**Kleine AG**

# Elliptische Kurven mit komplexer Multiplikation

**Sa., 26. Juli 2003, Köln**

In der Klassenkörpertheorie werden die abelschen Galoiserweiterungen eines Zahlkörpers oder eines lokalen Körpers klassifiziert. Insbesondere ergibt sich daraus die Existenz besonders „hübscher" Erweiterungen - die sog. Strahlklassenkörper und als Spezialfall den Hilbertschen Klassenkörper. Ein Nachteil dieser Theorie ist, daß man diese Klassenkörper allgemein nicht explizit hinschreiben kann.

Im Fall der rationalen Zahlen können die Strahlklassenkörper durch zyklotomische Erweiterungen veranschaulicht werden, für beliebige Zahlkörper benutzt man zur Veranschaulichung abelsche Varietäten mit komplexer Multiplikation. Wir werden uns in dieser AG hauptsächlich auf imaginär-quadratische Zahlkörper $K$ bzw. elliptische Kurven mit komplexer Multiplikation, d.h. mit Endomorphismenring isomorph zu $\mathcal{O}_K$ beschränken. Wir werden sehen, daß die $j$-Invariante einer solchen Kurve den Hilbertschen Klassenkörper von $K$ erzeugt und die $\mathfrak{a}$-Teilungspunkte der Kurve die explizite Konstruktion des Strahlklassenkörpers modulo $\mathfrak{a}$ ermöglichen. Die Reziprozitätsabbildung kann ebenfalls mit Hilfe elliptischer Kurven beschrieben werden.

Als Hauptquelle dieser kleinen AG wird [Silv, Chapter II] dienen.

**1. Vortrag: Klassenkörpertheorie**

In diesem Vortrag sollte kurz die Klassenkörpertheorie und die wichtigsten Sätze, die wir für die folgenden Vortäge benötigen, wiederholt werden. Das beinhaltet Artin Reziprozität, sowie den Hilbertschen und die Strahlklassenkörper. Am besten wäre es, sich dabei an [Silv, Chapter II.3] zu orientieren und evtl. Details aus anderen Quellen zu ergänzen, z.B. durch Tate's Artikel in [CaF].

Es könnte auch nicht schaden, noch einmal daran zu erinnern, wie die Theorie im Fall von $\mathbf{Q}$ aussieht (Satz von Kronecker-Weber [Silv, Thm.5.1]).

Dauer: 45 min.

**2. Vortrag: Elliptische Kurven mit komplexer Multiplikation**

In diesem Vortrag soll gezeigt werden, daß jedes gebrochene Ideal $0 \neq \mathfrak{a} \subset K$ eine elliptische Kurve $\mathbf{C}/\mathfrak{a}$ mit komplexer Multiplikation definiert. Die Klassengruppe $\mathrm{Cl}(\mathcal{O}_K)$ operiert transitiv auf der Menge der Isogenieklassen elliptischer Kurven mit komplexer Multiplikation. Dies liefert einen Homomorphismus $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Cl}(\mathcal{O}_K)$.

- Definition und Konstruktion elliptischer Kurven mit komplexer Multiplikation ([Silv, Chapter II.1]), die Operation von $\mathrm{Cl}(\mathcal{O}_K)$ auf der Menge der Isomorphieklassen von elliptischen Kurven mit CM durch $\mathcal{O}_K$ ([Silv, Prop. II.1.2]) ausführlich erklären und evtl. das Beispiel [Silv, Ex. II.1.3.1] angeben.

- Die Struktur der $\mathfrak{a}$-Torsionspunkte, d.h. [Silv, Prop. II.1.4] und [Silv, Cor. II.1.5].

- Kurz die Sätze (ohne Beweis) [Silv, Prop.II.2.1] und [Silv, Thm. II.2.2] skizzieren und die Abschätzung [Silv, Rem. II.2.2.1] angeben.

- Den Homomorphismus $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Cl}(\mathcal{O}_K)$ definieren und [Silv, Prop. II.2.4] zitieren.

Dauer: 60 min.

**3. Vortrag: Der Hilbertsche Klassenkörper**

Ziel dieses Vortrags ist es zu beweisen, daß die $j$-Invariante einer elliptischen Kurve mit komplexer Multiplikation durch $\mathcal{O}_K$ den Hilbertschen Klassenkörper von $K$ erzeugt.

- Beweis von Theorem [Silv, Thm. II.4.3]. Ein wesentlicher Punkt dabei ist Satz [Silv, Prop. II.4.2], dessen Beweis vielleicht nur kurz skizziert werden sollte. Für später benötigen wir dann noch das Lemma [Silv, Lem. II.4.5].

- Für den folgenden Vortrag sind dann noch Satz [Silv, Prop. II.5.3.] (mit Beweis) und das Korollar [Silv, Cor. II.5.4] wichtig.

Dauer: 60 min.

**4. Vortrag: Strahlklassenkörper und der Hauptsatz**

In diesem Vortrag soll bewiesen werden, daß die Strahlklassenkörper einer imaginär-quadratischen Erweiterung $K$ von $\mathbf{Q}$ durch die Torsionspunkte einer elliptischen Kurve $E$ mit Multiplikation von $\mathcal{O}_K$ beschrieben werden. Darüber hinaus soll die Realisierung der Reziprozitätsabbildung für elliptische Kurven erklärt werden.

- Definition von Weberfunktionen mit Beispiel [Silv, Ex. II.5.5.1] und als erstes Hauptresultat [Silv, Thm. II.5.6] (evtl. mit Beweis?) und [Silv, Cor. II.5.7]. Dazu als konkretes Beispiel [Silv, Ex. II.5.8.1].

- Das zweite grosse Ziel ist der Hauptsatz der CM [Silv, Thm. II.8.2] mit soviel Beweis wie möglich.

- Wenn darüber hinaus noch Zeit ist, kann kurz die Anwendung des Hauptsatzes auf L-Reihen erwähnt werden ([Silv, II.9+II.10]).

Dauer: 60 min.

**5. Vortrag: Abelsche Varietäten und CM-Körper**

Dieser Vortrag soll einen Ausblick auf die Theorie der komplexen Multiplikation im Fall von abelschen Varietäten geben. Eine kurze Zusammenfassung der Ergebnisse findet sich in [M, Chapter 9-10], ausführlichere Quellen sind beispielsweise [La, Chapter I+II] und [Sh, Chapter II+IV].

- CM-Körper und CM-Typen ([La, I.2]), Konstruktion von abelschen Varietäten mit CM ([La, I.4]).
- $\mathfrak{a}$-Multiplikation und Konstruktion der universellen Isogenie ([La, III.1+III.2]).
- Definition des Reflexkörpers und der Reflexnorm ([La, I.5]).
- Ziel ist der Hauptsatz [La, Thm. III.6.1].
- Darüber hinaus können auch noch CM-Charaktere und ihre Anwendung ([La, IV.1]) erwähnt werden.

Dauer: 45 min.

## Literatur


[CaF] J. W. S. Cassels, A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press 1969

[La] S. Lang, *Complex Multiplication*, Grundlehren 255, Springer 1983

[M] J. Milne, *Introduction to Shimura Varieties*, http://www.jmilne.org/math, preliminary version, June 2003

[Sh] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press 1998

[Silv] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer 1994