Ασκήσεις Βασικής Άλγεβρας και Λύσεις τους

4 Δεκεμβρίου 2013

1 Ασκήσεις και Λύσεις. 2013-14

1. (α′) Έστω m, n δύο φυσικοί αριθμοί, τέτοιοι ώστε $MK\Delta(m, n+5) = MK\Delta(m+5, n) = 1$. Αποδείξτε ότι $MK\Delta(mn, m+n+5) = 1$.

   (β′) Να βρεθούν οι φυσικοί αριθμοί k, τέτοιοι ώστε $9^k = 1 mod(14)$

   Η παραπάνω άσκηση ήταν Θέμα εξετάσεων Σεπτεμβρίου 2004

2 Βασική άλγεβρα
Συνεργασία μιας ομάδας με διάθεση διδασκαλίας

Ασκήσεις στο μάθημα Βασική Άλγεβρα

Οι ασκήσεις αυτές[1] γράφονται και λύνονται με σκοπό να βοηθήσουν στη μελέτη των φοιτητών του Τμήματος Μαθηματικών κατά την περίοδο Απρίλιος -Σεπτέμβριος 2008

1. **[Άσκηση 1]** Θέματα εξετάσεων Φεβρουαρίου 2008 και λύσεις τους[2]

   Θέμα 1 *0,5 μονάδες*

   Ομάδα Α Δώστε τον ορισμό του ιδεώδους ενός δακτυλίου

   Ομάδα Β Δώστε τον ορισμό της κανονικής υποομάδας μιας ομάδας

   Θέμα 2 *1 μονάδα*

   Ομάδα Α Έστω G μία ομάδα και Η μία κανονική υποομάδα της G. Να ορισθεί το σύνολο πηλίκο G/H και να δειχθεί ότι αυτό επιδέχεται τη δομή μίας ομάδας.

   Ομάδα Β Έστω R ένας δακτύλιος και Ι ένα ιδεώδες αυτού. Να ορισθεί το σύνολο-πηλίκο R/I και να δειχθεί ότι αυτό επιδέχεται τη δομή ενός δακτυλίου

   Θέμα 3 *0,5 μονάδες*

   Ομάδα Α Διατυπώστε το πρώτο θεώρημα ισομορφισμών στους δακτυλίους

   Ομάδα Β Διατυπώστε το πρώτο θεώρημα ισομορφισών στις ομάδες

   Θέμα 4 *1 μονάδα*

   Ομάδα Α Δώστε ένα παράδειγμα μίας άπειρης ομάδας G που είναι τέτοια, ώστε κάθε μη-τετριμμένη υποομάδα της είναι ισόμορφη με την G. (Δικαιολογήστε την απάντησή σας)

   Ομάδα Β Δώστε ένα παράδειγμα μίας πεπερασμένης ομάδας G που είναι τέτοια, ώστε κάθε μη-τετριμμένη υποομάδα της είναι ισόμορφη με την G. (Δικαιολογήστε την απάντησή σας)

   Θέμα 5 *1 μονάδα*

[1] Στην ομάδα αυτή προς το παρόν συμμετέχουν οι Α.Καρασούλου, Κ.Λέντζος,Κ.Μηλίγκου, Ε.Ράπτης, Σ.Χασάπης

[2] Οι λύσεις προτείνονται από την ομάδα διδασκόντων το μάθημα Βασική άλγεβρα Δ.Δεριζιώτη, Ι.Εμμανουήλ, Ε.Ράπτη, Μ.Φραγκουλοπούλου

Ομάδα Α Έστω Ι το ιδεώδες του δακτυλίου $\mathbb{Z}_3[x]$ που παράγεται από το πολυώνυμο $x^3 + 2x + 1$. Να δειχθεί ότι ο δακτύλιος -πηλίκο $R = (\mathbb{Z}_3[x]/I)$ έχει μόνο δύο ιδεώδη

