1.3 Weierstraß Normalform
1.4 Explizit Formulas for the Group Law

Luca Leon Happel

31 Mai 2021

Erinnerung

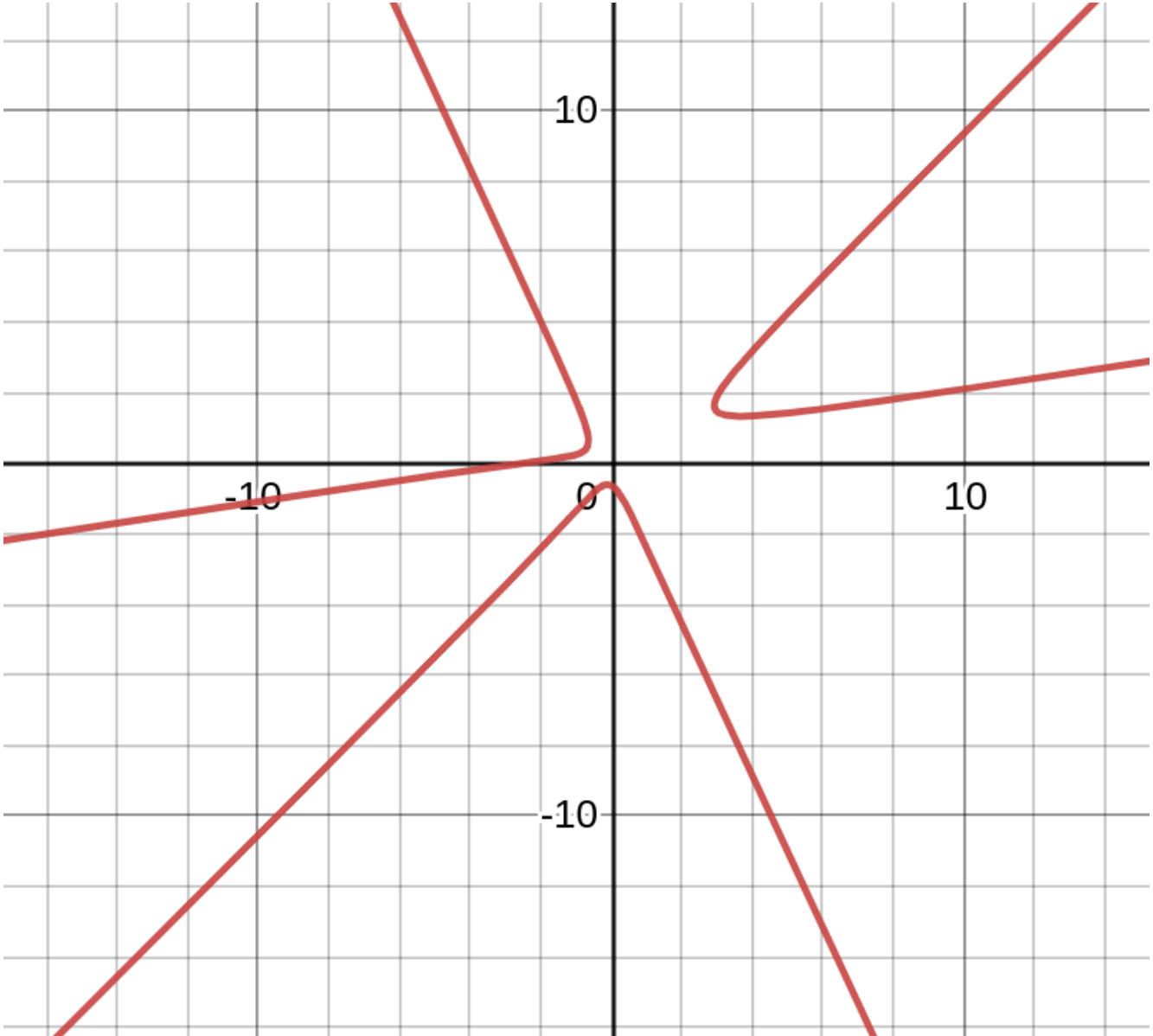
Mordell's Theorem
Wenn eine nicht singuläre rationale kubische Kurve in der Ebene einen rationalen Punkt hat, so ist die Gruppe der rationalen Punkte endlich erzeugt.
Möchten wir beweisen!

vereinfachen

Um dies beweisen zu können, müssen wir unsere Ausgangssituation vereinfachen!

