Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

Elliptische Kurven

Vorlesung 3

Elliptische Kurven lassen sich nicht in der affinen Ebene realisieren, vielmehr handelt es sich um projektive Kurven, die in der projektiven Ebene realisiert werden.

Der projektive Raum

Die Geraden durch einen Punkt

DEFINITION 3.1. Es sei K ein Körper. Der *projektive n-dimensionale Raum* $\mathbb{P}_K^n$ besteht aus allen Geraden des $\mathbb{A}_K^{n+1}$ durch den Nullpunkt, wobei diese Geraden als Punkte aufgefasst werden. Ein solcher Punkt wird repräsentiert durch *homogene Koordinaten* $(a_0, a_1, \ldots, a_n)$, wobei nicht alle $a_i = 0$ sein dürfen, und wobei zwei solche Koordinatentupel genau dann den gleichen Punkt repräsentieren, wenn sie durch Multiplikation mit einem Skalar $\lambda \in K^\times$ ineinander übergehen.

Wir werden den projektiven Raum nach und nach mit zusätzlichen Strukturen versehen.

SATZ 3.2. *Es sei K ein Körper und sei $\mathbb{P}_K^n$ ein projektiver Raum. Es sei $i \in \{0, 1, \ldots, n\}$ fixiert. Dann gibt es eine natürliche Abbildung*

$$\varphi_i \colon \mathbb{A}_K^n \longrightarrow \mathbb{P}_K^n,\ (u_1, \ldots, u_n) \longmapsto (u_1, \ldots, u_i, 1, u_{i+1}, \ldots, u_n).$$

Diese Abbildung ist injektiv und induziert eine Bijektion zu denjenigen Punkten des projektiven Raumes, bei denen die i-te homogene Koordinate nicht 0 *ist. Die Umkehrabbildung wird durch*

$$\begin{aligned}\mathbb{P}_K^n \supset D_+(X_i) := \{(x_0, x_1, \ldots, x_n) \mid x_i \neq 0\} &\longrightarrow \mathbb{A}_K^n(x_0, x_1, \ldots, x_n) \\ &\longmapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)\end{aligned}$$

gegeben. Der projektive Raum wird überdeckt von diesen $n+1$ affinen Räumen. Das Komplement eines solchen affinen Raumes $\mathbb{A}^n_K \cong D_+(X_i) \subset \mathbb{P}^n_K$ ist ein $(n-1)$-dimensionaler projektiver Raum.

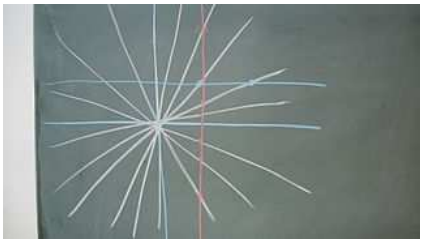
Beweis. Die Abbildung ist offensichtlich wohldefiniert, da die 1 sicher stellt, dass mindestens eine homogene Koordinate nicht 0 ist. Die Abbildung ist injektiv, da aus einer Gleichung der Form (für homogene Koordinaten)

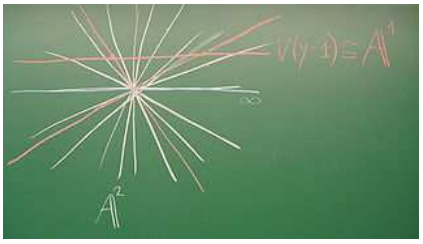
$$(u_1, \ldots, u_i, 1, u_{i+1}, \ldots, u_n) = \lambda(v_1, \ldots, v_i, 1, v_{i+1}, \ldots, v_n)$$

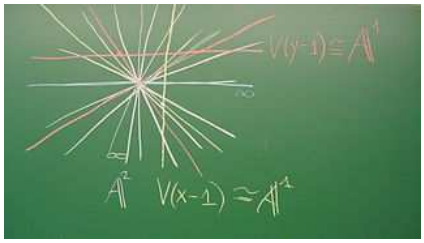
sofort $\lambda = 1$ wegen der 1 folgt. Die Umkehrabbildung ist auf der angegebenen Teilmenge wohldefiniert, und ist invers zu der Abbildung. Die Überdeckungseigenschaft ist klar, da für jeden Punkt des projektiven Raumes mindestens eine homogene Koordinate nicht 0 ist. Das Komplement zu $D_+(X_i)$ ist

$$V_+(X_i) = \{(x_0, x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \mid x_j \in K\}$$

mit keinerlei Einschränkung an die übrigen n Variablen und mit der Identifizierung von zwei solchen Tupeln, wenn sie durch Multiplikation mit einem Skalar ineinander übergehen. □