Ομάδα Β Έστω F ένα σώμα και $\phi : F \longrightarrow R$ ένας ομομορφισμός δακτυλίων. Αν ο φ δεν είναι 1-1, δείξτε ότι φ(α)=0 για κάθε στοιχείο α του F

Θέμα 6 *1 μονάδα*

Ομάδα Α Έστω Κ ένα σώμα και a, b δύο στοιχεία του με το a μη-μηδενικό. Αν Ι είναι το ιδεώδες του δακτυλίου $K[x]$ που παράγεται από το πολυώνυμο $ax + b$, δείξτε ότι ο δακτύλιος πηλίκο $K[x]/I$ είναι ισόμορφος με το σώμα Κ

Ομάδα Β Έστω $\mathbb{R}$ το σώμα των πραγματικών αριθμών και Ι το ιδεώδες του δακτυλίου $\mathbb{R}[x]$ που παράγεται από το πολυώνυμο $x^2 + 1$. Δείξτε ότι ο δακτύλιος πηλίκο $\mathbb{R}[x]/I$ είναι ισόμορφος με το σώμα $\mathbb{C}$ των μιγαδικών αριθμών

Θέμα 7 *0,8 μονάδες*

Ομάδα Α Έστω $G =< a >$ μία κυκλική ομάδα τάξης 120. Να δειχθεί ότι $< a^{42} >=< a^{54} >$

Ομάδα Β Έστω $G =< a >$ μία κυκλική ομάδα τάξης 100. Να δειχθεί ότι $< a^{28} >=< a^{36} >$

Θέμα 8 *0,7 μονάδες*

Ομάδα Α Δείξτε ότι το γινόμενο δύο ιδεωδών ενός δακτυλίου είναι ιδεώδες

Ομάδα Β Δείξτε ότι το άθροισμα δύο ιδεωδών ενός δακτυλίου είναι ιδεώδες

Θέμα 9 *0,5 μονάδες*

Ομάδα Α Να βρεθεί ένα πολυώνυμο του $\mathbb{Z}_5[x]$ βαθμού το πολύ 4, το οποίο επάγει την ίδια πολυωνυμική συνάρτηση από το $\mathbb{Z}_5$ στον εαυτό του με αυτήν που επάγει το πολυώνυμο $x^{10} + 2x^6 + 3x^4 + 1$

Ομάδα Β Να βρεθεί ένα πολυώνυμο του $\mathbb{Z}_7[x]$ βαθμού το πολύ 6, το οποίο επάγει την ίδια πολυωνυμική συνάρτηση από το $\mathbb{Z}_7$ στον εαυτό του με αυτήν που επάγει το πολυώνυμο $3x^{14} + 2x^8 + 3x^6 + 4$

Θέμα 10 *1 μονάδα*

Ομάδα Α Έστω n ένας φυσικός αριθμός με $n > 1$ και a ένας ακέραιος σχετικά πρώτος με τον n. Δείξτε ότι η απεικόνιση $\sigma_a : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, με $\sigma_a[b] = [ab]$ για κάθε στοιχείο $[b]$ του $\mathbb{Z}_n$, είναι μία μετάθεση του $\mathbb{Z}_n$

Ομάδα Β Έστω n ένας φυσικός αριθμός με $n > 1$ και b ένας ακέραιος σχετικά πρώτος με τον n. Δείξτε ότι η απεικόνιση $\sigma_b : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, με $\sigma_b[a] = [ba]$ για κάθε στοιχείο $[a]$ του $\mathbb{Z}_n$, είναι μία μετάθεση του $\mathbb{Z}_n$

Θέμα 11 *1 μονάδα*

Ομάδα Α Στο $10^ο$ θέμα έστω $a = 4$ και $n = 9$. Γράψτε τη μετάθεση σ_4 του $\mathbb{Z}_9$ ως γινόμενο ξένων ανά δύο κύκλων.

Ομάδα Β Στο $10^ο$ θέμα έστω $b = 3$ και $n = 10$. Γράψτε τη μετάθεση σ_3 του $\mathbb{Z}_{10}$ ως γινόμενο ξένων ανά δύο κύκλων.

