Gröbner-bázis

Legyen F egy test, $R = F[x_1, x_2, \ldots x_n]$ az F feletti n-határozatlanú polinomok gyűrűje és $f_1, f_2, \ldots f_s \in R$.

Probléma. Közös gyökök keresése.

Jelölje

$$I = \langle f_1, f_2, \ldots f_s \rangle = \left\{ \sum_{1 \le i \le s} q_i f_i \colon q_i \in R \right\}$$

Az adott polinomok az I ideál bázisát alkotják.

Definíció. Az I ideál *varietásán* a

$$V(I) = \{ u \in F^n \colon f(u) = 0 \ \forall f \in I \}$$

Megjegyzés.

$V(I) = \emptyset$?

Adott $f \in R$ esetén $f \in I$?

$I = R$?

A I ideál Gröbner-bázisa egy olyan bázis, ahol könnyű a kérdésekre válaszolni.

$n = 1$ esetben $F[x]$ euklideszi gyűrű, ekkor

$$\langle f_1, f_2, \ldots f_s \rangle = \langle \text{lnko}(f_1, f_2, \ldots f_s) \rangle.$$

Ha $s = 2$ és $f, g \in F[x]$, akkor

$$f = qg + r, \ \deg r < \deg g.$$

Azaz

$$f \in \langle g \rangle \Leftrightarrow r = 0$$

és $V(g) = \{u_1, \ldots u_d\}$, ahol $x - u_i$, $i = 1 \ldots d$ a g polinom lineáris faktorai.

Monomiális rendezés

Definíció. A ‘ $\preceq$ ‘ $\subseteq \mathbf{N}^n$ rendezési relációt *megengedettnek* nevezzük, ha

(i) $(0,\ldots,0) \preceq \nu$ minden $\nu \in \mathbf{N}^n$,

(ii) minden $\nu_1, \nu_2, \nu \in \mathbf{N}^n$ esetén

$$\nu_1 \preceq \nu_2 \Rightarrow \nu_1 + \nu \preceq \nu_2 + \nu.$$

Definíció. A $T = \{x_1^{i_1} \cdots x_n^{i_n}\}$ halmaz elemeit *monomoknak* nevezzük.

Legyenek

$$\alpha = x_1^{i_1} \cdots x_n^{i_n},\ \beta = x_1^{j_1} \cdots x_n^{j_n} \in T.$$

Lexikografikus rendezés.

$\alpha \prec_{lex} \beta \Leftrightarrow$ létezik olyan $l \in 1,\ldots,n$, hogy $i_l < j_l$ és $i_{l+1} = j_{l+1}, \ldots, i_n = j_n$.

Tiszta lexikografikus rendezés.

$\alpha \prec_{plex} \beta \Leftrightarrow$ létezik olyan $l \in 1,\ldots,n$, hogy $i_l < j_l$ és $i_1 = j_1, \ldots, i_{l-1} = j_{l-1}$.

Példa.

Legyen $\prec = \prec_{plex}$ és $z \prec y \prec x$, ekkor

$$1 \prec z \prec z^2 \prec \cdots \prec y \prec yz \prec yz^2 \cdots \prec y^2 \prec y^2z^2$$

$$\prec x \prec xz \prec xz^2 \prec \cdots \ .$$

Legyen

$$f = \sum_{\alpha \in \mathbf{N}^n} c_\alpha x^\alpha \in R$$

egy nem nulla polinom, $c_\alpha \in F$ és $\prec$ egy monomiális rendezés. Ekkor

$$\mathrm{discr}(f) = max\{\alpha \in \mathbf{N}^n \colon c_\alpha \neq 0\}$$

a polinom *multifoka*,

$$\mathrm{lc}(f) = c_{\mathrm{discr}(f)} \in F \setminus \{0\}$$

a polinom *főegyütthatója*,

$$\mathrm{lm}(f) = x^{\mathrm{discr}(f)} \in R$$

a polinom *főmonomomja*, és

$$\mathrm{Lc}(f) = \mathrm{lc}(f) \cdot \mathrm{lm}(f)$$

a polinom *főtagja*.

