Stichworte:

- Der affine und projektive Raum über einem Körper k
- verschiedene parallele Geraden schneiden sich nicht im Affinen
- im Projektiven schneiden sich zwei verschiedene projektive Geraden stets in genau einem Punkt
- projektive Geraden entstehen aus affinen Geraden durch Homogenisierung
- $\mathbb{P}^2(k)$ und geometrische Interpretationen
- $f \in k[x,y] \rightsquigarrow$ affine Kurve
- Tangente einer affinen Kurve
- singulärer Punkt, Beispiele

---

§2.2 Der affine Raum, affine Kurven und der zweidimensionale projektive Raum

Wir stellen den zweidimensionalen affinen und projektiven Raum vor, d.h. die wohlbekannte affine Ebene $k^2 = k \times k$ und ihre Ergänzung zur projektiven Ebene $\mathbb{P}^2(k)$ durch "unendlich ferne Punkte". Kurven im Affinen wie z.B. elliptische Kurven werden dann in der projektiven Ebene interpretiert, weil es rechentechnisch einfacher und mathematisch natürlicher ist.

2.2.1 Die affine und projektive Ebene

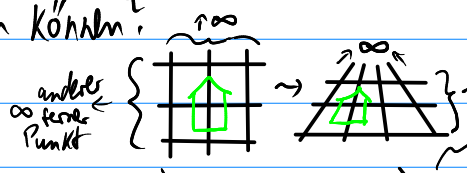
Sei k ein beliebiger Körper. Wir stellen uns meistens $\mathbb{R}$ vor, weil wir über geometrische Objekte nachdenken möchten; k ist in den Anwendungen aber meist ein endlicher Körper.

1) **Def.:** Den zweidimensionalen k-VR $k^2 = k \times k$ schreiben wir auch als $\mathbb{A}^2(k) := \{(x_1, x_2);\ x_1, x_2 \in k\}$ und nennen ihn den zweidimensionalen affinen Raum über k bzw. affine Ebene über k.

2) **Def.:** Eine Gerade in $\mathbb{A}^2(k)$ ist eine Teilmenge des $\mathbb{A}^2(k)$ der Form $g(a,b,c) := \{(x,y) \in \mathbb{A}^2(k);\ ax + by + c = 0\}$ für ein Tripel $(a,b,c) \in k^3 \setminus \{(0,0,c);\ c \in k\}$.

3) **Bem.:** Zwei verschiedene Geraden in $\mathbb{A}^2(k)$ schneiden sich in genau einem Punkt, es sei denn, sie sind parallel, d.h. dann haben sie keinen gemeinsamen Punkt in $\mathbb{A}^2(k)$. Soweit nichts Neues.

4) Bem.: Die Ausnahme, dass in der "Ebene" $k \times k$ Geraden parallel sein können, möchten wir uns beim Rechnen gerne ersparen. Wir ergänzen die Ebene um "unendlich ferne Punkte" und erklären, dass sich zwei parallele Geraden in genau! so einem Punkt schneiden. Durch diese Ergänzung wird die affine Ebene zur projektiven Ebene.
Wie kann das sinnvoll so umgesetzt werden, dass alle Punkte Koordinaten bekommen, mit denen man wie üblich rechnen kann, so dass bei der Schnittpunktberechnung auch die unendl. fernen Punkte erhalten werden können?



$\rightsquigarrow$ ($ax+by+c \cdot z \overset{!}{=} ax+by+d \cdot z$ lösbar $\rightarrow z=0$)

$\rightarrow$ Parallelen $g(a,1,c)$, $g(a,1,d)$ sollen sich dann schneiden, auch rechnerisch. Wir lösen das so, dass in unserer neuen "Ebene" eine dritte "Koordinate" z hinzukommt, welche bei diesen Parallelen im Schnittpunkt also $=0$ sein müsste, wie folgt:

5) Def.: Die projektive Ebene über k ist die Menge

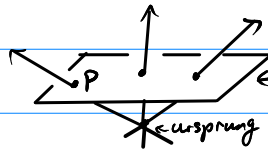
$$\mathbb{P}^2(k) = \{ [y_1 : y_2 : y_3];\ y_1, y_2, y_3 \in k, \text{ nicht } y_1 = y_2 = y_3 = 0 \}$$

mit der Vereinbarung, dass $[y_1 : y_2 : y_3] = [\tilde{y}_1 : \tilde{y}_2 : \tilde{y}_3]$ genau dann gilt, wenn es ein $\lambda \in k \setminus \{0\}$ gibt mit $y_1 = \lambda \tilde{y}_1$, $y_2 = \lambda \tilde{y}_2$, $y_3 = \lambda \tilde{y}_3$.

