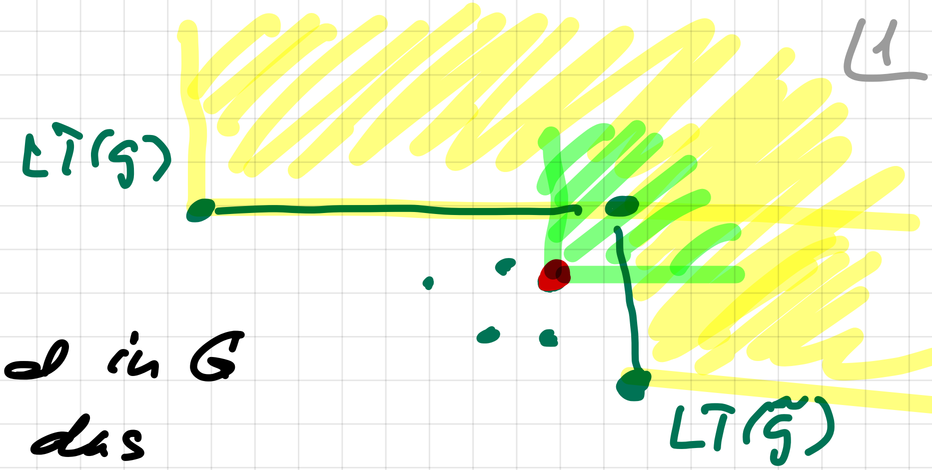


Um die Terminierung zu zeigen, betrachten wir $\langle LT(G) \rangle$.

Wenn ein $r = Rem(S(g, \tilde{g}); G)$ mit $r \neq 0$ in R und anschließend in G aufgenommen wird, vergrößert sich das Ideal $\langle LT(G) \rangle$; denn nach dem Aufbau des Divisionsalgorithmus ist keiner der Terme von r durch einen der Leitterme von G teilbar. Insbesondere ist auch $LT(r)$ durch keinen der Leitterme von G teilbar.

D.h. $LT(r) \notin \langle LT(G) \rangle$. Nach der Kettenbedingung für Ideale stabilisiert sich jede Kette von Idealen.

D.h. nach einem Zeitpunkt der Ausführung ändert sich $\langle LT(G) \rangle$ nicht mehr. Nach diesem Zeitpunkt hat man $R = \emptyset$ und das Verfahren terminiert.

$\square$

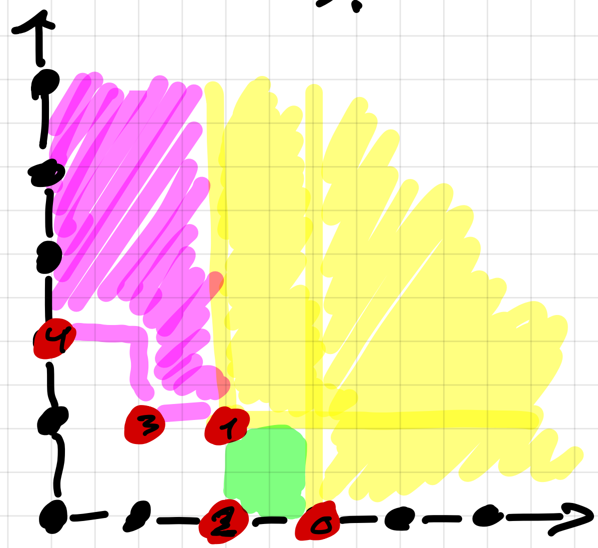
2.62. Bsp.

$$f_0 = x^3 - 2xy$$
$$f_1 = x^2y - 2y^2 + x$$

grlex als zugrundeliegende Monomordnung

Die Gröbnerbasis von $\langle f_0, f_1 \rangle$ wird mit Hilfe des Buchberger algorithmus berechnet. (der Algorithmus aus dem vorigen Beweis).