Θέμα 12 *1 μονάδα*

Ομάδα Α Γράφοντας την μετάθεση σ_a του 10^o θέματος ως γινόμενο ξένων ανά δύο κύκλων, δείξτε ότι οι κύκλοι αυτοί κατατάσσονται σε δύο κατηγορίες: Η μία περιλαμβάνει κύκλους των οποίων τα σημεία είναι αντιστρέψιμα $modn$ και η άλλη περιλαμβάνει κύκλους των οποίων τα σημεία δεν είναι αντιστρέψιμα $modn$.
(Με *σημεία* του κύκλου $(i_1, i_2, \cdots, i_\kappa)$
εννοούμε τα στοιχεία $i_1, i_2, \cdots, i_\kappa$)

Ομάδα Β Γράφοντας την μετάθεση σ_b του 10^o θέματος ως γινόμενο ξένων ανά δύο κύκλων, δείξτε ότι οι κύκλοι αυτοί κατατάσσονται σε δύο κατηγορίες: Η μία περιλαμβάνει κύκλους των οποίων τα σημεία είναι αντιστρέψιμα $modn$ και η άλλη περιλαμβάνει κύκλους των οποίων τα σημεία δεν είναι αντιστρέψιμα $modn$.
(Με *σημεία* του κύκλου $(i_1, i_2, \cdots, i_\kappa)$
εννοούμε τα στοιχεία $i_1, i_2, \cdots, i_\kappa$)

Απαντήσεις

Θέμα 1 *0,5 μονάδες*

Ομάδα Α **Απάντηση:** Είναι ο ορισμός 2.5.5 στο βιβλίο

Ομάδα Β **Απάντηση:** Σελίδα 352 στο βιβλίο

Θέμα 2 *1 μονάδα*

Ομάδα Α **Απάντηση:** Σελίδα 351 στο βιβλίο

Ομάδα Β Σελίδα 152 στο βιβλίο

Θέμα 3 *0,5 μονάδα*

Ομάδα Α **Απάντηση:** Θεώρημα 2.6.6 στο βιβλίο

Ομάδα Β **Απάντηση:** Σελίδα 4.7.6 στο βιβλίο

Θέμα 4 *1 μονάδα*

Ομάδα Α **Απάντηση:** Γνωρίζουμε ότι κάθε άπειρη κυκλική ομάδα είναι ισόμορφη με την προσθετική ομάδα $(\mathbb{Z}, +)$ των ακεραίων αριθμών. Επίσης γνωρίζουμε ότι κάθε μη-τετριμμένη υποομάδα της $(\mathbb{Z}, +)$ είναι και αυτή άπειρη κυκλική. Άρα κάθε μη-τετριμμένη υποομάδα της $(\mathbb{Z}, +)$ ως άπειρη κυκλική είναι ισόμορφη με την $(\mathbb{Z}, +)$

Ομάδα Β **Απάντηση:** Έστω p ένας πρώτος αριθμός. Τότε η προσθετική ομάδα $(\mathbb{Z}_p, +)$ των κλάσεων υπολοίπων $modp$ δεν έχει καμμία γνήσια υποομάδα εκτός από την τετριμμένη, δηλαδή εάν Η είναι μία μη-τετριμμένη υποομάδα της $(\mathbb{Z}_p, +)$, τότε $H = (\mathbb{Z}_p, +)$. Αυτό είναι άμεση συνέπεια του θεωρήματος $Lagrange$ και του γεγονότος ότι η τάξη της $(\mathbb{Z}_p, +)$ είναι p.
Ας σημειωθεί ότι κάθε ομάδα που έχει την ιδιότητα του ερωτήματος είναι ισόμορφη με την $(\mathbb{Z}_p, +)$ για κάποιο πρώτο $modp$. Πράγματι,

επειδή ισόμορφες ομάδες έχουν την ίδια τάξη μία μη-τετριμμένη υποομάδα μιας πεπερασμένης ομάδας G είναι ισόμορφη με την G αν είναι η ίδια η G. Αν $g \neq 1$ είναι ένα στοιχείο της G, τότε η κυκλική υποομάδα $< g >$ που παράγεται από το $< g >$ είναι όλη η ομάδα G. Οι μόνες κυκλικές ομάδες που δεν έχουν γνήσιες υποομάδες είναι αυτές που έχουν τάξη ένα πρώτο αριθμό p. Κάθε τέτοια ομάδα είναι ισόμορφη με την $(\mathbb{Z}_p, +)$.

