Die Struktur der Torsionsgruppe

Alle Bezeichnungen seien wie in der letzten Vorlesung.

Da eine Isogenie insbesondere ein Gruppenhomomorphismus ist, können wir von ihrem Kern sprechen als der Menge aller Punkte, die auf O abgebildet werden. Dabei müssen wir allerdings festlegen, welche Punkte wir betrachten: Nur die mit Koordinaten in k, oder auch solche mit Koordinaten in K? Da die Gruppe $E[n]$ als Untergruppe von $E(K)$ definiert ist, treffen wir die letztere Wahl und definieren

Definition: *a)* Der Kern einer Isogenie $\varphi\colon E_1 \to E_2$ ist

$$\operatorname{Kern}\varphi = \left\{ P \in E_1(K) \;\middle|\; \varphi(P) = O \in E_2(K) \right\}.$$

b) Der Grad $\deg\varphi$ von φ ist $\varepsilon_\varphi \cdot \#\operatorname{Kern}\varphi$, wobei $\#\operatorname{Kern}\varphi$ die Anzahl der Elemente im Kern bezeichnet.

Lemma: Sind $\varphi\colon E_1 \to E_2$ und $\psi\colon E_2 \to E_3$ zwei Isogenien, so ist $\deg(\psi\circ\varphi) = \deg\varphi \cdot \deg\psi$.

Beweis: Ein Punkt $P \in E_1(K)$ liegt genau dann im Kern von $\psi\circ\varphi$, wenn $\varphi(P) \in E_2(K)$ in Kern von ψ liegt. Jedes Element dieses Kerns hat gleich viele Urbilder in $E_1(K)$, also $\#\operatorname{Kern}\varphi$ Stück, so daß $\#\operatorname{Kern}(\psi\circ\varphi) = \#\operatorname{Kern}\psi \cdot \#\operatorname{Kern}\varphi$ ist. Da nach einem Lemma aus der letzten Vorlesung auch $\varepsilon_{\varphi\circ\psi} = \varepsilon_\varphi \cdot \epsilon_\psi$ ist, folgt die Behauptung. ∎

Die Isogenien, die uns im Zusammenhang mit Torsionspunkten interessieren, sind natürlich die Isogenien $[n]\colon E \to E$, die einen Punkt P auf sein n-faches nP abbilden. Wie wir im Zusammenhang mit dem Algorithmus von MONTGOMERY gesehen haben, gibt es rationale Funktionen $r_n, s_n \in k(x)$, derart, daß für einen affinen Punkt $P = (x, y)$ gilt

$$nP = \big(r_n(x), y s_n(x)\big).$$

Dabei ist natürlich $r_1(x) = x$ und $s_1(x) = 1$. Für $n = 2$ führt die Verdoppelungsformel auf

$$r_2(x) = \frac{3x^2 + a^2}{4(x^3 + ax + b)} - 2x = \frac{F'(x)^2}{4F(x)} - 2$$

$$s_2(x) = -\frac{F'(x)^2}{2F(x)}\big(r_2(x) - xi\big) - 1 = -\frac{F'(x)}{2F(x)}\left(\frac{F'(x)^2}{4F(x)} - 3x\right) - 1$$

wobei $F(x) = x^3 + ax + b$ die rechte Seite der WEIERSTRASS-Gleichung bezeichnet.

Um r_{n+1} und s_{n+1} rekursiv aus r_n und s_n berechnen zu können, betrachten wir die Funktionen $\lambda_n \in k(x)$ mit

$$\lambda_n(x) = \frac{s_n(x) -}{r_n(x) - x}\,.$$

Das Quadrat des Produkts $y\lambda_n \in k(E)$ ist

$$y^2\lambda_n(x,y)^2 = y^2\frac{s_n(x) - 1}{r_n(x) - x} = F(x)\left(\frac{s_n - 1}{r_n - x}\right)^i 2\,,$$

liegt also in $k(x)$.

