1 Die Punktegruppe

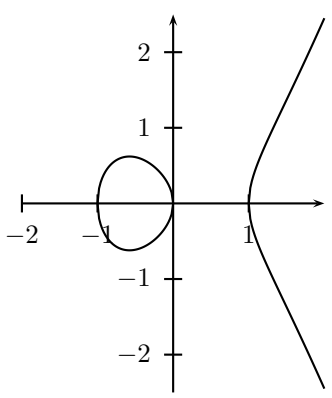
1.1 Elliptische Kurven

Eine *elliptische Kurve* $\mathcal{E}$ über einem Körper $\mathbb{K}$ kann, wenn der Körper nicht die Charakteristik 2 hat, mit der Weierstrass Normalform

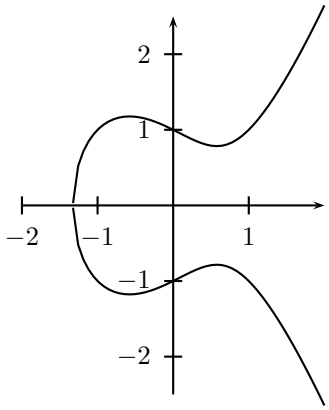
$$\mathcal{E} : y^2 = x^3 + ax^2 + bx + c$$

beschrieben werden. Hierbei sind $a, b, c \in \mathbb{K}$ und das rechte Polynom 3. Grades in x hat keine doppelten Nullstellen.

Beispiel 1. *2 Elliptische Kurven über* $\mathbb{R}$



$\mathcal{E}_1 : y^2 = x^3 - x$



$\mathcal{E}_2 : y^2 = x^3 - x + 1$

Die Menge einer solchen Punktgruppe stellen wir uns wie folgt vor.

Definition 2. ***Menge der Punktegruppe*** $(\mathcal{E}(\mathbb{K}), +)$
Die Punktegruppe einer elliptischen Kurve $\mathcal{E}$ *über* $\mathbb{K}$ *ist die Menge der Punkte, die auf der Kurve liegen und der Fernpunkt* $\mathcal{O} := (\infty, \infty)$.

$$\mathcal{E}(\mathbb{K}) := \left\{P = (x, y) \in \mathbb{K}^2 : y^2 = x^3 + ax^2 + bx + c\right\} \cup \{\mathcal{O}\}$$

Die Operation auf dieser Menge, die wir mit + bezeichnen, wollen wir uns zunächst graphisch vorstellen. Die Summe zweier Punkt P und Q wird dabei konstruiert, indem man eine Gerade $\overline{PQ}$ durch P und Q legt und dann den 3. Schnittpunkt mit $\mathcal{E}$ an der X-Achse spiegelt. Dabei gibt es folgende Ausnahmen zu beachten:

— Addiert man einen Punkt P zu sich selbst ist die Gerade $\overline{PP}$ nicht eindeutig bestimmt. Damit die Addition stetig bleibt nimmt man die Tangente an $\mathcal{E}$ in P.

— Sind P und Q senkrecht übereinander, so hat die Gerade $\overline{PQ}$ und $\mathcal{E}$ keinen dritten Schnittpunkt. Sie schneiden sich im Fernpunkt $\mathcal{O}$.

— Addiert man zu einem Punkt P den Fernpunkt $\mathcal{O}$, dann stellt man sich $\mathcal{O}$ über P vor. Die Gerade $\overline{P\mathcal{O}}$ schneidet also $\mathcal{E}$ genau gegenüber von P und nach dem Spiegeln ergibt die Addition $P + \mathcal{O} = P$.

Was wir uns nun überlegen wollen ist, daß $(\mathcal{E}(\mathbb{K}), +)$ mit der geometrisch beschriebenen Addition wirklich eine *Gruppe* ist. Diese Gruppe ist sogar *kommutativ*.

(i) *Abgeschlossenheit* $+ : \mathcal{E}(\mathbb{K})^2 \to \mathcal{E}(\mathbb{K})$

Da wir mit unserer Addition nie die Menge $\mathcal{E}(\mathbb{K})$ verlassen gibt es hier kein Problem.

(ii) *Neutrales Element* $P + 0 = P$

Schon während der Definition fiel uns auf, daß der Fernpunkt beliebig oft auf einen Punkt addiert werden kann ohne diesen zu ändern. $\mathcal{O}$ ist das neutrale Element.

(iii) *Inverse Elemente* $-P$

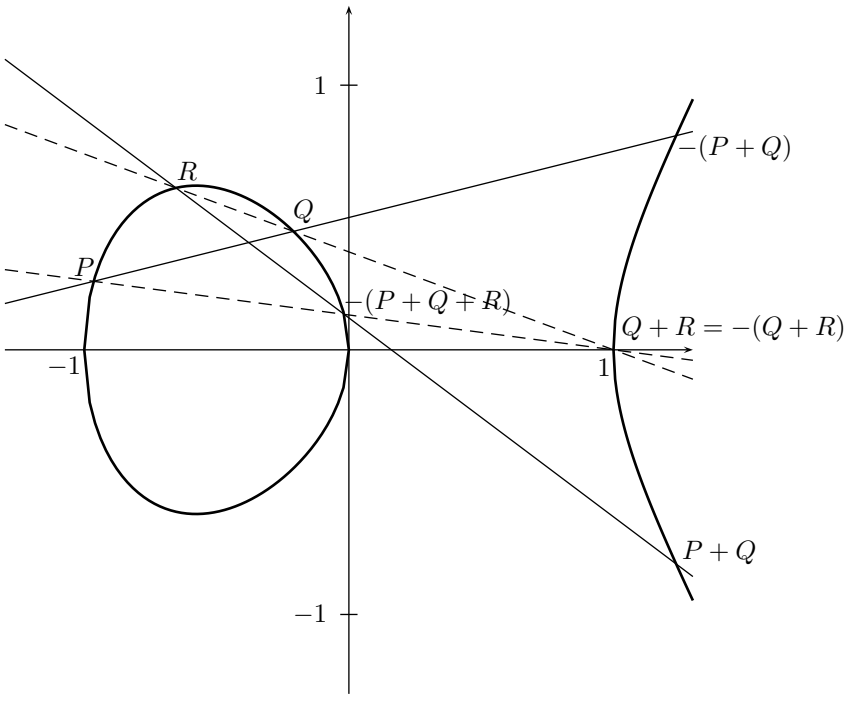
Das inverse Element zu jedem Punkt ist sein Spiegelbild an der X-Achse. Da eine Gerade durch zwei übereinanderliegende Punkte zum Fernpunkt, dem neutralen Element läuft.

