9/11/17

**Ορισμός:** Ένα πολυώνυμο $r$ ονομάζεται ανάγωγο modulo $F$, όπου $F=\{f_1, f_2, \ldots, f_s\}$ αν $r=0$ ή κανένα μονώνυμο του $r$ δεν διαιρείται από κάποιο αρχικό μονώνυμο $lm(f_i)$ για κάθε $1 \le i \le s$.

Παράδειγμα

Έστω ο δακτύλιος $K[x,\psi,z]$ και διάταξη: $>_{lex}$ με $x>\psi>z$.

Έστω $f_1 = x^2\psi + \psi - 3x$

$f_2 = \psi^2 z - z$

$f_3 = z^2 x - x^2 + \psi x - z$

Άρα $F=\{f_1, f_2, f_3\}$

Άρα κάποια πιθανά $r$ είναι τα εξής:

$r_1 = 0$ ✓

$r_2 = x\psi z + 3x^2$ ✓

$r_3 = x^2\psi^2 + x\psi + 7x$ ✗

$r_4 = x\psi z - \psi^2 x + 2\psi^2 z$ ✗

! Το $r_3$ δεν είναι γιατί: $x^2\psi^2 \mid x^2\psi \to f_1$

Το $r_4$ δεν είναι γιατί: $2\psi^2 z \mid \psi^2 z \to f_2$

**Ορισμός:** Αν $f \xrightarrow{F}_{+} r$ και το $r$ είναι ανάγωγο, τότε το $r$ ονομάζεται υπόλοιπο modulo $F$ και η διαδικασία της αναγωγής ονομάζεται διαίρεση.

Παραδείγματα — Ασκήσεις

1) Έστω ο δακτύλιος $\mathbb{Q}[x,\psi,z,w]$ με διάταξη: lex, με $x>\psi>z>w$.

Έστω • $F=\{f_1 = x^3-\psi,\ f_2 = x^4 - z\}$.

• $f = x^5 - w$

Να γίνει η διαίρεση $f \xrightarrow{F}_{+} r$

Λύση

Επιλέγω τυχαία το $f_1$

! Αφού και $Im(f_1)$ και $Im(f_2)$ διαιρούν το $x^5$

Άρα έχω:

$$f \xrightarrow{f_1} x^5 - w - \frac{x^5}{x^3}(x^3-\psi) = -w + x^2\psi \underset{x>\psi>z>w}{\overset{lex}{=}} x^2\psi - w$$

Ανάγωγο μόδιο f

Άρα η διαδικασία ονομάζεται "διαίρεση" με "υπόλοιπο μόδιο f": $x^2\psi - w$

Δ Παρατήρηση: Έστω ότι επέλεγα το $f_2$.

Θα είχα δηλαδή:

$$f \xrightarrow{f_2} x^5 - w - \frac{x^5}{x^4}(x^4 - z) = xz - w$$

ανάγωγο μόδιο f.

Άρα η διαδικασία ονομάζεται "διαίρεση" με "υπόλοιπο μόδιο f": $xz - w$

2) Έστω ο δακτύλιος $Q(x,\psi,z)$ με διάταξη: $>_{lex}$ με $x>\psi>z$

Έστω • $F = \{f_1 = x^3-\psi,\ f_2 = xz-1,\ f_3 = \psi^2 - z\}$

• $f = x^3\psi + 2x^2z + 3x^2 - x\psi^2 + 7$.

Να γίνει η διαίρεση $f \xrightarrow{F}_+ h$.

Λύση

Αρχίζω με το $f_1$

! Εδώ μόνο με το $f_1$ μπορώ να αρχίσω.

Άρα έχω:

$$f \xrightarrow{f_1} x^3\psi + 2x^2z + 3x^2 - x\psi^2 + 7 - \frac{x^3\psi}{x^3}(x^3-\psi) \overset{>_{lex}}{=}$$

$$= 2x^2z + 3x^2 - x\psi^2 + \psi^2 + 7 \xrightarrow{f_2} 2x^2z + 3x^2 - x\psi^2 + \psi^2 + 7 - \frac{2x^2z}{xz}(xz-1) \overset{>_{lex}}{=}$$

$$= 3x^2 - x\psi^2 + 2x + \psi^2 + 7 \xrightarrow{f_3} 3x^2 - x\psi^2 + 2x + \psi^2 + 7 - \frac{-x\psi^2}{\psi^2}(\psi^2 - z) \overset{>_{lex}}{=}$$

$$= 3x^2 + 2x + \psi^2 + 6 \xrightarrow{f_3} 3x^2 + 2x + \psi^2 + 6 - \frac{\psi^2}{\psi^2}(\psi^2 - z) \overset{>_{lex}}{=} 3x^2 + 2x + z + 6$$

Ανάγωγο μόδιο f.