Nach der Additionsformel ist dann $r_{n+1}(x) = \big(y\lambda_n(x)\big)^2 - r_n(x) - x$ und

$$ys_{n+1} = -iy\lambda_n(r_{n+1} - x) - y = y\left(\left(\frac{s_n - 1}{r_n - x}\right)(r_{n+1} - x) - 1\right)\,.$$

Setzt man alles ein, führt das auf die gewünschte Rekursion

$$r_{n+1}(x) = F(x)\cdot\left(\frac{s_n(x) - 1}{r_n(x) - x}\right)^2 - r_n(x) - x$$

$$s_{n+1}(x) = -\frac{s_n(x) - 1}{r_n(x) - x}\big(r_{n+1}(x) - x\big) - 1\,.$$

Damit können wir nun induktiv Aussagen über die Funktionen r_n und s_n beweisen.

Lemma: Für jedes $n \in \mathbb{N}$ ist $r_n'(x) = ns_n(x)$. Insbesondere ist $[n]$ genau dann separabel, wenn $p = \operatorname{char} k$ kein Teiler von n ist.

Beweis durch vollständige Induktion.

Der Induktionsanfang mit $r_1(x) = x$ und $s_1(x) = 1$ ist klar.

Für den Induktionsschritt nehmen wir an, die Behauptung sei für ein $n \in \mathbb{N}$ richtig und wollen zeigen, daß sie auch für $n+1$ gilt. Um Indizes zu vermeiden setzen wir zur Abkürzung

$$r = r_n, \quad s = s_n, \quad R = r_{n+1}, \quad S = s_{n+1} \quad \text{und} \quad \lambda = i\lambda_n = \frac{s-1}{r-x}\,.$$

Wir wissen, daß $r' = ns$ ist und wollen $R' = (n+1)S$ zeigen.

Mit obigen Abkürzungen werden die Rekursionsformeln zu

$$R(x) = F(x)\lambda(x)^2 - r(x) - x$$

und

$$\begin{aligned} S(x) &= -\lambda(x)\big(R(x) - x\big) - 1 \\ &= -\lambda(x)\big(F(x)\lambda(x)^2 - r(x) - 2x\big) - 1 \\ &= -F(x)\lambda(x)^3 + \lambda(x)\big(r(x) + 2x\big) - 1 \end{aligned}$$

Differentiation der Formel für R führt auf

$$R' = F'\lambda^2 + 2F\lambda\lambda' - r' - 1\,.$$

Um zu zeigen, daß dies gleich $(n+1)S$ ist, betrachten wir die Differenz

$$\begin{aligned} \Delta &= R' - (n+1)S \\ &= F\lambda^2 + 2F\lambda\lambda' - r' - 1 + (n+1)F\lambda^3 - (n+1)\lambda(r+2x) + (n+1) \\ &= \lambda^2\big((F' + (n+1)F\lambda\big) + \lambda\big(2F\lambda' - (n+1)(r+2x)\big) + (n+1) - r' - 1\,. \end{aligned}$$

Nach Induktionsannahme ist $r' = ns$; der λ-freie Teil dieser Formel ist also

$$(n+1) - r' - 1 = n - ns = n(s-1)\,.$$

Setzen wir dies ein und dividieren wir alles durch $s-1$, erhalten wir wegen der Definition $\lambda = (s-1)/(r-x)$ die Formel

$$\frac{\Delta}{s-1} = \frac{s-1}{(r-x)^2}(F' + (n+1)F\lambda) + \frac{1}{r-x}(2F\lambda' - (n+1)(r+2x)) - n\,.$$