(iv) *Kommutativität* $P + Q = Q + P$

Dies gilt weil wir beim Addieren immer als erstes eine Gerade durch Beide Punkte ziehen und die Gerade gleichbleibt, egal mit welchem der beiden Punkte man anfängt.

(v) *Assoziativität* $P + (Q + R) = (P + Q) + R$

Die Assoziativität werden wir uns an einem Bild verdeutlichen, aber nicht formal beweisen, da dies sehr technisch ist.



1.2 Additionsformeln für Charakteristik > 3

Nun werden wir unsere Addition noch genauer über *Additionformeln* beschreiben. Die wohl einfachste Formel beschäftigt sich mit dem Invertieren.

Die **Inversen** Elemente in unserer Gruppe findet man mit einer Spiegelung an der X-Achse, sprich man dreht das Vorzeichen der Y-Koordinate um.

$$-P = -(x_P, y_P) = (x_P, -y_P)$$

Wir wollen uns für diesen Abschnitt auf Elliptische Kurven über einem Körper $\mathbb{K}$ mit Charakteristik größer 3 beschränken, da sich diese in der kurzen Weierstrassform schreiben lassen und damit die Formeln angenehmer werden:

$$\mathcal{E} : y^2 = x^3 + ax + b$$

Das Addieren **verschiedener** Punkte kommt zuerst. Seien $P = (x_P, y_P), Q = (x_Q, y_Q), R = (x_R, y_R)$ im Verhältnis

$$P \neq Q \qquad\qquad P + Q = R$$

dann berechnet sich R wie folgt:

Ist $x_P = x_Q$, sprich die Punkte sind übereinander, dann sind P und Q invers zueinander $R = \mathcal{O}$.

Sonst ist $x_P \neq x_Q$ und wir können die Steigung der Gerade $\overline{PQ}$ berechnen:

$$s = \frac{y_Q - y_P}{x_Q - x_P}$$

R berechnet sich dann aus dieser Steigung s:

$$x_R = s^2 - x_P - x_Q$$
$$y_R = s \cdot (x_P - x_R) - y_P$$

Nun wollen wir 2 **gleiche** Punkte addieren, also einen Punkt verdoppeln. Sei dazu $P = (x_P, y_P), R = (x_R, y_R)$ im Verhältnis

$$2 \cdot P = R$$

Die Steigung der Tangente an $\mathcal{E}$ in P ergibt sich wie folgt:

$$s = \frac{3x_P^2 + a}{2y_P}$$

ist y_P hier 0, dann sind steht die Tangente senkrecht und schneidet $\mathcal{E}$ nicht mehr $R = \mathcal{O}$. Sonst kann man aus der Steigung genau wie zuvor auch R berechnen:

$$x_R = s^2 - 2x_P$$

$$y_R = s \cdot (x_P - x_R) - y_P$$

1.3 Additionsformeln für Charakteristik $= 2$

Zuletzt überlegen wir uns noch, daß das Finden des Punktes $P + Q$ letztlich dem Lösen eines nichtlinearen Gleichungsystems entspricht. Man sucht nämlich den Punkte, der die (lineare) Geradengleichung, beschrieben durch P und Q, erfüllt und auch die (nichtlineare) Gleichung, die alle Punkte auf der Elliptische Kurve charakterisiert.

Die Berechnung von **Inversen** ist in dieser Gruppe etwas anders als vorher:

$$-P = (x_P, y_P + x_P)$$

Für Körper der Charakteristik 2 muß man den Begriff von „Gerade durch P und Q“ in diesem Kontext erweitern und daraus ergeben sich dann die nun folgenden Formeln. Elliptische Kurven über diesen Körpern lassen sich auch nicht in die zum Rechnen angenehme kurze Weierstrassform bringen, sondern sie werden beschrieben mit:

$$\mathcal{E} : y^2 + xy = x^3 + ax^2 + b$$

Das Addieren **verschiedener** Punkte kommt erneut zuerst. Seien $P = (x_P, y_P), Q = (x_Q, y_Q), R = (x_R, y_R)$ im Verhältnis

$$P \neq Q \qquad\qquad P + Q = R$$

dann berechnet sich R wie folgt:

$$s := \frac{y_P + y_Q}{x_P + x_Q}$$

$$x_R = s^2 + s + x_P + x_Q + a$$

$$y_R = s \cdot (x_P + x_R) + x_R + y_P$$

Für das Addieren von zwei **gleichen** Punkten, also die Verdoppelung von $P = (x_P, y_P)$

$$2 \cdot P = R$$

ergibt sich:

$$s = \frac{x_P + y_p}{x_P}$$

$$x_R = s^2 + s + a = x_P^2 + \frac{b}{x_P^2}$$

$$y_R = x_P^2 + s \cdot x_R + x_R$$