KAPITEL 12

Kurven vom Geschlecht 1 — elliptische Kurven

1. Einführung

Sofern nichts anderes gesagt, verstehen wir unter einer Kurve immer eine über dem Grundkörper K definierte, absolut irreduzible, nichtsinguläre, projektive Kurve.

Beispiel: Ist $C \subseteq \mathbb{P}^2$ eine nichtsinguläre Kubik,

$$C = \{a_0x_0^3 + a_1x_0^2x_1 + a_2x_0^2x_2 + \cdots + a_9x_2^3 = 0\},$$

so hat C Geschlecht $g = \frac{(3-1)(3-2)}{2} = 1$.

Was können wir allgemein über eine Kurve C vom Geschlecht $g = 1$ sagen?

(1) Für kanonische Divisoren gilt: $\operatorname{grad}(K_C) = 2g-2 = 0$ und $\ell(K_C) = g = 1$. Sei $f \in \mathcal{L}(K_C) \setminus \{0\}$. Dann gilt $K_C + \operatorname{div}(f) \geq 0$. Wegen $\operatorname{grad}(K_C + \operatorname{div}(f)) = \operatorname{grad}(K_C) = 0$ gilt bereits $K_C + \operatorname{div}(f) = 0$, also ist auch der triviale Divisor 0 kanonisch. Der einzige effektive kanonische Divisor ist also der Divsor 0. Wir können also stets $K_C = 0$ annehmen.

(2) Der Satz von Riemann-Roch wird dann zu

$$\ell(D) = \operatorname{grad}(D) + \ell(-D).$$

Insbesondere folgt

$$\ell(D) = \operatorname{grad}(D) \quad \text{für } \operatorname{grad}(D) \geq 1.$$

(3) Wie kann man C als projektive Kurve realisieren? Im Fall $g(C) = 0$ war $C \simeq \phi_{-K_C}(C) \subseteq \mathbb{P}^2$ eine ebene Quadrik. Im Fall $g(C) = 1$ haben wir leider keinen natürlichen über K definierten Divisor zur Verfügung. (Ich weiß keine Antwort auf diese Frage. Wichtige Ausnahme: Kurven vom Geschlecht 1 über einem endlichen Körper)

Es gibt Kurven vom Geschlecht 1 über $\mathbb{Q}$, die keine $\mathbb{Q}$-rationalen Punkt besitzen, wie folgendes Beispiel zeigt.

Beispiel: Sei $\alpha \in \mathbb{F}_8$ mit $\alpha^3 + \alpha + 1 = 0$. Es ist $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$. Wir betrachten über $\mathbb{F}_2$ ($x \mapsto x^2$ ist der Frobeniusautomorphismus, $x \mapsto x^2$ und $x \mapsto x^4$ also die nichttrivialen Elemente der Galoisgruppe):

$$f = (x_0 + \alpha x_1 + \alpha^2 x_2)(x_0 + \alpha^2 x_1 + \alpha^4 x_2)(x_0 + \alpha^4 x_1 + \alpha^8 x_2).$$

Ausmultiplizieren liefert

$$f = x_0^3 + x_0x_1^2 + x_0x_1x_2 + x_0x_2^2 + x_1^3 + x_1x_2^2 + x_2^3.$$

$\{f = 0\} \subseteq \mathbb{P}^2$ besteht aus 3 Geraden, die nicht durch einen Punkt gehen, hat also keinen $\mathbb{F}_2$-rationalen Punkt.
Wir definieren jetzt über $\mathbb{Q}$:

$$F = x_0^3 + x_0x_1^2 + x_0x_1x_2 + x_0x_2^2 + x_1^3 + x_1x_2^2 + x_2^3 \in \mathbb{Q}[x_0, x_1, x_2]$$

und $C = \{F = 0\} \subseteq \mathbb{P}^2$. Man rechnet nach, dass C nichtsingulär ist. Da F modulo 2 keine nichttrivialen Nullstellen hat, hat C keine $\mathbb{Q}$-rationalen Punkte, wie man durch Reduktion modulo 2 sieht.

Datei: algku12.tex. Version vom 18.7.2021

Bemerkung: Ist C eine über $\mathbb{F}_p$ definierte Kurve vom Geschlecht 1, so gilt folgende Abschätzung von Hasse [**HKT**, S.343, Theorem 9.18 (Hasse-Weil Bound)] oder [**Luetkebohmert**, S.162, Satz 7.4.1 (Weil-Schranke)]:

$$|\#C(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}.$$

Daraus folgt sofort

$$\#C(\mathbb{F}_p) \neq \emptyset.$$

Wir betrachten jetzt Kurven vom Geschlecht 1 mit einem K-rationalen Punkt.

2. Elliptische Kurven

DEFINITION. *Eine* **elliptische Kurve** *E über K ist eine (absolut irreduzible, nichtsinguläre, projektive) Kurve vom Geschlecht 1 zusammen mit einem Punkt $O \in E(K)$.*

Da wir jetzt bei elliptischen Kurven nichttriviale, über K definierte Divisoren kennen, können wir sie als projektive Kurven realisieren:

SATZ. *Sei (E, O) eine elliptische Kurve über K. Dann ist E über K isomorph zu einer ebenen Kubik der Gestalt*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

mit $a_i \in K$, wobei O dem Punkt $(0:0:1)$ entspricht. Eine solche Gleichung nennt man auch eine **Weierstraßgleichung** *für E.*

Beweis:

- Wir wissen, dass ein ein Divisor D mit $\operatorname{grad}(D) \geq 2g+1 = 3$ sehr ampel ist, d.h. ϕ_D liefert eine Einbettung von C als Kurve vom Grad $\operatorname{grad}(D)$ in $\mathbb{P}^{\ell(D)-1}$. Wir wählen den über K definierten Divisor $D = 3 \cdot [O]$. Riemann-Roch liefert $\ell(3 \cdot [O]) = 3$, also erhalten wir
$$E \simeq \phi_{3[O]}(E) \subseteq \mathbb{P}^2$$
als Kurve vom Grad 3 im $\mathbb{P}^2$.
- Wie sieht $\phi_{3[O]}$ aus? Riemann-Roch liefert $\ell(n[O]) = n$ für $n \geq 1$. Sei t uniformisierend in O, d.h. $\operatorname{ord}_O(t) = 1$. Wir beschreiben jetzt die Vektorräume $\mathcal{L}(n[O])$:
- Natürlich ist $\mathcal{L}([O]) = \overline{K} \cdot 1$.
- Wegen $\ell(2[O]) = 2$ gibt es ein $x \in K(E)$ mit $\mathcal{L}(2[O]) = \overline{K} + \overline{K} \cdot x$. Wegen $x \notin \mathcal{L}([O])$ ist $\operatorname{ord}_O(x) = -2$ und wir können nach Multiplikation mit einer Konstanten $(t^2x)([O]) = 1$ erreichen.
- Analog erhält man ein $y \in K(E)$ mit $\mathcal{L}(3[O]) = \overline{K} + \overline{K}x + \overline{K}y$. Die Funktion y erfüllt $\operatorname{ord}_O(y) = -3$, also können wir wieder o.E. $(t^3y)(O) = 1$ annehmen. x und y haben außer in O keine Polstelle.
- Wir definieren jetzt $\phi = \phi_{3[O]} = (1 : x : y)$. Was ist $\phi(O)$? Es ist $\phi = (t^3 : t(t^2x) : t^3y)$, also wegen $t(O) = 0$:
$$\phi(O) = (0:0:1).$$
$\phi(E)$ ist eine zu E isomorphe ebene Kurve vom Grad 3. Wir brauchen jetzt nur noch eine nichttriviale Relation zwischen $1, x, y$ um die Kurvengleichung zu erhalten.
- Es gilt weiter
$$\mathcal{L}(4[O]) = \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2, \quad \mathcal{L}(5[O]) = \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 + \overline{K}xy,$$
$$\mathcal{L}(6[O]) = \overline{K} + \overline{K}x + \overline{K}y + \overline{K}x^2 + \overline{K}xy + \overline{K}x^3.$$
Nun ist $y^2 \in \mathcal{L}(6[O]) \setminus \mathcal{L}(5[O])$, also gibt es $a_1, a_2, a_3, a_4, a_6, c \in K$, $c \neq 0$ mit
$$y^2 = cx^3 + a_2x^2 + a_4x + a_6 - a_1xy - a_3y.$$
Multipliziert man mit t^6 und setzt dann O ein, so erhält man
$$(t^3y)^2(O) = c(t^2x)^3(O) + 0,$$

also $c = 1$. Damit haben wir

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Dieser Gleichung genügt dann auch $\phi(E)$ in $\mathbb{P}^2$, was wir noch zeigen wollten. ■