Multiplikation mit $(r-x)^3$ macht daraus die Formel

$$\frac{(r-x)^3}{s-1}\Delta = (s-1)(r-x)F' + \underbrace{(n+1)F(s-1)^2}_{A} + 2F(r-x)s'$$
$$- \underbrace{2F(s-1)(ns-1)}_{B} - (n+1)(r+2x)(r-x)^2 - n(r-x)^3\,,$$

die wir zunächst durch die Berechnung von $A - B$ vereinfachen wollen. Wenn wir beide Terme ausmultiplizieren, hebt sich vieles weg; übrig bleibt

$$A - B = -Fns^2 + Fn + Fs^2 - F = (Fs^2 - F)(1 - n) .$$

F ist das Polynom auf der rechten Seite der WEIERSTRASS-Gleichung; daher ist $F(x) = y^2$. Auch der Punkt $n(x, y) = \big(r(x), ys(s)\big)$ liegt auf E; daher ist auch $\big(ys(x)\big)^2 = F\big(r(x)\big)$ und

$$\begin{aligned} F(x)s(x)^2 - F(x) &= F\big(r(x)\big) - F(x) \\ &= r(x)^3 + ar(x) + b - x^3 - ax - b \\ &= \big(r(x) - x\big)\big(r(x)^2 + rx + x^2 + a\big) \end{aligned}$$

für alle x. Somit ist

$$A - B = (1 - n)(r - x)(r^2 + rx + x^2 + a) .$$

Setzen wir dies oben ein, wird die rechte Seite ein Vielfaches von $r - x$; nach Division beider Seiten durch $r - x$ erhalten wir die neue Gleichung

$$\begin{aligned} \frac{(r - x)^2}{s - 1}\Delta = (s - 1)F' + (1 - n)(r^2 + rx + x^2 + a) + 2Fs' \\ - (n + 1)(r + 2x)(r - x) - n(r - x)^2 \end{aligned}$$

Ableitung der Gleichung $Fs^2 = r^3 + ar + b$ führt auf

$$F's^2 + 2Fss' = 3r^2r' + ar' .$$

Setzen wir hier gemäß Induktionsannahme $r' = ns$ ein, können wir beide Seiten durch s dividieren und erhalten die neue Gleichung

$$F's + 2Fs' = 3nr^2 + an .$$

Somit ist

$$(s - 1)F' + 2Fs' = 3nr^2 + an - F'$$

und

$$\begin{aligned} \frac{(r - x)^3}{s - 1}\Delta &= (1 - n)(r^2 + rx + x^2 + a) + 3nr^2 + an - F's \\ &\quad - (n + 1)(r^2 + rx - 2x^2) - n(r^3 - 2rx + x^2) \\ &= - F' + 3x^2 + a = 0 . \end{aligned}$$

Also ist $\Delta = 0$ und damit $R' = r'_{n+1} = (n+1)S = (n+1)s_{n+1}$, wie behauptet.

∎

Für $n = 1$ und $n = 2$ haben wir r_n und s_n bereits explizit berechnet; mit der neuen Funktion $G = \frac{1}{2}F'$ die Formel für $n = 2$ etwas kompakter schreiben als

$$r_2(x) = \frac{G(x)^2}{F(x)} - 2x \qquad \text{und} \qquad s_2(x) = -\frac{G(x)^3}{F(x)^2} + 3x\frac{G(x)}{F(x)} - 1\,.$$

Wenden wir die Additionsformel an auf P und $2P$, müssen wir zunächst die Steigung

$$H(x) = \frac{s_2(x) - s_1(x)}{r_2(x) - r_1(x)}$$
$$\frac{1}{F(x)} \underbrace{\left(-\frac{-G(x)^3 + 3xG(x)F(x) - 2F(x)^2}{G(x)^2 - 3xF(x)} \right)}_{h_0(x)} = \frac{h_0(x)}{F(x)}$$

der Verbindungsgeraden berechnen und erhalten

$$r_3(x) = F(x)H(x)^2 - r_2(x) - x$$
$$s_3(x) = -H(x)(r_3(x) - x) - 1\,,$$

was wir durch Einsetzen noch expliziter machen könnten. Die Formeln werden jedenfalls für größer werdendes n immer komplexer.

