3.1.6. Beispiel

$$f = x^2 + y^3 - 5$$
$$g = x^2 - 2xy + 3y^2 - 7$$

SageMath:

Gröbnerbasis bzgl. der lex-Ordnung

$$x - \frac{1}{4}y^5 + \frac{1}{2}y^4 - \frac{9}{4}y^3 - \frac{1}{2}y^2 + \frac{13}{2}y$$
$$\underbrace{y^6 - 2y^5 + 9y^4 + 4y^3 - 32y^2 + 4}$$

Hat Nullstellen

$-1{,}58 \qquad -0{,}35 \qquad 0.36 \qquad 1.67$ ← reell

$0{,}94 \pm 3{,}26\sqrt{-1}$ ← komplex konjugiertes Paar

(numerische Approximationen).

3.1.7 Bsp.

$$f = x^2 + (y-4)^3 - 5$$

$$g = x^2 - 2xy + 3y^2 - 7$$

SageMath: Gröbnerbasis bzgl. der lex-Ordnung

$$x + \frac{1}{124}y^5 - \frac{13}{62}y^4 + \frac{273}{124}y^3 - \frac{655}{62}y^2 + \frac{1779}{62}y - 24$$

$$\underbrace{y^6 - 26y^5 + 273y^4 - 1372y^3 + 3888y^2 - 5952y + 3844}$$

laut Numerik hat dieses Polynom keine reellen Nullstellen

(3 Paare komplex konjugierter Nullstellen aus $\mathbb{C} \setminus \mathbb{R}$).

9.1.8 Bem. Es ist ziemlich klar, dass Elimination beim Berechnen eines impliziten Beschreibung aus einer parametrischen Beschreibung hilfreich sein sollte.

$$x_1 = p_1(t_1,\dots,t_m) \qquad p_1,\dots,p_n \in k[t_1,\dots,t_m]$$
$$\vdots$$
$$x_n = p_n(t_1,\dots,t_m)$$

Wir können mit Eliminationsidealen im Ring $k[t_1,\dots,t_m,x_1,\dots,x_n]$ (Elimination von $t_1,\dots,t_m$).

Allerdings soll ein Theorie dazu noch entwickelt werden, die begründet, dass Gröbnerbasen der Eliminationsideal die impliziten Beschreibungen ergeben.

3.1.9. Bemerkung. Elimination aus der Geometrischen Perspektive.

$I \subseteq k[x_1,\dots,x_n]$ Ideal, $I_\ell := I \cap k[x_{\ell+1},\dots,x_n]$

$V(I) \subseteq k^n$ $\qquad V(I_\ell) \subseteq k^{n-\ell}$

$\pi_\ell(x_1,\dots,x_n) := (x_{\ell+1},\dots,x_n) \qquad \pi_\ell : k^n \to k^{n-\ell}$

Wie stehen $\pi_\ell(V(I))$ und $V(I_\ell)$ zueinander?

Sei $(a_1,\dots,a_n) \in V(I)$, d.h.

$$f(a_1,\dots,a_n) = 0 \quad \text{für alle } f \in I.$$

Insbesondere gilt das für alle f aus I_ℓ, denn $I_\ell \subseteq I$.
Die Polynome aus I_ℓ hängen aber nicht von $x_1,\dots x_\ell$ ab. Also gilt $f(a_{\ell+1},\dots,a_n) = 0$ für alle $f \in I_\ell$. $\Rightarrow (a_{\ell+1},\dots,a_n) \in V(I_\ell)$.

Also gilt $\pi_\ell(V(I)) \subseteq V(I_\ell)$.