$g_0 = f_0$, $g_1 = f_1$



$$S(f_0, f_1) = y f_0 - x f_1$$
$$= y(x^3 - 2xy) - x(x^2y - 2y^2 + x)$$
$$= -2xy^2 + 2xy^2 - 2x^2$$
$$= -2x^2$$

$$\mathrm{Rem}(-2x^2; g_0, g_1) = -2x^2$$

$$g_2 = -2x^2 \quad \Big\} \text{ 1. Runde}$$

$\vdots$

$$g_3 = -2xy = \mathrm{Rem}(S(g_0, g_2); g_0, g_1, g_2)$$
$$g_4 = -2y^2 + x = \mathrm{Rem}(S(g_1, g_2); g_0, g_1, g_2)$$

2.6.3. Bsp. Sage:

```
R = PolynomialRing(QQ, 'x,y', order = 'lex')
x,y = R.gens()
F = [x^4 + y^4 - 10, x*y - 1]
I = R.ideal(F)
I.groebner_basis()
```

"deglex"

2.6.4 Bem. Wir können Gröbnerbasen auch als Teilmengen von $k[x_1,\dots,x_n]$ auffassen, denn die Reihenfolge der Polynome $(g_1,\dots,g_s)$ hat keine Auswirkung auf die Gröbner-Basis-Eigenschaft.

2.6.5. Lemma. Sei G Gröbnerbasis eines Ideals $I \subseteq k[x_1,\dots,x_n]$ mit $I \neq \{0\}$ und sei $p \in G$ ein Polynom mit $LT(p) \in \langle LT(G \setminus \{p\}) \rangle$. Dann ist $G \setminus \{p\}$ ebenfalls eine Gröbnerbasis.

Beweis: G Gröbnerbasis heißt $\langle LT(G)\rangle = \langle LT(I)\rangle$.

$$\langle LT(G\setminus\{p\})\rangle = \langle LT(G)\rangle = \langle LT(I)\rangle$$

$\Rightarrow$ $G\setminus\{p\}$ eine Gröbnerbasis von I. $\square$

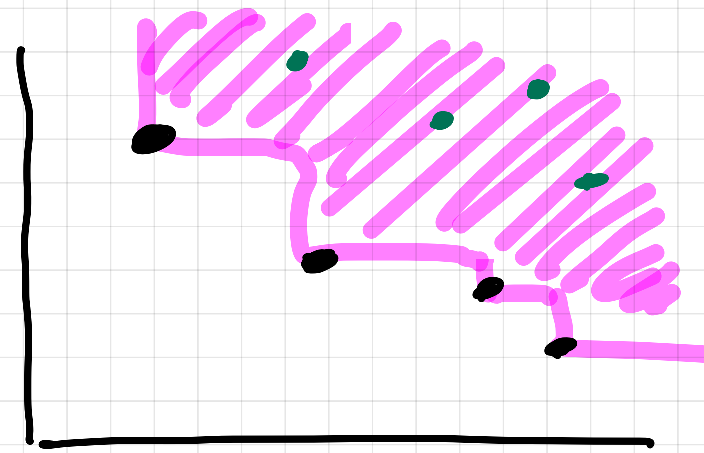
Wenn wir redundante Polynome weglassen und $LC(p) = 1$ für alle $p \in G$ durch Skalieren erzwingen, erhalten wir eine sogenannte minimale Gröbnerbasis:

9.6.6. Def. Eine Gröbnerbasis G von $I \subseteq k[x_1, \dots, x_n]$ wird *minimal* genannt wenn

$$LC(p) = 1 \quad \text{und} \quad LT(p) \notin \langle LT(G\setminus\{p\})\rangle$$

für alle $p \in G$ erfüllt ist.

Die minimalen Gröbnerbasen müssen nicht eindeutig sein.



Zum Beispiel: ist $\{g_1, g_2\}$ eine Gröbnerbasis mit

$$\mathrm{mdeg}(g_1) \succ \mathrm{mdeg}(g_2)$$

dann ist $\{g_1, ag_1 + g_2\}$ mit $a \in k$ ebenfalls eine Gröbnerbasis, denn

$$LT(g_1) = LT(g_1) \qquad LC(g_1) = LC(g_1) = 1$$

$$LT(g_2) = LT(ag_1 + g_2) \qquad LC(g_2) = LC(ag_1+g_2) = 1.$$

2.67. Def. Wir nennen eine Gröbnerbasis G von $I \subseteq k[x_1, \ldots, x_n]$ <u>reduziert</u> wenn Folgendes gilt:

(i) $LC(p) = 1$ für alle $p \in G$.

