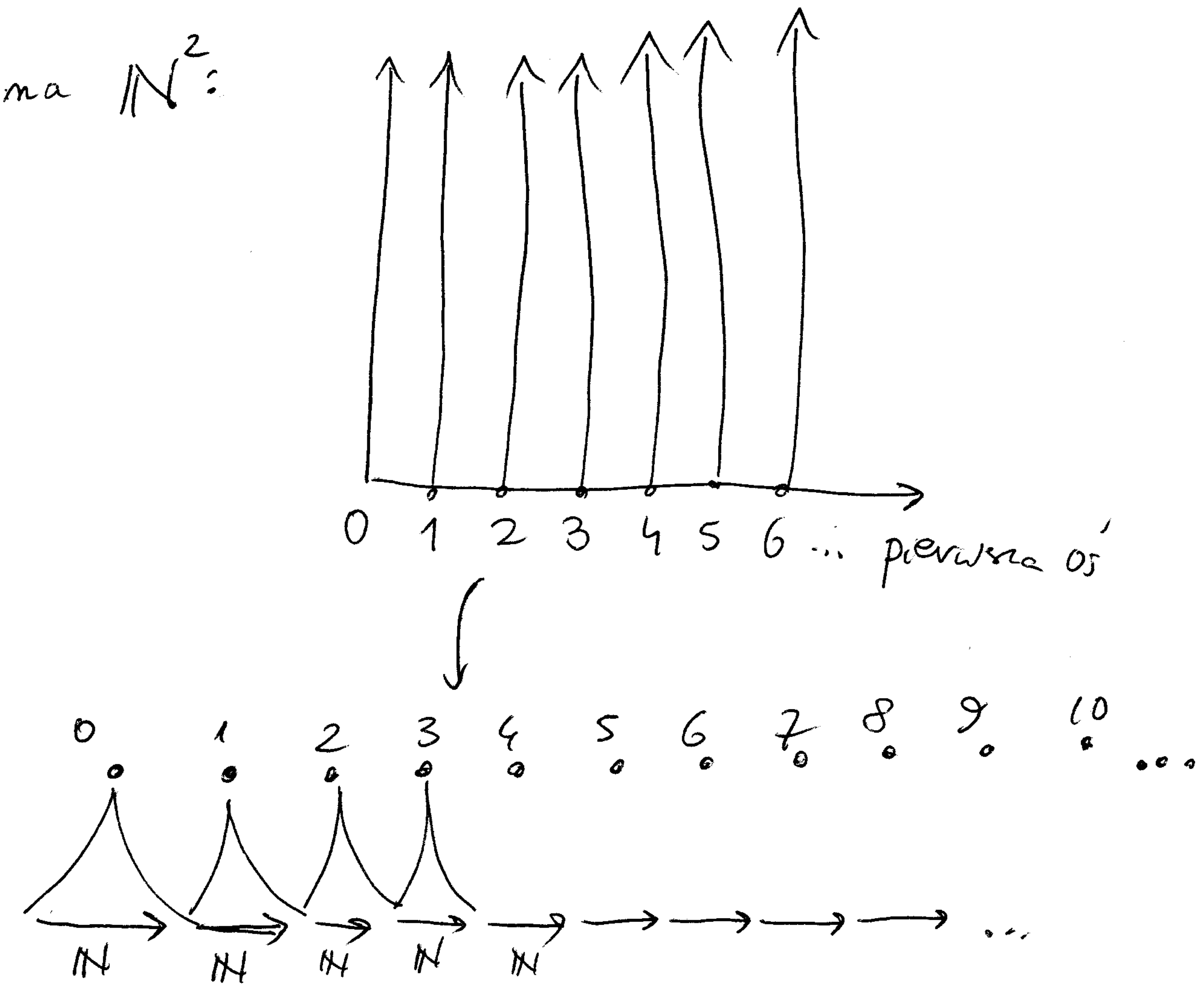
Wykład 13

Przykłady porządków dopuszczalnych na $\mathbb{N}^n$, $\mathbb{T}^n$, np. dla $n=2$