Θέμα 5 *1 μονάδα*

Ομάδα Α **Απάντηση:** Το εν λόγω πολυώνυμο δεν έχει καμμία ρίζα στο $\mathbb{Z}_3$ και επειδή ο βαθμός του είναι 3 αυτό είναι ανάγωγο. Γνωρίζουμε (Θεώρημα 2.6.3) ότι τότε ο εν λόγω δακτύλιος -πηλίκο είναι σώμα και ως σώμα έχει μόνο δύο ιδεώδη.

Ομάδα Β **Απάντηση:** Επειδή η φ δεν είναι 1-1 ο πυρήνας $Ker\phi$ είναι $Ker\phi \neq 0$. Αλλά ο πυρήνας ενός ομομορφισμού δακτυλίων είναι ιδεώδες. Επειδή το $\mathbb{F}$ είναι σώμα, τα μόνα ιδεώδη του είναι το $\{0\}$ και το $\mathbb{F}$. Άρα $Ker\phi = \mathbb{F}$

Θέμα 6 *1 μονάδα*

Ομάδα Α **Απάντηση:** Η απεικόνιση $\mathcal{E}$: K$[x]$ $\longrightarrow$K, $με$ $\mathcal{E}$ $(f(x)) = f(\frac{-\beta}{\alpha})$, είναι ένας επιμορφισμός δακτυλίων, που ο πυρήνας του είναι
Ker $\mathcal{E}$= $\{f(x) \in$ K$[x] \mid f(\frac{-\beta}{\alpha}) = 0$
$= \{(x + \beta/\alpha)g(x) \mid g(x) \in K[x]\} =< \alpha \cdot x + \beta >= I$ Οπότε από το πρώτο θεώρημα ισομορφισμών έχουμε $K[x]/I \approx K$
Ή πιο απλά: Τα στοιχεία του $K[x]/I$ είναι της μορφής $r + I, r \in K$, καθώς αν διαιρέσουμε ένα πολυώνυμο $f(x) \in K[x]$ δια του $\alpha x + \beta$, το υπόλοιπο είναι ένα στοιχείο r του K. Η απεικόνιση $K[x]/I \longrightarrow r$ είναι ένας ισομορφισμός

Ομάδα Β **Απάντηση:** Παράδειγμα 2.6.7 σελίδα 159 στο βιβλίο

Θέμα 7 *0,8 μονάδες*

Ομάδα Α **Απάντηση:** Έχουμε ΜΚΔ(42,120)=ΜΚΔ(54,120)=6
Γνωρίζουμε ότι $|< \alpha^{42} >|= \frac{120}{MK\Delta(42,120)} = 20$
και $|< \alpha^{54} >|= \frac{120}{MK\Delta(54,120)} = 20$
Επίσης γνωρίζουμε ότι για κάθε διαιρέτη κ της τάξης μιας πεπερασμένης κυκλικής ομάδας, υπάρχει μία μοναδική υποομάδα της ομάδας τάξης ίσης με κ. Άρα $< \alpha^{42} >=< \alpha^{54} >$

Ομάδα Β **Απάντηση:** Η απάντηση είναι ακριβώς η ίδια όπως στο θέμα 7 της ομάδας Α. Εδώ έχουμε ΜΚΔ(28,100)=ΜΚΔ(36,100)=4 και συνεπώς $< \alpha^{28} >=< \alpha^{36} >$