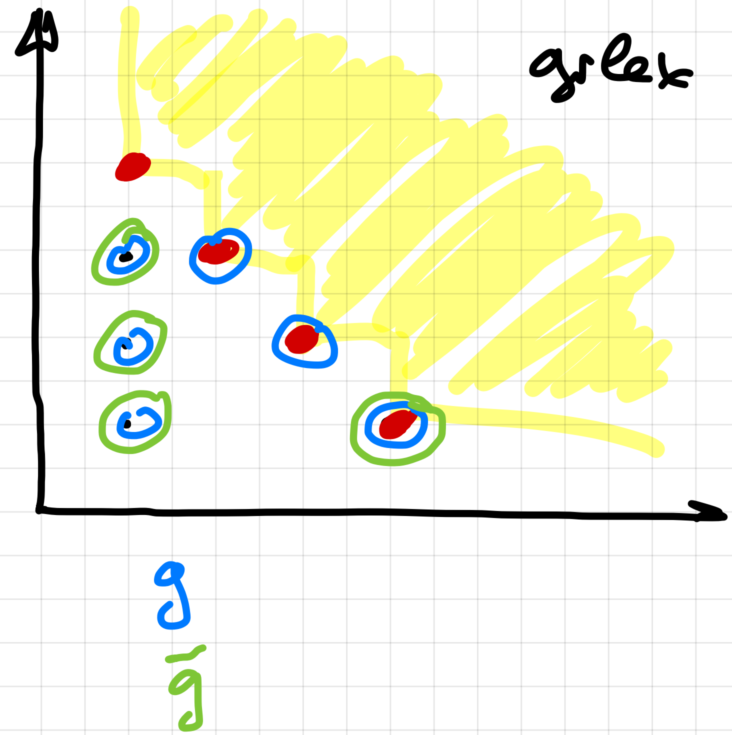
(ii) Für jedes $p \in G$ liegt <u>kein Term</u> von in $\langle LT(G \setminus \{p\}) \rangle$.

2.6.8 Prop. Für jedes Polynomideal $\{0\} \neq I \subseteq k[x_1, \dots, x_n]$ und jede Monomordnung $\leq$ für $k[x_1, \dots, x_n]$ gibt es eine <u>eindeutige</u> reduzierte Gröbnerbasis für I.

<u>Beweis:</u> <u>Existenz:</u> Wir reduzieren iterativ eine beliebige minimale Gröbnerbasis von I zu einer reduzierten Gröbnerbasis. Wir nennen ein Polynom $p \in G$ reduziert bzgl. G, wenn kein Term von p in $\langle LT(G \setminus \{p\}) \rangle$ enthalten ist. Diese Eigenschaft von p hängt nicht direkt von G sondern nur von $LT(G)$ ab.

Für $g \in G$ können wir $\tilde{g} = \mathrm{Rem}(g; G \setminus \{g\})$ einführen. Es stellt sich heraus, dass $\tilde{G} = G \setminus \{g\} \cup \{\tilde{g}\}$ ebenfalls eine Gröbnerbasis von I ist und, dass $\tilde{g}$ in $\tilde{G}$ reduziert ist.

Man hat $LT(\tilde{g}) = LT(g)$, weil G eine minimale Gröbnerbasis ist. Das heißt $LT(G) = LT(\widetilde{G})$, sodass $\widetilde{G}$ eine minimale Gröbnerbasis bleibt.



Alle Terme in g, die durch einen der Terme aus $LT(G \setminus \{g\})$ teilbar sind, werden durch das Restbilden entfernt. Also ist $\tilde{g}$ tatsächlich reduziert in $\widetilde{G}$. Nun können wir die Operation

$$G \longmapsto \widetilde{G}$$

iterativ bzgl. alle Polynome in G durchführen. Auf diese Weise wird jedes Polynom in G reduziert.