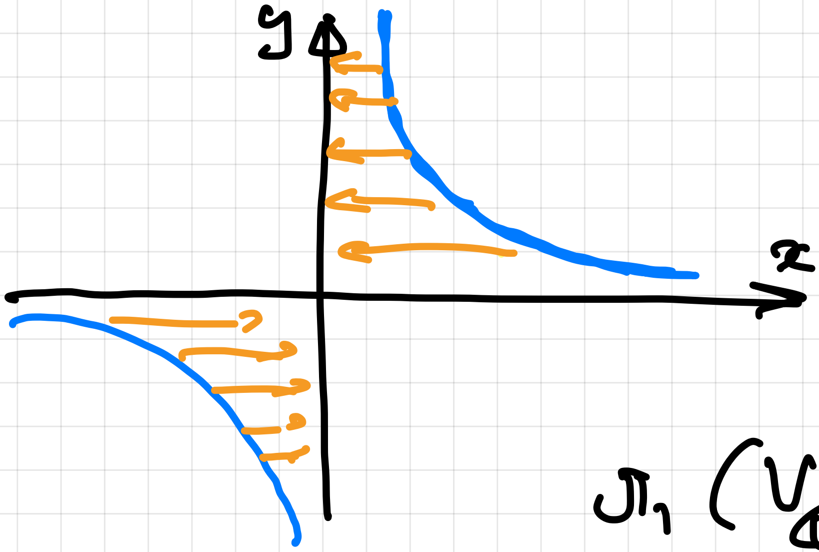
Es stellt sich heraus, dass im Fall $k=\mathbb{C}$ die Mengen $\pi_\ell(V(I))$ und $V(I_\ell)$ fast gleich sind, d.h.

$V(I_\ell) \setminus \pi_\ell(V(I))$ ist eine "kleine Menge"

$V(I_\ell) \setminus \pi_\ell(V(I))$ ist eine Varietät, die in $V(I_\ell)$ echt enthalten ist.

Im Gegensatz dazu zu $k=\mathbb{R}$ kann der Unterschied zwischen $\pi_\ell(V(I))$ und $V(I_\ell)$ erheblich sein.

3.1.10. Bsp. $I = \langle xy - 1 \rangle$



$$V_{\mathbb{C}}(I) = \{ (a,b) \in \mathbb{C} : ab = 1 \}$$

$$\pi_1(x,y) = y \qquad \pi_1 : \mathbb{C}^2 \to \mathbb{C}$$

$$\pi_1(V_{\mathbb{C}}(I)) = \mathbb{C} \setminus \{0\}$$

$$I_1 = \{0\} \Rightarrow V(I_1) = \mathbb{C}.$$

$$I = \langle x(y^2 + z^2 - 1) - 1 \rangle$$

$$V(I) = \{ (a, b, c) \in \mathbb{C} : a(b^2 + c^2 - 1) = 1 \}$$

$$\pi_1(x, y, z) = (y, z)$$

$$\pi_1(V(I)) = \mathbb{C}^2 \setminus V(y^2 + z^2 - 1)$$

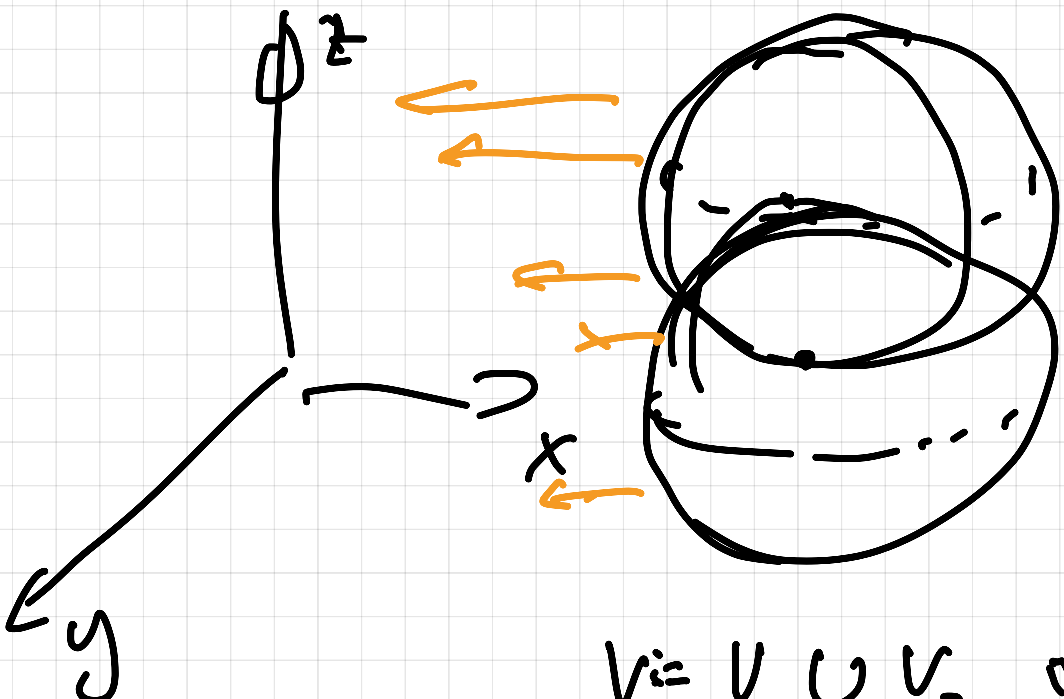
3.1.11. Bsp. Was erhält man durch Projektion von $V_{\mathbb{R}}(I)$ bzgl. des Körpers $\mathbb{R}$.

