Situation im univariaten Fall:

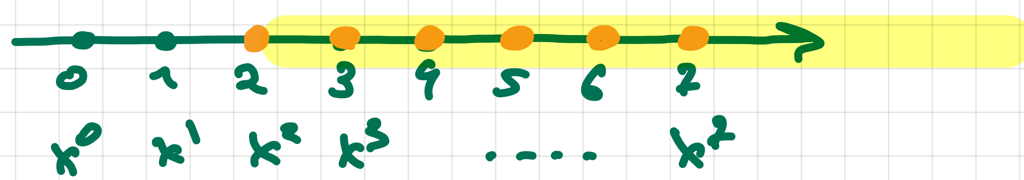
$$f \in \langle f_1,\dots,f_s\rangle \iff f \in \langle g\rangle \text{ mit } g := \mathrm{ggT}(f_1,\dots,f_s)$$

$$\iff$$ Der Rest der Division von f durch g ist 0

Hierbei:

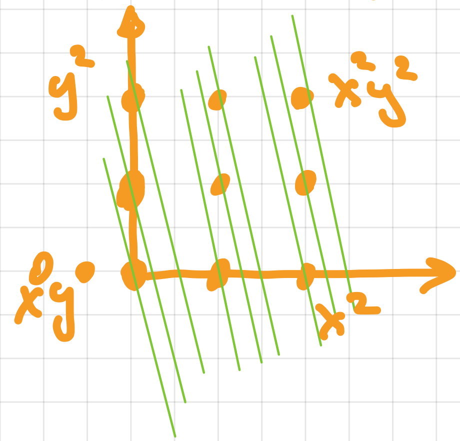
g kann durch den Euklidischen Algorithmus bestimmt werden (erfordert Polynomdivision)

g ist Nichtnullpolynom vom kleinsten Grad in $\langle f_1,\dots,f_s\rangle$



Im Multivariaten Fall:

- Eine Polynomdivision benötigt eine Monomordnung



$x \preceq_{lex} y$

$\frac{x}{y}$ kein Monom

- $\alpha \preceq \beta \not\Longrightarrow x^{\alpha}$ ist durch x^{β} teilbar (Division sieht also etwas anders aus)

- Ein Ideal ist i.A. nicht durch ein Polynom erzeugbar (wir müssen durch mehr als ein Polynom teilen können)

2.2.4. Bezeichnung. Wir bezeichnen als $\mathrm{Rem}(f; G)$ den Rest der Division von $f \in k[x_1, \dots, x_n]$ durch $G = (g_1, \dots, g_s)$ mit $g_1, \dots, g_s \in k[x_1, \dots, x_n] \setminus \{0\}$

2.3. Monomiale Ideale und das Lemma von Dickson

Wir verallgemeinern die Bezeichnung $\langle f_1, \dots, f_s \rangle$ auf unendliche Familien von Polynomen:

2.3.1 Def. Für eine (potenziell unendlich) indexierte Familie $(f_s)_{s \in S}$ von Polynomen aus $k[x_1, \dots, x_n]$ wird das Ideal das Ideal definiert, das durch diese Familie erzeugt ist: es ist das Ideal $\langle f_s : s \in S \rangle$ aller Polynome der Form

$$\sum_{s \in S} h_s f_s \quad \text{mit } h_s \in k[x_1, \dots, x_n] \text{ und mit } h_s \neq 0 \text{ nur für endlich viele } s \in S.$$

Bem. Es ist tatsächlich ein Ideal.

2.3.2. Def. Ist $A \subseteq \mathbb{Z}_{\geq 0}^n$ (potenziell unendlich), so nennt man das Ideal $\langle x^\alpha : \alpha \in A \rangle$ das *monomiale Ideal* zu A.

2.3.3. Def. Auf $\mathbb{Z}_{\geq 0}^n$ fixieren wir die Teilordnung $\geq$ wie folgt:

$$\alpha = (\alpha_1, \ldots, \alpha_n) \geq \beta = (\beta_1, \ldots, \beta_n) :\Longleftrightarrow \alpha_1 \geq \beta_1, \ldots, \alpha_n \geq \beta_n$$

$\alpha \leq \beta$ wird analog definiert.

