppe GL_2 über $\mathrm{GF}(q)$ besteht. Damit ist K also ein GL_2-Zahlkörper, genauer ein *ungerader* GL_2-Zahlkörper, worauf wir hier aber nicht eingehen. Der versprochene Zusammenhang zwischen Hecke-Symmetrien und Galois-Symmetrien besagt nun das Folgende: Sei $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ die Matrix, die zur p-Frobenius-Symmetrie gehört. Dann ist $a+d$, die so genannte *Spur*, im endlichen Körper gleich der Zahl (dem Koeffizienten) a_p aus der unendlichen Reihe von f. Letzterer kommt von der Hecke-Symmetrie T_p (er ist ihr Eigenwert). Weiterhin ist $ad-bc$, die *Determinante*, gleich p^{k-1}. Übrigens genügen Spur und Determinante in den meisten Fällen, um die Matrix eindeutig (bis auf Konjugierte) zu bestimmen.

Damit erhalten wir die schon am Anfang erwähnten grundlegenden Aussagen. Formulieren wir das gerade Beschriebene noch einmal mit anderen Worten: Die Arithmetik des Zahlkörpers K, die, wie wir oben gesehen haben, mit Hilfe der p-Frobenius-Symmetrien beschrieben werden kann, hängt

von den Zahlen a_p der Modulform ab! Kürzer formuliert: *Die Modulform bestimmt die Arithmetik des Zahlkörpers K*. Anders herum gesehen: *Die Modulform speichert die Arithmetik des Zahlkörpers K*. Man kann sogar über den Zahlkörper K noch mehr sagen, denn man kennt seine verzweigten Primzahlen: Alle diese teilen $N \cdot q$.

Vergessen wir auch nicht, dass wir zunächst ein Primideal *gewählt* haben. Wir hätten unendlich viele andere wählen können und für jedes andere hätten wir einen anderen Körper K erhalten. Somit gibt uns eine sehr symmetrische Modulform eine ganze *Familie*, oder auch ein so genanntes *kompatibles System*, von Zahlkörpern zusammen mit ihrer Arithmetik.

Die Serre-Vermutung

Die Serre-Vermutung bzw. der Satz von Khare, Wintenberger u.a. liefert, wie zu Anfang bereits angedeutet, eine Umkehrung des gerade beschriebenen Sachverhaltes: *Jeder ungerade GL_2-Zahlkörper stammt von einer sehr symmetrischen Modulform.* Die quantitative Form der Vermutung besagt dabei sogar, dass sich die Stufe der Modulform und das Gewicht ausrechnen lassen. Erstere ist in etwa gleich dem Produkt der im Zahlkörper verzweigten Primzahlen, die q nicht teilen. Letztere berechnet sich aus Eigenschaften der Primideale, die q teilen.

Halten wir noch einmal die Hauptaussage fest: *Die Arithmetik aller ungerader GL_2-Zahlkörper lässt sich mit Modulformen fassen.*

Ein trickreicher Beweis

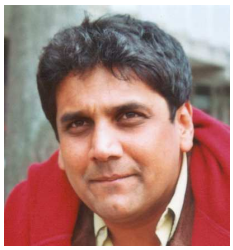


Abbildung 22: Chandrashekhar Khare

Der Beweis der Serre-Vermutung ist sowohl technisch schwer und tief liegend als auch trickreich. Wir können ihn hier verständlicherweise nicht wiedergeben. Der Haupttrick hingegen ist ziemlich zugänglich. Er basiert darauf, dass eine Modulform nicht nur einen GL_2-Zahlkörper liefert sondern eine ganze Familie.

Ist K ein ungerader GL_2-Zahlkörper, der laut der Serre-Vermutung von einer Modulform der Stufe N herkommen sollte, dann sagen wir kurz, dass N die *Stufe* von K ist.

Zunächst ist es Chandrashekhar Khare gelungen, die Serre-Vermutung zu beweisen für GL_2-Zahlkörper von Stufe $N = 1$.[9]

Außerdem haben Khare und Wintenberger, übrigens auch Luis Dieulefait (Barcelona), die folgende Reduktionsmethode erdacht, die nach harter technischer Arbeit und unter Zuhilfenahme vieler schwieriger Sätze, vor allem von Mark Kisin und Richard Taylor, schließlich zum Erfolg geführt hat: Sei ein ungerader GL_2-Zahlkörper K der Stufe N gegeben. Man kann zu einer Familie von GL_2-Zahlkörpern übergehen, zu der K gehört. Dann stellt man fest, dass diese Familie auch einen anderen ungeraden GL_2-Zahlkörper L von Stufe M enthält, wobei M durch eine Primzahl weniger teilbar ist als N. Der entscheidende Schluss ist nun, dass, wenn der

[9] Khare 2006

Zahlkörper L von einer Modulform herkommt, bereits die ganze Familie von einer Modulform herkommt (wie oben beschrieben). Insbesondere kommt auch der Zahlkörper K von einer Modulform her.

