9. Woche: Elliptische Kurven - Gruppenarithmetik

Elliptische Kurven

Definition Elliptische Kurve

Eine **elliptische Kurve** E über dem Körper K ist eine „nichtsinguläre“ Kurve, gegeben durch eine Gleichung der Form

$$E \quad : \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

oder, mit anderen Worten

$$F(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$$

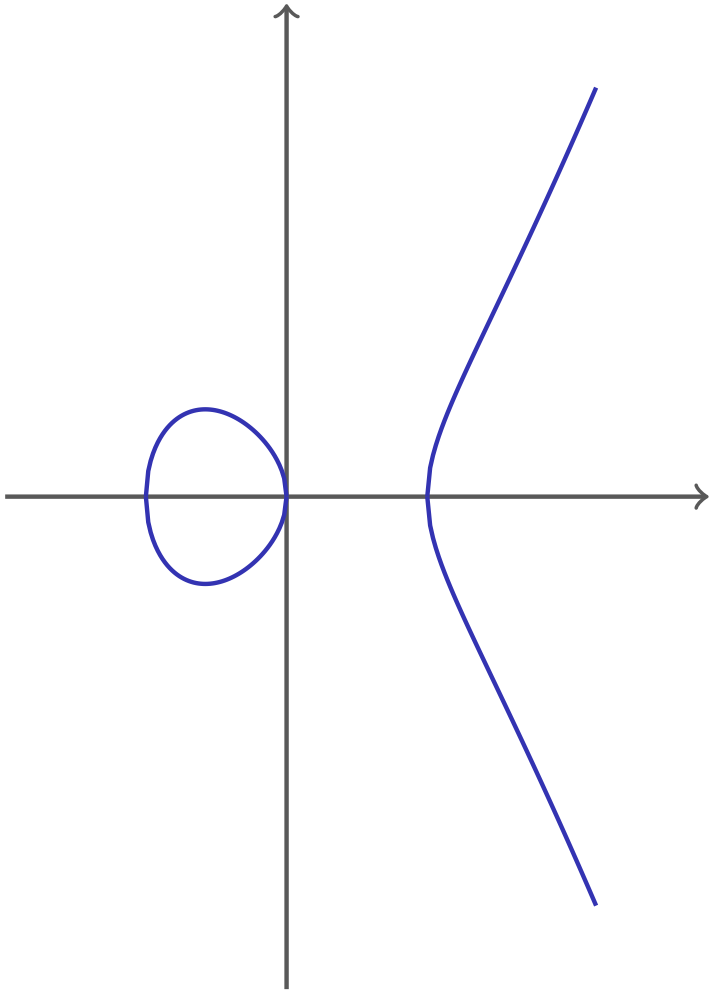
wobei a_1, a_2, a_3, a_4 und a_6 Elemente aus K sind.

Wie sehen solche Kurven aus?

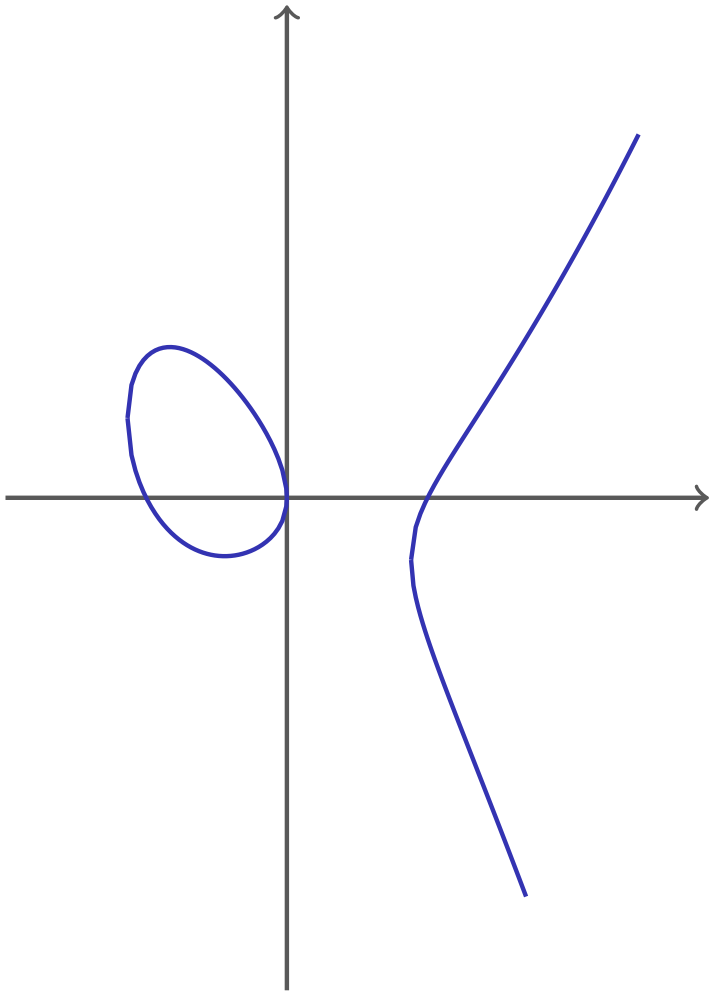
Was bedeutet *singulär* oder *nichtsingulär*?

