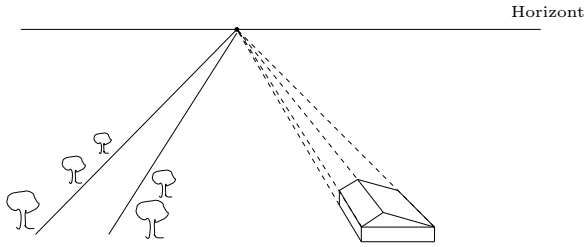
§ 16 Etwas projektive Geometrie

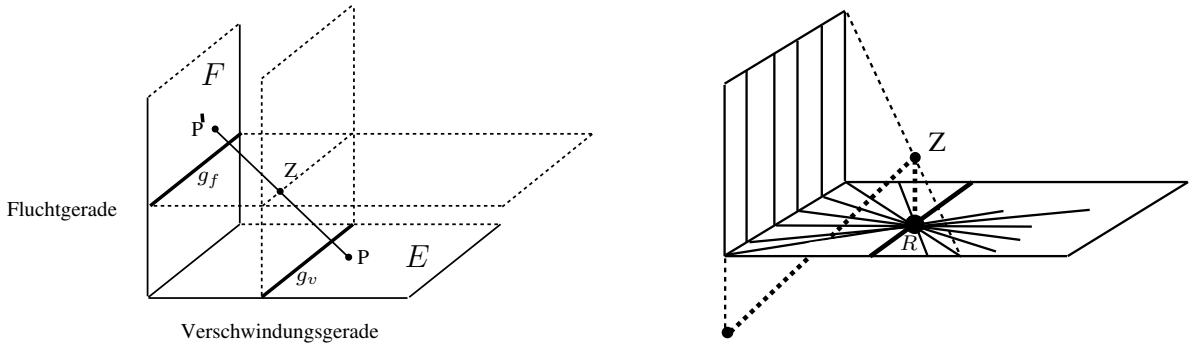
16.1 Motivation: Zentralprojektion

Auf Fotografien und Bildern treffen sich parallele Geraden oft in einem Punkt am Horizont. Bei perspektivischen Zeichnungen sind solche Punkte, sogenannte *Fluchtpunkte*, wesentliche Konstruktionshilfen.



Figur 16.1: Parallele Geraden treffen sich im „Unendlichen“.

Wir behandeln nun zuerst eine **Zentralprojektion** ζ in $\mathbb{R}^3$ mit Zentrum Z von einer Ebene E auf eine dazu nicht parallele Ebene F. Dabei wird einem Punkt P von E der Schnittpunkt P' der Geraden ZP mit F zugeordnet. (Siehe Figur 16.2 a) !)



a) b)

Figur 16.2: Zentralprojektion der Ebene E auf die Ebene F mit Zentrum Z

Nicht alle Punkte von E haben einen Bildpunkt und nicht alle Punkte von F ein Urbild: Die Schnittgerade g_v der durch Z gehenden zu F parallelen Ebene mit E besteht genau aus denjenigen Punkten, die kein Bild besitzen. Analog besitzen die Punkte der Schnittgeraden g_f der mit Z inzidierenden zu E parallelen Ebene mit F kein Urbild. (Siehe ebenfalls Figur 16.2 a) !). Die Gerade g_v heißt **Verschwindungsgerade**, die Gerade g_f **Fluchtgerade**,
Bei der Abbildung $\zeta : E \setminus g_v \to F \setminus g_f$ werden Geraden von $E \setminus g_v$ (die ja mit Z eine Ebene aufspannen) auf Geraden von $F \setminus g_f$ (die Schnitte dieser Ebenen mit F) abgebildet – und umgekehrt haben Geraden von $F \setminus g_f$ als Urbilder Geraden von $E \setminus g_v$.

