Prof. G. Böckle, Dr. J. M. Cerviño 21. Juni 2007

Seminar im SS2007 (Mathematik, Diplom, Lehramt):

Elliptische Kurven

Zeit und Ort: Di 16-18, Raum V15 R02 G76

Anhand von Cassels' Buch *Lectures on Elliptic Curves* will das Seminar eine Einführung in die Theorie der elliptischen Kurven und deren zahlentheoretische Bedeutung geben. Ziel ist es, dass die TeilnehmerInnen selbständig dieses Gebiet anhand des vorgegebenen Texts erarbeiten. Obwohl der Text elementar geschrieben ist, und keine allzugroßen Grundlagen voraussetzt, werden doch viele interessante Themen gestreift, wie z.B. *p-adische Körper*, *lokal-global Prinzipien*, *elliptische Kurven über $\mathbb{Q}$ und über p-adischen Körpern*, *der Satz von Mordell(-Weil)*. In den späteren Kapiteln können auch Kohomologie-Gruppen auftreten. Die Vorträge bauen (i.a.) aufeinander auf.

Je nach Schwierigkeit der Vorträge wird von den TeilnehmerInnen erwartet, dass sie 1-2 Vorträge halten. Zu jedem Vortrag sollte zusätzlich eine (wenigstens) einseitige Ausarbeitung mit den wesentlichen Definitionen und Sätzen kommen. Finden sich nicht genügend TeilnehmerInnen, so werden gegebenefalls auch die Organisatoren einige Vorträge übernehmen.

Mindestvoraussetzung für die Teilnahme sind die Kenntnisse der Linearen Algebra und der Algebra I oder Algebraischen Zahlentheorie.

Bemerkung: Auch wenn das nicht in jedem Vortrag explizit gesagt, wird: Jeder Vortrag sollte mindestens ein sinnvolles **konkretes Beispiel** enthalten.

1 Kurven vom Geschlecht Null

Neben den Beispielen in Cassels' Ch. 1 sollen birationale Abbildungen erläutert werden und eine informelle Einführung in projektive ebene Kurven gegeben werden.

Literatur: [Ca], Ch. 0,1, [ST], §1.1 und App. A.1, A.2

Vortragender: G. Böckle.

2 p-adische Zahlen

Das gesamte Kapitel soll dargestellt werden. Zusätzlich zum Text sollen noch einige Beispiele aus den Aufgaben 1. und 3., S.12 besprochen werden. Außerdem soll die folgende Aussage kurz eräutert werden:
Sei $f(x) \in \mathbb{Z}_p[x]$ normiert und vom Grad $n > 0$ und seien $\alpha, \beta \in \mathbb{Q}_p$ mit $\beta = f(\alpha)$. Dann gilt $|\alpha| > 1 \iff |\beta| > 1$ und in diesem Fall gilt weiter $|\alpha|^n = |\beta|$.

Literatur: [Ca], Ch. 2.

Vortragender: Lars Tennstedt.

3 Das lokal-global Prinzip für ebene Quadriken (ternäre quadratische Formen)

Die Inhalte von Kapitel 3 und 5 sollen möglichst vollständig dargestellt werden. Der Inhalt von Kapitel 4 (Gitterpunktsatz von Minkowski) soll korrekt zitiert werden. Das Wort 'localization' ist mit 'Vervollständigung' zu übersetzen.

Eine zweite Möglichkeit, je nach Geschmack des Vortragenden, das lokal-global Prinzip für ebene Quadriken zu zeigen, wäre es, den ursprünglichen, und im Vergleich zu Cassels', eher arithmetischeren (und auch *schärferen*) Beweis von H. Hasse (s. [Ha]) zu wiederholen. *Schärfer* in dem Sinne, dass er algorithmisch ist und somit für jedes konkrete Beispiel eine explizit berechenbare (nicht triviale) Lösung angibt, wenn es sie gibt. Dies kann man schön an Beispielen zeigen. Dieses Prinzip ist nach ihm als *Hasse-Prinzip* bekannt.

