Arithmetische Knoten

Alexander Schmidt

Seit April 2013 besteht die DFG-Forschergruppe 1920 mit dem Titel „Symmetrie, Geometrie und Arithmetik“. Beteiligte Wissenschaftler sind W. Kohnen, G. Böckle, A. Schmidt, R. Weissauer und O. Venjakob von der Ruprecht-Karls-Universität Heidelberg sowie J. H. Bruinier von der TU Darmstadt.

Im Rahmen der Forschergruppe werden Fragen der arithmetischen Geometrie untersucht. Das Spektrum der Forschungstätigkeit umfasst Iwasawatheorie, étale Homotopietheorie, automorphe Formen und ihre Deformationen, spezielle Werte von L-Funktionen und vieles mehr. Alle diese Gebiete sind eng miteinander verknüpft.

Ein wesentliches Merkmal der arithmetischen Geometrie ist es, zahlentheoretische Fragestellungen in eine geometrische Gestalt zu bringen, sodass geometrische Intuition und Methoden zum Einsatz kommen können. Dies soll in diesem Artikel am Beispiel arithmetischer Kurven illustriert werden.

1 Étale Homotopiegruppen

Die Homotopiegruppen eines (punktierten) topologischen Raumes X sind definiert als die Mengen der Homotopieklassen stetiger Abbildungen der n-Sphären in den gegebenen Raum:

$$\pi_n(X) = [S^n, X].$$

Diese Mengen tragen für $n \geq 1$ eine natürliche Gruppenstruktur. Räume, die stetig ineinander deformiert werden können, haben isomorphe Homotopiegruppen. Die Gruppe $\pi_n(X)$ ist für $n \geq 2$ abelsch; $\pi_1(X)$, auch Fundamentalgruppe genannt, kann jedoch hochgradig nichtkommutativ sein. Unter milden Annahmen an den Raum X kann sie auch als Symmetriegruppe der universellen Überlagerung $\tilde{X}$ interpretiert werden:

$$\pi_1(X) \cong \mathrm{Aut}_X(\tilde{X}).$$

Eine besondere Rolle spielen asphärische Räume, d.h. solche mit $\pi_n(X) = 0$ für $n \geq 2$. Diese erhält man durch Austeilen der Operation der Fundamentalgruppe aus einem kontrahierbaren Raum. Ein Beispiel ist die Kreislinie S^1, die man aus der reellen Gerade durch Austeilen der Translationswirkung von $\mathbb{Z}$ erhält. Es gilt:

$$\pi_n(S^1) \cong \begin{cases} 0 & n \neq 1, \\ \mathbb{Z} & n = 1. \end{cases}$$

Nach einer Konstruktion, die auf Artin und Mazur [AM69] zurückgeht, kann man auch Objekten der algebraischen Geometrie, den Schemata, Homotopiegruppen zuordnen. Dabei ordnet man einem Schema X zunächst einen (gewöhnlichen) topologischen Raum X_{et} zu. Auf diese recht technische Konstruktion wollen wir in diesem Artikel nicht weiter eingehen – streng genommen ist X_{et} nicht ein einzelner Raum, sondern ein inverses System von Räumen, die man auf kombinatorische Weise aus den étalen Überdeckungen von X erhält. Man definiert dann die étalen Homotopiegruppen des Schemas X durch

$$\pi_n^{\mathrm{et}}(X) = \pi_n(X_{\mathrm{et}}).$$

Wir betrachten dies zunächst im Spezialfall von Körpern: Für einen Körper K ist sein Spektrum $Spec(K)$ der Einpunktraum zusammen mit den Elementen aus K als „holomorphen“ Funktionen. Der topologische Raum $Spec(K)_{\mathrm{et}}$ ist kompliziert, man kann aber zeigen, dass seine höheren Homotopiegruppen (d.h. π_n für $n \geq 2$) verschwinden. Als Fundamentalgruppe begegnen wir einer alten Bekannten, der absoluten Galoisgruppe, also der Automorphismengruppe des separablen Abschlusses $\bar{K}$ von K:

$$\pi_1^{\mathrm{et}}(Spec(K)) \cong \mathrm{Gal}_K = \mathrm{Aut}_K(\bar{K}).$$

Besonders einfach stellt sich dies für den Körper $K = \mathbb{R}$ der reellen Zahlen dar. Der Körper der komplexen Zahlen $\mathbb{C}$ ist ein separabler Abschluss von $\mathbb{R}$ und $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$ ist zyklisch von der Ordnung 2, erzeugt von der komplexen Konjugation. Wir erhalten:

$$\pi_n^{\mathrm{et}}(Spec(\mathbb{R})) \cong \begin{cases} 0 & n \neq 1, \\ \mathbb{Z}/2\mathbb{Z} & n = 1. \end{cases}$$

