3.2 Resultanten.

3.2.1. Definition. Teiler von Polynomen $f, g \in k[x]\setminus k$, die zu $k[x]\setminus k$ gehören, nennen wir gemeinsame Faktor/Teiler von f und g.

Entweder sind zwei Polynome $f, g \in k[x]\setminus k$ teilerfremd, d.h. $\mathrm{ggT}(f, g) = 1$, oder sonst haben f und g einen gemeinsamen Teiler/Faktor.

3.2.2. Lemma. Für $f, g \in k[x]\setminus k$ sind die folgenden Bedingungen äquivalent:

(i) f und g haben einen gemeinsamen Faktor

(ii) $Af + Bg = 0$ gilt für gewisse $A, B \in k[x]$ mit $(A, B) \neq (0, 0)$ und $\deg A < \deg g$, $\deg B < \deg f$.

Beweis: (i) $\Rightarrow$ (ii): Angenommen, $h \in k[x] \setminus k$ ist ein gemeinsamer Faktor von f und g.

Dann gilt $-\left(\frac{g}{h}\right) \cdot f + \left(\frac{f}{h}\right) \cdot g = 0$

Das heißt, wir können $A = -\frac{g}{h}$ und $B = \frac{f}{h}$ setzen. Es gilt $A \neq 0$, $B \neq 0$ und

$\deg(A) = \deg(g) - \deg(h) < \deg(g)$

$\deg(B) = \deg(f) - \deg(h) < \deg(f)$.

(ii) $\Rightarrow$ (i): Wir zeigen die Kontraposition (nicht(i)) $\Rightarrow$ (nicht(ii))

Angenommen, f und g haben keinen gemeinsamen Faktor. Dann gilt $\mathrm{ggT}(f,g) = 1 \Rightarrow$

$\langle f, g \rangle = \langle \mathrm{ggT}(f,g) \rangle = \langle 1 \rangle \Rightarrow$

$1 = C \cdot f + D \cdot g$ für gewisse $C, D \in k[x]$.

Seien $A, B \in k[x]$ mit $(A,B) \neq (0,0)$ und $Af + Bg = 0$. Wir zeigen, dass

$\deg(A) \geq \deg(g)$ oder $\deg(B) \geq \deg(f)$ erfüllt ist.

Es gilt:

$$
\begin{aligned}
A = A \cdot 1 = A(Cf + Dg) &= CAf + ADg \\
&= C(-Bg) + ADg \\
&= (AD - BC)g
\end{aligned}
$$

Analog:

$$
\begin{aligned}
B = B \cdot 1 = B(Cf + Dg) &= BCf + D(Bg) \\
&= BCf + D(-Af) \\
&= (BC - AD)f.
\end{aligned}
$$

Ist $A \neq 0$, so ist $AD - BC$ auch kein Nullpolynom und es gilt

$$
\begin{aligned}
\deg(A) &= \deg(AD - BC) + \deg(g) \\
&\geq \deg(g)
\end{aligned}
$$

Ist $B \neq 0$, so ist $BC - AD \neq 0$ und es gilt

$$\deg(B) = \deg(BC - AD) + \deg(f) \geq \deg f.$$

$\square$

3.2.3. Bemerkung. Für $m \in \mathbb{Z}_{\geq 0}$ bezeichne als $k[x]_m$ den $(m+1)$-dimensionalen k-Vektorraum

$$k[x]_m := \{ h \in k[x] : \deg(h) \leq m \}$$

Sei

$m := \deg(f)$, $\ell := \deg(g)$. Das Lemma enthält die lineare Abbildung.

$$\underset{\in\, \underbrace{k[x]_{\ell-1}\times k[x]_{m-1}}_{\text{hat Dimension } \ell+m}}{(A,B)} \xmapsto{\;T\;} \underset{\in\, \underbrace{k[x]_{m+\ell-1}}_{\text{hat Dimension } m+\ell}}{\underbrace{Af+Bg}}$$

(ii) $\iff$ T hat Nicht-Nullvektoren (A,B) im Kern.