Θέμα 8 *0,7 μονάδες*

Ομάδα Α **Απάντηση:** Πρόταση 2.5.8 στο βιβλίο

Έστω Ι και J δύο ιδεώδη ενός δακτυλίου R. Το γινόμενο IJ Ορίζεται ως το σύνολο

$$IJ = \{\alpha_1\beta_1 + \cdots \alpha_\kappa\beta_\kappa \mid \alpha_i \in I, \beta_i \in J, \kappa \geq 1\}$$

που είναι μη κενό σύνολο αφού τα Ι και J είναι μη κενά.
Έστω τώρα $\alpha = \alpha_1\beta_1 + \cdots \alpha_\kappa\beta_\kappa, \beta = \alpha'_1\beta'_1 + \cdots + \alpha'_s\beta'_s \in IJ$,
$\alpha_i, \alpha_j \in I, \beta_i, \beta_j \in J, i = 1, 2, \cdots \kappa, j = 1, 2, \cdots, s$
Τότε $\alpha - \beta = \alpha_1\beta_1 + \cdots \alpha_\kappa\beta_\kappa + \alpha_{\kappa+1}\beta_{\kappa+1} + \cdots + \alpha_{\kappa+s}\beta_{\kappa+s} \in IJ$
όπου $\alpha_{\kappa+j} = -\alpha_j, \beta_{\kappa+j} = -\beta_j, j = 1, 2, \cdots, s$
Επίσης αν $r \in R$, τότε τα στοιχεία $r\alpha_i \in I$ και $\beta_i r \in J$. Αρα
$(r\alpha_1)\beta_1 + \cdots + (r\alpha_\kappa)\beta_\kappa = r(\alpha_1\beta_1 + \cdots \alpha_\kappa\beta_\kappa) \in IJ$ και
$\alpha_1(\beta_1 r) + \cdots + \alpha_\kappa(\beta_\kappa r) = (\alpha_1\beta_1 + \cdots \alpha_\kappa\beta_\kappa)r \in IJ$
Δηλαδή το μη κενό σύνολο IJ ικανοποιεί όλες τις ιδιότητες που απαιτούνται για να είναι ιδεώδες του R

Ομάδα Β **Απάντηση:** Πρόταση 2.5.8 στο βιβλίο

Θέμα 9 *0,5 μονάδες*

Ομάδα Α **Απάντηση:** Το υπόλοιπο της διαίρεσης του $f(x) = x^{10} + 2x^6 + 3x^4 + 1$ δια του $x^5 - x$ είναι το πολυώνυμο $g(x) = 3x^4 + 3x^2 + 1$ και συνεπώς $x^5 - x \mid f(x) - g(x)$, άρα οι πολυωνυμικές συναρτήσεις που επάγονται από τα $f(x), g(x)$ είναι ίσες. Ένας άλλος τρόπος είναι να εφαρμόσουμε την παρεμβολή του Lagrange (Θεώρημα 2.2.8)

Ομάδα Β **Απάντηση:** Η απάντηση εδώ είναι όπως στο θέμα 9 της ομάδας Α. Εδώ το υπόλοιπο της δαίρεσης του $x^{14} + 2x^8 + 3x^6 + 4$ δια του $x^7 - x$ είναι το πολυώνυμο $g(x) = 3x^6 + 5x^2 + 4$

Θέμα 10 *1 μονάδα*

Ομάδα Α **Απάντηση:** Έστω $\mathbb{Z}_n = \{[\alpha_1], [\alpha_2], \cdots, [\alpha_n]\}$. Για να είναι η σ_α μία μετάθεση αρκεί να δείξουμε ότι
$\mathbb{Z}_n = \{[\alpha\alpha_1], [\alpha\alpha_2], \cdots, [\alpha\alpha_n]\}$ δηλαδή αρκεί να δείξουμε οτι για κάθε $i \neq j, 1 \leq i, j \leq n$ έχουμε $[\alpha\alpha_i] \neq [\alpha\alpha_j$.
Πράγματι, αν $[\alpha\alpha_i] = [\alpha\alpha_j]$, δηλαδή αν $[\alpha][\alpha_i] = [\alpha][\alpha_j]$, τότε επειδή ο α είναι πρώτος προς τον n, η κλάση $[\alpha]$ είναι αντιστρέψιμη και συνεπώς
$[\alpha]^{-1}[\alpha][\alpha_i] = [\alpha]^{-1}[\alpha][\alpha_j]$, δηλαδή $[\alpha_i] = [\alpha_j]$ και άρα $i = j$

