24/12/2020

**Παράδειγμα** Το ιδεώδες $(x^2+1) = \{f\cdot(x^2+1) \mid f \in \mathbb{R}[x]\}$ είναι MAXIMAL ιδεώδες του πολυωνύμικου δακτυλίου $\mathbb{R}[x]$ και τα σώματα $\mathbb{C}$ και $\mathbb{R}[x]/(x^2+1)$ είναι ισόμορφα.

**ΟΡΙΣΜΟΣ**: Έστω $R \neq \{0\}$ μεταθ. δακτύλιος με μονάδα. Τότε ο πολυωνυμικός δακτύλιος $R[x]$ σε μία μεταβλητή επί του $R$ είναι $R[x] = \{a_0+a_1x+a_2x^2+\dots+a_nx^n : n\geq 0, a_i\in R, a_n\neq 0\}\cup\{0\}$

με τις γνωστές πράξεις:

$$\left(\sum_i a_i x^i\right) + \left(\sum_i b_i x^i\right) = \sum_i (a_i+b_i)\cdot x^i$$

$$\left(\sum_i a_i x^i\right)\cdot\left(\sum_i b_i x^i\right) = \sum_j c_j x^j$$

με $c_j = \sum_{i=0}^{j} a_i b_{j-i}$

Συμβολίζουμε για $f\in R[x]\setminus\{0\}$ με $\deg(f)$ τον βαθμό του $f$. Δηλαδή αν $f = a_0+a_1x+a_2x^2+\dots+a_nx^n$, με $a_i\in R$ και $a_n\neq 0$, τότε $\deg(f)=n$.

**Παράδειγμα** Αν $f = 3+5x^5+7x^7 \in \mathbb{Q}[x]$, $\deg(f)=7$.

**Πρόταση** Έστω $R$ ακέραια περιοχή. Τότε ο πολυωνυμικός δακτύλιος $R[x]$ είναι ακέραια περιοχή, και επιπλέον, για $f,g\in R[x]\setminus\{0\}$ ισχύει $\deg(f\cdot g) = \deg(f)+\deg(g)$.

Επιπλέον, ταυτίζοντας το $R$ με τα σταθερά πολυώνυμα έχουμε ότι το $f\in R[x]$ είναι αντιστρέψιμο στο $R[x]$ (δηλ. υπάρχει $g\in R[x]$ με $f\cdot g =$ σταθερό πολυώνυμο με τιμή 1) αν και μόνο αν $f\in R$ και $f$ αντιστρ. στο $R$.

ΑΠΟΔΕΙΞΗ Έστω $f = a_0 + a_1x + \dots + a_nx^n$, με $a_n, b_m \neq 0$
$g = b_0 + b_1x + \dots + b_mx^m$ και $a_i, b_j \in R$

Τότε $f \cdot g = a_nb_mx^{m+n} +$ μικρότερου όρου.
Αφού $R$ ακέραια περιοχή και $a_n, b_m \in R \setminus \{0\}$ έπεται $a_nb_m \neq 0$ στο $R$. Συνεπώς, $f \cdot g \neq 0$ και $\deg(fg) = n+m = \deg f + \deg g$

Έστω $r \in R$ αντιστρέψιμο. Τότε υπάρχει $s \in R$ με $r \cdot s = 1_R$. Άρα, αφού $R \subset R[x]$ υποδακτύλιος, έχουμε $r \in R[x]$ αντιστρ. με αντίστροφο το $s \in R[x]$.
Έστω τώρα $f \in R[x]$ αντιστρ. στο $R[x]$. Άρα υπάρχει $g \in R[x]$ με $f \cdot g = 1$. Άρα $\deg(fg) = \deg 1 \Rightarrow$
$\deg f + \deg g = 0$. (*)
Αλλά, για $f, g \in R[x] \setminus \{0\}$ $\deg(f) \geq 0$, $\deg(g) \geq 0$.
Από (*) $\Rightarrow \deg(f) = \deg(g) = 0$. Συνεπώς $f, g \in R$
Άρα $f \cdot g = 1_R \Rightarrow f$ αντιστρέψιμο στο $R$.