6) Formal: $\mathbb{P}^2(k)$ ist die Menge der Äquivalenzklassen in k^3 bzgl. der Äquivalenzrelation $(y_1, y_2, y_3) \sim (\tilde{y}_1, \tilde{y}_2, \tilde{y}_3) :\Leftrightarrow \exists \lambda \in k, \lambda \neq 0$: $y_i = \lambda \tilde{y}_i$, $i = 1,2,3$,
d.h. $\mathbb{P}^2(k) := (k^3 \setminus \{(0,0,0)\}) / \sim$.

Wir schreiben $[y_1 : y_2 : y_3]$ für die Äquivalenzklasse, die von (y_1, y_2, y_3) repräsentiert wird und nennen sie einen projektiven Punkt, und y_1, y_2, y_3 nennen wir projektive Koordinaten von $[y_1 : y_2 : y_3]$.

7) Ist $y_3 \neq 0$, gilt $[y_1 : y_2 : y_3] = \left[\frac{y_1}{y_3} : \frac{y_2}{y_3} : 1\right]$, d.h. die dritte (oder jede andere Koordinate $\neq 0$) kann dann auf 1 gebracht ("normiert") werden.



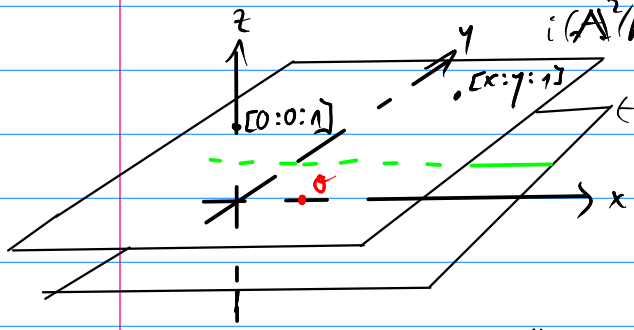
$P = [x : y : 1]$ $\quad i(\mathbb{A}^2(k)) = \{[x : y : 1];\ x, y \in k\}$

Einem projektiven Punkt $[x : y : z]$ entspricht in unserem Modell in k^3 der Ursprungsgeraden $\{(\lambda x, \lambda y, \lambda z);\ \lambda \in k\}$.

Diese Punkte sind entweder $[x:y:1]$ oder $[x:y:0]$ mit $x,y \in k$ (nicht $[0:0:0]$!)
z.B. durch die Abbildung $i: \mathbb{A}^2(k) \to \mathbb{P}^2(k)$
$(x,y) \mapsto [x:y:1]$
Kann die affine Ebene in die projektive eingebettet werden (d.h. i ist injektiv!)

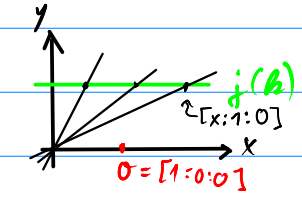
8.) Aber $\mathbb{P}^2(k)$ enthält zusätzlich noch die projektiven Punkte $[x:y:0]$, $x,y \in k$. Offenbar ist $\{[x:y:0];\ x,y \in k, \overset{\text{nicht}}{x=y=0}\}$ eine Gerade in $\mathbb{P}^2(k)$, die wir unendlich ferne Gerade g_∞ nennen möchten, denn mit
$j: k \to g_\infty,\ x \mapsto [x:1:0]$ läßt sich k darin einbetten
(d.h. j ist injektiv), wobei auffällt, daß $g_\infty \setminus \mathrm{im}(j)$ aus genau dem weiteren Punkt $O := [1:0:0]$ besteht, d.h. $g_\infty \setminus \mathrm{im}(j) = \{O\}$.