Elliptische Kurven (über $\mathbb{R}$) I

$$y^2 = x^3 - x$$

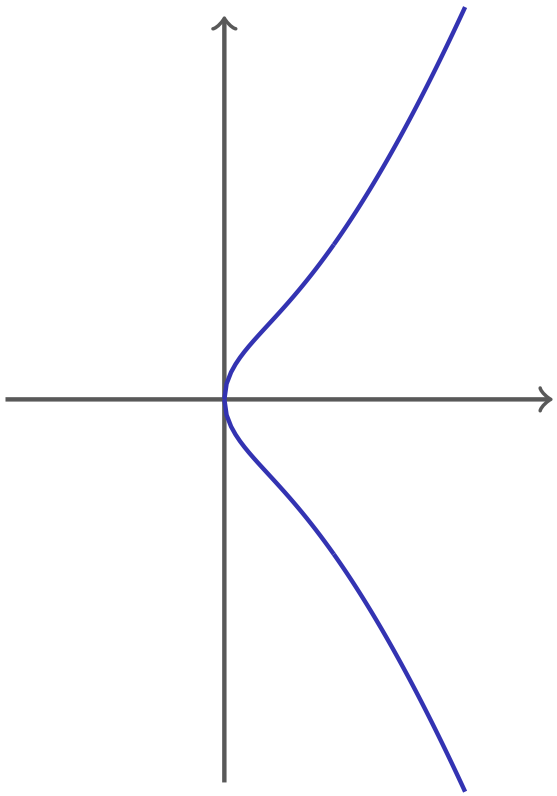


$$y^2 + xy = x^3 - x - 1/4$$

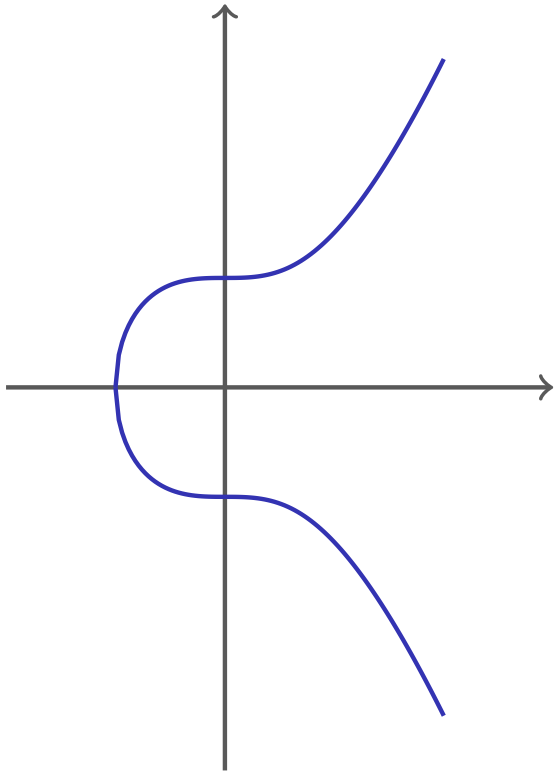


Elliptische Kurven (über $\mathbb{R}$) II

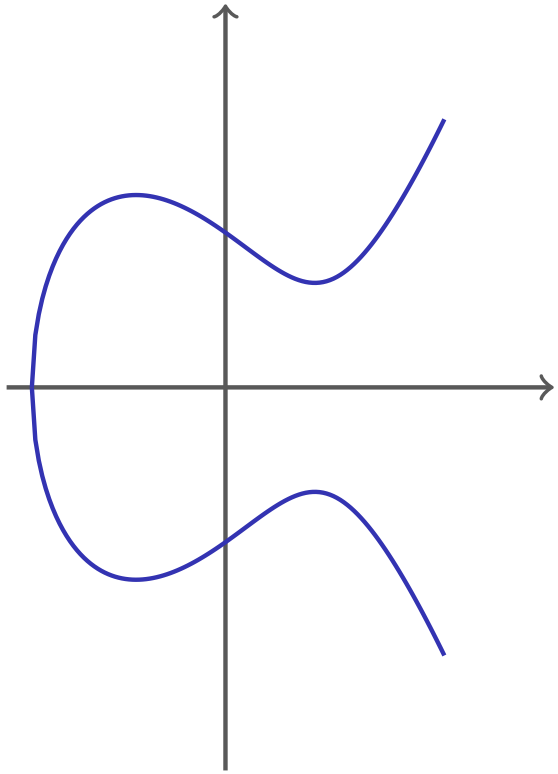
$y^2 = x^3 + x$



$y^2 = x^3 + 1$

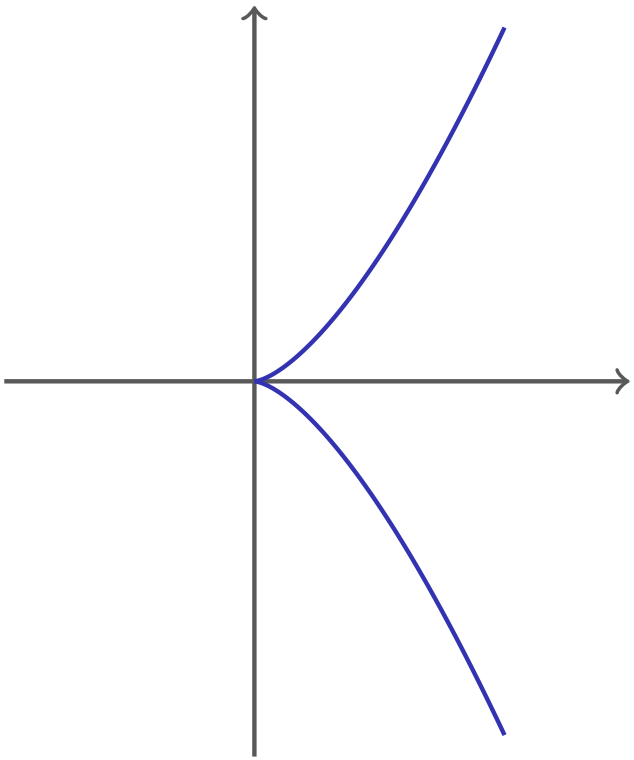


$y^2 = x^3 - 2x + 2$

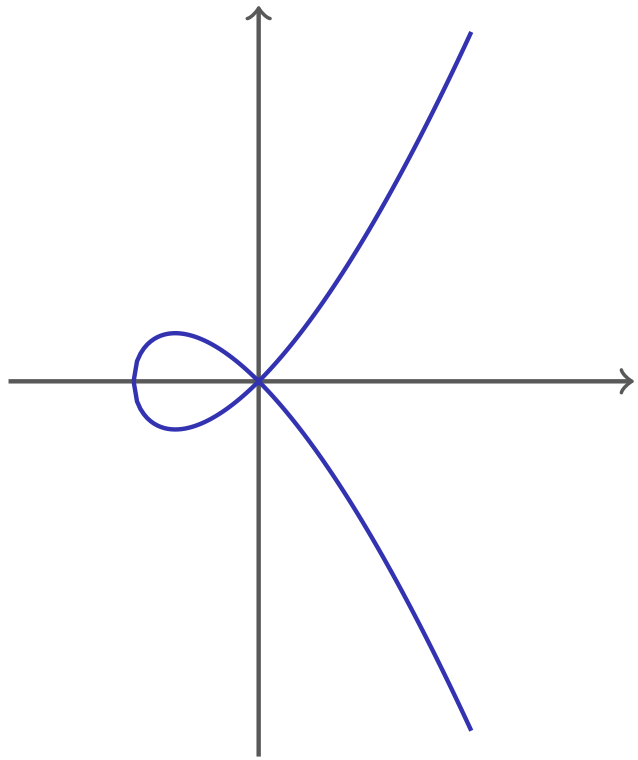


Keine Elliptischen Kurven (über $\mathbb{R}$)

$y^2 = x^3$



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



Man beachte: In diesen zwei Fällen ist die Tangente an einem Punkt nicht überall eindeutig definiert. Hier ist dieser Punkt der Ursprung. Das ist ein *singulärer Punkt*. Formale Definition folgt.

Singuläre Elliptische Kurve

Definition Singularität

Eine Kurve, definiert über dem Körper K durch eine Gleichung $F(X, Y) = 0$ (wobei $F(X, Y)$ irreduzibel über dem algebraischen Abschluss $\bar{K}$ von K ist) heisst *singulär* in einem Punkt (x_0, y_0) (auf der Kurve), falls beide Ableitungen in dem Punkt verschwinden, d.h.

$$F(x_0, y_0) = 0 \ , \ \frac{\partial F}{\partial x}(x_0, y_0) = 0 \text{ und } \frac{\partial F}{\partial y}(x_0, y_0) = 0 \ .$$

Eine Kurve heisst *nichtsingulär*, wenn in $\bar{K}$ kein Punkt $(x_0, y_0) \in \mathbb{A}^2(\bar{K})$ existiert für den beide Ableitungen verschwinden.

Eine Gleichung obiger Form nennt man *Weierstrass-Gleichung*.

Punkte auf der Kurve I

Sei, der Einfachheits halber, E/K definiert durch die Gleichung

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

(„$/K$" bedeutet: mit Koeffizienten in K).
Dann existiert ein Punkt mit Koordinaten in K (kurz: ein K-Punkt), mit x-Koordinate gleich $x_0 \in K$, wenn die Gleichung

$$y^2 = x_0^3 + ax_0 + b$$

mindestens eine Lösung besitzt. Drei Fälle:

1. $x_0^3 + ax_0 + b = 0$, d.h. x_0 ist eine Nullstelle von $x^3 + ax + b$: nur ein solcher K-Punkt existiert, dessen y-Koordinate gleich 0 ist;
2. $x_0^3 + ax_0 + b \neq 0$ und Quadrat: zwei solche Punkte;
3. $x_0^3 + ax_0 + b \neq 0$ und Nicht-Quadrat: kein solcher Punkt.

Punkte auf der Kurve II

Falls $K = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (Primkörper), dies bedeutet, es existieren genau

$$1 + \left(\frac{x_0^3 + ax_0 + b}{p} \right)$$

$\mathbb{F}_p$-Punkte mit x-Koordinate gleich x_0. Infolgedessen hat $E(\mathbb{F}_p)$

$$\sum_{x_0 \in \mathbb{F}_p} \left(1 + \left(\frac{x_0^3 + ax_0 + b}{p} \right) \right)$$

Punkte in $\mathbb{F}_p \times \mathbb{F}_p$.

Nun, man kann sich vorstellen, dass die Abbildung $x \mapsto x^3 + ax + b$ „unabhäbgig" ist von der Eigenschaft „quadratischer Rest sein", d.h. man erwartet ungefähr p Punkte auf der Kurve, nicht $2p$ oder 0.

