12/10/2017

Βάσεις Gröbner (Υπολογιστική Άλγεβρα)

R δακτύλιος μεταθετικός και με μοναδιαίο στοιχείο

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

$1 \in R \qquad 1 \cdot a = a \cdot 1 = a \quad \forall a \in R$

$k[x_1, x_2, \dots, x_n]$, k σώμα

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$

o δακτύλιος των πολυωνύμων σε n-μεταβλητές

Μονώνυμο $x_1^{\omega_1} x_2^{\omega_2} \dots x_n^{\omega_n}$, $\omega_i \geq 0$

Όρος λέγεται ένας αριθμός $\neq 0$ από το K πολλαπλασιασμένος με ένα μονώνυμο.

Πολυώνυμο είναι ένα πεπερασμένο άθροισμα από όρους

Ιδεώδες: $I \subset R$ ← μεταθετικός δακτύλιος με μοναδιαίο στοιχείο

(i) $I \neq \emptyset$

(ii) $a, b \in I \to a - b \in I$

(iii) $r \in R$ και $a \in I \Rightarrow ra \in I$

Παραδείγματα:

R μεταθετικός δακτύλιος με μοναδιαίο στοιχείο

$\{0\}$ ιδεώδες

R ιδεώδες

Υπάρχουν άλλο ιδεώδη?

Υπάρχουν όμως υπάρχουν και άλλοι οι οποίοι έχουν μόνο δύο ιδεώδη όπως για παράδειγμα ο δακτύλιος

$\mathbb{Z}_2 = \{[0]_2, [1]_2\}$

Γενικά όμως οι περισσότεροι δακτύλιοι έχουν περισσότερα ιδεώδη.

Για παράδειγμα:

→ R δακτύλιος

$a \in R$ $\quad \langle a \rangle = (a) = Ra = \{ra \mid r \in R\}$

(i) $a \in \langle a \rangle \Rightarrow \langle a \rangle \neq \emptyset$

(ii) $x, y \in \langle a \rangle \Rightarrow x = r_1 a,\ y = r_2 a$

$x - y = r_1 a - r_2 a = \underbrace{(r_1 - r_2)}_{\text{πολλαπλάσιο του } a} a \in \langle a \rangle$

(iii) $z \in R$ και $ra \in \langle a \rangle$

$\Rightarrow zra = \underbrace{(zr)}_{\text{πολλαπλάσιο του } a} \cdot a \in \langle a \rangle$.

→ $\mathbb{Z} = \{-2, -1, 0, 1, 2, \ldots$

$\mathbb{Z}$ αποτελεί και ομάδα και δακτύλιο

(γιατί μπορώ να αθροίσω και να διαιρώ)

Μερικά τα ιδεώδη: $\mathbb{Z} = \langle 1 \rangle$ $\quad \{0\} = \langle 0 \rangle$ $\quad \langle 3 \rangle = 3\mathbb{Z} = \{-6, -3, 0, 3, 6$

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

* πολλαπλάσια του 1 είναι όλος ο δακτύλιος

$R = \langle 1 \rangle$.

→ Έχουμε ένα δακτύλιο R με $a_1, a_2 \in R$

$\langle a_1,a_2\rangle = \{ r_1a_1 + r_2a_2 \mid r_1, r_2 \in R \}$.

(i) $0 = 0a_1 + 0a_2 \in \langle a_1,a_2\rangle$ άρα $\langle a_1,a_2\rangle \neq \emptyset$

(ii) $\left.\begin{array}{l} r_1a_1 + r_2a_2 \in \langle a_1,a_2\rangle \\ s_1a_1 + s_2a_2 \in \langle a_1,a_2\rangle. \end{array}\right\} \Rightarrow r_1a_1+r_2a_2-s_1a_1-s_2a_2 =$

λαμβάνω την διαφορά τους

$=(r_1-s_1)a_1 + (r_2-s_2)a_2$.

(iii) $r \in R$, $r_1a_1+r_2a_2 \in \langle a_1,a_2\rangle$.

$r(r_1a_1+r_2a_2) = rr_1a_1 + rr_2a_2 \in \langle a_1,a_2\rangle$.

Άρα $\langle a_1,a_2\rangle$ ιδεώδες.

→ $K[x_1,x_2]$

ο ίδιος δακτύλιος και το μηδέν είναι ιδεώδες

$f = 3x_1^4 + x_1^3x_2^2 - 7x_1x_2^4 + \sqrt{15}x_2^8$ ← τυχαίο πολυώνυμο.