9.) Somit: $\mathbb{P}^2(k) = i(\mathbb{A}^2(k)) \dot\cup \underbrace{j(k) \dot\cup \{O\}}_{= g_\infty}$ (disjunkte Vereinigung)

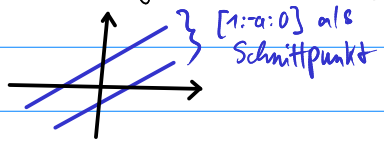


$\leftarrow$ x-y-Ebene für ∞ ferne Punkte:
$\to g_\infty = \{[x:y:0];\ x,y \in k\}$
$= j(k) \dot\cup \{O\}$
$\hat{=}$ { Ursprungsgeraden in der x-y-Ebene}

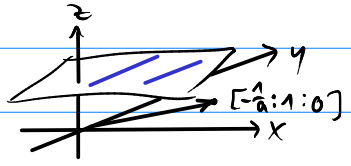
Ansicht auf die x-y-Ebene:



Die in $\mathbb{A}^2(k)$ parallelen Geraden $g(a,1,c) = \{(x,y) \in k^2;\ ax+y+c=0\}$ $\underbrace{\Leftrightarrow y = -ax-c}$
$= \{(x,-ax-c);\ x \in k\}$ und $g(a,1,d)$ müssen die projektiven Punkte
$[x:-ax-c:1]$ und $[x:-ax-d:1]$ enthalten.
Das klappt, wenn die Glg $ax+y+\{c/d\}=0$ zu $ax+y+\{c/d\}z=0$ ergänzt wird.
Sie schneiden sich dann im unendlich fernen Punkt $[1:-a:0] = [-\hat{a}:1:0]$, $a \neq 0$, welcher die gemeinsame Steigung $-a$ angibt, bzw. die gemeinsame "Richtung" $(1,-a)$:



in unserem 3-dim. "Modell":



bzw. $(-\hat{a},1)$
bzw. $(-1,a)$
bzw. $(\hat{a},-1)$

Geradengl.: $\underbrace{(a,1)\cdot(x,y)}_{\text{Skalarprodukt}} + c = 0$, der Normalenvektor ist $(a,1)$ und senkrecht zum Richtungsvektor $(1,-a)$.
Die gemeinsame Richtung $(1,-a)$ wird zum gemeinsamen Schnittpunkt $[-\hat{a}:1:0]$ erklärt.

10.) **Def.:** Eine projektive Gerade ist eine Teilmenge von $\mathbb{P}^2(k)$ der Form $G(a,b,c) = \{[x:y:z];\ ax+by+cz=0\}$ für $(a,b,c)\in k^3\setminus 0$

Man sagt, die "projektive" Gleichung $ax+by+cz=0$ ist "durch Homogenisierung" aus $ax+by+c=0$ entstanden: Durch die Ergänzung mit z haben nun alle Summanden ax, by und cz denselben Grad 1 als Polynom aus $k[x,y,z]$. Dieses Prinzip werden wir für allgemeinere Kurven für den Übergang vom Affinen ins Projektive übernehmen.

Projektive Geraden werden uns in Form von Tangenten dann wiederbegegnen.

Bsp: Die projektiven Geraden $G(a,1,c), G(a,1,d)$ schneiden sich in $[-\hat{a}:1:0]\in g_\infty$. (a≠0)

Bem.: Durch je zwei verschiedene Punkte des $\mathbb{P}^2(k)$ führt genau eine projektive Gerade.

2.2.2. Affine Kurven

Doch zunächst möchten wir im affinen Raum allgemeinere Kurven untersuchen. Dazu benutzen wir Polynome zu ihrer Beschreibung.

11.) **Def.:** Sei $f\in k[x,y]$ ein Polynom über k in zwei Variablen x und y. Wir bezeichnen die Menge der Nullstellen von f in $k\times k = \mathbb{A}^2(k)$ als

$$C_f(k) := \{(u,v)\in\mathbb{A}^2(k);\ f(u,v)=0\}.$$

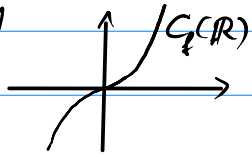
Jede solche Nullstellenmenge $C_f(k)$ nennen wir eine affine Kurve.

Ist klar, welches Polynom f vorliegt, schreiben wir auch kurz $C(k)$ für $C_f(k)$.

Geraden sind spezielle affine Kurven (zu linearen Polynomen $f(x,y,z)=ax+by+c$).

12.) **Bem.:** Für uns ist interessant, Kurven über verschiedenen Körpern k zu studieren. Der Fall eines endlichen Körpers ist für Anwendungen interessant, weil dann alle Kurven aus nur endlich vielen Punkten bestehen können.