Wir begnügen uns daher zunächst mit einer viel einfacheren Aussage: Wir betrachten nur Punkte der Ordnung zwei. Das sind bekanntlich genau die Punkte $(x_0, y_0) \in E(K)$, für die $y_0 = 0$ ist. Für gerade n ist natürlich $nP = O$, und für ungerade n ist $nP = P$. da die y-Koordinate von nP dann gleich $y_0 s_n(x_0) = 0$ ist, folgt daraus nichts über $s_n(x_0)$. Immerhin wissen wir, daß x_0 für eine elliptische Kurve wegen der Nichtsingularität eine einfache Nullstelle von F sein muß; also ist $F'(x_0) \neq 0$ und damit natürlich auch $G(x_0) = \frac{1}{2}F'(x_0)$.

Lemma: Für $(x_0, 0) \in E[2]$ ist $s_n(x_0) = n$ für alle ungeraden n.

Beweis durch Induktion nach n: Für $n = 1$ ist $s_1(x) = 1$ für alle x.

Für $n = 3$ haben wir s_3 gerade allgemein ausgerechnet; an der Stelle x_0 ist $F(x_0) = 0$, aber $G(x_0) \neq 0$; daher ist $h_0(x_0) = -G(x_0) \neq 0$ und

$$\begin{aligned} s_3(x) &= -H(x)(F(x)H(x)^2 - \frac{G(x)^2}{F(x)}) - 1 \\ &= -H(x) \cdot \frac{(h_0(x) - G(x))(h_0(x) + G(x))}{F(x)} - 1 \end{aligned}$$

Nachrechnen zeigt, daß

$$h_0(x) + G(x) = -\frac{2F(x)^2}{G(x)^2 - 3xF(x)}$$

ist; da $F(x_0)$ verschwindet, ist also $h_0(x_0) + G(x_0) = 0$.

Wir können s_3 auch schreiben als

$$\begin{aligned} s_3(x) &= -H(x)F(x) \underbrace{\left(h_0(x) - G(x)\frac{-2}{G(x)^2 - 3xF(x)} \right)}_{h_1(x)} - 1 \\ &= -\frac{h_0(x)}{F(x)} F(x)h_1(x) - 1 \,; \end{aligned}$$

somit ist

$$h_1(x_0) = -2G(x_0) \cdot \frac{-2}{G(x_0)^2} = \frac{4}{G(x_0)}$$

und $s_3(x_0) = -(-G(x_0))\frac{4}{G(x_0)} - 1 = 4 - 1 = 3$.

Für $n > 3$ berechnen wir nach der Additionsformel

$$r_{n+2}(x) = m^2 - r_n(x) - r_2(x) \qquad \text{mit} \qquad m = y\frac{s_n(x) - s_2(x)}{r_n(x) - r_2(x)}$$

und $ys_{n+2} = -m\big(r_{n+2}(x) - r_n(x)\big) - ys_n(x)$; Einsetzen der Formeln für $r_2(x)$ und $s_2(x)$ führt auf

$$m = \frac{y}{F(x)} \underbrace{\left(\frac{F(x)^2(s_n(x) + 1) + G(x)^3 - 3xG(x)F(x) + F(x)^2}{F(x) - G(x)^2 + 3xF(x)} \right)}_{h(x)} ,$$

wobei $h(x_0) = -G(x_0)$ nicht verschwindet.

Die Funktion $m/y = h(x)/F(x)$ hat somit einen einfachen Pol an der Stelle $x = x_0$. Außerdem ist

$$m^2 = y^2 \frac{h(x)^2}{F(x)^2} = \frac{h(x)^2}{F(x)}, \qquad m^3 = y\frac{h(x)^3}{F(x)^2}$$

$$s_{n+2} = -\frac{h(x)}{F(x)} \cdot \left(\frac{(h(x) - G(x))(h(x) + G(x))}{F(x)} \right) - s_n(x)\,,$$

Ähnlich wie bei $n = 3$ erhalten wir die Summe

$$h(x) + G(x) = \frac{F(x)^2(s_n(x) + 1) + G(x)F(x)(r_n(x) - x)}{F(x)r_n(x) - G(x)^2 + 2xF(x)}\,,$$

die wegen $F(x_0) = 0$ an der Stelle x_0 verschwindet, da zwar der Zähler, nicht aber der Nenner verschwindet.

