Blockseminar Algebra/Zahlentheorie

Themen

Jun. Prof. Dr. Jeroen Sijsling
Institut für Reine Mathematik
Wintersemester 2019-2020
✉ jeroen.sijsling@uni-ulm.de

Themen

1. Komplexe Tori

Eine erste Beschreibung elliptischer Kurven ist al *komplexe tori*, das heißt, als Quotienten $\mathbb{C}/\Lambda$. Hier ist Λ eine Untergruppe von $\mathbb{C}$, die zu $\mathbb{Z}^2$ isomorph ist, und die $\mathbb{C}$ erzeugt als $\mathbb{R}$-Vektorraum. Diese Menge besitzt ein natürliches Additionsgesetz. Man begegnet ihnen, wenn man versucht, elliptische Integrale $\int \frac{dx}{x(x-1)(x-\lambda)}$ zu berechnen. Die Erklärung dieser Aussage ist das erste Thema des Vortrags.

Darauf werden die meromorphen Funktionen auf $\mathbb{C}/\Lambda$ besprochen. Dies sind genau jene meromorphe Funktionen auf $\mathbb{C}$, die sich nicht ändern unter Translationen in Λ, also Funktionen auf $\mathbb{C}$ mit zwei unabhängigen Perioden. Mithilfe der komplexe Analyse fangen wir an, diese Funktionen zu verstehen.

Quelle: [1, §IV.1-2].

2. Die Weierstrass'sche $\mathfrak{p}$-Funktion

Wir konstruieren jetzt gegeben $\Lambda \subset \mathbb{C}$ eine explizite Λ-periodische Funktion $\mathfrak{p}$, der *die Weierstrass'sche $\mathfrak{p}$-Funktion* genannt wird. Man zeigt, dass alle meromorphe Funktionen auf $\mathbb{C}/\Lambda$ sich als Ausdrücke in $\mathfrak{p}$ und $\mathfrak{p}'$ schreiben lassen. Genauere Betrachtung liefert eine Beziehung der Form $\mathfrak{p}'^2 = 4\mathfrak{p}^3 + g_2\mathfrak{p} + g_3$. Wir nehmen diese später als Motivation unserer Definition einer allgemeinen elliptischen Kurve.

Zuletzt zeigen wir, dass homomorphismen zwischen komplexen Tori induziert werden von linearen Abbildungen $z \to cz$.

Quelle: [1, §IV.3-4].

3. Elliptische Kurven

Motiviert durch die bisherigen Betrachtungen definieren wir jetzt eine elliptische Kurve über einem allgemeinen Körper durch die Gleichung $E : y^2 = x^3 + ax + b$. Wir besprechen, warum sie nach Kegelschnitten die einfachsten algebraischen Kurven sind. Zudem beschreiben wir das algebraische Gruppengesetz (das überraschenderweise sich sehr von der analytischen Version unterscheidet!) und besprechen kurz ihre Zusammenhang mit einem abstrakteren Gruppe, nämlich die *Picard-Gruppe* von E.

Quelle: [2, §I.1-4].

4. Punkte endlicher Ordnung

Jetzt betrachten wir, was die Punkte endlicher Ordnung in der Gruppe gegeben von E sind. Zuerst betrachten wir Punkte von Ordnung 2 und 3; darauf betrachten wir E über $\mathbb{C}$ und verwenden die Ergebnisse der ersten zwei Vorträge, um zu zeigen, dass die n-Torsion in E isomorph mit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ ist. Wir schließen ab mit der Aussage, dass ein Punkt (x, y) endlicher Ordnung auf E die Eigenschaft hat, das y eine bestimmte Invariante von E, nämlich die *Diskriminante*, teilt. Dies wird in der nächsten Vortrag angewendet.

Quelle: [2, §II.1-3].

5. Der Satz von Nagell–Lutz

Dieser Vortrag enthält ein wichtiges Ergbenis, nämlich den Satz von Nagell–Lutz, der die Punkte endlicher Ordnung E^{tors} auf einer elliptischen Kurve E über $\mathbb{Q}$ beschreibt. Der Beweis ist subtil, und sehr schön. Die Punkte unendlicher Ordnung auf E, oder genauer der Quotient E/E^{tors}, sind schwieriger zu beschreiben. Diese Gruppe ist aber endlich erzeugt: das ist der Satz von Mordell–Weil, der in diesem Vortrag kurz beschrieben werden kann.

