Εξέταση στην Αλγεβρα

Τμήμα Μαθηματικών, Πανεπιστήμιο Πατρών

21 Ιανουαρίου 2019

Θέμα 1: Α. Βρείτε το μέγιστο κοινό διαιρέτη των πολυωνύμων:

$$x^{12} + 8 \text{ και } x^{16} - 16 \text{ στο } \mathbb{R}[x],$$

και των

$$x^5 + 25x^3 + 50x + 10 \text{ και } x^5 + 1 \text{ στο } \mathbb{Q}[x],$$

Β. Ποιός από τους δακτύλιους $\frac{\mathbb{Z}_3[x]}{<x^4+1>}$ και $\frac{\mathbb{Z}_3[x]}{<x^2+x+1>}$ είναι σώμα και γιατί;

Λύση: Α. Είναι $x^{12} + 8 = (x^4)^3 + 2^3 = (x^4 + 2)((x^4)^2 - 2x^4 + 4) = (x^4 + 2)(x^8 - 2x^4 + 4)$ και $x^{16} - 16 = (x^8 - 4)(x^8 + 4) = (x^4 - 2)(x^4 + 2)(x^8 + 4)$. Παρατηρούμε ότι το $x^4 + 2$ είναι κοινός παράγοντας κι ότι το $x^8 - 2x^4 + 4 = x^4(x^4 - 2) + 4$ δεν έχει κοινούς παράγοντες με το $x^4 - 2$ (γιατί τότε ένας κοινός τους παράγοντας θα έπρεπε να διαιρεί το 4), ούτε με το $x^8 + 4$ (γιατί τότε ένας κοινός τους παράγοντας θα έπρεπε να διαιρεί το $2x^4$). Αρα ο μκδ τους είναι το $x^4 + 2$.

Το $x^5 + 25x^3 + 50x + 10$ είναι ανάγωγο, εφαρμόζοντας το κριτήριο του Eisenstein για $p = 5$, οπότε δεν έχει κοινό παράγοντα με το $x^5 + 1$, αφού δε διαιρεί το τελευταίο. Αρα ο μκδ τους είναι το 1.

Β. Παρατηρούμε ότι το $x^2 + x + 1$ δεν είναι ανάγωγο στο $\mathbb{Z}_3[x]$ αφού έχει ρίζα το $[1] \in \mathbb{Z}_3$. Αντιθέτως το $x^4 + 1$ είναι ανάγωγο στο $\mathbb{Z}_3[x]$ αφού δεν έχει ρίζα, άρα παράγει μεγιστικό ιδεώδες, οπότε ο δακτύλιος - πηλίκο είναι σώμα.

Θέμα 2: Α. Αποδείξτε ότι το σύνολο

$$I = \{a_n x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x] \mid 5|a_n,\ ...,\ 5|a_1,\ 5|a_0\}$$

είναι ιδεώδες του $\mathbb{Z}[x]$. Είναι κύριο ιδεώδες το I;

Β. Αποδείξτε ότι $\mathbb{Z}[x]/ < 5 > \cong \mathbb{Z}_5[x]$.

Λύση: Α. Το δοθέν σύνολο περιέχει το μηδενικό πολυώνυμο, αφού όλοι του οι όροι (δηλαδή το μηδέν) διαιρείται από το 5. Αν τα πολυώνυμα $f(x)$, $g(x)$ ανήκουν στο δοθέν σύνολο, δηλαδή ο οποιοσδήποτε συνετελεστής τους διαιρείται από το 5, τότε το άθροισμά τους, που θα έχει συντελεστές είτε κάποιους εκ των συντελεστών του μεγιστοβάθμιου από τα δύο, είτε $a_k + b_k$ (με a_k συντελεστές του $f(x)$ και b_k συντελεστές του $g(x)$), οι οποίοι διαιρούνται από το 5, επίσης θα διαιρείται από το 5. Αν το $f(x) = a_n x^n + ... + a_1 x + a_0$ ανήκει στο δοθέν σύνολο και το $g(x) = b_m x^m + ... + b_1 x + b_0$ είναι οποιοδήποτε πολυώνυμο, τότε το γινόμενό τους έχει γενικό συντελεστή $c_k = \Sigma_{i+j=k} a_i b_j$, ο οποίος διαιρείται από το 5, αφού όλα το a_i διαιρούνται. Αρα το δοθέν σύνολο αποτελεί ιδεώδες του $\mathbb{Z}[x]$.

