Elliptische Kurven und ihre Anwendung in der Kryptographie

DMK-Weiterbildung vom 8. September 2022

Philipp Habegger
Departement Mathematik und Informatik
Universität Basel
philipp.habegger@unibas.ch

Letzte Revision 29. August 2022, 14:02

Inhaltsverzeichnis

0 Vorwort **3**
0.1 Notation 3

1 Kongruente Zahlen **4**

2 Elliptische Kurven **7**
2.1 Definition der Elliptischen Kurve 7
2.2 Das Gruppengesetz 10
2.2.1 Die Verknüpfung 10
2.2.2 Die Inversionsabbildung 14
2.2.3 Das neutral Element 14
2.3 Überprüfung der Gruppenaxiome 14

0 Vorwort

Der Inhalt dieses Skripts bildet die Grundlage der Weiterbildungsveranstaltung der Deutschschweizerische Mathematik-Kommission vom 8. September 2022, welche ich an der Universität Basel gehalten habe.
Ich bin dankbar um die Meldung von Fehlern und Ungenaugigkeiten an meine Email-Adresse auf der Titelseite.

0.1 Notation

Wir verwenden die folgenden Konventionen.

- Die Menge der natürlichen Zahlen ist $\mathbb{N} = \{1, 2, 3, \ldots\}$.
- Wir wählen eine Nullstelle von $X^2 + 1$ in $\mathbb{C}$ und bezeichnen sie mit $\sqrt{-1}$.

1 Kongruente Zahlen

Definition 1.1. *Eine natürliche Zahl $n \in \mathbb{N}$ heisst **kongruente Zahl**, falls n die Fläche eines rechwinkligen Dreiecks mit rationalen Seitenlängen ist.*

Bemerkung 1.2. *Per Definition ist n genau dann eine kongruente Zahl, wenn es positive $a, b, c \in \mathbb{Q}$ gibt, so dass $a^2 + b^2 = c^2$ und $n = ab/2$.*

Beispiele 1.3.

(i) Die Zahl $n = 6$ ist kongruent, da es ein rechtwinkliges Dreieck mit Seitenlängen $a = 3, b = 4, c = 5$ gibt und da $6 = 3 \cdot 4/2$.

(ii) Für jede kongruente Zahl n und jede rationale Zahl $\lambda \neq 0$ ist $\lambda^2 n$ eine kongruente Zahl, sofern es eine ganze Zahl ist. Um das zu beweisen, dürfen wir $\lambda > 0$ annehmen. Nach Voraussetzung ist $n = ab/2$ mit $a^2 + b^2 = c^2$. Also $a'^2 + b'^2 = c'^2$, wobei $a' = \lambda a, b' = \lambda b, c' = \lambda c$ wiederum rational. Die Fläche des entsprechenden rechtwinkligen Dreiecks ist die Zahl $a'b'/2 = \lambda^2 ab/2 = \lambda^2 n$ kongruent, falls sie ganz ist.

(iii) Aus (i) und (ii) folgt, dass es unendlich viele kongruente Zahlen gibt, denn $\{6\lambda^2 : \lambda \in \mathbb{N}\}$ besteht aus kongruente Zahlen. Weiterhin ist jede kongruente Zahl ein rationales Vielfaches einer quadratfreien kongruenten Zahl.

(iv) Es gilt $(3/2)^2 + (20/3)^2 = (41/6)^2$ und damit ist $n = 5 = (3/2) \cdot (20/3)/2$ kongruent.

(v) Auch $n = 7$ ist kongruent wegen $(35/12)^2 + (24/5)^2 = (337/60)^2$.

Für jedes Tripel (a, b, c) mit a, b, c positive rationalen Zahlen mit $a^2 + b^2 = c^2$ existieren $u > v > 0$ rational mit $a = u^2 - v^2, b = 2uv, c = u^2 + v^2$. Hieraus können wir auf systematische Art alle kongruente Zahlen produzieren. Es gilt folgt folgende Aussage.

Lemma 1.4. *Die Menge der kongruenten Zahlen ist*

$$\{n \in \mathbb{N} : \text{ es gibt } u > v > 0 \text{ in } \mathbb{Q} \text{ mit } n = (u^2 - v^2)uv \ \}.$$

Ist $n = 1$ eine kongruente Zahl? Die Antwort ist nein und dies wurde von Pierre Fermat bewiesen.