$$V_1 = V_{\mathbb{R}}\left(1 - x^2 - y^2 - \left(z - \tfrac{1}{2}\right)^2\right)$$

Sphäre: Radius 1 Zentrum in $(0,0,-\frac{1}{2})$

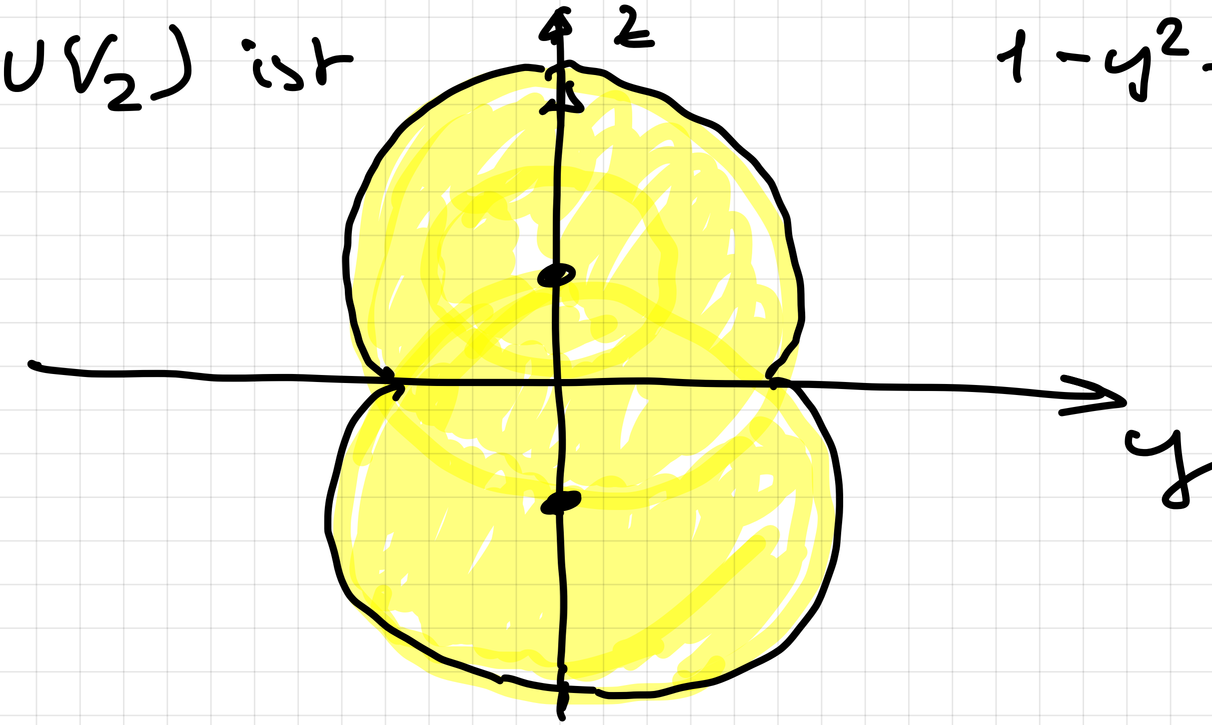
$$V_2 = V_{\mathbb{R}}\left(1 - x^2 - y^2 - \left(z + \tfrac{1}{2}\right)^2\right)$$