Το τυχαίο στοιχείο του I έχει τη μορφή $f(x) = a_n x^n + ... + a_1 x + a_0 = 5b_n x^n + ... + 5b_1 x + 5b_0 = 5(b_n x^n + ... + b_1 x + b_0)$, άρα το ιδεώδες παράγεται από το σταθερό πολυώνυμο 5, είναι επομένως κύριο.

Β. Η συνάρτηση $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_5[x]$, με

$$\varphi(a_n x^n + ... + a_1 x + a_0) = [a_n]x^n + ... + [a_1]x + [a_0],$$

όπου $[a_i]$ δηλώνει την κλάση ισοδυναμίας στο $\mathbb{Z}_5$ του $a_i \in \mathbb{Z}$, γνωρίζουμε ότι είναι ομομορφισμός. Είναι και επί, αφού κάθε στοιχείο του $\mathbb{Z}_5[x]$ είναι της μορφής $[a_n]x^n + ... + [a_1]x + [a_0]$ για κάποια $[a_i] \in \mathbb{Z}_5$. Ο πυρηνας του φ απαρτίζεται από εκείνα τα τα $f(x) = a_nx^n + ... + a_1x + a_0$, των οποίων η εικόνα είναι $[a_n]x^n + ... + [a_1]x + [a_0] = [0]$, δηλαδή $[a_n] = [0]$, ..., $[a_0] = [0]$. Αυτό σημαίνει ότι $5|a_n$, ..., $5|a_1$, $5|a_0$, δηλαδή ο πυρήνας απαρτίζεται από πολυώνυμα που είναι πολλαπλάσια του 5. Καταλήγουμε από το πρώτο θεώρημα ισομορφισμού.

Θέμα 3: Α. Αν η μετάθεση σ ενός πεπερασμένου συνόλου X είναι περιττή, αποδείξτε ότι και η σ^{-1} είναι περιττή. Αν για κάποιο $n \in \mathbb{N}$ ισχύει $\sigma^{n+1} = id$, τι είδους μετάθεση είναι (ως προς το πρόσημο) η σ^n;

Β. Αν α, β, γ είναι τρεις μεταθέσεις ενός συνόλου X, οι οποίες είναι ανά δύο ξένες μεταξύ τους και το $x_0 \in X$ είναι τέτοιο ώστε $\alpha(x_0) \neq x_0$, αποδείξτε ότι

$$(\gamma \cdot \alpha \cdot \beta)(x_0) = \alpha(x_0)$$

Λύση: Α. Αφού $\sigma \circ \sigma^{-1} = id$, για τα πρόσημα των μεταθέσεων έχουμε

$$1 = \text{sign}(id) = \text{sign}(\sigma \circ \sigma^{-1}) = \text{sign}(\sigma) \cdot \text{sign}(\sigma^{-1}) = (-1) \cdot \text{sign}(\sigma^{-1})$$

Αρα $\text{sign}(\sigma^{-1}) = -1$, δηλαδή η σ^{-1} είναι περιττή.

Επειδή $\sigma^{n+1} = \sigma^n \circ \sigma = \sigma \circ \sigma^n = id$, έχουμε $\sigma^n = \sigma^{-1}$, άρα βάσει του προηγούμενου η σ^n είναι περιττή.

Β. Αφού $\alpha(x_0) \neq x_0$ και η β είναι ξένη προς την α, έχουμε $\beta(x_0) = x_0$. Αρα $(\alpha \cdot \beta)(x_0) = \alpha(x_0)$. Εφαρμόζοντας τη γ παίρνουμε $(\gamma \cdot \alpha \cdot \beta)(x_0) = (\gamma \cdot \alpha)(x_0)$. Ομως η α είναι ένα - προς - ένα, άρα $(\alpha \cdot \alpha)(x_0) \neq \alpha(x_0)$. Επειδή η γ είναι ξένη προς την α, παίρνουμε ότι $(\gamma \cdot \alpha)(x_0) = \alpha(x_0)$, οπότε προκύπτει το ζητούμενο.