Bem. $\alpha \geq \beta \iff x^\alpha$ ist durch x^β teilbar.
$\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$

2.3.4. Def. Für $A, B \subseteq \mathbb{Z}_{\geq 0}^n$ nenn wir

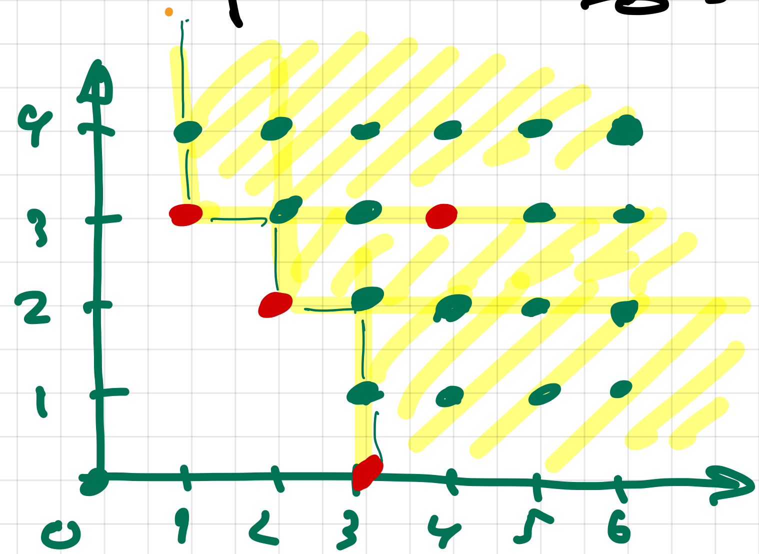
$$A + B := \{\alpha + \beta : \alpha \in A, \beta \in B\}$$

die Minkowski-Summe von A und B.

Bez: lin_k := lineare Hülle bzgl. k.

2.3.5. Lemma. Sei $A \subseteq \mathbb{Z}^n_{\geq 0}$. Dann gilt:

$$\langle x^\alpha : \alpha \in A \rangle = \mathrm{lin}_k \{ x^\beta : \beta \in A + \mathbb{Z}^n_{\geq 0} \}$$



Beweis:

"$\supseteq$": Für x^β mit $\beta \in A + \mathbb{Z}^n_{\geq 0}$ gilt $x^\beta = x^{\alpha+\gamma}$ mit $\alpha \in A$ und $\gamma \in \mathbb{Z}^n_{\geq 0}$;

$$\Rightarrow \quad x^\beta = x^{\alpha+\gamma} = \underbrace{x^\alpha}_{\in \langle x^\alpha : \alpha \in A \rangle} \cdot x^\gamma \in \langle x^\alpha : \alpha \in A \rangle$$

$$\Rightarrow \quad \mathrm{lin}_k \{ x^\beta : \beta \in A + \mathbb{Z}^n_{\geq 0} \} \subseteq \langle x^\alpha : \alpha \in A \rangle.$$

"$\subseteq$": Wir betrachten ein beliebiges Polynom aus $\langle x^\alpha : \alpha \in A \rangle$. Das hat die Form

$$\sum_{\alpha \in A} h_\alpha x^\alpha$$ mit $h_\alpha \in k[x_1, \dots, x_n]$ und $h_\alpha \neq 0$ nur für endlich viele α's.

h_α hat die Form $h_\alpha = \sum_\gamma \underbrace{c_{\alpha,\gamma}}_{\in k} x^\gamma \Rightarrow$

$$h_\alpha x^\alpha = \sum_\gamma c_{\alpha,\gamma} x^\gamma \cdot x^\alpha = \sum_\gamma c_{\alpha,\gamma} x^{\alpha+\gamma}$$

mit $\alpha + \gamma \in A + \mathbb{Z}^n_{\geq 0}$ für alle $\gamma \in \mathbb{Z}^n_{\geq 0}$.

D.h. $h_\alpha x^\alpha \in \operatorname{lin}_k \{x^\beta : \beta \in A + \mathbb{Z}^n_{\geq 0}\}$.

$\Rightarrow \sum_\alpha h_\alpha x^\alpha \in \operatorname{lin}_k \{x^\beta : \beta \in A + \mathbb{Z}^n_{\geq 0}\}$.