Ομάδα Β **Απάντηση:** Όπως στην ομάδα Α

Θέμα 11 *1 μονάδα*

Ομάδα Α **Απάντηση:** Εδώ έχουμε $\mathbb{Z}_9 = \{[0], [1], [2], [3], [4], [5], [6], [7], [8]\}$, οπότε $\sigma_4[0] = [0], \sigma_4[1] = [4], \sigma_4[2] = [8], \sigma_4[3] = [3], \sigma_4[4] = [7], \sigma_4[5] = [2], \sigma_4[6] = [6], \sigma_4[7] = [1], \sigma_4[8] = [5]$, άρα $\sigma_4 = ([1][4][7])([2][8][5])$

Ομάδα Β **Απάντηση:** Όπως στο θέμα 11 της ομάδας Α. Εδώ βρίσκουμε $\sigma_3 = ([1][3][9][7])([2][6][8][4])$

Θέμα 12 *1 μονάδα*

Ομάδα Α **Απάντηση:** Έστω ότι ο κύκλος $S = ([\alpha_{i_1}], [\alpha_{i_2}], \cdots, [\alpha_{i_k}])$ εμφανίζεται στην παράσταση της σ_α ως γινόμενο ξένων ανά δύο κύκλων. Αν ένα σημείο του κύκλου αυτού έστω το $[\alpha_{i_j}]$ είναι αντιστρέψιμη κλάση $modn$ γράφοντας την S ως $([\alpha_{i_j}], [\alpha][\alpha_{i_j}], [\alpha]^2[\alpha_{i_j}], \cdots, [\alpha]^{k-1}[\alpha_{i_j}])$, βλέπουμε ότι όλα τα σημεία της είναι αντιστρέψιμα, αφού είναι γινόμενα αντιστρεψίμων κλάσεων $modn$. Αυτό αποδεικνύει ταυτόχρονα ότι αν ένα σημείο του S είναι μη αντιστρέψιμο $modn$, τότε όλα τα σημεία του είναι μη αντιστρέψιμα, αφού το γινόμενο μιας αντιστρέψιμης κλάσης επί μιας μη αντιστρέψιμης είναι μή αντιστρέψιμη κλάση

Ομάδα Β **Απάντηση:** Όπως στο Α

2. **[Άσκηση 2]** Έστω G μια ομάδα. Δείξτε ότι η απεικόνιση $\phi : G \to G$ με $\phi(a) = a^2$ για κάθε $a \in G$ είναι ομομορφισμός ομάδων αν και μόνον αν η G είναι αβελιανή.

   Απάντηση: Η ϕ είναι ομομορφισμός αν και μόνον αν για κάθε $a, b \in G$ έχουμε

   $$\phi(ab) = \phi(a)\phi(b).$$

   Αντικαθιστώντας τον τύπο της ϕ, η παραπάνω σχέση ισοδύναμα γράφεται:

   $$(ab)^2 = \phi(ab) = \phi(a)\phi(b) = a^2b^2,$$

   ισοδύναμα $(ab)(ab) = a^2b^2 \Leftrightarrow a(ba)b = a(ab)b$. Πολλαπλασιάζοντας από αριστερά με a^{-1} και από δεξιά με b^{-1} μπορούμε ισοδύναμα να γράψουμε $ba = ab$. Συνεπώς η ϕ είναι ομομορφισμός αν και μόνον αν η G είναι αβελιανή.