1. leksykograficzny $<_{lex}$

na $\mathbb{N}^2$:



$$ot(\mathbb{N}^2, \leq_{lex}) = \, ?$$

$$ot(\mathbb{N}, \leq) = \omega$$

$$\mathbb{N}^2 \longleftrightarrow \mathbb{T}^2$$

$$\langle n, k\rangle \longrightarrow x_1^n x_2^k$$

$$<_{lex} \longleftrightarrow <_{lex}$$

dlatego:

$$\langle 0,1\rangle <_{lex} \langle 1,0\rangle$$

$$\Updownarrow \qquad \Updownarrow$$

$$x_2 <_{lex} x_1$$

$<_{lex}$ na $\mathbb{T}^2$:

$$\big(\underset{\bar{x}^{\bar{0}}}{\underset{\shortparallel}{1}} < x_2 < x_2^2 < \ldots\big) < \big(x_1 < x_1x_2 < x_1x_2^2 < \ldots\big) <$$

$$< \big(x_1^2 < x_1^2x_2 < x_1^2x_2^2 < \ldots\big) < \ldots$$

2. stopniowo-leksykograficzny $<_{deg\,lex}$ na $\mathbb{T}^n$, $\mathbb{N}^n$

$x^{\bar{\alpha}} <_{deglex} x^{\bar{\beta}} \iff$

$$\Big[\deg x^{\bar{\alpha}} < \deg x^{\bar{\beta}} \vee \big(\deg x^{\bar{\alpha}} = \deg x^{\bar{\beta}} \wedge x^{\bar{\alpha}} <_{lex} x^{\bar{\beta}}\big)\Big]$$

tu: $ot(\mathbb{T}^n, <_{deglex}) = \omega$

Zał, że k: ciało, $f(\bar{x}) \in k[\bar{x}] \setminus \{0\}$. $|\bar{x}| = n$

$<$: porządek dopuszczalny na $\mathbb{T}^n$, $\mathbb{N}^n$.

$f = a_1 x^{\bar{\alpha}_1} + a_2 x^{\bar{\alpha}_2} + \ldots + a_r x^{\bar{\alpha}_r}$,

$\bar{\alpha}_1 > \bar{\alpha}_2 > \ldots > \bar{\alpha}_r$, $a_i \neq 0$ dla $i = 1, \ldots, r$

- $lp(f) = x^{\bar{\alpha}_1}$: jednomian wiodący f
- $lc(f) = a_1$: współczynnik wiodący f
- $lt(f) = a_1 x^{\bar{\alpha}_1}$: wyraz wiodący f

$lp(0) = lc(0) = lt(0) = 0$.

Dzielenie z resztą wg $<$:

Def. 13.4. $f, \overset{0}{\underset{*}{g}}, h \in k[\bar{x}]$.

$f \xrightarrow{g} h$ (f redukuje się do h modulo g w 1 kroku), gdy

$lp(g)$ dzieli pewien niezerowy wyraz v w f

oraz $h = f - \frac{v}{lt(g)} g$

tzn: h : usuwamy z f wyraz v

nie zmieniamy wyrazów v' w f t. że $v' < v$.

Przykład $f = \overbrace{6x^2y}^{v} - x + 4y^3 - 1$, $g = \underbrace{2xy}_{lt(g)} + y^3$

$< = lex$, $y < x$

$v = (3x) \cdot lt(g)$

$h = f - (3x) \cdot g = -3xy^3 - x + 4y^3 - 1$

Def. 13.5. $f, h, f_1, \dots, f_s \in k[\bar{x}]$, $*0*$

$F = \{f_1, \dots, f_s\}$

$f \xrightarrow{F}_+ h$ (f redukuje się do h modulo F), gdy

$\exists t \, \exists h_1, \dots, h_t = h \, \exists 1 \leq i_1, \dots, i_t \leq s$

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \dots \; h_{t-1} \xrightarrow{f_{i_t}} h_t = h$$

Gdy h nie można dalej zredukować, to

$h = r_F(f)$: pełna redukcja f modulo F.