Beispiel: Wir betrachten über $\mathbb{F}_{13}$ die durch

$$f = x_0^3 + 2x_1^3 + 4x_2^3$$

definierte ebene Kubik. Sie ist nichtsingulär und hat deswegen Geschlecht 1. Wir betrachten den Punkt $P = (1 : 2 : 4)$. Mit SAGE erhalten wir

$$\begin{aligned}
\mathcal{L}(2[P]) &= \left[\frac{4x_0 + 8x_1}{5x_0 + x_1 + 8x_2}, \frac{3x_0 + x_2}{-x_0 + 5x_1 + x_2}\right], \\
\mathcal{L}(3[P]) &= \left[\frac{6x_0^3 + x_0^2x_1 + 10x_0x_1^2 + x_1^3 + 8x_0^2x_2 + x_0x_1x_2 - x_0x_2^2}{9x_0^3 - x_0^2x_1 + x_1x_2^2}, \frac{x_0^3 + x_0^2x_1 + 5x_0x_1^2 + 3x_0^2x_2 + 9x_0x_1x_2 + x_1^2x_2 + 10x_0x_2^2}{9x_0^3 - x_0^2x_1 + x_1x_2^2}, 1\right]
\end{aligned}$$

Wir schreiben dies mit $x = \frac{x_1}{x_0}$, $y = \frac{x_2}{x_0}$:

$$\begin{aligned}
\mathcal{L}(2[P]) &= \left[\frac{8x + 4}{x + 8y + 5}, \frac{y + 3}{5x + y + 12}\right], \\
\mathcal{L}(3[P]) &= \left[\frac{x^3 + 10x^2 + xy - y^2 + x + 8y + 6}{xy^2 - x + 9}, \frac{x^2y + 5x^2 + 9xy + 10y^2 + x + 3y + 1}{xy^2 - x + 9}, 1\right]
\end{aligned}$$

Wir lösen die Gleichung $f(1, x, y) = 0$ in $F_{13}[[t]]$ im Punkt $P = (2, 4)$ wie zuvor erläutert:

$$\begin{aligned}
x &= 2 + t, \\
y &= 4 + 8t + t^2 + 12t^3 + 3t^4 + 5t^5 + 4t^7 + 8t^8 + 7t^9 + 2t^{10} + 10t^{11} + 9t^{12} + 8t^{14} + 8t^{15} + t^{16} + t^{17} + \\
&\quad +9t^{18} + 6t^{19} + 5t^{20} + 3t^{21} + 10t^{22} + t^{23} + 3t^{25} + 7t^{26} + 3t^{27} + 9t^{28} + 7t^{29} + 2t^{30} + O(t^{31}).
\end{aligned}$$

Damit sehen die Funktionen in obigen Vektorräumen so aus:

$$\begin{aligned}
\mathcal{L}(2[P]) &= [\frac{9}{t^2} + \frac{10}{t} + 9 + 12t + 10t^4 + 9t^6 + 2t^7 + 4t^8 + 8t^9 + 10t^{10} + 3t^{11} + 10t^{12} + 11t^{13} + 7t^{15} + 2t^{16} + O(t^{18}), \\
&\quad \frac{7}{t^2} + \frac{2}{t} + 8 + 5t + 2t^4 + 7t^6 + 3t^7 + 6t^8 + 12t^9 + 2t^{10} + 11t^{11} + 2t^{12} + 10t^{13} + 4t^{15} + 3t^{16} + O(t^{18})], \\
\mathcal{L}(3[P]) &= [\frac{8}{t^3} + \frac{6}{t^2} + \frac{10}{t} + 12 + 11t + 2t^2 + 3t^4 + 8t^5 + t^6 + 2t^7 + 9t^8 + 2t^9 + t^{11} + 4t^{12} + 10t^{13} + 9t^{14} + 7t^{15} + 11t^{16} + O(t^{17}), \\
&\quad \frac{1}{t^3} + \frac{12}{t^2} + \frac{4}{t} + 1 + 5t + 10t^2 + 8t^4 + t^5 + 6t^7 + 11t^8 + 7t^9 + 6t^{10} + 12t^{11} + 2t^{13} + 6t^{14} + 8t^{15} + 12t^{16} + O(t^{17}), 1]
\end{aligned}$$

Sei X das erste Element aus $\mathcal{L}(2[P])$ dividiert durch 9, Y das erste Element aus $\mathcal{L}(3[P])$ dividiert durch 8:

$$\begin{aligned}
X &= \frac{1}{t^2} + \frac{4}{t} + 1 + 10t + 4t^4 + t^6 + 6t^7 + 12t^8 + 11t^9 + 4t^{10} + 9t^{11} + 4t^{12} + 7t^{13} + 8t^{15} + 6t^{16} + O(t^{18}), \\
Y &= \frac{1}{t^3} + \frac{4}{t^2} + \frac{11}{t} + 8 + 3t + 10t^2 + 2t^4 + t^5 + 5t^6 + 10t^7 + 6t^8 + 10t^9 + 5t^{11} + 7t^{12} + 11t^{13} + 6t^{14} + 9t^{15} + 3t^{16} + O(t^{17}).
\end{aligned}$$

Nun sind wir in der Situation wie im vorangegangenen Beweis zu den elliptischen Kurven. Es ist nicht schwer, eine Gleichung herzuleiten:

```
R.<t>=LaurentSeriesRing(GF(13))
X=t^-2 + 4*t^-1 + 1 + 10*t + 4*t^4 + t^6 + 6*t^7 + 12*t^8 + 11*t^9 + 4*t^10 + 9*t^11 + 4*t^12 + 7*t^13 +
Y=t^-3 + 4*t^-2 + 11*t^-1 + 8 + 3*t + 10*t^2 + 2*t^4 + t^5 + 5*t^6 + 10*t^7 + 6*t^8 + 10*t^9 + 5*t^11 +
```

Man findet:

$$Y^2 - X^3 - 9XY - 6X^2 - 11Y - 12X - 8 = O(t^{14}),$$

also

$$Y^2 - 9XY - 11Y = X^3 + 6X^2 + 12X + 8.$$

FOLGERUNG. *Ist* $\mathrm{char}(K) \neq 2,3$ *und* (E,O) *eine elliptische Kurve über* K*, so ist* E *isomorph zu einer ebenen Kurve*

$$y^2 = x^3 + ax + b$$

mit $a, b \in K$*, wo* O *dem Punkt* $(0:0:1)$ *entspricht.*

Beweis: Wir können mit einer Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

starten. Das Ziel erreichen wir durch quadratische und kubische Ergänzung. Wir können auch einen Koordinatenwechsel ansetzen:

$$y = y' + Ax' + B, \quad x = x' + C.$$

Wählt man

$$A = -\frac{1}{2}a_1, \quad B = -\frac{1}{2}a_3 + \frac{1}{6}a_1a_2 + \frac{1}{24}a_1^3, \quad C = -\frac{1}{3}a_2 - \frac{1}{12}a_1^2,$$

so erhält man eine Gleichung $y'^2 = x'^3 + ax' + b$ der gewünschten Form. ■

Während für Kurven vom Geschlecht 0 die Picardgruppe Pic^0 trivial ist, gilt für Kurven vom Geschlecht 1 folgender Satz:

SATZ. *Sei* (E,O) *eine elliptische Kurve. Dann ist die Abbildung*

$$\psi : E \to \mathrm{Pic}^0(E), \quad P \mapsto \textit{Klasse von } [P] - [O]$$

eine Bijektion.

