Λήμμα του Gauss και κριτήριο του Eisenstein

Π. Καραζέρης

10 Ιουνίου 2015

1 Λήμμα. *Κάθε $f(x) \in \mathbb{Q}[x]$ (πολυώνυμο με ρητούς συντελεστές) μπορεί να γραφεί στη μορφή*

$$f(x) = \frac{u}{m}(a_0 + a_1x + ... + a_nx^n)$$

όπου $u,\ m,\ a_0, ..., a_n\ \in \mathbb{Z}$, $\mu\kappa\delta(a_0, ..., a_n) = 1$, $\mu\kappa\delta(u, m) = 1$.

Απόδειξη: Αν $f(x) = q_0 + q_1x + ... + q_nx^n$, με $q_i = \frac{b_i}{c_i}$, $b_i,\ c_i \in \mathbb{Z}$, $c_i \neq 0$, τότε προφανώς το πολυώνυμο μπορεί να γραφεί ως

$$f(x) = \frac{1}{c_0c_1...c_n}(u_0 + u_1x + ... + u_nx^n)$$

με τους $u_0, ..., u_n$ ακέραιους. Θέτοντας $w = \mu\kappa\delta(u_0, ..., u_n)$, τότε είναι $u_i = wa_i$, $i = 0, ..., n$, όπου $\mu\kappa\delta(a_0, ..., a_n) = 1$. Αρα

$$f(x) = \frac{w}{c_0c_1...c_n}(a_0 + a_1x + ... + a_nx^n)$$

Διαιρώντας αριθμητή και παρονομαστή με το μέγιστο κοινό διαιρέτη των w και $c_0c_1...c_n$ προκύπτει το ζητούμενο. ∎

2 Λήμμα. *Αν A είναι ένας αντιμεταθετικός δακτύλιος, I είναι ένα ιδεώδες του, τότε το σύνολο $I[x]$ των πολυωνύμων με συντελεστές στο ιδεώδες I είναι ένα ιδεώδες του $A[x]$ και*

$$\frac{A[x]}{I[x]} \ \cong\ (\frac{A}{I})[x]$$

Απόδειξη: Ο ισχυρισμός ότι το $I[x]$ είναι ιδελωδες του πολυωνυμικού δακτύλιου είναι προφανής, αφού αθροίσματα συντελεστών στο I και γινόμενα συντελεστών στο I με συντελεστές στον A παραμένουν στοιχεία του I.

Δεδομένου του κανονικού ομομορφισμού $\varepsilon\colon A \to A/I$, ορίζουμε

$$\varphi\colon A[x] \to (\frac{A}{I})[x]$$

με

$$\varphi(a_0 + a_1 + ... + a_n x^n) = \varepsilon(a_0) + \varepsilon(a_1) + ... + \varepsilon(a_n)x^n$$

Εύκολα διαπιστώνουμε ότι είναι ομομορφισμός. Πχ, διατηρεί τον πολλαπλασιασμό γιατί

$$\begin{aligned}
\varphi(\sum_{i=0}^{m} a_i x^i \cdot \sum_{j=0}^{n} b_j x^j) &= \varphi(\sum_{k=0}^{m+n}(\sum_{i=0}^{k} a_i b_{k-i})x^k) \\
&= \sum_{k=0}^{m+n} \varepsilon(\sum_{i=0}^{k} a_i b_{k-i})x^k \\
&= \sum_{k=0}^{m+n}(\sum_{i=0}^{k} \varepsilon(a_i)\varepsilon(b_{k-i}))x^k \\
&= \sum_{i=0}^{m} \varepsilon(a_i)x^i \cdot \sum_{j=0}^{n} \varepsilon(b_j)x^j \\
&= \varphi(\sum_{i=0}^{m} a_i x^i) \cdot \varphi(\sum_{j=0}^{n} b_j x^j)
\end{aligned}$$

Επίσης προφανώς, ο ομομορφισμός αυτός είναι επί. Ο πυρήνας του αποτελείται από εκείνα τα πολυώνυμα για τα οποία

$$0 = \varphi(a_0 + a_1 + ... + a_n x^n) = \varepsilon(a_0) + \varepsilon(a_1) + ... + \varepsilon(a_n)x^n$$

στον $(A/I)[x]$, δηλαδή για τα οποία είναι $\varepsilon(a_i) = [a_i]_I = [0]_I$, ή αλλιώς $a_i \in I$, για $i = 0, ..., n$. Επομένως έχουμε $\ker\varphi = I[x]$, οπότε το $I[x]$ είναι ιδεώδες και, από το πρώτο θεώρημα ισομορφισμού

$$\frac{A[x]}{I[x]} \cong \frac{A[x]}{\ker\varphi} \cong \mathrm{Im}\varphi \cong (\frac{A}{I})[x]$$

