EINFÜHRUNG IN DIE THEORIE DER ELLIPTISCHEN KURVEN (VORLÄUFIGES PROGRAMM)

Dies ist ein vorläufiges Programm für das Seminar. Abhängig von der Anzahl der Teilnehmer und den Vorkenntnissen kann es sich noch ein wenig ändern.

Nachfolgend werden die einzelnen Vorträge kurz beschrieben und ergänzende Literatur vorgeschlagen. Die Referenzen zu [Sil86] sind in den allermeisten Fällen zur weiteren Allgemeinbildung gedacht und für etwas ambitioniertere Teilnehmer. Dies gilt insbesondere, da Vorkenntnisse aus der algebraischen Geometrie angenommen werden. Es wird dringend empfohlen sich mindestens eine Woche vor dem Vortrag mit mir in Verbindung zu setzen.

Die Vorträge 8 und 10 sind nicht notwendig für das weitere Verständnis des Seminars und werden daher wie die letzten Vorträge nur unter Vorbehalt vergeben (nämlich dem, dass sich Vortragende für die anderen Vorträge finden.) Die letzte Sitzung findet am 12.2.2004 statt. Daher kann es theoretisch auch noch einen Vortrag 16 geben, der aber hier noch nicht aufgeführt ist.

Bei manchen Vorträgen ist es gut, wenn sich die Vortragenden unter einander absprechen, so zum Beispiel bei den Vorträgen 6 und 7 und auch bei den letzten Vorträgen.

1. Einführungsvortrag (Sigrid Wortmann, 16.10.2003)

In der ersten Sitzung werden - sofern noch nicht geschehen - die Vorträge vergeben. Zuvor soll in einem kurzen Übersichtsvortrag das Seminarthema vorgestellt werden.

2. Kubische Kurven im affinen und projektiven Raum (23.10.2003)

Kubische Kurven werden in der allgemeinsten Form durch eine Gleichung $ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$ in der affinen Ebene definiert. Die Gleichung heißt rational, falls alle Koeffizienten in $\mathbb{Q}$ sind. Durch Homogenisieren erhält man eine Gleichung im projektiven Raum $\mathbb{P}^2$. Durch projektive Transformationen kann man die Gleichung auf handlichere Formen bringen, beispielsweise die Normalform $y^2 = x^3 + ax^2 + bx + c$ oder die Weierstrass Form $y^2 = 4x^3 - g_2x - g_3$, die aus der Funktionentheorie bekannt ist. Falls die Kurve nicht singulär ist (und einen rationalen Punkt besitzt) nennen wir sie *elliptische Kurve.* ([ST92, I.3, App.A.1-2.2], [Cas91, 6,8], [Sil86, III.1])

3. Das Gruppengesetz (30.10.2003)

Auf einer elliptischen Kurve, genauer auf den K-rationalen Punkten $E(K) = \{(x, y) \in K^2 \mid y^3 = f(x)\}$ (für einen Körper K) läßt sich ein Gruppengesetz definieren. Die Konstruktion ist sehr explizit, aber ihr liegt ein fundamentales Resultat zugrunde, nämlich der Satz von Bezout. Dieser besagt, dass sich eine Kurve vom Grad d_1 und eine Kurve vom Grad d_2 im projektiven Raum genau in d_1d_2 Punkten schneiden. Daher müssen eine elliptische Kurve und eine Gerade sich im *projektiven* Raum in genau drei Punkten schneiden (mit Multiplizitäten

gezählt). Der Beweis dieses Satzes ist nicht möglich, aber zumindest sollte die Aussage erklärt werden. ([ST92, I.4, App.A.3-2.4], [Cas91, 7], [Sil86, III.2])

4. Punkte endlicher Ordnung und der Satz von Nagell-Lutz I (6.11.2003)

Da man auf den Mengen $E(K)$ eine Gruppenstruktur erklärt hat, kann man nach denjenigen Punkten P fragen, für die es ein $m \in \mathbb{Z}$ gibt mit $mP = \mathcal{O}$. Existieren solche Punkte und wenn ja für welche m? Offensichtlich ist die Antwort von der Wahl von K abhängig. In diesem Vortrag soll das Problem für $m = 2, 3$ und $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ dargestellt werden. Im rationalen Fall gibt das Theorem von Mazur (ohne Beweis) eine vollständige Übersicht. ([ST92, II.1-3], [Cas91, 12])

5. Punkte endlicher Ordnung und der Satz von Nagell-Lutz II (13.11.2003)

Der Satz von Nagell-Lutz besteht aus zwei Teilen. Zum einen besagt er, dass ein rationaler Punkt von endlicher Ordnung schon ein ganzer Punkt ist (d.h. in $E(\mathbb{Z})$ liegt) und gibt eine *notwendige* Bedingung für die y-Komponente des Punkte. ([ST92, II.4-5], [Cas91, 12],[Sil86, VIII.7])

6. Der Satz von Mordell-Weil Teil I: Höhen (20.11.2003)

Der Satz von Mordell-Weil (manchmal auch Satz von Mordell oder endlicher Basissatz von Mordell) besagt, dass die Gruppe $E(\mathbb{Q})$ der rationalen Punkte einer elliptischen Kurve endlich erzeugt ist. Ein wichtiges Hilfsmittel sind Höhenfunktionen. Hat man nämlich eine Höhenfunktion mit guten Eigenschaften (diejenigen aus Lemma 1-3), dann folgt der Satz von Mordell-Weil schnell aus dem schwachen Mordell-Weil mithilfe des Descent Theorems. ([ST92, III.1-3], [Cas91, 13,16,17], [Sil86, VIII.3-6])