Eindeutigkeit. Seien $G, \tilde{G}$ reduzierte Gröbnerbasen von I. Wegen der Minimalität gilt $LT(G) = LT(\tilde{G})$. Somit hat man für jedes $g \in G$ ein $\tilde{g} \in \tilde{G}$ mit dem selben Leitterm und umgekehrt. Das heißt, es gibt eine Bijektion $g \longleftrightarrow \tilde{g}$ durch die Vorgabe der Leitterme. Nun zeigen wir, dass für $g \in G$ und $\tilde{g} \in \tilde{G}$ mit $LT(g) = LT(\tilde{g})$ die Gleichheit $g = \tilde{g}$ gilt. Da $g, \tilde{g} \in I$ gilt, gilt auch $g - \tilde{g} \in I$. Die Leitterme von g und $\tilde{g}$ kompensieren sich in der Differenz $g - \tilde{g}$. Alle anderen Terme sind aber durch keinen der Terme aus $LT(G) = LT(\tilde{G})$ teilbar. Das heißt, beim Teilen von $g - \tilde{g}$ durch G werden alle Terme von $g - \tilde{g}$ direkt in den Rest aufgenommen. Das bedeutet $\mathrm{Rem}(g - \tilde{g}; G) = g - \tilde{g}$.

Andererseits ist $\mathrm{Rem}(g-\tilde{g}; G) = 0$; denn $g - \tilde{g} \in I$ und G ist Gröbnerbasis von I.

$\Rightarrow g - \tilde{g} = 0 \Rightarrow g = \tilde{g}$. $\square$

2.6.9. Bsp. $f = x^2 + y^3 - 5$

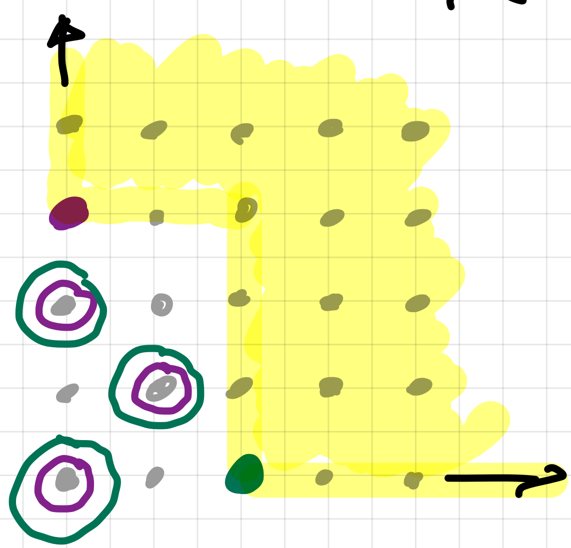
$g = x^2 - 2xy + 3y^2 - 7$

Monomordnung: grlex

Wir konstruieren eine reduzierte Basis von $\langle f, g \rangle$:

$h = y^3 + 2xy - 3y^2 + 2$

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



$\{h, r\}$ Gröbnerbasis (reduziert)

$\{h+r, r\}$ $LT(h+r) = y^3$, $LT(r) = x^2$

$\Rightarrow \{h+r, r\}$ ist ~~auch~~ eine Gröbnerbasis. Diese Basis ist minimal, aber nicht reduziert.

$\{h+r, r\}$ ist nicht reduziert, denn
der Term x^2 von $h+r$ ist durch $LT(r) = x^2$ teilbar.
$\{h, h+r\}$ ist keine Gröbnerbasis, denn $LT(h) = LT(h+r) = y^3$.

2.6.10. Bemerkung.

$$\underbrace{\begin{matrix} x - 2y + z = 7 \\ x + y + 5z = 10 \end{matrix}}_{\substack{\text{Original System} \\ \text{(Linear)}}} \rightsquigarrow \underbrace{\begin{matrix} x + \frac{11}{3} z = 9 \\ y + \frac{4}{3} z = 1 \end{matrix}}_{\substack{\text{Das neue System} \\ \text{aus der Gröbnerbasis} \\ \text{(bzgl. der lex ordnung)}}}$$

$$\left(\begin{array}{ccc|c} 1 & -2 & 1 & 7 \\ 1 & 1 & 5 & 10 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & \frac{11}{3} & 9 \\ 0 & 1 & \frac{4}{3} & 1 \end{array}\right)$$

Die reduzierte Stufenform, die man mit Gauß-Verfahren berechnen kann.