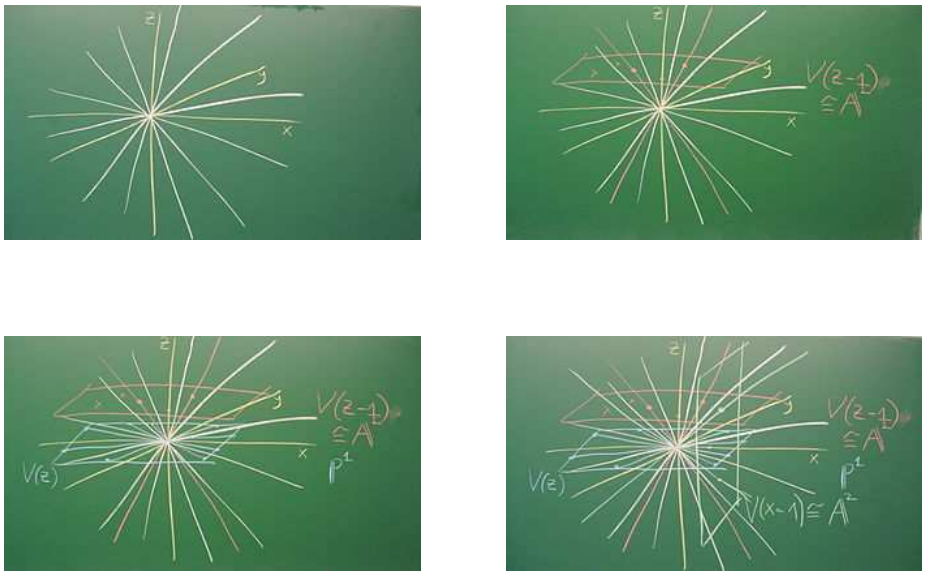






Beispiel 3.3. Die projektive Gerade $\mathbb{P}^1_K$ ist als die Menge der Geraden durch den Nullpunkt in der affinen Ebene $\mathbb{A}^2_K$ gegeben. Eine solche Gerade ist entweder die x-Achse oder aber eine Gerade, die die Gerade $V(y-1)$ (also die zur x-Achse parallele Gerade durch $(0,1)$) in genau einem Punkt schneidet. Umgekehrt liefert jeder Punkt $P \in V(y-1) \cong \mathbb{A}^1_K$ eine eindeutig bestimmte Gerade durch den Nullpunkt. D.h. die projektive Gerade besteht aus einer affinen Gerade und einem weiteren Punkt, den man den „unendlich fernen“ Punkt nennt. Wichtig ist dabei aber, dass dieser unendlich ferne Punkt nicht

wesensverschieden von den anderen Punkten ist. Wenn man eine beliebige Gerade G durch den Nullpunkt nimmt sowie eine dazu parallele Gerade $L \neq G$, so übernimmt L die Rolle der affinen Geraden, und G repräsentriert dann einen (von dieser affinen Geraden aus gesehen) unendlich fernen Punkt.



Beispiel 3.4. Die Punkte in der projektiven Ebene $\mathbb{P}^2_K$ entsprechen den Geraden durch den Nullpunkt im affinen Raum $\mathbb{A}^3_K$. Jeder Punkt der projektiven Ebene wird repräsentiert durch ein Tupel (x, y, z), wobei nicht alle x, y, z gleichzeitig 0 sein dürfen und wobei zwei Koordinatentupel identifiziert werden, wenn sie durch Multiplikation mit einem Skalar $\lambda \neq 0$ ineinander überführt werden können. Die projektive Ebene wird überdeckt durch drei affine Ebenen, nämlich

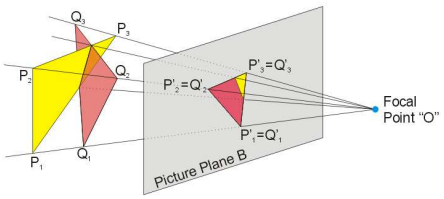
$$D_+(X),\ D_+(Y) \text{ und } D_+(Z)\,.$$