Satz 1.5 (Fermat)**.** *Eins ist keine kongruente Zahl.*

Beweis. TODO □

Korollar 1.6. *Die reelle Zahl $\sqrt{2}$ ist irrational.*

Beweis. Es gilt $a^2 + b^2 = 2^2$ und $ab/2 = 1$ für $a = b = \sqrt{2}$. Aber 1 ist nicht eine kongruente Zahl wegen Fermats Satz. Damit kann $\sqrt{2}$ nicht rational sein. □

Eine klassische Fragestellung ist das folgende Problem.

Problem 1.7. *Gegeben eine natürliche Zahl n. Ist n eine kongruente Zahl oder nicht?*

Es ist heute kein Algorithmus bekannt, der entscheidet, ob eine gegebene natürliche Zahl kongruent ist oder nicht. Daher kennen wir keinen systematischen Zugang zu der Frage oben.
In der Definition von kongruente Zahl kommen

Lemma 1.8. *Sei $n \in \mathbb{N}$.*

1. *Seien $a, b, c \in \mathbb{Q}$ mit $a^2 + b^2 = c^2, a \neq c$ und $n = ab/2$. Wir definieren*

$$x = \frac{nb}{c-a} \quad \text{und} \quad y = \frac{2n^2}{c-a}.$$

   Dann gilt $y^2 = x^3 - n^2x$.

2. *Seien $x, y \in \mathbb{Q}$ mit $y^2 = x^3 - n^2x$. Falls $y \neq 0$, dann ist n eine kongruente Zahl.*

Beweis. Teil (i) ist eine direkt Rechnung. Es gilt

$$y^2 = \frac{4n^4}{(c-a)^2} = \frac{a^4b^4}{4(c-a)^2}$$

und

$$x^3 - n^2x = n^3\frac{b^3}{(c-a)^3} - n^3\frac{b}{c-a} = n^3\frac{b}{c-a}\left(\frac{b^2}{(c-a)^2} - 1\right) = n^3b\frac{b^2-(c-a)^2}{(c-a)^3} = \frac{a^3b^4}{8}\frac{b^2-(c-a)^2}{(c-a)^3}.$$

Es gilt

$$y^2 - (x^3 - n^2x) = \frac{a^3b^4}{8(c-a)^3}\left(2a(c-a) - b^2 + (c-a)^2\right) = \frac{a^3b^4}{8(c-a)^3}(c^2 - a^2 - b^2) = 0,$$

was für (i) zu zeigen.
Für den Beweis von (ii) setzen wir

$$a = \left|\frac{n^2-x^2}{y}\right|, \quad b = \left|\frac{2nx}{y}\right|, \quad \text{und} \quad c = \left|\frac{n^2+x^2}{y}\right|.$$

Eine direkt Rechnung zeigt $a^2 + b^2 = c^2$. Weiterhin gilt

$$\frac{ab}{2} = \frac{|(n^2-x^2)(2nx)|}{2y^2} = \frac{2n|n^2x - x^3|}{2y^2} = \frac{n|-y^2|}{y^2} = n.$$

Da a, b, c nicht negative rationale Zahlen sind, reicht es zu zeigen, dass $abc \neq 0$. Es gilt $c = (n^2 + x^2)/|y| \geq n^2/|y| > 0$.
Es gilt $y^2 = (x^2 - n^2)x \neq 0$. Daraus folgt $x^2 - n^2 \neq 0$ und $x \neq 0$. Also folgt $a \neq 0$ und $b \neq 0$.
Es folgt, dass n eine kongruente Zahl ist. □

Für jede natürliche Zahl $n \in \mathbb{N}$ definiert Lösungsmenge der kubischen Gleichung

$$Y^2 = X^3 - n^2 X \tag{1.1}$$

definiert eine Kurve in der reelle (oder komplexen) Ebene. Von besonderem Interesse sind die **rationalen Punkte** dieser Kurve, d.h. Punkte, deren Koordinaten rational sind.
Die Punkte $(0,0), (\pm n, 0)$ liegen augenscheinlich auf der Kurve für jedes n. Gibt es mindestens ein weiterer rationaler Punkt, d.h. ein Punkt dessen Ordinate nicht verschwindet, so ist n eine kongruente Zahl. Weiterhin ist die Umkehrung auch wahr.
Die Gleichung (1.1) ist ein Spezialfall der Weierstrass-Gleichung, welche im Allgemeinen eine elliptische Kurve definiert.
Den Satz von Fermat, Satz 1.5, lässt sich wie folgt umformulieren.