Άρα η διαδικασία ονομάζεται "διαίρεση" με "υπόλοιπο μόδιο f": $3x^2+2x+z+6$

## • Αλγόριθμος Διαίρεσης

**Δ** · Ο αλγόριθμος για διαίρεση $K[x_1, x_2, \ldots, x_n]$ με τυχαία διάταξη: "≤"

• Αν έχω $f$ και $F = \{f_1, f_2, \ldots, f_s\}$ θα καταλήγω σε:

$$\boxed{f = u_1 f_1 + u_2 f_2 + \ldots + u_s f_s + r.}$$

### - Αλγόριθμος "Ψευδοκώδικας"

Είσοδος: $f, f_1, f_2, \ldots, f_s \in K[x_1, \ldots, x_n]$ με $f_i \neq 0$

Έξοδος: $u_1, u_2, \ldots, u_s, r$ τ.ω.: $f = u_1 f_1 + u_2 f_2 + \ldots + u_s f_s + r$.

$\max\{lm(u_1) \cdot lm(f_1), lm(u_2) \cdot lm(f_2), \ldots, lm(u_s) \cdot lm(f_s), lm(r)\} = lm(f)$.

**Αρχή**

$u_1 = 0, u_2 = 0, \ldots, u_s = 0$

$r = 0$

$h = f$.

Όσο $h \neq 0$ επανάλαβε.

Αν υπάρχει $i$ τ.ω.: $lm(f_i) \mid lm(h)$ τότε

διάλεξε το μικρότερο $i$ τ.ω.: $lm(f_i) \mid lm(h)$.

Θέσε $u = u_i + \frac{lt(h)}{lt(f_i)}$.

$h = h - \frac{lt(h)}{lt(f_i)} \cdot f_i$

Αλλιώς

$r = r + lt(h)$

$h = h - lt(h)$

Τέλος

Τέλος

## Παραδείγματα.

1) Έστω ο δακτύλιος $Q(x,\psi,z)$ με διάταξη: [illegible] με $x>\psi>z$.

Έστω
- $F=\{f_1=x^2\psi-z,\ f_2=x\psi^2-1,\ f_3=x\psi z-\psi-2z+1\}$
- $f=x^2\psi^2+2x^2\psi z-x\psi z+\psi^2-z^2+2$.

Να γίνει η διαίρεση $f \xrightarrow{F}_+ r$.

**Λύση**

Θα καταλήξω σε:

$$f=\underbrace{\boxed{\psi+2z}}_{u_1}f_1+\underbrace{\boxed{0}}_{u_2}f_2+\underbrace{\boxed{-1}}_{u_3}f_3+\boxed{\psi^2+\psi z+z^2-\psi-2z+1}$$

**Αρχικά** $h=f$

$u_1=u_2=u_3=r=0$.

**Ξεκινάω** και έχω.

"$\psi$ (πάει στο $u_1$, αφού διαιρώ το $f_1$)"

- $h=\underbrace{x^2\psi^2}_{\text{διάλεξα αυτόν}}+2x^2\psi z-x\psi z+\psi^2-z^2+2-\frac{x^2\psi^2}{x^2\psi}(x^2\psi-z)=$

$=2x^2\psi z-x\psi z+\psi^2+\psi z-z^2+2\neq 0$ (άρα συνεχίζω)

διάλεξα αυτόν $\qquad =2z$ (πάει στο $u_1$)

- $h=2x^2\psi z-x\psi z+\psi^2+\psi z-z^2+2-\frac{2x^2\psi^2 z}{x^2\psi}(x^2\psi-z)=$

$=-x\psi z+\psi^2+\psi z-z^2+2\neq 0$ (άρα συνεχίζω)

διάλεξα αυτόν $\qquad =-1$ (πάει στο $u_3$)

- $h=-x\psi z+\psi^2+\psi z-z^2+2-\frac{-x\psi z}{x\psi z}(x\psi z-\psi-2z+1)=$

$=\psi^2+\psi z+z^2+2-\psi-2z+1 \overset{\text{πράξεις}}{=} \psi^2+\psi z+z^2-\psi-2z+3\neq 0$.

