# Vorlesung Kryptographie

WiSe '23/'24, hhu
K. Halupczok

## K16: Der Satz von Bézout

Stichworte:
- Spezialfall des Satzes von Bézout: $F_1, F_2 \in k[X]$ homogen, dann: $ggT(F_1, F_2) = 1 \Rightarrow \#(C_{F_1} \cap C_{F_2}) \leq (\deg F_1)\cdot(\deg F_2)$,
- Satz von von Bézout: $F_1, F_2 \in k[X]$ homogen, $ggT(F_1, F_2) = 1$ $\Rightarrow \sum_{P \in C_{F_1} \cap C_{F_2}} m(C_P; C_{F_1}, C_{F_2}) \leq (\deg F_1)\cdot(\deg F_2)$, und "=", falls $k$ algebraisch abgeschlossen.
- Resultante zweier Polynome $\in S[X]$, $S$ Körper oder Polynomring
- Zwei projektive Kurven $C_{F_1}$ und $C_{F_2}$ mit $(\deg F_1)\cdot(\deg F_2) - 1$ vielen Schnittpunkten und $ggT(F_1, F_2) = 1$, haben einen weiteren Schnittpunkt gemeinsam.

---

16.1. Einleitung: Wir zeigen in diesem Kapitel, dass projektive ebene Kurven i.a. nicht allzuviele Schnittpunkte haben, als "Lemma von Bézout".
Der Satz von Bézout hingegen besagt dies sogar für die Summe aller Schnittmultiplizitäten. Wir werden nur die schwache Version verwenden.

16.2. Satz (Lemma von Bézout):
Zwei Kurven $C_{F_1}, C_{F_2}$ in $\mathbb{P}^2(k)$ können sich in nicht mehr als $(\deg F_1)\cdot(\deg F_2)$ vielen Schnittpunkten treffen, es sei denn, $F_1$ und $F_2$ haben einen gemeinsamen Teiler vom Grad $\geq 1$.

D.h.: $ggT(F_1, F_2) = 1 \Rightarrow \#(C_{F_1} \cap C_{F_2}) \leq (\deg F_1)\cdot(\deg F_2)$,
bzw. $\deg ggT(F_1, F_2) = 0 \Rightarrow \#(C_{F_1} \cap C_{F_2}) \leq (\deg F_1)\cdot(\deg F_2)$.

16.3 Bem.: Der Satz 16.2 ist eine sehr schwache Form des Satzes von Bézout, welcher besagt:

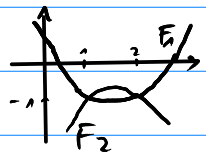
Satz von Bézout: Sei $k$ ein algebraisch abgeschlossener Körper und seien $F_1, F_2 \in k[X,Y,Z]$ zwei homogene Polynome mit $ggT(F_1, F_2) = 1$, die zwei ebene projektive Kurven $C_{F_1}$ und $C_{F_2}$ definieren.
Dann ist $$\sum_{P \in C_{F_1} \cap C_{F_2}} m(P; C_{F_1}, C_{F_2}) = (\deg F_1) \cdot (\deg F_2).$$

Ist $k$ beliebiger Körper, gilt dies mit "$\leq$" statt "$=$".

16.4 Bem.: Zum Beweis dieses allgemeinen Bézout-Satzes werden mehr Mittel aus der algebraischen Geometrie benötigt, als wir hier zeigen können. Für unsere Zwecke, das Studium elliptischer Kurven, reicht die schwache Version Satz 16.2, die wir hier beweisen, und insb. die spezielle Verschärfung Satz 16.17.

16.5 Bem.:
- Die Kurven können singuläre Punkte enthalten.
- Den Fall $\deg F_1 = 1$, d.h. wenn $F_1$ eine Gerade $C_{F_1}$ erklärt, haben wir bereits in Bem. 15.21 gezeigt.
- Den Begriff der Schnittmultiplizität müsste man für Schnittpunkte zweier beliebiger ebener Kurven verallgemeinern. Wir verzichten hier darauf.
- Aus diesem (allgemeinen) Satz von Bézout folgt bereits die schwache Version Satz 16.2: Denn für Schnittpunkte ist $m(P; C_{F_1}, C_{F_2}) \geq 1$, also ist $$\#(C_{F_1} \cap C_{F_2}) = \sum_{P \in C_{F_1} \cap C_{F_2}} 1$$
$$\leq \sum_{P \in C_{F_1} \cap C_{F_2}} m(P; C_{F_1}, C_{F_2}) \leq (\deg F_1) \cdot (\deg F_2).$$

16.6. **Bsp.:** Geg. seien die Parabeln $F_1(X,Y,Z) = X^2 - 3XZ + Z^2 - YZ$
und $F_2(X,Y,Z) = -X^2 + 3XZ - 3Z^2 - YZ$



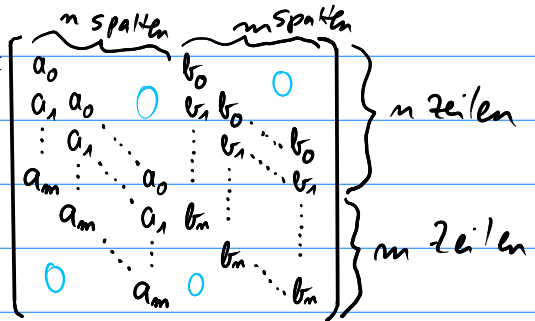

mit den beiden affinen reellen Schnittpunkten $[1:-1:1]$ und $[2:-1:1]$.
Laut Bézout-Satz haben die Parabeln noch zwei weitere Schnittpunkte über $\mathbb{C}$.
Diese sind nicht im Affinen, weil die Gleichung $F_1(X,Y,1) = F_2(X,Y,1)$ genau die Lösungen $(1,-1)$, $(2,-1)$ hat. Mit der Gleichung $F_2(X,Y,0) = F_2(X,Y,0)$ $\Leftrightarrow X^2 = -X^2$ erhält man $X=0$, also den (unendlich fernen) Punkt $[0:1:0] =: O$ als einzigen projektiven Schnittpunkt. Eine genaue Analyse würde zeigen, dass $O$ die Schnittmultiplizität 2 hat.

## Algebraische Vorbereitung zum Beweis von Satz 16.2: die Resultante

16.7. **Def.:** Seien $f, g \in k[X]$ Polynome vom Grad $m = \deg f$, $n = \deg g$, etwa gegeben durch

$$f = a_m X^m + a_{m-1} X^{m-1} + \dots + a_1 X + a_0,\quad g = b_n X^n + b_{n-1} X^{n-1} + \dots + b_0 \in k[X],$$
$$a_m \neq 0 \neq b_n.$$

Sei $M(f,g) :=$




$\in k^{(m+n)\times(m+n)}$.

Dann ist $\operatorname{Res}(f,g) = \det M(f,g) \in k$ die Resultante von $f$ und $g$.

16.8. **Bem.:**
- Anstelle von $k$ können auch beliebige kommutative Ringe mit 1 in der Def. stehen.
- $\operatorname{Res}(f,g)$ kann als Polynom in den Unbestimmten $a_0, \dots, a_m, b_0, \dots, b_n$ angesehen werden. Für einen darin vorkommenden Term $\prod_{i,j} a_i^{\nu_i} b_j^{\mu_j}$ gilt $\sum_{i=0}^{m} \nu_i (m-i) + \sum_{j=0}^{n} \mu_j (n-j) = mn$. [ohne Beweis]

16.9. **Bsp.:** $k = \mathbb{R}$, $f(x) = x^2 + 2x - 1$, $g(x) = 4x^3 - 3x + 5$

$$\rightsquigarrow M(f,g) = \begin{bmatrix} -1 & 0 & 0 & 5 & 0 \\ 2 & -1 & 0 & -3 & 5 \\ 1 & 2 & -1 & 0 & -3 \\ 0 & 1 & 2 & 4 & 0 \\ 0 & 0 & 1 & 0 & 4 \end{bmatrix}$$

Wir benutzen hier nur die folgende Eigenschaft von Resultanten, das sogenannte "Resultantenkriterium" (genaues: (i)⇔(iii)):

16.10. **Satz**: Sei $S$ ein faktorieller Ring (z.B. Polynomring oder ein Körper), $f,g \in S[X]$ Polynome mit $\deg f = m$, $\deg g = n$. Dann sind äquivalent:
(i) $f,g \in S[X]$ haben einen gemeinsamen nichtkonstanten Teiler in $S[X]$,
(ii) es gibt $f_0, g_0 \in S[X]\setminus\{0\}$ mit $\deg f_0 \le m-1$, $\deg g_0 \le n-1$ und $f_0 g = g_0 f$,
(iii) $\mathrm{Res}(f,g) = 0$

**Bew.**: (i) ⇒ (ii): Sei $h$ gemeinsamer Teiler, $\deg h \ge 1$. Dann setze $f_0 = \frac{f}{h}$, $g_0 = \frac{g}{h}$ ↝✓
(i) ⇐ (ii): Sind $f_0, g_0$ wie in (ii), und $h = \mathrm{ggT}(f,g)$, folgt $\mathrm{ggT}(\frac{f}{h}, \frac{g}{h}) = 1$.
Nach Vor. ist $\frac{f}{h} \cdot g_0 = f_0 \frac{g}{h}$, also ist $\frac{f}{h} \mid f_0$, d.h. $\deg \frac{f}{h} \le \deg f_0 \le m-1$, also $\deg h \ge 1$.
(ii) ⇔ (iii): $f_0, g_0$ entsprechen der nichttriv. Lösungen des LGS
$\sum_{k=1}^{n} c_k T^{k-1} f + \sum_{k=1}^{m} c_{n+k} T^{k-1} g = 0$. Bezüglich der Basis $T^0, T^1, \dots, T^{n+m-1}$ über $S$ wird das LGS gerade durch die Matrix $M(f,g)$ beschrieben. ↝✓ □

## Beweis von Satz 16.2:

16.11. Wir nehmen zum Beweis OE an, dass $k$ ein unendlicher Körper ist, andernfalls können wir z.B. zum algebraischen Abschluss $\bar{k}$ übergehen, der jedenfalls unendlich ist, vgl. dazu Bem. 14.26;
denn für eine Körpererweiterung könnte es mehr Schnittpunkte geben.

Sei $d_1 = \deg F_1$ und $d_2 = \deg F_2$.
Angenommen, $C_{F_1}$ und $C_{F_2}$ hätten (mind.) $d_1 d_2 + 1$ viele Punkte gemeinsam (wir zeigen, dass dann $\deg \mathrm{ggT}(F_1, F_2) \ge 1$ sein müsste).
Seien $P_0, P_1, \dots, P_{d_1 d_2}$ Schnittpunkte von $C_{F_1}$ und $C_{F_2}$.

16.12. Wir können OE annehmen, dass die Punkte $P_i = (x_i, y_i)$, $i = 0, \dots, d_1 d_2$, verschiedene x-Koordinaten und verschiedene y-Koordinaten haben (sonst erreicht man dies wieder durch eine Verschiebung/lineare Transformation, da k unendlich ist).

16.13. Wir können eine Gerade $G(\alpha, \beta, \gamma) = \{[x:y:z] \in \mathbb{P}^2(k); \alpha x + \beta y + \gamma z = 0\}$ finden, die durch keine dieser Punkte $P_0, \dots, P_{d_1 d_2}$ geht, weil k unendlich ist. Diese Gerade sei OE $g_\infty$, die unendlich ferne Gerade (durch eine Verschiebung/lineare Transformation lässt sich dies erreichen).

16.14 Somit ist das Problem auf ein affines Problem zurückgeführt worden. Die zugehörigen affinen Kurven seien durch $f_1, f_2 \in k[x,y]$ gegeben, d.h. $f_1(x,y) := F_1(x,y,1)$, $f_2(x,y) := F_2(x,y,1)$, mit $\deg f_1 \leq d_1$, $\deg f_2 \leq d_2$. Wir können OE sogar $\deg f_1 = d_1$, $\deg f_2 = d_2$ annehmen (nach geeigneter Transformation der Koordinaten der Art $X \to X + \varepsilon Y$, $Y \to Y$ ergeben sich für $F_1(X,Y,0) = \sum_{i+j=d_1} c_{ij} X^i Y^j$, $F_2(X,Y,0) = \sum_{i+j=d_2} d_{ij} X^i Y^j$ die Terme $(\sum_{i+j=d_1} c_{ij} \varepsilon^i) Y^{d_1}$ in $\tilde{F}_1(X,Y,0)$ und $(\sum_{i+j=d_2} d_{ij} \varepsilon^i) Y^{d_2}$ in $\tilde{F}_2(X,Y,0)$ ).

16.15. Wir betrachten $f_1, f_2 \in (k[x])[y]$ als Polynome in y mit Koeffizienten $\in k[x]$ und berechnen die Resultante $R(f_1, f_2) \in k[x]$, diese hat den Grad $= d_1 d_2$ in x nach Bem. 16.8. Sei $R(x) := R(f_1, f_2) \in k[x]$.

16.16. Für jedes $x_i$ haben die Polynome $f_1(x_i, y), f_2(x_i, y) \in k[y]$ einen Faktor $y - y_i \in k[y]$ gemeinsam. Für die $x = x_i$ muss $R(x)$ also verschwinden: $R(x_i) = 0$, $i = 0, \dots, d_1 d_2$.
Also hat $R(x)$ mehr Nullstellen ($d_1 d_2 + 1$ viele) als sein Grad $d_1 d_2$,
$R(x)$ muss also das Nullpolynom (in $x$) sein.
Aber dann haben $f_1, f_2 \in (k(x))[y]$ einen gemeinsamen Teiler vom Grad $\geq 1$
wegen Satz 16.10, (iii) $\Rightarrow$ (i). □

Wir zeigen noch die folgende Verschärfung in einem Spezialfall:

16.17. **Satz:** Sei $k$ ein (beliebiger) Körper, $F_1, F_2 \in k[X, Y, Z]$ homogene Polynome mit $d_1 = \deg F_1$, $d_2 = \deg F_2$ und $\operatorname{ggT}(F_1, F_2) = 1$, und es seien $d_1 d_2 - 1$ viele Schnittpunkte von $C_{F_1}$ und $C_{F_2}$ gegeben.
Dann haben sie einen weiteren Schnittpunkt $\in \mathbb{P}^2(k)$ gemeinsam.

**Bew.:** Wie im Beweis von Satz 16.2 von Bézout erhalten wir ein Polynom $R(x) \in k[x]$ vom Grad $= d_1 d_2$. Es hat $d_1 d_2 - 1$ viele Nullstellen $x_1, \dots, x_{d_1 d_2 - 1}$ laut Vor., ist also durch $(X - x_1) \cdots (X - x_{d_1 d_2 - 1})$ teilbar, der Quotient ist vom Grad 1, also $= r \cdot (X - a) \in k[X]$ mit einer (weiteren) Nullstelle $a \in k$.
Somit haben $f_1(a, y), f_2(a, y) \in k[y]$ einen gemeinsamen Faktor vom Grad $\geq 1$.
Dieser Grad ist $= 1$. [Denn wäre er $\geq 2$, würde er über $\bar{k}$ in mind. 2 Linearfaktoren zerfallen, die dann zu zwei weiteren Schnittpunkten mit gleicher $x$-Koordinate $a$ führen würden, so dass es $\geq (d_1 d_2 - 1) + 2 > d_1 d_2$ viele Schnittpunkte geben müsste im $\nsubseteq$ zu Satz 16.2.] Also gibt es nur noch genau einen weiteren Schnittpunkt $(a, y)$ von $C_{F_1}$ und $C_{F_2}$. □

16.18. **Bsp.:** Sei $k$ bel. Körper, $F_1, F_2 \in k[X, Y, Z]$ homogen, $\deg \operatorname{ggT}(F_1, F_2) = 0$, und sei $\deg F_1 = 1$, $\deg F_2 = 3$. Dann ist $\sum_{P \in C_{F_1} \cap C_{F_2}} m(P; C_{F_1}, C_{F_2}) \in \{0, 1, 3\}$.

Die Summe der Schnittmultiplizitäten kann hier also nicht $= 2$ sein!