<u>Beweis</u>: Betrachte $E = \overline{P_1P_2} \cup \overline{P_3P_4} \cup \overline{P_5P_6}$, $E \cap F = \{P_1, \dots, P_6, q_1, \dots\}$

$F = \overline{P_2P_3} \cup \overline{P_4P_5} \cup \overline{P_6P_1}$

Angenommen q_1, q_2, q_3 liegen auf einer Geraden L, Betrachte $q_4 \in L$ und $G_{\lambda,\mu} = \lambda E + \mu F$ mit $q_4 \in G_{\lambda,\mu}$.

$G_{\lambda,\mu} = \ell \cdot q$ mit $P_1, \dots, P_6 \in V(q)$. Umgekehrt ist $p_1, \dots, p_6$ in $V(q)$, so ex ℓ mit $G_{\lambda,\mu} = q\ell$

10.07.18 Anwendung von Bézout: <u>Gruppengesetz</u> auf einer Kubik

Sei $f \in K[x_0, x_1, x_2]$ eine irreduzible Kubik, die eine glatte Kurve E definiert

Sei $p_0 \in E$ ein fester Punkt. Wir definieren eine Addition auf E

$$E \times E \to E, \quad (p,q) \mapsto p+q$$

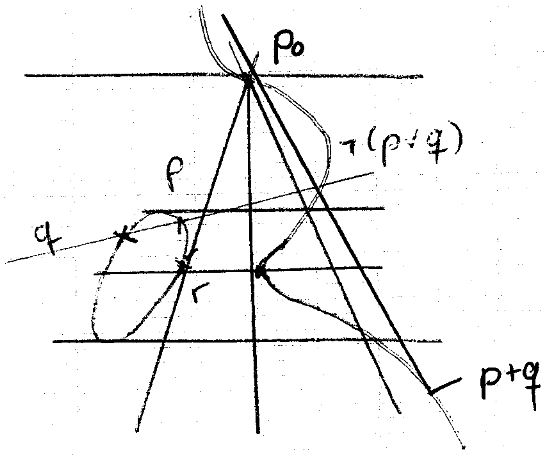
wie folgt. $(p,q) \mapsto$ dritter Schnittpunkt von $\overline{pq} \cap E$ $=: \neg(p \vee q)$

$p+q :=$ dritte Schnittpunkt von der Geraden $\overline{\neg(p\vee q), p_0}$ mit E

Im Beispiel ist $f = x_2^2 x_0 - (x_1^3 + a x_1 x_0^2 + b x_0^3)$ die Homogenisierung von einer kubischen Gleichung

$$Y^2 = X^3 + aX + b, \quad a, b \in K$$

in Weierstraßscher Normalform und $p_0 = (0:0:1)$



Im Fall $p = q$ ersetze $\overline{pq}$ durch T_pE

Das Gruppengesetz ist klarer Weise kommutativ, neutrales Element ist p_0, das Inverse zu p ist

$-p = \overline{pp_0} \cap E$.

Nicht so klar ist das Assoziativgesetz

$(p+q)+r = p+(q+r)$

Für den Beweis betrachten wir die Linearschar

$$L = L(3;\ p, q, r,\ \neg(p \vee q),\ \neg(q \vee r),\ p+q,\ q+r, p_0)$$

Es gilt $\dim L \geq \binom{3+2}{2} - 8 = 2$

Wir zeigen $\dim L = 2$ mit Bézout. Angenommen $\dim L \geq 3$

Wähle zwei Punkte $s_1 \in \overline{p_0, (p+q)} - \{p_0, p+q, \neg(p \vee q)\}$

$s_2 \in \overline{p_0, (q+r)} - \{p_0, q+r, \neg(q \vee r)\}$

und ein $g \in L(3, \ldots, s_1, s_2) \neq 0$

Dann gilt $V(g) \cap \overline{p_0, (q+r)}$ enthält 4 Punkte. Nach Bézout enthält $V(g)$ die Gerade $\overline{p_0, (q+r)}$, Analog $V(g) \supset \overline{p_0, (p+q)}$

Aus $g = \underset{\overline{p_0,(q+r)}}{\underset{\shortparallel}{l_1}}\ \underset{\overline{p_0,(p+q)}}{\underset{\shortparallel}{l_2}}\ l_3$ folgt, dass l_3 muss $\{p, q, r\}$ enthalten. Aber diese liegen nicht auf einer Geraden $\lightning$

Also $\dim L = 2$

$L \ni f_1, f_2$ verschieden bilden Basis, also $f = \lambda_1 f_1 + \lambda_2 f_2$

Also $V(f) = E$ enthält den Schnittpunkt

$$\overline{p+q, r} \cap \overline{p, q+r}$$

Also alle drei Kurven f, f_1, f_2 enthalten diesen Punkt, was zu zeigen war.

$$\neg(p+q) \vee r = \neg p \vee (q+r)$$

und $(p+q)+r = p+(q+r)$

<u>Bem</u>: Ist f definiert über K und $p_0 \in E(K)$. Dann ist $E(K) \subset E(\overline{K})$ eine Untergruppe