Punkte auf der Kurve III: Hasse-Weil

In der Tat gilt das für *alle* elliptische Kurven über *allen* endlichen Körpern:

Satz von Hasse-Weil

Sei $\mathbb{F}_q$ ein Körper mit q Elementen und sei $E/\mathbb{F}_q$ eine elliptische Kurve. Dann:

$$|\#E(\mathbb{F}_q) - (q+1)| \leqslant 2\sqrt{q} \ .$$

Mit anderen Worten: die Anzahl der Punkte ist $q+1$ mit einem „Fehler" von maximal $2\sqrt{q}$.

Beweis: schwierig (braucht Zahlentheorie und Algebraische Geometrie).

Supersinguläre und gewöhnliche Kurven

Eher für die Neugierigen: Eine EK über $\mathbb{F}_q$ ($q = p^d$) heißt *supersingulär*, falls $\#E = q + 1 - t$ mit $p \mid t$. Sonst heißt die elliptische Kurve *gewöhnlich*.
Eine elliptische Kurve über einem Primkörper $\mathbb{F}_p$ ist genau dann gewöhnlich, wenn sie $p+1$ Punkte hat.

Isomorphe Kurven

Definition: Isomorphie von Kurven in Weierstrass Form

Zwei Kurven E_1, E_2 über K, gegeben als Weierstrass Gleichungen

$$\begin{aligned} E_1 : y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6 \\ E_2 : y^2 + \bar{a}_1xy + \bar{a}_3y &= x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6 \end{aligned}$$

werden als *isomorph über K* bezeichnet, falls $u, r, s, t \in K$ existieren, sodass durch eine Veränderung der Variablen der Form

$$(x, y) \to (u^2x + r, u^3y + u^2sx + t)$$

die eine Gleichung in die andere umgeformt werden kann. Diese Umformung wird *admissible change of variables* genannt.

E_1 ist genau dann singulär wenn E_2 singulär ist. (Übung.)
D.h. E_1 ist genau dann elliptisch wenn E_2 elliptisch ist.

Getwistete Kurven

Zwei elliptische Kurven über K sind getwistet wenn isomorph über eine Körpererweiterung von K aber nicht über K.
Sei K nicht algebraisch abgeschlossen mit char(K) ungerade und $d \in K \setminus K^2$. Also $\sqrt{d} \notin K$.
Dann

$$E_1 \ : \ y^2 = x^3 + ax + b$$

und

$$E_2 \ : \ y^2 = x^3 + \frac{a}{d^2}x + \frac{b}{d^3}$$

sind isomorph über $K(\sqrt{d})$, wobei die isomorphie durch

$$E_1 \to E_2 \ , (x, y) \mapsto \left(\frac{1}{d}\, x, \frac{1}{d^{3/2}}\, y \right)$$

gegeben ist. Die zwei Kurven sind aber über K *nicht* isomorph.

Vereinfachte Weierstrass-Form

Falls $char(K) \neq 2, 3$, dann kann E, definiert durch

$$E \quad : \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ ,$$

durch

$$(x, y) \to \left(x - \frac{1}{3}\, a_2 - \frac{1}{12}\, a_1^2, y - \frac{1}{2}\, a_1\, x + \frac{1}{6}\, a_1\, a_2 + \frac{1}{24}\, a_1^3 - \frac{1}{2}\, a_3 \right)$$

umgeformt werden zu

$$y^2 = x^3 + ax + b \qquad (*)$$

mit $a, b \in K$ wobei

$$a = \frac{1}{2}\, a_1\, a_3 + a_4 - \frac{1}{6}\, a_2\, a_1^2 - \frac{1}{48}\, a_1^4 - \frac{1}{3}\, a_2^2 \ ,$$

$$b = -\frac{1}{6}\, a_1\, a_2\, a_3 + a_6 + \frac{1}{18}\, a_1{}^2 a_2^2 + \frac{1}{72}\, a_1^4 a_2 - \frac{1}{24}\, a_1^3 a_3 + \\ + \frac{1}{4}\, a_3^2 - \frac{1}{3}\, a_4\, a_2 - \frac{1}{12}\, a_4\, a_1^2 + \frac{1}{864}\, a_1^6 + \frac{2}{27}\, a_2^3 \ .$$

Eine Gleichung der Form (*) heisst *Vereinfachte Weierstrass Gleichung* – oder: die Kurve ist in *vereinfachter Weierstrass-Form*.

Singularität für die Vereinfachte Weierstrass-Form

Satz

Sei die Kurve E definitert durch die Gleichung $y^2 = x^3 + ax + b$ über dem Körper K von Charakteristik $\neq 2, 3$. Dann ist E singulär g.d.w.: $\Delta = 4a^3 + 27b^2 = 0$.

E singulär $\Leftrightarrow$ existiert Lösung vom System $\begin{cases} y^2 = x^3 + ax + b \\ \frac{\partial f}{\partial x} = 3x^2 + a = 0 \\ \frac{\partial f}{\partial y} = 2y = 0 \end{cases}$

Aus der 2. Gleichung ergibt sich $x^2 = -\frac{a}{3}$.

Aus der 3. und 1. Gleichung erhalten wir $y = 0$ und $0 = x^3 + ax + b$.

Dies ist $\Leftrightarrow x(x^2 + a) + b = 0 \Leftrightarrow x(\frac{-a}{3} + a) + b = 0 \Leftrightarrow x = -\frac{3b}{2a}$

Und aus $x^2 = \frac{9b^2}{4a^2} = -\frac{a}{3}$ erhalten wir $4a^3 + 27b^2 = 0$.

Falls $4a^3 + 27b^2 = 0$, verifiziert man einfach dass $x = -\frac{3b}{2a}$ und $y = 0$ Lösung vom System ist $\Rightarrow$ singulärer Punkt.

Vereinfachte Weierstrass-Form in Char 2

Falls $char(K) = 2$ kann die vereinfachte Version der Kurvengleichung $y^2 = x^3 + ax + b$ nicht mehr verwendet werden. So eine Gleichung definiert in Charakteristik 2 *immer* eine singuläre Kurve (Übung). Hier muss man auf

$$E: \ y^2 + xy = x^3 + a_2x^2 + a_6 \qquad (*)$$

mit $a_6 \neq 0$ zurück greifen.

Übung: Wenn $char(K) = 2$, dann gibt es eine admissible Variable change von einer allgemeinen Weierstrass Gleichung zur Form (*).

Und in Charakteristik 3? (Übung/Recherche)

Das Gruppengesetz, Hintergrund-Infos

Die Menge der K-rationalen Punkte vereinigt mit dem neutralen Element $\mathcal{O}$ (d.h. dem unendlich fernen Punkt ∞) auf E bildet eine abelsche Gruppe.

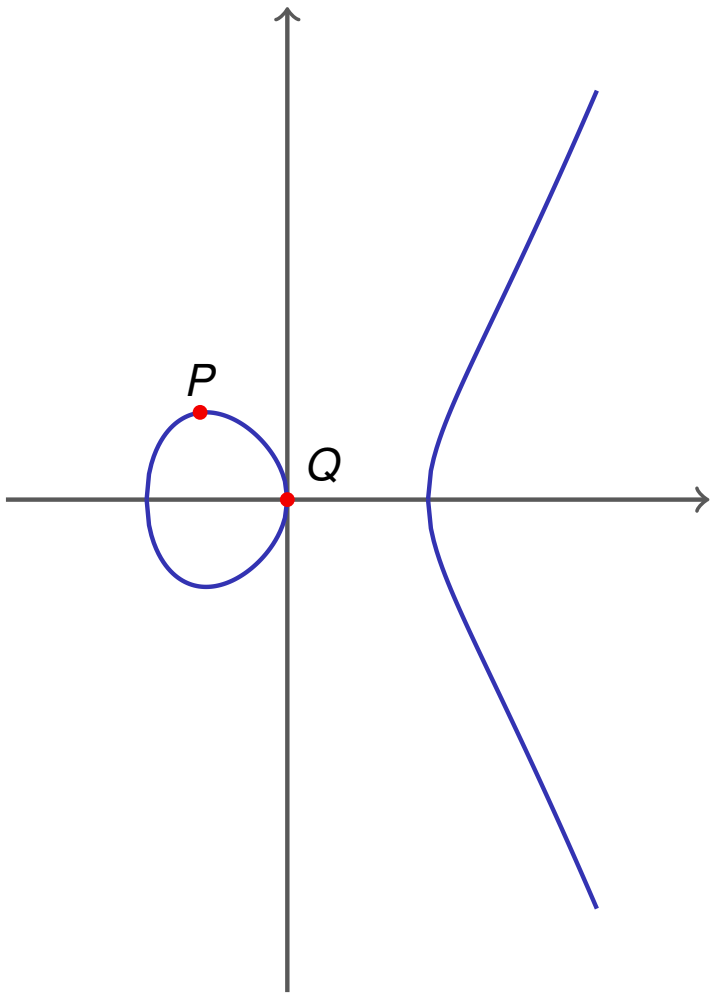
Falls K algebraisch abgeschlossen, trifft eine Gerade die elliptische Kurve immer in drei Punkten (mit Multiplizitäten gezählt).

