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

Elliptische Kurven

Vorlesung 23

Elliptische Kurven in positiver Charakteristik

Wir betrachten nun elliptische Kurve über einem endlichen Körper $\mathbb{F}_q$ mit q Elementen. Dabei ist $q = p^e$, wobei p die Charakteristik des Körpers ist, und zu jeder Primzahlpotenz gibt es nach Satz 11.11 (Körper- und Galoistheorie (Osnabrück 2018-2019)) bis auf Isomorphie genau einen Körper. Die Primkörper der Charakteristik p sind die Restklassenkörper $\mathbb{Z}/(p)$. In einem Körper mit p^e Elementen und allgemeiner in jeder $\mathbb{Z}/(p)$-Algebra R gibt es den Frobeniushomomorphismus $R \to R$, der ein Ringhomomorphismus ist, der für viele Fragen in positiver Charakteristik entscheidend ist. In $\mathbb{Z}/(p)$ ist der Frobenius die Identität. Da man häufig über einem Grundkörper arbeiten möchte und dabei die Elemente des Grundkörpers als Konstanten ansehen möchte, ist es sinnvoll, neben dem Frobenius auch die linearen Fortsetzungen des Frobenius zur Verfügung zu haben. Wir erläutern den Unterschied an einem affinen Koordinantering einer elliptischen Kurve E über $\mathbb{Z}/(p)$, die durch eine Gleichung der Form $Y^2 = X^3 + aX + b$ mit $a, b \in \mathbb{Z}/(p)$ gegeben ist. Auf der zugehörigen Algebra

$$R = \mathbb{Z}/(p)[X,Y]/(Y^2 - X^3 - aX - b)$$

bildet der Frobenius alle Koeffizienten, die ja aus $\mathbb{Z}/(p)$ stammen, auf sich selbst ab, und stimmt daher mit dem $\mathbb{Z}/(p)$-linearen Einsetzungshomomorphismus $X \mapsto X^p$, $Y \mapsto Y^p$ überein. Zu einer Körpererweiterung $\mathbb{Z}/(p) \subseteq K$, man denke an $K = \mathbb{F}_{p^e}$ oder an den algebraischen Abschluss $K = \overline{\mathbb{Z}/(p)}$, beschreibt die K-Algebra $R_K = K[X,Y]/(Y^2 - X^3 - aX - b)$ den entsprechenden Ausschnitt aus der elliptischen Kurve E_K. Der Frobenius auf R_K wirkt auf dem erweiterten Koeffizientenbereich K nicht identisch, es liegt also kein K-Algebrahomomorphismus vor. Der K-lineare Frobenius ist nun einfach die K-lineare Fortsetzung des Frobenius von R nach R_K, d.h. es ist der K-lineare Einsetzungshomomorphismus $X \mapsto X^p$, $Y \mapsto Y^p$. Zur Abgrenzung zum linearen Frobenius nennt man den eigentlichen Frobenius auch den absoluten Frobenius.

Diese Konzepte übertragen sich auf eine Varietät V über einem endlichen Körper $\mathbb{F}_q$. Der absolute Frobenius überführt die $\mathbb{F}_q$-rationalen Punkte von V in sich selbst und ist auf jeder Algebra zu einer offenen affinen Teilmenge der Frobeniushomomorphismus. Bei der Fortsetzung auf $V_{\overline{\mathbb{F}_q}}$ ist die $\overline{\mathbb{F}_q}$-lineare Fortsetzung entscheidend, da wir den Morphismusbegriff bezogen auf einen (in der Regel algebraische abgeschlossenen) Grundkörper entwickelt haben.

Siehe auch den sechsten Anhang zu dieser Vorlesung. Da bei einer elliptischen Kurve aber alles bis auf das neutrale Element $\mathfrak{O}$ in einer affinen Menge liegt, kann man einen pragmatischen Standpunkt einnehmen und immer mit dem Einsetzungshomomorphismus und der zugehörigen Punktabbildung $(x,y) \mapsto (x^q, y^q)$ arbeiten.