Παραδ. 1 Τα αντιστρέψιμα στοιχεία του $\mathbb{Z}$ είναι τα $-1$ και $1$. Άρα τα αντιστρέψιμα στοιχεία του πολυωνυμικού δακτυλίου $\mathbb{Z}[x]$ είναι τα σταθερά πολυώνυμα $-1$ και $1$.

Συμβολισμός Αν $\mathbb{F}$ σώμα, θέτουμε $\mathbb{F}^* = \mathbb{F} \setminus \{0_{\mathbb{F}}\}$

Παραδ. 2 Έστω $\mathbb{F}$ σώμα. Τότε τα αντιστρέψιμα στοιχεία του $\mathbb{F}$ είναι το σύνολο $\mathbb{F}^*$. Άρα, από πρόταση, τα αντιστρ. στοιχεία του πολυων. δακτυλίου $\mathbb{F}[x]$ είναι ακριβώς τα μηδενικά σταθερά πολυώνυμα (δηλ. το $\mathbb{F}^* \subseteq \mathbb{F}[x]$)

Πρόταση Έστω $\mathbb{F}$ σώμα, $f, g \in \mathbb{F}[x]$ με $g \neq 0$
(δηλ. $g$ όχι το μηδενικό πολυώνυμο)
Τότε υπάρχουν (μοναδικά) $h, r \in \mathbb{F}[x]$ ώστε
$f = h \cdot g + r$ και $r = 0$ ή ($r \neq 0$ και $\deg r < \deg g$)

Απόδειξη
Μοναδικότητα Έστω $f = hg + r = h'g + r'$
(με $r, r'$ όπως παραπάνω)

και $r \neq r'$. Τότε, $hg + r = h'g + r' \Rightarrow$

$r - r' = (h' - h)g$.

Αφού $r \neq r'$ $\deg(r - r')$ ορίζεται

και $\deg(r - r') = \deg(h - h') + \deg g$ (*)

Αλλά $\begin{cases} r = 0 \\ \deg r < \deg(g) \end{cases}$ και $\begin{cases} r = 0 \\ \deg r' < \deg g \end{cases} \Rightarrow$

$\deg(r - r') < \deg(g)$, αντίφαση από την (*)

Άρα, $r = r' \Rightarrow hg = h'g \Rightarrow (h - h')g = 0 \overset{g \neq 0}{\Rightarrow} h = h'$.

Υπαρξη Αλγόριθμος εύρεσης $h, r$. Θέτουμε $n = \deg g$,

άρα $g = a_0 + a_1 x + \ldots + a_n x^n$, με $a_n \in F^*$

Βήμα 1 Αν $f = 0_{F[x]}$ ή $(f \neq 0_{F[x]}$ και $\deg f < n$

Θέτουμε $h = 0_{F[x]}$ και $r = f$. Ισχύει η (*)

Βήμα 2 Έστω τώρα $f \neq 0$ και $\deg(f) = m \geq n$.

Τότε $f = b_0 + b_1 x + \ldots + b_m x^m$, με $b_m \neq 0$

Θέτουμε $f_1 = f - (b_m \cdot a_n^{-1}) x^{m-n} \cdot g$

Άρα "διαγράψαμε" το μεγαλύτερο όρο του $f$, δηλ. $(f_1 = 0$ ή $(f_1 \neq 0$ και $\deg f_1 < \deg f)$

Επιχειρούμε στο Βήμα 1, για το $f_1$ (αντί του $f$)

Η διαδικασία τελειώνει γιατί σε κάθε βήμα πέφτει ο βαθμός

Παράδειγμα $F = \mathbb{R}$, $f = x^5$, $g = x^2 + x + 1$

$$\begin{array}{r|l} x^5 & x^2+x+1 \\ \hline -x^5 - x^4 - x^3 & x^3 - x^2 + 1 \\ \hline -x^4 - x^3 & \\ \hline x^4 + x^3 + x^2 & \\ \hline x^2 & \\ \hline -x^2 - x + 1 & \\ \hline -x - 1 & \end{array}$$

άρα $h = x^3 - x^2 + 1$

$r = -x - 1$.

