Hauptseminar Algebra (S2A1)
Rationale Punkte auf Elliptischen Kurven

Wintersemester 2023/24

Prof. Dr. D. Huybrechts

Das Seminar richtet sich vor allem an die Hörer der Vorlesung 'Einführung in die Algebra (Galois Theorie)' im Wintersemester 2023/24. Voraussetzung für die Teilnahme am Seminar ist der erfolgreiche Abschluss der Vorlesungen Lineare Algebra I und II.

Grundlage für das Seminar ist das Buch:

J. Silverman, J. Tate: *Rational Points on Elliptic Curves.* Second Edition. Springer. Undergraduate Texts in Mathematics (1992).

welches wir gemeinsam fast vollständig lesen werden. Gelegentlich werden wir theoretischere Teile aus anderen Büchern über elliptische Kurven hinzuziehen (s.u.).

Das Format des Seminars wird etwas anders sein als z.B. beim Seminar S1G1. Von allen Teilnehmenden wird erwartet, dass sie das Buch parallel zum Seminar über das ganze Semester hinweg verfolgen und sich mit dem Stoff beschäftigen. (Das Buch ist vom Charakter mehr ein Lesebuch als ein Seminarbuch.) Es soll weniger um Stoffvermittlung gehen als um die Beschäftigung mit der Materie. Das Seminar soll also vor allem Spaß machen und Interesse wecken. In späteren Semestern werden wir uns mit fortgeschritteneren Themen der (unendlichen) Theorie elliptischer Kurven beschäftigen.

Der Stoff der Vorträge wird in kleinen Gruppen erarbeitet, diskutiert und vorbereitet. Sie können davon ausgehen, dass in Vorbereitung auf die einzelnen Vorträge alle anderen das entsprechende Kapitel ebenfalls gelesen oder zumindest überflogen haben. Die Vorträge werden dann vor allem dazu dienen in die Tiefe zu gehen, Hintergrundinformationen zu liefern, Beispiele zu präsentieren und Lösungen zu Übungsaufgaben vorzustellen. Je mehr Diskussion und Interaktion im Seminar stattfindet, desto besser. Die Vorträge selbst sollten von allen Gruppenmitgliedern bestritten werden (mind. 45 min pro Person).

Programm: Das Programm wird sich im Verlaufe des Seminars noch verändern. Je nach Interesse der Teilnehmer werden wir auf das eine oder andere Thema näher eingehen (oder nicht). Das konkrete Programm für jedes Seminar sollten wir gemeinsam spätestens eine Woche vorher besprechen.

Ganz grob wird eine Gruppe für je eins der Kapitel im Buch verantwortlich sein. Es könnte allerdings sein, dass wir mehr als die angesetzten Termine für die einzelnen Themen benötigen. Das werden wir flexible gestalten.

1. Geometry and arithmetic. 2-3 Termine.
Vorbereitung: Alle haben die Einleitung und Abschnitt 1.1 im Detail gelesen und die anderen Kapitel zumindest überflogen.

– Geometrische Beschreibung der Gruppenstruktur einer kubischen Kurve. Formulieren des Satzes von Mordell (in vager Form): Die rationalen Punkte bilden ein endlich erzeugte abelsche Gruppe. In der Vorlesung werden wir eine Klassifikation solcher Gruppen beweisen. Für die Assoziativität der Gruppenstruktur benutzt man Bézouts Theorem (siehe Seite 10 und Anhang A3).

– Weierstraßschem Normalform: Die Null wird als Punkt im Unendlichen festgelegt, wobei die Gerade im Unendlichen eine 'Tritangente' in O ist. An dieser Stelle bietet es sich an, mehr über den Vergleich zwischen dem 'affinen' Standpunkt (Lösungen $(x, y) \in K^2$ einer kubischen Gleichung $F(x, y)$) und dem 'projektiven' Standpunkt (Lösungen $[x : y : z] \in \mathbb{P}^2$) einer homogenen kubischen Gleichung zu sagen (siehe Anhänge A1 und A2). Die Gleichung $y^2 = f(x)$ definiert genau dann eine elliptische Kurve, falls f keine mehrfachen Nullstellen hat. Details zum Übergang zur WNF findet man im Anhang B oder in einem der angegebenen Bücher (z.B. von Knapp).

– Explizite Formeln mittels Weierstraßscher Normalform. Das Gruppengesetzt wird in dieser Form übersichtlicher, insbesondere die Verdopplungsformel.