LEMMA 23.1. *Es sei K ein endlicher Körper mit $q = p^e$ Elementen und C eine projektive Kurve über K. Dann besitzt der e-te absolute Frobenius den Grad q.*

Beweis. Es gibt eine endliche Abbildung

$$\varphi\colon C \longrightarrow \mathbb{P}^1_K$$

(siehe Satz Anhang 13.2 (Singularitätentheorie (Osnabrück 2019)) für die Algebraversion), sagen wir vom Grad d. Das Diagramm

$$\begin{array}{ccc} C & \stackrel{F^e}{\longrightarrow} & C \\ \varphi\downarrow & & \downarrow\varphi \\ \mathbb{P}^1_K & \stackrel{F^e}{\longrightarrow} & \mathbb{P}^1_K \end{array}$$

kommutiert. Entsprechend kommutiert das Diagramm

$$\begin{array}{ccc} Q(C) & \longleftarrow & Q(C) \\ \uparrow & & \uparrow \\ K(T) & \longleftarrow & K(T) \end{array}$$

der Funktionenkörper. Die vertikalen Abbildungen haben den Grad d. Aufgrund der Gradformel genügt es, den Grad des e-ten Frobenius F^e auf dem Körper $K(T)$ zu bestimmen. Dieser ist als K-Algebrahomomorphismus durch $T \mapsto T^q$ gegeben. Unter der Abbildung

$$K[T] \longrightarrow K[T],\, T \longmapsto T^q,$$

ist (das hintere) $K[T]$ eine freie $K[T]$-Algebra mit der Basis $1, T, T^2, \ldots, T^{q-1}$, was sich auf die Quotientenkörper überträgt. Die Dimension von $K(T)$ über $K(T)$ ist also q. □

LEMMA 23.2. *Es sei V eine Varietät über einem Körper K der Charakteristik $p > 0$ und sei $F\colon V \to V$ der absolute Frobenius. Dann gilt $F^*\omega = 0$ für jede Differentialform ω.*

Beweis. Wir können eine affine Situation annehmen mit dem zugehörigen K-Algebra R. Die Erzeuger dx des Kähler-Moduls werden dabei auf $dx^p = px^{p-1}dx = 0$ abgebildet. □

Die vorstehende Aussage gilt ebenso für den K-linearen Frobenius.

LEMMA 23.3. *Es sei E eine elliptische Kurve über dem endlichen Körper $K = \mathbb{F}_q$ mit $q = p^e$ Elementen und es sei*

$$\Phi\colon E_{\overline{K}} \longrightarrow E_{\overline{K}}$$

der e-te $\overline{K}$-lineare Frobenius. Dann ist

$$[m]+n\Phi\colon\ E_{\overline{K}} \longrightarrow E_{\overline{K}}$$

genau dann separabel, wenn m kein Vielfaches von p ist.

Beweis. Unter Verwendung von Satz 16.7, Lemma 16.9 und Lemma 23.2 gilt für jede Differentialform ω die Gleichheit

$$([m]+n\Phi)^*\omega \ = \ m\omega + n\Phi^*\omega \ = \ m\omega.$$

Bei $\omega \neq 0$ ist dies genau dann gleich 0, wenn $m = 0$ ist, was bedeutet, dass m ein Vielfaches von p ist. Es liegt also die Alternative vor, dass bei $m = 0$ in K der Rückzug der Differentialformen die Nullabbildung ist und bei $m \neq 0$ aber surjektiv. Wegen Lemma 19.3 (Algebraische Zahlentheorie (Osnabrück 2020-2021)) entspricht dies den Fällen, dass der relative Kählermodul ungleich oder gleich 0 ist, was nach Satz Anhang 7.10 (Körper- und Galoistheorie (Osnabrück 2018-2019)) die (Nicht-)separabilität der Erweiterung der Funktionenkörper charakterisiert. □

Korollar 23.4. *Es sei E eine elliptische Kurve über dem endlichen Körper $K = \mathbb{F}_q$ mit $q = p^e$ Elementen und es sei*

$$\Phi\colon\ E_{\overline{K}} \longrightarrow E_{\overline{K}}$$

der e-te $\overline{K}$-lineare Frobenius. Dann ist

$$\mathrm{Id}_E -\Phi\colon\ E_{\overline{K}} \longrightarrow E_{\overline{K}}$$

separabel.

Beweis. Dies folgt direkt aus Lemma 23.3. □

Es sei V eine Varietät über einem endlichen Körper $\mathbb{F}_q$, $q = p^e$. Eine grundlegende Idee ist, die Punkte $V(\mathbb{F}_{q^n})$ als Fixpunkte der Morphismen Φ^n aufzufassen, wobei Φ den e-ten absoluten Frobenius bezeichnet.

