K15
-1-

Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

K15: Projektive Kurven

Stichworte: Homogene Polynome definieren projektive Kurven,
Homogenisierung: affine Kurve $\rightsquigarrow$ projektive Kurve,
singuläre Punkte im Projektiven, projektive Tangenten,
nicht singuläre projektive Kurven haben "ihre Tangenten schön",
Schnittmultiplizität im Schnittpunkt einer Gerade mit einer Kurve C_F,
deren Summe ist $\leq \deg F$, $m(P;T,C_F) \geq 2$ bei Tangente T an Kurve C_F mit $\deg F \geq 2$

15.1. Einleitung:
Durch Homogenisierung können wir affine Kurven zu projektiven Kurven machen. Dabei hilft das Konzept homogener Polynome. Wir untersuchen projektive Tangenten und die Schnittmultiplizität im Schnittpunkt einer Geraden mit einer Kurve.

15.2. Def.: Sei $F \in k[X,Y,Z]$ ein Polynom über k in drei Variablen, und $F \neq 0$. Dann heißt F homogen vom Grad d, falls gilt

$$F(X,Y,Z) = \sum_{\nu_1,\nu_2,\nu_3 \geq 0} \alpha_{\nu_1,\nu_2,\nu_3} \, X^{\nu_1} Y^{\nu_2} Z^{\nu_3}$$

und $\alpha_{\nu_1,\nu_2,\nu_3} \neq 0 \Rightarrow \nu_1 + \nu_2 + \nu_3 = d$,
d.h. wenn alle Monome in F den Grad d haben.

15.3. Bsp.: $F(X,Y,Z) = aX + bY + cZ$ $(d=1)$ oder $F(X,Y,Z) = Y^2 Z - X^3 - XZ^2$ $(d=3)$.

15.4. Bem.: Klar ist, dass ein $f \in k[X,Y]$ durch Ergänzung von Z-Potenzen zu einem homogenen Polynom $F_f \in k[X,Y,Z]$ gemacht werden kann: Ist $f(X,Y) = \sum_{\nu_1,\nu_2 \geq 0} \alpha_{\nu_1,\nu_2} X^{\nu_1} Y^{\nu_2}$ vom Grad d, so setze $F_f(X,Y,Z) := \sum_{\nu_1,\nu_2 \geq 0} \alpha_{\nu_1,\nu_2} X^{\nu_1} Y^{\nu_2} Z^{d-\nu_1-\nu_2}$.
Man nennt F_f dann die Homogenisierung von f. Für diese gilt $F_f(X,Y,1) = f(X,Y)$.

K15

-2-

15.5. **Lemma:** Ist $F \in k[X,Y,Z]$ homogen vom Grad d, so gilt für alle $\alpha, \beta, \gamma \in k$ und $\lambda \in k \setminus \{0\}$: $F(\alpha,\beta,\gamma)=0 \Leftrightarrow F(\lambda\alpha, \lambda\beta, \lambda\gamma)=0$

Bew.: Nachrechnen zeigt $F(\lambda\alpha, \lambda\beta, \lambda\gamma) = \lambda^d F(\alpha,\beta,\gamma)$, woraus die Beh. folgt. $\square$

Somit können wir projektive Kurven definieren:

15.6. **Def.:** Sei $F \in k[X,Y,Z]$ homogen. Dann bezeichnen wir die Nullstellenmenge mit $C_F(k) := \{[u:v:w] \in \mathbb{P}^2(k);\ F(u,v,w)=0\}$.
Ist F klar, wird auch einfach $C(k)$ für $C_F(k)$ geschrieben.
Jede solche Nullstellenmenge heißt eine projektive ebene Kurve.

15.7. **Bsp.:** Die affine Kurve $C_f(x,y)$ zu $f(x,y) = y^2 - x^3 - x$ kann durch Homogenisieren zu $C_{F_f}(x,y,z)$ mit $F_f(x,y,z) = y^2z - x^3 - xz^2$ gemacht werden. Die injektive Abb. $i: \mathbb{A}^2(k) \to \mathbb{P}^2(k)$, $(x,y) \mapsto [x:y:1]$ bildet $C_f(k)$ nach $C_{F_f}(k)$ ab.
Die projektive Kurve $C_{F_f}(k)$ hat aber noch genau einen weiteren Punkt (auf g_∞), nämlich $[0:1:0]$, d.h. $C_{F_f}(k) = i(C_f(k)) \cup \{[0:1:0]\}$.

15.8. **Lemma:** $C_{F_f}(k) \cap i(\mathbb{A}^2(k)) = i(C_f(k))$ für jede affine Kurve C_f und ihre projektive Kurve C_{F_f}.

Bew.: $[x:y:1] \in C_{F_f}(k) \cap i(\mathbb{A}^2(k)) \Leftrightarrow 0 = F_f(x,y,1) = f(x,y) \Leftrightarrow [x:y:1] \in i(C_f(k))$. $\square$

15.9. **Bem.:**
- Werden hier i auch weglassen, es ist klar, was gemeint ist.
- Anstelle von i können auch die Einbettungen $i_2(x,y) = [1:x:y]$, $i_3(x,y) = [x:1:y]$ betrachtet werden, das Lemma gilt dann entsprechend.
- Geht man für eine projektive Kurve $C_F(k)$ zu einer dieser Schnitte mit $\mathbb{A}^2(k)$ über, so sagt man, man "geht zu affinen Koordinaten" über.

K15

15.10. Def.: Sei $F \in k[X,Y,Z]$ homogen vom Grad d.
Die projektive ebene Kurve $C_F(k)$ heißt singulär im Punkt $P=[a:b:c] \in C_F(k)$, falls alle Ableitungen von F in P verschwinden, d.h. falls $\frac{\partial F}{\partial X}(a,b,c) = \frac{\partial F}{\partial Y}(a,b,c) = \frac{\partial F}{\partial Z}(a,b,c) = 0$. Die Kurve $C_F(k)$ heißt nicht-singulär bzw. glatt, falls $C_F(\bar{k})$ keinen singulären Punkt enthält, wobei $\bar{k}$ den algebraischen Abschluss von k bedeutet.

15.11. Diese Def. hängt nicht davon ab, welche projektiven Koordinaten a,b,c eines Punktes $P=[a:b:c]$ betrachtet werden. Sie passt auch mit der alten Def. von "singulärem Punkt" für affine Kurven zusammen, wie folgendes Lemma 15.12 zeigt; nach diesem genügt es, singuläre Punkte, die im Affinen liegen, auf Singularität im Affinen zu testen.

15.12. Lemma: Sei $F(X,Y,Z) = \sum_{\nu \geq 0} \alpha_\nu X^{\nu_1} Y^{\nu_2} Z^{\nu_3}$ homogen vom Grad d
und $f(x,y) = \sum_{\substack{\nu_1,\nu_2 \\ \nu_1+\nu_2 \leq d}} \alpha_{\nu_1,\nu_2,d-\nu_1-\nu_2} x^{\nu_1} y^{\nu_2} = F(x,y,1)$, d.h. $F = F_f$,

weiter sei $P \in C_F(k)$ mit $P = i(Q) \in i(\mathbb{A}^2(k))$.
Dann gilt: $C_F(k)$ singulär in $P \iff C_f(k)$ singulär in Q.

Bew.: Haben $Q \in C_f(k)$, etwa $Q=(a,b)$, dann ist $P = i(Q) = [a:b:1]$.
Es ist
$$\frac{\partial F}{\partial X}(X,Y,Z) = \sum_{\substack{\nu_1>0 \\ \nu_2,\nu_3\geq 0}} \alpha_\nu \nu_1 X^{\nu_1-1} Y^{\nu_2} Z^{\nu_3}, \text{ also } \frac{\partial F}{\partial X}(a,b,1) = \frac{\partial f}{\partial x}(a,b),$$
entsprechend gilt $\frac{\partial F}{\partial Y}(a,b,1) = \frac{\partial f}{\partial y}(a,b)$, sowie $\frac{\partial F}{\partial Z}(a,b,1) = \sum_{\substack{\nu_1,\nu_2,\nu_3 \geq 0 \\ \nu_1+\nu_2+\nu_3 = d}} \alpha_\nu \nu_3 a^{\nu_1} b^{\nu_2}$
$$= \sum_{\nu_1,\nu_2 \geq 0} \alpha_{\nu_1,\nu_2,d-\nu_1-\nu_2} (d-\nu_1-\nu_2) a^{\nu_1} b^{\nu_2} = d \cdot f(a,b) - a\frac{\partial f}{\partial x}(a,b) - b\frac{\partial f}{\partial y}(a,b).$$
Durch Vergleich der Ableitungen folgt die Beh. „$\Leftarrow$". $\square$

15.13. **Def.:** Sei $C_F(k)$ eine projektive ebene Kurve und $P=[a:b:c]$ ein nicht-singulärer Punkt auf $C_F(k)$. Die projektive Gerade
$$C_T(k) \text{ mit } T(X,Y,Z) := \frac{\partial F}{\partial X}(a,b,c)\,X + \frac{\partial F}{\partial Y}(a,b,c)\,Y + \frac{\partial F}{\partial Z}(a,b,c)\,Z$$
heißt Tangente in P an $C_F(k)$.

Wir schreiben $T_P(C_F) := C_T(k)$ dafür.

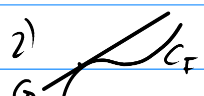
15.14. In nicht-singulären Punkten haben projektive ebene Kurven also eine "schöne" Tangente. Die Vor. "nichtsing." braucht man, damit nicht alle drei Ableitungen gleichzeitig verschwinden und so eine projektive Gerade definiert werden kann. Bei Übergang zu affinen Koordinaten erhält man wieder die üblichen (affinen) Tangenten, weil wir dann $Z=1$ setzen.

15.15. **Bsp.:** char $k \neq 2$, $f(x,y) := y^2-2x^2-2$, $F_f(x,y,z) = y^2-2x^2-2z^2$.
Dann: $(1,2) \in C_f(k)$, $\frac{\partial f}{\partial x}(1,2) = -4\cdot 1 = -4$, $\frac{\partial f}{\partial y}(1,2) = 2\cdot 2 = 4$, d.h. $(1,2)$ nicht-sing.
Die (affine) Tangente von C_f in $Q=(1,2)$ ist $t_Q(C_f) = \{(x,y)\in k^2;\ -4x+4y-4=0\}$,
die (projektive) Tangente von C_F in $P=[1:2:1]=i(Q)$ ist
$$T_P(C_F) = \{[X:Y:Z]\in \mathbb{P}^2(k);\ -4X+4Y-4Z=0\}.$$

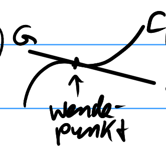
15.16. **Motivation:** Wir möchten studieren, wie sich ebene Kurven mit Geraden schneiden und die folgenden Fälle unterscheiden können:

1) 

transversaler Schnitt

2) 

einfache Tangente

3) 

← Tangente liefert hier sehr gute Approx. an Kurve

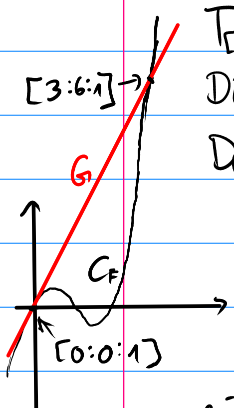
15.17 **Def.:** Schnittmultiplizität bzw. auch Vielfachheit genannt, mit der sich eine proj. Kurve mit einer Geraden schneidet:
Sei $C_F(k)$ eine projektive Kurve zum homogenen Polynom $F \in k[X,Y,Z]$, sei $G(\alpha,\beta,\gamma)$ eine projektive Gerade und $P=[a:b:c] \in G(\alpha,\beta,\gamma)$ ein Pkt. drauf.

- Ist P kein Schnittpunkt von $C_F(k)$ und G, setzen wir $m(P;G,C_F):=0$.

- Ansonsten hat das Polynom $\Psi(t):=F(a+ta',\ b+tb',\ c+tc') \in k[t]$ eine Nullstelle in $t=0$, wobei $P'=[a':b':c'] \in G$ sind.
Dann sei: $m(P;G,C_F)$ die Ordnung der Nullstelle $t=0$ von $\Psi \in k[t]$, falls $\Psi \neq 0$.
Die Zahl $m(P;G,C_F)$ heißt Schnittmultiplizität bzw. Vielfachheit, mit der sich G und C_F im Punkt P schneiden.

15.18 **Bem.:** Es ist $m(P;G,C_F)$ unabhängig von der Wahl von $P' \in G(\alpha,\beta,\gamma)$.

15.19 **Bsp.:** Sei $f(x,y)=x(x-1)(x-2)-y \in \mathbb{R}[x,y]$, d.h. $f(x,y)=x^3-3x^2+2x-y$ und $F(X,Y,Z)=F_f(X,Y,Z)=X^3-3X^2Z+2XZ^2-YZ^2$.
Da $\frac{\partial f}{\partial x}=3x^2-6x+2$, $\frac{\partial f}{\partial y}=-1$, hat C_f in $(0,0)\in C_f$ die affine Tangente
$t_{(0,0)}(C_f)=\{(x,y)\in\mathbb{R}^2;\ 2x-y=0\}$, projektiv aufgefasst lautet die Tangente
$T_{[0:0:1]}(C_F)=\{[X:Y:Z]\in\mathbb{P}^2(\mathbb{R});\ 2X-Y+0\cdot Z=0\}=G(2,-1,0)$.



Die Gerade $G(2,-1,0)$ schneidet C_F in $[3:6:1]$ und in $[0:0:1]$.
Dann haben wir $m([3:6:1];G,C_F)=1$,
weil $\Psi(t)=F(3+t\cdot 0,\ 6+t\cdot 0,\ 1+t\cdot 1)$
$$=3^3-3\cdot 3^2(1+t)+2\cdot 3\cdot(1+t)^2-6\cdot(1+t)^2$$
$$=0\cdot t^2+(-3^3+6\cdot 2-12)t+(\underbrace{3^3-3^3+6-6}_{=0})=-3^3t^1$$
eine einfache Nullstelle in $t=0$ hat, sowie $m([0:0:1];G,C_F)=2$, weil
$\tilde{\Psi}(t)=F(0+3t,\ 0+6t,\ 1+t)=(3t)^3-3(3t)^2(1+t)+\underbrace{2(3t)(1+t)^2-(6t)(1+t)^2}_{=0}=-3^3t^2$.

15.20. <u>Erläuterung:</u> Ist $m(P;G,C_F)=1$, liegt ein transversaler Schnitt der Geraden G mit der Kurve C_F vor. Ist $m(P;G,C_F)=2$, so ist G eine "einfache" Tangente an C_F. Falls $m(P;G,C_F)\geq 3$, ist die Tangente eine sehr gute Approximation an C_F von "Ordnung ≥ 3" (da die Schnittmultiplizität genau die Nullstellenordnung von $\Psi(t)$ in $t=0$ ist). Ist $m(P;G,C_F)$ ungerade ≥ 3, so heißt P ein <u>Wendepunkt</u> von C_F.

15.21. <u>Bem.:</u> Ist der Körper k algebraisch abgeschlossen, zerfällt Ψ vollständig in Linearfaktoren. Es folgt, dass dann die Summe der Schnittmultiplizitäten aller Schnittpunkte von G mit C_F genau $=\deg\Psi=\deg F$ ist, d.h. $\sum_{P\in G\cap C_F} m(P;G,C_F)=\deg F$.

Ist k ein beliebiger Körper, folgt $\sum_{P\in G\cap C_F} m(P;G,C_F)\leq\deg F$.

15.22. <u>Bem.:</u> Alle diese Ergebnisse gelten nicht, wenn das lineare Polynom, welches G erklärt, ein Teiler des Polynoms F ist, denn dann lassen sich keine Schnittmultiplizitäten erklären: Ist $G=G(\alpha,\beta,\gamma)$ durch $\alpha X+\beta Y+\gamma Z=0$ erklärt und $F(X,Y,Z)=(\alpha X+\beta Y+\gamma Z)\cdot H(X,Y,Z)$ für ein $H\in k[X,Y,Z]$, so folgt $G\subseteq C_F$ und für $[a:b:c],[a',b',c']\in G$ ist dann

$$\Psi(t)=F(a+ta',b+tb',c+tc')=(\alpha(a+ta')+\beta(b+tb')+\gamma(c+tc'))\cdot H(\dots)=0\cdot H(\dots)=0$$

das Nullpolynom, also die Nullstellenordnung von $t=0$ nicht definiert.

15.23. Wir zeigen nun, dass wir bei Tangenten in einem Kurvenpunkt immer die Schnittmultiplizität ≥ 2 haben, sofern der Grad der Kurve auch ≥ 2 ist.

15.24. **Satz:** Sei $P \in \mathbb{P}^2(k)$ ein nicht-singulärer Punkt auf C_F, wobei $\deg F \geq 2$ sei, und $T = T_P(C_F)$ die Tangente an C_F im Punkt P. Dann: $m(P; T, C_F) \geq 2$.

Beweis: Sei $T = G(\alpha, \beta, \gamma) = \{[x : y : z];\ \alpha x + \beta y + \gamma z = 0\}$ die Tangente in $P = [a : b : c] \in G \cap C_F$, also $\alpha = \frac{\partial F}{\partial x}(a, b, c)$, $\beta = \frac{\partial F}{\partial y}(a, b, c)$, $\gamma = \frac{\partial F}{\partial z}(a, b, c)$.
Sei $Q = [a' : b' : c'] \in G$ ein bel. weiterer Punkt auf G, und $\Psi(t) = F(a + ta', b + tb', c + tc')$.
Dann ist $\Psi(0) = 0$, da $P \in C_F$, und laut Kettenregel (vgl. Satz 13.5)) ist

$$\Psi'(0) = \frac{\partial F}{\partial x}(a, b, c) \cdot a' + \frac{\partial F}{\partial y}(a, b, c) \cdot b' + \frac{\partial F}{\partial z}(a, b, c) \cdot c' = \alpha a' + \beta b' + \gamma c' = 0,$$

weil $Q \in G$. Mit $\Psi(0) = 0$, $\Psi'(0) = 0$ folgt $m(P; T, C_F) \geq 2$. $\square$