$r_n(x)$ ist natürlich nicht konstant, und $r_n(x_0) = x_0$, da $nP = P$ ist. Das Polynom $r_n - X$ verschwindet daher in x_0. Da x_0 eine einfache Nullstelle von F ist, können wir F als Ortsuniformisierende im Punkt x_0 wählen; es gibt daher eine Funktion t_n, so daß $r_n(x) - x = F(x) \cdot t_n(x)$ ist. Damit ist

$$h(x) + G(x) = F(x)^2 \frac{s_n(x) + 1 + G(x)t_n(x)}{F(x)r_n(x) - G(x)^2 + 2xF(x)}$$

und

$$\begin{aligned} s_{n+2}(x) = &-\frac{h(x)}{F(x)^2}\big(h(x) - G(x)\big) \cdot F(x)^2 \frac{s_n(x) + 1 + G(x)t_n(x)}{F(x)r_n(x) - G(x)^2 + 2xF(x)} \\ &- 2F(x)t_n(x)) - s_n \\ = &\, h(x)\big(h(x) - G(x)\big) \frac{s_n(x) + 1 + G(x)t_n(x)}{F(x)r_n(x) - G(x)^2 + 2xF(x)} \\ &- 2F(x)t_n(x)) - s_n(x)\,. \end{aligned}$$

An der Stelle x_0 ist $h(x_0) + G(x_0) = 0$, also $h(x_0) - G(x_0) = -2G(x_0)$ und $F(x_0) = 0$, also

$$s_{n+2}(x_0) = 2G(x_0)^2 \frac{s_n(x_0) + 1 + G(x_0)t_n(x_0)}{-2G(x_0)^2} - s_n(x_0)$$

Da nach Induktionsannahme $s_n(x_0) = n$ ist, folgt $s_{n+2}(x_0) = n + 2$, wie behauptet.

■

Lemma: Falls n kein Vielfaches der Charakteristik ist, gilt

$$\deg r_n = 2, \quad \deg s_n = 0, \qquad \frac{r_n}{x}(O) = \frac{1}{n^2}, \quad s_n(O) = \frac{1}{n^3}$$

Beweis durch Induktion nach n.

Für $n = 1$ und $n = 2$ folgt das aus den expliziten Formeln für r_n und s_n.

Eine natürliche Zahl größer zwei, die nicht durch $p = \operatorname{char} k$ teilbar ist, läßt sich stets darstellen als eine Summe $n+m$ zweier natürlicher Zahlen n, m derart, daß weder n noch m noch $n - m$ durch p teilbar ist. Es reicht daher zu zeigen:

Sind $n, m \in \mathbb{N}$ so, daß weder n noch m noch $n \pm m$ Vielfache von p sind und gilt die Behauptung für alle natürlichen Zahl kleiner $n + m$, so gilt sie auch für $n + m$. Nach der Additionsformel ist

$$r_{n+m}(x) = \lambda - r_n(x) - r_m(x) \qquad \text{mit} \qquad \lambda = \frac{s_n(x) - s_m(x)}{r_n(x) - r_m(x)}\,,$$

und nach Induktionsannahme ist

$$\frac{r_{n+m}}{\lambda}(O) = \left(\frac{\frac{1}{n^3} - \frac{1}{m^3}}{\frac{1}{n^2} - \frac{1}{m^2}}\right)^2 - \left(\frac{1}{n^2} + \frac{1}{m^2}\right) = \frac{1}{(n+m)^2}\,.$$

Ähnlich folgen auch die anderen Behauptungen. ∎

Definition: *a)* Ein *Divisor* auf E ist eine formale Summe der Form

$$D = \sum_{i=1}^{r} e_i P_i, \quad e_i \in \mathbb{Z}, \quad P_i \text{ verschiedene Punkte aus } E(K)$$

b) Der Grad eines solchen Divisors D ist $\deg D = \sum_{i=1}^{r} e_i$.