Beweis:

- ψ *ist surjektiv:* Sei D ein Divisor vom Grad 0. Dann hat $D + [O]$ Grad 1, nach Riemann-Roch ist $\ell(D + [O]) = 1$, also gibt es eine Funktion $f \in \overline{K}(E)^*$ mit $D + [O] + \mathrm{div}(f) \geq 0$. Der Divisor $D + [O] + \mathrm{div}(f)$ ist effektiv vom Grad 1, also ein Punkt: $D + [O] + \mathrm{div}(f) = [P]$. Damit gilt $D \sim [P] - [O]$, also Klasse von $D = \psi(P)$.
- ψ *ist injektiv:* Sei $\psi(P) = \psi(Q)$. D.h. $[P]-[O] \sim [Q]-[O]$, und damit auch $[P] \sim [Q]$. Es gibt also eine Funktion f mit $[P] = [Q] + \mathrm{div}(f)$ und damit $\mathrm{div}(f) = [P] - [Q]$. Also ist $f \in \mathcal{L}([Q]) = \overline{K}$ und damit $P = Q$. ■

Diese Bijektion erlaubt uns jetzt eine Gruppenstruktur auf (E,O) einzuführen:

DEFINITION. *Sei* (E,O) *eine elliptische Kurve und* $\psi : E \to \mathrm{Pic}^0(E), P \mapsto$ *Klasse von* $([P] - [O])$*. Für* P_1, P_2 *definieren wir*

$$P_1 \oplus P_2 = \psi^{-1}(\psi(P_1) + \psi(P_2)).$$

Dadurch wird E *zu einer abelschen Gruppe mit* O *als neutralem Element.*

Bemerkungen:

- Für $P, Q, R \in E$ gilt:

$$\begin{aligned} P \oplus Q = R \quad &\iff \quad \psi(P) + \psi(Q) = \psi(R) \\ &\iff \quad [P] - [O] + [Q] - [O] \sim [R] - [O] \\ &\iff \quad [P] + [Q] \sim [O] + [R] \iff [R] \sim [P] + [Q] - [O]. \end{aligned}$$

  Wie findet man also R? Der Divisor $[P] + [Q] - [O]$ hat Grad 1, also ist $\mathcal{L}([P] + [Q] - [O])$ 1-dimensional. Sei $\mathcal{L}([P] + [Q] - [O]) = \overline{K}f$. Dann ist $[P] + [Q] - [O] + \mathrm{div}(f)$ effektiv vom Grad 1, also ein Punkt, nämlich $[R]$.
- Aus der Überlegung eben folgt sofort, dass $E(K)$ abgeschlossen bzgl. $\oplus$ ist, also eine Untergruppe.
- Das inverse Element zu P ist durch die Gleichung $[P] + [P'] \sim 2[O]$ bestimmt.

Wir wollen für ebene Kubiken die Gruppenstruktur geometrisch deuten, wozu wir ein paar Aussagen über Geradenschnitte brauchen:

LEMMA. *Sei $E \subseteq \mathbb{P}^2$ eine nichtsinguläre Kurve vom Grad 3 und $H = \operatorname{div}(h)$ ein Geradenschnitt, insbesondere $\operatorname{grad}(H) = 3$. Dann gilt: Ist D ein effektiver Divisor, der linear äquivalent zu H ist, so ist D selbst schon ein Geradenschnitt, d.h. es gibt eine Gerade $g = b_0x_0 + b_1x_1 + b_2x_2 = 0$ mit $D = \operatorname{div}(g)$.*

Beweis: Nach Riemann-Roch gilt $\ell(H) = \operatorname{grad}(H) = 3$, also ist

$$\mathcal{L}(H) = \overline{K}\frac{x_0}{h} + \overline{K}\frac{x_1}{h} + \overline{K}\frac{x_2}{h}.$$

Wegen $D \sim H$ gibt es eine Funktion f mit $D = H + \operatorname{div}(f)$. Wegen $D \geq 0$ ist $f \in \mathcal{L}(H)$, also gibt es $b_0, b_1, b_2 \in \overline{K}$ mit

$$f = \frac{b_0x_0 + b_1x_1 + b_2x_2}{h},$$

woraus sofort $D = \operatorname{div}(b_0x_0 + b_1x_1 + b_2x_2)$ folgt. ■

Aufgabe: Zeige die analoge Aussage für alle nichtsingulären ebenen Kurven. Die entsprechende Eigenschaft wird auch lineare Normalität genannt.

Geometrische Deutung der Addition für nichtsinguläre ebene Kubiken: Sei $E = \{f = 0\} \subseteq \mathbb{P}^2$ eine nichtsinguläre Kurve vom Grad 3 und $O \in E(K)$. Wie kann man die oben definierte Addition beschreiben?

(1) Seien P und Q Punkte auf E. Dann gibt es eine eindeutig bestimmte Gerade $g = 0$ und einen weiteren Punkt $R' \in E$ mit

$$[P] + [Q] + [R'] = \operatorname{div}(g).$$

$g = 0$ ist die Gerade durch P und Q bzw. die Tangente in P an E im Fall $P = Q$.

(2) Analog gibt es eine eindeutig bestimmte Gerade $h = 0$ durch O und R' und einen weiteren Punkt $R \in E$ mit

$$[O] + [R'] + [R] = \operatorname{div}(h).$$

Im Fall $O = R'$ ist $h = 0$ die Tangente in O an E.

(3) Nun wollen wir $P \oplus Q$ bestimmen. Es gilt für $S \in E$:

$$\begin{aligned}
P \oplus Q = S &\iff [P] - [O] + [Q] - [O] \sim [S] - [O] \iff [S] + [O] \sim [P] + [Q] \\
&\iff [S] + [O] + [R'] \sim [P] + [Q] + [R'] \sim \operatorname{div}(g) \\
&\iff [S] + [O] + [R'] \text{ ist Geradenschnitt nach dem Lemma} \\
&\iff [S] + [O] + [R'] = \operatorname{div}(h) = [R] + [O] + [R'] \\
&\iff S = R.
\end{aligned}$$

Damit gilt also $R = P \oplus Q$.

(4) Wir wollen noch das Inverse zu $P \in E$ bestimmen. Sei dazu $g = 0$ die Tangente in O an E und $\operatorname{div}(g) = 2[O] + [O']$.

$$\begin{aligned}
P \oplus P' = O &\iff [P] - [O] + [P'] - [O] \sim [O] - [O] \\
&\iff [P] + [P'] \sim 2[O] \\
&\iff [P] + [P]' + [O'] \sim 2[O] + [O'] = \operatorname{div}(g) \\
&\iff [P] + [O'] + [P'] \text{ ist Geradenschnitt}
\end{aligned}$$

Ist $h = 0$ die Gerade durch P und O', so ist also P' eindeutig bestimmt durch $[P] + [O'] + [P'] = \operatorname{div}(h)$.

Wir fassen zusammen:

SATZ. *Sei E eine nichtsinguläre ebene Kubik und $O \in E(K)$.*

(1) *Die Addition zweier Punkte $P, Q \in E$ ergibt sich geometrisch wie folgt:*
- *Bestimme die Gerade $g = 0$ durch P und Q und damit den 3. Schnittpunkt R' mit* $\operatorname{div}(g) = [P] + [Q] + [R']$.
- *Bestimme die Gerade $h = 0$ durch R' und O und damit den 3. Schnittpunkt R mit* $\operatorname{div}(h) = [R'] + [O] + [R]$.

Dann gilt $P \oplus Q = R$.

(2) *Bestimme die Tangente $t = 0$ in O an E und damit den 3. Schnittpunkt O' mit* $\operatorname{div}(t) = 2[O] + [O']$.
Bestimme für $P \in E$ die Gerade $s = 0$ durch P und O' und damit den 3. Schnittpunkt P' mit $\operatorname{div}(s) = [P] + [O'] + [P']$. *Dann ist $\ominus P = P'$, d.h. $P \oplus P' = O$.*

Beispiel: Wir betrachten wieder $E = \{f = 0\}$ über $\mathbb{Q}$ mit

$$f = 3x_0^2x_1 + x_0x_1^2 + 3x_0x_1x_2 + x_0x_2^2 - x_1^3 + 2x_1^2x_2 - x_2^3$$

und $O = (1 : 0 : 0)$.

- Die Tangente in O ist $x_1 = 0$, woraus man schnell $O' = (1 : 0 : 1)$ errechnet.
- Wir wollen $2 \cdot O' = O' \oplus O'$ berechnen. Die Tangente in O' ist $x_0 + 6x_1 - x_2 = 0$, einsetzen in f liefert
$$f(x_0, x_1, x_0 + 6x_1) = -x_1^2(205x_1 + 51x_0),$$
woraus sich als 3. Schnittpunkt mit der Tangente $R' = (205 : -51 : -101)$ ergibt. Die Gerade zwischen O und R' hat die Gleichung $x_2 = \frac{101}{51}x_1$, mit
$$f(x_0, x_1, \frac{101}{51}x_1) = \frac{1}{132651}x_1(5x_0 + 205x_1)(7803x_0 - 3110x_1)$$
erhält man als 3. Schnittpunkt $R = (3110 : 7803 : 15453)$, also
$$2 \cdot (1 : 0 : 1) = (3110 : 7803 : 15453).$$
(Über $\mathbb{R}$ ist $(205 : -51 : -101) \approx (1 : -0.25 : -0.49)$ und $(3110 : 7803 : 15453) \approx (1 : 2.51 : 4.97)$.)
- Wir berechnen jetzt $(1 : 0 : 1) \oplus (3110 : 7803 : 15453)$: Die Gerade durch die beiden Punkte ist
$$x_2 = x_0 + \frac{12343}{7803}x_1,$$
einsetzen in f liefert
$$\frac{1}{475099770627}x_1(269008425x_0 + 274115666x1)(7803x_0 - 3110x_1),$$
so dass man für den 3. Schnittpunkt
$$(274115666 : -269887425 : -151409259)$$
erhält. Die Gerade durch diesen Punkt und O ist
$$x_2 = \frac{989603}{1758225}x_1,$$
sie schneidet E in dem 3. Punkt
$$3 \cdot (1 : 0 : 1) = (1043360347 : 60614806875 : 34116563425).$$
- Die Addition kann man natürlich auch einfach programmieren, was wir auch für die folgenden Rechnungen gemacht haben.
- Welche $\mathbb{Q}$-rationalen Punkte hat E?
- Vorbemerkung: Ist $P = (p_0 : p_1 : p_2) \in \mathbb{P}^2(\mathbb{Q})$, so können wir o.E. $p_0, p_1, p_2 \in \mathbb{Z}$ und $\operatorname{ggT}(p_0, p_1, p_2) = 1$ annehmen. Die Höhe des Punktes P definieren wir dann als
$$H(P) = \max(|p_0|, |p_1|, |p_2|).$$
- Wir haben alle Punkte der Höhe ≤ 340 in $E(\mathbb{Q})$ bestimmt. Sie stehen in nachfolgender Tabelle. Dabei steht Pn für einen Punkt der Höhe n. Gibt es mehrere, haben wir sie mit $a, b, c, \ldots$ durchnumeriert.