Przykład $<$ = deglex, $y > x$.

$$f_1 = \underbrace{yx}_{lt(f_1)} - x, \quad f_2 = \underbrace{y^2}_{lt(f_2)} - x \in \mathbb{Q}[x, y]$$

$F = \{f_1, f_2\}$, $f = y^2 x$

$$y^2 x \xrightarrow{f_1} y^2 \xrightarrow{f_2} x$$

$$y^2 x - y \cdot f_1 = y^2 \qquad y^2 - 1 \cdot f_2 = x$$

$$y^2 x \xrightarrow{F}_+ x, \quad x = r_F(f).$$

Def. 13.6. Zał, że $I \lhd k[\bar{x}]$.

$G = \{g_1, \dots, g_t\} \subseteq I$: <u>baza Gröbnera</u> ideału I, gdy:

$(\forall f \in I \setminus \{0\}) \, \exists i \in \{1, \dots, t\} \quad lp(g_i) \mid lp(f)$.

Def. 13.7. Dla $S \subseteq k[\bar{x}]$

$$Lt(S) = (\{lt(s) : s \in S\}) \lhd k[\bar{x}]$$

TW. 13.8. Niech $\{0\} \neq I \lhd k[\bar{x}]$, $G = \{g_1, \dots, g_t\} \subseteq I \setminus \{0\}$.

$\circlearrowright$:

(1) G : baza G. dla I

(2) $(\forall f \in k[\bar{x}])(f \in I \iff f \xrightarrow{G}_{+} 0)$

(3) $(\forall f \in k[\bar{x}])\Big(f \in I \iff f = \sum_{i=1}^{t} h_i g_i$ dla pewnych $h_i \in k[\bar{x}]$ t. że $lp(f) = \max_i lp(h_i) lp(g_i)\Big)$

(4) $Lt(G) = Lt(I)$

<u>D-d</u>. (1) $\Rightarrow$ (2) : w (2) $\Rightarrow$: jasne

$\Leftarrow$: $f \xrightarrow{g_i} h \Rightarrow f + I = h + I$.

(4) $\Rightarrow$ (1) :

$f \in I \quad lt(f) \in Lt(G)$

$lt(f) = \sum h_i lt(g_i) \Rightarrow lt(g_i) \mid lt(f)$ dla pewnego i.

$(2) \Rightarrow (3)$, $(3) \Rightarrow (1)$ | Ćwiczenie.
$(1) \Rightarrow (4)$

Wn. 13.9.
Jeśli G: baza G. dla I, to $I = (G)$ i mamy algorytm rozstrzygający dla danego $f \in k[\bar{x}]$, czy $f \in I$.

D-d.: $f \in I \Leftrightarrow f \xrightarrow{G}_+ 0$

(• Zad. $r_G(f)$ jest wyznaczona jednoznacznie?)

Wn. 13.10.
$\forall I \triangleleft k[\bar{x}]\ \exists G$: baza G. dla I.

D-d. Niech $G \underset{sk}{\subseteq} I$ t. że $Lt(G) = Lt(I)$

Niech $I = (f_1, \ldots, f_s) \triangleleft k[\bar{x}]$.
Problem: Jak znaleźć bazę G. dla I?

Def. 13.11. Niech $f, g \in k[\bar{x}] \setminus \{0\}$, $l = \underset{w\ \Pi^n}{NWW}(lp(f), lp(g))$.

$$S(f,g) = \frac{l}{lt(f)} f - \frac{l}{lt(g)} g$$

S-wielomian dla pary f, g
(wielomian syzygii)

<u>Przykład</u>. $<\ = \text{deglex}$, $y > x$

$$f = \underbrace{2yx}_{lp(f)} - y\ , \quad g = \underbrace{3y^2}_{lp(g)} - x$$

$$l = y^2x \qquad S(f,g) = \frac{y^2x}{2yx} f - \frac{y^2x}{3y^2} g = \frac{1}{2} y f - \frac{1}{3} x g =$$

$$= -\frac{1}{2} y^2 + \frac{1}{3} x^2 .$$

(zabija wiodące wyrazy w f i g)

Lemat 13.12. Zał, że $f_1, \dots, f_s \in k[\bar{x}]$, $\bar{0} \neq \bar{\beta} \in \mathbb{N}^n$, $lp(f_i) = x^{\bar{\beta}}$ dla $i = 1, \dots, s$.

