Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

Elliptische Kurven

Vorlesung 25

Ein Polynom $F(X,Y) \in \mathbb{Z}[X,Y]$ kann man als ein Polynom über jedem Körper auffassen. Zu einem Körper K gibt es einen eindeutig bestimmten Ringhomomorphismus $\mathbb{Z} \to K$ und dieser legt einen Ringhomomorphismus

$$\mathbb{Z}[X,Y] \longrightarrow K[X,Y]$$

und somit ein Polynom $F(X,Y) \in K[X,Y]$ fest. Hierbei werden einfach die Koeffizienten des Polynoms als Elemente in dem Körper K interpretiert. Je nachdem, ob K Charakteristik 0 oder positive Charakteristik p besitzt, liegt eine Faktorisierung

$$\mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow K$$

bzw.

$$\mathbb{Z} \longrightarrow \mathbb{Z}/(p) \longrightarrow K$$

vor, wobei die hintere Abbildung eine Körpererweiterung ist. Somit ist es erst einmal wichtig zu verstehen, was mit F geschieht, wenn man zu den Primkörpern $\mathbb{Q}$ bzw. $\mathbb{Z}/(p)$ übergeht. Im zweiten Fall spricht man davon, das Polynom F (bzw. die Gleichung bzw. die Kurve) modulo p zu betrachten. Ein Extremfall liegt vor, wenn in F alle Koeffizienten Vielfache einer Primzahl p sind, denn dann wird F modulo p zum Nullpolynom. Dies kann nicht passieren, wenn die Koeffizienten zusammen teilerfremd sind. Es ist aber ein typisches Phänom, dass modulo p gewisse Koeffizienten bzw. andere Invarianten des Polynoms zu 0 werden. Da aber eine ganze Zahl nur endlich viele Primteiler besitzt, ist dieses Verhalten ein Ausnahmeverhalten für gewisse Primzahlen. Im Allgemeinen gilt das Prinzip, dass das Verhalten in Charakteristik 0 mit dem Verhalten modulo p für alle Primzahlen bis auf endlich viele Ausnahmen weitgehend übereinstimmt. Statt für alle Primzahlen bis auf endlich viele Ausnahmen spricht man auch von für fast alle Primzahlen oder für hinreichend große Primzahlen. Dabei hängt aber die Ausnahmemenge stets von der in Frage stehenden Eigenschaft ab.

Rationale Punkte und Reduktion

Bisher haben wir elliptische Kurven über einem Körper betrachtet einschließlich der Frage, wie sich Eigenschaften der Kurve (wie der Anzahl der rationalen Punkte) bei einer Körpererweiterung verhalten. In nahezu allen Beispielen waren aber die elliptische Kurven durch eine Gleichung gegeben, deren Koeffizienten in $\mathbb{Z}$ lagen. Eine solche Gleichung definiert einerseits eine elliptische Kurve über $\mathbb{Q}$ und dann über $\mathbb{R}$, $\mathbb{C}$ und über (sämtlichen endlichen oder unendlichen) Körpererweiterungen von $\mathbb{Q}$ und andererseits, wenn man die

Koeffizienten modulo einer Primzahl p auffasst, über den endlichen Körpern $\mathbb{Z}/(p)$ und damit über beliebigen endlichen Körpern. Bei diesem Reduktionsprozess kann für einzelne Primzahlen die Kurve singulär werden, bis auf endlich viele Primzahlen entsteht aber wieder eine glatte Kurve. In dieser Situation kann man Eigenschaften der elliptischen Kurve in Charakteristik 0 mit Eigenschaften der elliptischen Kurven in positiven Charakteristiken in Verbindung bringen.

Eine wichtige Technik für diese Verbindung ist, dass $\mathbb{Q}$-rationale Punkte der Kurve auch $\mathbb{Z}/(p)$-rationale Punkte definieren. Diese Beziehung gilt, wie Lemma 25.1 zeigt, nicht nur für Kurven, sondern für beliebige projektive Varietäten, und nicht nur, wenn die Koeffizienten aus $\mathbb{Z}$ sind, sondern allgemeiner, wenn sie aus einem Dedekindbereich sind.