Betrachtet man nun, was mit einem Geradenbüschel durch einen Punkt R von g_v passiert, so sieht man, dass die Bilder dieser Geraden in F keinen Punkt gemeinsam haben und damit parallel sind. (Siehe Figur 16.2 b)!) „Der Bildpunkt von R liegt also auf dieser Parallelenschar im Unendlichen“. Dadurch motiviert definiert man:

16.2 Projektive Erweiterung der reellen affinen Ebene

Als *projektive Erweiterung* $\mathrm{PG}(\mathcal{A})$ der reellen affinen Ebene $\mathcal{A} = \mathrm{AG}(\mathbb{R}^2) =: \mathrm{AG}(2,\mathbb{R})$ bezeichnen wir folgende Geometrie:

(i) *Punkte* von $\mathrm{PG}(\mathcal{A})$ sind die Punkte von $\mathcal{A}$ (die **eigentlichen Punkte**) und die Parallelenscharen der Geraden von $\mathcal{A}$. Also: Jede Menge aller zu einer Geraden parallelen Geraden bildet per definitionem einen neuen Punkt, einen sogenannten „**uneigentlichen oder idealen Punkt**“.

(ii) *Geraden* von $\mathrm{PG}(\mathcal{A})$ sind die Geraden von $\mathcal{A}$, jede erweitert um den eindeutig bestimmten uneigentlichen Punkt in ihrer Richtung, und eine weitere Gerade, bestehend aus allen uneigentlichen Punkten, die **uneigentliche Gerade** g_∞.

(iii) Ein eigentlicher Punkt *inzidiert* mit einer eigentlichen Geraden, falls das auch in $\mathcal{A}$ der Fall ist. Ein uneigentlicher Punkt inzidiert mit einer eigentlichen Geraden, falls diese zu seiner Parallenschar gehört. Und g_∞ inzidiert genau mit den uneigentlichen Punkten.

Übungsaufgabe 16.1 Zeigen sie, dass in $\mathrm{PG}(\mathcal{A})$ je zwei Punkte durch genau eine Gerade verbunden sind und je zwei Geraden sich in genau einem Punkt schneiden.

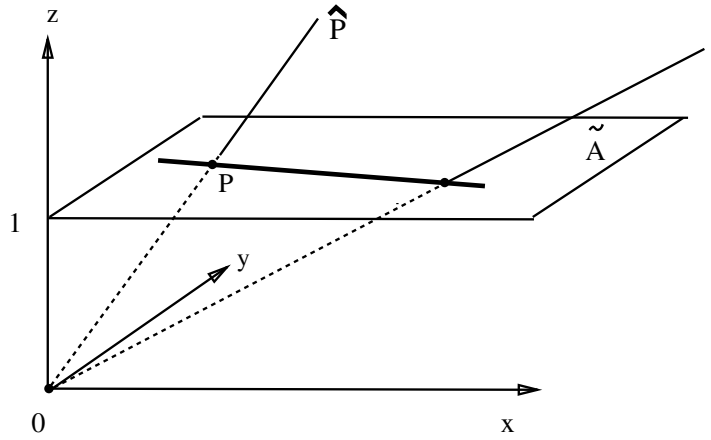
Um die neue Geometrie koordinatisieren zu können, wählen wir Z als den Nullpunkt O unseres Koordinatensystem und E als die (zu $\mathcal{A}$ isomorphe) Ebene $\tilde{A}$ mit der Gleichung $z = 1$; nun ordnen wir jedem Punkt P von $\tilde{A}$ die Gerade $\hat{P} := PO$ zu und jeder Geraden g von $\tilde{A}$ die Ebene, die von g und O aufgespannt wird. (Siehe Figur 16.3a).

16.3 Definition: homogene Koordinaten

Ein eigentlicher Punkt der affinen Ebene $\mathcal{A}$ mit den Koordinaten $(x,y) \in \mathcal{A}$ (bzw. $(x,y,1) \in \tilde{A}$) entspricht der Geraden $(x,y,1)\mathbb{R}$; die uneigentlichen Punkte entsprechen den Geraden der Form $(x,y,0)\mathbb{R}$. Umgekehrt definiert jede Gerade einen eigentlichen oder uneigentlichen Punkt.
Jedem Koordinatentripel (ξ_1,ξ_2,ξ_0) mit $\xi_0 \neq 0$ ordnen wir daher einen affinen Punkt zu durch:

$$\hat{P} := (\xi_1,\xi_2,\xi_0)\mathbb{R} \mapsto (\frac{\xi_1}{\xi_0},\frac{\xi_2}{\xi_0},1) = P.$$

(ξ_1,ξ_2,ξ_0) heißt *homogenes Koordinatentripel* von P; es ist nur bis auf einen Faktor eindeutig bestimmt.
Analog lässt sich jedem $(\xi_1,\xi_2,0)$ mit $\xi_1 \neq 0 \vee \xi_2 \neq 0$ ein uneigentlicher Punkt zuordnen. Man kommt damit zu der in folgender Definition beschriebenen Geometrie:



Figur 16.3a: Zur Einführung homogener Koordinaten
$(x, y) \mapsto P = (x, y, 1) \mapsto \hat{P} = (x, y, 1)\mathbb{R})$.