Lemma 23.5. *Es sei V eine Varietät über einem endlichen Körper $\mathbb{F}_q$, $q = p^e$. Es sei*

$$\Phi\colon\ V_{\overline{\mathbb{F}_q}} \longrightarrow V_{\overline{\mathbb{F}_q}}$$

den $\overline{\mathbb{F}_q}$-lineare Frobenius des absoluten e-ten Frobenius auf V. Dann gilt für einen Punkt $P \in V(\overline{\mathbb{F}_q})$ die Beziehung $\Phi^n(P) = P$ genau dann, wenn P von einem Punkt $P' \in V(\mathbb{F}_{q^n})$ herrührt.

Beweis. Dies kann man auf die affine Situation zurückführen, die Aussage folgt dann aus Lemma Anhang 6.9. □

Lemma 23.6. *Es sei E eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$ mit $q = p^e$ Elementen und es sei*

$$\Phi\colon\ E_{\overline{\mathbb{F}_q}} \longrightarrow E_{\overline{\mathbb{F}_q}}$$

der $\overline{\mathbb{F}_q}$-lineare Frobenius des e-ten absoluten Frobenius auf E. Dann gilt

$$\#\left(E(\mathbb{F}_{q^n})\right) \, = \, \operatorname{Grad}\left(\operatorname{Id}_{E_{\overline{\mathbb{F}_q}}} - \Phi^n\right).$$

Beweis. Wir können die Situation direkt über $\mathbb{F}_{q^n}$ auffassen, d.h. wir können $n = 1$ annehmen. Die Punkte aus $E(\mathbb{F}_q)$ entsprechen nach Lemma 23.5 den Fixpunkten unter Φ auf $\overline{E} = E_{\overline{\mathbb{F}_q}}$. Wegen Lemma 14.3 ist auch

$$\operatorname{Id}_{\overline{E}} - \Phi \colon \overline{E} \longrightarrow \overline{E}$$

eine Isogenie. Die Fixpunkte von Φ auf $\overline{E}$ sind somit der Kern von $\operatorname{Id}_{\overline{E}} - \Phi$ und dieser besteht insbesondere nur aus $\mathbb{F}_{q^n}$-Punkten. Diese Abbildung ist nach Korollar 23.4 separabel und daher ist die Anzahl der Elemente im Kern nach Korollar 15.10 gleich dem Grad von $\operatorname{Id}_{\overline{E}} - \Phi$. □

Beispiel 23.7. WIr betrachten die durch die Gleichung

$$Y^2 \, = \, X^3 + X$$

über dem Körper $\mathbb{Z}/(5)$ gegebene elliptische Kurve E. Wegen

$$h(X) \, = \, X^3 + X \, = \, X(X+2)(X+3)$$

liegt in der Tat Glattheit vor. Die über $\mathbb{Z}/(5)$ definierten Punkte sind

$$\mathfrak{O}, (0,0), (3,0), (2,0)\,,$$

was nach Lemma 18.2 genau die vier Torsionspunkte zur Ordnung 2 sind. Der Frobenius ist durch $X \mapsto X^5$, $Y \mapsto Y^5$ gegeben und besitzt nach Lemma 23.1 den Grad 5, auf der Punktebene ist es die Abbildung

$$\Phi \colon E_{\overline{\mathbb{Z}/(5)}} \longrightarrow E_{\overline{\mathbb{Z}/(5)}}, \, (x,y) \longmapsto (x^5, y^5).$$

Entsprechend wird die Abbildung $\operatorname{Id}_{E_{\overline{\mathbb{Z}/(5)}}} - \Phi$ durch

$$\Phi \colon E_{\overline{\mathbb{Z}/(5)}} \longrightarrow E_{\overline{\mathbb{Z}/(5)}}, \, (x,y) \longmapsto (x,y) - (x^5, y^5),$$

gegeben. Unter Verwendung von Satz 6.5 ist

$$\begin{aligned} (x,y) - (x^5,y^5) &= (x,y) + (x^5, -y^5) \\ &= \left(\alpha^2 - x - x^5, \, -\alpha^3 + \alpha(x + x^5) - y + \alpha x\right) \end{aligned}$$

mit $\alpha = \frac{-y^5 - y}{x^5 - x} = \frac{x^2 + x^6 + x^{10} + 1}{-y^5 + y}$. Nach Lemma 23.6 ist der Grad dieser Abbildung gleich 4. Diese Abbildung stimmt mit der Verdoppelungsabbildung überein, siehe Aufgabe 22.19.

