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

Elliptische Kurven

Vorlesung 18

Torsionsuntergruppen einer elliptischen Kurve

Zu einem Gitter $\Gamma \subseteq \mathbb{C}$ ist die zugehörige elliptische Kurve $\mathbb{C}/\Gamma$ eine Gruppe, die als topologische Gruppe isomorph zu $S^1 \times S^1$. Auf dieser Ebene sind also alle elliptischen Kurven über $\mathbb{C}$ untereinander gleich. Die Gruppenstruktur kann man insbesondere dadurch verstehen, dass man

$$S^1 = \mathbb{R}/\mathbb{Z}$$

versteht. Eine reelle Zahl r definiert in S^1 genau dann das Nullelement, wenn $r \in \mathbb{Z}$ ist. Eine reelle Zahl r definiert in S^1 genau dann ein Torsionselement, wenn $r \in \mathbb{Q}$ ist. Wenn $r = \frac{m}{n}$ eine gekürzte Darstellung ist, dann ist n die Ordnung von $[r]$ in S^1. Wenn die Darstellung nicht notwendigerweise gekürzt ist, so ist n ein Vielfaches der Ordnung. Insbesondere sind zu gegebenem $n \in \mathbb{N}_+$ die verschiedenen Elemente $[\frac{0}{n}], [\frac{1}{n}], [\frac{2}{n}], \ldots, [\frac{n-1}{n}]$ diejenigen Elemente, deren Ordnung ein Vielfaches von n ist. Diese bilden eine Untergruppe der Kreisgruppe, die aus n Elementen besteht, und isomorph zur zyklischen Gruppe $\mathbb{Z}/(n)$ ist.

Lemma 18.1. *Es sei $\Gamma \subseteq \mathbb{C}$ ein Gitter. Dann ist die Torsionsuntergruppe $\mathrm{Tor}_n(\mathbb{C}/\Gamma)$ zur Ordnung n des komplexen Torus $\mathbb{C}/\Gamma$ isomorph zu $\mathbb{Z}/(n) \times \mathbb{Z}/(n)$ und besteht aus n^2 Elementen.*

Beweis. Dies folgt direkt aus $\mathbb{C}/\Gamma \cong S^1 \times S^1$. □

Bei $\Gamma = \langle w_1, w_2 \rangle$ kann man die Torsionsuntergruppe $\mathrm{Tor}_n(\mathbb{C}/\Gamma)$ explizit als $[\frac{i}{n}w_1 + \frac{j}{n}w_2]$, $0 \leq i, j \leq n-1$, angeben.

Wenn eine elliptische Kurve über einem beliebigen Körper K definiert ist, so ist die Menge der K-Punkte eine kommutative Gruppe. Wenn $K \subseteq L$ ein Erweiterungskörper ist, so ist auch die Menge der L-Punkte der Kurve eine kommutative Gruppe, die typischerweise aus mehr Elementen besteht, also

$$E(K) \subseteq E(L).$$

Es gibt im Allgemeinen auch mehr Torsionselement über L als über K.

Lemma 18.2. *Es sei E eine elliptische Kurve über einem Körper K der Charakteristik $\neq 2$ mit der affinen Gleichung $y^2 = h(x)$ mit einem kubischen Polynom $h(x)$ ohne mehrfache Nullstelle. Dann sind die Punkte der Ordnung*

2 *die Punkte* $(a,0,1)$*, wobei* a *die Nullstellen von* h *durchläuft. Insbesondere ist*

$$\#\left(\mathrm{Tor}_2\left(E(K)\right)\right) \leq 4.$$

Bei K *algebraisch abgeschlossen ist* $\mathrm{Tor}_2\left(E(K)\right) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

Beweis. Die Bedingung

$$P + P = \mathfrak{O} = (0,1,0)$$

bedeutet, dass die Tangente durch P durch $\mathfrak{O}$ verläuft. Die Geraden durch $\mathfrak{O}$ sind neben der unendlich fernen Geraden durch die affinen Gleichungen $X = c$ mit einem $c \in K$ gegeben. Die (Richtung der) Tangente zu (a,b) ist nach Bemerkung 2.4 als Kern von $(h'(a), 2b)$ gegeben, also durch die Gleichung $h'(a)X - 2bY = 0$. Übereinstimmung gibt es bei $b = 0$, was wegen der Kurvengleichung erfordert, dass a eine Nullstelle von h ist. □