Sphäre: Radius 1 Zentrum in $(0,0,\frac{1}{2})$



$V := V_1 \cup V_2$ ist auch eine Varietät

$\pi_1(V_1 \cup V_2)$ ist



$1 - y^2 - (z-\frac{1}{2})^2 = x^2 \geq 0$

$$\| $$

$$\underbrace{\pi_1(V_1) \cup \pi_1(V_2)}_{\text{ist gegeben durch}} = \{y^2 + (z-\tfrac{1}{2})^2 \leq 1\} \cup \{y^2 + (z+\tfrac{1}{2})^2 \leq 1\}.$$

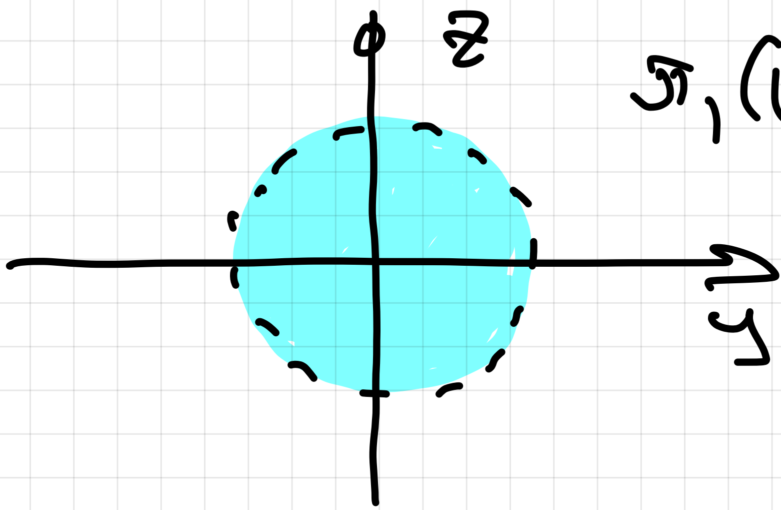
$$y^2 + (z-\tfrac{1}{2})^2 \leq 1 \quad \underline{\text{oder}} \quad y^2 + (z+\tfrac{1}{2})^2 \leq 1$$

$$V = V_{\mathbb{R}}\left(x^2(1-y^2-z^2)-1\right)$$

$$x^2(1-y^2-z^2) = 1 \implies 1-y^2-z^2 = \frac{1}{x^2} > 0.$$

$$\pi_1\left(V_{\mathbb{R}}(x^2(1-y^2-z^2)-1)\right)$$

$$= \{ y^2+z^2 < 1 \}$$



$\pi_1(V)$

Anhang A: Bestimmung der Nullstellen univariater Polynome

A1. Weierstraß-Durand-Kerner-Verfahren.

Sei $f \in \mathbb{C}[X]$ Polynom vom Grad $d := \deg f > 0$ und sei $\mathrm{LC}(f) = 1$. Wir sind an einem numerischen Verfahren zur Bestimmung aller Nullstellen von f interessiert.

Sei $p(X,z) = (X - z_1) \cdot \ldots \cdot (X - z_d)$ mit $z = (z_1, \ldots, z_d) \in \mathbb{C}^d$. Wir sind an einem z interessiert, für welches die Gleichung

$$p(X,z) = f(X) \quad \text{in } \mathbb{C}[X]$$

erfüllt ist.

Nehmen wir an, wir kennen ein solches z annähernd und wollen unsere Approximation zu $z+h$ verbessern, mit $h = (h_1, \dots, h_d) \in \mathbb{C}^d$ (kleine Updates). Es gilt

$$p(x, z+h) \approx p(x, z) + \sum_{i=1}^{d} \frac{\partial p(x, z)}{\partial z_i} \cdot h_i$$

$$= p(x, z) - \sum_{i=1}^{d} \left(\prod_{k \in \{1, \dots, d\} \setminus \{i\}} (x - z_k) \right) h_i$$

Die Gleichung $p(x, z+h) = f(x)$ in h lässt sich also durch die Näherung

$$p(x, z) - \sum_{i=1}^{d} \left(\prod_{k \in \{1, \dots, d\} \setminus \{i\}} (x - z_k) \right) h_i = f(x)$$

ersetzen.