∎

3 Πρόταση. *(Λήμμα του Gauss) Αν $f(x) \in \mathbb{Z}[x]$ είναι ένα μονικό πολυώνυμο και $f(x) = a(x) \cdot b(x)$ με $a(x)$, $b(x)$ στο $\mathbb{Q}[x]$, τότε $f(x) = \bar{a}(x) \cdot \bar{b}(x)$, όπου $\bar{a}(x)$, $\bar{b}(x) \in \mathbb{Z}[x]$ είναι μονικά πολυώνυμα (με ακέραιους συντελεστές) και $deg(a(x)) = deg(\bar{a}(x))$, $deg(b(x)) = deg(\bar{b}(x))$*

Απόδειξη: Θεωρούμε τα $a(x), b(x)$, στη μορφή που μας επιτρέπει το Λήμμα 1

$$a(x) = \frac{u_1}{m_1}(a_0 + a_1 x + ... + a_m x^m) = \frac{u_1}{m_1}A(x) \qquad b(x) = \frac{u_2}{m_2}(b_0 + b_1 x + ... + b_n x^n) = \frac{u_2}{m_2}B(x)$$

Εχουμε λοιπόν $f(x) = \frac{u_1u_2}{m_1m_2}A(x)B(x) = \frac{v}{w}A(x)B(x)$, με $\mu\kappa\delta(v,w) = 1$ (απλοποιώντας το κλάσμα $\frac{u_1u_2}{m_1m_2}$), ή $wf(x) = vA(x)B(x)$, με $A(x),\ B(x) \in \mathbb{Z}[x]$.

Αν $w = 1$, αφού το $f(x)$ είναι μονικό, είναι $ua_mb_n = 1$, άρα $u = a_m = b_n = 1$, οπότε αληθεύει ο ισχυρισμός μας.

Αν $w \neq 1$, υπάρχει πρώτος p με $p|w$. Επειδή $\mu\kappa\delta(v,w) = 1$, ο p δε διαιρεί τον v. Επίσης, επειδή $\mu\kappa\delta(a_0,...,a_m) = \mu\kappa\delta(b_0,...,b_n) = 1$, υπάρχουν a_i, b_j τα οποία δε διαιρεί ο p. Από το Λήμμα 2 έχουμε

$$\frac{\mathbb{Z}[x]}{(p\mathbb{Z})[x]} \cong \frac{\mathbb{Z}}{p\mathbb{Z}}[x] \cong \mathbb{Z}_p[x] \quad (*)$$

και το τελευταίο είναι ακέραια περιοχή. Επίσης η κλάση ισοδυναμίας $wf(x) + p\mathbb{Z}[x]$ ισούται με 0 στο $\frac{\mathbb{Z}}{p\mathbb{Z}}[x]$, ενώ αφού το p δε διαιρεί τα v, $A(x)$, $B(x)$, έχουμε ότι οι κλάσεις $v + p\mathbb{Z}[x]$, $A(x) + p\mathbb{Z}[x]$, $B(x) + p\mathbb{Z}[x]$ είναι διάφορες της κλάσης του μηδενός, άτοπο. ∎

4 Θεώρημα. *(Κριτήριο του Eisenstein) Αν $f(x) = a_0 + ... + a_{n-1}x^{n-1} + x^n$ είναι μονικό πολυώνυμο με ακέραιους συντελεστές και υπάρχει ένας πρώτος αριθμός p τέτοιος ώστε $p|a_0$, ..., $p|a_{n-1}$ αλλά ο p^2 δε διαιρεί τον a_0, τότε το $f(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$.*

Απόδειξη: Υποθέτουμε ότι $f(x) = a(x)b(x)$, όπου $a(x),\ b(x)$ είναι πολυώνυμα βαθμού ≥ 1 στο $\mathbb{Q}[x]$. Από το Λήμμα του Gauss μπορούμε να υποθέσουμε ότι $a(x)$, $b(x)$ είναι μονικά πολυώνυμα με ακέραιους συντελεστές. Θεωρώντας πάλι τον ισομορφισμό $(*)$ στην παραπάνω απόδειξη, έχουμε ότι η κλάση $f(x) + p\mathbb{Z}[x]$ είναι ίση με την κλάση $x^n + p\mathbb{Z}[x]$ στο δακτύλιο $\frac{\mathbb{Z}}{p\mathbb{Z}}[x]$, δεδομένου ότι $p|a_0$, ..., $p|a_{n-1}$. Επομένως θα έχουμε ότι

$$x^n + p\mathbb{Z}[x] = (\ a(x) + p\mathbb{Z}[x]) \cdot (\ b(x) + p\mathbb{Z}[x])$$