- Da $E(\mathbb{Q})$ eine Gruppe bildet, kann man natürlich fragen, welche Struktur diese Gruppe hat. Nach ein paar Versuchen haben wir

$$A_1 = (1:0:1) = P1b, \quad A_2 = (1:1:-1) = P1d, \quad A_3 = (3:-4:2) = P4$$

gewählt, womit sich alle gefundenen Punkte der Tabelle linear kombinieren ließen. (In der Tabelle stehen bei jedem Punkt die Koeffizienten n_1, n_2, n_3 von $P = n_1A_1 + n_2A_2 + n_3A_3$.) Die Frage stellt sich jetzt: Gilt

$$E(\mathbb{Q}) = \mathbb{Z}A_1 + \mathbb{Z}A_2 + \mathbb{Z}A_3,$$

bzw. $E(\mathbb{Q}) \simeq \mathbb{Z}^3$?

Geometrische Addition für $y^2 = x^3 + ax + b$:

- E sei also affin gegeben durch $f = 0$ mit $f = x^3 + ax + b - y^2$ bzw. projektiv durch $F = 0$ mit $F = x_1^3 + ax_0^2x_1 + bx_0^3 - x_0x_2^2$ und $O = (0:0:1)$. Wir setzen weiter voraus, dass die Charakteristik $\neq 2, 3$ ist.
- Wann ist E singulär? Es gilt

$$\frac{\partial F}{\partial x_0} = 2ax_0x_1 + 3bx_0^2 - x_2^2, \quad \frac{\partial F}{\partial x_1} = 3x_1^2 + ax_0^2, \quad \frac{\partial F}{\partial x_2} = -2x_0x_2.$$

Wäre $x_0 = 0$, so würde $x_1 = x_2 = 0$ folgen, was nicht geht. Also o.E. $x_0 = 1$ und $x_1 = x$, $x_2 = y$. Es folgt $y = 0$ und $2ax + 3b = 0$, $3x^2 + a = 0$. Für $a = 0$ erhält man $b = 0$ und $x = 0$, für $a \neq 0$ durch Elimination $x = -\frac{3b}{2a}$ und die Bedingung $4a^3 + 27b^2 = 0$. Definiert man

$$\Delta = 4a^3 + 27b^2,$$

so kann man dies zusammenfassen:

$$E \text{ ist singulär} \iff \Delta = 0.$$

- Der einzige unendlich ferne Punkt, d.h. Punkt auf der Geraden $x_0 = 0$ ist O. Damit folgt auch sofort $O' = O$. Die Geraden durch O haben die Form $c_0x_0 + c_1x_1 = 0$, außer x_0 sind dies also die Geraden $x = c$ mit $c \in \overline{K}$.
- Was ist $\ominus P$ für $P = (x_0, y_0)$? Die Gerade durch P und O' hat die affine Gleichung $x = x_0$, einsetzen in f liefert

$$f(x_0, y) = x_0^3 + ax_0 + b - y^2 = y_0^2 - y^2 = -(y - y_0)(y + y_0).$$

Also ist der 3. Punkt auf der Geraden $(x_0, -y_0)$ und es folgt

$$\ominus(x_0, y_0) = (x_0, -y_0).$$

- Seien $P_1 = (x_1, y_1)$ und $P_2 = (x_,y_2)$ Punkte auf E. Wir wollen $P_1 \oplus P_2$ berechnen. Gilt $x_1 = x_2$ und $y_2 = -y_1$, so ist $P_1 \oplus P_2 = O$, also können wir voraussetzen, dass dieser Fall nicht vorliegt. Im Fall $x_1 = x_2$ ist also $y_1 = y_2 \neq 0$.
- Sei $y = \lambda x + \mu$ die Gerade und P_1 und P_2. Zunächst ist immer $\mu = y_1 - \lambda x_1$. Ist $P_1 \neq P_2$, so ist

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}.$$

Ist $P_1 = P_2$, so müssen wir die Tangente berechnen, also

$$\frac{\partial f}{\partial x}(P_1)(x - x_1) + \frac{\partial f}{\partial y}(P_1)(y - y_1) = 0,$$

bzw.

$$y - y_1 = \frac{3x_1^2 + a}{2y_1}(x - x_1),$$

woraus sofort

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

folgt.

P	Punkt	$P = n_1A_1 + n_2A_2 + n_3A_3$
$P1a$	$(1:0:0)$	$0,0,0$
$P1b$	$(1:0:1)$	$1,0,0$
$P1c$	$(0:1:1)$	$0,2,-1$
$P1d$	$(1:1:-1)$	$0,1,0$
$P3a$	$(1:1:3)$	$1,-2,0$
$P3b$	$(2:-3:3)$	$1,-1,0$
$P4$	$(3:-4:2)$	$0,0,1$
$P5a$	$(4:-5:-1)$	$0,-2,1$
$P5b$	$(5:-3:-3)$	$1,-2,1$
$P5c$	$(5:-4:-3)$	$-1,2,0$
$P6$	$(5:6:-3)$	$1,0,-1$
$P9$	$(1:6:9)$	$0,-1,1$
$P11$	$(11:-4:-6)$	$1,1,-1$
$P12$	$(7:12:-2)$	$1,-3,1$
$P13$	$(3:8:-13)$	$0,-1,0$
$P21$	$(19:-21:-9)$	$0,1,-1$
$P22$	$(22:-3:-9)$	$0,2,0$
$P46$	$(19:-36:46)$	$-1,3,-1$
$P48$	$(1:-48:-36)$	$2,-2,0$
$P49$	$(4:49:21)$	$1,-1,1$
$P51$	$(7:-33:51)$	$-1,0,1$
$P54$	$(41:-54:9)$	$0,3,-1$
$P57$	$(22:57:3)$	$-1,1,0$
$P75$	$(19:75:15)$	$1,2,-1$
$P92$	$(11:92:34)$	$0,0,-1$
$P101$	$(101:-3:69)$	$-1,4,-1$
$P120$	$(120:-1:23)$	$2,-4,1$
$P135$	$(47:-100:135)$	$1,-4,2$
$P147$	$(109:-147:91)$	$1,2,-2$
$P152$	$(152:-3:53)$	$-1,1,1$
$P159$	$(79:30:159)$	$-1,2,-1$
$P187$	$(76:121:-187)$	$2,0,-1$
$P189$	$(170:189:-117)$	$0,-2,2$
$P205$	$(205:-51:-101)$	$-1,0,0$
$P209$	$(209:-196:-119)$	$2,-3,0$
$P236$	$(236:-9:-61)$	$1,-1,-1$
$P311$	$(311:-4:79)$	$0,3,-2$
$P312$	$(-7:-192:312)$	$1,1,0$
$P319$	$(319:-42:-129)$	$1,-4,1$
$P324$	$(-211:-240:324)$	$0,4,-2$
$P336$	$(1:336:204)$	$-1,3,0$

$\mathbb{Q}$-rationale Punkte der Höhe ≤ 340 auf

$$E = \{3x_0^2x_1 + x_0x_1^2 + 3x_0x_1x_2 + x_0x_2^2 - x_1^3 + 2x_1^2x_2 - x_2^3 = 0\}.$$

- Wir berechen den 3. Schnittpunkt $(\widetilde{x}, \widetilde{y})$ mit der Geraden und setzen dazu $y = \lambda x + \mu$ in f ein:

  $$f(x, \lambda x + \mu) = x^3 + ax + b - (\lambda x + \mu)^2 = x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + (b - \mu^2).$$

  Dies muss gleich dem Polynom

  $$(x - x_1)(x - x_2)(x - \widetilde{x}) = x^3 - (x_1 + x_2 + \widetilde{x})x^2 + \ldots$$

sein, woraus durch Koeffizientenvergleich bei x^2 sofort

$$\widetilde{x} = \lambda^2 - x_1 - x_2 \text{ und damit } \widetilde{y} = \lambda\widetilde{x} + \mu$$

folgt. Der 3. Schnittpunkt auf der Verbindungsgeraden von $(\widetilde{x}, \widetilde{y})$ und O ist $(\widetilde{x}, -\widetilde{y})$, also folgt schließlich für $(x_3, y_3) = (x_1, y_1) \oplus (x_2, y_2)$:

$$x_3 = \lambda^2 - x_1 - x_2 \text{ und } y_3 = -\lambda x_3 - \mu.$$

- Damit sieht man jetzt auch: $P_1 \oplus P_2 \oplus P_3 = O$ genau dann, wenn P_1, P_2, P_3 auf einer Geraden liegen.