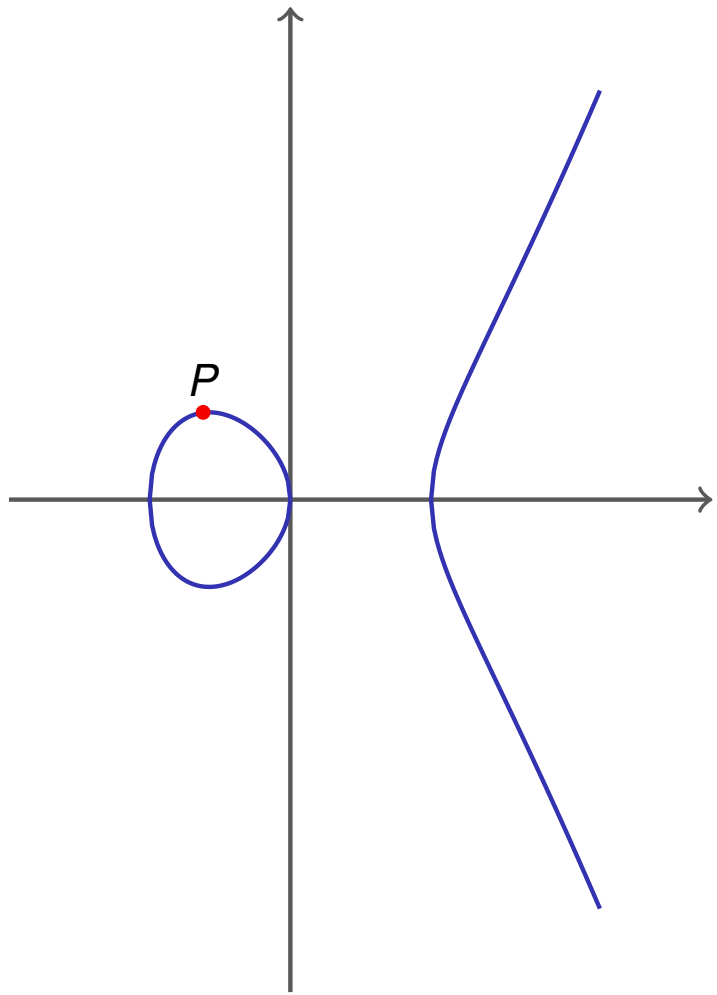
Dies folgt aus einem wichtigen Satz von Bezout: für Kurven in (allgemeinen) Weierstrass Form und nicht vertikale Geraden kann mann dies einfach beweisen (Übung), zusammen mit der nächsten Aussage:

Falls die elliptische Kurve über einem Korper K definiert ist und zwei Schnittpunkte in einer Körpererweiterung L/K liegen, dann liegt auch der dritte Schnittpunkt in L.