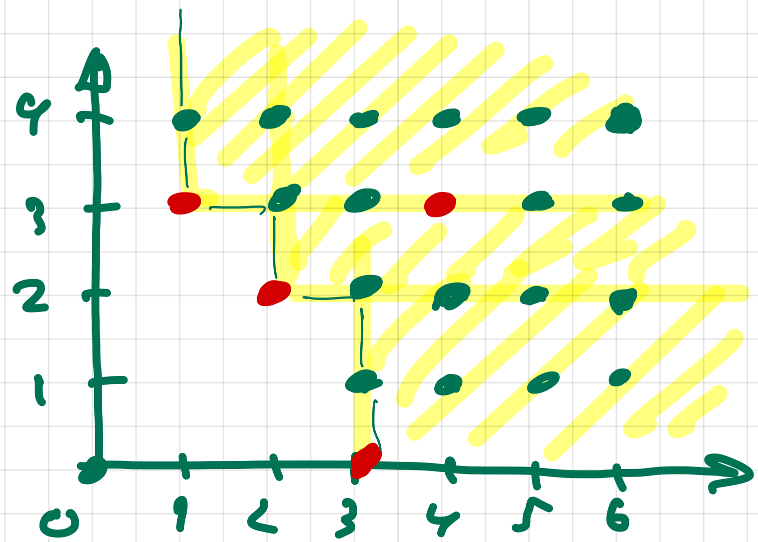
$\square$

2.3.6. Korollar. Wenn für $A, B \subseteq \mathbb{Z}_{\geq 0}^n$ die Gleichung $A + \mathbb{Z}_{\geq 0}^n = B + \mathbb{Z}_{\geq 0}^n$ gilt, dann gilt $\langle x^\alpha : \alpha \in A \rangle = \langle x^\beta : \beta \in B \rangle$.

Beweis: Direkte Konsequenz aus 2.3.5.

2.3.7. Beispiel:

$A = \{(3,0), (2,2), (1,3), (4,3)\}$



$\langle x^\alpha : \alpha \in A \rangle =$

$= \operatorname{lin}_k \{ x^\beta : \beta \in \mathbb{Z}_{\geq 0}^n,$

$\beta \geq (3,0)$ oder $\beta \geq (2,2)$ oder $\beta \geq (1,3) \}$

2.3.8 Theorem (Lemma von Dickson)

Für jedes $A \subseteq \mathbb{Z}_{\geq 0}^n$ existiert eine endliche Teilmenge B von A mit $\langle x^\alpha : \alpha \in A \rangle = \langle x^\beta : \beta \in B \rangle$.

Beweis: Nach Korollar 2.3.6 reicht es eine endliche Teilmenge $B \subseteq A$ mit $A + \mathbb{Z}_{\geq 0}^n = B + \mathbb{Z}_{\geq 0}^n$ zu finden.

„$\supseteq$" gilt wegen $A \supseteq B$. Es bleibt nun $A + \mathbb{Z}_{\geq 0}^n \subseteq B + \mathbb{Z}_{\geq 0}^n$.

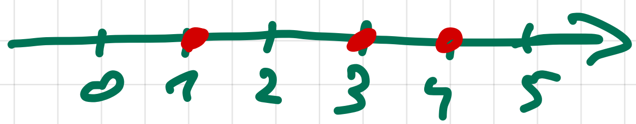
Dafür reicht es ein B zu finden, bei dem für jedes $\alpha \in A$ ein $\beta \in B$ existiert, für das $\alpha \geq \beta$ gilt.

(Mit anderen Worten: $A \subseteq B + \mathbb{Z}_{\geq 0}^n$)

Die Existenz eines endlichen $B \subseteq A$ mit $A \subseteq B + \mathbb{Z}_{\geq 0}^n$ zeigen wir durch Induktion über n.

$n = 1$:

$A = \emptyset \implies B = \emptyset$ passt.



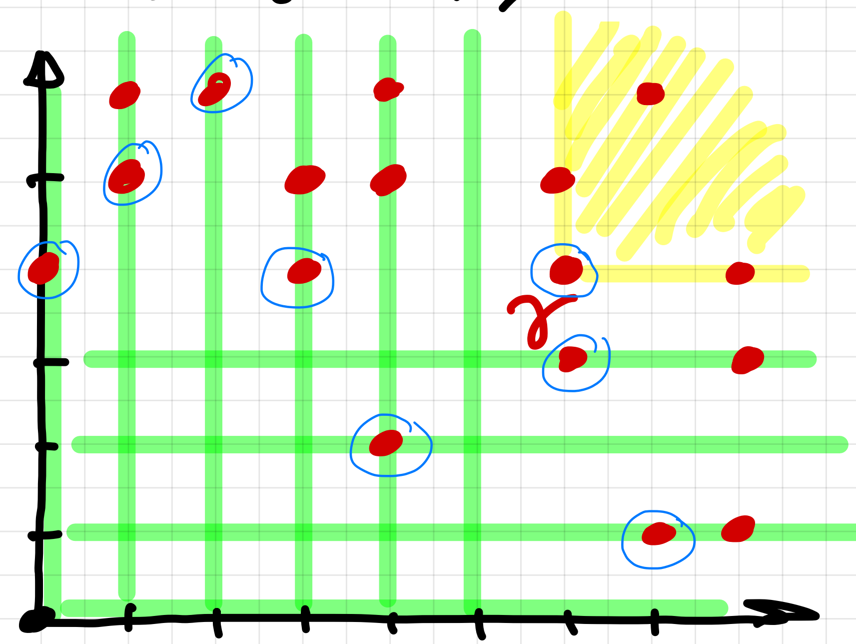
$A \neq \emptyset \implies B = \{\min(A)\}$ ist eine passende Wahl.