In dieser Gleichung setzen wir für x die Werte $z_1, \ldots, z_d$ ein. Für $x = z_j$ erhält man.

$$- \prod_{k \in \{1,\ldots,d\} \setminus \{j\}} (z_j - z_k) h_j = f(z_j)$$

$$\Rightarrow \quad h_j = - \frac{f(z_j)}{\prod_{k \in \{1,\ldots,d\} \setminus \{j\}} (z_j - z_k)} \quad (j = 1, \ldots, d)$$

W-D-K-Verfahren ist das iterative Verfahren auf der Basis solcher Updates.

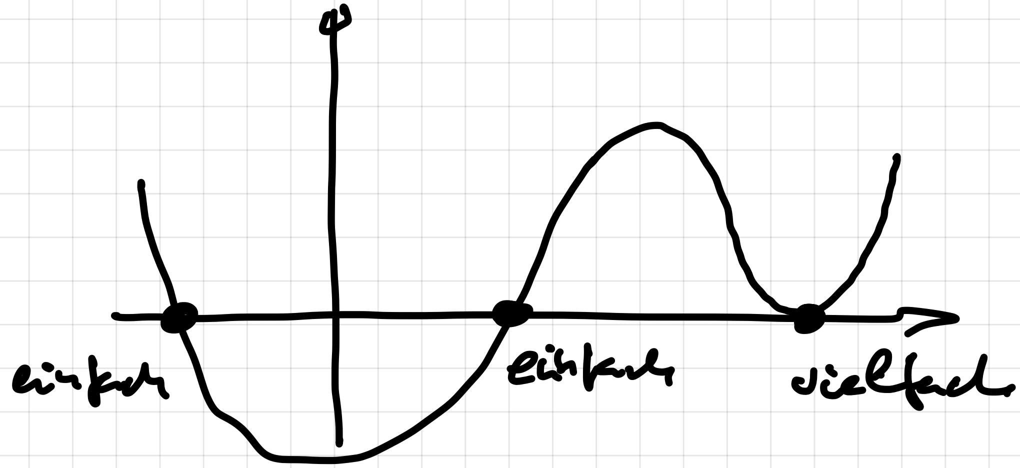
Man startet mit einem $z^{(0)}$ und konstruiert $z^{(1)}, z^{(2)}, z^{(3)}, \ldots$ iterativ mit Hilfe

$$z_j^{(m+1)} = z_j^{(m)} - \frac{f(z_j^{(m)})}{\prod\limits_{k \in \{1,\dots,d\} \setminus \{j\}} (z_j^{(m)} - z_k^{(m)})}$$

W-D-K ist Spezialfall des Newtonverfahrens.

Für die Konvergenz gelten die Theoreme zum Newtonverfahren.

A.2 Reduktion zum Fall einfacher Nullstellen.



Def. A.2.1. Für $f \in \mathbb{C}[x] \setminus \{0\}$ und $a \in \mathbb{C}$ führen wir $\mathrm{mult}(f,a)$ ein, als das $m \in \mathbb{Z}_{\geq 0}$ mit

$$f(x) = (x-a)^m g(x) \quad \text{mit } g \in \mathbb{C}[x] \text{ und } g(a) \neq 0.$$

Wir nennen a *m-fache Nullstelle* von f.

0-fache Nullstellen sind keine Nullstellen.

1-fache Nullstellen sind *einfache Nullstellen*.

m-fache Nullstellen mit $m > 1$ sind *vielfache Nullstellen*.

A.2.2. Proposition. Für $f, g \in \mathbb{C}[x]\setminus\{0\}$ gilt:

$$f \text{ teilt } g \Longleftrightarrow \operatorname{mult}(f,a) \leq \operatorname{mult}(g,a) \text{ für alle } a \in \mathbb{C}.$$

Beweis:

f teilt $g \Rightarrow f q = g$ für ein $q \in \mathbb{C}[x]$.