Gruppengesetz auf Elliptische Kurven, geometrisch I

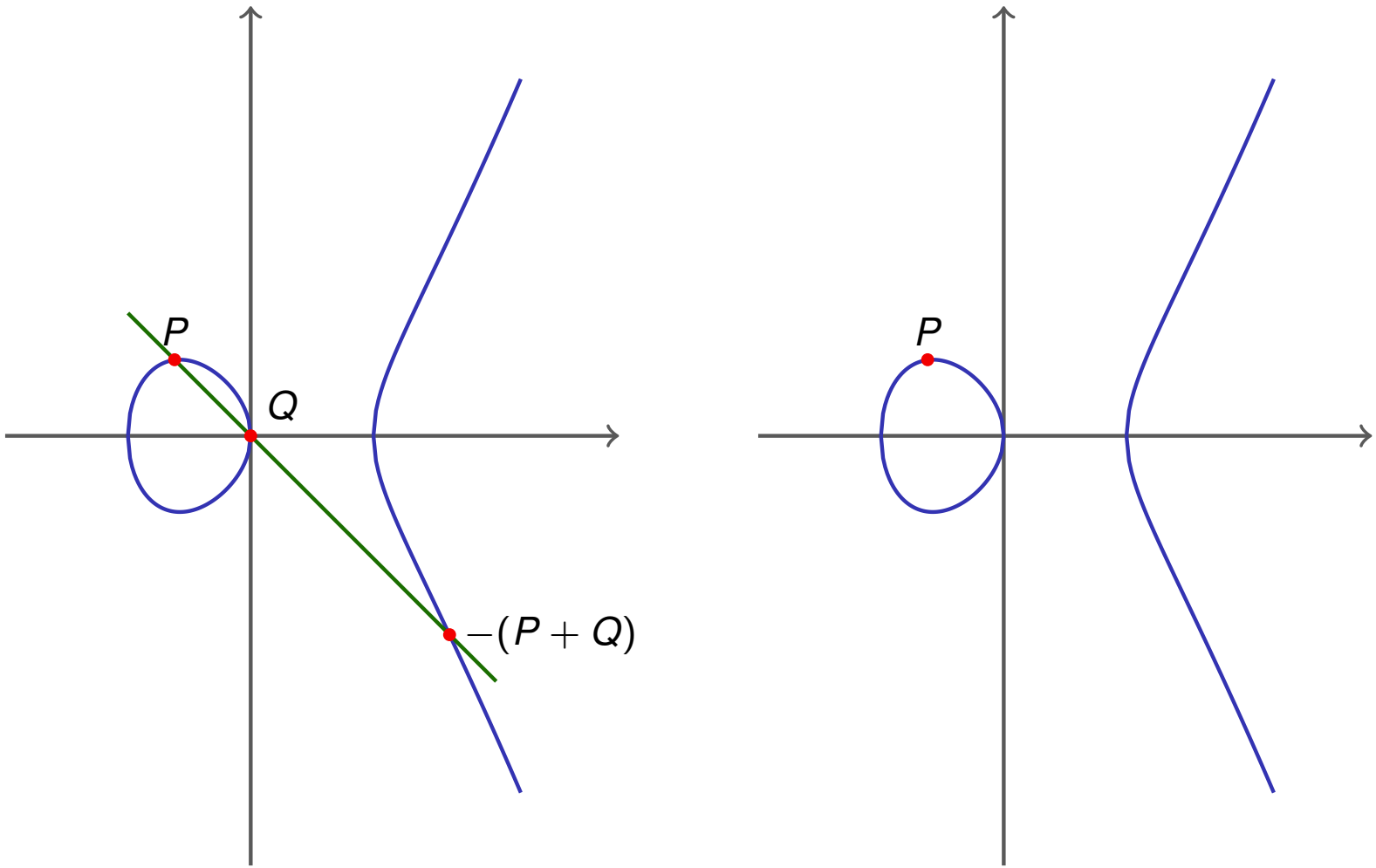
$$y^2 = x^3 - x$$





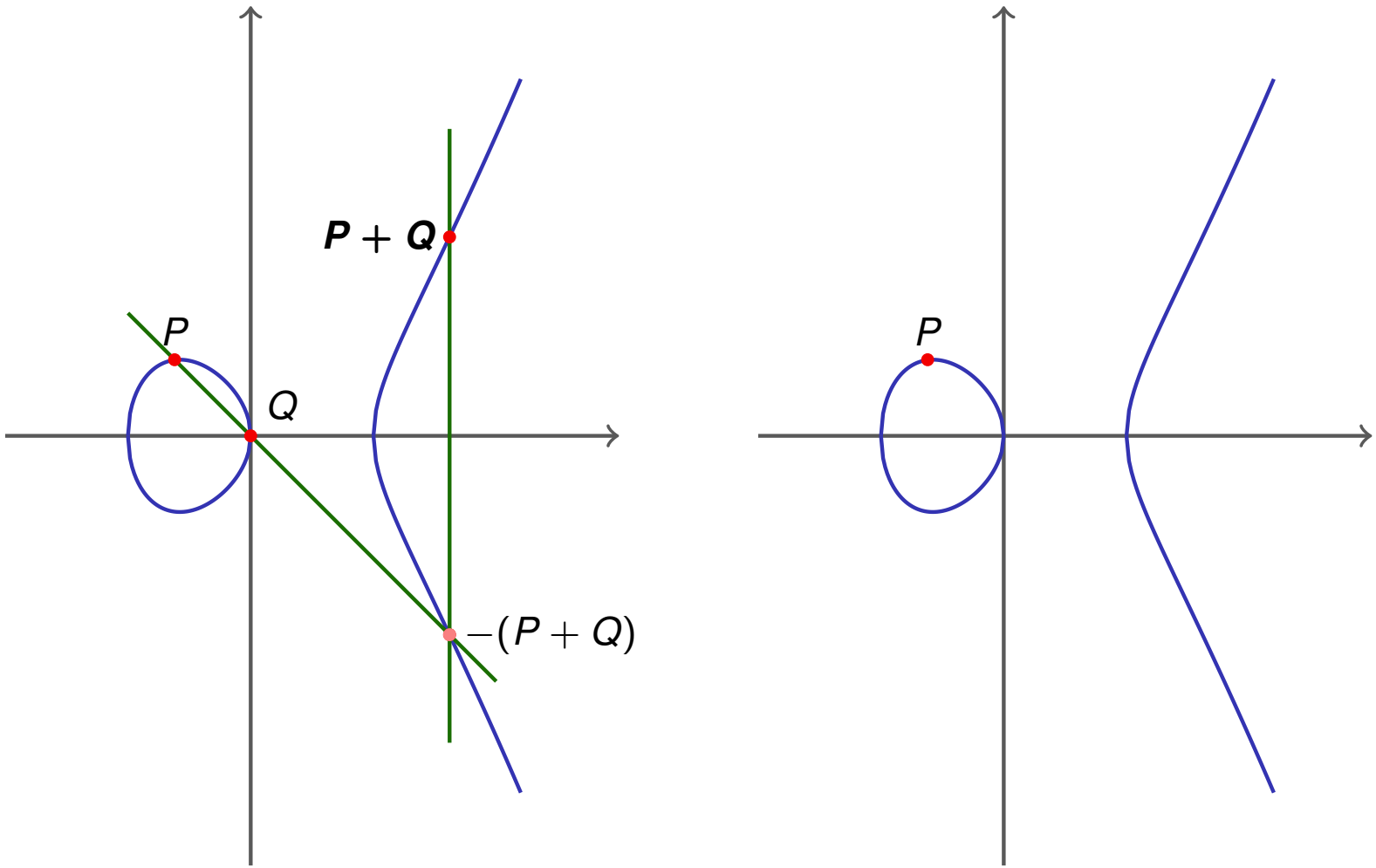
Gruppengesetz auf Elliptische Kurven, geometrisch I

$$y^2 = x^3 - x$$



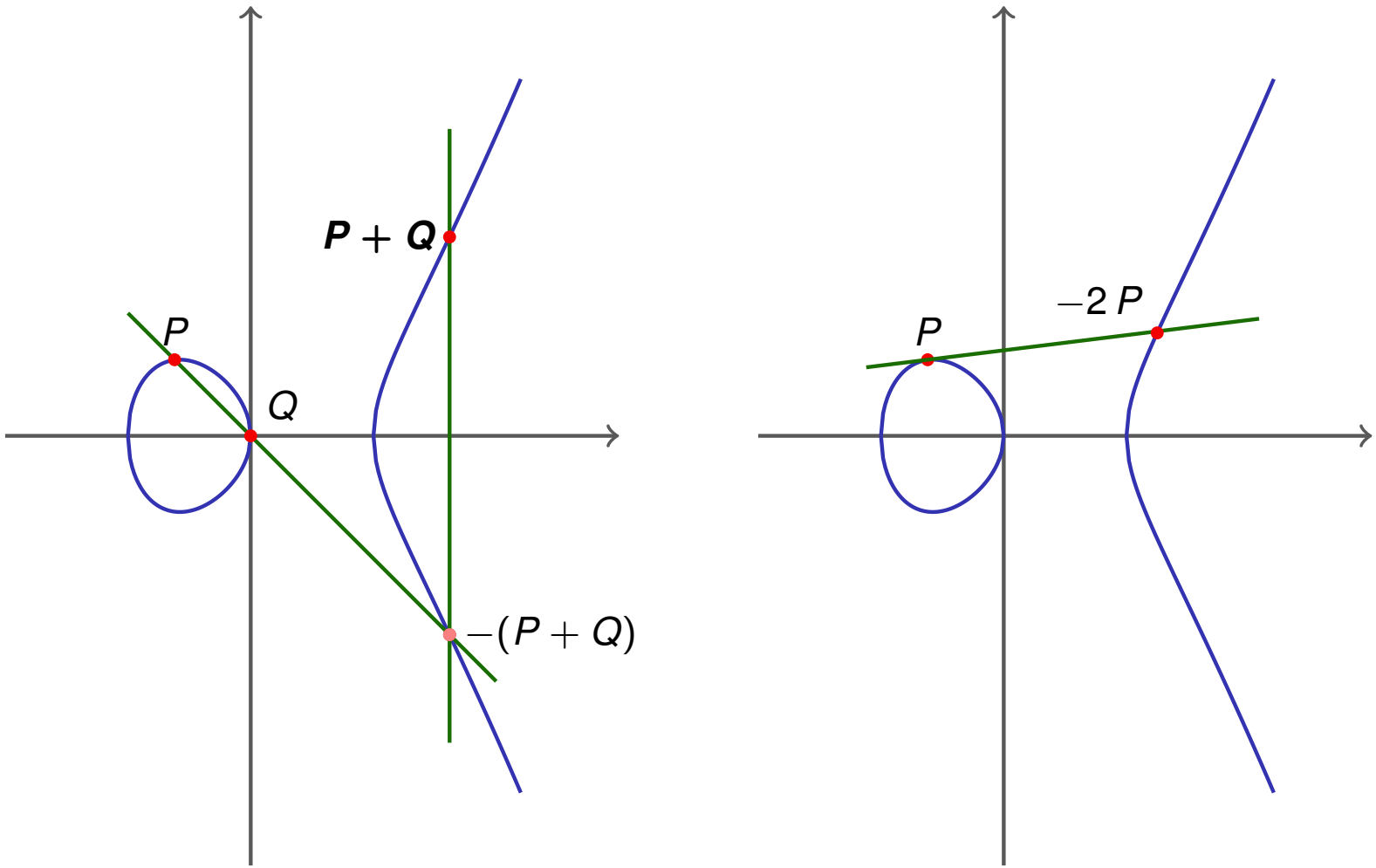
Gruppengesetz auf Elliptische Kurven, geometrisch I