13.) **Bsp:** Sei $k=\mathbb{R}$ und $f(x,y)=y-x^3-x$. Die Nullstellenmenge $C_f(k)$ besteht dann aus allen Punkten $(x,y)\in k^2$, welche die Gleichung $y=x^3+x$ erfüllen. Das reelle Schaubild sieht so aus:



Für $k=\mathbb{F}_5$ können nur wenige Punkte auf der "Kurve" liegen:

Die Tabelle

a	0	1	2	3	4
a^3	0	1	3	3	-1
a^3+a	0	2	0	0	3

zeigt, dass $C_f(\mathbb{F}_5)=\{(0,0),(1,2),(2,0),(3,0),(4,3)\}$ ist, und

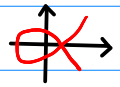
mit $f_0(x,y)=y^2-x^3-x$ haben wir $C_{f_0}(\mathbb{F}_5)=\{(0,0),(2,0),(3,0)\}$.

Ist $\tilde{k} \subseteq k$ ein Teilkörper von k (wie z.B. $\mathbb{Q} \subseteq \mathbb{R}$), so folgt auch stets $C_f(\tilde{k}) \subseteq C_f(k)$. Unsere Kurvenpunkte in $A(\mathbb{F}_5)$ finden wir deswegen z.B. in $A(\mathbb{F}_{25})$ wieder.

14.) Def.: Eine (affine) Tangente an eine affine Kurve $C_f(k)$ im Punkte $(a,b) \in C_f(k)$ ist die Gerade

$$t_{(a,b)}(C_f) = \{(x,y): \frac{\partial f}{\partial x}(a,b)x + \frac{\partial f}{\partial y}(a,b)y + d = 0\},$$

falls diese existiert (wir brauchen, dass $\frac{\partial f}{\partial x}(a,b), \frac{\partial f}{\partial y}(a,b)$ nicht beide $=0$), Dabei ist $d \in k$ so gewählt, dass $(a,b) \in t_{(a,b)}(C_f)$ gilt.

15.) Es ist nicht klar, ob Tangenten stets eindeutig existieren, denn:
Affine Kurven können sich selbst schneiden oder scharfe "Spitzen" haben:
Bsp.: $f(x,y) = y^2 - x^3$: 
$f(x,y) = y^2 - x^3 + 3x^2 - 4$: 

16.) Def.: Die affine Kurve $C_f(k)$ heißt singulär im Punkt $(a,b) \in C_f(k)$, falls $\frac{\partial f}{\partial x}(a,b) = \frac{\partial f}{\partial y}(a,b) = 0$ gilt.

17.) Bem.: Affine Kurven, die in keinem Punkt singulär sind, haben überall eine wohldefinierte Tangente.

18.) Bem.: Es kann vorkommen, dass $C_f(k)$ gar keine singulären Punkte enthält, wohl aber über einem Erweiterungskörper von k, wie etwa $\bar{k}$, dem algebraischen Abschluss von k.

19.) Bsp.: $f(x,y) = y^2 - x^4 - 2x^2 - 1 \rightsquigarrow C_f(\mathbb{R})$ hat keine singulären Punkte:
Es ist $\frac{\partial f}{\partial x}(a,b) = -4a^3 - 4a = -4a(a^2+1)$, $\frac{\partial f}{\partial y}(a,b) = 2b$.
Allerdings sind $(i,0), (-i,0) \in \mathbb{C}$ singuläre Punkte in $C_f(\mathbb{C})$, wo $\mathbb{C} = \bar{\mathbb{R}}$.

20.) Bsp: $f(x,y) = y^2 - x^3 - x$, $k = \mathbb{F}_p \rightsquigarrow$ Ableitungen: $\frac{\partial f}{\partial x}(x,y) = -3x^2 - 1$, $\frac{\partial f}{\partial y}(x,y) = 2y$, d.h. die singulären Punkte (a,b) sind die mit $b^2 = a^3 + a$, $-3a^2 = 1$, $2b = 0$.

- Für $p \neq 2$ ist $2b = 0$ nur für $b = 0$ richtig, dann ist $0 = a(a^2+1)$ und $3a^2 = -1$
  $\rightsquigarrow 0 = a(\underbrace{3a^2}_{=-1} + 3) \rightsquigarrow 2a = 0 \overset{p \neq 2}{\rightsquigarrow} a = 0$ im $\not\downarrow$ zu $3a^2 = -1$. Also ex. keine sing. Punkte für $p \neq 2$.
- Für $p = 2$ ist $C_f(\mathbb{F}_2) = \{(0,0),(1,0)\} \rightsquigarrow \frac{\partial f}{\partial x}(1,0) = 0 = \frac{\partial f}{\partial y}(1,0)$, d.h. $(1,0)$ ist sing. Punkt.