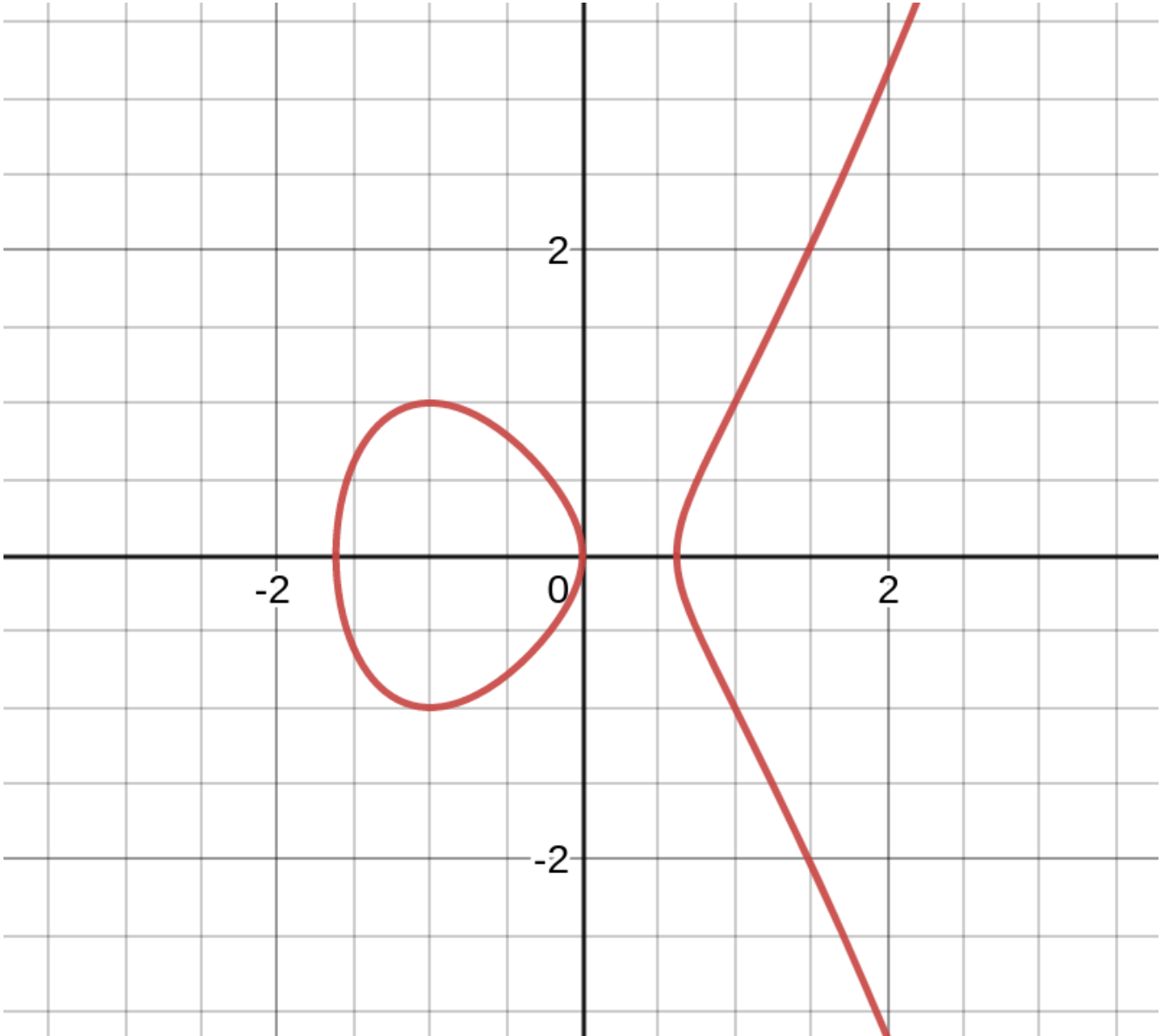
Kubische Kurve

Figure: $C : ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$



allgemeine Weierstraß Normalform

Figure: $C : y^2 = x^3 + ax^2 + bx + c$



Weierstraß Normalform

Es gibt die klassische Weierstraß Normalform

$$y^2 = 4x^3 - g_2x - g_3$$