LEMMA 25.1. *Es sei R ein Dedekindbereich mit Quotientenkörper $Q = Q(R)$ und es sei $\mathfrak{m}$ ein maximales Ideal von R mit Restekörper $K = R/\mathfrak{m}$. Dann gelten folgende Aussagen.*

(1) *Es gibt eine natürliche wohldefinierte Abbildung*

$$\mathbb{P}^n_Q \longrightarrow \mathbb{P}^n_K, (a_0, a_1, \ldots, a_n) \longmapsto (ha_0 \mod \mathfrak{m}, ha_1 \mod \mathfrak{m}, \ldots, ha_n \mod \mathfrak{m}),$$

wobei h so zu wählen ist, dass $ha_i \in R_\mathfrak{m}$ für alle i und eines der ha_i in $R_\mathfrak{m}$ eine Einheit ist.

(2) *Für eine über R definierte projektive Varietät $Y \subseteq \mathbb{P}^n_R$ gibt es eine natürliche Abbildung $Y(Q) \to Y(K)$.*

Beweis. (1) Es sei $(a_0, a_1, \ldots, a_n) \in \mathbb{P}^n_Q$. Durch Multiplikation mit einem Hauptnenner können wir annehmen, dass alle a_i zu R gehören. Diese Multiplikation ändert nicht den projektiven Punkt. Da $R_\mathfrak{m}$ nach Korollar 22.18 (Zahlentheorie (Osnabrück 2016-2017)) ein diskreter Bewertungsring ist, gilt dort mit einer Ortsuniformisierenden $\pi \in R_\mathfrak{m} \subseteq Q$ die Beziehung

$$a_i = \pi^{r_i} u_i$$

mit Einheiten $u_i \in R_\mathfrak{m}$. Es sei r das Minimum der r_i. Wir multiplizieren das Tupel mit π^{-r} und erhalten eine weitere Realisierung des gegebenen Punktes mit der verlangten Eigenschaft (nicht alle Koeffizienten gehören notwendigerweise zu R, aber zu $R_\mathfrak{m}$). Von diesem Tupel kann man koeffizientenweise die Reduktion modulo $\mathfrak{m}$ nehmen. Da ein Koeffizient eine Einheit ist, ist auch die Reduktion eines Koeffizienten eine Einheit und so handelt es sich in der Tat um das homogene Koordinatentupel eines projektiven Punktes über K. Wenn man eine weitere Realisierung des Punktes mit den verlangten Eigenschaften betrachtet, so unterscheiden sich diese um einen Faktor, der eine Einheit in $R_\mathfrak{m}$ und somit in K ist. Daher definieren sie den gleichen projektiven Punkt über K.

(2) Die projektive Varietät Y ist durch homogene Polynome mit Koeffizienten aus R gegeben. Diese Polynome kann man modulo $\mathfrak{m}$ interpretieren. Aus $F(a_0, a_1, \ldots, a_n) = 0$ folgt direkt, wenn die a_i die Bedingungen aus (1) erfüllen und der Überstrich Restklassenbildung bezeichnet,

$$\overline{F(a_0, a_1, \ldots, a_n)} = \overline{F}(\overline{a_0}, \overline{a_1}, \ldots, \overline{a_n}) = 0,$$

also erfüllt der Punkt modulo $\mathfrak{m}$ die entsprechende Gleichung und gehört zu $Y(K)$.

□

Bemerkung 25.2. Im Fall $R = \mathbb{Z}$ kann man die Konstruktion aus Lemma 25.1 einfach dadurch realisieren, dass man zu einem Punkt $(a_0, a_1, \ldots, a_n) \in \mathbb{P}^n_{\mathbb{Q}}$ (bzw. in $Y(\mathbb{Q})$) zu einem teilerfremden Tupel aus $\mathbb{Z}$ übergeht und dann die Reduktion modulo einer Primzahl p bestimmt. Dabei ist das teilerfremde Tupel unabhängig von p.

