ΒΑΣΕΙΣ Grobner (Υπολογιστικής άλγεβρας)

Grobner - Buchberger.

Δακτύλιος (R): μεταθετικός δακτύλιος και έχει μοναδιαίο στοιχείο

$ab = ba \quad \forall a,b \in R$

$\exists 1 \in R$ τ.ω. $a1 = a \quad \forall a \in R$

ΟΡΙΣΜΟΣ: Ένα υποσύνολο I ενός δακτυλίου

• R λέγεται ιδεώδες του R αν 1) $I \neq \emptyset$

2) Για κάθε $a,b \in I \Rightarrow a-b \in I$

3) Για κάθε $a \in I$ και $r \in R \Rightarrow ra \in I$

. Παραδείγματα

Ο δακτύλιος (μεταθετικός με μοναδιαίο στοιχείο)

R ιδεώδες του R

• $\{0\}$ ιδεώδες του R

Έστω $a \in R$ $\langle a \rangle = \{ra / r \in R\} = Ra$ ιδεώδες που παράγεται από το a. Το a είναι γεννήτορας του ιδεώδους αυτού

$\mathbb{Z}$ $2 \in \mathbb{Z}$ $\langle 2 \rangle = \mathbb{Z}2 = \{r \cdot 2 / r \in \mathbb{Z}\}$

οι άρτιοι

$\langle 3 \rangle = \mathbb{Z}3$

$\langle n \rangle = \mathbb{Z}n$ ιδεώδη

$\langle 1 \rangle = \mathbb{Z}$

$R \quad a,b \in R$

$\langle a,b \rangle = \{ r_1 a + r_2 b \ / \ r_1, r_2 \in R \}$

$\langle a,b \rangle$ ιδεώδες

i) $0 = 0 \cdot a + 0 \cdot b \in \langle a,b \rangle$

ii) Έστω

$x,y \in \langle a,b \rangle \Longrightarrow \left. \begin{array}{l} x = r_1 a + r_2 b \\ y = r_1' a + r_2' b \end{array} \right\} \Rightarrow$

$x - y = (r_1 - r_1')a + (r_2 - r_2')b$

iii) Έστω $x \in \langle a,b \rangle$ και $r \in R$ θ.δ.ο $x \cdot r \in \langle a,b \rangle$ ή $rx \in \langle a,b \rangle$

$\Rightarrow x = r_1 a + r_2 b$

$rx = r r_1 a + r r_2 b$

Επομένως $\langle a,b \rangle$ ιδεώδες

a,b ονομάζονται γεννήτορες του $\langle a,b \rangle$

Το ιδεώδες $I = \langle a,b \rangle$ παράγεται από τα a και b

<u>Παράδειγμα</u>: Έστω $a_1, \dots, a_n \in R$

Το σύνολο $\langle a_1, a_2, \dots, a_n \rangle = \{ r_1 a_1 + \dots + r_n a_n \ / \ r_1, \dots, r_n \in R \}$

είναι πάντα ιδεώδες του R.

$a_1, \dots, a_n$ γεννήτορες του I. Το I παράγεται από τα $a_1, \dots, a_n$

... ωνα r σωμα)

Έστω R δακτύλιος και $\Sigma \subseteq R$

$<\Sigma> = \{ r_1\sigma_1 + \dots + r_n\sigma_n \,/\, r_1,\dots,r_n \in R,\ \sigma_1,\dots,\sigma_n \in \Sigma \}$

πεπερασμένα αθροίσματα

$\mathbb{Z}$ $\quad <6,14> = \{ r_1 6 + r_2 14 \,/\, r_1, r_2 \in \mathbb{Z} \} = <2>$

$<a_1,\dots,a_n> = <d>$

αιτο $\quad$ ο ΜΚΔ των $a_1,\dots,a_n$

$K[x]$ το σύνολο των πολυωνύμων με συντελεστές από το σώμα K στην μεταβλητή x.