Sei $n \geq 2$ und sei die Behauptung für Teilmenge von $\mathbb{Z}_{\geq 0}^{n-1}$ bereits verifiziert. Wir betrachten eine beliebige Teilmenge $A \subseteq \mathbb{Z}_{\geq 0}^{n}$.

$A = \emptyset \implies B = \emptyset$ ist eine passende Wahl.

$A \neq \emptyset \implies$ wir fixieren ein beliebiges $\gamma = (\gamma_1, \dots, \gamma_n) \in A$

Wir nehmen γ in B auf.



Für jedes

$\alpha = (\alpha_1, \dots, \alpha_n) \in A$

mit $\alpha \not\geq \gamma$ gilt

$\alpha_1 \in \{0, \dots, \gamma_1 - 1\}$ oder

$\alpha_2 \in \{0, \dots, \gamma_2 - 1\}$ oder

$\vdots$

$\alpha_n \in \{0, \dots, \gamma_n - 1\}$ (d.h. man hat ein i mit $\alpha_i \leq \gamma_i - 1$)

$$\implies A \subseteq \{\alpha \in \mathbb{Z}_{\geq 0}^{n} : \alpha \geq \gamma\} \cup \bigcup_{i=1}^{n} \bigcup_{m=1}^{\gamma_i - 1} A_{i,m}$$ mit

$$A_{i,m} := \{ \alpha = (\alpha_1, \dots, \alpha_n) \in A : \alpha_i = m \}$$

Bei der Menge $A_{i,m}$ ist die i-te Komponente der Elemente von $A_{i,m}$ fest. Wir können also $A_{i,m}$ mit einer Teilmenge von $\mathbb{Z}_{\geq 0}^{n-1}$ identifizieren, indem man die i-te Komponente weglässt.

Nach der Induktionsvoraussetzung existiert also ein endliches $B_{i,m} \subseteq A_{i,m}$ mit:

$$\forall \alpha \in A_{i,m} \; \exists \beta \in B_{i,m} : \alpha \geq \beta.$$

$\Rightarrow$ Für die Menge A ist

$$\underline{B = \{\gamma\} \cup \bigcup_{i=1}^{n} \bigcup_{m=1}^{\gamma_i - 1} B_{i,m}}$$

eine passende Wahl.

$\square$

2.3.9. Korollar Sei $\prec$ strikte totale Ordnung auf $\mathbb{Z}_{\geq 0}^n$, die für alle $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$ mit $\alpha \prec \beta$ die Bedingung $\alpha + \gamma \prec \beta + \gamma$ erfüllt. Dann sind die folgenden Bedingungen äquivalent:

(i) Jede nichtleere Teilmenge A von $\mathbb{Z}_{\geq 0}^n$ besitzt das kleinste Element bzgl. $\prec$.

(ii) 0 ist das kleinste Element von $\mathbb{Z}_{\geq 0}^n$ bzgl. $\prec$.

Beweis: (i) $\Rightarrow$ (ii): Wäre das kleinste Element γ von $\mathbb{Z}_{\geq 0}^n$ bzgl. $\prec$ ungleich 0, so hätte man

$$\gamma = \gamma + 0 \prec \gamma + \gamma = 2\gamma \Rightarrow$$

$$\gamma \prec 2\gamma \Rightarrow \text{↯ zur Wahl von } \gamma.$$

(ii) $\Rightarrow$ (i): Nach dem Beweis von 2.3.8 existiert ein endliches $B \subseteq A$ mit $\forall \alpha \in A \; \exists \beta \in B : \alpha \succeq \beta$.