Satz 18.3. *Es sei* E *eine elliptische Kurve über einem algebraisch abgeschlossenen Körper* K*. Es sei* n *teilerfremd zur Charakteristik von* K*. Dann gilt für die Torsionsuntergruppen zur Ordnung* n *die Isomorphie*

$$\mathrm{Tor}_n\left(E(K)\right) \cong \mathbb{Z}/(n) \times \mathbb{Z}/(n).$$

Ohne die Voraussetzung der Teilerfremdheit gilt

$$\#\left(\mathrm{Tor}_n\left(E(K)\right)\right) \leq n^2.$$

Beweis. Die Abbildung

$$[n]\colon E \longrightarrow E,\ P \longmapsto nP,$$

ist eine Isogenie und besitzt nach Satz 14.2 den Grad n^2. Daher besteht ihr Kern als eine Faser maximal aus n^2 Elementen. Unter der numerischen Bedingung ist die Isogenie nach Korollar 16.10 separabel und daher besteht ihr Kern nach Korollar 15.11 aus n^2 Elementen. Da der Kern eine kommutative n-Torsionsgruppe ist, muss es sich nach Aufgabe 18.6 um $\mathbb{Z}/(n) \times \mathbb{Z}/(n)$ handeln. □

Korollar 18.4. *Es sei* E *eine elliptische Kurve über einem Körper* K*. Dann gilt für die Torsionsuntergruppen zur Ordnung* n *die Abschätzung*

$$\#\left(\mathrm{Tor}_n\left(E(K)\right)\right) \leq n^2.$$

Beweis. Dies folgt aus Satz 18.3, indem man die elliptische Kurve über $\overline{K}$ betrachtet. □

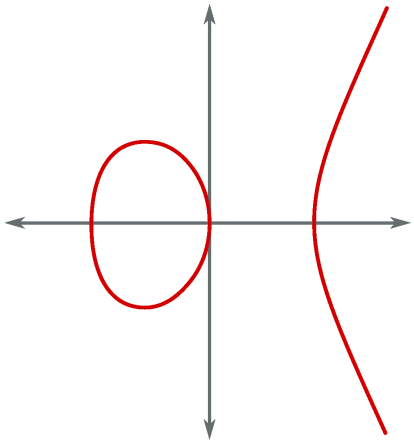
Wenn E über einem Körper K definiert, so muss man zwischen den über K und den über $\overline{K}$ definierten Torsionspunkten unterscheiden. Wir bezeichnen die in einem algebraischen Abschluss von K gewonnenen n-Torsionspunkte mit $E[n]$, also

$$E[n] = \mathrm{Tor}_n\left(E(\overline{K})\right).$$

Beispiel 18.5. Auf der durch $y^2 = x^3 - x$ gegebenen elliptischen Kurve gibt es über $\mathbb{Q}$ nur die vier Punkte $(0,0)$, $(1,0)$, $(-1,0)$, $\mathfrak{O}$, die Torsionspunkte sind. Wenn man die Gleichung über dem Erweiterungskörper $\mathbb{Q}[\mathrm{i}]$ betrachtet, erhält man neue Punkte. So ist $(\mathrm{i}, -1+\mathrm{i})$ ein weiterer Punkt, es ist ja

$$(-1+\mathrm{i})^2 = -2\mathrm{i} = \mathrm{i}^3 - \mathrm{i}.$$

Ferner ergibt sich der Punkt $(-\mathrm{i}, 1+\mathrm{i})$, und zwei weitere Punkte, da man y durch $-y$ ersetzen kann.



Das reelle Bild der Kurve $y^2 = x^3 - x$.

Definition 18.6. Es sei E eine elliptische Kurve über einem Körper K. Dann nennt man den Rang der kommutativen Gruppe $E(K)$ den *Rang* von E.

Beispiel 18.7. Auf der durch $y^2 = x^3 - 2x$ gegebenen elliptischen Kurve gibt es über $\mathbb{Q}$ die beiden Torsionspunkte $(0,0)$, $\mathfrak{O}$. Daneben gibt es noch den Punkt $(-1,1)$, dieser ist kein Torsionspunkt.

Die beiden folgenden elliptische Kurven über $\mathbb{Q}$ besitzen eine vergleichsweise große Torsionsgruppe.

Beispiel 18.8. Auf der durch $y^2 = x^3 + 1$ gegebenen elliptischen Kurve gibt es über $\mathbb{Q}$ die sechs Torsionspunkte $\mathfrak{O}$, $(-1,0)$, $(0,1)$, $(0,-1)$, $(2,3)$, $(2,-3)$. Dabei hat $(-1,0)$ nach Lemma 18.2 die Ordnung 2 und es gibt (über $\mathbb{Q}$ und über $\mathbb{R}$) keinen weiteren Punkt mit Ordnung 2. In Aufgabe 6.3 haben wir gesehen, dass $(0,1)$ und $(0,-1)$ zueinander negative Elemente der Ordnung 3 sind. In Beispiel 6.6 haben wir $(0,1)+(2,3) = (-1,0)$ berechnet. Also ist

$$(2,3) = (-1,0) - (0,1) = (-1,0) + (0,1)$$

und daher besitzen $(2,3)$ und $(2,-3)$ die Ordnung 6.