διάλεξα αυτόν

Το $\psi^2$ δεν διαιρείται από τα $\mathrm{lm}(f_i)$ άρα πηγαίνει στο υπόλοιπο. Ομοίως για τα $\psi z$, $z^2$, $-\psi$, $-2z$, $3$.

- Άρα τελικά $h=0$ (είμαι στο τέλος)

Άρα $f=(\psi+2z)f_1-f_3+\psi^2+\psi z-\psi-2z+3$

2) Έστω ο διατύπωση $Q(x)$ ως τυπική διάταξη "<"

Έστω: • $f = x^5 + 2x^4 - x^3 + x + 7$

• $f_1 = x^3 - 2x + 1$

Να γίνει η διαίρεση $f \xrightarrow{f_1} r$.

•

Λύση

Θα καταλήξω σε:

$$f = \underbrace{\boxed{x^2+2x+1}}_{q_1} f_1 + \underbrace{\boxed{3x^2+x+6}}_{r}$$

Αρχικά: $h = f$

$q_1 = r = 0$

Επανάληψη μέχρι ότου:

$x^2$ (πάει στο $q_1$)

• $h = x^5 + 2x^4 - x^3 + x + 7 - \frac{x^5}{x^3}(x^3 - 2x + 1) = 2x^4 - x^3 + x + 7 + 2x^3 - x^2 =$

$\overset{\text{"<"}}{=} 2x^4 + x^3 - x^2 + x + 7 \neq 0$ (άρα συνεχίζω)

επιλέγω αυτόν

$2x$ (πάει στο $q_1$)

• $h = 2x^4 + x^3 - x^2 + x + 7 - \frac{2x^4}{x^3}(x^3 - 2x + 1) = x^3 - x^2 + x + 7 + 4x^2 - 2x =$

$\overset{\text{"<"}}{=} x^3 + 3x^2 - x + 7 \neq 0$ (άρα συνεχίζω)

επιλέγω αυτόν

$1$ (πάει στο $q_1$)

• $h = x^3 + 3x^2 - x + 7 - \frac{x^3}{x^3}(x^3 - 2x + 1) = 3x^2 - x + 7 + 2x - 1 =$

$\overset{\text{"<"}}{=} 3x^2 + x + 6 \neq 0$

επιλέγω αυτόν

Το $3x^2$ δεν διαιρείται από το $lm(f_1) = x^3$ άρα πάει στο υπόλοιπο

Όμοια για τα $x$, $6$

Άρα τελικά $h = 0$ (άρα σταματώ)

Άρα $f = (x^2 + 2x + 1) f_1 + 3x^2 + x + 6$

β) Έστω ο διαμέριση $R(x,\psi,z,w)$ με διάταξη: "λεξ" με $x>\psi>z>w$
Έστω $F=\{f_1=x-\psi+2z-w,\ f_2=\psi+z-w,\ f_3=z+2w\}$
$f=2x+3\psi+4z+5w$
Να γίνει η διαίρεση $f \xrightarrow{F}_+ r$.

Λύση

Θα καταλήξω σε:
$f=\underbrace{\boxed{2}}_{u_1} f_1+\underbrace{\boxed{5}}_{u_2} f_2+\underbrace{\boxed{-5}}_{u_3} f_3+\underbrace{\boxed{22w}}_{r}$

Αρχικά $h=f$
$u_1=u_2=u_3=r=0$

Ξεκινάω και έχω
2 πάει στο $u_1$
• $h=2x+3\psi+4z+5w-\underset{x}{\overset{//}{2x}}(x-\psi+2z-w)=3\psi+4z+5w+2\psi-4z+2w=$

$\overset{\lambda\epsilon\xi}{=}$ $5\psi+7w \neq 0$ (άρα συνεχίζω).
εξετάζω αυτόν
5 πάει στο $u_2$
• $h=5\psi+7w-\underset{\psi}{\overset{//}{5\psi}}(\psi+z-w)=7w-5z+5w=$

$\overset{\lambda\epsilon\xi}{=}$ $-5z+12w\neq 0$ (άρα συνεχίζω)
εξετάζω αυτό.
$-5$
• $h=-5z+12w-\underset{z}{\overset{//}{-5z}}(z+2w)=12w+10w=22w\neq 0$

Το $22w$ δεν διαιρείται από κανένα $\text{lm}(f_i)$ άρα πάει στο υπόλοιπο.
Άρα $h=0$ (άρα σταματάω)
Άρα $f=2f_1+5f_2-5f_3+22w$.