Satz 1.9 (Fermat – Version 2)**.** *Die rationalen Punkten der Lösungsmenge von* $Y^2 = X^3 - X$ *in der Ebene ist*

$$\{(0,0), (\pm 1, 0)\}.$$

2 Elliptische Kurven

In diesem Abschnitt werden elliptische Kurven ad hoc eingeführt. Teil des Datums einer elliptischen Kurve ist ein Grundkörper K. Dies ist a priori ein beliebiger Körper. Aber für uns sind die wichtigsten Wahlen von Grundkörper die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ und die komplexen Zahlen $\mathbb{C}$. Für Anwendungen in der Krytographie spielen die endlichen Körper eine zentrale Rolle.
Es sei angemerkt, dass die Theorie elliptische Kurven im arithmetischen Fall, d.h. für den $K = \mathbb{Q}$ und verwandte Körper, ihre volle Tiefe entfaltet. Falls der Grundkörper, so wie $\mathbb{C}$, algebraisch abgeschlossen ist, verschwinden die arithmetischen Aspekte.

2.1 Definition der Elliptischen Kurve

Definition 2.1. *Sei K wie oben ein Körper. Eine **Weierstrass-Gleichung** ist eine Gleichung vom Typ*

$$E : Y^2 = X^3 + aX + b \tag{2.1}$$

mit Unbekannten X, Y und Koeffizienten $a, b \in K$, welche die Bedingung

$$\Delta_E = -2^4(4a^3 + 27b^2) \neq 0 \tag{2.2}$$

*erfüllt. Die Grösse Δ_E, ein Element aus K, heisst **Diskriminante** der Weierstrass-Gleichung E. Zur Weierstrass-Gleichung E gehört das Weierstrass-Polynom[1] $Y^2-(X^3+aX+b)$.*

Beispiele 2.2.

(i) In (1.1) hatten wir die Gleichung $Y^2 = X^3 - n^2X$ für $n \in \mathbb{N}$ betrachtet. Es handelt sich um eine Weierstrass-Gleichung E, für $K = \mathbb{Q}$ (oder jeden Körper, der $\mathbb{Q}$ enthält) mit $\Delta_E = -2^4 3^3 n^4$.

(ii) Die Gleichung

$$Y^2 = X^3,$$

definiert keine Weierstass-Gleichung, da (2.2) nicht erfüllt ist.

Bemerkung 2.3. *Sei K ein Körper der Charakteristik 2, z.B. $K = \mathbb{F}_2$, und $a, b \in K$. Dann ist $Y^2 = X^3 + aX + b$ keine Weierstrass-Gleichung, da (2.2) nicht erfüllt ist. In K gilt $2 = 0$.*

[1] Diese Beizeichnung ist nicht standard.

Das ist unbefriedigend, da für Anwendung in der Kryptographe endliche Körper der Charakteristik 2 wichtig sind. Um Charakteristik 2 (und auch 3) abzudecken, muss man die Definition von Weierstrass-Gleichung verallgemeinern. Wir werden dies hier nicht tun, da es etwas technisch ist. Kurzum reicht es mit den sogenannten langen Weierstrass-Gleichungen vom Typ

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

mit entsprechender (aber kompliziertere) Diskriminanten-Bedingung

$$\begin{aligned}
&- a_6a_1^6 + a_4a_3a_1^5 + ((-a_3^2 - 12a_6)a_2 + a_4^2)a_1^4 + (8a_4a_3a_2 + (a_3^3 + 36a_6a_3))a_1^3 \\
&+ ((-8a_3^2 - 48a_6)a_2^2 + 8a_4^2a_2 + (-30a_4a_3^2 + 72a_6a_4))a_1^2 \\
&+ (16a_4a_3a_2^2 + (36a_3^3 + 144a_6a_3)a_2 - 96a_4^2a_3)a_1 \\
&+ ((-16a_3^2 - 64a_6)a_2^3 + 16a_4^2a_2^2 + (72a_4a_3^2 + 288a_6a_4)a_2 \\
&+ (-27a_3^4 - 216a_6a_3^2 + (-64a_4^3 - 432a_6^2))) \neq 0.
\end{aligned}$$

zu arbeiten.
In Charakteristik $\neq 2$ und $\neq 3$ kann man jede lange Weierstrass-Gleichung mittels quadratisch und kubischem Ergänzen durch eine affine lineare Transformation auf eine Weierstrass-Gleichung umformen.