$0 \in \mathbb{Z}^n_{\geq 0}$ ist das kleinste Element von $\mathbb{Z}^n_{\geq 0}$ bzgl. $\leq$. Wenn $\alpha \in A$, $\beta \in B$ und $\alpha \geq \beta$ gilt,

so gilt auch $\alpha - \beta \succeq 0$. $\Longrightarrow$

$(\alpha - \beta) + \beta \succeq 0 + \beta \Longrightarrow \alpha \succeq \beta$.

Sei γ das kleinste Element von B bzgl. $\leq$.

Für jedes $\alpha \in A$ gibt es ein $\beta \in B$ mit

$\alpha \geq \beta$. $\Longrightarrow \alpha \succeq \beta \Longrightarrow \alpha \succeq \beta \succeq \gamma$

$\Longrightarrow \alpha \succeq \gamma$.

$\Longrightarrow \gamma \in B \subseteq A$ ist das kleinste Element von A bzgl. $\leq$.

$\square$

2.4. Hilbertscher Basissatz und die Gröbnerbasen.

2.4.1 Def. Sei $I \subseteq k[x_1, \dots, x_n]$ ein Ideal mit $I \neq \{0\}$.

Wir definieren $LT(I) := \{LT(f) : f \in I \setminus \{0\}\}$

und nennen $\langle LT(I) \rangle = \langle LT(f) : f \in I \setminus \{0\} \rangle$
$$= \langle LM(f) : f \in I \setminus \{0\} \rangle$$
das Initial-Ideal von I.

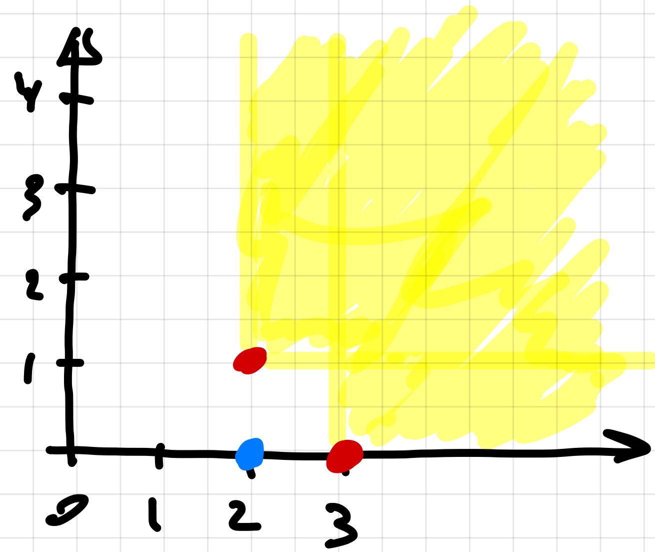
Bem. $\langle LT(I) \rangle$ ist ein Monomideal.

Bem. Im Fall $I = \langle f_1, \dots, f_s \rangle$ gilt im Allgemeinen
$$\langle LT(I) \rangle \neq \langle LT(f_1), \dots, LT(f_s) \rangle.$$

2.4.2. Bsp. $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$

Monomordnung: $\leq_{grlex}$

$$\langle LT(f_1), LT(f_2)\rangle = \langle x^3, x^2y\rangle$$



$$x^2 = -y f_1 + x f_2$$

$$= -y(x^3 - 2xy)$$

$$+ x(x^2y - 2y^2 + x)$$

$\Rightarrow x^2 \in \langle LT(I)\rangle$ mit $I = \langle f_1, f_2\rangle$

aber $x^2 \notin \langle LT(f_1), LT(f_2)\rangle$.

2.4.3. Prop. Für jedes Ideal $I \subseteq k[x_1,\dots,x_n]$ mit $I \neq \{0\}$ gibt es endlich viele Polynome $g_1,\dots,g_s \in I\setminus\{0\}$ mit $\langle LT(I)\rangle = \langle LT(g_1),\dots,LT(g_s)\rangle$.

Beweis: eine direkte Folgerung aus dem Lemma von Dickson. $\square$

2.4.4 Theorem (Hilbertscher Basissatz)

Jedes Ideal $I \subseteq k[x_1, \dots, x_n]$ ist endlich erzeugt, d.h. es existieren endlich viele Polynome $g_1, \dots, g_s \in I$ mit $I = \langle g_1, \dots, g_s \rangle$.