Dabei besteht $D_+(Z)$ aus allen Punkten, wo die dritte Koordinate nicht 0 ist. Durch Multiplikation mit z^{-1} kann man diese Punkte mit

$$\left(\frac{x}{z},\ \frac{y}{z},\ \frac{z}{z}\right) = (u,\ v,\ 1)$$

identifizieren, so dass wirklich eine affine Ebene vorliegt. Das Komplement der affinen Ebene $D_+(Z)$ ist die Menge $V_+(Z)$ der Punkte, wo die dritte Komponente 0 ist. Da man nach wie vor Punkte identifiziert, die durch Multiplikation mit einem Skalar ineinander überführbar sind, ist $V_+(Z)$ eine projektive Gerade. Ein Punkt $(x, y, 0)$ auf dieser Geraden und der Nullpunkt $(0, 0, 1)$ von $D_+(Z)$ definieren die Gerade durch den Nullpunkt mit dem Richtungsvektor (x, y) (und der homogenen Geradengleichung $yX - xY = 0$ bzw. $V_+(yX - xY)$). Man kann sich also die projektive Ebene gut vorstellen als

eine affine Ebene, in der jede Gerade durch den Nullpunkt noch einen zusätzlichen („unendlich fernen“) Punkt definiert.



Zwischen dem affinen Raum $\mathbb{A}_K^{n+1}$ und dem projektiven Raum $\mathbb{P}_K^n$ gibt es keine natürliche Abbildung. Allerdings gibt es die sogenannte *Kegelabbildung*, die auf dem punktierten $(n+1)$-dimensionalen affinen Raum definiert ist.

Definition 3.5. Die Abbildung

$$\mathbb{A}_K^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}_K^n,\ (x_0,\, x_1,\, \ldots,\, x_n) \longmapsto (x_0,\, x_1,\, \ldots,\, x_n)\,,$$

die einem Punkt $\neq 0$ die durch diesen Punkt und den Nullpunkt bestimmte Gerade zuordnet, heißt *Kegelabbildung*.

Die Kegelabbildung ist also in der Spitze des Kegels nicht definiert.

Nullstellen von homogenen Polynomen

Für ein beliebiges Polynom $F \in K[X_0, \ldots, X_n]$ ergibt es keinen Sinn zu sagen, ob ein Punkt $P \in \mathbb{P}_K^n$ eine Nullstelle davon ist, da diese Eigenschaft nicht invariant unter der Multiplikation mit einem Skalar ist und daher vom Repräsentanten von P abhängt. Für homogene Polynome sieht das anders aus.

Lemma 3.6. *Es sei K ein Körper und sei $F \in K[X_0, \ldots, X_n]$ ein homogenes Polynom vom Grad d. Dann gilt für einen Punkt $(x_0, \ldots, x_n)$ und einen Skalar λ die Beziehung*

$$F(\lambda x_0, \ldots, \lambda x_n) \;=\; \lambda^d F(x_0, \ldots, x_n).$$

Insbesondere verschwindet F in $(x_0, \ldots, x_n)$ genau dann, wenn F für ein beliebiges $\lambda \neq 0$ in $\lambda(x_0, \ldots, x_n)$ verschwindet.

Beweis. Dies kann man auf den Fall eines Monoms vom Grad d zurückführen. Für $X_0^{d_0} \cdots X_n^{d_n}$ mit $\sum_{i=0}^n d_i = d$ und $\lambda \in K$ gilt

$$(\lambda X_0)^{d_0} \cdots (\lambda X_n)^{d_n} \;=\; (\lambda^{d_0} X_0^{d_0}) \cdots (\lambda^{d_n} X_n^{d_n}) \;=\; \lambda^d (X_0^{d_0} \cdots X_n^{d_n}).$$

□

Man beachte, dass es durch diese Aussage zwar wohldefiniert ist, ob ein homogenes Polynom an einem projektiven Punkt verschwindet oder nicht, dass es aber keinen Sinn ergibt, einem homogenen Polynom einen Wert an jedem Punkt des projektiven Raumes zuzuordnen. Ein homogenes Polynom definiert keine Funktion auf dem projektiven Raum.

Definition 3.7. Es sei K ein Körper. Zu einem homogenen Polynom $F \in K[X_0, X_1, \ldots, X_n]$ bezeichnet man die Menge

$$V_+(F) = \{P = (x_0, \ldots, x_n) \in \mathbb{P}^n_K \mid F(x_0, \ldots, x_n) = 0\}$$

als die *projektive Nullstellenmenge* zu F.