Sei $a \in \mathbb{C}$ und seien

$$f(x) = (x-a)^m u(x)$$
$$g(x) = (x-a)^n v(x)$$

mit $m, n \in \mathbb{Z}_{\geq 0}$, $u, v \in \mathbb{C}[x]$ und $u(a) \neq 0 \neq v(a)$.

Zu zeigen: $m \leq n$. Wäre $m > n$, so hätte man Folgendes:

$$fq = g \Rightarrow (x-a)^m u(x) q(x) = (x-a)^n v(x)$$

$$\Rightarrow \underbrace{(x-a)^{m-n} u(x) q(x)}_{\substack{\in \mathbb{C}[x] \\ = 0 \text{ an der Stelle } x=a}} = \underbrace{v(x)}_{\substack{\in \mathbb{C}[x] \\ \neq 0 \text{ an der Stelle } x=a}} \quad ↯$$

$\Rightarrow \quad \mathrm{mult}(f,a) = m \leq n = \mathrm{mult}(g,a)$.

Umgekehrt: sei $\mathrm{mult}(f,a) \leq \mathrm{mult}(g,a)$ für alle $a \in \mathbb{C}$. OBdA sei $LC(f) = 1$. Wir faktorisieren f als $f = (x-a_1)^{m_1} \cdot \ldots \cdot (x-a_\ell)^{m_\ell}$ mit

$a_1, \ldots, a_\ell \in \mathbb{C}$ (paarweise verschieden)

und $m_1, \ldots, m_\ell \in \mathbb{Z}_{>0}$

Da die Vielfachheit von a_i bzgl. g mindestens m_i ist, ist $(x-a_i)^{m_i}$ Faktor von g. Somit hat g das Polynom f als Faktor. $\Rightarrow$ f teilt g.

$\square$

A.2.3. Korollar. Für $f = (x-a_1)^{m_1} \cdot \ldots \cdot (x-a_\ell)^{m_\ell}$,

$g = (x-a_1)^{n_1} \cdots (x-a_\ell)^{n_\ell}$ mit

$a_1, \ldots, a_\ell \in \mathbb{C}$ (paarweise verschieden) und

$m_1, \ldots, m_\ell, n_1, \ldots, n_\ell \in \mathbb{Z}_{\geq 0}$ gilt

$$\operatorname{ggT}(f,g) = (x-a_1)^{p_1} \cdot \ldots \cdot (x-a_\ell)^{p_\ell}$$

mit $p_i = \min\{m_i, n_i\}$.

Beweis: Das Polynom in der Behauptung ist laut A.2.2 Teiler von f und g. Wenn $h \in \mathbb{C}[x] \setminus \{0\}$ ein Polynom ist, das f und g teilt, dann gilt nach A.2.2 $h = c \cdot (x-a_1)^{q_1} \cdot \ldots \cdot (x-a_\ell)^{q_\ell}$ mit $q_i \leq m_i$ und $q_i \leq n_i$ $(c \in \mathbb{C} \setminus \{0\})$.

Also ist $q_i \leq \min\{m_i, n_i\} = p_i \overset{A.2.2}{\Longrightarrow}$ h teilt das Polynom in der Behauptung. $\square$

A.2.4. Proposition. Sei $f \in \mathbb{C}[x] \setminus \mathbb{C}$ und sei $a \in \mathbb{C}$ eine Nullstelle von f (d.h. $\mathrm{mult}(f,a) \geq 1$).

Dann gilt $\mathrm{mult}(\underbrace{f'}_{\text{Formale Ableitung von } f}, a) = \mathrm{mult}(f,a) - 1$

Beweis: Sei $m = \mathrm{mult}(f,a)$, d.h.

$$f(x) = (x-a)^m u(x) \quad \text{mit } u \in \mathbb{C}[x] \text{ und } u(a) \neq 0.$$