Beispiel 25.3. Die Aussage Lemma 25.1 gilt nicht, wenn R ein eindimensionaler noetherscher Integritätsbereich ist. Wenn $R \to S$ die Normalisierung ist und über dem maximalen Ideal $\mathfrak{m} \subseteq R$ zwei maximale Ideale $\mathfrak{p}, \mathfrak{q} \subseteq S$ liegen (siehe Beispiel 2.8 für ein konkretes Beispiel), mit $f \in \mathfrak{p}$, $f \notin \mathfrak{q}$ und $f = a/b \in S$ mit $a, b \in R$, so kann man den rationalen Punkt $(a, b) \in \mathbb{P}^1_{Q(R)}$ betrachten. Aufgefasst in $\mathbb{P}^1_{Q(S)}$ ist $(a, b) = (f, 1)$, mit dieser Darstellung kann man direkt die Fortsetzungen in $\mathbb{P}^1_{S/\mathfrak{p}}$ und in $\mathbb{P}^1_{S/\mathfrak{q}}$. Im ersten Fall ist der Wert der Reduktion von f gleich 0, im zweiten Fall $\neq 0$, und so kann es keine wohlbestimmte Fortsetzung nach $\mathbb{P}^1_{R/\mathfrak{m}}$ geben.

Lemma 25.4. *Es sei Y eine projektive Varietät über $\mathbb{Z}$ und es sei*

$$P_1, \ldots, P_m \in Y(\mathbb{Q})$$

eine endliche Punktmenge. Dann sind für hinreichend große Primzahlen p die Punkte $\overline{P}_1, \ldots, \overline{P}_m \in Y_{\mathbb{F}_p}$ alle untereinander verschieden.

Beweis. Wir können direkt mit Lemma 25.1 annehmen, dass Y der projektive Raum $\mathbb{P}^n_{\mathbb{Z}}$ über $\mathbb{Z}$ ist. Ferner können wir jeden Punkt nach Bemerkung 25.2 durch ein teilerfremdes ganzzahliges Tupel repräsentieren, in diesem Fall kann man alle Reduktionen direkt ausrechnen. Die Gleichheit von Punkten $P_i = (a_{i0}, a_{i1}, \ldots, a_{in})$ und $P_j = (a_{j0}, a_{j1}, \ldots, a_{jn})$ kann man über die Minoren testen, siehe Aufgabe 3.3. Zu jedem Punkteindexpaar $1 \leq i < j \leq m$ ist für zumindest ein Koeffizientenindexpaar $0 \leq r < s \leq n$ der Ausdruck $a_{ir}a_{js} - a_{jr}a_{is} \neq 0$. Wenn man p so wählt, dass p kein Teiler von diesen Minoren $\neq 0$ ist, so ergibt sich, dass modulo p die Punkte verschieden bleiben.
□

Korollar 25.5. *Es sei R ein Dedekindbereich und sei $E = V_+(F) \subseteq \mathbb{P}^2_R$ durch ein homogenes Polynom der Form $Y^2Z - X^3 - aXZ^2 - bZ^3$ mit $a, b \in R$ gegeben, das über $Q(R)$ eine elliptische Kurve definiert. Dann liegt für jedes*

maximale Ideal $\mathfrak{m} \subseteq R$*, für das* F *eine elliptische Kurve über* $R/\mathfrak{m}$ *definiert, ein Gruppenhomomorphismus*

$$E(Q(R)) \longrightarrow E(R/\mathfrak{m})$$

vor (wobei jeweils der Punkt $(0,1,0)$ *als neutrales Element genommen wird).*

Beweis. Die Abbildung gibt es aufgrund von Lemma 25.1. Da die Gruppenaddition unter Bezug auf Geraden definiert wird, und da, wieder nach Lemma 25.1, die Eigenschaft, auf einer Geraden zu liegen, unter der Reduktion erhalten bleibt, verträgt sich die Reduktion mit der Gruppenoperation. Dabei ist die Geradengleichung $rX+sY+tZ = 0$ so anzusetzen, dass die Koeffizienten in $R_{\mathfrak{m}}$ teilerfremd sind. □