Lemma 23.8. *Es seien E_1 und E_2 elliptische Kurven über einem Körper K. Dann ist der Grad*

$$\operatorname{Hom}_K\left(E_1, E_2\right) \longrightarrow \mathbb{Z}, \, \varphi \longmapsto \operatorname{Grad}\left(\varphi\right),$$

eine positiv definite quadratische Form (hierbei bekommt die konstante Abbildung nach $\mathfrak{O}$ den Grad 0).

Beweis. Die Positivität ist klar, das quadratische Verhalten bei Multiplikation mit n auf E_2 ergibt sich aus Satz 14.2. Im Allgemeinen erfordert dies das Konzept der dualen Isogenie. □

Die Hasse-Schranke

Es sei eine Gleichung der Form

$$y^2 = f(x)$$

mit einem Polynom $f \in K[x]$ über einem endlichen Körper K mit q Elementen gegeben. In einem endlichen Körper der Charakteristik $\neq 2$ besitzt die Hälfte der Einheiten eine Quadratwurzel, siehe Aufgabe 7.11 (Zahlentheorie (Osnabrück 2016-2017)). Wenn f nicht zu speziell ist, so kann man die folgende heuristische Überlegung durchführen. Die Werte $f(x)$, $x \in K$, sind in K „zufällig“ verteilt und daher ist es „gleichwahrscheinlich“, ob ein Quadrat oder ein Nichtquadrat getroffen wird. In Fall eines Nichtquadrats gibt es keine Lösung für y, im Falle eines Quadrats gibt es zwei Lösungen für y. Im „Durchschnitt“ sollte es also zu jedem Element $x \in K$ einen Punkt der Kurve geben. Wenn man den unendlich fernen Punkt mitbedenkt, sollte man $q+1$ Punkte auf der Kurve mit Koordinaten in K erwarten, also

$$\#\left(C(K)\right) \sim q+1.$$

Ohne weitere Bedingung an f gilt dies nicht, wie einfache Beispiele zeigen.

Beispiel 23.9. Bei einer Gleichung der Form

$$y^2 = f(x) = g(x)^2$$

über einem endlichen Körper K mit q Elementen, wo also f ein Quadrat in $K[x]$ ist, kann man die Umformung

$$(y-g(x))(y+g(x)) = 0$$

durchführen. Für x mit $g(x) \neq 0$ gibt es dann zwei Lösungen für y, nämlich $y = \pm g(x)$. Somit ist, wenn g nicht das Nullpolynom ist, die Anzahl der Lösungen der Gleichung (wegen Nullstellen von g) ungefähr gleich $2q$.

Die folgende Aussage heißt die *Hasse-Schranke*.

Satz 23.10. *Es sei E eine elliptische Kurve über einem endlichen Körper mit q Elementen. Dann ist*

$$\left|\#\left(E(K)\right) - q - 1\right| \leq 2\sqrt{q}.$$

Beweis. Es sei F^e der e-te absolute Frobenius $F^e\colon E \to E$ und

$$\Phi\colon E_{\overline{K}} \longrightarrow E_{\overline{K}}$$

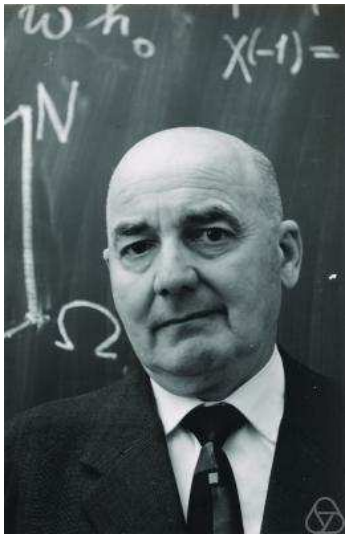
der zugehörige $\overline{K}$-lineare Frobenius. Nach Lemma 23.6 ist

$$\#\left(E(K)\right) = \operatorname{Grad}\left(\mathrm{Id}_{E_{\overline{K}}} - \Phi\right).$$

Nach Satz 22.7 ist die Gradabbildung auf dem Endomorphismenring eine positiv definite quadratische Form. Da die Identität den Grad 1 und Φ nach Lemma 23.1 den Grad q besitzt, gilt mit Satz Anhang 5.5 die Abschätzung

$$\left(\operatorname{Grad}\left(\operatorname{Id}_{E_{\overline{K}}} - \Phi\right)\right) - 1 - q\Big)^2 \leq 4 \cdot 1 \cdot q.$$

Wurzelziehen ergibt die Aussage. □



Helmut Hasse

Beispiel 23.11. Wir betrachten die elliptische Kurve, die durch

$$y^2 = x^3 + 1$$

gegeben ist, für verschiedene endliche Körper der Charakteristik $p \geq 5$.