Diesen Vortrag sollte nur halten, wer die Vorlesung Algebraische Zahlentheorie besucht hat.

Literatur: [Ca], Ch. 3-5; oder [Ha, Abschnitt B. Unäre und binäre Formen, S. 134–137, S. 301ff.].

Vortragende: Jasmin Matz.

4 Kubische Kurven (ternäre kubische Formen)

Man präsentiere [Ca], Ch. 6. Dies beinhaltet folgende Aussage: Ist $\mathbf{C}$ eine ebene Kurve, gegeben durch ein homogenes Polynom F vom Grad d, und $\mathbf{G}$ eine Gerade, gegeben durch eine Linearform L, so gilt entweder $L|F$, und in diesem Fall liegt $\mathbf{G}$ in $\mathbf{C}$, oder $\mathbf{C}$ und $\mathbf{G}$ schneiden sich in höchstens d Punkten.

Allgemeiner skizziere man einen Beweis der folgenden schwachen Form des Satzes von Bézout: Seien $\mathbf{C}$ und $\mathbf{C}'$ Kurven vom Grad d und d', gegeben durch homogene Polynome F und G. Sind dann F und G teilerfremd, so schneiden sich $\mathbf{C}$ und $\mathbf{C}'$ in höchstens dd' Punkten, [BK], S.291–295. Zum Beweis zeige man zunächst die grundlegenden Eigenschaften der Resultante zweier Polynome, [Ca], Ch. 16, [Bo], Ch. 4 §6.6 (enthält die einfachsten Beweise), und [BK], S.225ff.

Literatur: [Bo], Ch. 4 §6.6, [BK], S.225ff., S.291ff., [Ca], Ch.6.

Vortragender: Lars Tennstedt.

5 Gruppengesetze auf Nicht-singulären Kubischen Kurven

Sei k ein Körper, $\mathbf{C}$ eine nicht-singuläre kubische Kurve über k und $\mathcal{O}$ ein k-wertiger Punkt auf $\mathbf{C}$. Man zeige, dass die in [Ca], Ch. 7, angegebene 'Addition' eine Gruppenstruktur auf der Menge der k-wertigen Punkte von $\mathbf{C}$ definiert. Zum Beweis der Assoziativität (s. [BK], S.399ff., 314ff.) überlege und verwende man folgende Zwischenresultate:
Seien $\mathbf{C}$ und $\mathbf{C}'$ zwei kubische Kurven, die sich über k^{alg} in höchstens 9 Punkten schneiden und sei $\mathbf{G}$ eine Gerade über einem Körper k. Dann gelten:

(a) Liegt $\mathbf{G}$ weder auf $\mathbf{C}$ noch auf $\mathbf{C}'$ und enthält $\mathbf{G}$ drei der obigen neun Schnittpunkte, so existiert eine Quadrik $\mathbf{Q}$, so dass

$$\mathbf{Q} \cap \mathbf{C} = \mathbf{C}' \cap \mathbf{C} \setminus (\mathbf{G} \cap \mathbf{C}).$$

(b) Enthält eine Quadrik $\mathbf{Q}$ eine Gerade, so ist die die Quadrik definierende Gleichung, das Produkt zweier Linearformen, das heißt $\mathbf{Q}$ ist die Vereinigung zweier Geraden.

Anschließend gebe man Beispiele über $\mathbb{Q}$, über einem endlichen Körper.

Literatur: [BK], S.314ff., S.399ff., [Ca], Ch. 7, [St], S. 23-25, [ST], §1.2 und App. A.4.

Vortragender: Benjamin Otto, 8.5.07

6 Die Weierstrass-Form einer Elliptischen Kurve

In diesem Vortrag kommt zum ersten Mal der Begriff *elliptische Kurve* vor. Für uns wird eine solche (zunächst einmal) eine glatte ebene Kurve mit einer (*algebraischen*) abelschen Gruppenstruktur auf der (nicht leeren) Menge der rationalen Punkten sein. Man definiere die Normalform ("canonical form"), und man zeige jede solche Kurve sei eine elliptische Kurve. Dieses Kapitel bietet einige Beispiele, wie man bestimmte elliptische Kurven in Normalform bringt - enthält aber keinen wirklichen Beweis der Existenz der Normalform für jede elliptische Kurve -. Zumindest sollte man erläutern können wie man von einer ebenen Kurve, die einen Wendepunkt besitzt zur Weierstraßschen Normalform kommen kann.