Wenn man $V_+(F) \subseteq \mathbb{P}^n_K$ bestimmen möchte, so kann man die disjunkte Zerlegung

$$\mathbb{P}^n_K = D_+(X_0) \uplus V_+(X_0)$$

(ebenso für jede andere Variable) ausnutzen. Zur Bestimmung von $V_+(F) \cap D_+(X_0)$ setzt man in F die Variable X_0 gleich 1 und muss die Lösungen im affinen Raum $\mathbb{A}^n_K \cong D_+(X_0)$ von $F\frac{1}{X_0} = 0$ finden. Dabei wird das Polynom inhomogen, gleichzeitig eliminiert man eine Variable. Die Dimension bleibt gleich, die Situation wird aber affin. Zur Bestimmung von $V_+(F) \cap V_+(X_0)$ setzt man in F die Variable X_0 gleich 0 und muss die Lösungen im projektiven Raum $\mathbb{P}^{n-1}_K \cong V_+(X_0)$ von $F\frac{0}{X_0} = 0$ finden. Hier eliminert man eine Variable, das Polynom bleibt homogen, man bleibt projektiv, die Dimension reduziert sich um 1.

Beispiel 3.8. Die einfachsten homogenen Polynome in $K[X_0, X_1, \ldots, X_n]$ sind die vom Grad 1, also Ausdrücke der Form

$$F = a_0X_0 + a_1X_0 + \cdots + a_nX_n,$$

wobei nicht alle Koeffizienten gleichzeitig 0 sein dürfen. Die affine Nullstellenmenge $V(F)$ im $\mathbb{A}^{n+1}_K$ ist ein n-dimensionaler affiner Raum durch den Nullpunkt, die projektive Nullstellenmenge $V_+(F)$ im $\mathbb{P}^n_K$ ist isomorph zu einem $(n-1)$-dimensionalen projektiven Raum.

Definition 3.9. Es sei K ein Körper und $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ ein Ideal. Das Ideal heißt *homogen*, wenn für jedes $H \in \mathfrak{a}$ mit der homogener Zerlegung $H = \sum_i H_i$ auch $H_i \in \mathfrak{a}$ für alle homogenen Bestandteile H_i ist.

Definition 3.10. Zu einem homogenen Ideal $\mathfrak{a} \subseteq K[X_0, \ldots, X_n]$ nennt man

$$V_+(\mathfrak{a}) = \{P = (x_0, \ldots, x_n) \in \mathbb{P}^n_K \mid F(P) = 0 \text{ für alle homogenen } F \in \mathfrak{a}\}$$

das *projektive Nullstellengebilde* oder die *projektive Varietät* zu $\mathfrak{a}$.

Definition 3.11. Der projektive Raum $\mathbb{P}^n_K$ wird mit der *Zariski-Topologie* versehen, bei der die Mengen $V_+(\mathfrak{a}) \subseteq \mathbb{P}^n_K$ zu einem homogenen Ideal $\mathfrak{a} \subseteq K[X_0, X_1, \ldots, X_n]$ als abgeschlossen erklärt werden.

Die offenen Mengen des projektiven Raumes sind demnach die Mengen der Form $D_+(\mathfrak{a}) := V_+(\mathfrak{a})$ zu einem homogenen Ideal $\mathfrak{a} \subseteq K[X_0, X_1, \ldots, X_n]$. Dabei sind die offenen Mengen $D_+(X_i)$ isomorph zu einem affinen Raum der Dimension n.

BEMERKUNG 3.12. Ein Punkt $P = (a_0, \ldots, a_n) \in \mathbb{P}^n_K$ ist abgeschlossen, und zwar ist $P = V_+(\mathfrak{a})$ mit

$$\mathfrak{a} = (a_i X_j - a_j X_i : 0 \leq i, j \leq n).$$

Wenn $a_0 \neq 0$ ist, so kann man dies auch als $\left(X_j - \frac{a_j}{a_0} X_0 : j \neq 0\right)$ schreiben. Die Erzeuger $a_i X_j - a_j X_i$, $i \neq 0$, sind dann überflüssig. Dieses Ideal ist offenbar homogenen, und P liegt in $V_+(\mathfrak{a})$. Sei $a_0 \neq 0$ angenommen. Für einen weiteren Punkt $Q = (b_0, \ldots, b_n) \in V_+(\mathfrak{a})$ folgt sofort $b_j - \frac{a_j}{a_0} b_0 = 0$ für alle j bzw.

$$(b_0, \ldots, b_n) = \frac{b_0}{a_0}(a_0, \ldots, a_n),$$

so dass es sich projektiv um den gleichen Punkt handelt.