Wir fassen das Ergebnis zusammen:

SATZ. *In Charakteristik $\neq 2, 3$ ist die Kurve $y^2 = x^3 + ax + b$ genau dann nichtsingulär, wenn $\Delta = 4a^3 + 27b^2 \neq 0$ gilt. In diesem Fall ist E mit dem Punkt $O = (0 : 0 : 1)$ eine elliptische Kurve, für die das Additionsgesetz wie folgt aussieht, wenn (x_i, y_i) Punkte auf E sind.*

$$\begin{aligned}
\ominus(x_1, y_1) &= (x_1, -y_1) \\
(x_1, y_1) \oplus (x_1, -y_1) &= O \\
(x_1, y_1) \oplus (x_2, y_2) &= (x_3, y_3) \textit{ mit} \\
&\quad x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = -\lambda x_3 - y_1 + \lambda x_1 \textit{ und} \\
&\quad \lambda = \left\{ \begin{array}{cc} \frac{y_1 - y_2}{x_1 - x_2} & \textit{für } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \textit{für } x_1 = x_2 \textit{ und } y_1 = y_2 \neq 0. \end{array} \right\}
\end{aligned}$$

Außerdem gilt: $P_1 \oplus P_2 \oplus P_3 = O$ genau dann, wenn $[P_1] + [P_2] + [P_3]$ ein Geradenschnitt ist.

Beispiel: Sei E gegeben durch $y^2 = x^3 + 17$. Man findet $P = (-2, 3) \in E$ und rechnet mit den Formeln dann nach

$$P \oplus P = (8, -23), \quad P \oplus P \oplus P = (\frac{19}{25}, \frac{522}{125}).$$

Man suche mit dem Computer weitere Punkte und versuche die Gruppenstruktur von $E(\mathbb{Q})$ zu erraten.

Allgemeine Additionstheoreme: Ist E eine elliptische Kurve in Charakteristik $\neq 2, 3$, gegeben durch eine Gleichung $y^2 = x^3 + ax + b$ (mit $\Delta = 4a^3 + 27b^2 \neq 0$), so geben folgende Formeln die Addition an:

$$(z_{i0} : z_{i1} : z_{i2}) = (x_0 : x_1 : x_2) \oplus (y_0 : y_1 : y_2).$$

(Für jeden Punkt $P \in E$ gibt es mindestens ein i mit $(z_{i0}(P), z_{i1}(P), z_{i2}(P)) \neq 0$.)

```
z10 := a*x0^2*y0*y1-a*x0*x1*y0^2-x0^2*y2^2+x2^2*y0^2+3*x0*x1*y1^2
       -3*x1^2*y0*y1;
z11 := -3*b*x0^2*y0*y1+3*b*x0*x1*y0^2-a*x0^2*y1^2+a*x1^2*y0^2
       -x0*x1*y2^2+x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
z12 := 3*b*x0^2*y0*y2-3*b*x0*x2*y0^2+a*x0^2*y1*y2-a*x1*x2*y0^2
       +2*a*x0*x1*y0*y2-2*a*x0*x2*y0*y1-x0*x2*y2^2+x2^2*y0*y2
       +3*x1^2*y1*y2-3*x1*x2*y1^2;

z20 := 3*b*x0^2*y0*y1-3*b*x0*x1*y0^2+a*x0^2*y1^2-a*x1^2*y0^2
       +x0*x1*y2^2-x2^2*y0*y1+2*x0*x2*y1*y2-2*x1*x2*y0*y2;
z21 := a^2*x0^2*y0*y1-a^2*x0*x1*y0^2-3*b*x0^2*y1^2+3*b*x1^2*y0^2
       -a*x0*x1*y1^2+a*x1^2*y0*y1+x1^2*y2^2-x2^2*y1^2;
z22 := -a^2*x0^2*y0*y2+a^2*x0*x2*y0^2+3*b*x0^2*y1*y2-3*b*x1*x2*y0^2
       +6*b*x0*x1*y0*y2-6*b*x0*x2*y0*y1+2*a*x0*x1*y1*y2
       -2*a*x1*x2*y0*y1-a*x0*x2*y1^2+a*x1^2*y0*y2+x1*x2*y2^2-x2^2*y1*y2;

z30 := 6*b*x0*x2*y0^2+6*b*x0^2*y0*y2+2*a*x1*x2*y0^2+2*a*x0^2*y1*y2
       +4*a*x0*x2*y0*y1+4*a*x0*x1*y0*y2+2*x2^2*y0*y2+2*x0*x2*y2^2
       +6*x1*x2*y1^2+6*x1^2*y1*y2;
z31 := 2*a^2*x0*x2*y0^2+2*a^2*x0^2*y0*y2-6*b*x1*x2*y0^2-6*b*x0^2*y1*y2
```

```
       -12*b*x0*x2*y0*y1-12*b*x0*x1*y0*y2-4*a*x1*x2*y0*y1
       -4*a*x0*x1*y1*y2-2*a*x1^2*y0*y2-2*a*x0*x2*y1^2+2*x2^2*y1*y2
       +2*x1*x2*y2^2;
z32 := -2*x0^2*y0^2*a^3-18*x0^2*y0^2*b^2-6*a*b*x0*x1*y0^2
       -6*a*b*x0^2*y0*y1-2*a^2*x1^2*y0^2-2*a^2*x0^2*y1^2
       -8*a^2*x0*x1*y0*y1+18*b*x1^2*y0*y1+18*b*x0*x1*y1^2+6*a*x1^2*y1^2
       +2*x2^2*y2^2;
```

Außerdem gilt:

$$\ominus(x_0 : x_1 : x_2) = (x_0 : x_1 : -x_2).$$

Damit erhält man:

FOLGERUNG. *Auf einer elliptischen Kurve E sind die Addition $E \times E \to E$ und die Inversenbildung $E \to E$ Morphismen.*

Indem man einen Punkt fest einsetzt, folgt:

FOLGERUNG. *Ist (E, O) eine elliptische Kurve und $P_0 \in E$, so ist die Translation*

$$\tau_{P_0} : E \to E, \quad P \mapsto P \oplus P_0$$

ein Isomorphismus. Es ist $\tau_{P_0}^{-1} = \tau_{\ominus P_0}$.

3. Isomorphie elliptischer Kurven

Wir wollen uns jetzt der Frage zuwenden, wieweit die Weierstraßgleichung einer elliptischen Kurve eindeutig bestimmt ist.

(1) Seien (E, O) und (E', O') zwei elliptische Kurven in Weierstraßgleichung: $y^2 = x^3 + ax + b$ und $y'^2 = x'^3 + a'x' + b'$ und $\phi : E \to E'$ ein Isomorphismus. Indem wir ϕ eventuell um eine Translation abändern, können wir $\phi(O) = O'$ annehmen.