Beispiel 18.9. Auf der durch $y^2 = x^3 + 4x$ gegebenen elliptischen Kurve gibt es über $\mathbb{Q}$ die vier Torsionspunkte $\mathfrak{O}$, $(0,0)$, $(2,4)$, $(2,-4)$. Dabei besitzt

$(0,0)$ nach Lemma 18.2 die Ordnung 2 und sonst über $\mathbb{Q}$ (und $\mathbb{R}$) keinen weiteren Punkt der Ordnung 2. Die Punkte $(2,4)$ und $(2,-4)$ haben nach Aufgabe 6.5 die Ordung 4.

Der Tate-Modul

Da man bei einer elliptischen Kurve E zwischen den m-Torsionspunkten von $E(K)$ und denen von $E(\overline{K})$ unterscheiden muss, setzen wir

$$E[m] \,=\, \mathrm{Tor}_m\left(E(\overline{K})\right).$$

Da wir die folgende Konstruktion insbesondere auf $E(\overline{K})$, setzen wir für eine kommutative Gruppe G bereits

$$G[m] \,=\, \mathrm{Tor}_m\,(G).$$

Es sei G eine kommutative Gruppe und ℓ eine Primzahl. Die Torsionsuntergruppen $G[\ell^n]$ zur Ordnung ℓ^n stehen zueinander in der Beziehung

$$G[\ell^{n+1}] \longrightarrow G[\ell^n],\, g \longmapsto \ell g,$$

da ja aus

$$\ell^{n+1}g \,=\, \ell^n(\ell g)$$

folgt, dass ein Element der Ordnung ℓ^{n+1} unter Multiplikation mit ℓ auf ein Element der Ordnung ℓ^n abgebildet wird. Es liegt somit ein gerichtetes System

$$G[\ell^{n+1}] \xrightarrow{\cdot\ell} G[\ell^n] \xrightarrow{\cdot\ell} G[\ell^{n-1}] \xrightarrow{\cdot\ell} \ldots \xrightarrow{\cdot\ell} G[\ell^2] \xrightarrow{\cdot\ell} G[\ell^1] \xrightarrow{\cdot\ell} G[\ell^0] = \{0\}$$

vor. Über dieses System kann man den projektiven Limes bilden. Er besteht aus Folgen $(g_n)_{n\in\mathbb{N}}$ mit $g_n \in G[\ell^n]$ und mit $\ell g_{n+1} = g_n$. Diese Konstruktion ergibt eigentlich nur dann Sinn, wenn es zu jedem ℓ^n auch Torsionselemente gibt.

Definition 18.10. Es sei G eine kommutative Gruppe und ℓ eine Primzahl. Unter dem ℓ-adischen *Tate-Modul* von G versteht man die Gruppe

$$T_\ell(G) \,=\, \varprojlim_{n\in\mathbb{N}} G[\ell^n],$$

wobei $G[\ell^n]$ die Torsionsuntergruppe der Ordnung ℓ^n bezeichnet.

Lemma 18.11. *Es seien G und H kommutative Gruppen und sei ℓ eine Primzahl. Dann gelten die folgenden Eigenschaften.*

(1) *Ein Gruppenhomomorphismus $\varphi\colon G \to H$ induziert einen Homomorphismus*

$$\varphi_\ell\colon T_\ell(G) \longrightarrow T_\ell(H)$$

der zugehörigen ℓ-adischen Tate-Moduln.

(2) *Dabei liegt insgesamt ein Gruppenhomomorphismus*

$$\operatorname{Hom}(G,H) \longrightarrow \operatorname{Hom}(T_\ell(G),T_\ell(H)),\ \varphi \longmapsto \varphi_\ell,$$

vor.

(3) *Die Abbildung*

$$\operatorname{End}(G) \longrightarrow \operatorname{End}(T_\ell(G)),\ \varphi \longmapsto \varphi_\ell,$$

ist ein Ringhomomorphismus des Endomorphismenringes von G in den Endomorphismenring des Tate-Moduls.