Bemerkung 25.6. Eine elliptische Kurve über $\mathbb{Q}$ kann man, vorausgesetzt, sie besitzt einen Wendepunkt, nach Lemma 5.3 in einer kurzen Weierstraßform $Y^2 = X^3+aX+b$ mit $a,b \in \mathbb{Z}$ realisieren und erhält so ein Modell der Kurve über $\mathbb{Z}$ und auch für die zugehörigen kubischen Kurven über $\mathbb{Z}/(p)$. Eine Kurve über $\mathbb{Q}$ kann aber durch verschiedene Gleichungen mit ganzzahligen Koeffizienten beschrieben werden, die zu verschiedenen kubischen Kurven über $\mathbb{Z}$ führen. Es ist keineswegs klar, ob und in welchem Sinne es eine optimale Realisierung einer elliptischen Kurve über $\mathbb{Q}$ als eine elliptische Kurve über $\mathbb{Z}$ gibt. Es gibt keine elliptische Kurve über $\mathbb{Z}$, die für jede Primzahl eine glatte Kurve definiert. Ein naheliegender Ansatz ist, dass die realisierende Kurve über $\mathbb{Z}$ für möglichst viele Primzahlen zu einer glatten Kurve führt. Dies ist durchführbar, allerdings darf man sich dabei nicht auf kurze Weierstraßgleichungen beschränken, siehe Aufgabe 25.18. Ein anderer Ansatz, der sich nicht an optimalen kubischen Gleichungen, sondern an der Eigenschaft, überall eine glatte (aber nicht notwendigerweise projektive) Gruppe zu liefern, orientiert, firmiert unter dem Namen *Neron-Modell*.

Kongruente Zahlen und der Rang von elliptischen Kurven

Wir untersuchen weiter den Zusammenhang zwischen kongruenten Zahlen und elliptischen Kurven und knüpfen dabei an Lemma 4.13 und Lemma 4.14 an. Zuerst zeigen wir mit Hilfe der Reduktionstechniken, dass die Torsionsuntergruppen der für die kongruenten Zahlen relevanten elliptischen Kurven minimal sind.

Satz 25.7. *Es sei* $n \in \mathbb{N}_+$ *und sei* E *die durch* $y^2 = x^3 - n^2x$ *gegebene elliptische Kurve über* $\mathbb{Q}$*. Dann ist die Torsionsuntergruppe von* $E(\mathbb{Q})$ *gleich* $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$*.*

Beweis. Die Punkte $(0,0)$, $(n,0)$, $(-n,0)$, $\mathfrak{O}$ sind vier Punkte, die die angegebene Gruppe bilden, siehe Lemma 18.2. Es ist zu zeigen, dass es darüber hinaus keine weiteren Torsionselemente gibt. Nehmen wir an, dass es weitere Torsionspunkte gibt. Dann gibt es ein Torsionselement ungerader Ordnung

oder aber, wenn es kein Torsionselement ungerader Ordnung gibt, ein weiteres Torsionselement, dessen Ordnung eine Zweierpotenz ist. Im ersten Fall besitzt $E(\mathbb{Q})$ eine Untergruppe ungerader Ordnung und im zweiten Fall eine Untergruppe der Ordnung 8. Es sei

$$H = \{P_1, \ldots, P_m\} \subseteq E(\mathbb{Q})$$

diese endliche Untergruppe. Nach Lemma 25.4 und Korollar 25.5 ist für jede hinreichend große Primzahl p die Einschränkung der natürlichen Abbildung

$$E(\mathbb{Q}) \longrightarrow E(\mathbb{Z}/(p))$$

auf H ein injektiver Gruppenhomomorphismus und daher enthält $E(\mathbb{Z}/(p))$ eine zu H isomorphe Untergruppe. Nach Beispiel 23.12 besitzt $E(\mathbb{Z}/(p))$ für