(2) Es ist

$$\mathcal{L}(2[O]) = \overline{K} + \overline{K}x \text{ und } \mathcal{L}(2[O']) = \overline{K} + \overline{K}x'$$

und

$$\mathcal{L}(3[O]) = \overline{K} + \overline{K}x + \overline{K}y \text{ und } \mathcal{L}(3[O']) = \overline{K} + \overline{K}x' + \overline{K}y'.$$

Da ϕ ein Isomorphismus ist, hat $\phi^*([O'])$ Grad 1, also $\phi^*([O']) = [O]$. Daher gilt für $n \in \mathbb{N}$ und $f \in \overline{K}(E')$:

$$f \in \mathcal{L}(n[O']) \Rightarrow \operatorname{div}(f) + n[O'] \geq 0 \Rightarrow 0 \leq \operatorname{div}(\phi^* f) + n[O] \Rightarrow \phi^* f \in \mathcal{L}(n[O]).$$

Wendet man dies für $n = 2, 3$ an, so sieht man, dass es $v, v_1, w, w_1, w_2 \in K$ gibt mit $v, w \neq 0$ und

$$\phi^* x' = x'' = vx + v_1 \text{ und } \phi^* y' = y'' = wy + w_1 x + w_2.$$

Natürlich gilt $y''^2 = x''^3 + a'x'' + b''$. Andererseits ist $y^2 = x^3 + ax + b$ die kleinste Relation zwischen x und y. Durch Einsetzen sieht man sofort, dass keine Terme xy und y auftreten, was $w_1 = w_2 = 0$ ergibt. Da auch kein Term x^2 auftritt, folgt auch $v_1 = 0$. Also bleibt $x'' = vx$ und $y'' = wy$. Wir setzten jetzt ein:

$$\begin{aligned} 0 &= x''^3 + a'x'' + b' - y''^2 = v^3x^3 + a'vx + b' - w^2y^2 = \\ &= v^3x^3 + a'vx + b' - w^2(x^3 + ax + b) = \\ &= (v^3 - w^2)x^3 + (a'v - w^2a)x + (b' - w^2b), \end{aligned}$$

was durch Koeffizientenvergleich sofort

$$v^3 = w^2, \quad a'v = w^2a, \quad b' = w^2b$$

ergibt. Setzt man $u = \frac{w}{v}$, so ergibt sich

$$u^2 = v, \quad u^3 = w \text{ und } a' = u^4a, \quad b' = u^6b.$$

(3) Gilt umgekehrt für ein $u \in K$, $u \neq 0$:

$$a' = u^4 a, \quad b' = u^6 b,$$

so führt der Koordinatenwechsel $(x, y) \mapsto (u^2 x, u^3 y)$ die Kurve E in E' über.

Damit haben wir bewiesen:

SATZ. *Zwei elliptische Kurven $E : y^2 = x^3 + ax + b$ und $E' : y^2 = x^3 + a'x + b'$ sind genau dann über K isomorph, wenn es ein $u \in K^*$ gibt mit*

$$a' = u^4 a \text{ und } b' = u^6 b.$$

In diesem Fall liefert $(x, y) \mapsto (u^2 x, u^3 y)$ einen Isomorphismus $E \to E'$.

Wir werden nun eine wichtige Invariante einführen: Ist E eine elliptische Kurve und sind $y^2 = x^3 + ax + b$ und $y^2 = x^3 + a'x + b'$ zwei Weierstraßgleichungen für E, so gibt es also ein $u \in K$ mit $a' = u^4 a$ und $b' = u^6 b$. Für die Diskriminanten gilt:

$$\Delta' = 4a'^3 + 27b'^2 = u^{12}\Delta \neq 0$$

und damit

$$\frac{4a'^3}{4a'^3 + 27b'^2} = \frac{4a^3}{4a^3 + 27b^2}.$$

Daher ist dieser Ausdruck unabhängig von der Auswahl der Weierstraßgleichung und man definiert:

DEFINITION. *Ist E eine elliptische Kurve in Charakteristik $\neq 2, 3$ und $y^2 = x^3 + ax + b$ eine beschreibende Weierstraßgleichung, so definiert man die j-Invariante von E durch*

$$j = j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Aus obiger Überlegung folgt auch sofort:

FOLGERUNG. *Sind E und E' zwei über K isomorphe elliptische Kurven, so gilt: $j(E) = j(E')$.*

Elliptische Kurven zu vorgebener j-Invariante: Sei also $j \in K$ gegeben. Wir wollen sehen, ob es dazu elliptische Kurven gibt, und wie diese aussehen.

(1) Wir gehen aus von $j = 1728 \frac{4a^3}{4a^3 + 27b^2}$. Zunächst ist klar:

$$j = 0 \iff a = 0 \quad \text{und} \quad j = 1728 \iff b = 0.$$

(2) Wir setzen also jetzt $j \neq 0, 1728$ voraus. Dann haben wir die Umformungen:

$$\begin{aligned} j = 1728 \frac{4a^3}{4a^3 + 27b^2} &\iff 4ja^3 + 27jb^2 = 1728 \cdot 4a^3 \\ &\iff 27jb^2 = 4(1728 - j)a^3 \\ &\iff (\frac{b}{2})^2 = \frac{1728 - j}{j} (\frac{a}{3})^3 \text{ und nach Multiplikation mit } (\frac{1728 - j}{j})^2 \\ &\iff (\frac{1728 - j}{2j} b)^2 = (\frac{1728 - j}{3j} a)^3. \end{aligned}$$

Also gibt es wie üblich ein $t \in K$ mit

$$\frac{1728 - j}{2j} b = t^3, \quad \frac{1728 - j}{3j} a = t^2$$

oder anders geschrieben

$$a = \frac{3j}{1728 - j} t^2, \quad b = \frac{2j}{1728 - j} t^3.$$

(3) Wann liefern t_1 und t_2 eine isomorphe Kurve? Genau dann, wenn es ein $u \in K^\times$ gibt mit

$$u^4 = \frac{a_{t_1}}{a_{t_2}} = (\frac{t_1}{t_2})^2 \quad \text{und} \quad u^6 = \frac{b_{t_1}}{b_{t_2}} = (\frac{t_1}{t_2})^3,$$

was nach Divison mit

$$u^2 = \frac{t_1}{t_2}$$

äquivalent ist.

Damit erhalten wir folgenden Satz:

SATZ. (1) *Ist $j \in K$ und $j \neq 0, 1728$, so haben genau die Kurven E_t mit $y^2 = x^3 + a_t x + b_t$ und*

$$a_t = \frac{3j}{1728 - j} t^2, \quad b_t = \frac{2j}{1728 - j} t^3, \quad t \in K^*$$

j-Invariante j. Weiterhin sind E_{t_1} und E_{t_2} genau dann isomorph über K, wenn es ein $u \in K$ gibt mit $t_2 = u^2 t_1$. Ist $t_\alpha, \alpha \in A$ ein Repräsentantensystem der Gruppe K^*/K^{*2}, so repräsentieren die Kurven E_{t_α} alle Isomorphieklassen elliptischer Kurven über K mit j-Invariante j.

(2) *Ist $j = 0$, so haben genau die Kurven E_b mit $y^2 = x^3 + b$ j-Invariante 0. Zwei Kurven E_{b_1} und E_{b_2} sind genau dann isomorph über K, wenn es ein $u \in K, u \neq 0$ gibt mit $b_2 = u^6 b_1$. Repräsentieren $b_\beta, \beta \in B$ die Klassen K^*/K^{*6}, so die Kurven E_β die Isomorphieklassen elliptischer Kurven über K mit j-Invariante 0.*

(3) *Ist $j = 1728$, so haben genau die Kurven E_a mit $y^2 = x^3 + ax$ j-Invariante 1728. Zwei Kurven E_{a_1} und E_{a_2} sind genau dann isomorph über K, wenn es ein $u \in K, u \neq 0$ gibt mit $a_2 = u^6 a_1$. Repräsentieren $a_\alpha, \alpha \in A$ die Klassen K^*/K^{*4}, so die Kurven E_α die Isomorphieklassen elliptischer Kurven über K mit j-Invariante 1728.*

FOLGERUNG. *Für elliptische Kurven E und E' gilt:*

$$E \sim_{\overline{K}} E' \quad \Longleftrightarrow \quad j(E) = j(E').$$

Beispiel: Für $K = \mathbb{R}$ gilt

$$\mathbb{R}^{*2} = \mathbb{R}^{*4} = \mathbb{R}^{*6} = \{r \in \mathbb{R} : r > 0\},$$

modulo zweiten, vierten und sechsten Potenzen bilden ± 1 ein Repräsentantensystem. Also erhält man folgendes Repräsentantensystem für die elliptischen Kurven über $\mathbb{R}$, wo j alle reellen Zahlen durchläuft:

$$\begin{aligned} j \neq 0, 1728: &\quad y^2 = x^3 + \frac{3j}{1728 - j} x + \frac{2j}{1728 - j} \text{ und } y^2 = x^3 + \frac{3j}{1728 - j} x - \frac{2j}{1728 - j} \\ j = 0: &\quad y^2 = x^3 + 1 \text{ und } y^2 = x^3 - 1 \\ j = 1728: &\quad y^2 = x^3 + x \text{ und } y^2 = x^3 - x \end{aligned}$$