**Ορισμός:** Έστω $\mathbb{F}$ σώμα, και $f,g \in \mathbb{F}[x]$. Λέμε ότι το $h \in \mathbb{F}[x]$ είναι ένας ΜΚΔ των $f$ και $g$ αν:

1) $h|f$ στο $\mathbb{F}[x]$ (δηλ. υπάρχει $s_1 \in \mathbb{F}[x]$ με $f = hs_1$ και $h|g$ στο $\mathbb{F}[x]$)

2) Αν $p \in \mathbb{F}[x]$ και $p|f$ και $p|g$ στο $\mathbb{F}[x]$ τότε $p|h$.

**Πρόταση:** Έστω $f,g \in \mathbb{F}[x]$ με $(f,g) \neq (0,0)$ και $h,h'$ δύο ΜΚΔ των $f,g$. Τότε υπάρχει $\lambda \in \mathbb{F}^*$ με $h' = \lambda h$.

Αντιστρόφως, αν $h$ ένας ΜΚΔ των $f,g$ και $\lambda \in \mathbb{F}^*$, τότε ο $\lambda h$ είναι ένας ΜΚΔ των $f,g$.

**ΑΠΟΔΕΙΞΗ** Από τον ορισμό, έχουμε $h|h'$ στο $\mathbb{F}[x]$ και $h'|h$ στο $\mathbb{F}[x]$.

Αφού $f \neq 0$ ή $g \neq 0 \Rightarrow h \neq 0$ και $h' \neq 0$

Συνεπώς, υπάρχουν $r_1, r_2 \in \mathbb{F}[x]$ με $\left.\begin{matrix} h' = r_1 h \\ h = r_2 h' \end{matrix}\right\} \Rightarrow$

$h = r_2 r_1 h \Rightarrow (1 - r_1 r_2)h = 0$ στο $\mathbb{F}[x] \Rightarrow$

$1 - r_1 r_2 = 0 \Rightarrow r_1, r_2$ αντίστρ. στο $\mathbb{F}[x]$

$\mathbb{F}[x]$: ακέραια περιοχή

$\overset{\text{ΠΡΟΤΑΣΗ}}{\Rightarrow} r_1, r_2 \in \mathbb{F}^*$ $h \neq 0$ θέτουμε $\lambda = r_1$.

Από τους ορισμούς έπεται εύκολα ότι αν $h$ ένας ΜΚΔ των $f,g$ και $\lambda \in \mathbb{F}^*$, τότε ο $\lambda h$ είναι ένας ΜΚΔ των $f,g$ γιατί το $\lambda h$ και το $h$ διαιρούνται και διαιρούν από το ίδιο πολυώνυμο.

## ΑΛΓΟΡΙΘΜΟΣ ΥΠΟΛΟΓΙΣΜΟΥ ΜΚΔ

Έστω $\mathbb{F}$ σώμα, $f,g \in \mathbb{F}[x]$ με $g \neq 0$.

**Βήμα 1** Ευκλείδια διαίρεση $f$ με $g$: $f = h_1 g + r_1$ και $(r_1 = 0)$ ή $r_1 \neq 0$ και $\deg r_1 < \deg g$

Αν $r_1 = 0$, τότε $g|f$ και $g$ ένας ΜΚΔ των $f,g$

**Βήμα 2** Ευκλ. διαίρεση $g$ με $r_1$

Υποθ. $r_1 \neq 0$. Άρα $g = h_2 r_1 + r_2$ με ($r_2 = 0$) ή ($r_2 \neq 0$ και $\deg r_2 < \deg r_1$). Αν $r_2 = 0$, τότε $r_1$ ένας ΜΚΔ των $(f,g)$

Αν όχι Ευκλ. Διαίρεση $r_1$ με $r_2$ κλπ.