$$y^2 = x^3 - x$$



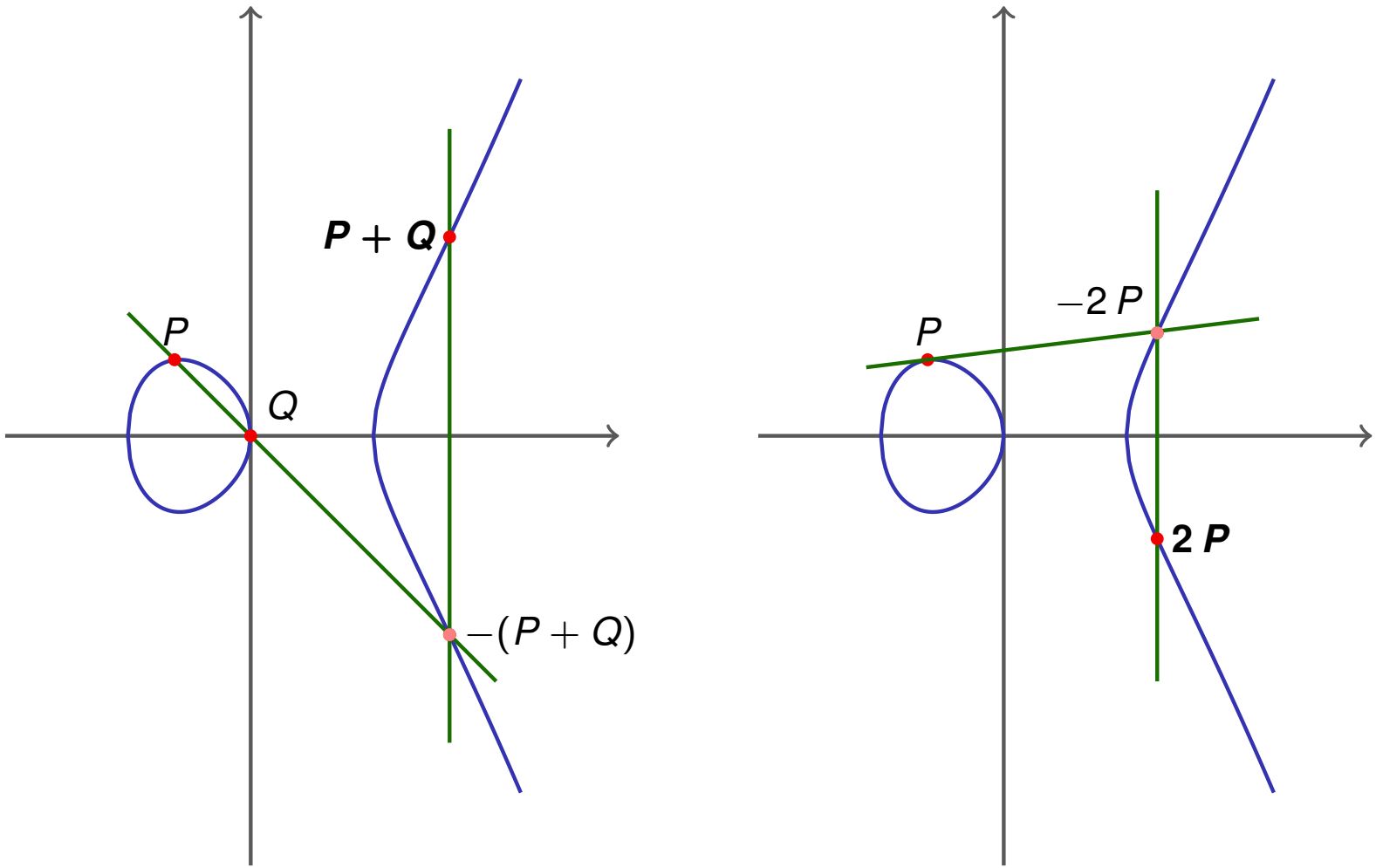
Gruppengesetz auf Elliptische Kurven, geometrisch I

$$y^2 = x^3 - x$$



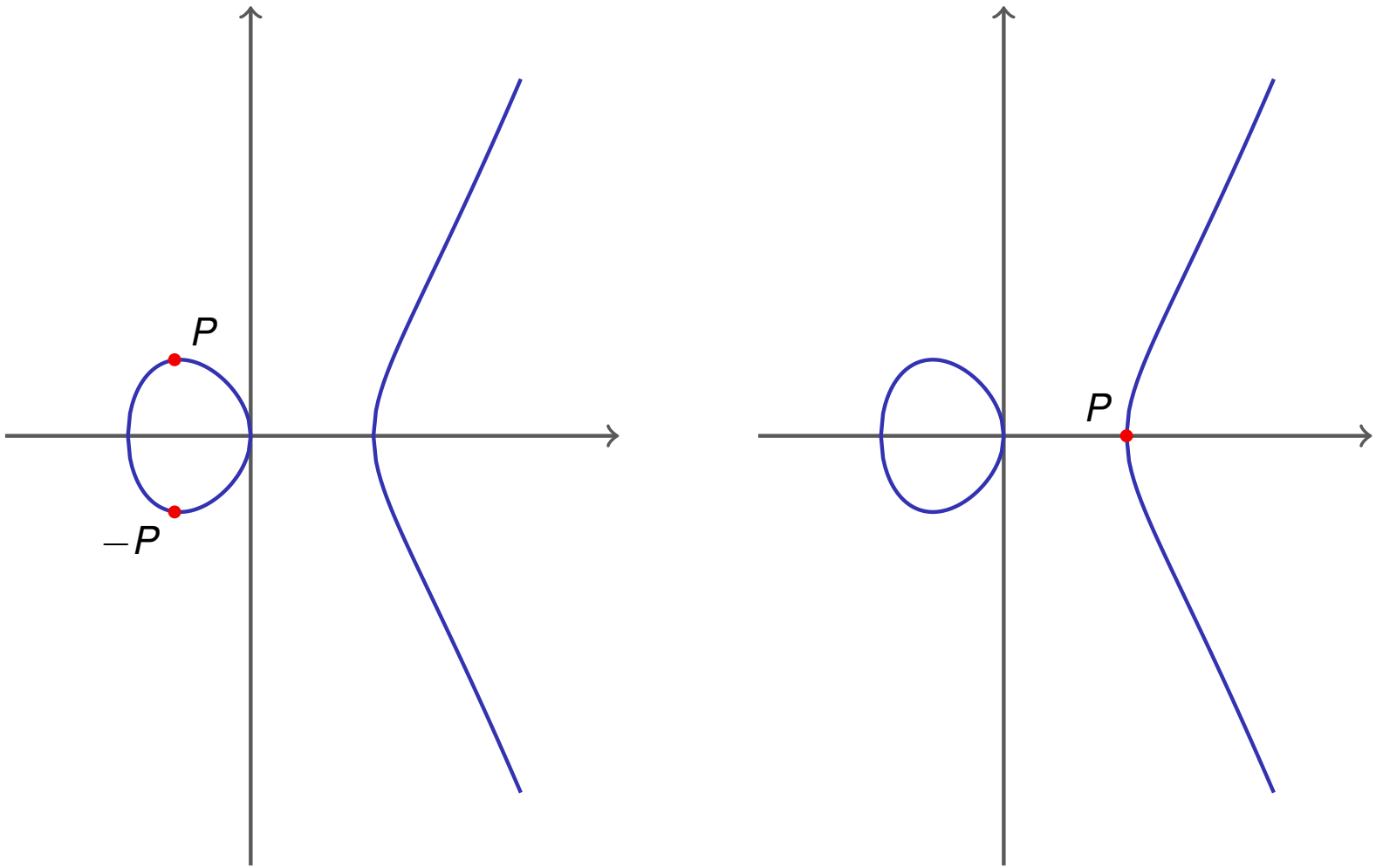
Gruppengesetz auf Elliptische Kurven, geometrisch I