und die allgemeine Weierstraß Normalform

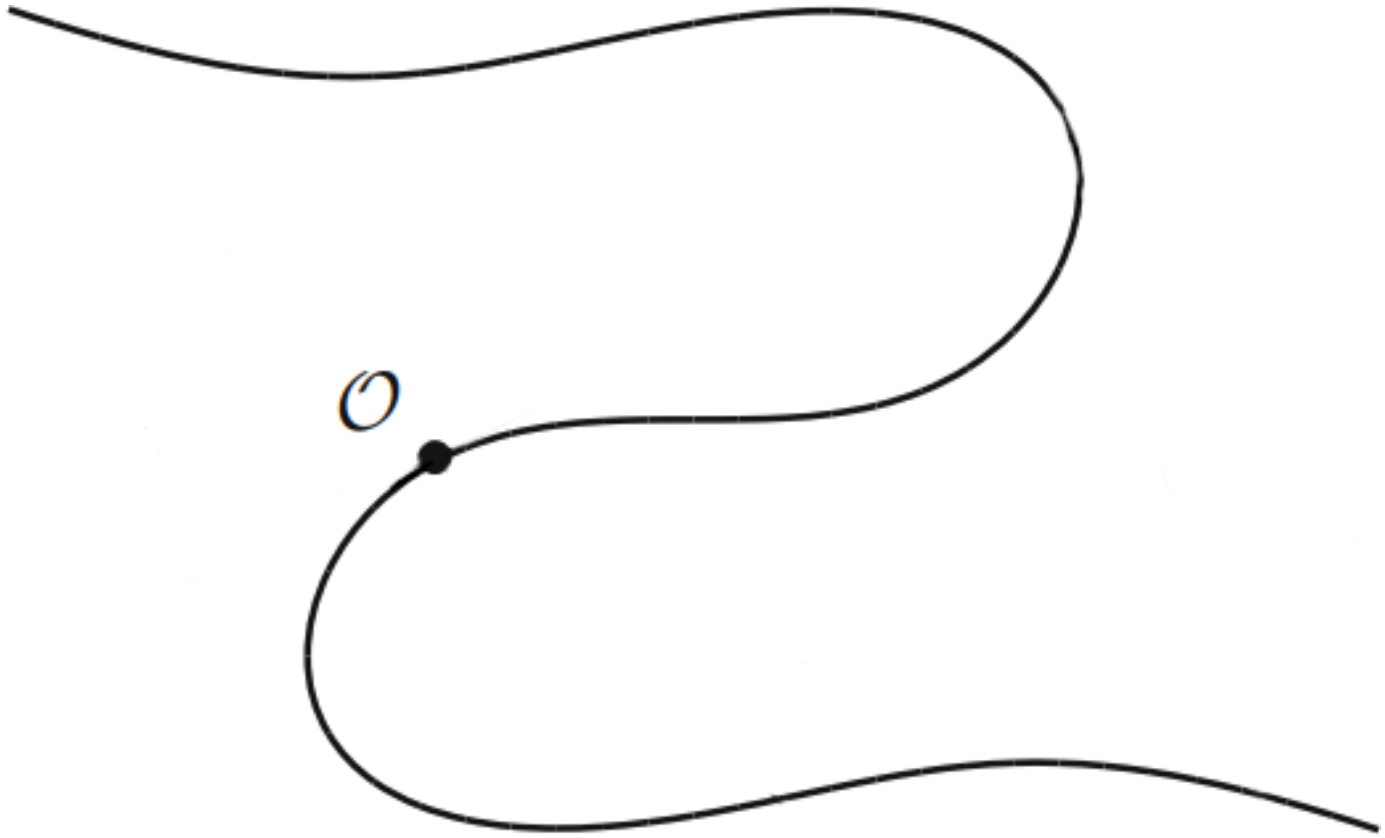
$$y^2 = x^3 + ax^2 + bx + c$$

wobei die Koeffizienten jeweils rational sind. Wir werden die allgemeine betrachten. Die WNF erlaubt uns, einfacher mit elliptischen Kurven umzugehen, da jede elliptische Kurve birational äquivalent zu einer WNF ist.