Dann gilt:

$$\begin{aligned} f'(x) &= ((x-a)^m u(x))' \\ &= ((x-a)^m)' u(x) + (x-a)^m u'(x) \\ &= m(x-a)^{m-1} u(x) + (x-a)^m u'(x) \\ &= (x-a)^{m-1} \underbrace{(m\, u(x) + (x-a) u'(x))}_{\substack{= m\, u(a) \neq 0 \\ \text{an der Stelle } x=a}} \end{aligned}$$

$$\Longrightarrow \mathrm{mult}(f', a) = m - 1 = \mathrm{mult}(f,a) - 1.$$

A.2.5. Korollar. Für $f = (x-a_1)^{m_1} \cdot \ldots \cdot (x-a_\ell)^{m_\ell}$ mit $a_1, \ldots, a_\ell \in \mathbb{C}$ (paarweise verschieden) und $m_1, \ldots, m_\ell \in \mathbb{Z}_{>0}$ ist

$$\mathrm{ggT}(f, f') = (x-a_1)^{m_1-1} \cdot \ldots \cdot (x-a_\ell)^{m_\ell-1}$$

Insbesondere gilt

$$g := \frac{f}{\mathrm{ggT}(f, f')} = (x-a_1) \cdot \ldots \cdot (x-a_\ell).$$

Das heißt, $V_{\mathbb{C}}(f) = V_{\mathbb{C}}(g) = \{a_1, \ldots, a_\ell\}$ und jede Nullstelle von g ist einfach.

Beweis: Direkte Folgerung aus A.2.3 und A.2.4. $\square$

A.3. Suche nach den reellen Nullstellen mit dem Satz von Sturm.

A.3.1 Def. Seien $a_0, \dots, a_\ell$ Werte aus $\mathbb{R}$. Wir führen die <u>Anzahl der Vorzeichenänderungen</u> $\operatorname{signvar}(a_0, \dots, a_\ell)$ der Folge $a_0, \dots, a_\ell$ als die Anzahl der Unterfolgen $a_i, \dots, a_m$ mit $0 \le i < m \le \ell$, in denen das Anfangs- und das Endglied verschiedene Vorzeichen haben (d.h. $a_i \cdot a_m < 0$) und die Glieder a_j mit $i < j < m$ alle gleich Null sind.

Bsp.

$$\operatorname{signvar}(\underbrace{2, -1}_{\text{Nr. 1}}0, 3, 0, 0, -1, 0, 0, -2, \underbrace{-3, 5}_{\text{Nr. 4}}, 0) = 4.$$

Nr. 2

Nr. 3

Als Vorbereitung zur nächsten Definition rekapitulieren wir den Euklidischen Algorithmus zur Berechnung von ggT.

<u>Wiederholung:</u> $f \in k[x],\quad g \in k[x] \setminus \{0\}$

$$\underset{\substack{\shortparallel\\ \mathrm{Rem}(f,g)}}{f = q \cdot g + r} \qquad \deg r < \deg g$$

Der Algorithmus basiert auf der Beobachtung $\mathrm{ggT}(f,g) = \mathrm{ggT}(\mathrm{Rem}(f,g), g)$.

Wir können die Zwischenergebnisse des Euklidischen Algorithmus durch eine Folge von Polynomen beschreiben:

$$f_0 = f$$
$$f_1 = g$$
$$\vdots$$
$$f_{i-1} = q_i \cdot f_i + f_{i+1} \quad \text{mit } \deg f_{i-1} < \deg f_i$$
$$(i = 1, \dots, l-1)$$
$$\vdots$$
$$f_{l-1} = q_l \cdot f_l + f_{l+1} \quad \text{mit } f_{l+1} = 0$$

$$f_l = \operatorname{ggT}(f, g)$$

Oder mit anderen Bezeichnungen:

$$f_0 = f$$
$$f_1 = g$$
$$f_{i+1} = \operatorname{Rem}(f_{i-1}; f_i) \qquad i = 1, \dots, l-1$$
$$f_{l+1} = 0 = \operatorname{Rem}(f_{l-1}; f_l)$$

$$f_l = \operatorname{ggT}(f, g)$$

Der Euklidische Algorithmus benutzt die Tatsache dass $\operatorname{ggT}(f_i, f_{i+1})$ unverändert bleibt und mit $\operatorname{ggT}(f_0, f_1) = \operatorname{ggT}(f, g)$ übereinstimmt.