Wir können für die beiden Räume $k[x]_{\ell-1} \times k[x]_{m-1}$ und $k[x]_{m+\ell-1}$ Basen fixieren und T als eine Matrix bzgl. dieser Basen darstellen.

Denn kann (ii) als Singularität einer solchen Matrix formuliert werden.

$(x^{\ell+m-1}, \dots\dots, x^0)$ ist unsere Basis für $k[x]_{m+\ell-1}$

$$\left.\begin{array}{l} (x^{\ell-1},0), \dots, (x^0,0) \\ (0,x^{m-1}), \dots, (0,x^0) \end{array}\right\}$$ ist unsere Basis für $k[x]_{\ell-1} \times k[x]_{m-1}$.

3.2.4. Definition. Für $f = u_0 x^\ell + u_1 x^{\ell-1} + \dots + u_{\ell-1} x + u_\ell \in k[x]$ und $g = v_0 x^m + v_1 x^{m-1} + \dots + v_{m-1} x + v_m \in k[x]$ mit $u_0 \neq 0 \neq v_0$ ($\ell, m \in \mathbb{N}$) definieren wir die <u>Sylvester-Matrix</u> von f und g bzgl. x als

$$Syl(f,g;x) := \begin{array}{c} \left[\begin{array}{cccccccc} u_0 & & & & v_0 & & & \\ \vdots & u_0 & & & \vdots & v_0 & & \\ \vdots & \vdots & u_0 & & \vdots & \vdots & \ddots & \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & & v_0 \\ u_\ell & \vdots & \vdots & u_0 & v_m & v_m & & \vdots \\ & u_\ell & \vdots & \vdots & & & \ddots & \vdots \\ & & u_\ell & \vdots & & & & v_m \\ & & & u_\ell & & & & \end{array}\right] \\ \underbrace{\hphantom{u_0\; u_0\; u_0\; u_0\;}}_{m}\underbrace{\hphantom{v_0\; v_0\; v_0\; v_0}}_{\ell} \end{array} \in k^{(m+\ell)\times(m+\ell)}$$

Die Resultante von f und g bzgl. x ist

$$\operatorname{Res}(f, g; x) := \det(\operatorname{Syl}(f, g); x).$$

3.2.5 Bemerkung. Zur Berechnung $\operatorname{Res}(f, g; x)$:

$\operatorname{Res}(f, g; x)$ ist kein Polynom in x.

3.2.6. Bemerkung. Wir verbinden $\operatorname{Res}(f, g; x)$ mit der Eigenschaft (ii) in Lemma 3.2.2.

Wir schreiben A und B wie folgt:

$$A = a_0 x^{m-1} + a_1 x^{m-2} + \dots + a_{m-1} \quad (\deg A < \deg g = m)$$

$$B = b_0 x^{l-1} + b_1 x^{l-2} + \dots + b_{l-1} \quad (\deg B < \deg f = l)$$

$$(x^{m+l-1}, \dots\dots, x^0) \operatorname{Syl}(f, g) = (x^{m-1} f, \dots, x^0 f, x^{l-1} g, \dots, x^0 g)$$

$$(x^3, x^2, x^1, x^0)\begin{pmatrix} u_0 & & v_0 & \\ u_1 & u_0 & v_1 & v_0 \\ u_2 & u_1 & v_2 & v_1 \\ & u_2 & & v_2 \end{pmatrix} = (x^3u_0 + x^2u_1 + x^1u_2,\ x^2u_0 + x^1u_1 + x^0u_2,$$
$$x^3v_0 + x^2v_1 + x^1v_2,$$
$$x^2v_0 + x^1v_1 + v_2)$$

Beispiel:

$$= (xf, f, xg, g)$$

$$f = u_0x^2 + u_1x + u_2$$
$$g = v_0x^2 + v_1x + v_2$$

$\Longrightarrow$

$$(x^{m+\ell-1}, \dots, x^0)\,\mathrm{Syl}(f,g)\begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \\ b_0 \\ \vdots \\ b_{\ell-1} \end{pmatrix}$$

$$= (x^{m-1}f, \dots, x^0f, x^{\ell-1}g, \dots, x^0g)\begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \\ b_0 \\ \vdots \\ b_{\ell-1} \end{pmatrix} = (x^{m-1}a_0 + \dots + x^0 \cdot a_{m-1})\,f$$
$$+ (x^{\ell-1}b_0 + \dots + x^0 b_{\ell-1}) \cdot g$$
$$= Af + Bg.$$

3.2.7. Bemerkung. Wenn wir $f, g \in k[x_1, \dots, x_n]$ so bezeichnen wir als

$\mathrm{Res}(f, g, x_i)$ die Resultante von f, g als Polynome in x_i mit Koeffizienten in $k[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$.