Nun wollen wir die Bedingung (2.2) rechtfertigen. Die partiell Ableitung eines Polynoms ist formal über jedem Körper definiert, es ist kein Grenzwertbegriff notwendig.

Lemma 2.4. *Sei F das Weierstrass-Polynom einer Weierstrass-Gleichung (2.1). Sei $(x, y) \in K^2$ mit $F(x, y) \neq 0$. Dann gilt*

$$\frac{\partial F}{\partial X}(x, y) \neq 0 \quad \textit{oder} \quad \frac{\partial F}{\partial Y}(x, y) \neq 0.$$

Beweis. Es gilt $F = Y^2 - X^3 - aX - b$ und $-2^4(4a^3 + 27b^2) \neq 0$. Insbesondere gilt $2 \neq 0$ in K. Weiterhin

$$\frac{\partial F}{\partial Y} = 2Y.$$

Sicher ist diese Ableitung $\neq 0$ an jedem Punkt (x, y) mit $y \neq 0$. Es reicht also zu zeigen, dass $\frac{\partial F}{\partial X}(x, 0) \neq 0$, falls $F(x, 0) = 0$.
Nun gilt

$$\underbrace{(X^3 + aX + b)}_{=F}(288aX - 432b) + \underbrace{(-3X^2 - a)}_{=\partial F/\partial X}(96aX^2 - 144bX + 64a^2) = -2^4(4a^3 + 27b^2) \neq 0$$

nach Voraussetzung. Wir substituieren X durch x und finden $\frac{\partial F}{\partial X}(x, 0) \neq 0$ da $F(x, 0)$. □

Bemerkung 2.5. *Im Fall $K = \mathbb{R}$ können wir dieses letzte Lemma geometrisch wie folgt interpretieren. Sei $(x, y) \in \mathbb{R}^2$ eine Nullstelle von F, dem Weierstrass-Polynom einer Weierstrass-Gleichung. Wir setzen*

$$\alpha = -\frac{\partial F}{\partial Y}(x, y) \quad \textit{und} \quad \beta = \frac{\partial F}{\partial X}(x, y).$$

Dann ist (α, β) nicht der Nullvektor.
Aus dem Satz von der impliziten Funktion folgt, wir die Nullstellenmenge von F in $\mathbb{R}^2$ in der Nähe von (x, y) durch den Graph einer glatten Funktion (nach einem möglichen Koordinatentausch) ausdrücken können.
Weiterhin ist die Menge

$$T = \{(x + \alpha t, y + \beta t) : t \in \mathbb{R}\}$$

eine Gerade durch (x, y). Wir definieren $f(t) = F(x + t\alpha, y + t\beta)$ für alle $t \in \mathbb{R}$. Dann gilt

$$\frac{d\gamma}{dt}(t) = \underbrace{F(x, y)}_{=0} + \left(\underbrace{\alpha \frac{\partial F}{\partial X}(x, y) + \beta \frac{\partial F}{\partial Y}(x, y)}_{=0} \right) t + \textit{(Terme der Ordnung} \geq 2 \textit{ in } t\textit{)}.$$

Also hat $t \mapsto F(x + t\alpha, y + t\beta)$ eine mehrfache Nullstelle bei $t = 0$. Dies bedeutet, dass T die Tangent an der Nullstellenmenge von F ist.
Zusammengefasst: die Gerade durch (x, y) mit Richtungsvektor

$$\left(-\frac{\partial F}{\partial Y}(x, y), \frac{\partial F}{\partial X}(x, y) \right)$$

liegt tangential an der Nullstellenmenge von F.