στον $\frac{\mathbb{Z}}{p\mathbb{Z}}[x]$. Για να είναι εφικτή αυτή η ισότητα πρέπει να είναι $a(x)+p\mathbb{Z}[x] = x^r+p\mathbb{Z}[x]$, $b(x)+p\mathbb{Z}[x] = x^{n-r}+p\mathbb{Z}[x]$, με $1 < r < n$, δηλαδή να υπάρχουν πολυώνυμα $g(x)$, $h(x)$ με ακέραιους συντελεστές, ώστε $a(x) = x^r + pg(x)$, $b(x) = x^{n-r} + ph(x)$, οπότε

$$f(x) = (x^r + pg(x)) \cdot (x^{n-r} + ph(x)) = x^n + px^rh(x) + px^{n-r}g(x) + p^2g(x)h(x).$$

Αυτό σημαίνει ότι $a_0 = p^2c_0d_0$, όπου $c_0,\ d_0$ είναι οι σταθεροί όροι των $g(x)$, $h(x)$, αντίστοιχα. Κάτι τέτοιο αντίκειται στην υπόθεσή μας ότι ο p^2 δε διαιρεί τον a_0. Επομένως το $f(x)$ είναι ανάγωγο επί του $\mathbb{Q}[x]$. ∎

Πέρα από τις όποιες απευθείας εφαρμογές του παραπάνω κριτηρίου στον έλεγχο του κατά πόσο ένα πολυώνυμο είναι ανάγωγο, υπάρχουν και οι εξής επιπλέον έμμεσοι τρόποι χρήσης του: Οι απεικονίσεις $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}[x]$ που δίνονται από τους τύπους

$$\varphi(f(x)) = f(x+c) \qquad \text{και} \qquad \varphi(f(x)) = f(cx)$$

όπου $c \in \mathbb{Z}$, $c \neq 0$ στη δεύτερη περίπτωση, διατηρούν τον πολλαπλασιασμό πολυωνύμων. Πράγματι, πχ για την πρώτη περίπτωση, είναι

$$\begin{aligned}
\varphi(\sum_{i=0}^{m} a_i x^i \cdot \sum_{j=0}^{n} b_j x^j) &= \varphi(\sum_{k=0}^{m+n}(\sum_{i=0}^{k} a_i b_{k-i})x^k) \\
&= \sum_{k=0}^{m+n}(\sum_{i=0}^{k} a_i b_{k-i})(x+c)^k \\
&= \sum_{i=0}^{m} a_i (x+c)^i \cdot \sum_{j=0}^{n} b_j (x+c)^j \\
&= \varphi(\sum_{i=0}^{m} a_i x^i) \cdot \varphi(\sum_{j=0}^{n} b_j x^j)
\end{aligned}$$

Ετσι, αν το πολυώνυμο $f(x)$ αναλύεται ως γινόμενο $f(x) = a(x)b(x)$, το ίδιο θα συμβαίνει και για την εικόνα μέσω του φ, $\varphi(f(x)) = \varphi(a(x)) \cdot \varphi(b(x))$. Ισοδύναμα, αν το $\varphi(f(x))$ είναι ανάγωγο, τότε και το $f(x)$ είναι ανάγωγο.

Μια κλασική εφαρμογή αυτού του τεχνάσματος είναι ή απόδειξη ότι το πολυώνυμο

$$f(x) = x^{p-1} + ... + x + 1,$$

όπου ο p είναι πρώτος αριθμός, είναι ανάγωγο. Γιατί, ανακαλώντας ότι

$$f(x) = x^{p-1} + ... + x + 1 = \frac{x^p - 1}{x - 1}$$

και θεωρώντας το μετασχηματισμό $\varphi(f(x)) = f(x+1)$ βρίσκουμε ότι το

$$f(x+1) = \frac{(x+1)^p - 1}{x+1-1} = \frac{(x+1)^p - 1}{x} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}$$

είναι ανάγωγο, αφού το p διαιρεί κάθε $\binom{p}{i}$ με $i = 1, ..., p-1$ αλλά το p^2 δε διαιρεί το $\binom{p}{1} = p$.