$$y^2 = x^3 - x$$



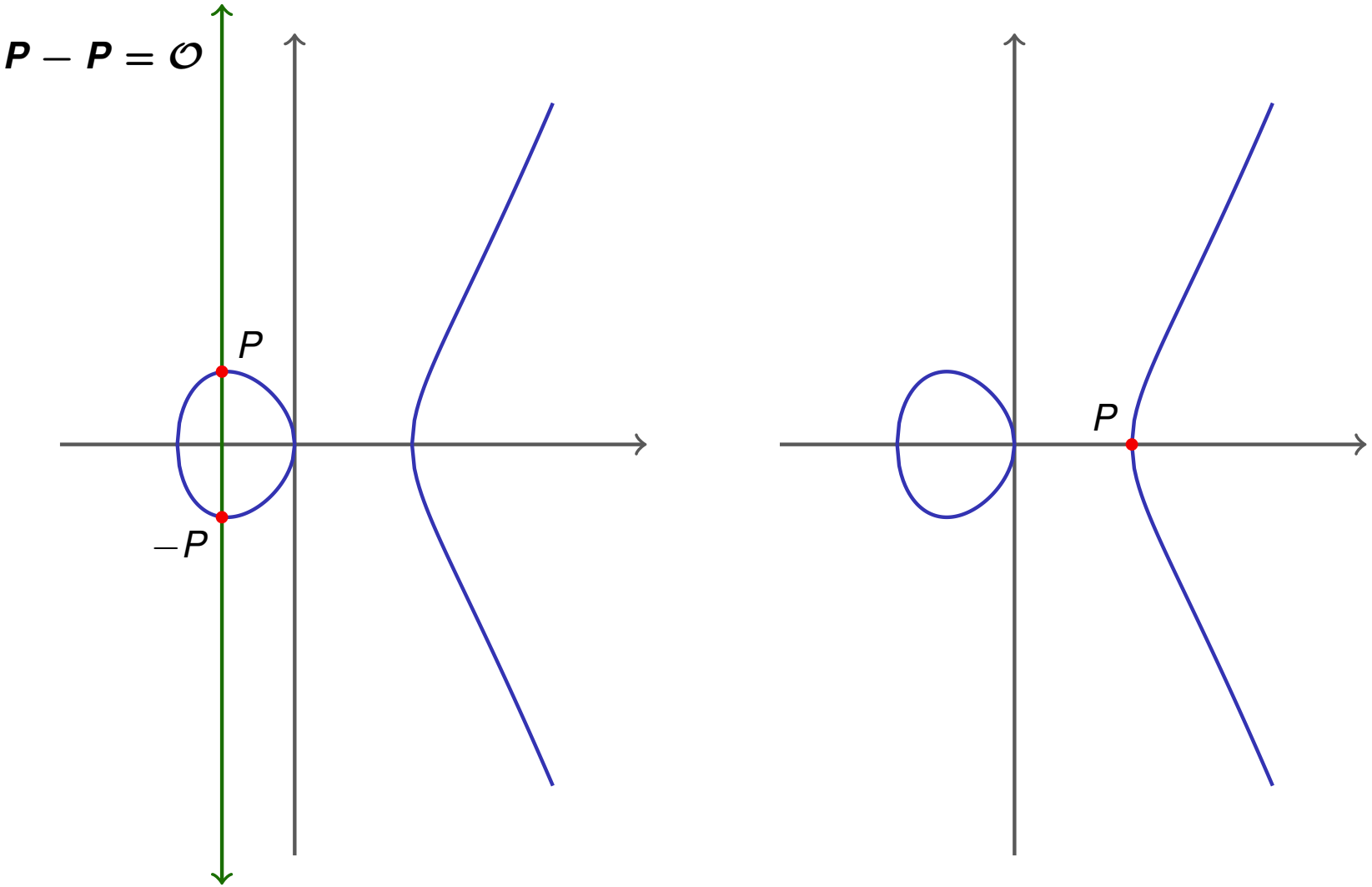
Gruppengesetz auf Elliptische Kurven, geometrisch II

$$y^2 = x^3 - x$$



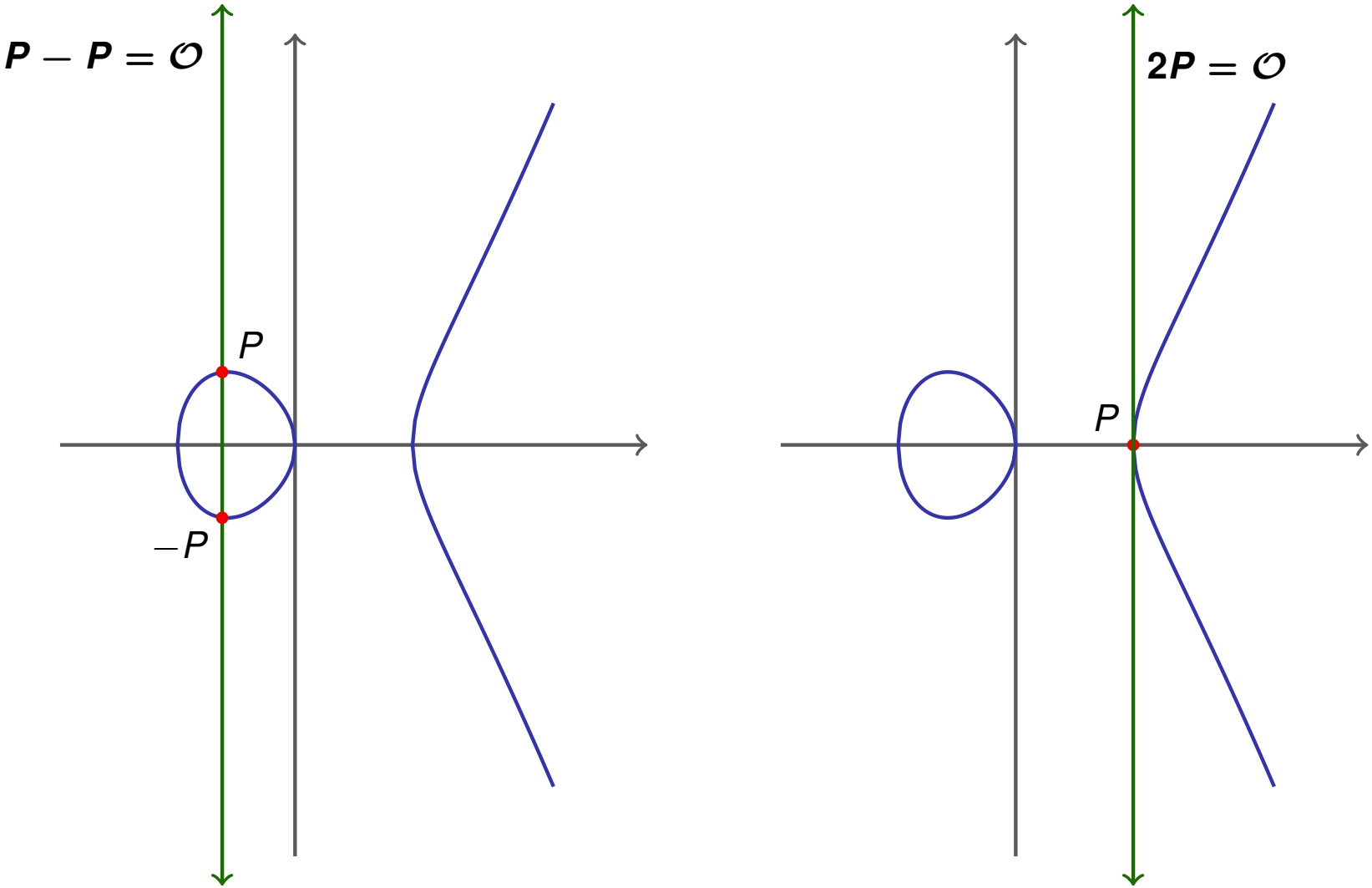
Gruppengesetz auf Elliptische Kurven, geometrisch II

$$y^2 = x^3 - x$$



Gruppengesetz auf Elliptische Kurven, geometrisch II

$$y^2 = x^3 - x$$



Gruppengesetz auf Elliptische Kurven, geometrisch III

Neutrales Element: Der unendlich ferne Punkt. Notation: $\mathcal{O}$ oder ∞.