Die Schlussfolgerung von Lemma 2.4 besagt, dass die Nullstellenmenge einer Weierstrass-Gleichung an jedem Punkt einer Bedingung genügt, welche sich zumindest im reellen Fall als "Glattheitsbedigung" verstehen lässt.

Definition 2.6. *Sei F das Weierstrass-Polynom einer Weierstrass-Gleichung. Falls $(x, y) \in K$ und $y \neq 0$, dann heisst*

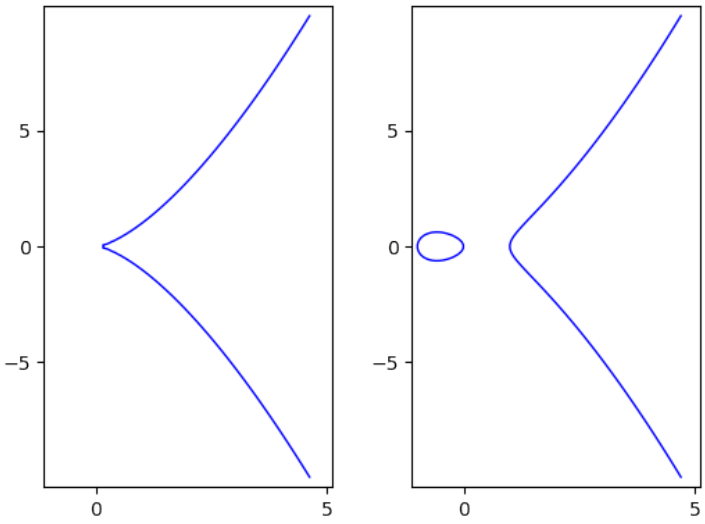
$$\frac{\frac{\partial F}{\partial X}}{-\frac{\partial F}{\partial Y}}(x, y) = \frac{3x^2 + a}{2y}$$

Tangentensteigung *an (x, y).*

Sei m die Tangentensteigung an (x, y). So wie in Beispiel 2.5 zeigt man, dass $F(x+t, y+mt)$ bei $t = 0$ eine Nullstelle der Ordnung ≥ 2 hat.

Beispiel 2.7. *Die Lösungsmenge von $Y^2 = X^3$ hat bei $(0, 0)$ eine "Spitze". Die Nullstellenmenge ist an diesem Punkt nicht glatt, vgl. Abbildung 2.1 links.*
In der gleichen Abbildung rechts ist eine glatte Kurve zu sehen.

Abbildung 2.1: Lösungsmenge von $Y^2 = X^3$ (links) und $Y^2 = X^3 - X$ (rechts)



2.2 Das Gruppengesetz

In diesem Abschnitt werden wir zeigen, wie man auf der Lösungsmenge einer Weierstrass-Gleichung zusammen mit einem zusätzlichen Punkt, eine Gruppenstruktur definieren kann. Die Konstruktion kann man rein geometrisch veraschaulichen. Wie oben bezeichnet K ein Körper in dem sich alles abspielt (sofern nicht anders vermerkt).

Definition 2.8. *Sei $Y^2 = X^3 + aX + b$ eine Weierstrass-Gleichung E. Wir definieren*

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

*wobei $\mathcal{O}$ zunächst ein weiteres Element ist, welches nicht in K^2 liegt. Man nennt $E(K)$ die **Menge der K-rationalen Punkten von** E.*

Beispiel 2.9. *Für die Weierstrass-Gleichung E gegeben durch $Y^2 = X^3 - X$ und für $K = \mathbb{Q}$ besagt der Satz von Fermat, Satz 1.9, dass*

$$E(\mathbb{Q}) = \{(0, 0), (\pm 1, 0), \mathcal{O}\}.$$

aus vier Elementen besteht.

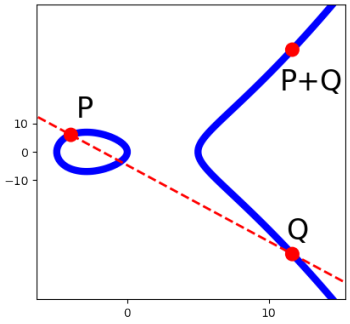
Wir werden zeigen, dass wir $E(K)$ mit der Struktur einer abelschen Gruppe verstehen können. Dazu müssen wir eine Verknüpfung $+\colon E(K) \times E(K) \to E(K)$, eine Inversionsabbildung $-\colon E(K) \to E(K)$, sowie ein neutrales Element in $E(K)$ produzieren.