7. Der Satz von Mordell-Weil Teil II: der schwache Mordell-Weil (27.11.2003)

Nach den Vorarbeiten des letzten Vortrags bleibt der sogenannte schwache Mordell-Weil (der auch als schwacher Basissatz bezeichnet wird) zu zeigen (das ist Lemma 4 in [ST92]). Der entscheidende Schritt ist die Definition einer Abbildung, die in [ST92] als "useful homomorphism" und in [Cas91] als "2-isogeny" bezeichnet wird. ([ST92, III.4-5,],[Cas91, 13-15],[Sil86, VIII.1-3])

8. Mordell-Weil: Anwendungen und Beispiele (4.12.2003)

Der Satz von Mordell-Weil ist theoretischer Natur. Er sagt weder, wie man sich rationale Punkte verschaffen kann, noch gibt er eine Beschränkung des Rangs. Auch weiss man aus dem Beweis, dass die Gruppe $E(\mathbb{Q})/2$ endlich ist, aber man hat keine Aussage über die Ordnung. In diesem Vortrag sollen diese Probleme an Beispielen studiert werden. Eine andere Frage ist, ob man eine analoge Aussage für die nicht-singulären Punkte einer singulären Kurve erhält. Es stellt sich heraus, dass diese Gruppe niemals endlich erzeugt ist. ([ST92, III.6-7])

9. Ganze Punkte kubischer Kurven: Siegels Theorem (11.12.2003)

Der Satz von Siegel, den wir in der angegebenen Allgemeinheit nicht beweisen werden, soll formuliert werden und die Aussage erklärt werden. Insbesondere ist der Satz nicht für lineare oder quadratische Gleichungen richtig. Ramanujans Beobachtung für die Summe zweier Kuben wird durch einen Spezialfall des Satzes von Siegel, dem Satz von Thue, verallgemeinert. Dieser wird aus dem Diophantischen Approximationssatz gefolgert. ([ST92, V.1-3], [Sil86, IX.1])

10. Diophantische Approximation (18.12.2003)

Der Diophantische Approximationssatz, der im letzten Vortrag benutzt wurde, soll bewiesen werden. Dabei muss man wahrscheinlich den angegebenen Beweis geeignet kürzen. Wichtig ist es, die Beweisidee zu verstehen. ([ST92, V.3-7])

11. Elliptische Kurven über endlichen Körpern (8.1.2004)

Analog zu kubischen Kurven über den rationalen Zahlen, kann man kubische Kurven über endlichen Körpern $\mathbb{F}_p$ betrachten und ihre rationalen Punkte (d.h. Lösungen mit Koordinaten in $\mathbb{F}_p$.) Als Spezialfälle hat man diejenigen kubischen Kurven, die sich als Reduktion modulo p einer kubischen Kurve über $\mathbb{Q}$ ergeben. Es gibt eine allgemeine Theorie der Reduktion modulo p von projektiven Kurven, aber im Fall elliptischer Kurven läßt sich auch direkt sehen, dass die Reduktionsabbildung ein Homomorphismus ist. Unter gewissen Voraussetzungen ist dies sogar ein Isomorphismus. ([ST92, IV.1,IV.3,App.A.5], [Cas91, 10,25], [Sil86, V.1-2])

12. Lokal-Global-Prinzip (15.1.2004)

Lokal-Global-Prinzipien (bzw. ihre Ungültigkeit) sind von fundamentaler Bedeutung in der Arithmetischen Geometrie und Zahlentheorie. In diesem Vortrag soll das Lokal-Global-Prinzip für Kegelschnitte erklärt werden. Dazu sollten kurz die p-adischen Körper wiederholt werden. ([Cas91, 2-5])

13. Lokal-Global-Prinzip für elliptische Kurven (22.1.2004)

Für elliptische Kurven kann man kein Lokal-Global-Prinzip zeigen. Dies soll an einem Beispiel, dass auf Selmer zurückgeht gezeigt werden. Die Existenz eines rationalen Punkts hängt dabei mit der Existenz von rationalen Punkten auf gewissen anderen Kurven zusammen. Diese sogenannten Twists sollen dann eingeführt werden. Hierzu wird die absolute Galoisgruppe von $\mathbb{Q}$ benötigt. Je nach Vorkenntnissen der Teilnehmer sollte man dazu noch etwas sagen. ([Cas91, 18-20], [Sil86, X.1-2])

14. Homogene Räume und Galoiskohomologie (29.1.2004)

Zwei Konstruktionen sind zu verstehen. Zum einen (prinzipal) homogene Räume für elliptische Kurven und die erste Galoiskohomologie $H^1(G_{\mathbb{Q}}, E)$ einer elliptischen Kurve. Zwischen beiden Gruppen gibt es eine 1-1-Korrespondenz. ([Cas91, 21-22] ,[Sil86, X.3])

15. Die Tate-Šafarevič-Gruppe (5.2.2004)

Die Weil-Chatelet-, Selmer- und Tate-Šafarevič-Gruppen sollen definiert werden. Wieso beschreibt die letzte Gruppe die Obstruktion zum Lokal-Global-Prinzip? ([Cas91, 23], [Sil86, X.4])

References

[Cas91] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[ST92] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

E-mail address: wortmann@mathi.uni-heidelberg.de

Sigrid Wortmann, Zi.108, INF 288, Tel.06221-544896