Es sei $K = \mathbb{Z}/(5)$. Die rechte Seite der Gleichung ist durch

x	0	1	2	3	4
x^3+1	1	2	4	3	0

gegeben. Im Körper mit 5 Elementen besitzen $0, 1, 4$ Quadratwurzeln und daher sind die Lösungen der Gleichung gleich

$$(0,1),\ (0,-1),\ (2,2),\ (2,-2),\ (4,0),\ \mathfrak{O}\,,$$

also 6 Stück, was genau mit $p+1$ übereinstimmt.

Es sei $K = \mathbb{Z}/(7)$. Die rechte Seite der Gleichung ist durch

x	0	1	2	3	4	5	6
x^3+1	1	2	2	0	2	0	0

gegeben. Im Körper mit 7 Elementen besitzen $0, 1, 2, 4$ Quadratwurzeln, es kommen also nur Quadrate in der rechten Seite der Gleichung vor. Daher sind die Lösungen der Gleichung gleich

$$(0,1),\ (0,-1),\ (1,3),\ (1,-3),\ (2,3),\ (2,-3),\ (3,0),\ (4,3),\ (4,-3),\ (5,0),\ (6,0),\ \mathfrak{O},$$

also 12 Stück. Es ist

$$12-8\ =\ 4\ \leq\ 2\sqrt{7}\ \sim\ 5,29,$$

von der Hasse-Schranke her könnte es noch einen Punkt mehr geben, wir sind aber schon relativ nah an der oberen Schranke.

Es sei $K = \mathbb{Z}/(11)$. Die rechte Seite der Gleichung ist durch

x	0	1	2	3	4	5	-5	-4	-3	-2	-1
x^3+1	1	2	-2	-5	-1	5	-3	3	-4	4	0

gegeben. Im Körper mit 11 Elementen besitzen $0, 1, 3, 4, 5, -2$ Quadratwurzeln, es kommen also nur Quadrate in der rechten Seite der Gleichung vor. Daher sind die Lösungen der Gleichung gleich

$$(0,1),\ (0,-1),\ (2,3),\ (2,-3),\ (5,4),\ (5,-4),\ (-4,5),\ (-4,-5),\ (-2,2),\ (-2,-2),\ (-1,0),\ \mathfrak{O},$$

also 12 Stück, was genau mit $p+1$ übereinstimmt. Von der Hasse-Schranke her, die bei kleinen Primzahlen ziemlich grob ist, wäre eine Lösungsanzahl zwischen 6 und 18 denkbar.

Beispiel 23.12. Es sei $n \in \mathbb{N}_+$. Wir betrachten die Gleichung

$$Y^2\ =\ X^3-n^2X\ =\ X(X-n)(X+n)$$

über einem endlichen Körper K mit $q = p^e$ Elementen, wobei die Charakteristik p kein Teiler von $2n$ sei. Nach Beispiel 4.10 definiert dies eine elliptische Kurve.

Es sei $q = 3 \mod 4$. Dann ist die Anzahl der K-Punkte der Kurve gleich $q+1$. Hier ist also der Ausdruck, für den es nach Satz 23.10 eine Schranke gibt, sogar gleich 0. Neben den vier Punkten der Ordnung 2 (vergleiche Lemma 18.2) betrachten wir die Elemente $x \in K \setminus \{0, n, -n\}$. Aufgrund der Bedingung an die Charakteristik sind die herausgenommenen Punkte verschieden und ferner ist $-x \neq x$. Ferner ist $(-x)^3-n^2(-x) = -(x^3-n^2x) \neq x^3-n^2x$. Nach Satz 9.6 (Körper- und Galoistheorie (Osnabrück 2018-2019)) bzw. Aufgabe 17.16 (Algebraische Zahlentheorie (Osnabrück 2020-2021)) ist -1 kein Quadrat in K. Daher ist für jedes Paar $x, -x$ genau eines der beiden Elemente x^3-n^2x oder $(-x)^3-n^2(-x)$ ein Quadrat in K, was dann zu zwei Punkten auf der elliptischen Kurve führt. Dies ergibt $q-3$ Punkte und somit gibt es insgesamt $q+1$ Punkte.

Abbildungsverzeichnis