Konstruktion der Weierstraß Normalform - Schritt 1

Sei C eine kubische Kurve im Projektiven Raum mit $\mathcal{O}$, einem rationalen Punkt auf C. Verändere/wähle Achsen so, dass wir eine einfachere Form erhalten.

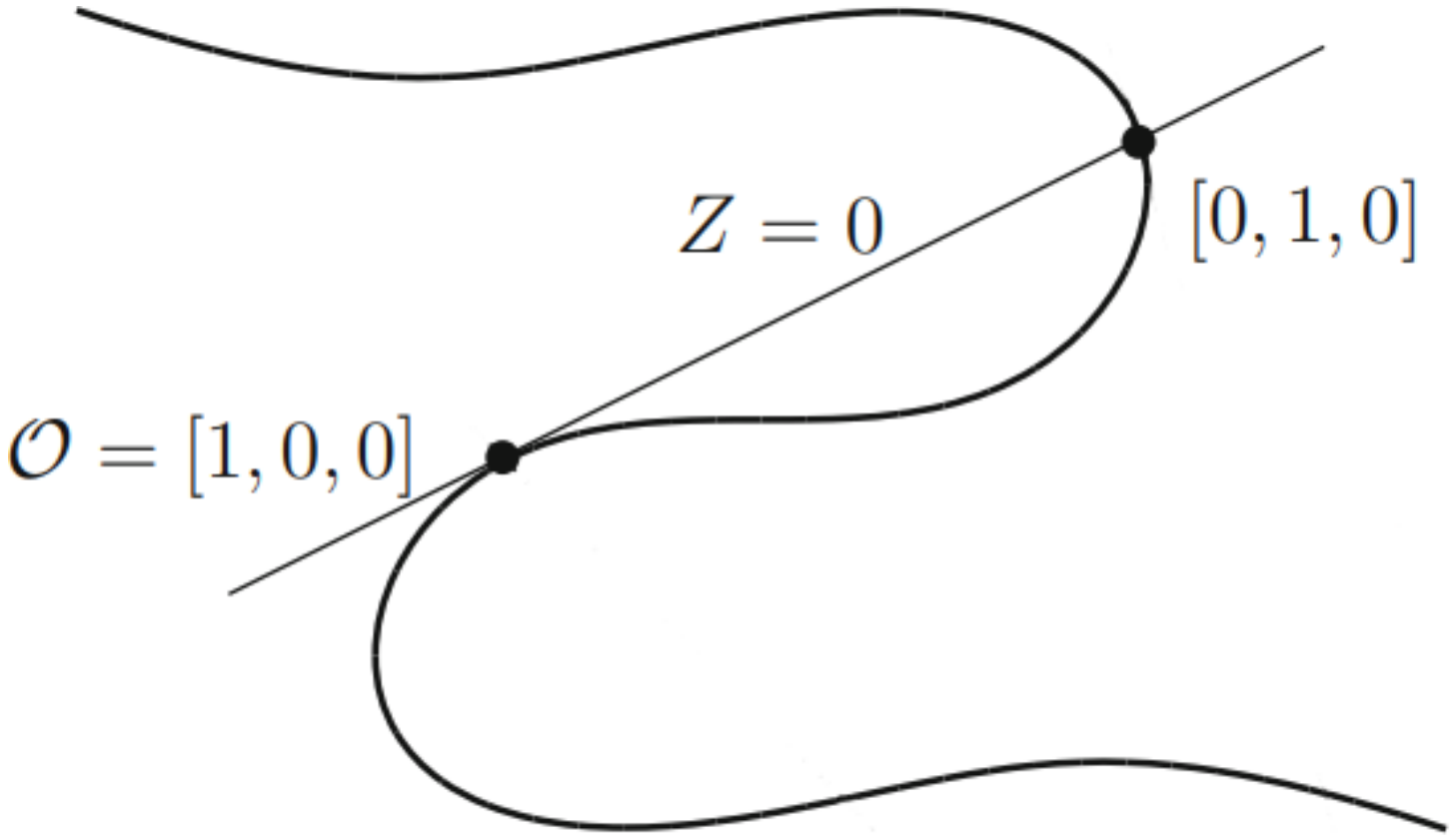
Konstruktion der Weierstraß Normalform - Schritt 1