Θέμα 4: Αν οι H, K είναι ομάδες αποδείξτε ότι το σύνολο $H^* = \{(h, 1) \in H \times K \mid h \in H\}$ είναι κανονική υποομάδα της $H \times K$, η οποία είναι ισόμορφη με την H. Αποδείξτε ότι η ομάδα - πηλίκο $\frac{H \times K}{H^*}$ είναι ισόμορφη με την K.

Λύση: Είναι προφανές ότι το σύνολο H^* βρίσκεται σε ένα - προς - ένα και επί αντιστοιχία με την υποομάδα H μέσω της συνάρτησης $\varphi \colon H \to H^*$, με $\varphi(h) = (h, 1)$ κι ότι η συνάρτηση αυτή είναι ισομορφισμός, αφού η δεύτερη συντεταγμένη δεν επιρρεάζει τις αλγεβρικές πράξεις. Δείχνουμε λοιπόν ότι είναι κανονική υποομάδα (που είναι το βασικό ζητούμενο). Ας είναι λοιπόν $(h_1, k_1) \in H \times K$ και $(h, 1) \in H^*$. Ψάχνουμε $(h_0, 1) \in H^*$ ώστε $(h_1, k_1) \cdot (h, 1) = (h_0, 1) \cdot (h_1, k_1)$, δηλαδή $(h_1h, k_1) = (h_0h_1, k_1)$. Αρκεί λοιπόν να πάρουμε $h_0 = h_1hh_1^{-1}$.

Θεωρούμε τώρα τη συνάρτηση $p \colon H \times K \to K$, με $p(h, k) = k$. Προφανώς είναι ομομορφισμός και επί (κάθε $k \in K$ είναι $k = p(1, k)$). Ο πυρήνας της είναι $\ker(p) = \{(g, h) \in H \times K \mid p(h, k) = k = 1\} = \{(g, h) \in H \times K \mid (h, k) = (h, 1)\} = H^*$. Καταλήγουμε από το πρώτο θεώρημα ισομορφισμού.

Θέμα 5: Α. Βρείτε τις υποομάδες της $\mathbb{Z}_{35}$.

Β. Δίνεται το στοιχείο $1 + 3i \in \mathbb{Z}[i]$. Εξετάστε αν το στοιχείο αυτό διαιρείται από το $1 + 2i$ και το $2 + 2i$.

Λύση: Α. Κάθε υποομάδα πρέπει να έχει τάξη που θα διαιρεί το 35, από το θεώρημα του Lagrange. Επομένως μπορούν να έχουν τάξη μόνο 1, 5, 7 και 35. Η πρώτη και η τελευταία είναι οι $\bar{0}$ και $\mathbb{Z}_{35}$, αντίστοιχα. Οι άλλες δύο είναι οι $\{\bar{0}, \bar{7}, \bar{14}, \bar{21}, \bar{28}\}$ και $\{\{\bar{0}, \bar{5}, \bar{10}, \bar{15}, \bar{20}, \bar{25}, \bar{30}\}$.

Β. Το $1 + 3i$ έχει νόρμα $1^2 + 3^2 = 10$. Αν διαιρείτο από το $2 + 2i$ θα έπρεπε η νόρμα του τελευταίου, $2^2 + 2^2 = 8$, να διαιρεί το 10, που είναι αδύνατο. Η νόρμα του $1 + 2i$ που είναι $1^2 + 2^2 = 5$ διαιρεί το 10, αυτό όμως δε μας επιβάλλει ότι το $1+2i$ διαιρεί το $1+3i$. Πράγματι, αν ήταν $1+3i = (1+2i)(a+bi) = (a-2b)+(2a+b)i$, με $a, b \in \mathbb{Z}$, θα ήταν $a-2b=1$ και $2a+b=3$. Πολλαπλασιάζοντας τη δεύτερη επί 2 και προσθέτοντας στην πρώτη βλέπουμε ότι τότε θα ήταν $5a=7$, άτοπο. Αρα ούτε το $1+2i$ διαιρεί το $1+3i$.