Das ist wohldefiniert, denn der Ring $k[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$ ist im Körper $K = k(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ enthalten. Das heißt, wir können $\mathrm{Res}(f, g, x_i)$ bzgl. der Betrachtung $f, g \in K[x_i]$ einführen.

3.2.8 Proposition. Polynome $f, g \in k[x] \setminus k$ haben genau dann einen gemeinsamen Faktor, wenn

$$\mathrm{Res}(f, g; x) = 0$$ ist.

Beweis: $\mathrm{Res}(f,g;x)=0 \Rightarrow \det(\mathrm{Syl}(f,g;x))=0$

$\Rightarrow \mathrm{Syl}(f,g;x)$ ist singulär $\Longrightarrow$

Das homogene lineare Gleichungssystem mit der Matrix $\mathrm{Syl}(f,g;x)$ hat eine Nichtnulllösung

$$\begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \\ b_0 \\ \vdots \\ b_{\ell-1} \end{pmatrix} \in k^{m+\ell} \qquad (\ell := \deg(f),\ m := \deg(g)).$$

$$\Rightarrow \quad \mathrm{Syl}(f,g;x) \begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \\ b_0 \\ \vdots \\ b_{\ell-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$(x^{m+\ell-1}, \dots, x^0)\, \mathrm{Syl}(f,g;x) \begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \\ b_0 \\ \vdots \\ b_{\ell-1} \end{pmatrix} = 0$$

$\Rightarrow Af + Bg = 0$ mit $A = a_0 x^{m-1} + \dots + a_{m-1}$ und

$B = b_0 x^{\ell-1} + \dots + b_{\ell-1}$

wobei $(A, B) \neq (0,0)$ gilt.

Lemma 3.2.2

$\Longrightarrow$ f und g haben einen gemeinsamen Faktor.

Die andere Richtung ist analog: Lemma 3.2.2

f, g haben einen gemeinsamen Faktor $\Longrightarrow$

$Af + Bg = 0$ für gewisse $A, B \in k[x]$ mit $(A, B) \neq (0,0)$

und $\deg A < \deg g$

$\deg B < \deg f$

Die Koeffizienten von A und B ergeben einen Nichtnullvektor, der bei der Multiplikation mit $Syl(f, g; x)$ einen Nullvektor ergibt.

$\Rightarrow$ $Syl(f, g; x)$ ist singulär $\Longrightarrow$

$Res(f, g; x) = \det(Syl(f, g; x)) = 0.$ $\square$

3.2.9. Bemerkung.

Für Polynome $f = u_0 x^\ell + \dots + u_{\ell-1} x + u_\ell$
$\in \mathbb{Z}[u_0, \dots, u_\ell, x]$

und $g = v_0 x^m + \dots + v_{m-1} x + v_m$
$\in \mathbb{Z}[v_0, \dots, v_m, x]$

(d.h. die Koeffizienten von f und g als Polynome in x sind Unbestimmte).

Ist $\mathrm{Res}(f, g; x) \in \mathbb{Z}[u_0, \dots, u_\ell, v_0, \dots, v_\ell]$.

Das sieht man direkt aus der Leibniz-Formel für $\mathrm{Res}(f, g; x) = \det(\mathrm{Syl}(f, g; x))$.