Satz Mordell (1924): E definiert über $\mathbb{Q}$.
Dann ist $E(\mathbb{Q}) \subset E(\mathbb{C})$ eine <u>endlich</u> <u>erzeugte</u> abelsche Gruppe

$$E(\mathbb{Q}) = \mathbb{Z}^r + T, \quad T \text{ Torsionsgruppe}$$

§6 Projektive Varietäten

Def. Eine projektive algebraische Menge $X \subset \mathbb{P}^n$ ist eine Menge der Gestalt
$$X = V(I) = \{ p \in \mathbb{P}^n \mid f(p) = 0 \text{ für alle } f \in I \text{ homogen} \}$$

I homogenes Ideal.
Umgekehrt $X \subset \mathbb{P}^n$.
$$I(X) = \{ f \in \bar{K}[x_0, \dots, x_n] \text{ homogen mit } f(p) = 0 \text{ für alle } p \in X \}$$

Bsp. $A \subset \mathbb{A}^n \cong U_0 \subset \mathbb{P}^n$.
$I_{\mathbb{A}^n}(A) \subset K[x_1, \dots, x_n]$, $I_{\mathbb{P}^n}(A) = \{ f^h \mid f \in I(A) \}$
$I_{\mathbb{P}^n}(A)$ kann aus $I_{\mathbb{A}^n}(A)$ durch eine GB bestimmt werden mit Monomordnung, die Grad verfeinert

Thm (Proj. Nullstellensatz)
Sei $I \subset K[x_0, \dots, x_n]$ ein homogenes Ideal, d.h. von homogenen Elementen erzeugt.
Dann gilt
(1) $\mathbb{P}^n(\bar{K}) \supset V(I) = \emptyset$ gdw ein N ex mit $I \supset (x_0, \dots, x_n)^N$
(2) Falls $V(I) \neq \emptyset$, dann gilt
$$I(V(I)) = \mathrm{rad}(I \cdot \bar{K}[x_0, \dots, x_n]).$$

Bew. $I \subsetneq K[x_0, \dots, x_n]$ definiert auch eine algebraische Menge
$$C(I) \subset \mathbb{A}^{n+1}$$
$C(I)$ ist ein Kegel und enthält 0.
Es gilt: $V(I) \neq \emptyset$ gdw $C(I) \supsetneq \{0\}$.
(1) und (2) folgen.

Korollar: Es ex Bijektionen
$$\left\{ \begin{matrix} \text{alg Teilmengen} \\ \text{von } \mathbb{P}^n \end{matrix} \right\} \underset{V}{\overset{I}{\rightleftarrows}} \left\{ \begin{matrix} \text{homogene Radikalideale} \\ \subset \bar{K}[x_0, \dots, x_n] \text{ ungleich} \\ (x_0, \dots, x_n) \end{matrix} \right\}$$

Bem: Man nennt $(x_0, \dots, x_n)$ manchmal das irrelevante maximale Ideal.

Def. $X \subset \mathbb{P}^n$ eine alg. Menge

$$I = I(X) \subset \bar{K}[x_0, \dots, x_n] =: S,$$

dann heißt $S_X := S/I$ der homogene Koordinatenring von X.

X nennt man proj. Varietät, wenn $I(X)$ ein Primideal ist.

S und S_X sind graduierte Ringe

$$S = \bigoplus_{d \geq 0} S_d \qquad , \quad S_d = K[x_0, \dots, x_n]_d$$

$$S_X = \bigoplus_{d \geq 0} (S_X)_d = \bigoplus_{d \geq 0} \left(S_d / I(X)_d \right)$$

Die Multiplikation respektiert die Graduierung

$$S_d \times S_e \xrightarrow{\mu} S_{d+e} \quad , (f, g) \mapsto f \cdot g$$

Analog für S_X.

Def.

Ein graduierter Modul Modul M über einem graduierten Ring $R = \bigoplus_{d \geq 0} R_d$ ist ein Modul zusammen mit einer Zerlegung

$$M = \bigoplus_{d \in \mathbb{Z}} M_d,$$

sodass $R_e \cdot M_d \subset M_{d+e}$.

Also S_X ist ein graduierter S-Modul.

Ein Morphismus $\varphi: M \to N$ zwischen R-Moduln ist ein R-Modul Homomorphismus, der $\varphi(M_d) \subset N_d$ erfüllt.