Für einen endlichen Körper $\mathbb{F}$ gilt:

$$\pi_n^{\mathrm{et}}(Spec(\mathbb{F})) \cong \begin{cases} 0 & n \neq 1, \\ \widehat{\mathbb{Z}} & n = 1. \end{cases}$$

Hier bezeichnet $\widehat{\mathbb{Z}}$ die proendliche Komplettierung der Gruppe $\mathbb{Z}$. Wir sehen eine große Ähnlichkeit zwischen $Spec(\mathbb{F})_{\mathrm{et}}$ und der Kreislinie S^1. Beide Räume sind im kohomologischen Sinne eindimensional und haben (fast) die gleichen Homotopiegruppen.

Auch sehen wir, dass alle endlichen Körper die gleichen Homotopiegruppen haben, durch diese also nicht unterschieden werden können. Bei Zahlkörpern ist dies fundamental anders. Ein inzwischen klassisches Resultat von Neukirch und Uchida [Ne69, Uc76] besagt, dass zwei endliche Erweiterungskörper von $\mathbb{Q}$ mit isomorpher Fundamentalgruppe bereits isomorph sind. Die Fundamentalgruppen von Zahlkörpern sind Untergruppen von endlichem Index in der absoluten Galoisgruppe von $\mathbb{Q}$. Deren Studium ist ein zentrales Anliegen der Arithmetik.

DOI 10.1515/dmvm-2014-0086

2 Beschränkte Verzweigung

Betrachtet man eine Primzahl nicht als rationale Zahl, sondern als Element einer endlichen Körpererweiterung von $\mathbb{Q}$, so bleibt sie im allgemeinen nicht prim. Beispielsweise gilt

$$5 = (2+i)(2-i)$$

im Körper $\mathbb{Q}(i)$ der Gaußschen Zahlen. Es ist bekannt, dass in einer fest gegebenen endlichen Erweiterung von $\mathbb{Q}$ fast alle Primzahlen quadratfrei bleiben. Die endlich vielen Ausnahmeprimzahlen nennt man die Verzweigungsstellen der Erweiterung. Bezeichnet man für eine endliche Primzahlmenge S die maximale Erweiterung von $\mathbb{Q}$, in der höchstens die Primzahlen aus S verzweigen mit $\mathbb{Q}_S$, so gilt daher

$$\overline{\mathbb{Q}} = \bigcup_{S \text{ endlich}} \mathbb{Q}_S.$$

Somit bleibt die volle Information über die absolute Galoisgruppe von $\mathbb{Q}$ in der Familie ihrer Faktorgruppen

$$G_S = \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q}), \quad S \text{ endlich},$$

erhalten. Eine genaue Kenntnis der Gruppen G_S hätte viele zahlentheoretische Anwendungen, unter anderem den Großen Fermatschen Satz. Leider ist unser Wissen über die G_S bis heute noch nicht ausreichend, um den Großen Fermatschen Satz auf diese klassische Weise zu zeigen – Wiles' Beweis geht einen gänzlich anderen Weg.

Im Sinne der Homotopietheorie können die Gruppen G_S als Fundamentalgruppen offener Teilmengen des Schemas $Spec(\mathbb{Z})$ interpretiert werden. Die arithmetische Kurve $Spec(\mathbb{Z})$ entsteht aus $Spec(\mathbb{Q})$ durch Anheften der Räume $Spec(\mathbb{F}_p)$, wobei p alle Primzahlen durchläuft:

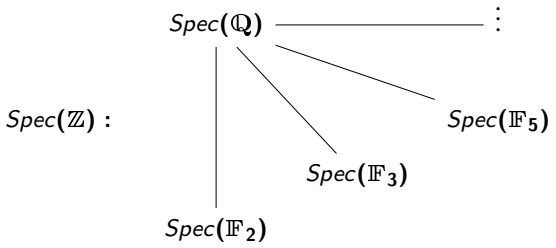

Abbildung 1. *Schematische Darstellung von* $Spec(\mathbb{Z})$

Nimmt man eine Primzahlmenge S aus $Spec(\mathbb{Z})$ heraus, so gilt

$$G_S \cong \pi_1^{\mathrm{et}}(Spec(\mathbb{Z}) \smallsetminus S).$$

Im Fall $S = \emptyset$ besagt ein klassisches Theorem von Minkowski („$\mathbb{Q}$ hat keine unverzweigten Erweiterungen"), dass