Konstruktion der Weierstraß Normalform - Schritt 2

Wir nehmen die Tangente von $\mathcal{O}$ und verwenden sie als unser $Z = 0$, also unsere Z-Achse.

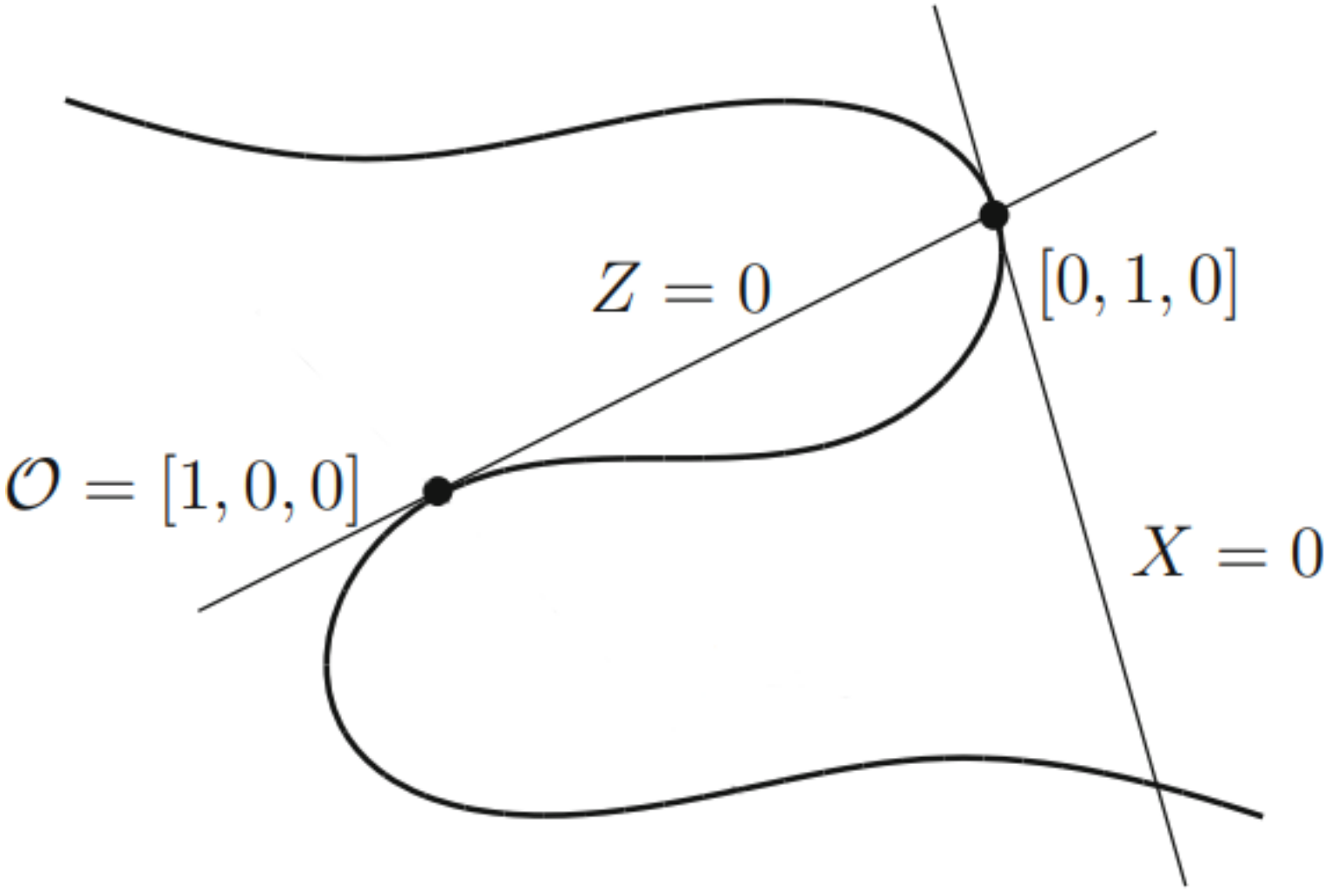
Konstruktion der Weierstraß Normalform - Schritt 2