Folgende Übungsaufgaben könnten bzw. sollten mit eingearbeitet werden: Exercise 1.16 (erklärt die Beziehung zwischen elliptischen Kurven und Ellipsen, benutzt Exercise 1.15). Exercise 1.19 (Verdopplungsformel, siehe auch Seite 27 und 42). Exercise 1.11 (abstrahiert die Konstruktion der Gruppenstruktur, Exercise 1.10 wird wohl verwendet). Exercise 1.12 & 1.13 (interessante Rechenbeispiele).

Weiterführender fakultativer Stoff: (i) Details zum Satz von Legendre (siehe Seite 7, unten, oder das Buch von Knapp) (ii) Hasses Prinzip (siehe Seite 8). Dazu müsste man etwas über p-adische Zahlen sagen (siehe auch Exercise 2.6). Das wäre auch für Kapitel 2 von Nutzen. Literatur: Serre: *A course in arithmetics* oder eine der vielen anderen Quellen. (Anwendung auf Exercise 1.7?) Hasses Prinzip gilt nicht mehr für kubische Gleichung. Selmers elliptische Kurve auf Seite 11 ist ein berühmtes Gegenbeispiel.

2. Points of finite order. 2 Termine.

– Man könnte mit dem Ende beginnen und als Motivation Mazurs Theorem 2.7 formulieren. Dies beschreibt die möglichen Ordnungen von rationalen Torsionspunkten (wird aber nicht im Buch bewiesen). Das Theorem 2.5 von Nagell und Lutz beschreibt die rationalen Torsionspunkte genauer, ihre Koordinaten sind ganzzahlig! Ziel des Kapitels ist der vollständige Beweis dieses Theorems von Nagell und Lutz und man könnte damit beginnen, als erstes die Strategie in §2.5 zu erklären.

– Überblick über die Beschreibung einer elliptischen Kurve über $\mathbb{C}$ als Torus $\mathbb{C}/(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2)$ mittels der Weierstraßschen $\wp$-Funktion. Hier gibt es eine ganze Reihe von Dingen, die man als blackbox formulieren muss bzw. nur motivieren kann. Für die Konvergenz der Reihen auf Seite 41 siehe Exercise 2.3.

– Explizite Beschreibung der Punkte der Ordnung zwei und drei. Der Unterschied zwischen rationalen, reellen und komplexen Punkten.

– Lemma 2.2 zeigt die Endlichkeit, die zweite Hälfte des Theorems, unter der Voraussetzung der Ganzzahligkeiten der Koordinaten. Eine Verschärfung ist Exercise 2.11.

– Der schwierige Teil des Beweises ist §2.4. Hier muss man die grobe Strategie erklären, also

die Mengen $C(p^n)$ einführen und Proposition 2.3 formulieren und erklären. Der Beweis von Corollary 2.4, welches insbesondere die Ganzzahligkeit beweist, sollte vollständig gebracht werden. Von den Rechnungen vor Proposition 2.3 sollte man sich überzeugen und vielleicht ein typisches Argument vorführen.

– Die konkreten Beispiele auf Seite 57 bilden einen schönen Abschluss für das Kapitel.

Folgende Übungsaufgaben könnten bzw. sollten mit eingearbeitet werden: Exercise 2.1 (um ein Gefühl für abelsche Gruppen zu bekommen). Exercise 2.3 (falls wir Lust auf konvergente Reihen haben). Exercise 2.6 (p-adische Zahlen, eventuell haben wir das schon früher abgehandelt). Jeder sollte eigentlich ein paar Beispiele in Exercise 2.12 machen. Exercise 2.5 machen wir irgendwann auch in der Vorlesung

3. The group of rational points. 3 Termine.

Wir beweisen (fast vollständig) den berühmten Satz von Mordell: Die Gruppe der rationalen Punkte einer elliptischen Kurve ist endlich erzeugt $C(\mathbb{Q}) \cong \mathbb{Z}^{\oplus r} \oplus$ finite group. Der Rang r wird durch die Vermutung von Birch and Swinnerton-Dyer bestimmt, siehe Conjecture 6.24 und Nagell–Lutz sagt insbesondere, dass der Torsionsteil endlich ist. Der Beweis verwendet die Weierstraßscher Normalform sind und viele explizite Rechnungen. Aber wie reduziert man auf den Fall, dass die Koeffizienten a, b, c ganzzahlig sind?