Literatur: [Ca], Ch. 8, [ST], §1.3 und 1.4.

Vortragender: Nils Schwinning, 15.5.07

7 Additionsgesetze auf singulären Kubischen und elementare Reduktionstheorie

Da die Kurvengleichungen hier sehr explizit sind, sind die hier auftretenden Addtionsgesetze einfacher darzustellen als im nicht-singulären Fall. Bei der Reduktionstheorie soll unbedingt das Hensel'sche Lemma bewiesen werden - weitere Variationen dieses Lemmas sind ebenfalls willkommen! – Es ist eine Verallgemeinerung des Newton-Verfahrens zum finden von Nullstellen von Funktionen reeller Zahlen auf den Fall p-adischer Zahlen.
Man beachte: Bei der Reduktion ergeben sich oft singuläre kubische!

Literatur: [Ca], Ch. 9,10.

Vortragender: Christian Schöler, 22.05.07

8 Die p-adischen Punkte einer Elliptischen Kurve

Zu Beginn sollte man nochmal kurz die elementare Reduktionstheorie, sowie die Additionsgesetze singulärer Kubischer wiederholen. Das zentrale Resultat ist die Defintion eine Filtrierung der Punkte der elliptischen Kurve über $\mathbb{Q}_p$, sowie die daraus resultierenden Folgerungen (Beispiele!).

Literatur: [Ca], Ch. 11, [ST], §2.4.

Vortragender: Andrey Timofeev, 5.6.07

9 Die Gruppe der $\mathbb{Q}$-rationalen Punkte einer Elliptischen Kurve

Die erste Aussage über Torsionspunkte folgt leicht aus den Resultaten des vorangegangenen Vortrags. Anschließend präsentiere man einige Teile von Übungsaufgabe 2, zusammen mit ihrem Beweis.

Im weiteren Stelle man den Satz von Mordell-Weil vor, und erläutere die Strategie zu seinem Beweis. Um den Begriff *Abstieg* zu erläutern zeige man, wie im Text, dass $x^4+y^4 = z^2$ keine nicht-trivialen Lösungen in $\mathbb{Z}$ besitzt.

Literatur: [Ca], Ch. 12, 13, [ST], §2.5.

Vortragender: Benjamin Otto, 12.6.07

10 Die schwache Form des Satzes von Mordell-Weil I

In diesem Vortrag wird unter anderem zum ersten Mal der Funktionenkörper einer elliptischen Kurve betrachtet. Dies ist ein wichtiges Konzept, von dem Cassels im weiteren öfter Gebrauch machen wird. Daher bitte die Bedeutung herausstellen. (Für diesen Vortrag ist Galoistheorie notwendig.)

Literatur: [Ca], Ch. 14, [ST], §3.5.

Vortragender: Lars Adam, um **14-16 Uhr**, am 19.6.07

11 Die schwache Form des Satzes von Mordell-Weil II

Für diesen Vortrag sind gute Algebrakenntnisse notwendig.

Literatur: [Ca], Ch. 15, [ST], §3.5.

Vortragender: Lars Adam, um **16-18 Uhr**, am 19.6.07

12 Höhen und der Beweis des Satzes von Mordell-Weil

Zunächst wiederhole man die wesentlichen Resultate über die Resultante aus Vortrag 4 und ergänze diese falls notwendig. Anschließend sollen Höhen eingeführt werden und der Beweis des Satzes von Mordell gegeben werden.

Literatur: [Ca], Ch. 17, [ST], §3.1-3.