16.4 Definition: Reelle projektive Ebene

Die *projektive Ebene* $\mathrm{PG}(2, \mathbb{R})$ =$\mathrm{PG}(\mathbb{R}^3)$ ist wie folgt definiert:

(i) Punkte sind die $1-$dim Unterräume von $\mathbb{R}^3$.

(ii) Geraden sind die $2-$dim Unterräume von $\mathbb{R}^3$.

(iii) Inzidenz ist Enthaltensein.

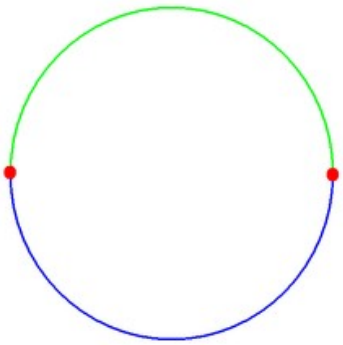
16.5 Anmerkungen zur projektiven Geometrie

a.) Eine Verallgemeinerung auf beliebige Schiefkörper und auf andere Dimensionen ist möglich.

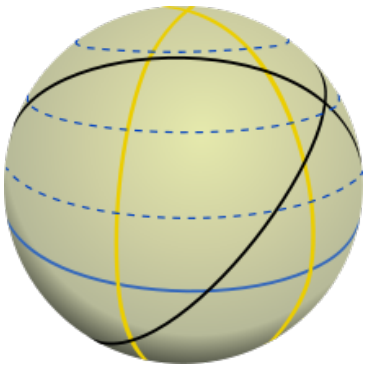
b.) Der Vorteil der projektiven Geometrie ist u.a., dass

- die Punkte, Geraden, Ebenen etc. jetzt lineare Unterräume und keine anderen affinen Unterräume sind
- affin-lineare Abbildungen, wie man zeigen kann, nun durch lineare Abbildungen dargestellt werden
- Fallunterscheidungen bzgl. Existenz von Schnittpunkten von Geraden in einer Ebene nicht nötig sind
- Punkte und Hyperebenen „dual“ zueinander sind
- die reelle affine Ebene (nach Auszeichnung einer Geraden als uneigentliche Gerade) in $\mathrm{PG}(2, \mathbb{R})$ wiederzufinden ist (bzw. der $n-$dim affine Raum über K durch Auszeichnung einer Hyperebene in $\mathrm{PG}(K^{n+1})$ als uneigentliche Hyperebene erhalten wird.)
- Kurven, z.B. Kegelschnitte, sich “vereinheitlichen” lasssen: Hyperbeln und Parabeln als 'Ellipsen' mit uneigentlicher Sekante bzw. Tangente.

c.) Eine weitere Darstellung der reellen projekiven Ebene geht von der schon bei der Koordinatisierung (16.3) benutzten Zuordnung der Punkte und Geraden der projektiven Ebene zu den Geraden und Ebenen durch den Nullpunkt im $\mathbb{R}^3$. Nur wird diesmal nicht mit einer Ebene geschnitten, sondern mit einer Nullpunkt-Sphäre (Oberfläche einer Kugel mit dem Nullpunkt als Mittelpunkt). Der Schnitt mit einer Geraden durch den Mittelpunkt der Kugel führt dann zu einem Paar *antipodaler* Punkte als einem projektiven Punkt (s.Figur 16.3b) und der Schnitt mit einer Nullpunkt-Ebene zu einem *Großkreis* (als einer projektiven Geraden) (s.Figur 16.3c).



Figur 16.3b:
Antipodales Punktepaar



Figur 16.3c: Kugeloberfläche mit verschiedenen Großkreisen (durchgezogene Linien). Die gelben Großkreise sind hier Längenkreise. Neigung der 2 schwarzen Großkreise gegen den Äquator (blau) ca. 55° und 60°.

Alternativ kann man sich dabei auch auf eine Halbkugel beschränken, sodass nur antipodale Punkte auf dem Äquator (als uneigentlicher Geraden) identifiziert werden müssen.