Mit dieser Notation und $f \in R_\ell$, $\ell \neq 0$ ist die Multiplikation mit f.

$$M \to M, \quad m \mapsto m \cdot f$$

kein Morphismus. Um dies auszuräumen definiert man den um ℓ getwisteten Modul

$$M(\ell) = \bigoplus_{d \in \mathbb{Z}} M(\ell)_d = \bigoplus_{d \in \mathbb{Z}} M_{\ell+d}$$

Dann gibt Multiplikation mit $f \in R_e$ ein graduierter R-Modul-Homomorphismus

Beispiel: $S(-j)$ ist der freie S-Modul mit Erzeuger vom Grad j

$$S(-j)_j = S_{-j+j} = S_0 \ni 1$$

Def. Sei M ein endlich erzeugter graduierter $S = K[x_0, \ldots, x_n]$-Modul. Die Hilbertfunktion $h_M : \mathbb{Z} \to \mathbb{Z}$ ist durch

$$h_M(d) = \dim_K M_d$$

definiert

Thm (Hilbert) Sei M ein endlich erzeugter graduierter S-Modul ($S = K[x_0, \ldots, x_n]$). Dann ex ein Polynom $p_M(t) \in \mathbb{Q}[t]$ sodass

$$h_M(d) = p_M(d) \quad ; \; d \gg 0$$

p_M heißt Hilbertpolynom.

Beweis: Der Syzygien-Algorithmus funktioniert auch im graduierten Fall!

Er produziert eine endliche freie Auflösung der Länge $c \leq n+1$.

$$0 \leftarrow M \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_c \leftarrow 0.$$

Dabei $F_i = \bigoplus S(-j)^{\beta_{ij}}$ und β_{ij} ist die Anzahl der freien Erzeuger von F_i mit Grad j.

Für jedes $d \in \mathbb{Z}$:

$$0 \leftarrow M_d \leftarrow (F_0)_d \leftarrow \cdots \leftarrow (F_c)_d \leftarrow 0$$

eine exakte Sequenz von endl. dimensionalen K-VR.

Also

$$\dim M_d = \sum_{i=0}^{c} (-1)^i \dim (F_i)_d$$

$$= \sum_{i=0}^{c} (-1)^i \sum_j \beta_{ij} \dim S(-j)_d.$$

Nun gilt $\dim S(-j)_d = \dim S_{d-j} = \binom{d-j+n}{n}$

Interpretieren wir

$$\binom{t-j+n}{n} = \frac{(t-j+n)(t-j+n-1)\cdots(t-j+1)}{n(n-1)\cdots 1} \in \mathbb{Q}[t]$$

So definiert die Rechte Seite $p_M(t) \in \mathbb{Q}[t]$ und Gleichheit, falls d so groß ist, dass alle auftretenden $d-j+n \geq n$ □

Prop: M endl. erzeugter graduierter S-Modul.
$I = \mathrm{Ann}(M)$, $d = \dim V(I) \subset P^n$
Dann gilt
$$P_M(t) = c_M \, t^d/d! + O(t^{d-1}) \in \mathbb{Q}[t] \quad , c_M > 0, c_M \in \mathbb{Z}$$

Beweis: $X = V(I)$ und $K[Y_0, .., Y_d] \hookrightarrow K[X_0, .., X_n]/I$ eine Noether normalisierung.
Beachte Krulldimension:
$$\dim S/I = \dim C(I) = \dim V(I) + 1$$
Dann ist M ein endlich erzeugter S/I Modul und S/I ein endlich erzeugter $K[Y_0, .., Y_d]$-Modul.
Also M ist ein endlich erzeugter $K[Y_0, .., Y_d]$-Modul.
$R = K[Y_0, .., Y_d]$
Also hat M eine endliche freie Auflösung über $R = K[Y_0, .., Y_d]$
Somit $d!\, P_M(t) \in \mathbb{Z}[t]$ hat Grad $\leq d$.
Um die Aussage über c_M einzusehen betrachte ein assoziiertes Primideal $\mathfrak{P}$ von M der $\operatorname{codim} \mathfrak{P} = \operatorname{codim} I$
Also auch ein minimales Primideal von I
Dann ist auch $K[Y_0, .., Y_d] \hookrightarrow S/\mathfrak{P}$
ganze Ringerweiterung.
Es sei $\mathfrak{P} = \mathrm{Ann}(m)$ mit $m \in M_e$. $S/\mathfrak{P}(-e) \hookrightarrow M$
Es folgt $P_M(t) \geq \binom{t-e+d}{d}$

Also $\deg P_M(t) \leq d$ und $P_M(t)$ wächst wie ein Polynom von Grad d und somit
$$\deg P_M = d \text{ und } c_M \in \mathbb{Z}_{>0}$$

Def.: $X \subset \mathbb{P}^n$ proj alg. Menge
$$\deg X = c_{S/I(X)}$$

Beispiel: $f \in \overline{K}[X_0, .., X_n]$ homogen v. Grad d quadratfrei $X = V(f)$. $S_X = S/f$
$$0 \leftarrow S/f \leftarrow S \xleftarrow{f} S(-d) \leftarrow 0$$

$$P_X(t) = \binom{t+n}{n} - \binom{t-d+n}{n}$$

$$= t^n/_{n!} + \frac{(t-d)^n}{n!} + \frac{\sum_{i=0}^{n} i t^{n-1}}{n!} - \text{''} + O(t^{n-2})$$

$$= \frac{n\ d\ t^{n-1}}{n!} + O(t^{n-2}) = d \cdot t^{n-1}/_{n!} + O(t^{n-2})$$

und $\deg X = \deg S$ $\square$