Das Ideal $\mathfrak{a}$ ist kein maximales Ideal im Polynomring, es ist aber maximal unter allen homogenen Idealen, die von $(X_0, \ldots, X_n)$ verschieden sind. In $\mathbb{A}^{n+1}_K$ definiert es eine Gerade durch den Nullpunkt, und zwar die Gerade, die dem projektiven Punkt P entspricht.

Der projektive Raum über $\mathbb{R}$ und über $\mathbb{C}$

Wir wollen uns ein Bild über die projektiven Räume für $\mathbb{K} = \mathbb{R}$ und $\mathbb{K} = \mathbb{C}$ machen. Die (reell) n-dimensionale Sphäre ist $S^n = \{x \in \mathbb{R}^{n+1} \mid \|x\| = 1\}$. Dabei ist $\|x\| = \sqrt{x_0^2 + \cdots + x_n^2}$ die *euklidische Norm.*

SATZ 3.13. *Man kann den reell-projektiven Raum $\mathbb{P}^n_{\mathbb{R}}$ durch die n-dimensionale Sphäre $S^n \subset \mathbb{R}^{n+1}$ modulo der Äquivalenzrelation repräsentieren, die antipodale Punkte miteinander identifiziert.*

Den komplex-projektiven Raum $\mathbb{P}^n_{\mathbb{C}}$ kann man durch die $(2n+1)$-dimensionale Sphäre $S^{2n+1} \subset \mathbb{R}^{2n+2} \cong \mathbb{C}^{n+1}$ modulo der Äquivalenzrelation repräsentieren, die zwei Punkte $z, w \in S^{2n+1}$ miteinander identifiziert, wenn man $z = \lambda w$ mit einem $\lambda \in S^1 \subseteq \mathbb{C}$ schreiben kann.

Beweis. Wir behandeln die beiden Fälle parallel. Jeder Punkt der Sphäre S definiert eine (reelle oder komplexe) Gerade durch den Nullpunkt im umliegenden Raum $\mathbb{R}^{n+1}$ oder $\mathbb{C}^{n+1}$ und damit einen Punkt im projektiven Raum. Zwei Punkte $z, w \in S$ definieren genau dann die gleiche Gerade, wenn es einen Skalar $\lambda \in \mathbb{K}$ mit $z = \lambda w$ gibt. Wegen der Multiplikativität der Norm ist dann auch $\|z\| = |\lambda| \cdot \|w\|$, woraus sich wegen $z, w \in S$ sofort $|\lambda| = 1$ ergibt. Dies bedeutet im reellen Fall $\lambda = \pm 1$ und im komplexen Fall, dass $\lambda \in S^1 \subset \mathbb{C}$ ist, also zum Einheitskreis gehört. □

Wir haben insgesamt Abbildungen

$$S^n \subset \mathbb{R}^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}^n_{\mathbb{R}}$$

(im reellen Fall) bzw.

$$S^{2n+1} \subset \mathbb{R}^{2n+2} \setminus \{0\} \cong \mathbb{C}^{n+1} \setminus \{0\} \longrightarrow \mathbb{P}^n_{\mathbb{C}}$$

(im komplexen Fall). Nach dem vorstehenden Satz sind die Gesamtabbildungen jeweils surjektiv. Man versieht die reell und die komplex-projektiven Räume mit der Quotiententopologie zur metrischen Topologie des reellen Vektorraumes unter dieser Abbildung, d.h. man erklärt eine Teilmenge $U \subseteq \mathbb{P}^n_{\mathbb{K}}$ für offen, wenn das Urbild in $\mathbb{K}^{n+1} \setminus \{0\}$ offen ist. (dies ist äquivalent dazu, dass das Urbild auf der jeweiligen Sphäre offen ist). Mit dieser (*metrischen* oder *natürlichen*) Topologie auf dem projektiven Raum sind diese Abbildungen stetig. Dies hat folgende Konsequenz.