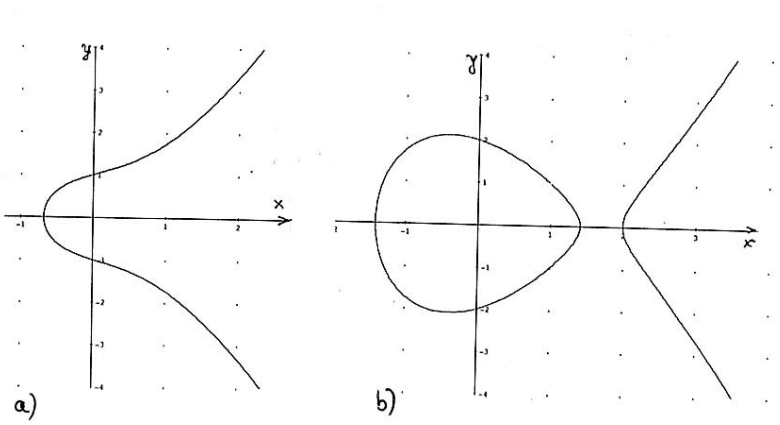
16.6 Anwendung bei Elliptischen Kurven

(a) *Definition*
Sei K ein Körper; oft wird hier $K \in \{\mathbb{R}, \mathrm{GF}(p)\}$ genommen. Seien ferner $b, c \in K$ fest gewählt. Wir betrachten zunächst in der affinen Eben $\mathrm{AG}(K^2)$ über K die kubische Kurve (vgl. Figur 16.4) der Punkte, die die Gleichung

$$(*) \quad y^2 = x^3 + bx + c$$

erfüllen, also

$$\mathcal{C} := \big\{(x, y) \in K^2 \mid y^2 = x^3 + bx + c\big\}.$$



Figur 16.4: Beispiele kubischer Kurven im Reellen mit Gleichung
$y^2 = f(x)$, wobei $f(x)$ ein Polynom vom Grad 3 ist mit
a) einer reellen Nullstelle b) drei reellen Nullstellen ist

$\mathcal{C}$ ist eine *elliptische Kurve* (vom sogenannten 'Weierstrass-Typ') (vgl. Figuren 16.4/16.5)
(b) *Projektive Koordinaten*
Ersetzt man x und y in Gleichung $(*)$ durch

$$x = \frac{\xi_1}{\xi_0} \quad \text{und} \quad y = \frac{\xi_2}{\xi_0} \quad \text{mit} \quad \xi_0 \neq 0,$$

so ergibt sich (nach Multiplikation mit ξ_0^3)

$$(*') \quad \xi_2^2\xi_0 = \xi_1^3 + b\xi_1\xi_0^2 + c\xi_0^3.$$

Für die affinen Punkte ist $(*)$ zu $(*')$ äquivalent. Für einen uneigentlichen Punkt (mit Koordinate $\xi_0 = 0$) ist $(*')$ genau für $\mathcal{O} := K(0,1,0)$ erfüllt. Dieser Punkt kommt also als einziger projektiver Punkt zu $\mathcal{C}$ hinzu.
$\mathcal{O}$ liegt auf den Geraden mit Gleichung $\xi_1 - c\xi_0 = 0$, also auf den Geraden mit affiner Gleichung $x = c$ (für $c \in K$). Daher ist $\mathcal{O}$ der Fernpunkt in $y-$Richtung.
(c) *Anmerkung 1:*