Ha $f, f_1, f_2, \ldots f_s \in R$ többváltozós polinomok és $\preceq$ egy adott monomiális rendezés ekkor léteznek olyan $q_1, q_2, \ldots, q_s \in R$ polinomok, melyekre

$$f = q_1 f_1 \cdots q_s f_s + r$$

és r egyetelen monomja sem osztható

$$\mathrm{lc}(f_1), \ldots, \mathrm{lc}(f_s)$$

egyikével sem.

(Az r maradék jele $f\mathrm{rem}(f_1, f_2 \ldots, f_s)$)

Definíció. Az $I \subseteq R$ ideált *monomiális ideálnak* nevezzük, ha létezik olyan $A \subseteq \mathbf{N}^n$, melyre

$$I = \langle x^A \rangle = \langle \{x^\alpha \in T\colon \alpha \in A\} \rangle.$$

Lemma. (Dickson) Minden monomiális ideál végesen generálható, vagyis minden $A \subseteq \mathbf{N}^n$ esetén létezik olyan $B \subseteq A$ véges halmaz, melyre $\langle x^A \rangle = \langle x^B \rangle$.

Lemma. Legyen I egy ideál $R = F[x_1, x_2, \dots x_n]$-ben. Ha $G \subseteq I$ egy olyan véges halmaz, melyre $\langle lc(G) \rangle = \langle lc(I) \rangle$, akkor $\langle G \rangle = I$.

Tétel. (Hilbert-féle bázistétel)

Minden $I \subseteq R = F[x_1, x_2, \dots x_n]$ ideál végesen generálható, vagyis létezik olyan $G \subseteq I$ véges halmaz, melyre $\langle G \rangle = I$ és $\langle lc(G) \rangle = \langle lc(I) \rangle$.

Definíció. A tételben szereplő G véges halmazt az I ideál $\prec$ rendezésre vonatkozó *Gröbner-bázisának nevezzük.*

Következmény. Legyen $I_1 \subseteq I_2 \subseteq \ldots$ R-beli ideálok egy növekvő lánca. Ekkor létezik olyan $n \in \mathbf{N}$, melyre $I_n = I_{n+1} = \ldots$.

Definíció. Azokat a gyűrűket, melyekben teljesül az ideál-lánc feltétel *Noether-gyűrűknek* nevezzük.

Megjegyzés. Ha F test, akkor $F[x_1, x_2, \ldots x_n]$ Noether-gyűrű.

Tétel. Legyen G az $I \subseteq R$ ideál $\prec$ monomiális rendezésre vonatkozó Gröbner-bázisa és legyen $f \in R$. Ekkor

$$f \in I \Leftrightarrow f rem G = 0.$$

Buchberger-algoritmus

Definíció. Legyenek $g, h \in R$ nem nulla polinomok

$$\alpha = (\alpha_1, \dots \alpha_n) = \mathsf{discr}(g),$$

$$\beta = (\beta_1, \dots \beta_n) = \mathsf{discr}(h),$$

$$\gamma = (\max\{\alpha_1, \beta_1\}, \dots, \max\{\alpha_n, \beta_n\}).$$

A g és h polinomok *S-polinomján* az

$$S(g,h) = \frac{x^\gamma}{\mathsf{lc}(g)} g - \frac{x^\gamma}{\mathsf{lc}(h)} h \in R$$

polinomot értjük.

Tétel. A $G = \{g_1, g_2, \dots, g_s \subseteq R\}$ halmaz akkor és csak akkor lesz a $\langle G \rangle$ ideál Gröbner-bázisa, ha

$$S(g_i, g_j) rem(g_1, \dots, g_s) = 0 \; \forall \, 1 \leq i \leq j \leq s.$$