2.2.1 Die Verknüpfung

Sei E eine Weierstrass-Gleichung gegeben durch $Y^2 = X^3 + aX + b$ mit $a, b \in K$. In einem ersten Schritt werden wir eine Verknüpfung

$$+\colon E(K) \times E(K) \to E(K)$$

Abbildung 2.2: $E : Y^2 = X^3 - 5^2X, P = (-4, 6), Q = (\frac{1681}{144}, -\frac{62279}{1728})$



definieren. Es ist üblich, die Verknüpfung mit "+" zu bezeichnen. Später werden wir feststellen, dass die so konstruierte Gruppe eine abelsche Gruppe ist.
Seien P und Q Elemente von $E(K)$. Es folgt eine Aufspaltung in verschiendene Fälle. Wir werden bereits in der Konstruktion überprüfen, dass die Verküpfung + die Bedingung

$$P + Q = Q + P \quad \text{für alle} \quad P, Q \in E(K)$$

erfüllt. Hieraus werden wir folgern, dass die Gruppe $E(K)$ abelsch ist.

Fall 1: Die Menge $\{P, Q, \mathcal{O}\}$ hat drei Elemente. In diesem Fall gilt $P = (x_1, y_1)$ und $Q = (x_2, y_2)$. Weiterhin haben wir $P \neq Q$. Daher gibt es genau eine Gerade G durch P und Q.
Wir unterscheiden zwei Unterfälle.
Unterfall 1a. Es gilt $x_1 \neq x_2$. In diesem Fall hat die Gerade G (endliche) Steigung $m = \frac{y_2 - y_1}{x_2 - x_1} \in K$. In anderen Worten, sie hat die Gesalt

$$G = \{(x, mx + q) : x \in K\}$$

mit $q = y_1 - mx_1$. Vgl. Abbildung 2.2 darin ist G gestrichelt.
Daher sind P und Q Schnittpunkte der Gerade G mit der Menge $E(K) \setminus \{\mathcal{O}\}$. Mit Vielfachheiten gezählt hat die Gerade G jedoch drei Schnittpunkte mit der Lösungsmenge von $Y^2 = X^3 + aX + b$. Wir können dies wie folgt direkt überprüfen. Dazu defineren wir das Polynom

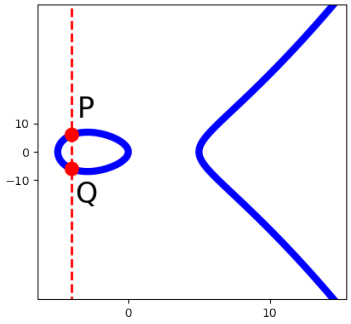
$$A = (mX + q)^2 - (X^3 + aX + b) = -X^3 + m^2X + (\text{Terme von Grad} \leq 1 \text{ in } X) \in K[X].$$

Das Polynom A hat Grad 3 und wir kennen bereits zwei verschiedene Nullstellen: $x_1, x_2 \in K$. Daher lässt sich A durch $X - x_1$ und $X - x_2$ teilen. Es gilt also $A = -(X - x_1)(X - x_2)(X - x_3)$, dabei muss x_3 als wiederum ein Element in K sein, denn es gilt $x_1 + x_2 + x_3 = m^2$, also

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_2 - x_1.$$

Nach Konstruktion ist das Paar (x_3, y_3) mit $y_3 = mx_3 + q$ eine Nullstelle von $Y^2 - (X^3 + aX + b)$. Weiterhin ist auch $(x_3, -y_3)$ eine Nullstelle.