Eine reduzierte Stufenform für ein lineares Gleichungssystem entspricht der reduzierten Gröbner Basis bzgl. der Lex-Ordnung.

D.h. der Algorithmus von Buchberger ist in einem gewissen Sinne eine Verallgemeinerung von Gauß-Verfahren.

Im vorigen Beispiel:

$$h = y^3 + 2xy - 3y^2 + 2$$
$$r = x^2 - 2xy + 3y^2 - 7$$

deglex.	y^3 $>$	x^2 $>$	xy $>$	y^2 $>$	1
h	1	0	2	-3	2
r	0	1	-2	3	-7

Wir können die reduzierte Gröbner Basis durch diese Matrix angeben, die eine reduzierte Stufenform hat.

2.6.11. Korollar. Sei $\leq$ eine Monomordnung für $k[x_1, \ldots, x_n]$. Dann sind zwei Nichtnullideale I, J genau dann gleich, wenn ihre reduzierten Gröbnerbasen (als Mengen) gleich sind.

Beweis: direkte Folgerung aus Prop. 2.6.8. $\square$

2.6.12. Bem. Um $f \in \langle f_1, \ldots, f_s \rangle$ algorithmisch zu entscheiden, kann man folgendermaßen vorgehen. Man konstruiert eine Gröbnerbasis G für $\langle f_1, \ldots, f_s \rangle$ und testet ob $\mathrm{Rem}(f; G) = 0$ gilt.

2.6.13 Aufgaben

① Konstruieren Sie Gröbnerbasen von

$$\langle x^2y-1,\ xy^2-x\rangle$$

$$\langle x^2+y,\ x^4+2x^2y+y^2+3\rangle$$

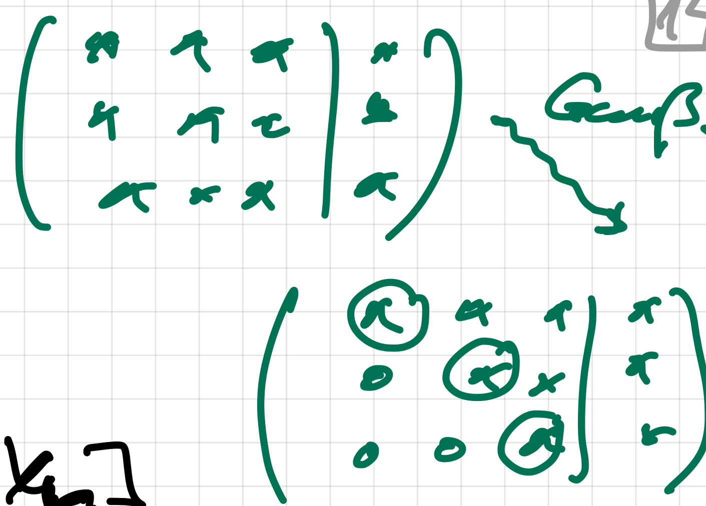
$$\langle x-z^4,\ y-z^5\rangle$$

bzgl. verschiedener Monomordnungen (lex und grlex).

② Zeigen dass $ggT(f,g)$ (mit Leitkoeffizient $=1$) die reduzierte Gröbnerbasis von $\langle f,g\rangle$ ist, für $f,g \in k[x]\setminus\{0\}$.

3. Elimination

3.1. Eliminationsideale



3.1.1. Def. Für ein Ideal $I \subseteq k[x_1,\dots,x_n]$ und $\ell \in \{0,\dots,n\}$ nennt man

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

das *ℓ-te Eliminationsideal* von I.

3.1.2. Prop. Für $\ell \in \{0,\dots,n\}$ und ein Ideal $I \subseteq k[x_1,\dots,x_n]$ ist $I_\ell = I \cap k[x_{\ell+1},\dots,x_n]$ ein Ideal im Ring $k[x_{\ell+1},\dots,x_n]$.

Beweis: $0 \in I,\ 0 \in k[x_{\ell+1},\dots,x_n] \Rightarrow 0 \in I_\ell$.