Dieses erlaubt einem dann ein schrittweises (induktives) Vorgehen. Für Stufe $N = 1$ hat Khare die Serre-Vermutung bewiesen. Im nächsten Schritt beweist man die Serre-Vermutung für GL_2-Zahlkörper von Stufe N, wobei N nur von einer einzigen Primzahl geteilt wird. Mittels der Reduktionsmethode kann man zu einem Zahlkörper L von Stufe $M = 1$ übergehen, der nach Khares Satz über Stufe 1 von einer Modulform kommt. Somit kommt auch K von einer Modulform.

Im folgenden Schritt können wir die Serre-Vermutung für Zahlkörper K zeigen, deren Stufe von genau zwei Primzahlen geteilt wird. Denn mit der Reduktionsmethode kann man zu einem Zahlköper L übergehen, dessen Stufe nur aus einer einzigen Primzahl besteht. Dieser kommt aber von einer Modulform nach vorherigem Schritt. Folglich kommt wiederum K auch von einer Modulform.

So fährt man fort und kann den Fall beliebiger Stufe behandeln.

7 Abschließende Bemerkungen und Ausblick

Modulformen wurden in diesem Artikel bereits facettenreich dargestellt: als geometrische Objekte und als unendliche Reihen. Gerecht sind wir ihnen hiermit allerdings immer noch nicht geworden. Das liegt unter anderem daran, dass *elliptische Kurven* aus Platzgründen nicht erwähnt werden konnten. Sie spielen aber eine gewichtige Rolle in der Theorie. Nach Wiles' Arbeiten zu Fermats letztem Satz kann man jeder elliptischen Kurve über den rationalen Zahlen eine Modulform zuordnen. Weiterhin kann man Modulformen als Funktionen auffassen, die jeder elliptischen Kurve eine Zahl zuweisen; Modulformen sind also Funktionen auf dem Klassifikationsraum der elliptischen Kurven. Dieses ist der konzeptionelle Hintergrund von Modulkurven. Diese Fakten über Modulformen gehen in die Beweise der oben erwähnten Sätze entscheidend ein und sind wichtig für unser Verständnis der Materie.

Ein weiterer Punkt sollte Erwähnung finden, nämlich die Verwendung von elliptischen Kurven und allgemeiner Modulformen in der Kryptographie, also zum Verschlüsseln und Signieren von Nachrichten. Dazu benötigt man so genannte *Einwegfunktionen*. Das sind Funktionen, die man schnell berechnen kann, deren Umkehrungen allerdings in praktischen Maßstäben unberechenbar sind. Elliptische Kurven über endlichen Körpern geben solche Funktionen: Man kann schnell einen Punkt auf der elliptischen Kurve multiplizieren. Ist hingegen ein Punkt gegeben, der ein Faktor eines anderen Punktes ist, so kennt man keine effiziente Methode, um den Faktor zu bestimmen. Viel allgemeiner kann man mittels Modulformen so genannte abelsche Varietäten (Jacobische Varietäten) finden, die elliptische Kurven verallgemeinern und auch ähnliche Einwegfunktionen bereit stellen.

Der hier dargestellte Zusammenhang zwischen Zahlentheorie und Geometrie passt sich in eine sehr große 'Philosophie', um das Wort 'Programm' zu vermeiden, ein: die *Langlands-Philosophie*. Diese geht zurück auf die Idee von Robert Langlands (geb. 1936, Princeton), dass automorphe Formen, das sind weit reichende Verallgemeinerungen von Modulformen, zu bestimmten Galois-Darstel-

lungen, das sind Verallgemeinerungen von GL_2-Zahlkörpern, korrespondieren sollten. Hatte Langlands wohl hauptsächlich an komplexe Darstellungen gedacht, wurde seine Idee in verschiedenste Kontexte übertragen. Die Serre-Vermutung kann als ein Teil einer *mod p Langlands-Philosophie* aufgefasst werden.