$$\pi_1^{\mathrm{et}}(Spec(\mathbb{Z})) = 0$$

gilt. Man kann überdies zeigen, dass die höheren Homotopiegruppen von $Spec(\mathbb{Z})$ 2-Torsionsgruppen sind. Um den 2-Torsionseffekt zu eliminieren, wählen wir eine feste ungerade Primzahl p und betrachten die p-Komplettierung $Spec(\mathbb{Z})^{\wedge p}_{\mathrm{et}}$. Grob gesprochen geht mit dem Prozess der p-Komplettierung alle Information „weg von p" verloren, sodass der Raum im Sinne der Homotopietheorie einfacher wird. In unserer Situation bedeutet dies, dass $Spec(\mathbb{Z})^{\wedge p}_{\mathrm{et}}$ triviale Homotopie hat. Das ändert sich jedoch, wenn man Primzahlen entnimmt. Die Fundamentalgruppen

$$G_S(p) = \pi_1((Spec(\mathbb{Z}) \smallsetminus S)^{\wedge p}_{\mathrm{et}})$$

sind schon seit den 1960er Jahren Objekt intensiver Forschung [Ko70]. Sie könn(t)en wesentlich besser verstanden werden, wenn die höhere Homotopie verschwindet. In diesem Fall stimmt nämlich die Kohomologie der Fundamentalgruppe mit der des Raumes überein und letztere ist besser verstanden.

3 Zahm oder wild

Nachdem wir $Spec(\mathbb{Z})_{\mathrm{et}}$ durch Komplettierung nach einer fest gewählten ungeraden Primzahl p vereinfacht haben, erhält diese natürlich eine Sonderrolle.

Liegt p in S, so ist die Situation vergleichsweise einfach: Es gilt $\pi_n((Spec(\mathbb{Z}) \smallsetminus S)^{\wedge p}_{\mathrm{et}}) = 0$ für $n \geq 2$ [Sc96] und die Fundamentalgruppe hat gute gruppentheoretische Eigenschaften. Insbesondere ist die kohomologische Dimension der Gruppe $G_S(p)$ kleiner gleich 2. Man nennt dies den *wilden* Fall (weil „wilde" Verzweigung zugelassen ist).

Liegt p nicht in S, so spricht man vom *zahmen* Fall. Das Entfernen von Primzahlen $q \not\equiv 1 \bmod p$ aus S ändert nichts an den Homotopiegruppen von $(Spec(\mathbb{Z}) \smallsetminus S)^{\wedge p}_{\mathrm{et}}$, weshalb wir von nun an stillschweigend annehmen werden, dass alle Primzahlen in S kongruent $1 \bmod p$ sind.

Im zahmen Fall war lange Zeit wenig bekannt. Seit 1964 wusste man nach dem Satz von Golod und Shafarevich [GS64] immerhin, dass $G_S(p)$ unendlich ist, sobald S mindestens vier Primzahlen enthält. Aber schon die Frage nach der kohomologischen Dimension der Gruppe $G_S(p)$ war lange offen und ist auch heute noch nicht in voller Allgemeinheit geklärt. Das erste Beispiel überhaupt, in dem $G_S(p)$ im zahmen Fall endliche kohomologische Dimension besitzt, wurde erst im Jahr 2005 gefunden. Dabei wurden Analogien zur Knotentheorie ausgenutzt.

4 Verschlingungsinvarianten

Wir haben gesehen, dass $Spec(\mathbb{Z})^{\wedge p}_{\mathrm{et}}$ triviale Homotopiegruppen hat. Die Dimension dieses Raumes (im kohomologischen Sinne) ist gleich drei. Er hat daher sehr ähnliche Eigenschaften wie der $\mathbb{R}^3$. Wir haben auch gesehen, dass $Spec(\mathbb{F}_q)_{\mathrm{et}}$ für eine Primzahl q sehr ähnlich

zur Kreislinie S^1 ist. Eine im $\mathbb{R}^3$ eingebettete Kreislinie nennt man auch Knoten. Dies führt uns zu dem vagen Bild, dass $(Spec(\mathbb{Z}) \setminus S)^{\wedge p}_{et}$ wie das Komplement endlich vieler disjunkter Knoten im $\mathbb{R}^3$ aussieht. Zwei Knoten im $\mathbb{R}^3$ können sich umeinander verschlingen, oder nicht.