Lemma 3.14. *Für den reell-projektiven und den komplex-projektiven Raum sind die Teilmengen $D_+(X_i)$ offen in der natürlichen Topologie und homöomorph zu $\mathbb{R}^n$ bzw. $\mathbb{C}^n$. Insbesondere sind die reell- und komplex-projektiven Räume topologische Mannigfaltigkeiten.*

Beweis. Das Urbild von $D_+(X_i)$ unter der kanonischen Abbildung $\mathbb{A}^{n+1}_{\mathbb{K}} \setminus \{0\} \to \mathbb{P}^n_{\mathbb{K}}$ ist $D(X_i)$, also das Komplement eines n-dimensionalen Untervektorraumes und damit offen in der natürlichen Topologie. Wir betrachten die stetigen Abbildungen

$$\mathbb{K}^n \cong V(X_i - 1) \subset D(X_i) \longrightarrow D_+(X_i)\,.$$

Die Gesamtabbildung ist eine Bijektion und $D_+(X_i)$ trägt die Quotiententopologie unter der zweiten Abbildung. Wir müssen zeigen, dass die Bijektion eine Homöomorphie ist. Dazu genügt es, die Offenheit der Abbildung zu zeigen. Sei also $U \subseteq V(X_i - 1) \cong \mathbb{K}^n$ offen und U' das zugehörige Bild in $D_+(X_i)$. Die Offenheit von U' ist nach Definition der Quotiententopologie äquivalent dazu, dass das Urbild $U'' \subseteq D(X_i)$ von U' offen ist. Diese Menge U'' besteht aus allen Punkten in $D(X_i)$, die auf einer Geraden durch den Nullpunkt und durch einen Punkt aus U liegen. Sei Q ein solcher Punkt, und $Q = \lambda P$ mit $P \in U$ und $\lambda \in \mathbb{K}^\times$. Sei B eine offene Ballumgebung um P in $V(X_i - 1)$. Dann ist auch der dadurch definierte Kegel in $D(X_i)$ offen und liegt ganz in U''. □

Korollar 3.15. *Die reell-projektiven und die komplex-projektiven Räume sind kompakt und hausdorffsch in der natürlichen Topologie.*

Die projektive Gerade über $\mathbb{C}$ ist eine Sphäre.

Beweis. Es gibt eine surjektive stetige Abbildung von einer Sphäre auf einen jeden projektiven Raum. Die Sphäre ist eine abgeschlossene und beschränkte Teilmenge eines reellen endlichdimensionalen Vektorraumes und daher nach dem Satz von Heine-Borel kompakt. Da das Bild einer kompakten Menge unter einer stetigen Abbildung nach Satz Anhang B.12 (Lineare Algebra (Osnabrück 2017-2018)) wieder kompakt ist, folgt, dass die projektiven Räume kompakt sind.

Für die Hausdorff-Eigenschaft seien $P, Q \in \mathbb{P}^n_{\mathbb{K}}$ zwei verschiedene Punkte. Man kann annehmen, dass sie beide auf einem der affinen überdeckenden Räume $D_+(X_i)$ liegen. Damit gibt es nach Lemma 3.14 trennende Umgebungen. □

Abbildungsverzeichnis

Quelle = Loewenzahn 20.jpg , Autor = Waugsberg, Lizenz = CC-BY-SA-2.5 1

Quelle = Projektiveline1bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0 2

Quelle = Projektiveline2bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0 2

Quelle = Projektiveline3bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0 2

Quelle = Projektiveplane1bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0 3

Quelle = Projektiveplane2bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0 3

Quelle = Projektiveplane3bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0 3

Quelle = Projektiveplane4bb.jpg , Autor = Darapti, Lizenz = CC-BY-SA-3.0 3

Quelle = Perspective Projection Principle.jpg , Autor = Benutzer Fantagu auf Commons, Lizenz = CC-BY-SA-3.0 4

Quelle = Blue-sphere.png , Autor = Benutzer Kieff auf Commons, Lizenz = PD 8

Erläuterung: Die in diesem Text verwendeten Bilder stammen aus Commons (also von http://commons.wikimedia.org) und haben eine Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren Dateinamen auf Commons angeführt zusammen mit ihrem Autor bzw. Hochlader und der Lizenz. 9

Lizenzerklärung: Diese Seite wurde von Holger Brenner alias Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und unter die Lizenz CC-by-sa 3.0 gestellt. 9