Alle diese 'Philosophien' suggerieren weitere tiefe und nützliche Zusammenhänge zwischen Geometrie und Zahlentheorie und werden die mathematische Forschung noch über lange Jahre bereichern.

Danksagung

Den Begriff der Symmetrie auch für Galois-Automorphismen zu verwenden, geht auf einen Vorschlag von Bas Edixhoven zurück. Wie nützlich dieser Hinweis von vor drei Jahren war, ist mir erst beim Schreiben dieses Artikels klar geworden.

Für sehr konstruktive Bemerkungen möchte ich G. Frey, G. Hein und meinem Vater danken.

8 Summary

Recently one of the most important structural conjectures in pure mathematics, Serre's modularity conjecture, has become a theorem, proved mainly by Khare and Wintenberger. Serre's conjecture establishes a link between seemingly different areas: number theory and geometry. This link is made through modular forms, which are functions dating back to the 19th century.

The main aim of the article is to describe the content of Serre's conjecture in a non-technical language. Moreover, links to past and ongoing research in Essen are mentioned, as well as some consequences of Serre's conjecture.

The article first surveys the objects involved in Serre's conjecture: modular forms and Galois representations. According to a theorem by Deligne and Shimura, any Hecke eigenform gives an odd 2-dimensional Galois representation. This is illustrated by means of a simple example. Serre's conjecture postulates that the converse is also true: any odd 2-dimensional irreducible Galois representation comes from a Hecke eigenform.

The remainder of the article is devoted to explaining these objects in more detail. Different types of 'numbers' and 'fields' are introduced, discussed and compared: algebraic numbers, real numbers, complex numbers, number fields and finite fields. Subsequently, complex geometry, in particular Riemann surfaces, are touched upon, and geometry over number fields (arithmetic geometry) is treated using a simple example. The article emphasizes the role played by symmetries. It takes the point of view that modular forms link geometry and number theory via symmetries: Möbius transforms, Hecke operators and Galois and Frobenius automorphisms are united as different kinds of symmetries. These objects are explained. Modular forms are presented as objects coming from and being rooted in geometry. The link between modular forms and Galois representations provided by Serre's modularity conjecture is finally explained in more detail and one small glimpse on its proof is provided. A final

section mentions further properties of modular forms without explanation and puts Serre's conjecture into the context of Langlands' philosophy.

Bildnachweise

- Das Foto von J.-P. Serre wurde aufgenommen von Xavier Taixés i Ventosa.
- Foto von E. Hecke: The MacTutor History of Mathematics archive, `http://www-history.mcs.st-andrews.ac.uk/`
- Die Abbildung der Delta-Funktion ist von Linas Vepstas von `http://en.wikipedia.org/wiki/Image:Discriminant_real_part.jpeg` (veröffentlicht unter der Gnu Free Documentation License).
- Das Foto von C. Khare wurde freundlicher Weise von C. Khare zur Verfügung gestellt.
- Alle anderen Abbildungen wurden vom Autor erstellt.

Literatur

- Aczel, Amir D.: Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem, Delta, 1997.
- Frey, Gerhard (Hrsg.): On Artin's conjecture for odd 2-dimensional representations, Lecture Notes in Math., 1585, Springer, Berlin, 1994.
- Huxley, Aldous: Brave new world. Eine freie Version findet sich auf `http://www.huxley.net/bnw/`
- Khare, Chandrashekhar: Serre's modularity conjecture: the level one case. Duke Math. J. 134 (2006), no. 3, 557–589.
- Khare, Chandrashekhar und Wintenberger, Jean-Pierre: Serre's modularity conjecture (I and II). Vorveröffentlichung, 2007.
- Serre, Jean-Pierre: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{Q}/Q)$, Duke Math. J. 54 (1987), no. 1, 179–230
- Singh, Simon: Fermats letzter Satz: Die abenteuerliche Geschichte eines mathematischen Rätsels, DTV, 2000.
- Wiese, Gabor: Multiplicities of Galois representations of weight one. With an appendix by Niko Naumann. Algebra Number Theory 1 (2007), no. 1, 67–85.
- Wiese, Gabor: On the faithfulness of parabolic cohomology as a Hecke module over a finite field. J. Reine Angew. Math. 606 (2007), 79–103.
- Wiese, Gabor: Dihedral Galois representations and Katz modular forms. Doc. Math. 9 (2004), 123–133.