Beweis. Zu jedem $n \in \mathbb{N}$ liegt ein Gruppenhomomorphismus

$$\varphi\colon\ G[\ell^n] \longrightarrow H[\ell^n]$$

vor. Dabei liegt ein kommutatives Diagramm

$$\begin{array}{ccc} G[\ell^{n+1}] & \stackrel{\cdot\ell}{\longrightarrow} & G[\ell^n] \\ \varphi\downarrow & & \downarrow\varphi \\ H[\ell^{n+1}] & \stackrel{\ell}{\longrightarrow} & H[\ell^n] \end{array}$$

vor. Daher setzen sich die Gruppenhomomorphismen zu einem Homomorphismus zwischen den projektiven Limiten zusammen. □

Nach Aufgabe 18.22 ist der Tate-Modul ein Modul über der Komplettierung $\hat{\mathbb{Z}}_\ell$ von $\mathbb{Z}_{(\ell)}$ und der Homomorphismus aus Lemma 18.11 (1) ist ein $\hat{\mathbb{Z}}_\ell$-Modulhomomorphismus.

Für eine elliptische Kurve über einem Körper K betrachten wir stets den Tate-Modul zur elliptischen Kurve über dem algebraischen Abschluss von K.

Definition 18.12. Zu einer elliptischen Kurve über einem Körper K und einer Primzahl ℓ versteht man unter dem ℓ-adischen *Tate-Modul* den projektiven Limes

$$T_\ell(E) \ = \ \varprojlim_{n\in\mathbb{N}} E[\ell^n] \ = \ \varprojlim_{n\in\mathbb{N}} \operatorname{Tor}_{\ell^n}\left(E(\overline{K})\right).$$

Man bezeichnet hier die Primzahl mit ℓ, da sie zumeist verschieden von der Charakteristik des Körpers gewählt wird. Wenn ℓ nicht die Charakteristik ist, so ist

$$E[\ell^n] \ \cong \ \mathbb{Z}/(\ell^n) \times \mathbb{Z}/(\ell^n)$$

nach Satz 18.3. Unter den natürlichen Abbildungen

$$\ell\colon\ E[\ell^{n+1}] \cong \mathbb{Z}/(\ell^{n+1}) \times \mathbb{Z}/(\ell^{n+1}) \longrightarrow E[\ell^n] \cong \mathbb{Z}/(\ell^n) \times \mathbb{Z}/(\ell^n)$$

wird ein Erzeugerpaar auf ein Erzeugerpaar abgebildet. Man kann also die gerichtete Familie identifizieren mit der zweifach genommenen Restklassenfamilie

$$\longrightarrow \mathbb{Z}/(\ell^3) \longrightarrow \mathbb{Z}/(\ell^2) \longrightarrow \mathbb{Z}/(\ell) \longrightarrow 0\,,$$

wobei die Homomorphismen in der Restklassenfamilie einfach die Restklassenringhomomorphismen sind. Der zugehörige projektive Limes ist nach Definition die ℓ-adische Komplettierung des lokalen Ringes $\mathbb{Z}_{(\ell)}$ am maximalen Ideal (ℓ). Diese wird mit $\hat{\mathbb{Z}}_\ell$ bezeichnet. Daher gibt es eine nichtkanonische Isomorphie

$$T_\ell(E) \cong \hat{\mathbb{Z}}_\ell \times \hat{\mathbb{Z}}_\ell.$$

Im Fall eines komplexen Torus $\mathbb{C}/\Gamma$ zu einem komplexen Gitter $\Gamma \subseteq \mathbb{C}$ gibt es aber eine kanonische Isomorphie

$$T_\ell(E) \cong \varprojlim_{n\in\mathbb{N}} \Gamma/\ell^n\Gamma,$$

also zur Vervollständigung des Gitters bezüglich der Untergruppen $\ell^n\Gamma$, $n \in \mathbb{N}$, siehe Aufgabe 18.12 und Aufgabe 18.25. Da das Gitter aufgrund von Satz 8.11 die Fundamentalgruppe und die erste Homologiegruppe des Torus ist, sollte man die Tate-Moduln als (ℓ-adische) Versionen der ersten Homologie der elliptischen Kurve ansehen.

Satz 18.13. *Es seien E_1 und E_2 elliptische Kurven über einem Körper K und sei ℓ eine Primzahl. Dann gelten folgende Eigenschaften.*

(1) *Eine Isogenie*

$$\varphi\colon E_1 \longrightarrow E_2$$

definiert einen Gruppenhomomorphismus

$$\varphi_\ell\colon T_\ell(E_1) \longrightarrow T_\ell(E_2).$$

(2) *Dabei liegt insgesamt ein Gruppenhomomorphismus*

$$\operatorname{Hom}_K(E_1, E_2) \longrightarrow \operatorname{Hom}(T_\ell(E_1), T_\ell(E_2)),\ \varphi \longmapsto \varphi_\ell,$$

vor.