c) f sei eine rationale Funktion auf E; die Nullstellen und Polstellen von f seien die Punkte $P_1, \ldots P_r$. Der Divisor von f ist

$$\operatorname{div}(f) = \sum_{i=1}^{r} \operatorname{ord}_{P_i}(f) \cdot P_i\,.$$

Ein Divisor dieser Form heißt *Hauptdivisor.*

d) Für eine endliche Menge M von Punkten auf E schreiben wir

$$(M) = \sum_{P \in M} P$$

Die Divisoren bilden eine abelsche Gruppe $\mathrm{Div}(E)$, wenn wir die formalen Summen in der offensichtlichen Weise addieren, und die Divisoren vom Grad Null bilden eine Untergruppe $\mathrm{Div}^0(E)$. Die Hauptdivisoren bilden ebenfalls eine Untergruppe mit $(f) + (g) = (fg)$: man kann zeigen, daß sie in $\mathrm{Div}^0(E)$ liegt, d.h. jeder Hauptdivisor hat den Grad Null.

Es gibt einen Homomorphismus

$$\begin{cases} \mathrm{Div}(E) \to E \\ \underbrace{\sum e_p(P)}_{\text{Addition in Div } E} \to \underbrace{\sum e_p P}_{\text{Addition auf } E} \end{cases} .$$

Ein wesentlicher klassischer Satz in der Theorie elliptischer Kurven, für dessen Beweis uns leider die Zeit fehlt, ist der

Satz von Abel–Jacobi: Dieser Homomorphismus induziert einen Isomorphismus

$$\mathrm{Div}^0(E)/\mathcal{H} \to E\,.$$

Lemma: $0 \neq n \neq \pm m \in \mathbb{Z}$ seien so, daß weder m noch n, noch $n \pm m$ durch $p = \mathrm{char}\, k$ teilbar sind. Dann gilt:

$$\mathrm{div}(r_n - r_m) = (E[n+m]) + (E[n-m]) - 2(E[n]) - 2(E[m])$$

Beweis: Ist P eine Nullstelle von $r_n - r_m$, so haben nP und mP die gleiche x-Koordinate, d.h. $(n-m)P = O$ oder $(n+m)P = O$. Ist P ein Pol von $r_n - r_m$, ist $(r_n - r_m)(P) = \infty$, d.h. $r_n(P) = \infty$ oder $r_m P = \infty$, d.h. $nP = O$ oder $m(P) = O$. Die Punkte, die in $\mathrm{div}(r_n - r_m)$ mit Koeffizient ungleich Null vorkommen, kommen also alle auch in mindestens einem der vier Summanden rechts vor. Zu zeigen bleibt, daß die Koeffizienten auf beiden Seiten die gleichen sind.

1. Fall: $P = O$ liegt in $E[n+m] \cap E[n-m] \cap E[n] \cap E[m]$; er sollte also nach der zu beweisenden Formel in $\operatorname{div}(r_n - r_m)$ mit Koeffizient -2 auftreten. Wir wissen aus dem vorherigen Lemma, daß

$$\frac{r_n - r_m}{x}(O) = \frac{1}{n^2} - \frac{1}{m^2} = \frac{m^2 - n^2}{n^2 m^2} = \frac{(m+n)(m-n)}{n^2 m^2} \notin \{0, \infty\}$$

also ist die Ordnung von $\frac{r_n - r_m}{x}$ in O gleich 0, d.h. $r_n - r_m$ hat dort die gleiche Ordnung wie x, also -2.

2. Fall: $P \in E[n] \cap E[m]$. Dann liegt P auch in $E[n \pm m]$, also sollte wieder $\operatorname{ord}_P(r_n - r_m) = -2$ sein. Für die Translation

$$\tau_P : \begin{cases} E \to E \\ Q \mapsto P + Q \end{cases}$$

und jede Funktion $f \in k(E)$ ist $\operatorname{ord}_{P+Q}(f) = \operatorname{ord}_Q(f \circ \tau_P)$. Daher läßt sich dieser Fall via τ_p auf den bereits behandelten Spezialfall $P = O$ zurückführen.