τα πολλαπλάσια αυτού του πολυωνύμου είναι ιδεώδη

$g = 13x_1^{2017} - 11/2 \cdot x_1^3x_2^5 + \pi \cdot x_1^8 \cdot x_2^{2013}$

$\langle f,g\rangle$

πεπερασμένα

αθροίσματα

→ Αν $S \subseteq R$

$\langle S\rangle = \{ r_1s_1 + r_2s_2 + \dots + r_ks_k \}$. $\left\{\begin{array}{l} s_1, s_2, \dots, s_k \in S. \\ r_1, r_2, \dots, r_k \in R \end{array}\right.$

$k \geq 1$.

$\mathbb{Z}_6 = \{[0]_6, [1]_6, \dots, [5]_6\}$

Βάση του ιδεώδους I λέγεται ένα σύνολο $S \subseteq R$ τέτοιο ώστε $I = \langle S \rangle$

Παρατήρηση:

Κάθε ιδεώδες έχει βάση διότι $I = \langle I \rangle$.

Πρώτα ιδεώδη: Το ιδεώδες P του R λέγεται πρώτο ιδεώδες αν ισχύει:

$$ab \in P \Rightarrow a \in P \text{ ή } b \in P.$$

→ $R/I = \{a + I \mid a \in R\}$.

Δακτύλιος πηλίκο

$$(a+I) + (b+I) = (a+b) + I$$

$$\underbrace{(a+I)(b+I)}_{\text{σύμπλοκα}} = ab + I$$

ΘΕΩΡΗΜΑ:

P πρώτο ιδεώδες αν και μόνο αν R/P είναι ακέραια περιοχή.

ΘΕΩΡΗΜΑ:

M μέγιστο ιδεώδες αν και μόνο αν R/M είναι σώμα

ΠΡΟΤΑΣΗ:

Κάθε μέγιστο ιδεώδες είναι πρώτο

ΑΣΚΗΣΗ: Στον δακτύλιο $\mathbb{Z}[\underbrace{\sqrt{-5}}_{(\sqrt{5}\cdot i)}] = \{a+b\sqrt{-5} \mid a,b\in\mathbb{Z}\} \subset \mathbb{C}$

κληρονομεί όλες τις ιδιότητες του δακτυλίου $\mathbb{C}$

με τα μόνα στοιχεία που μπορώ να διαιρέσω είναι το 1 και το -1.

Δείξτε ότι το ιδεώδες $P_1 = \langle 2, 1+\sqrt{-5} \rangle$ είναι πρώτο.

$$\mathbb{Z}[\sqrt{-5}]/P_1 = \{a+b\sqrt{-5} + P_1 \mid a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]\}$$

$a+b\sqrt{-5} + \langle 2, 1+\sqrt{-5}\rangle$. ← σύμπλοκο.

$= a-b+b+b\sqrt{-5} + \langle 2, 1+\sqrt{-5}\rangle$.

$= \underbrace{a-b + b(1+\sqrt{-5})}_{} + \underbrace{\langle 2, 1+\sqrt{-5}\rangle}_{}$. $= a-b + \langle 2, 1+\sqrt{-5}\rangle = 2k+u+\langle 2, 1+\sqrt{-5}\rangle =$

$= u + \langle 2, 1+\sqrt{-5}\rangle$.

στοιχείο του ιδεώδους + ιδεώδες = ιδεώδες.

$a-b = 2k+u$, $0 \le u < 2$

$0+I$ και $1+I$ } δύο σύμπλοκα

$$\mathbb{Z}[\sqrt{-5}] \xrightarrow{\phi} \mathbb{Z}_2$$

$$\phi(a+b\sqrt{-5}) = a-b \bmod 2.$$

ϕ ομομορφισμός

$\ker\phi \underset{\subset}{\overset{\supset}{=}} \langle 2, 1+\sqrt{-5}\rangle$.

ϕ επί.

$\mathbb{Z}[\sqrt{-5}] / P_1 \simeq \mathbb{Z}_2 \Rightarrow P_1$ μέγιστο $\Rightarrow P_1$ πρώτο

↑ σώμα

R δακτύλιος (μεταθετικός + 1)

I, J ιδεώδη του R.

$I + J = \{a+b \mid a \in I, b \in J\}$ → ιδεώδες.

⊛ Δυο ιδεώδη μπορώ να τα προσθέσω και να τα αθροίσω

$I \cdot J = \{a_1 b_1 + a_2 b_2 + \dots + a_s b_s \mid a_i \in I, b_i \in J, s \geq 1\}$

πεπερασμένα αθροίσματα.