Das ist ein Nichtnullpolynom, weil man Paare f, g aus $k[x]$ mit und ohne gemeinsame Faktoren hat. ($f = x^\ell, g = x^m \Rightarrow \mathrm{Res} = 0$
$f = x^\ell, g = x^m + 1 \Rightarrow \mathrm{Res} \neq 0$)

f, g mit einem gem. Faktor $\Longrightarrow \langle f,g\rangle \neq k[x]$

f, g teilerfremd $\Longrightarrow \langle f,g\rangle = k[x]$, $1 = Af + Bg$

3.2.10 Proposition. Seien $f \in a_0 x^{l} + \dots a_{l-1}x + a_l \in \mathbb{Z}[a_0,\dots,a_l,x]$
und $g \in b_0 x^m + \dots + b_{m-1}x + b_m \in \mathbb{Z}[b_0,\dots,b_m,x]$

Dann gibt es $A, B \in \mathbb{Z}[a_0,\dots,a_l,b_0,\dots,b_m]$ mit

$$\underset{\in\,\mathbb{Z}[a_0,\dots,a_l,\,b_0,\dots,b_m]}{A}\ \underset{\in\,\mathbb{Z}[a_0,\dots,a_l,b_0,\dots,b_m,x]}{f} + \underset{\in\,\mathbb{Z}[a_0,\dots,a_l,\,b_0,\dots,b_m]}{B}\ \underset{\in\,\mathbb{Z}[a_0,\dots,a_l,b_0,\dots,b_m,x]}{g} = \underbrace{\mathrm{Res}(f,g;x)}_{\in\,\mathbb{Z}[a_0,\dots,a_l,b_0,\dots,b_m]}.$$

$\in \mathbb{Z}[a_0,\dots,a_l,b_0,\dots,b_m]$ unabhängig von x.

$\in \mathbb{Z}[a_0,\dots,a_l,b_0,\dots,b_m,x]$ Abhängigkeit von x

Beweis: Für die komplementäre Matrix $\mathrm{Syl}(f,g;x)^{\#}$ gilt

$$\mathrm{Syl}(f,g;x)\ \underbrace{\mathrm{Syl}(f,g;x)^{\#}}_{\in\,\mathbb{Z}[a_0,\dots,a_l,b_0,\dots,b_m]^{(m+l)\times(m+l)}} = \det(\mathrm{Syl}(f,g;x)) \cdot \underbrace{\mathrm{id}_{m+l}}_{\text{Einheitsmatrix der Größe } m+l}.$$

$$\Rightarrow \quad \mathrm{Syl}(f,g;x)\,\mathrm{Syl}(f,g;x)^{\#} = \mathrm{Res}(f,g;x)\cdot \mathrm{id}_{m+l}$$

$$\Rightarrow \quad (x^{m+l},\dots,x^0)\,\mathrm{Syl}(f,g;x)\,\mathrm{Syl}(f,g;x)^{\#} = \mathrm{Res}(f,g;x)\,(x^{m+l},\dots,x^0)$$

$$\Rightarrow \quad (x^{m-1}f,\dots,x^0 f,\ x^{l-1}g,\dots,x^0 g)\,\mathrm{Syl}(f,g;x)^{\#} = \mathrm{Res}(f,g;x)\,(x^{m+l},\dots,x^0)$$

$$\Rightarrow \quad (x^{m-1}f,\dots,x^0 f,\ x^{l-1}g,\dots,x^0 g)\,\underbrace{\mathrm{Syl}(f,g;x)^{\#}\begin{pmatrix}0\\ \vdots\\ 0\\ 1\end{pmatrix}} = \mathrm{Res}(f,g;x)\,(x^{m+l},\dots,x^0)\begin{pmatrix}0\\ \vdots\\ 0\\ 1\end{pmatrix}$$

$$\Rightarrow \quad (x^{m-1}f,\dots,x^0 f,\ x^{l-1}g,\dots,x^0 g)\begin{pmatrix}u_0\\ \vdots\\ u_m\\ v_0\\ \vdots\\ v_l\end{pmatrix} = \mathrm{Res}(f,g;x)$$

$$u_0,\dots,u_m,v_0,\dots,v_l \in \mathbb{Z}[a_0,\dots,a_l,b_0,\dots,b_m]$$

$$\Rightarrow \quad Af + Bg = \mathrm{Res}(f,g;x) \text{ mit } \begin{aligned} A &= u_0 x^{m-1} + \dots + u_m x^0 \\ B &= v_0 x^{l-1} + \dots + v_l \end{aligned}$$

A, B erfüllen die Bedingungen aus der Behauptung. $\square$

3.2.11 Proposition. Für $f, g \in \mathbb{C}[x] \setminus \mathbb{C}$ gibt es genau dann ein $c \in \mathbb{C}$ mit $f(c) = g(c) = 0$, wenn $\mathrm{Res}(f, g; x) = 0$ ist.