Man beachte, dass die Gleichung $\operatorname{ggT}(f, g) = \operatorname{ggT}(\operatorname{Rem}(f; g), g)$ zur Gleichung $\operatorname{ggT}(f, g) = \operatorname{ggT}(c \cdot \operatorname{Rem}(f; g), g)$ mit $c \in k \setminus \{0\}$ verallgemeinert werden kann. Wir können also eine (leicht) modifizierte Version des Euklidischen Algorithmus betrachten, die der Wahl $c = -1$ entspricht.

$f_0 = f$

$f_1 = g$

$\vdots$

$f_{i-1} = q_i \cdot f_i - f_{i+1}$ mit $\deg f_{i+1} < \deg f_i$

$(i = 1, \dots, l-1)$

$\vdots$

$f_l = q_{l-1} \cdot f_{l-1} - f_{l+1}$ mit $f_{l+1} = 0$.

Man hat: $\text{ggT}(f, g) = f_l$

(man beachte, dass $\text{ggT}(f, g)$ nur bis auf einen Faktor aus $K \setminus \{0\}$ definiert).

Oder mit anderen Bezeichnungen:

$f_0 = f$

$f_1 = g$

$f_{i+1} = -\text{Rem}(f_{i-1}, f_i) \quad (i = 1, \dots, l-1)$

$$\boxed{f_l = \text{ggT}(f, g)}$$

$f_{l+1} = 0 = -\text{Rem}(f_{l-1}, f_l)$

A.3.2 Definition. Sei $f \in \mathbb{R}[x] \setminus \mathbb{R}$. Die *Sturmfolge* von f ist die Folge der Polynome $f_0, \dots, f_\ell$ mit

$$f_0 = f$$
$$f_1 = f'$$
$$f_{i+1} = -\operatorname{Rem}(f_{i-1}, f_i) \quad \text{für } i = 1, \dots, \ell-1$$
$$f_{\ell+1} = 0 = -\operatorname{Rem}(f_{\ell-1}, f_\ell).$$

Für $a \in \mathbb{R}$ definieren wir

$$\sigma(f, a) = \operatorname{signvar}(f_0(a), \dots, f_\ell(a)).$$

A.3.3 Theorem (Sturm). Sei $f \in \mathbb{R}[x] \setminus \mathbb{R}$.

Seien $a, b \in \mathbb{R}$, $a < b$ und sei $f(a) \neq 0 \neq f(b)$.

Dann ist die Anzahl der Nullstellen von f in $[a,b]$, ohne Berücksichtigung der Vielfachheiten, gleich $v(f;a) - v(f;b)$.

A.3.4. Bsp. $f = (x+1)^4 (x-3)^2 (x-7)$

$$v(f,0) = \left(-63, -201, \frac{4896}{49}, -\frac{18816}{169}\right)$$

$$= (-, -, +, -) \quad \text{2 Vorzeichenänd.}$$

$$v(f;10) = \left(2152227, 2114959, \frac{3364768}{7}, \frac{58430127}{169}\right)$$

$$= (+, +, +, +) \quad \text{0 Vorzeichenänd.}$$

$$v(f,0) - v(f,10) = 2 \Rightarrow \text{2 Nullstellen in } [0,10]$$

A.2.6. Bemerkung. Man kann A.2.5 natürlich auch für Polynome $f \in \mathbb{R}[X]\setminus\mathbb{R}$ benutzen, dabei faktorisiert man f aber trotzdem bzgl. $\mathbb{C}$ d.h. $f = (X-a_1)^{m_1} \cdot \ldots \cdot (X-a_\ell)^{m_\ell}$ und die Nullstellen aus $\mathbb{C}\setminus\mathbb{R}$ treten in komplex konjugierten Paaren auf. Das Polynom g liegt aber trotzdem in $\mathbb{R}[X]$, weil laut den Euklidischen Algorithmus

$ggT(f, f') \in \mathbb{R}[X]$ ist, auch wenn man $\mathbb{C}[X]$ als den Umgebungsring festlegt. Das heißt: für $f \in \mathbb{R}[X]\setminus\mathbb{R}$ ist g ein Polynom aus $\mathbb{R}[X]$ und seine reelle sowie komplexe Nullstellen sind einfach.