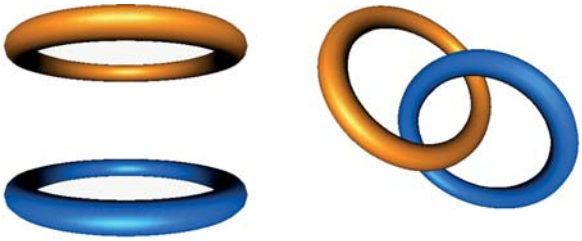

Abbildung 2. *Unverschlungene und verschlungene Knoten*

Wir wollen nun verstehen, was das für zwei Primzahlen (die wir ja nun als Knoten aufzufassen versuchen) bedeuten könnte. Dies geschieht auf dem Umweg über die Homologie. Zunächst kann man die Trivialität der Verschlingungszahl in homologischen Termen ausdrücken. Dies kann dann in die Sprache der Etalkohomologie übersetzt und schließlich wieder in unserer konkreten Situation interpretiert werden. Man erhält die folgende Definition, die zuerst von Labute [La06] betrachtet wurde.

Definition: Seien ℓ und q zwei verschiedene Primzahlen kongruent 1 mod p. *Wir sagen, dass sich q in $Spec(\mathbb{Z})^{\wedge p}_{et}$ um ℓ schlingt, wenn q keine p-te Potenz modulo ℓ ist.*

Für $p = 3$ sehen die ersten Verschlingungsdaten folgendermaßen aus (v bedeutet verschlungen):

Tabelle 1. *Tabelle von Verschlingungsdaten in $Spec(\mathbb{Z})^{\wedge 3}_{et}$*

$q \setminus \ell$	7	13	19	31
7	–	v		v
13		–	v	v
19		v	–	v
31	v			–

Enttäuscht sehen wir, dass unsere geometrische Intuition offenbar unzutreffend war, weil das Diagramm nicht symmetrisch ist. So schlingt sich z. B. die 7 um die 13, die 13 aber nicht um die 7. Nichtsdestotrotz erweist sich dieses Konzept von Verschlingung als sinnvoll. Man definiert einen gerichteten Graphen folgendermaßen:

Definition: Das *Verschlingungsdiagramm* $\Gamma_S(p)$ zu p und S ist der folgende gerichtete Graph:

- Ecken sind die Primzahlen in S.
- Es verläuft eine gerichtete Kante von q nach ℓ, wenn sich q in $Spec(\mathbb{Z})^{\wedge p}_{et}$ um ℓ schlingt.

Beispiel:

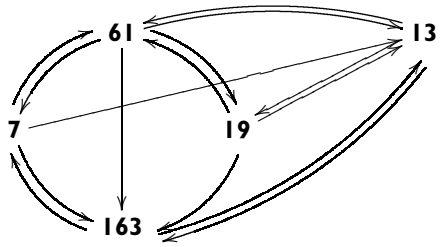

Abbildung 3. *Das Verschlingungsdiagramm für $p = 3$ und $S = \{7, 13, 19, 61, 163\}$*

Definition: $\Gamma_S(p)$ heißt *nichtsingulärer Kreis*, wenn es eine Anordnung $S = \{q_1, \dots, q_n\}$ gibt, sodass gilt:

- Der Kreis $q_1 q_2 \cdots q_n q_1$ liegt in $\Gamma_S(p)$, der inverse Kreis $q_1 q_n \cdots q_2 q_1$ jedoch nicht.
- Für i und j ungerade verläuft keine Kante von q_i nach q_j in $\Gamma_S(p)$.

Insbesondere implizieren diese Bedingungen, dass n gerade und mindestens gleich vier ist. An Abbildung 3 sieht man, dass $\Gamma_{\{7,19,61,163\}}(3)$ ein nichtsingulärer Kreis ist.

Ironischerweise ist es die gerade eben noch als ungünstig angesehene Asymmetrie der Verschlingungsdaten, die die obige Definition erst möglich macht.

5 Asphärizität im zahmen Fall

Bei der Untersuchung der Gruppen $G_S(p)$ hatte man im zahmen Fall seit den 1970er Jahren nur geringe Fortschritte gemacht. Dies änderte sich erst im Jahr 2005, als Labute [La06] eine Verbindung zwischen der Struktur des Verschlingungsdiagramms und der zur Gruppe $G_S(p)$ assoziierten graduierten Liealgebra herstellen konnte. Das folgende Theorem, siehe [Sc06], ist eine Verallgemeinerung seines Resultats.