Beweis: Ist $f(c) = g(c) = 0 \Rightarrow x - c$ gemeinsamer Faktor von f und g $\Rightarrow \mathrm{Res}(f, g; x) = 0$.

Umgekehrt: $\mathrm{Res}(f, g; x) = 0 \Rightarrow f, g$ haben einen gemeinsamen Faktor $h \in \mathbb{C}[x] \setminus \mathbb{C}$. $\Rightarrow$

$f(c) = g(c) = 0$ für jede Nullstelle von h

(h hat Nullstellen in $\mathbb{C}$ nach dem fundamentalen Satz von Algebra). $\square$

3.2.10 Aufgaben.

(1) $f = ax + b$ $\quad$ $\mathrm{Res}(f, g; x) = \det \begin{pmatrix} a & c \\ b & d \end{pmatrix}$

$g = cx + d$

$= ad - bc$

(2x2 Determinante)

Was sind $A, B \in \mathbb{Z}[a, b, c, d, x]$
mit $Af + Bg = \mathrm{Res}(f, g; x)$?

$-c(ax + b) + a(cx + d) = -acx - bc + acx + ad$

$= ad - bc.$

(2) $f = x^2 + px + q$ $\quad$ $\mathrm{Res}(f, g; x) =$

$g = x + a$

$\det \begin{bmatrix} 1 & 1 & 0 \\ p & a & 1 \\ q & 0 & a \end{bmatrix} = a^2 + q - pa$

$= a^2 - pa + q$

$-a$ ist die einzige Nullstelle von g.

Damit es auch eine Nullstelle von f ist, soll $f(-a) = 0$ gelten.

Die Resultante ist genau $f(-a)$.

Was sind $A, B \in \mathbb{Z}[a,p,q,x]$

mit $Af + Bg = \mathrm{Res}(f,g;x)$?

$$1 \cdot (x^2 + px + q) + (-x + a - p)(x + a) = a^2 - pa + q$$

Was ist der Grad von A bzgl. x ?

Was ist der Grad von B bzgl. x ?

$-x(x+a) = -x^2 - ax$

px

$(p-a)x$

③ Wann hat x^2+px+q eine doppelte Nullstelle?
Was hat diese Bedingung mit Resultanten zu tun?
Bzw. wie kann man diese Bedingung mit Resultanten formulieren?

Schule „p-q-Formel."
Die gilt auch, wenn
$p, q \in \mathbb{C}$ sind.
$-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$ sind die beiden Nullstellen.

Sie fallen zusammen, wenn die Diskriminante
$\frac{p^2}{4} - q$ Null ist.

Bedingung: $\frac{p^2}{4} - q = 0.$

$a \in \mathbb{C}$ ist vielfache Nullstelle von $f \iff f(a) = f'(a) = 0$
(vgl. Anhang a).

$$\iff \mathrm{Res}(f, f'; x) = 0.$$

$$\mathrm{Res}(f, f'; x) = \det\begin{pmatrix} 1 & 2 & 0 \\ p & p & 2 \\ q & 0 & p \end{pmatrix} = 4q - p^2$$

$$f = x^2 + px + q$$

$$f' = 2x + p$$

4 Wann hat $f = x^3 + px + q$ eine vielfache Nullstelle?

Diskriminante ist ein Polynom, durch welches man vielfache Nullstellen abfragen kann.

$$\mathrm{Res}(f, f'; x) = \det\begin{bmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 \\ p & 0 & p & 0 & 3 \\ q & p & 0 & p & 0 \\ 0 & q & 0 & 0 & p \end{bmatrix} = 4p^3 + 27q^2.$$