(3) *Die Abbildung*

$$\operatorname{End}_K(E) \longrightarrow \operatorname{End}(T_\ell(E)),\ \varphi \longmapsto \varphi_\ell,$$

ist ein Ringhomomorphismus des Endomorphismenringes einer elliptischen Kurve in den Endomorphismenring des Tate-Moduls.

Beweis. Dies folgt direkt aus Lemma 18.11. □

Die Multiplikation mit m auf der elliptischen Kurve E definiert die Multiplikation mit m auf

$$E[\ell^n] \cong \mathbb{Z}/(\ell^n) \times \mathbb{Z}/(\ell^n).$$

Wenn m ein Vielfaches von ℓ^n ist, so handelt es sich um die Nullabbildung. Für n hinreichend groß ist dies aber ausgeschlossen und somit induziert die Multiplikation auf dem Tate-Modul $T_\ell(E)$ die Multiplikation mit m. Deren Determinante ist m^2 und stimmt mit dem Grad der Multiplikation überein. Dieser Sachverhalt gilt für sämtliche Isogenien, was wir ohne Beweis mitteilen. Für den Fall einer elliptischen Kurve über $\mathbb{C}$ siehe Aufgabe 18.28.

Satz 18.14. *Es sei E eine elliptische Kurve über dem Körper K, es sei*

$$\varphi\colon E \longrightarrow E$$

eine Isogenie und es sei ℓ eine von der Charakteristik von K verschiedene Primzahl. Es sei

$$\varphi_\ell\colon T_\ell(E) \longrightarrow T_\ell(E)$$

die induzierte $\mathbb{Z}_\ell$-lineare Abbildung auf dem ℓ-adischen Tate-Modul. Dann gelten die folgenden Aussagen.

(1) *Es ist*
$$\det(\varphi_\ell) = \operatorname{Grad}(\varphi).$$
(2) *Es ist*
$$\operatorname{Spur}(\varphi_\ell) = 1 + \operatorname{Grad}(\varphi) - \operatorname{Grad}(\operatorname{Id}_E - \varphi).$$
(3) *Das charakteristische Polynom von φ_ℓ ist*
$$T^2 - (1 + \operatorname{Grad}(\varphi) - \operatorname{Grad}(\operatorname{Id}_E - \varphi))T + \operatorname{Grad}(\varphi).$$

Es ist zu betonen, dass die Daten der linearen Algebra unabhängig von ℓ sind und dass sie in $\mathbb{Z}$ liegen.

Satz 18.15. *Es sei K ein Körper, $K \subseteq \overline{K}$ ein algebraischer Abschluss von K und E eine elliptische Kurve über K. Es sei $G_{\overline{K}|K}$ die absolute Galoisgruppe von K und sei ℓ eine Primzahl. Dann gibt es einen natürlichen Gruppenhomomorphismus*

$$G_{\overline{K}|K} \longrightarrow \operatorname{Aut} T_\ell(E),\ \sigma \longmapsto \big((P_n)_{n\in\mathbb{N}} \mapsto (\sigma(P_n))_{n\in\mathbb{N}}\big).$$

Beweis. Es sei $\sigma\colon \overline{K} \to \overline{K}$ ein Element der absoluten Galoisgruppe, also ein K-Algebraautomorphismus. Dieser induziert einen Automorphismus

$$E(\overline{K}) \longrightarrow E(\overline{K}),\ P \longmapsto \sigma(P),$$

wobei einfach $P = (x,y,z)$ auf $\sigma(P) = (\sigma(x),\sigma(y),\sigma(z))$ abgebildet wird. Dieser Automorphismus ist mit der Addition auf der elliptischen Kurve verträglich, da die Addition durch Polynome aus K definiert ist, und somit induziert σ einen Gruppenautomorphismus auf $E[\ell^n]$. Dabei liegen kommutative Diagramme

$$\begin{array}{ccc} E[\ell^{n+1}] & \xrightarrow{\cdot\ell} & E[\ell^n] \\ \sigma\downarrow & & \downarrow\sigma \\ E[\ell^{n+1}] & \xrightarrow{\ell} & E[\ell^n] \end{array}$$

vor und somit führt dies zu einem Automorphismus auf dem Tate-Modul. Die Gesamtzuordnung ist ein Gruppenhomomorphismus, da ja jeweils die Automorphismen hintereinandergeschaltet werden. □

Abbildungsverzeichnis