Ο αλγόριθμος τελειώνει γιατί

$\deg g > \deg r_1 > \deg r_2 > \dots \geq 0$

**Πόρισμα** Έστω $f, g \in \mathbb{F}[X]$ με $(f,g) \neq (0,0)$. Τότε υπάρχει $h$ ένας ΜΚΔ των $f, g$. Επιπλέον, ο Ευκλ. Αλγόριθμος τον υπολογίζει και επίσης υπολογίζει $z_1, z_2 \in \mathbb{F}[X]$ με $h = z_1 f + z_2 g$.

**Υπενθύμιση** 1) Έστω $n \in \mathbb{Z}$ με $n \geq 0$. Τότε $\mathbb{Z} \cdot n = (n) =$ πολλαπλάσια του $n$ ιδεώδες του $\mathbb{Z}$.

2) Κάθε ιδεώδες $I$ του $\mathbb{Z}$ είναι αυτού της μορφής δηλ. υπάρχει $n \in \mathbb{Z}$ με $n \geq 0$ και $I = (n)$.

3) Αν $n, m \in \mathbb{Z}$ με $n \geq 0$, $m \geq 0$ τότε $(n) = (m)$ αν και μόνο αν $n = m$.

Δηλαδή, δύο διαφορετικοί μη αρνητικοί ακέραιοι παράγουν διαφορετικά ιδεώδη.

Με άλλα λόγια η απεικόνιση

$$\Phi : \{ n \in \mathbb{Z}, n \geq 0 \} \longrightarrow \text{ΙΔΕΩΔΗ ΤΟΥ } \mathbb{Z}$$

με $\Phi(n) = (n)$ είναι 1-1 και επί.

Επιπλέον, $\Phi(n)$ ΠΡΩΤΟ ιδεώδες (για $n \geq 0$) αν και μόνο αν $n = 0$ ή $n$ πρώτος και $\Phi(n)$ ΜΑΧΙΜΑΛ ιδεώδες αν και μόνο αν $n$ πρώτος.

Έστω $I$ ιδεώδες του $\mathbb{Z}$. Αν $I = \{0\}$, $\Phi^{-1}(I) = 0$. Αν $I \neq \{0\}$.

$\Phi^{-1}(I) =$ ΜΚΔ όλων των στοιχείων του $I$

$=$ ο ελάχιστος θετικός ακέραιος που περιέχεται στο $I$

**ΠΡΟΤΑΣΗ** Έστω $\mathbb{F}$ σώμα, και $I$ ιδεώδες του πολυωνυμικού δακτυλίου $\mathbb{F}[X]$. Τότε υπάρχει $h \in \mathbb{F}[X]$ με $I = (h)$.
(δηλ. $I = \{f \cdot h \mid f \in \mathbb{F}[X]\}$)

**ΑΠΟΔΕΙΞΗ** Αν $I = \{0\}$ θέτουμε $h = 0$.
Υποθ. $I \neq \{0\}$. Το σύνολο $\{\deg(g) : g \in I, g \neq 0\}$ είναι μη κενό φραγμένο κάτω (από το $-1$) υποσύνολο του $\mathbb{Z}$.
Άρα, έχει ελάχιστο στοιχείο έστω $n_0 \in \mathbb{Z}_+$, $n_0 \geq 1$.
Έστω $h \in I$ με $\deg(h) = n_0$.

**ΙΣΧΥΡΙΣΜΟΣ** $I = (h)$ → σημαίνει υποσύνολο ή ίσο.

**ΑΠΟΔΕΙΞΗ** Αφού $h \in I \Rightarrow (h) \subset I$ (1)
Αντιστροφα, έστω $f \in I$ από Ευκλείδια Διαίρεση υπάρχουν $q, r \in \mathbb{F}[X]$ ώστε $f = qh + r$ και ($r = 0$) ή ($r \neq 0$ και $\deg r < \deg h$)
Αν $r \neq 0$, τότε $r = f - gh \in I$, $r \neq 0$ και $\deg r < \deg h$ αντίφαση. Άρα $r = 0$ και $f = gh \Rightarrow f \in (h) \Rightarrow I \subset (h)$ (2)
Από (1) και (2) έχουμε $I = (h)$