Niech $f = \sum_{i=1}^{s} c_i f_i$. $\quad c_i \in k$. Jeśli $lp(f) < x^{\bar{\beta}}$, to

$$f = \sum_{i<j} d_{ij} S(f_i, f_j) \qquad d_{ij} \in k$$

<u>D-d</u>. $lt(f_i) = a_i x^{\bar{\beta}}$, więc $S(f_i, f_j) = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j$

$$NWW(lp(f_i), lp(f_j)) = x^{\bar{\beta}}$$

Współczynnik w f przy $x^{\bar{\beta}}$ = zero, więc $c_1 a_1 + \dots + c_s a_s = 0$.

$$f = c_1 f_1 + \dots + c_s f_s = c_1 a_1 \left(\frac{1}{a_1} f_1\right) + \dots + c_s a_s \left(\frac{1}{a_s} f_s\right) =$$

$$= c_1 a_1 \left(\frac{1}{a_1} f_1 - \frac{1}{a_2} f_2\right) + (c_1 a_1 + c_2 a_2)\left(\frac{1}{a_2} f_2 - \frac{1}{a_3} f_3\right) +$$

$$+ (c_1 a_1 + c_2 a_2 + c_3 a_3)\left(\frac{1}{a_3} f_3 - \frac{1}{a_4} f_4\right) + \dots + (c_1 a_1 + \dots + c_{s-1} a_{s-1})\left(\frac{1}{a_{s-1}} f_{s-1} - \frac{1}{a_s} f_s\right)$$

$$+ \underbrace{(c_1 a_1 + \dots + c_s a_s)}_{0 =} \frac{1}{a_s} f_s$$

Tw. 13.13 (Buchberger, 1964).

Niech $G = \{g_1, \dots, g_t\} \subseteq k[\bar{x}] \setminus \{0\}$. Wtedy:

G: baza G. dla $I = (G) \iff \forall i \neq j \ S(g_i, g_j) \xrightarrow{G}_{+} 0$

D-d. $\Rightarrow$ jasne, bo $S(g_i, g_j) \in I$.

$\Leftarrow$: Warunek (3) w tw. 13.8:

$(\forall f \in k[\bar{x}])(f \in I \iff f = \sum_{i=1}^{t} h_i g_i$ dla pewnych $h_i \in k[\bar{x}]$

t.że $lp(f) = \max_i lp(h_i) lp(g_i))$

$\Rightarrow$: Niech $f \in I \setminus \{0\}$.

(*) $f = h_1 g_1 + \dots + h_s g_s$ dla pewnych $h_i \in k[\bar{x}]$ (ale $lp(h_i g_i)$ mogą być duże)

Niech $x^{\bar{\beta}} = \max_{1 \le i \le s} lp(h_i g_i)$

bso h_i t.że $x^{\bar{\beta}}$: minimalne.

1°. Jeśli $\forall f \in I \setminus \{0\}$ $x^{\bar{\beta}} = lp(f)$, to koniec.

2°. $(\neg 1°)$, tzn. dla pewnego $f \in I \setminus \{0\}$, $lp(f) < x^{\bar{\beta}}$.

Niech $S = \{i \in \{1, \dots, s\} : lp(h_i g_i) = x^{\bar{\beta}}\}$

$\underset{i}{\Psi} \longrightarrow h_i = \underset{k}{\underset{\Uparrow}{c_i}} x^{\bar{\beta}_i} + h_i', \quad lp(h_i') < x^{\bar{\beta}_i}$

Niech $g = \sum_{i \in S} c_i \underbrace{(x^{\bar{\beta}_i} g_i)}_{lp = x^{\beta}}$. $lp(g) < x^{\bar{\beta}}$, bo $lp(f) < x^{\bar{\beta}}$.