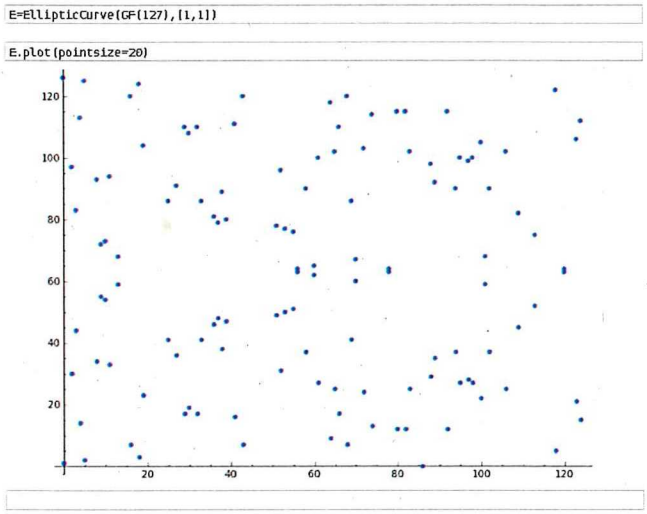
Auf $\overline{\mathcal{C}} := \mathcal{C} \cup \{O\}$ lässt sich eine Addition definieren, im Wesentlichen wie folgt:
$P + Q$ ist definiert als der Punkt, den man durch Spiegelung des Schnittpunktes der Geraden PQ mit $\mathcal{C}$ an der $x-$Achse erhält (s.z.B. Figur 16.6a), und $R + R$ als der an der $x-$Achse gespiegelte Schnittpunkt der Tangente an $\mathcal{C}$ in R (s.Figur 16.6b). Wie man zeigen kann, erhält man so zusammen mit $\mathcal{O}$ als neutralem Element eine kommutative Gruppe.

(d)*Anmerkung 2:*

Für einen geeigneten fest gewählten Punkt $P \in \mathcal{C}$ definiert man

$$Q = mP := P + P + \ldots + P \quad (\text{mit } m \text{ Summanden}).$$

Dabei ist die Berechnung von Q aus m und P vergleichsweise leicht, umgekehrt die Berechnung von $m := \log_P Q$ viel schwerer. Dieser Sachverhalt ist zum Chiffrieren

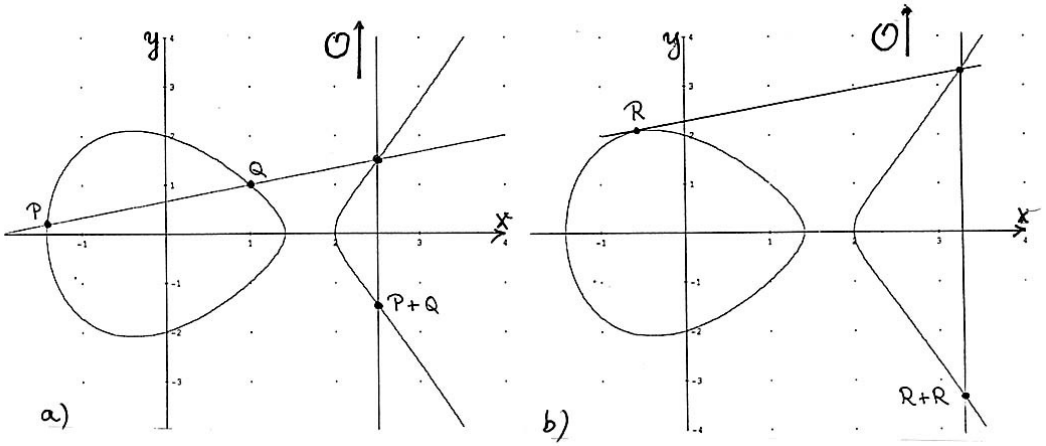


Figur 16.5: Elliptische Kurve über $\mathbb{Z}_{127}$ (erstellt mithilfe von Sage; vgl. Schulz/Witten/Esslinger: Rechnen mit Punkten einer elliptischen Kurve. LOG IN Heft 181/182 (2015))

in der Kryptographie ausnutzbar (–> Problem des diskreten Logarithmus.) Bei der Elliptischen-Kurven-Kryptographie (ECC) ist die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) (Stand 9.1.2023, gesehen 10.1.2023) empfohlene Schlüssellänge[52] von mindestens 250 Bit für die Ordnung des Basispunktes P (~~bei Verwendung bis 2023~~) deutlich niedriger als die empfohlene Schlüssellänge von ~~2000 Bit (übergangsweise bis Ende 2023, danach~~ von 3000 Bit) beim RSA-Verfahren[53] (–> Problem der Primfaktorzerlegung).

[52] https://www.bsi.bund.de>BSI>TechnischeRichtlinien>BSI-TR-02102

[53] s.z.B. R.-H.Schulz: Codierungstheorie. Eine Einführung, Verlag Fr.Vieweg&Sohn, 2.Auflage 2003.



Figur 16.6: Zur Definition der Summe von Punkten
einer elliptischen Kurve ('Sehnen/Tangenten-Addition')
(vgl. Schulz/Witten/Esslinger, l.c.)