Beispiel: Für $K = \mathbb{F}_5$ gilt

$$\mathbb{F}_5^{*2} = \{1, 4\}, \quad \mathbb{F}_5^{*4} = \{1\}, \quad \mathbb{F}_5^{*6} = \{1, 4\},$$

also

$$\mathbb{F}_5^*/\mathbb{F}_5^{*2} = \{\overline{1}, \overline{2}\}, \quad \mathbb{F}_5^*/\mathbb{F}_5^{*4} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}, \quad \mathbb{F}_5^*/\mathbb{F}_5^{*6} = \{\overline{1}, \overline{2}\}.$$

Damit erhält man folgende Tabelle:

j	Kurven E mit Anzahl von Punkten $\#E(\mathbb{F}_5)$
0	$y^2 = x^3 + 1 (N = 6), \quad y^2 = x^3 + 2 (N = 6)$
1	$y^2 = x^3 + 4x + 1 (N = 8), \quad y^2 = x^3 + x + 3 (N = 4)$
2	$y^2 = x^3 + x + 4 (N = 9), \quad y^2 = x^3 + 4x + 2 (N = 3)$
$1728 = 3$	$y^2 = x^3 \pm x (N = 4, 8), \quad y^2 = x^3 \pm 2x (N = 2, 10)$
4	$y^2 = x^3 + 3x + 2 (N = 5), \quad y^2 = x^3 + 2x + 1 (N = 7)$

(Beachte die symmetrische Verteilung der Anzahlen um 6.)

Aufgabe: Gib für $\mathbb{F}_{53}$ ein Repräsentantensystem der Isomorphieklassen elliptischer Kurven an und bestimme jeweils $\#E(\mathbb{F}_{53})$.

Beispiel: $K = \mathbb{F}_p$ ein endlicher Körper mit $p \geq 5$. Bezeichnet A die Anzahl der Isomorphieklassen elliptischer Kurven über $\mathbb{F}_p$, so gilt offensichtlich

$$A = (p-2)\#\mathbb{F}_p^*/\mathbb{F}_p^{*2} + \#\mathbb{F}_p^*/\mathbb{F}_p^{*4} + \#\mathbb{F}_p^*/\mathbb{F}_p^{*6}.$$

Der Kern der Abbildung $\mathbb{F}_p^* \overset{x\mapsto x^n}{\to} \mathbb{F}_p^*$ hat $ggT(p-1,n)$ Elemente, da $\mathbb{F}_p^*$ zyklisch ist. Daher gilt auch $\#\mathbb{F}_p^*/\mathbb{F}_p^{*n} = \mathrm{ggT}(p-1,n)$. Damit erhält man

$$A = 2(p-2) + \left\{ \begin{array}{lll} 10 & \text{für} & p \equiv 1 \bmod 12 \\ 6 & \text{für} & p \equiv 5 \bmod 12 \\ 8 & \text{für} & p \equiv 7 \bmod 12 \\ 4 & \text{für} & p \equiv 11 \bmod 12 \end{array} \right\}$$

4. Morphismen zwischen elliptischen Kurven

Wir wollen jetzt Morphismen zwischen elliptischen Kurven betrachten. Es gilt der wichtige Satz:

SATZ. *Seien (E_1, O_1) und (E_2, O_2) elliptische Kurven und $\phi : E_1 \to E_2$ ein nichtkonstanter Morphismus. Gilt $\phi(O_1) = O_2$, dann ist ϕ ein Gruppenhomomorphismus. Man nennt ϕ eine* **Isogenie** *und die Kurven E_1 und E_2* **isogen**.

FOLGERUNG. *Sind (E_1, O_1) und (E_2, O_2) elliptische Kurven und $\phi : E_1 \to E_2$ ein nichtkonstanter Morphismus, dann gibt es eine Isogenie ψ und eine Translation τ mit $\phi = \tau \circ \psi$.*

Zum Beweis des Satzes brauchen wir ein Lemma:

LEMMA. *Sei $\phi : C_1 \to C_2$ ein nichtkonstanter Morphismus zwischen Kurven. Dann gilt*

$$\phi_*(\textit{Hauptdivisor}) = \textit{Hauptdivisor}.$$

Beweisskizze: Wir beschränken uns auf den Fall, dass $\overline{K}(C_1)$ über $\overline{K}(C_2)$ galoissch ist mit Galoisgruppe G. Dann operiert G auch auf C_1. Insbesondere gilt für jeden Punkt $P \in C_1$:

$$\phi^*\phi_*[P] = \sum_{\sigma\in G} [\sigma P].$$

Sei $f \in \overline{K}(C_1)^*$ und $\mathrm{div}(f) = \sum_i n_i[P_i]$. Dann gilt

$$\begin{aligned} \phi^*\phi_*(\mathrm{div}(f)) &= \phi^*\phi_*(\sum_i n_i[P_i]) = \sum_i n_i\phi^*\phi_*[P_i] = \sum_i n_i \sum_{\sigma\in G}[\sigma P_i] = \sum_{\sigma\in G}\sigma(\sum_i n_i[P_i]) = \\ &= \sum_{\sigma\in G}\sigma(\mathrm{div}(f)) = \sum_{\sigma\in G}\mathrm{div}(\sigma f) = \mathrm{div}(\prod_{\sigma\in G}\sigma f). \end{aligned}$$

Nun ist aber $g = \prod_{\sigma\in G}\sigma f \in \overline{K}(C_2)$, also folgt $\phi^*\phi_*(\mathrm{div}(f)) = \phi^*(\mathrm{div}(g))$ und damit $\phi_*(\mathrm{div}(f)) = \mathrm{div}(g)$, also die Behauptung. ■

Beweis des Satzes: Zu zeigen ist für $P_1, P_2, P_3 \in E_1$:

$$P_1 \oplus P_2 = P_3 \quad \Rightarrow \quad \phi(P_1) \oplus \phi(P_2) = \phi(P_3).$$

Sei also $P_1 \oplus P_2 = P_3$. Dies bedeutet $[P_1] + [P_2] \sim [P_3] + [O_1]$ und damit $[P_1] + [P_2] - [P_3] - [O_1] \sim 0$, d.h. $[P_1] + [P_2] - [P_3] - [O_1]$ ist Hauptdivisor. Nach dem Lemma gilt dann

$$0 \sim \phi_*([P_1] + [P_2] - [P_3] - [O_1]) = [\phi(P_1)] + [\phi(P_2)] - [\phi(P_3)] - [O_2],$$

was auf die gleiche Weise wieder $\phi(P_1) \oplus \phi(P_2) = \phi(P_3)$ liefert, also die Behauptung. ■

Ist A eine abelsche Gruppe, so bilden die Endomorphismen $\phi : A \to A$ einen Ring durch die Definitionen

$$\begin{aligned} 0(a) &= 0, \\ 1(a) &= \mathrm{id}_A(a) = a, \\ (\phi_1 + \phi_2)(a) &= \phi_1(a) + \phi_2(a), \\ (\phi_1\phi_2)(a) &= \phi_1(\phi_2(a)). \end{aligned}$$

Dies überträgt sich sofort auf elliptische Kurven:

DEFINITION. *Ist (E, O) eine elliptische Kurve, so ist*

$$\mathrm{End}(E) = \{\phi : E \to E \text{ über } \overline{K} \text{ definierter Morphismus mit } \phi(O) = O\}$$

ein Ring, der sogenannte **Endomorphismenring von** E. *Betrachtet man nur über K definierte Morphismen, so schreibt man* $\mathrm{End}_K(E)$. *Die Einheitengruppe von* $\mathrm{End}(E)$

$$\mathrm{Aut}(E) = \{\phi : E \to E \text{ Isomorphismus mit } \phi(O) = O\}$$

heißt die **Automorphismengruppe von** E.

Wir haben oben für Charakteristik $\neq 2, 3$ gesehen, dass jeder Isomorphismus $\phi : E \to E'$ zwischen elliptischen Kurven mit $\phi(O) = O'$ durch einen Koordinatenwechsel $x \mapsto u^2x, y \mapsto u^3y$, $u \in \overline{K}^*$ gegeben ist. Wann liefert nun eine solche Transformation einen Automorphismus von E? Genau dann, wenn $(x, y) \mapsto (u^2x, u^3y)$ die Kurve E in sich überführt, d.h. die transformierte Gleichung muss identisch erfüllt sein, also:

$$u^6y^2 = u^6x^3 + au^2x + b \text{ bzw. } y^2 = x^3 + \frac{a}{u^4}x + \frac{b}{u^6},$$

was sofort die Bedingung $a = u^4a, b = u^6b$ liefert. Damit ergibt sich sofort folgender Satz:

SATZ. *In Charakteristik $\neq 2, 3$ gilt für eine elliptische Kurve E:*

(1) *Ist $j(E) \neq 0, 1728$, so ist*
$$\mathrm{Aut}(E) = \{P \mapsto P, P \mapsto -P\} \simeq \mathbb{Z}/(2).$$
(2) *Ist $j(E) = 1728$ (Typ $y^2 = x^3 + ax$), so ist*
$$\begin{aligned} \mathrm{Aut}(E) &= \{(x, y) \mapsto (x, y), (x, y) \mapsto (-x, iy), (x, y) \mapsto (-x, -iy), (x, y) \mapsto (x, -y)\} \\ &\simeq \mathbb{Z}/(4) \text{ mit } i^2 = -1. \end{aligned}$$
(3) *$j(E) = 0$ (Typ $y^2 = x^3 + b$), so ist*
$$\mathrm{Aut}(E) = \{(x, y) \mapsto (x, \pm y), (x, y) \mapsto (\zeta_3 x, \pm y), (x, y) \mapsto (\zeta_3^2 x, \pm y)\} \simeq \mathbb{Z}/(6).$$
mit einer primitiven 3-ten Einheitswurzel ζ_3.