– Der technische Teil des Beweises wird durch Lemma 3.1 (leicht), Lemma 3.2 & 3.3 (beide sehr rechenlastig, wir sollten höchstens eins davon im Detail behandeln) und Lemma 3.4 (konzeptionell interessant, aber aufwendig, siehe §3.4 & §3.5). Das 'descent argument', siehe Theorem 3.5, sollten wir im Detail anschauen. (Im Text wird erähnt, dass Fermats Theorem für $n = 4$ ein ähnliches Argument benutzt. Dies wird im Buch von Knapp ausgeführt.)

– In §3.4 wird der Quotient $C \to \bar{C}$ nach der Untergruppe erzeugt durch einen 2-Torsionspunkt sowohl arithmetisch als auch geometrisch beschrieben. Es lohnt sich, sich dafür Zeit zu nehmen. Der wichtige Satz ist hier Proposition 3.7. In §3.5 wird dann schließlich Lemma 3.4 abschließend bewiesen. Proposition 3.8 wird durch Exercise 3.5 ergänzt.

– In §3.6 wird der Rang diskutiert und in einigen Fällen auch wirklich berechnet. Man siehe auch Exercise 3.6. Hierfür sollten wir uns Zeit nehmen und tatsächlich ein oder zwei der Beispiele konkret berechnen. (Diese Art von Rechnungen haben Birch und Swinnerton-Dyer in den 60er Jahren zu ihrer berühmten Vermutung geführt. Die Rechner waren damals allerdings etwas größer `https://en.wikipedia.org/wiki/EDSAC`)

– Für §3.7 wird uns die Zeit fehlen. Es reicht, wenn an dieser Stelle vermerkt wird, dass Mordell nich für singuläre Kubiken gilt.

Folgende Übungsaufgaben könnten bzw. sollten mit eingearbeitet werden: Exercise 3.7 (zurück zu Nagell–Lutz). Exercise 3.8 (als Ergänzung zu den Beispielen in §3.6 ?). Exercise 3.13 (für Freunde der Gruppentheorie).

4. Cubic curves over finite fields. 2 Termine.

Statt $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$, betrachten wir jetzt endliche Körper (und tatsächlich nur solche von der Form $\mathbb{F}_p$). Prinzipiell läßt es sich in $\mathbb{F}_p$ leichter rechnen. Das Theorem von Hasse und Weil (die beiden waren übrigens keine Freunde) gibt für die Anzahl rationaler Punkte eine obere Schranke: $|C(\mathbb{F}_p) - p - 1| \leqslant 2\sqrt{p}$. Silverman und Tate geben keinen Beweis dieses Resultat, dafür siehe man das Buch von Silverman solo.

Den Einstieg in §4.1 sollte jeder als Vorbereitung lesen. Auch die historischen und weiterführenden Bemerkungen zu Sato–Tate, siehe Theorem 4.3, eignen sich besser fürs Selbststudium. (Falls wir über Sato–Tate sprechen, sollte das anhand von Exercise 4.5 geschehen.) Persönlich finde ich die Abschnitte §4.4 und §4.4 weniger spannend (z.B. als Exercise 4.6) und würde vorschlagen, diese (erst einmal) wegzulassen. (Sollten Sie aber eine Karriere im Geheimdienst anstreben, können wir uns noch umentscheiden.)

– In §4.2 wird eine spezielle elliptische Kurve untersucht: Die Fermat Kurve. Und für diese bewies schon Gauß die Hasse Ungleichung. Für gewisse Primzahlen gilt die viel stärkere Aussage $|C(\mathbb{F}_p)| = p + 1$. (Einheitswurzeln werden auch ein zentrales Thema der Vorlesung sein.)

– Abschnitt §4.3 ist theoretisch wichtig: Wir reduzieren elliptische Kurven über $\mathbb{Q}$ und rationale Punkte (endlicher Ordnung) auf diesen zu $\mathbb{F}_p$. Für die Reduktion wird das Resultat von Nagell und Lutz verwandt und die wichtige Aussage ist, dass die Gruppe aller rationalen Torsionspunkte injektiv nach $C(\mathbb{F}_p)$ abbildet. Die Beispiele sollten wir im Detail besprechen. Die Reduktionsabbildung ist auch für nicht-ganzzahlige Punkte definiert, dort aber nicht mehr injektiv. Das ist der Gegenstand von Exercise 4.12 (ein besseres Verständnis der Reduktionsabbildung erfordert mehr algebraische Geometrie).