Konstruktion der Weierstraß Normalform - Schritt 3

Diese Tangente schneidet die Kurve an einer weiteren Stelle $(0:1:0)$ und die Tangente an dieser Stelle wird unsere X-Achse. Wenn $\mathcal{O}$ ein Wendepunkt (point of inflection) ist, können wir eine beliebige Gerade wählen, welche nicht durch $\mathcal{O}$ geht.

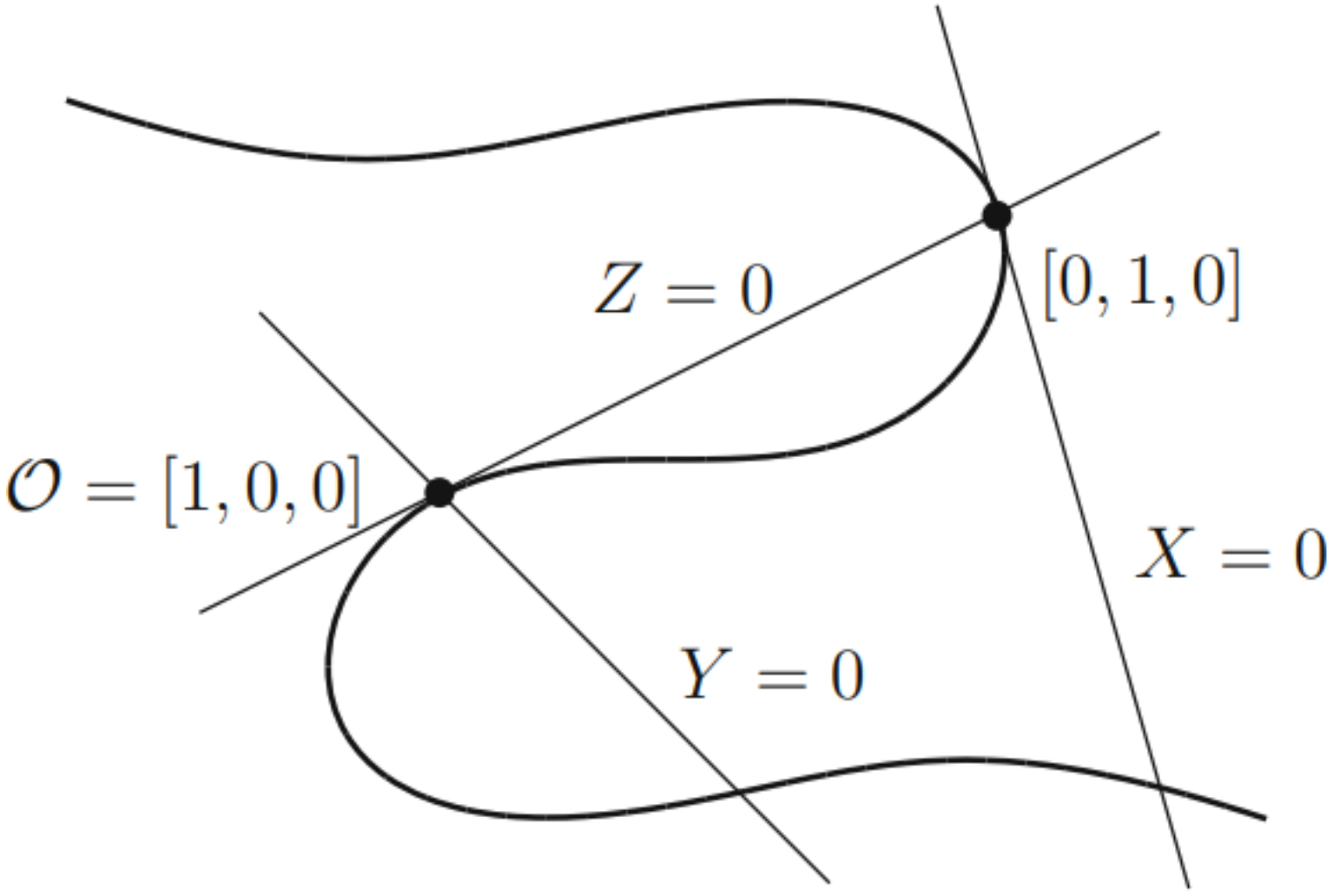
Konstruktion der Weierstraß Normalform - Schritt 3