$I^0 = \langle 1 \rangle = R$

$I' = I$, $I^n = I^{n-1} \cdot I$

$I^2 = I \cdot I$

➡ $\sqrt{I} = rad(I) = \{a \mid a^n \in I$ για κάποιο $n\}$

ριζικό

ριζικό του ιδεώδες.

Παράδειγμα:

$\mathbb{Z}$

① $\sqrt{\langle 4 \rangle} = \langle 2 \rangle$

το 2 είναι μέσα στο ιδεώδες γιατί $2^2 = 4$

άρα όλα τα πολλαπλάσια του 2 είναι μέσα

② $\sqrt{\langle 32 \rangle} = \langle 2 \rangle$

το 2 είναι μέσα γιατί $2^5 = 32$

άρα όλα τα πολλαπλάσια του 2 είναι και αυτά μέσα

③ $\sqrt{\langle 400 \rangle} = \langle 10 \rangle$

κύριο ιδεώδες

$a^n \in \langle 400 \rangle$

$400 \mid a^n$

$2 \mid 400 \mid a^n \Rightarrow 2 \mid a^n \Rightarrow 2 \mid a$

$\delta \mid ucc \mid a^n \Rightarrow \delta \mid a^n \Rightarrow \delta \mid a$

Άρα $1 \mid a$

(4) $\sqrt{\langle w \rangle} = \sqrt{p_1^{w_1} \cdot p_2^{w_2} \cdots p_s^{w_s}} = \langle p_1 p_2 \cdots p_s \rangle$

<u>Ανάγωγο στοιχείο</u> ονομάζεται ο αριθμός ο οποίος γράφεται ως γινόμενο της μονάδας με έναν άλλον αριθμό.

(π.χ) $7 = 1 \cdot 7$ το 6 δεν είναι γιατί $2 \cdot 3$.

$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

ανάγωγα ανάγωγο ανάγωγο.

$\langle 2 \rangle \langle 3 \rangle = \langle 6 \rangle = \langle 1 + \sqrt{-5} \rangle \langle 1 - \sqrt{-5} \rangle$.

↳ δεν είναι πρώτα ιδεώδες.

(π.χ) $P_1 = \langle 2, 1 + \sqrt{-5} \rangle$ πρώτο ιδεώδες

$P_2 = \langle 3, 1 + \sqrt{-5} \rangle$ πρώτο ιδεώδες

$P_3 = \langle 3, 1 - \sqrt{-5} \rangle$ πρώτο ιδεώδες.

$P_1 P_1 = \langle 2 \rangle$ $\qquad P_1 P_2 = \langle 1 + \sqrt{-5} \rangle$

$P_2 P_3 = \langle 3 \rangle$ $\qquad P_1 P_3 = \langle 1 - \sqrt{-5} \rangle$

$\langle 2 \rangle \langle 3 \rangle = \langle 6 \rangle = \langle 1 + \sqrt{-5} \rangle \langle 1 - \sqrt{-5} \rangle$

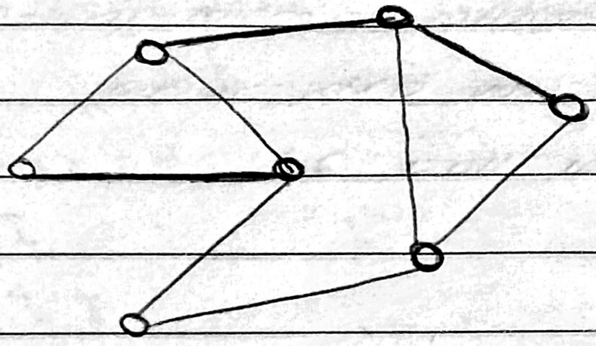
$P_1 P_1 \; P_2 P_3 = \langle 6 \rangle = P_1 P_2 P_1 P_3$

→ $I = \langle f_1, f_2, \ldots, f_s \rangle$ $\quad J = \langle g_1, g_2, \ldots, g_t \rangle$.

$I + J = \langle f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t \rangle$.

$I \cdot J = \langle f_1 g_1, f_1 g_2, \ldots, f_1 g_t, f_2 g_1, f_2 g_2, \ldots, f_2 g_t, f_s g_1, f_s g_2, \ldots, f_s g_t \rangle$

<u>Θεωρία Γραφημάτων:</u> (γράφοι)



χρωματισμός

γραφήματος

<u>Ακέραιος Προγραμματισμός:</u>

$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = d_1$

με ενδιαφέρουν οι ακέραιες λύσεις.