Abbildung 2.3: $E : Y^2 = X^3 - 5^2X, P = (-4, 6), Q = (-4, -6)$



In Unterfall 1a definieren wir

$$P + Q = (x_3, -y_3) \in E(K) \setminus \{\mathcal{O}\}.$$

Sind wir in Unterfall 1a, so ist auch das Paar (Q, P) in Unterfall 1a. Es gilt $P+Q = Q+P$, da die Gerade und sowohl (m, q) unabhängig von der Reihenfolge von P, Q ist.
Unterfall 1b. Es gilt $x_1 = x_2$. Nun liegt die Gerade G senkrecht zur Abszisse, vgl. Abbildung 2.3. Es gilt

$$y_1^2 = x_1^3 + ax_1 + b = x_2^3 + ax_2 + b = y_2^2$$

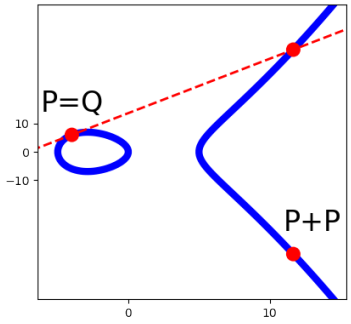
und daher $y_1 = -y_2$ da $P \neq Q$. Nun stehen wir vor einem Dilemma, die Gerade G hat keine weiteren Schnittpunkte mit $E(K)$ in der Ebene K^2. Jetzt kommt uns der Punkt $\mathcal{O}$ zur Hilfe.
In Unterfall 1b definieren wir

$$P + Q = \mathcal{O} \in E(K).$$

Vertauscht man P, Q so bleiben wir in Unterfall 1b und es gilt trivialerweise $P + Q = Q + P$.

Fall 2: Die Menge $\{P, Q, \mathcal{O}\}$ hat zwei Elemente. Auch hier gibt es mehrere Unterfälle.
Unterfall 2a: Es gilt $P = Q \neq \mathcal{O}$ und $P = (x, y)$ mit $y \neq 0$.
Die Gerade, welche in Fall 1 konstruiert wurde, ist nun nicht eindeutig bestimmt.
Etwas Intuition schafft die folgende Überlegung. Wir versetzen uns in die reelle Welt und ersetzen den Punkte Q durch eine Folge von Punkten $(Q_n)_{n\in\mathbb{N}}$ aus $E(\mathbb{R}) \setminus \{Q, \mathcal{O}\}$, dessen Koordinaten für $n \to \infty$ gegen $Q = P$ konvergieren. Die Gerade G_n durch P und Q_n ist wohldefiniert und die Summe $P + Q_n$ lässt sich mit der Vorschrift aus Fall 1 bestimmen. Anschaulich nähert sich die Gerade G_n der Tangente and $E(\mathbb{R}) \setminus \{\mathcal{O}\}$ durch den Punkte P. Vgl. Abbildung 2.4.
Für einen allgemeinen Körper können wir zwar nicht mit solchen Grenzbegriffen argumentieren, aber wir haben einen Ersatz für die Tangente in Bemerkung 2.5 und Definition 2.6 gefunden.

Abbildung 2.4: $E : Y^2 = X^3 - 5^2X, P = Q = (-4, 6)$



Für $y \neq 0$ dürfen wir Definition 2.6 anwenden. Das weitere Vorgehen ist vergleichbar mit Unterfall 1a. Wir setzen

$$m = \frac{3x^2 + a}{2y} \in K \quad \text{und} \quad q = y - mx \in K.$$

Das Polynom

$$A = (mX + a)^2 - (X^3 + aX + b) \in K[X]$$

hat nur eine Nullstelle der Ordnung ≥ 2 in x. Dies lässt sich rein formal mit Hilfe der Definition von m überprüfen. Also gilt $A = -(X - x)^2(X - x')$ für ein $x' \in K$. Dabei gilt

$$x' = m^2 - 2x = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x.$$

Der Punkt (x', y') mit $y' = mx' + q$ liegt in $E(K)$. Wie in Unterfall 1a liegt $(x', -y')$ auch in $E(K)$. In Unterfall 2a definieren wir

$$P + Q = P + P = (x', -y').$$

Trivialierweise gilt $P + Q = Q + P$ in diesem Unterfall.
Unterfall 2b: Es gilt $P = Q \neq \mathcal{O}$ und $P = (x, 0)$. Im Fall $y = 0$ ist die Tangente durch P and $E(K)$ parallel zur Ordinate. Wir definieren

$$P + Q = P + P = (x, 0) + (x, 0) = \mathcal{O}.$$

Trivialierweise gilt $P + Q = Q + P$ in diesem Unterfall.
Unterfall 2c: Es gilt $P = \mathcal{O} \neq Q$. Wir definieren

$$P + Q = \mathcal{O} + Q = Q.$$

Unterfall 2d: Es gilt $P \neq \mathcal{O} = Q$. Dieser Fall ist analog zu Unterfall 2b, wir definieren hier

$$P + Q = P + \mathcal{O} = P.$$

Vergleicht mah Unterfälle 2b und 2c, so sehen wir $P + Q = Q + P$, falls $P = \mathcal{O}$ oder $Q = \mathcal{O}$.