Quelle: [2, §II.4-5].

6. Isogenien

Wir haben jetzt unsere Objekte (elliptische Kurven) definiert. In diesem Vortrag betrachten wir die Homomorphismen zwischen solchen Kurven, die nicht identisch null sind. Sie heißen *Isogenien*. Wir zeigen, dass die Menge aller solchen Isogenien eine endlich erzeugte abelsche Gruppe bildet, oder anders gesagt, dass die Menge von Abbildungen zwischen zwei gegebenen elliptische Kurven sich relative einfach verstehen lässt. Zudem zeigen wir, dass Isogenien *unverzweigt* sind: sie haben über jedem Punkt die gleiche Anzahl Urbilder. Falls es Zeit gibt, definieren wer die duale Isogenie.

Quelle: [1, §III.4, III.6].

7. Elliptische Kurven über endlichen Körpern

Wir definieren das Tate–Modul einer elliptischen Kurve und verwenden diese für elliptischen Körper über endlichen Körpern, um ihre Anzahl von Punkten zu beschreiben. Der Hauptsatz ist die Hasse-Ungleichung, die behauptet, dass $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$ für eine elliptische Kurve über einem endlichem Körper $\mathbb{F}_q$. Verallgemeinungen dieser Satz werden kurz besprochen.

Quelle: [1, §III.8, §V.1].

8. Die Weil-Vermutungen

Wir beweisen die *Weil-Vermutungen*, die für eine elliptische Kurve über einem endlichem Körper $\mathbb{F}_q$ beschreibt, was ihre Anzahl Punkte ist über jeder Erweiterung $\mathbb{F}_{q^n}$ von $\mathbb{F}_q$. Er ist einer der schönsten Sätze in der algebraischen Geometrie, mit einem elementaren Beweis. Wir besprechen darauf kurz Konsequenzen und alternative Betrachtungsweisen.

Quelle: [1, §V.2].

9. Elliptic Curve Factorization

Sei $N = pq$ ein Produkt zweier Primzahlen. Wir wollen p und q finden. Es existiert ein Algorithmus, der elliptische Kurven zu diesem Zweck verwendet. Er ist eine Verallgemeinerung des $p-1$-*Verfahrens*, der abstrakt betrachten auf Berechnungen in der multiplikativen Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ basiert. Eine Variante von dieser Methode, erfunden von Lenstra, verwendet stattdessen die Gruppen von Punkten auf gut gewählten elliptischen Kurven. Sie ist einer der meist effizienten Methoden, um Zahlen zu zerlegen.

Quelle: [2, §IV.4].

10. Elliptic Curve Primality Testing

Eine Variante vom Thema des letzten Vortrags ist, zu beweisen, dass eine gegebene große Zahl eine Primzahl ist. Auch hier existieren Methoden, die elliptische Kurven verwenden. Es gibt wieder eine Analogie mit $(\mathbb{Z}/p\mathbb{Z})^*$: Jetzt wird das *Pocklington-Verfahren* verallgemeinert.

Quelle: Wird geliefert.

11. Der Mordell–Weil'sche Satz

Sei E eine elliptische Kurve über einem Zahlkörper K. Dann ist die Gruppe $E(K)$ von Punkten auf E mit Koordinaten in K endlich erzeugt. Wir können den Beweis nur Skizzieren: Die Idee, die auf sogenanntem *endlichen Abstieg* basiert, wurde schon von Fermat verwendet, einige dessen Ergebnisse wir zur Illustration "leihen" werden.

Quelle: [1, §VIII.1, VIII.3, VIII.4].

12. Die Vermutung von Szpiro

Genau wie ihre Diskriminante ist der *Führer* eine wichtige Invariante einer elliptischen Kurven. Wir definieren zuerst beide Begriffe. Die Vermutung von Szpiro beschreibt dann eine Beziehung zwischen den beiden. Wir betrachten, wie sie eine andere Aussage in der Zahlentheorie, nämlich die abc-*Vermutung*, impliziert, und besprechen diese letzte Vermutung kurz.

Quelle: [1, §VIII.11].

Literatur

[1] Silverman, *The Arithmetic of Elliptic Curves*

[2] Silverman, Tate, *Rational Points on Elliptic Curves*, second edition.