Lemat 13.12 ⇝

$$g = \sum_{\substack{i,j\in S \\ i<j}} \underset{\substack{\uparrow \\ k}}{d_{ij}} \underbrace{S(x^{\overline{\beta_i}}g_i, x^{\overline{\beta_j}}g_j)}_{lp < \overline{x}^{\overline{\beta}}}$$

dla $\underset{\substack{\uparrow \\ S}}{i} < \underset{\substack{\uparrow \\ S}}{j}$ $\quad S(x^{\overline{\beta_i}}g_i, x^{\overline{\beta_j}}g_j) =$

$$= \frac{x^{\beta}}{NWW(lp(g_i), lp(g_j))} S(g_i, g_j)$$

<u>więc</u> $S(g_i, g_j) \xrightarrow{G}_{+} 0 \Rightarrow S(x^{\overline{\beta_i}}g_i, x^{\overline{\beta_j}}g_j) \xrightarrow{G}_{+} 0$

Dlatego:

$$\underset{lp < x^{\overline{\beta}}}{S(x^{\overline{\beta_i}}g_i, x^{\overline{\beta_j}}g_j)} = \sum_{1\le \nu \le s} h_{ij\nu} g_\nu$$ dla pewnych $h_{ij\nu} \in k[\overline{x}]$ t. że $lp(h_{ij\nu} g_\nu) < x^{\overline{\beta}}$

Dlatego:

$$f = \sum_{i\in S} h_i g_i + \overbrace{\sum_{i\notin S} \underbrace{h_i g_i}_{lp < x^{\overline{\beta}}}}^{\Sigma_1} = \sum_{i\in S} (c_i x^{\overline{\beta_i}} + h_i') g_i + \Sigma_1 =$$

$$= \underbrace{\sum_{i\in S} c_i x^{\overline{\beta_i}} g_i}_{g} + \underbrace{\sum_{i\in S} \underbrace{h_i' g_i}_{lp < x^{\overline{\beta}}}}_{\Sigma_2} + \Sigma_1 = \sum_{\substack{i,j\in S \\ i<j}} \Big(d_{ij} \sum_{1\le\nu\le s} h_{ij\nu} g_\nu\Big) + \Sigma_1 + \Sigma_2 =$$

$$= \underbrace{\sum_{\nu=1}^{s} \Big(\sum_{\substack{i,j\in S \\ i<j}} d_{ij} h_{ij\nu}\Big) g_\nu}_{lp < x^{\overline{\beta}}} + \Sigma_2 + \Sigma_1 = \sum_{i=1}^{s} q_i g_i, \quad lp(q_i g_i) < x^{\overline{\beta}}$$

↯ z wyborem h_i (minimalności $\overline{\beta}$)

Algorytm Buchbergera. AII, 13 (10)

Dane: $I = (f_1, \ldots, f_s) \lhd k[\bar{x}]$. Cel: baza G. dla I.

Konstruujemy $H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots \subseteq k[\bar{x}]$ (skończone) rekurencyjnie

- $H_0 = \{f_1, \ldots, f_s\}$
- Zał., że H_n dane

  1°. dla pewnych $f \neq g \in H_n$, $h_{f,g} := r_{H_n}(S(f,g)) \neq 0$.

  Wtedy $H_{n+1} := H_n \cup \{h_{f,g}\}$.

  2°. Jeśli $\neg 1°$, to koniec i $G := H_n$.

To działa, bo:

1. Algorytm się zatrzymuje, bo:

   jeśli nie, to dostajemy $H_0 \subsetneq H_1 \subsetneq \ldots$ nieskończony

   Niech $I_n = Lt(H_n) \lhd k[\bar{x}]$. $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$

   $I_n \neq I_{n+1}$, bo:

   niech $h \in H_{n+1} \setminus H_n$, $h = h_{f,g}$, $f \neq g \in H_n$.

   $lt(h) \in I_{n+1}$ oraz $lt(h) \notin I_n$, bo

   jeśli $lt(h) \in I_n$, to h można dalej zredukować modulo H_n.

2. Gdy się zatrzyma, to

   $G = H_n$: baza G. dla I (tw. 13.13).