Fall 3: Die Menge $\{P, Q, \mathcal{O}\}$ hat ein Elemente. Es gilt $P = Q = \mathcal{O}$ und wir definieren

$$P + Q = \mathcal{O} + \mathcal{O} = \mathcal{O}.$$

Trivialerweise gilt $P + Q = Q + P$.

2.2.2 Die Inversionsabbildung

Sei $P \in E(K)$. Hier gibt es nur zwei Fälle.
Fall 1. Es gilt $P \neq \mathcal{O}$. In diesem Fall gilt $P = (x, y)$. Wegen $y^2 = x^3 + ax + b$ ist auch $(x, -y)$ eine Lösung der Weierstrass-Gleichung. Wir definieren

$$-P = (x, -y) \in E(K) \setminus \{0\}.$$

Fall 2. Es gilt $P = \mathcal{O}$. Wir definieren

$$-P = \mathcal{O} \in E(K).$$

2.2.3 Das neutral Element

Es sollte nun nicht überraschen, dass wir $\mathcal{O}$ als das neutrale Element designieren.

2.3 Überprüfung der Gruppenaxiome

Satz 2.10. *Sei E eine Weierstrass-Gleichung mit Koeffizienten in einen Körper K. Sei $\cdot$ die Verknüpfung aus Abschnitt 2.2.1. Dann ist $(E(K), +, \mathcal{O})$ eine abelsche Gruppe.*

Die Abbildung $+ \colon E(K) \times E(K) \to E(K)$ ist wohldefiniert. Weiterhin überprüfen wir mit der Hilfe von den Unterfällen 1b, 2b und Fall 3 der Konstruktion, dass

$$(-P) + P = \mathcal{O}$$

für alle $P \in E(K)$.
Weiterhin ist $\mathcal{O} + P = P$ für alle $P \in \mathcal{O}$, dies folgt aus den Unterfällen 2c, 2d und Fall 3 in der Konstruktion.
Schliesslich muss noch die Assoziativität der Verknüpfung gezeigt werden. Dies läuft auf die Gleichung

$$P + (Q + R) = (P + Q) + R$$

für alle $P, Q, R \in E(K)$ hinaus.
Das ist ein nicht-trivialer Schritt den wir hier nicht beweisen werden. Es gibt mehrere Ansätz die Assoziativität zu zeigen. Naheliegend ist es, die Gleichheit mit der Definition direkt zu überprüfen. Das ist im Prinzip möglich. Dazu müssen jedoch die vier Verknüpfungen $Q + R, P + (Q + R), P + Q$ und $(P + Q) + R$ gebildet werden. Pro Verknüpfung gibt es 7 Fälle zu unterscheiden. D.h. ingesamt gibt es $7^4 = 2041$ Fälle.

Obwohl einige Fälle trivialerweise stimmen, ist ein systematisches Arbeiten mit viel Aufwand verbunden.
Es gibt einen weiteren Zugang zur Assoziativität über die sogenannte **Picard-Gruppe**, einem Objekt der algebraischen Geometrie welches man E zuordnen kann. Die Picard-Gruppe ist aus theoretischen Überlegungen *a priori* eine abelsche Gruppe. Die Idee ist nun, eine bijektive Abbildung zwischen $E(K)$ und der Picard-Gruppe zu konstruieren, welche die oben dargestellte Verknüpfung mit dem Gruppengesetzt der Picard-Gruppe in Verbindung setzt.
Die Verknüpfung $E(K) \times E(K) \to E(K)$ sowie die Inversion $E(K) \to E(K)$ werden mit der Hilfe von Quotienten von Polynomen mit Koeffizienten in K beschrieben.

f36750f344144e009de3efe49ef8f9d1d5f6ba24