Konstruktion der Weierstraß Normalform - Schritt 4

Zuletzt wählen wir noch eine beliebige Gerade, welche durch $\mathcal{O}$ geht als unsere Y-Achse

Konstruktion der Weierstraß Normalform - Schritt 4



Konstruktion der Weierstraß Normalform - Schritt 5

$$\underbrace{x = \frac{X}{Z}, \quad y = \frac{Y}{Z}}_{\text{Projektive Transformation}}$$

Neue Form der Gleichung:

$$xy^2 + (ax + b)y = cx^2 + dx + e$$

Auf beiden Seiten mit x multiplizieren:

$$(xy)^2 + (ax + b)xy = cx^3 + dx^2 + ex$$

Konstruktion der Weierstraß Normalform - Schritt 6

Benenne xy in y um:

$$y^2 + (ax + b)y = cx^3 + dx^2 + ex$$

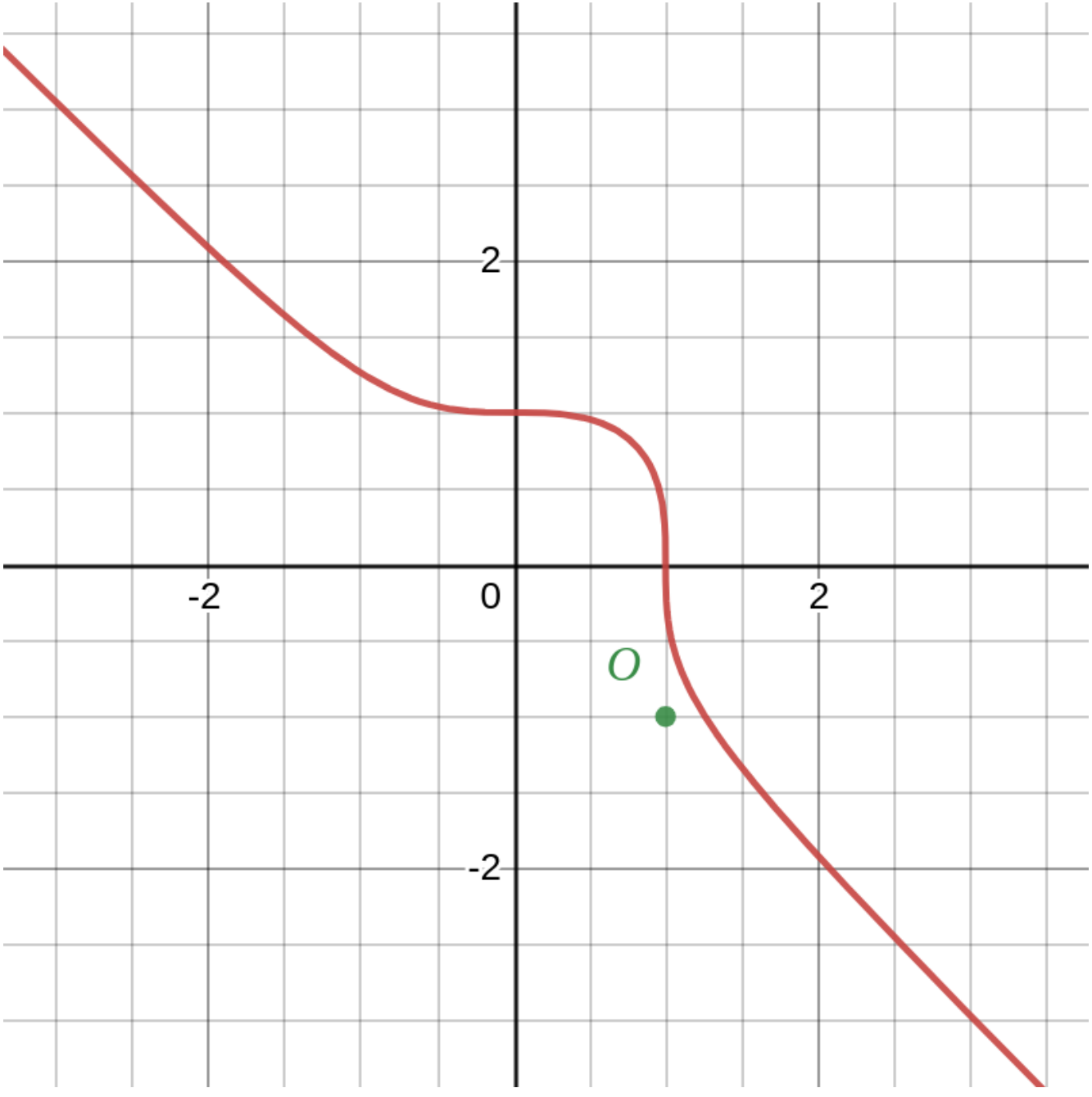
Benenne $\left(y - \frac{ax+b}{2}\right)$ in y (lineare Transformation) um, was effektiv durch quadratische Ergänzung unser Resultat:

$$y^2 = \text{kubische Funktion in } x$$

Beispiel

Betrachten wir das Beispiel $u^3 + v^3 = \alpha$ für $\alpha \in \mathbb{Q}$

Beispiel



Beispiel - Schritt 1

Zuerst projektivieren wir und erhalten $U^3 + V^3 = \alpha W^3$. Wir können leicht sehen, dass $\mathcal{O} = (1 : -1 : 0)$ eine Lösung ist. Weil $\mathcal{O}$ ein inflection point ist, können wir $X = 0$ fast frei wählen (wir dürfen die X-Achse nur nicht gleich der Y- oder der Z- Achse wählen). Schlussendlich erhalten wir

$$x = \frac{12\alpha}{u+v}, \quad y = 36\alpha\frac{u-v}{u+v}$$

Beispiel - Schritt 2

Durch Umformungen erkennen wir, dass x, y die Weierstraß Normalform $y^2 = x^3 - 432\alpha^2$ erfüllen. Explizit können wir dies nachprüfen, indem wir u, v einsetzen und ausmultiplizieren. So erhalten wir

$$-\frac{1728\alpha^3}{(u+v)^3} + \frac{1296\alpha^2 (u-v)^2}{(u+v)^2} + 432\alpha^2$$

Beispiel - Schritt 3

Ausmultiplizieren ergibt:

$$-\frac{1728\alpha^3}{u^3+3u^2v+3uv^2+v^3}+\frac{1296\alpha^2u^2}{u^2+2uv+v^2}$$

$$-\frac{2592\alpha^2uv}{u^2+2uv+v^2}+\frac{1296\alpha^2v^2}{u^2+2uv+v^2}+432\alpha^2$$

Wir können dies nun vereinfachen:

$$\frac{1728\alpha^2\left(-\alpha+u^3+v^3\right)}{u^3+3u^2v+3uv^2+v^3}$$

Wir sehen also, dass wenn $y^2=x^3-432\alpha^2$ eine Lösung hat, so hat auch $u^3+v^3=\alpha$ eine Lösung.

Beispiel - Schritt 4

Wir können den Prozess auch rückwärts gehen und u, v durch x, y darstellen, indem wir $u = \frac{36\alpha+y}{6x}$ und $v = \frac{36\alpha-y}{6x}$ verwenden.
Wenn wir rationale Lösungen für $y^2 = x^3 - 432\alpha^2$ haben, so haben wir auch rationale Lösungen für $u^3 + v^3 = \alpha$ und umgekehrt auch.
Es gibt nur endlich viele Ausnahmen (z.B. wenn $u = -v$) aber diese sind schnell zu finden.