**ΠΑΡΑΤΗΡΗΣΗ** ΠΡΟΣΟΧΗ! Στο πολυωνυμικό δακτύλιο $\mathbb{Z}[X]$ το ιδεώδες $(2, x)$ ΔΕΝ είναι κύριο, δηλ. δεν παράγεται από ένα στοιχείο. Επιπλέον, στον Πολ. Δακτ. $\mathbb{F}[x, y]$ δύο μεταβλ. επί ενός σώματος $\mathbb{F}$, το ιδεώδες $(x, y)$ ΔΕΝ είναι κύριο.

---

**ΠΡΟΤΑΣΗ** Έστω $\mathbb{F}$ σώμα $h_1, h_2 \in \mathbb{F}[X]$. Τότε $(h_1) = (h_2)$ αν και μόνο αν υπάρχει $\lambda \in \mathbb{F}^*$ με $h_2 = \lambda h_1$.

**ΑΠΟΔΕΙΞΗ** $(h_1) = (h_2)$ φανερά είναι ισοδύναμο με $h_1 \in (h_2)$ και $h_2 \in (h_1)$ δηλ. με $h_1 \mid h_2$ και $h_2 \mid h_1$ και βλέπε προηγούμενη απόδειξη.

**Ορισμός**: Έστω $R$ ακέραια περιοχή και $f \in R[x]$.
Το $f$ λέγεται ΜΟΝΙΚΟ αν $f \neq 0$ και $f = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$. (δηλ. ο μεγιστοβάθμιος συντελεστής

είναι $1_R$)

ΠΑΡΑΔΕΙΓΜΑ Στο $R[x]$ τα πολυώνυμα $1$, $x^3+3x+5$, $x^3-8$ είναι μονικά, ενώ το $2x^2+4x+2020$ δεν είναι μονικό.

Παρατήρηση Έστω $F$ σώμα, $0 \neq h \in F[x]$. Τότε υπάρχει μοναδικό $\lambda \in F^*$ ώστε $\lambda h$ ΜΟΝΙΚΟ πράγματι, έστω $h = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ με $a_n \in F \setminus \{0\}$. Φανερά $\lambda h$ ΜΟΝΙΚΟ αν και μόνο αν $\lambda = (a_n)^{-1}$.

Πόρισμα Έστω $F$ σώμα, $A_1$ το σύνολο των μονικών πολυωνύμων στο $F[x]$ και $A = A_1 \cup \{0\}$. Τότε η απεικόνιση $\Phi : A \to$ ΙΔΕΩΔΗ του $F[x]$ με $\Phi(f) = (f)$ είναι 1-1 και επί.

ΑΠΟΔΕΙΞΗ (επί) Έστω $I \neq \{0\}$ ιδεώδες του $F[x]$. Από Πρόταση υπάρχει $0 \neq h \in F[x]$ με $I = (h)$ και από παρατήρηση υπάρχει $\lambda \in F^*$ ώστε $\lambda h$ μονικό. Άρα, θέτοντας $f = \lambda h$ έχουμε $f$ ΜΟΝΙΚΟ και $\Phi(f) = I$.

1-1 Έστω $f \in A_1$. Τότε $f \neq 0$ και $f \in \Phi(f) \Rightarrow \Phi(f) \neq \Phi(0)$. Έστω $f_1, f_2 \in A_1$ με $\Phi(f_1) = \Phi(f_2)$. Συνεπώς, $(f_1) = (f_2) \overset{\text{ΠΡΟΤΑΣΗ}}{\Longrightarrow}$ υπάρχει $\lambda \in F^*$ με $f_2 = \lambda f_1$. Αφού $f_1, f_2$ ΜΟΝΙΚΑ $\Rightarrow \lambda = 1 \Rightarrow f_1 = f_2$. Συνεπώς $\Phi$ 1-1.