Also: $P + \mathcal{O} = \mathcal{O} + P = P$ für alle $P \in E(K)$.

Inverses Element: Der an der x-Achse gespiegelte Punkt. Falls P = Q, dann müssen wir im ersten Schritt die Tangente von P an E wählen.

Die Punkte der Ordnung zwei auf E sind die Punkte, deren y-Koordinate gleich 0 sind (also die Punkte, die auf der x-Achse liegen).

(Die Punkte der Ordnung drei auf E sind die Wendepunkte der Kurve (hier schneidet die Tangente mit Multiplizität drei). Es gibt nur einen solchen Punkt: der unendlich ferne Punkt.)

Arithmetisches Gruppengesetz für $char(K) \neq 2, 3$, I

Seien $P, Q \in E(L)$ Punkte auf der Kurve.

Fall 1 - Addition unterschiedlicher Punkte P, Q mit $P \neq \pm Q$

- Verbinde P, Q durch Gerade g. Steigung von g ist $\lambda = \frac{y_Q - y_P}{x_Q - x_P}$.
- Der y-Achsenabschnitt $\gamma = y_P - \lambda x_P$.
- Die Gerade lässt sich dann als $g: \ y = \lambda x + \gamma$ angeben.
- Der dritte Schnittpunkt der Geraden mit der Kurve ist der Punkt $-(P + Q)$. An der x-Achse spiegeln um $P + Q$ zu erhalten.
- Die Koordinaten $(x_3, -y_3)$ des Punktes $-(P + Q)$ erhält man über den Schnittpunkt von g und E:

$$y = \lambda x + \gamma = \lambda(x - x_P) + y_P$$
$$y^2 = (\lambda x + \gamma)^2$$

In Kurvengleichung einsetzen:

$$x^3 - \underline{(\lambda x + \gamma)^2} + ax + b = 0$$

Arithmetisches Gruppengesetz für $char(K) \neq 2, 3$, II

- In Kurvengleichung einsetzen:

$$x^3 - \underline{(\lambda x + \gamma)^2} + ax + b = 0$$

$$\text{d.h.} \quad x^3 - \lambda^2 x^2 + (\cdots)x + (\cdots)x^0 = 0$$

- Diese Gleichung ist nur von x abhängig.
  Ihre Nullstellen sind die x-Koordinaten von P, Q und $P + Q$.
  Sie lässt sich also als

$$(x - x_P)(x - x_Q)(x - x_3) = x^3 - \underline{(x_P + x_Q + x_3)x^2} + \ldots$$

  schreiben. Durch Koeffizientenvergleich erhält man nun:

$$\lambda^2 = x_P + x_Q + x_3$$

- Daraus lässt sich das gesuchte x_3 eindeutig bestimmen.
- $-y_3$ erhält man durch Einsetzen in die Gleichung von g.
- Für den gesuchten Punkt $P + Q = (x_3, y_3)$ gilt also:

$$x_3 = \lambda^2 - x_P - x_Q \quad \text{und} \quad y_3 = \lambda(x_P - x_3) - y_P \ . \qquad \square$$

Arithmetisches Gruppengesetz für $char(K) \neq 2, 3$, III

Fall 2 - Addition des selben Punktes (Verdopplung):
Bilde Tangente g der Kurve in P. Der zweite Schnittpunkt (bzw. dritte, wenn man „P“ doppelt zählt) der Tangente mit der Kurve bildet den Punkt $-2P$. Durch Spiegeln an der x-Achse erhält man $2P$. Im Detail:

- Aus der Kurvengleichung $y^2 = x^3 + ax + b$ folgt:

$$2\,y\,dy = (3x^2 + a)\,dx$$

und damit gilt für die Steigung (also die Tangente):

$$\frac{dy}{dx} = \frac{3x^2 + a}{2\,y} \quad \text{also} \quad \lambda = \frac{3x_P^2 + a}{2\,y_P}$$

- x_3 und y_3 ergeben sich dann aus wie im 1. Fall – man beachte, dass x_P eine zweifache Nullstelle ist.

$$x_3 = \lambda^2 - 2\,x_P \quad \text{und} \quad y_3 = \lambda(x_P - x_3) - y_P \ . \qquad \square$$

Arithmetisches Gruppengesetz für $char(K) \neq 2, 3$, IV

Fall 3 - Addition von P und $-P$:
Gerade senkenrecht: dritter Schnittpunkt im unendlichen.
Summe ist $\mathcal{O}$.

Fall 4 - Addition mit $\mathcal{O}$:
$P + \mathcal{O} = \mathcal{O} + P = P$.

Beobachtungen:

- Wenn $P, Q \in E(K)$ gilt, dann gilt auch: $P + Q \in E(K)$ (Abgeschlossenheit)
- Die Gruppenoperation ist assoziativ (mühsam, aber machbar).

Beispiel, I

$K = GF(13)$ und $E : y^2 = x^3 + 2x + 5$ über K

1) Die Kurve ist elliptisch: $4a^3 + 27b^2 = 4 \cdot 8 + 27 \cdot 5^2 = 32 + 25 = 5$ in $\mathbb{F}_{13}$

2) Bestimme die Punkte auf E:

y	y^2
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7=-6	10
...	...

x	$x^3 + 2x + 5$
0	5
1	8
2	4
3	12
4	12
5	10
6	12
7	11
8	0
9	11
10	11
11	6
12	2

$$\Rightarrow E = \{(2,2),(2,-2),(3,5),(3,-5),(4,5),(4,-5),$$
$$(5,6),(5,-6),(6,5),(6,-5),(8,0),\mathcal{O}\}$$

Beispiel, II

$K = \mathbb{F}_{13} = GF(13)$ und $E : y^2 = x^3 + 2x + 5$ über K (Fortsetzung).

$$E = \{(2,2),(2,-2),(3,5),(3,-5),(4,5),(4,-5),(5,6),(5,-6),$$
$$(6,5),(6,-5),(8,0),0\}$$

3) Bestimme $2P$ für $P = (4,-5) = (4,8)$

$$\lambda = \frac{3x_P^2 + 2}{2y_P} = \frac{11}{3} = 11 \cdot 9 \equiv 8$$

$\Rightarrow x_3 = \lambda - x_P - x_Q = 4$ und $y_3 = \lambda(x_P - x_3) - y_P = 5$, also:

$$2P = (4,5)$$

4) Bestimme $3P$ für $P = (4,-5) = (4,8)$
$3P = 2P + P = (4,5) + (4,-5)$
Da die beiden Punkte die gleiche X-Koordinate haben, liegt $3P$ im unendlichen, also $3P = 0$. Damit ist auch $ord(P) = 3$.

Das Gruppengesetz für $char(K) = 2$

Im Fall $char(K) = 2$ kann nicht mehr die vereinfachte Version der Kurvengleichung verwendet werden, sondern

$$E: \ y^2 + xy = x^3 + a_2x^2 + a_6$$

mit $a_6 \neq 0$. Veränderungen im Gruppengesetz:

- In Körper mit $char(K) = 2$ gilt $a + b = a - b$, $a + a = 0$.
- Die Inversion eines Punktes kann nicht mehr durch die Spiegelung geschehen. Für den Punkt $P = (x_P, y_P)$ gilt $-P = (x_P, x_P + y_P)$.
- Für die Addition von P, Q mit $P \neq \pm Q$ gilt für die Steigung: $\lambda = \dfrac{y_P + y_Q}{x_P + x_Q}$
- Für die Addition $P + P$ gilt für die Steigung: $\lambda = x_P + \dfrac{y_P}{x_P}$
- x_3 berechnet sich folgendermaßen $x_3 = \lambda^2 + \lambda + \underbrace{x_P + x_Q}_{=0 \text{ falls } P=Q} + a_2$
- y_3 erhält man als $y_3 = \lambda(x_P + x_3) + x_3 + y_P$

Details selber ausarbeiten.