**Ορισμός:** Έστω στον δακτύλιο $K[x_1, x_2, \dots, x_n]$ με μονωνυμική διάταξη, ένα σύνολο μη-μηδενικών πολυωνύμων $G = \{g_1, g_2, \dots, g_t\}$ που περιέχονται σε ένα μη-μηδενικό ιδεώδες λέγεται Βάση Gröbner του $I$, αν για κάθε μη-μηδενικό πολυώνυμο $f \in I$ υπάρχει $i \in \{1, 2, \dots, t\}$ τ.ώ. $lm(g_i) \mid lm(f)$

**Θεώρημα:** Έστω $K[x_1, x_2, \dots, x_n]$ ο πολυωνυμικός δακτύλιος σε $n$ μεταβλητές και "$>$" μια μονωνυμική διάταξη. Έστω $I \neq \{0\}$ και $G = \{g_1, \dots, g_t\} \subset I$, όπου $g_i \neq 0$ με $1 \leq i \leq t$. Το $G$ είναι Βάση Gröbner του $I$ $\underset{i}{\text{αν-ν}}$ ισχύει η πρόταση: $f \in I$ $\underset{ii}{\text{αν-ν}}$ $f \xrightarrow{G}_+ 0$

Απόδειξη

(⚠ Έχω να αποδείξω και το (i) και το (ii) μέσα στην ίδια απόδειξη)

Ξεκινώ από το (i)

($\rightarrow$) $G = \{g_1, g_2, \dots, g_t\}$ είναι Βάση Gröbner του $I$

Θα αποδείξω την (ii)

($\rightarrow$) Έστω $f \in I$ τότε $f \xrightarrow{G}_+ r$, όπου $r$ το υπόλοιπο της διαίρεσης

Έχω τις εξής περιπτώσεις: 1η: $r \neq 0$ $\vee$ 2η: $r = 0$

Άρα $f = u_1 g_1 + u_2 g_2 + \dots + u_t g_t + r \Rightarrow r = f - \underbrace{u_1 g_1}_{\in I} - \underbrace{u_2 g_2}_{\in I} - \dots - \underbrace{u_t g_t}_{\in I} \Rightarrow r \in I$

Εφόσον $G$: Βάση Gröbner $\xRightarrow{\text{υπάρχει}} \exists\, g_i$ τ.ώ. $lm(g_i) \mid lm(r) \Rightarrow$

$\Rightarrow r$ όχι αναγωγο modulo $G$. ΑΤΟΠΟ

Άρα αναγκαστικά $r = 0$.

($\leftarrow$) Έχω ότι $f \xrightarrow{G}_+ 0 \Rightarrow f = u_1 g_1 + u_2 g_2 + \dots + u_t g_t + \overset{r}{\overset{\parallel}{0}} \Rightarrow$

$\Rightarrow f = \underbrace{u_1 g_1}_{\in I} + \underbrace{u_2 g_2}_{\in I} + \dots + \underbrace{u_t g_t}_{\in I} \Rightarrow f \in I$

Τέλος απόδειξης για το (ii)

($\leftarrow$) Έχω ότι $f \in I$ αν-ν $f \xrightarrow{G}_+ 0$ και θέλω $G$: Βάση Gröbner

Έστω $f \neq 0$ και $f \in I$.

Έχω $f \xrightarrow{G}_{+} 0 \Rightarrow f = u_1 g_1 + u_2 g_2 + \dots + u_t g_t + \overset{r}{\overset{\shortparallel}{0}}$

Ισχύει ότι $lm(f) = \max\{lm(u_1) \cdot lm(g_1), lm(u_2) \cdot lm(g_2), \dots, lm(u_t) \cdot lm(g_t)\}$

Άρα $lm(f) = lm(u_i) \cdot lm(g_i) \Rightarrow lm(g_i) \mid lm(f)$.

Άρα $G$: βάση Gröbner