$f,g \in I_\ell \Rightarrow f,g \in I,\ f,g \in k[x_{\ell+1},\dots,x_n] \Rightarrow$

$f+g \in I$ (I ist ideal), $f+g \in k[x_{\ell+1},\dots,x_n] \Rightarrow f+g \in I_\ell$

$f \in I_\ell$, $h \in k[x_{\ell+1},\dots,x_n] \Rightarrow f \in I$, $f \in k[x_{\ell+1},\dots,x_n]$
$h \in k[x_{\ell+1},\dots,x_n]$

$$\Rightarrow \left.\begin{array}{l} f \cdot h \in I \text{ (weil } I \text{ ideal ist)} \\ f \cdot h \in k[x_{\ell+1},\dots,x_n] \end{array}\right\} \Rightarrow f \cdot h \in I_\ell .$$

$\square$

3.1.3 Bem. Ab jetzt nehmen wir an, dass $\emptyset$ die Gröbnerbasis vom Nullideal ist.

3.1.4. Theorem (Das Eliminationstheorem).

Sei $I \subseteq k[x_1, \dots, x_n]$ ein Ideal und G Gröbnerbasis von I bzgl. der lex-Ordnung. Dann ist $G_\ell := G \cap k[x_{\ell+1}, \dots, x_n]$ eine Gröbnerbasis des Ideals $I_\ell = I \cap k[x_{\ell+1}, \dots, x_n]$ bzgl. der lex-Ordnung.

Beweis: $G \subseteq I$, $G_\ell \subseteq G$, $G_\ell \subseteq k[x_{\ell+1}, \dots, x_n] \Rightarrow$

$$G_\ell \subseteq I_\ell \Rightarrow LT(G_\ell) \subseteq LT(I_\ell).$$

Um $\langle LT(G_\ell) \rangle = \langle LT(I_\ell) \rangle$ zu zeigen, zeigen wir dass für jedes $f \in I_\ell \setminus \{0\}$ der Leitterm von f durch einen Leitterm eines Polynoms aus G_ℓ teilbar ist.

Es gilt: $f \in I_\ell \subseteq I$ und G ist eine Gröbner-basis von I. Also ist $LT(f)$ durch $LT(g)$ für ein $g \in G$ teilbar. Wegen $f \in k[x_{\ell+1}, \dots, x_n]$ gilt $\text{mdeg}(f) = (\underbrace{0, \dots, 0}_{\ell}, \alpha_{\ell+1}, \dots, \alpha_n)$.

Es folgt, dass man für $\text{mdeg}(g)$ ~~die~~ Darstellung $\text{mdeg}(g) = (\underbrace{0, \dots, 0}_{\ell}, \beta_{\ell+1}, \dots, \beta_n)$ hat.

Denn hätte man unter ~~den~~ ersten ℓ Komponenten von $\text{mdeg}(g)$ einen positiven Wert, dann wäre $LT(f)$ nicht durch $LT(g)$ teilbar.

Nun betrachten wir ein beliebiges Monom x^γ mit $\gamma = (\gamma_1, \dots, \gamma_n)$, das in g enthalten ist.

$\mathrm{mdeg}(g) = (0, \dots, 0, \beta_{l+1}, \dots, \beta_n) \Longrightarrow$

$(\underbrace{0, \dots, 0}_{l}, \beta_{l+1}, \dots, \beta_n) \leq_{lex} (\gamma_1, \dots, \gamma_n)$

$\Rightarrow \gamma_1 = \dots = \gamma_l = 0$, denn wäre einer der Werte $\gamma_1, \dots, \gamma_l$ strikt positiv, dann hätte man $\gamma \succ_{lex} (0, \dots, 0, \beta_{l+1}, \dots, \beta_n) = \mathrm{mdeg}(g)$ ist $\lightning$. Wir haben gezeigt, dass kein Monom von g von den Variablen $x_1, \dots, x_l$ abhängig ist. Das bedeutet $g \in k[x_{l+1}, \dots, x_n]$.

$\Rightarrow g \in G \cap I_l =: G_l$. $\square$

19

3.1.5 Bem. Lex-Ordnung kann rechenintensiv sein.

Wenn man nur eines der Gröbnerbasen $G_1, \dots, G_n$ ausrechnen möchte, z.B. G_3, kann man versuchen eine dafür zugeschnittene Ordnung einzuführen, in der die Berechnungen schneller sind.

3.1.6. Beispiel

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

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