Vortragende: Jasmin Matz, um **14-16 Uhr**, am 26.6.07

13 Pythagoreische Tripel, Kongruenzzahlen und Elliptische Kurven

Dieser Vortrag ist dem Buch [Ko] von Koblitz entnommen. Er unterbricht die Entwicklung der allgemeinen Theorie, um eine konkrete zahlentheoretische Anwendung der Elliptischen Kurven zu geben:

Man stelle das Kongruenzzahl-Problem vor, [Ko], Ch. 1, § 1, und gebe die Umformulierung in Termen von elliptischen Kurven, [Ko], Ch. 1, § 1 und § 2. Anschließend beweise man [Ko], Ch. 1, § 9, Prop 17, 18 und 19. [Nach allem, was wir bisher gelernt haben, sind die Beweise natürlich viel kürzer als in Koblitz' Buch.]

Wenn noch etwas Zeit bleibt, könnte man auch noch das Theorem in [Ko], S. 221 vorstellen. Vielleicht macht das ja Appetit auf mehr?

Literatur: [Ko], Ch. 1 und S. 221.

Vortragender: Christian Schöler, um **16-18 Uhr**, am 26.6.07

14 L-Funktion einer elliptischen Kurve und BSD*-Vermutung

Aus Vortrag 13 haben wir gelernt, wie man anhand der elliptischen Kurve E_n ablesen kann, ob n eine Kongruenzzahl ist oder nicht. Dafür muss man wissen, ob der Rang von E_n über $\mathbb{Q}$ ungleich oder gleich Null ist. Ein Teil der von Birch und Swinnerton-Dyer aufgestellten Vermutung (hier BSD*) besagt für eine elliptische Kurve $E_{/\mathbb{Q}}$, dass der Rang von $E(\mathbb{Q})$ gleich der Ordnung der Polstelle bei $s = 1$ der zu E gehörende L-Funktion $L_E(s)$ ist. Ziel des Vortrages ist es, die L-Funktion einer elliptischen Kurve einzuführen, einen Konvergenzbereich ($\Re(s) > 3/2$) dafür anzugeben und die o.g. und auch die Paritätsvermutung

zu presentieren. Am Ende wäre es schön (mithilfe von Computersoftware, wie SAGE oder Magma oder Pari) ein Paar Ränge ausgerechnet zu sehen (z.B. von Kurven der Form E_n) - Live gerne!
Die benötigte explizite Formel der L-Funktion fuer $\Re(s) > 0$ ist eine Folge der beruehmten Vermutung von Taniyama-Shimura, die basierend auf Wiles' Methode zur Beweis der Fermat-Vermutung bewiesen wurde. Der Beweis der Formel unter Verwendung der Taniyama-Shimura Vermutung ist nicht schwer, würde aber den Rahmen des Seminars sprengen.

Literatur: [WS], §§1.1-1.4.

Vortragender: Nils Schwinning, um **16-18 Uhr**, in **V15 S02 C87**, am 4.07!

Literatur

[BK] E. Brieskorn, H. Knörrer, *Ebene algebraische Kurven*, Birkhäuser 1981.

[Bo] N. Bourbaki, *Elements of Mathematicis, Algebra II, Chapters 4–7*, Springer Verlag 1998.

[Ca] J. W. S. Cassels, *Lectures on Elliptic Curves*, Student Texts **24**, London Mathematical Society, Cambridge University Press, 1992.

[Ha] Helmut Hasse, *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen*, Journal für die reine und angewandte Mathematik, Vol. 152, S. 129–138 (1923);
`http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN243919689_0152`.

[Ko] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics **97**, Springer Verlag, 1984.

[Si] J. H. Silverman, *The Arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, 1992.

[ST] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[WS] W. Stein, *The Birch and Swinnerton-Dyer conjecture, a computational approach*
`http://modular.math.washington.edu/edu/2007/spring/bsd/bsd.pdf`

[St] M. Stoll, *Ellitpische Kurven I*, Vorlesungsskript 2000,
`http://www.faculty.iu-bremen.de/mstoll/vorlesungen/Elliptische-Kurven-SS2000.pdf`