$$p = 3 \mod 4$$

genau $p+1$ Punkte. Für diese Primzahlen muss also m nach Satz 4.16 (Körper- und Galoistheorie (Osnabrück 2018-2019)) ein Teiler von $p+1$ sein, also

$$p = -1 \mod m$$

gelten. Im ersten Fall, also bei m ungerade, führt jede hinreichend große Primzahl, die modulo 4 den Rest 3 und modulo m den Rest 1 besitzt, zu einem Widerspruch. Im zweiten Fall, also bei $m = 8$, führt jede Primzahl

$$p = 3 \mod 8$$

zu einem Widerspruch. Nach dem Satz von Dirichlet über Primzahlen in arithmetischen Progressionen gibt es jeweils unendlich viele Primzahlen mit den geforderten Eigenschaften, so dass sich also stets ein Widerspruch ergibt. □

Bemerkung 25.8. Nach einem Satz von Barry Mazur sind die möglichen Torsionsuntergruppen von elliptischen Kurven, die über $\mathbb{Q}$ definiert sind, bekannt. Es handelt sich um die zyklischen Gruppen $\mathbb{Z}/(n)$ mit $n = 1, 2, \ldots, 10$ oder $n = 12$ und die Produktgruppen $\mathbb{Z}/(2) \times \mathbb{Z}/(2k)$ mit $k = 1, 2, 3, 4$.

Lemma 25.9. *Es sei $n \in \mathbb{N}_+$ und sei E die durch $y^2 = x^3 - n^2x$ gegebene elliptische Kurve über $\mathbb{Q}$. Es sei P ein $\mathbb{Q}$-rationaler Punkt auf E mit $2P \neq \mathfrak{O}$. Dann ist $2P$ ein rationaler Punkt von E mit der Eigenschaft, dass der Nenner der x-Koordinate von $2P$ das Quadrat einer rationalen Zahl ist. In diesem Fall ist n eine kongruente Zahl.*

Beweis. Es sei $P = (x, y)$, nach Voraussetzung ist wegen Lemma 18.2 $y \neq 0$. Nach der Verdoppelungsformel ist die x-Koordinate von $2P$ gleich

$$\begin{aligned} -2x + \left(\frac{3x^2 - n^2}{2y}\right)^2 &= \frac{-8xy^2 + 9x^4 - 6x^2n^2 + n^4}{(2y)^2} \\ &= \frac{-8x(x^3 - n^2x) + 9x^4 - 6x^2n^2 + n^4}{(2y)^2} \end{aligned}$$

$$\begin{aligned} &= \frac{-8x^4 + 8x^2n^2 + 9x^4 - 6x^2n^2 + n^4}{(2y)^2} \\ &= \frac{x^4 + 2x^2n^2 + n^4}{(2y)^2} \\ &= \frac{(x^2 + n^2)^2}{(2y)^2}. \end{aligned}$$

Das Ergebnis folgt somit aus Lemma 4.14. □

SATZ 25.10. *Es sei $n \in \mathbb{N}_+$ und sei E die durch $y^2 = x^3 - n^2x$ gegebene elliptische Kurve über $\mathbb{Q}$. Dann ist n genau dann eine kongruente Zahl, wenn der Rang von $E(\mathbb{Q})$ zumindest 1 ist.*

Beweis. Es sei n eine kongruente Zahl. Nach Lemma 4.13 gibt es einen Punkt auf $E(\mathbb{Q})$, für den die zweite Koordinate definitiv nicht 0 ist. Nach Lemma 18.2 ist es daher kein Torsionspunkt der Ordnung 2 und nach Satz 25.7 kann es sich dabei überhaupt nicht um einen Torsionspunkt der Kurve handeln. Es ist also ein torsionsfreier Punkt und damit ist der Rang zumindest 1.

Wenn $E(\mathbb{Q})$ keine Torsionsgruppe ist, so gibt es insbesondere einen Punkt $P \in E(\mathbb{Q})$ mit $2P \neq \mathfrak{O}$. Nach Lemma 25.9 bedeutet dies, dass n eine kongruente Zahl ist. □

Abbildungsverzeichnis