3.Fall: $P \in E[n-m] \setminus E[n+m]$. Dann ist $(n-m)P = O$, also $nP = mP$, aber $nP \neq -mP$, da $P \notin E[n+m]$. Somit ist $nP \neq -nP$ und $mP \neq -mP$, d.h. $2nP$ und $2mP$ sind beide verschieden von O. Damit kann P weder in $E[2]$, noch in $E[n]$, noch in $E[m]$ liegen. Auf der rechten Seite hat P daher den Koeffizienten eins. Wegen $nP = mP$ stimmen insbesondere die y-Koordinaten $ys_n(P)$ und $ys_m(P)$ überein; da $P \notin E[2]$, ist $y \neq 0$, so daß auch $s_n(P) = s_m(P)$ sein muß. Aus $r_n'(P) = ns_n(P)$ folgt, daß

$$(r_n - r_m)'(P) = (n-m)s_n(P)$$

nicht verschwindet; daher ist P in der Tat ein einfachher Pol von $r_n - r_m$.

Die übrigen Fälle zeigt man analog. ∎

Satz: Ist n kein Vielfaches von $p = \operatorname{char} k$, so ist $\#E[n] = n^2$.

Beweis: Für $n = 1$ ist $E[1] = \{O\}$, für $n = 2$ wissen wir bereits, daß $E[2]$ vier Elemente enthält.

Für Werte größer zwei verwenden wir das gleiche Induktionsargument wie im letzten Induktionsbeweis, d.h. wir schreiben die Zahl in der

Form $n+m$, wobei n, m und $n \pm m$ alle nicht durch p teilbar sein sollen, und wir nehmen an, die Behauptung sei für alle Zahlen kleiner $n + m$ bewiesen. Für jede ganze Zahl $r \neq 0$ bezeichne d_r die Elementanzahl von $E[r]$.

Nach dem gerade bewiesenen Lemma hat $\operatorname{div}(r_n - r_m)$ den Grad

$$d_{m+n} + d_{m-n} - 2d_n - 2d_m \, .$$

Da Hauptdivisoren den Grad Null haben, verschwindet diese Summe, d.h.

$$\begin{aligned} d_{m+n} &= 2d_n + 2d_m - d_{m-n} \\ &= 2n^2 + 2m^2 - (m-n)^2 \\ &= 2n^2 + 2m^2 - m^2 + 2mn - n^2 \\ &= n^2 + m^2 + 2mn \\ &= (n+m)^2 \, . \end{aligned}$$

Dies beweist die Behauptung. ∎

Nun sei E eine elliptische Kurve über einem endlichen Körper k. Dann ist $E = E(k)$ eine endliche Gruppe; ihre Ordnung sei N. Dann ist

$$E(k) \leq E[N] \leq \mathbb{Z}/N \times \{Z/N \, .$$

Nach dem Struktursatz für endliche abelsche Gruppen gibt es natürliche Zahlen $n_r | n_{r-1} | \cdots | n_2 | n_1$ derart, daß

$$E[k] \cong \mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_r \, .$$

Da $E[k] \leq \mathbb{Z}/N \times \mathbb{Z}/N$ ist, folgt $r \leq 2$ und $n_2 \mid n_1 \mid N$. Somit gibt es natürliche Zahlen $n_2 | n_1$ derart, daß $E(k) \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2$ ist.

Mit etwas mehr Aufwand kann man zeigen, daß zusätzlich n_2 ein Teiler von $\#k - 1$ sein muß. Falls n_1 teilerfremd ist zu $\#k - 1$, kommt also nur $n_2 = 1$ in Frage, und $E(k)$ ist eine zyklische Gruppe der Ordnung n_1. Auch sonst wird $\operatorname{ggT}(n_1, \#k - 1)$ oft klein sein, so daß $E(k)$ eine große zyklische Untergruppe hat, was insbesondere für kryptographische Anwendungen sehr nützlich ist.