Theorem: Es sei $p \neq 2$ eine Primzahl und S eine endliche Menge von Primzahlen kongruent 1 *modulo p. Angenommen:*

(i) Es gibt eine Teilmenge $T \subseteq S$, sodass $\Gamma_T(p)$ ein nichtsingulärer Kreis ist.
(ii) Zu jedem $q \in S \setminus T$ existiert ein gerichteter Weg in $\Gamma_S(p)$, der in q beginnt und in $\Gamma_T(p)$ endet.

Dann gilt:

$$\pi_n\big((Spec(\mathbb{Z}) \setminus S)^{\wedge p}_{et}\big) = 0 \quad \text{für } n \geq 2$$

und die Gruppe $G_S(p)$ ist von kohomologischer Dimension 2.

Das Theorem wendet sich z. B. auf den Fall $p = 3$, $S = \{7, 19, 61, 163\}$ an. Dies war überhaupt das erste Beispiel, in dem das Verschwinden der höheren Homotopiegruppen in der zahmen Situation bewiesen werden konnte. Ein weiteres Beispiel ist $p = 3$, $S = \{7, 13, 19, 61, 163\}$ (siehe Abbildung 3). Für eine allgemeine endliche Primzahlmenge S kann man zeigen, dass

MDMV 22/2014 | 218–221

man durch Hinzunahme endlich vieler weiterer Primzahlen kongruent 1 modulo p zu S die Voraussetzungen des Theorems erfüllen kann. Unter den endlichen Primzahlmengen S mit $p \notin S$ liegen daher diejenigen mit $\pi_n((Spec(\mathbb{Z}) \smallsetminus S)^{\wedge p}_{et}) = 0$ für $n \geq 2$ kofinal. Ob die Bedingung (ii) des Theorems unnötig ist oder zumindest die höhere Homotopie ab einer gewissen Größe von S stets verschwindet, ist weiterhin eine offene Frage.

Die Beweismethode kann so weiterentwickelt werden, dass sie sich auch auf allgemeine arithmetische Kurven anwenden lässt. Man kann zeigen, dass auch diese viele asphärische offene Teilräume enthalten [Sc07, Sc10]. Leider verliert man hier die schöne Analogie zur Knotentheorie.

Die Frage nach der Asphärizität höherdimensionaler arithmetischer Schemata ist eines der Themen, die im Rahmen der Forschergruppe untersucht werden.

Literatur

[AM69] M. Artin, B. Mazur, *Etale Homotopy*. Lecture Notes in Mathematics 100, Springer-Verlag 1969

[GS64] E. S. Golod, I. R. Šafarevič, *Über den Klassenkörperturm*. (Russisch), Izv. Akad. Nauk SSSR Ser. Mat. 28 (1964), 261–272

[Ko70] H. Koch, *Galoissche Theorie der p-Erweiterungen*. Mit einem Geleitwort von I. R. Šafarevič. Deutscher Verlag der Wissenschaften, Berlin, 1970

[La06] J. P. Labute, *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbb{Q}$. Reine Angew. Math. 596 (2006), 155–182

[Ne69] J. Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*. Invent. Math. 6 (1969), 296–314

[Sc96] A. Schmidt, *Extensions with restricted ramification and duality for arithmetic schemes*. Compositio Math. 100 (1996), 233–245

[Sc06] A. Schmidt, *Circular sets of prime numbers and p-extensions of the rationals*. J. reine und angew. Math. 596 (2006), 115–130

[Sc07] A. Schmidt, *Rings of integers of type* $K(\pi, 1)$. Doc. Math. 12 (2007), 441–471

[Sc10] A. Schmidt, *Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven*. J. reine u. angew. Math. 640 (2010), 203–235

[Uc76] K. Uchida, *Isomorphisms of Galois groups*. J. Math. Soc. Japan 28 (1976), no. 4, 617–620

Prof. Dr. Alexander Schmidt, Mathematisches Institut, Ruprecht-Karls-Universität Heidelberg, Im Neuenheimer Feld 288, 69120 Heidelberg. schmidt@mathi.uni-heidelberg.de

Alexander Schmidt (geb. 1965) studierte Mathematik an der Humboldt-Universität Berlin. 1993 Promotion und 2000 Habilitation an der Ruprecht-Karls-Universität Heidelberg. Ab 2004 Professor an der Universität Regensburg, seit 2010 an der Universität Heidelberg. Alexander Schmidts Forschungsinteressen liegen in der Arithmetischen Geometrie mit Beziehungen zur Homotopietheorie. Zur Zeit beschäftigt er sich unter anderem mit Höherdimensionaler Klassenkörpertheorie. Er ist Sprecher der DFG-Forschergruppe 1920 „Symmetrie, Geometrie und Arithmetik“ Heidelberg/Darmstadt.