Aufgabe:

(1) Zeige, dass die Kurve $y^2 = x^3 - x$ in Charakteristik 3 eine Automorphismengruppe der Ordnung 12 besitzt.
(2) Zeige, dass $y^2 + y = x^3$ in Charakteristik 2 eine Automorphismengruppe der Ordnung 24 besitzt.

Die Bestimmung von $\mathrm{End}(E)$ ist nicht so einfach. Ist E eine elliptische Kurve und $n \in \mathbb{Z}, n \geq 0$, so ist die Multiplikation mit n

$$E \to E, \quad P \mapsto nP = P \oplus \cdots \oplus P$$

eine Endomorpmismus, der manchmal mit $[n]$ bezeichnet wird. Entsprechend definiert man $[-n]$:

$$E \to E, \quad P \mapsto n(\ominus P) = \ominus P \ominus \cdots \ominus P.$$

Diese Endomorphismen hat man bei jeder elliptischen Kurve.

SATZ. *Sei (E, O) eine elliptische Kurve. Dann gilt:*

(1) *Der Endomorphismenring* $\mathrm{End}(E)$ *ist nullteilerfrei, d.h. $\phi\psi = 0$ impliziert $\phi = 0$ oder $\psi = 0$.*

(2) *Die Abbildung*

$$\mathbb{Z} \to \mathrm{End}(E), \quad n \mapsto [n]$$

ist ein injektiver Ringhomomorphismus. Also kann man immer $\mathbb{Z} \subseteq \mathrm{End}(E)$ *schreiben.*

Beweis:

(1) Sei $\phi\psi = 0$. Ein Morphismus $E \to E$ ist surjektiv oder konstant. Ist ψ surjektiv, so folgt $0 = \phi(\psi(E)) = \phi(E)$, also $\phi = 0$. Ist ψ konstant, so $\psi = 0$ wegen $\psi(O) = O$.

(2) Wir beschränken uns auf elliptische Kurven der Form $y^2 = x^3 + ax + b$ in Charakteristik $\neq 2, 3$. Dass $\mathbb{Z} \to \mathrm{End}(E)$, $n \mapsto [n]$ ein Ringhomomorphismus ist, ist klar. Wir zeigen für jede Primzahl p, dass $[p] \neq 0$ gilt. Dann folgt nach 1. auch $[n] \neq 0$ für jede ganze Zahl $n \geq 0$.
1. Fall $p = 2$*:* Sei $P = (x, y) \in E$ mit $y \neq 0$. Dann gilt $P \neq -P$, also $2P \neq 0$.
2. Fall $p > 2$*:* Sei $e \in \overline{K}$ eine Nullstelle von $x^3 + ax + b$. Dann ist $P = (e, 0) \in E$ mit $P = -P$, also $2P = 0$. Es folgt mit $p = 2m + 1$:

$$pP = m(2P) + P = P \neq 0,$$

also die Behauptung. ■

Man unterscheidet drei Typen von Endomorphismenringen elliptischer Kurven:

(1) $\mathrm{End}(E) = \mathbb{Z}$.

(2) $\mathrm{End}(E)$ ist Unterring eines quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{-d})$ (mit $d \in \mathbb{N}$) und nicht von Typ 1. Man sagt, E hat **komplexe Multiplikation**.

(3) End ist Unterring einer Quaternionenalgebra $Q(a, b)$ und nicht von Typ 1 oder 2. Man sagt, E ist **supersingulär**. Dieser Fall kommt nur in Charakteristik p vor.

Ausführlich wird das Thema in [**Silverman**] behandelt.

Frage: Was kann man über die Struktur von $E(K)$ und $E(\overline{K})$ sagen?

Wir werden auf diese Frage nicht näher eingehen, sondern nur kurz den Fall $K = \mathbb{R}$ betrachten.

5. Elliptische Kurven über $\mathbb{R}$

Wir betrachten E mit $y^2 = x^3 + ax + b$, $a, b \in \mathbb{R}$ und $\Delta = 4a^3 + 27b^2 \neq 0$. Es gibt zwei Fälle:

(1) $x^3 + ax + b$ hat genau eine reelle Nullstelle, die andern beiden sind komplex konjugiert, also

$$x^3 + ax + b = (x - \alpha)(x + \frac{1}{2}\alpha + \beta i)(x + \frac{1}{2}\alpha - \beta i)$$

mit $\alpha, \beta \in \mathbb{R}, \beta \neq 0$, was durch Koeffizientenvergleich

$$a = -\frac{3}{4}\alpha^2 + \beta^2, \quad b = -\frac{1}{4}\alpha^3 - \alpha\beta^2$$

und damit

$$\Delta = \frac{1}{4}\beta^2(9\alpha^2 + 4\beta^2)^2 > 0$$

liefert. Man kann zeigen, dass $E(\mathbb{R})$ zusammenhängend ist, und dass $E(\mathbb{R}) \simeq \mathbb{R}/\mathbb{Z}$ gilt.

(2) $x^3 + ax + b$ hat 3 reelle Nullstellen, also

$$x^3 + ax + b = (x - \alpha)(x - \beta)(x + \alpha + \beta),$$

was sofort

$$a = -\alpha^2 - \alpha\beta - \beta^2, \quad b = \alpha^2\beta + \alpha\beta^2$$

und damit

$$\Delta = -(\alpha + 2\beta)^2(2\alpha + \beta)^2(\alpha - \beta)^2 < 0$$

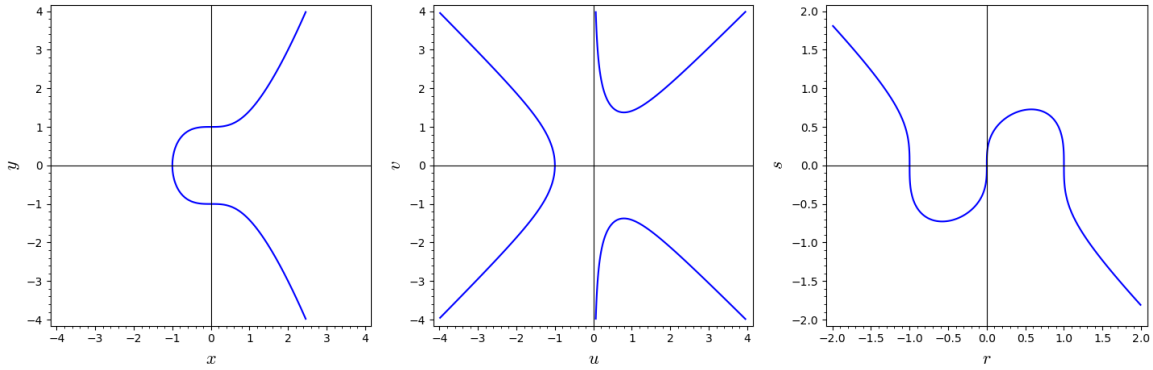
liefert. Man kann zeigen, dass $E(\mathbb{R})$ zwei Zusammenhangskomponenten hat, und dass gilt $E(\mathbb{R}) \simeq \mathbb{Z}/(2) \oplus \mathbb{R}/\mathbb{Z}$.

SATZ. *Ist E mit $y^2 = x^3 + ax + b$ eine elliptische Kurve über $\mathbb{R}$, so gilt*

$$E(\mathbb{R}) \simeq \begin{cases} \mathbb{R}/\mathbb{Z} & \text{für } \Delta > 0 \\ \mathbb{Z}/(2) \oplus \mathbb{R}/\mathbb{Z} & \text{für } \Delta < 0. \end{cases}$$

Beispiele:

(1) $y^2 = x^3 + 1$ mit $\Delta = 27$:



(2) $y^2 = x^3 - x$ mit $\Delta = -4$: