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, $ggT(F_1, F_2) = 1$
$$\Rightarrow \sum_{P \in C_{F_1} \cap C_{F_2}} m(P; C_{F_1}, C_{F_2}) \leq (\deg F_1)\cdot(\deg F_2),$$
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.

2.3.2 Der Satz von Bézout

Wir zeigen in diesem Abschnitt, dass Kurven (projektive ebene) i.a. nicht allzuviele Schnittpunkte haben:

1.) **Satz**: 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 ≥ 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. $\deg ggT(F_1, F_2) = 0 \Rightarrow \#(C_{F_1} \cap C_{F_2}) \leq (\deg F_1)\cdot(\deg F_2)$.

2.) **Bem.**: Der Satz 1.) 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 "=".

3.) **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 1.), die wir hier beweisen, und insb. die spezielle Verschärfung Satz 15.) auf S. 5.

3) <u>Bem.:</u> • Die Kurven können singuläre Punkte enthalten.

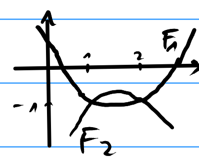
• Den Fall $\deg F_1 = 1$, d.h. wenn F_1 eine Gerade C_{F_1} erklärt, haben wir bereits in V9_Bem.20.) gezeigt.

• 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 1.): Denn für Schnittpunkte ist $m(P; C_{F_1}, C_{F_2}) \geq 1$, also ist

$$\#(C_{F_1} \cap C_{F_2}) = \sum_{P \in C_{F_1} \cap C_{F_2}} 1 \leq \sum_{P \in C_{F_1} \cap C_{F_2}} m(P; C_{F_1}, C_{F_2}) \leq (\deg F_1) \cdot (\deg F_2).$$

4) <u>Bsp.:</u> 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 $F_2(X,Y,0) = F_1(X,Y,0)$ $\Leftrightarrow X^2 = -X^2$ erhält man $X=0$, also den (∞ fernen) Punkt $[0:1:0] =: \mathcal{O}$ als einzigen projektiven Schnittpunkt. Eine genaue Analyse würde zeigen, dass $\mathcal{O}$ die Schnittmultiplizität 2 hat.

<u>Algebraische Vorbereitung</u> zum Beweis von Satz 1.): die <u>Resultante</u>

5) <u>Def.:</u> Seien $f, g \in k[X]$ Polynome vom Grad $m = \deg f$, $n = \deg g$, etwa gegeben durch

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

Sei
$$M(f,g) := \begin{array}{c} \overbrace{\hphantom{a_0 \; 0 \; 0}}^{n \text{ Spalten}} \; \overbrace{\hphantom{b_0 \; 0 \; 0}}^{m \text{ Spalten}} \\ \begin{bmatrix} a_0 & & 0 & b_0 & & 0 \\ a_1 & a_0 & & b_1 & b_0 & \\ \vdots & a_1 & \ddots & \vdots & b_1 & \ddots \; b_0 \\ a_m & \vdots & a_0 & \vdots & \vdots & b_1 \\ & a_m & a_1 & b_n & & \vdots \\ & & \ddots & & b_n & \\ 0 & & a_m & 0 & & b_n \end{bmatrix} \end{array} \begin{array}{l} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ Zeilen} \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} m \text{ Zeilen} \end{array} \in k^{(m+n)\times(m+n)}.$$

Dann ist $\mathrm{Res}(f,g) = \det M(f,g) \in k$ die <u>Resultante von f und g</u>.

6.) **Bem.:** • Anstelle von k können auch beliebige kommutative Ringe mit 1 in der Def. stehen.
• $\mathrm{Res}(f,g)$ 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]

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

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

"Resultantenkriterium" } Wir benutzen hier nur die folgende Eigenschaft von Resultanten (genauer: (i)$\Leftarrow$(iii)):

8.) **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) $\Rightarrow$ (ii): Sei h gemeinsamer Teiler, $\deg h \geq 1$. Dann setze $f_0 = \frac{f}{h}$, $g_0 = \frac{g}{h}$ $\rightsquigarrow \checkmark$
(i) $\Leftarrow$ (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 $\deg h \geq 1$.
(ii) $\Leftrightarrow$ (iii): f_0, g_0 entsprechen den nichttriv. Lösungen des LGS
$$\sum_{k=1}^{n} c_k T^{k-1} f + \sum_{k=1}^{m} c_{m+k} T^{k-1} g = 0.$$
Bezüglich der Basis $T^0, T^1, \dots, T^{m+n-1}$ über S wird das LGS gerade durch die Matrix $M(f,g)$ beschrieben. $\rightsquigarrow \checkmark$ $\square$

9.) **Beweis von Satz 1.):**

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 V7 Bem. 22.);
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 $\deg \mathrm{ggT}(F_1, F_2) \geq 1$ sein müsste).
Seien $P_0, P_1, \dots, P_{d_1 d_2}$ Schnittpunkte von C_{F_1} und C_{F_2}.

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

11.) 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 <u>keine</u> dieser Punkte $P_0, \ldots, P_{d_1 d_2}$ geht, weil k unendlich ist. Diese Gerade sei OE g_∞, die unendlich ferne Gerade (durch eine Verschiebung/lineare Transformation lässt sich dies erreichen).

12.) 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 $\left(\sum_{i+j=d_1} c_{ij} \varepsilon^i\right) Y^{d_1}$ in $\tilde{F}_1(X, Y, 0)$ und $\left(\sum_{i+j=d_2} d_{ij} \varepsilon^i\right) Y^{d_2}$ in $\tilde{F}_2(X, Y, 0)$).

13.) 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. 6.). Sei $R(x) := R(f_1, f_2) \in k[x]$.

14.) 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: $R(x_i) = 0$, $i = 0, \ldots, d_1 d_2$.
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 ≥ 1 wegen Satz 8.), (iii) $\Rightarrow$ (i). $\square$

15) <u>Satz:</u> 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 $ggT(F_1, F_2) = 1$, 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.

<u>Bew.:</u> Wie im Beweis von Satz 1.) von Bezout erhalten wir ein Polynom $R(x) \in k[X]$ vom Grad $= d_1 d_2$. Es hat $d_1 d_2 - 1$ viele Nullstellen $x_1, \ldots, x_{d_1 d_2 - 1}$ 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 ≥ 1. Dieser Grad ist $= 1$. [Denn wäre er ≥ 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 $\lightning$ zu Satz 1.).] Also gibt es nur noch genau einen weiteren Schnittpunkt (a, y) von C_{F_1} und C_{F_2}. □

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