Folgende Übungsaufgaben könnten bzw. sollten mit eingearbeitet werden: Exercises 4.1 & 4.2 (als Ergänzung zu §4.2). Exercise 4.12 (siehe oben)

5. Integer points on cubic curves. 1 Termine.

Siegels Theorem sagt, dass jede elliptische Kurve nur endlich viele Punkte mit ganzzahligen Koordinaten hat. In gewisser Weise ist dies eine unvollständige Umkehrung von Nagell–Lutz. Der Beweis dieses Satzes ist nicht elementar.

– §5.2 behandelt einen speziellen Typ elliptischer Kurven: $x^3 + y^3 = m$. Warum diese Gleichungen 'taxicabs' heißen, ist eine klassische Geschichte über Ramanujam (die auch im Film 'The man who knew infinity' erzählt wird).

– §5.3-5.5 behandeln einen bereits wesentlich schwierigeren Fall, nämlich $x^3 + 2y^3 = m$. Hier werden Methoden der diophantischen Approximiation vorgestellt. Aus Zeitgründen lassen wir diesen Teil komplett weg (aber ich bin bereit überstimmt zu werden).

6. Complex multiplication. 1 Termin.

Ich befürchte, dass wir für dieses Kapitel kaum Zeit haben werden. Wir beschänken uns daher erst einmal auf die Abschnitte §6.1 & 6.2. Hier benutzen wir Stoff aus der Vorlesung benutzen (der dann hoffentlich auch schon abgehandelt wurde). Es geht um Körpererweiterungen von $\mathbb{Q}$, also Zahlkörpern, und wie man elliptische Kurven benutzen kann, diese zu produzieren. Proposition 6.1 wird in der Vorlesung bewiesen werden, aber Theorem 6.2 (Kronecker–Weber) nicht. Dieses besagt, dass jede abelsche Galois-Erweiterung in einem Kreisteilungskörper lebt. Im Buch wird ein Beispiel behandelt und das sollten wir uns anschauen. Kroneckers Jugendtraum ist der Wunsch, in ähnlicher Weise alle Zahlkörper behandeln zu können. In §6.2 wird die Analogie zwischen Einheitswurzeln und Torsionspunkten auf elliptischen Kurven diskutiert. Wir lernen, wie man auf diese Weise nicht-abelsche Galois-Erweiterungen produziert.

Wir entscheiden später, wie wir mit dem Rest dieses Kapitel verfahren wollen. (Eine Möglichkeit wäre, dass ich zum Ende des WS oder zum Beginn des SS einen oder zwei Übersichtsvorträge

hierzu halte.)

Notationen: Einige der Notationen sind etwas ungewöhnlich. Wir sollten O für das Nullelement der abelschen Gruppe einer elliptischen Kurve benutzen (statt dem Symbol $\mathcal{O}$, das üblicherweise für etwas ganz anderes steht). Punkte in der projektiven Ebene sollten wir mit $[a : b : c]$ (statt $[a, b, c]$) bezeichnen. An manchen Stellen schreiben die Autoren $\mathbb{Z}_m$ statt $\mathbb{Z}/m\mathbb{Z}$, wir sollten bei der letzteren Bezeichung bleiben.

Organisatorisches:

– Anmeldungen für das Seminar werden ab sofort per email huybrech@math.uni-bonn.de entgegengenommen und bis spätestens 25.8. (mit der Angabe Ihrer Präferenzen für zwei Themen). Sie können sich auch bereits als Zweier- oder Dreiergruppe anmelden.

– Start: 12. Oktober, Time: Donnerstag 14:15-16:00. SR N 0.003.

– Mehrere Exemplare des Buches stehen zur Ausleihe in der Bibliothek. Ein Exemplar steht auf dem Seminarbrett, sollte also immer zur Verfügung stehen.

– Weitere Bücher zum Thema:

A. Knapp: *Elliptic Curves.* Princeton University Press. Mathematical Notes 40 (1993).

N. Koblitz: *Introduction to Elliptic Curves and Modular Forms.* Springer Graduate Texts in Mathematics 97 (1993).

J. Silverman: *The Arithmetic of Elliptic Curves.* Springer Graduate Texts in Mathematics 106 (2009).

L. Washington: *Elliptic Curves.* CRC Press, Taylor & Francis Group (2008).