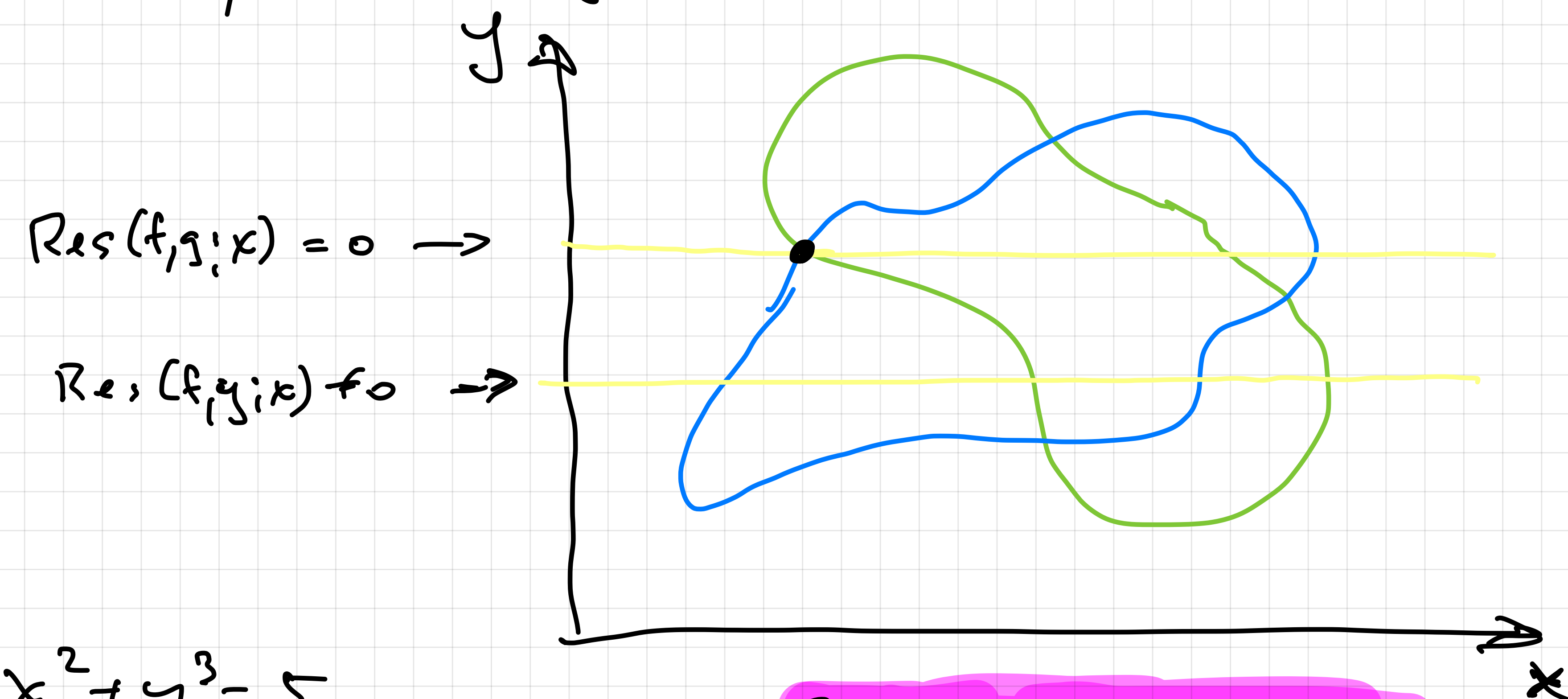
$$f = x^3 + px + q$$

$$f' = 3x^2 + p$$

(5) $\begin{cases} x^2 + y^3 - 5 = 0 \\ x^2 - 2xy + y^2 - 7 = 0 \end{cases}$

Wir könnten dieses System mit Resultanten lösen?

Man möchte daraus eine Gleichung $r(y) = 0$ herleiten, nur in y.



$f = x^2 + y^3 - 5$

$g = x^2 - 2xy + y^2 - 7$

$\mathrm{Res}(f,g;x) = 0$

ist eine solche Gleichung in y.