<u>Παραδείγματα</u>: $\mathbb{R}[x]$ π.χ $f(x) = 3 + 5x - \sqrt{2}x^2 + \sqrt{7}x^4$

$K[x,y]$ <u>π.χ</u> $f(x,y) = 3x^2y^2 - 7xy^3 + 5x$

$\mathbb{R}[x,y]$

<u>Παρατήρηση</u>

$<x^2, y^2>$ δεν είναι κύριο

$<x^n, x^{n-1}y, x^{n-2}y^2, \dots, xy^{n-1}, y^n>$

δεν έχει σύνολο γεννητόρων με λιγότερο από $n+1$ πλήθος στοιχείων.

Τα ιδεώδη του $\mathbb{Q}$ είναι τα: $\underset{<1>}{\mathbb{Q}}, \underset{<0>}{\{0\}}$

<u>Απόδ.</u>

Γενικά τα ιδεώδη του F (όπου F σώμα)

Είναι τα : F, $\{0\}$

$$\underset{\langle 1\rangle}{F} , \quad \underset{\langle 0\rangle}{\{0\}}$$

Έστω I ιδεώδες του F και $I \neq \{0\}$

$I \neq \{0\} \Rightarrow \exists\, a \in I$ τ.ς $a \neq 0 \Rightarrow \exists\, a^{-1} \in F$

$$\underset{\in F}{a^{-1}} \underset{\in I}{a} = 1 \in I \qquad I \subseteq F \text{ προφανώς } (1)$$

Έστω $b \in F \Rightarrow b = \underset{\in F}{b} \cdot \underset{\in I}{1} \in I$ Άρα $F \subseteq I$ (2)

(1) και (2) $\Rightarrow I = F$.

I, J ιδεώδη του R

$I + J = \{a + b \,/\, a \in I,\ b \in J\}$

$I + J$ είναι ιδεώδες ← Θεώρημα

Άθροισμα των I και J.

Απόδ.

i) $0 = \underset{\in I}{0} + \underset{\in J}{0} \Rightarrow 0 \in I + J$

ii) Έστω $x, y \in I + J \Rightarrow x = \underset{\in I}{a_1} + \underset{\in J}{b_1}$, $y = \underset{\in I}{a_2} + \underset{\in J}{b_2}$

$$x - y = \underbrace{a_1 - a_2}_{\in I} + \underbrace{b_1 - b_2}_{\in J} \Rightarrow x - y \in I + J$$

iii) Αν $x \in I + J$ και $r \in R$ τότε Θ.δ.ο

$r \cdot x \in I + J$

$x \in I + J \Rightarrow x = \underset{\in I}{a_1} + \underset{\in J}{b_1} \Rightarrow rx = \underset{\in I}{ra_1} + \underset{\in J}{rb_1}$ Άρα

$IJ = \{a_1b_1 + a_2b_2 + \dots + a_sb_s \mid a_i \in I,\ b_i \in J\}$

<u>Θεώρημα</u> $I\cdot J$ ιδεώδες του R.

<u>Απόδ</u>

i) $0 = \underbrace{0}_{\in I}\underbrace{0}_{\in J} \Rightarrow 0 \in I\cdot J$

ii) Έστω $x, y \in I\cdot J$ Θ.δ.ο $x-y \in I\cdot J$

$\Rightarrow x = a_1b_1 + \dots + a_sb_s \quad a_i, c_i \in I$

$y = c_1d_1 + \dots + c_td_t \quad b_i, d_i \in J$

$x - y = a_1b_1 + \dots + a_sb_s - c_1d_1 - \dots - c_td_t$

Άρα $x - y \in I\cdot J$

iii) Έστω $x \in I\cdot J$ και $r \in R$

Τότε: $a_1b_1 + a_2b_2 + \dots + a_sb_s$

$rx = \underbrace{ra_1}_{\in I}\underbrace{b_1}_{\in J} + ra_2b_2 + \dots + ra_sb_s$

Άρα $rx \in I\cdot J$

Άρα $I\cdot J$ είναι ιδεώδες του R.

• R μεταθετικός δακτύλιος με μονάδα (μοναδιαίου στοιχείου)

I ιδεώδες του $R \overset{\text{ορ}}{\Longleftrightarrow}$ i) $I \neq \emptyset$ $(0 \in I)$
ii) $a, b \in I \Rightarrow a - b \in I$