   Κωνσταντίνος Λέντζος

3. **[Άσκηση 3]** Έστω F σώμα, $f(x) \in F[x]$ και $I =< f(x) >$ το κύριο ιδεώδες που παράγεται από το πολυώνυμο $f(x)$. Να δείξετε ότι ο δακτύλιος πηλίκο $F[x]/I$ είναι σώμα αν και μόνον αν το πολυώνυμο $f(x)$ είναι ανάγωγο (επί του F).

   Απάντηση: Έστω ότι ο δακτύλιος πηλίκο είναι σώμα και $g(x), h(x) \in F[x]$ με $f(x) = g(x)h(x)$. Τότε

   $$\begin{aligned}(g(x) + I)(h(x) + I) &= g(x)h(x) + I \\ &= f(x) + I \\ &= 0 + I\end{aligned}$$

Έτσι $g(x)+I=0+I$ ή $h(x)+I=0+I$. Ισοδύναμα $g(x)\in I$ ή $h(x)\in I$, ή ισοδύναμα $f(x)\mid g(x)$ ή $f(x)\mid h(x)$ και συνεπώς το $f(x)$ είναι ανάγωγο.

Αντίστροφα τώρα υποθέτουμε ότι το $f(x)$ είναι ανάγωγο και θα δείξουμε ότι ο δακτύλιος πηλίκο $F[x]/I$ είναι σώμα. Κατα αρχήν παρατηρούμε ότι ο $F[x]/I$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο $1+I\neq 0+I$. Θεωρούμε ένα στοιχείο $g(x)+I\neq 0+I$, τότε $g(x)\notin I$ και άρα $f(x)\nmid g(x)$. Συνεπώς μκδ$(f(x),g(x))=1$. Υπάρχουν λοιπόν πολυώνυμα $a(x),b(x)\in F[x]$ με

$$a(x)f(x)+b(x)g(x)=1.$$

Τότε $(a(x)f(x)+I)+(b(x)g(x)+I)=1+I$ και άρα $b(x)g(x)+I=1+I$ από το οποίο έπεται ότι

$$(b(x)+I)(g(x)+I)=1+I.$$

Συνεπώς το τυχαίο μη μηδενικό στοιχείο $g(x)+I$ του δακτυλίου $F[x]/I$ είναι αντιστρέψιμο και έτσι ο δακτύλιος αυτός είναι σώμα όπως επιθυμούσαμε.

Κωνσταντίνος Λέντζος

4. [**Άσκηση 4**] Σωστό ή Λάθος;

   (α′) Έστω a και b στοιχεία ενός μεταθετικού δακτυλίου R με $ab=0$, τότε τα a,b είναι διαιρέτες του μηδενός.

   (β′) Κάθε ακεραία περιοχή είναι σώμα.

   (γ′) Τα μοναδικά αντιστρέψιμα στοιχεία του δακτυλίου $\mathbb{Z}$ είναι το 1 και το -1.

   (δ′) Το σύνολο $i\mathbb{R}=\{ir|r\in R\}$ των φανταστικών αριθμών εφοδιασμένο με τις συνήθεις πράξεις είναι σώμα.

   (ε′) Ο δακτύλιος $M_2(\mathbb{Z}_2)$ των 2×2 πινακων με στοιχεία από το $\mathbb{Z}_2$ έχει 16 στοιχεία.

   (ϛ′) Ο δακτύλιος $M_2(\mathbb{Z}_2)$ είναι μεταθετικός.

   (ζ′) Η πράξη του πολλαπλασιασμού σε ένα σώμα είναι πράξη μεταθετική.

   (η′) Η πράξη της πρόσθεσης σε έναν δακτύλιο είναι πράξη μεταθετική.

   (θ′) Σε κάθε δακτύλιο R ισχύει $a^2-b^2=(a+b)(a-b)$ για κάθε $a,b\in R$.

   (ι′) Αν για δύο ακεραίους a,b υπάρχουν ακέραιοι m,n ώστε $am+bn=1$ τότε μκδ$(a,b)=1$.

   (ια′) Οι δακτύλιοι $\mathbb{Q}[x]/<x^2+1>$ και $\mathbb{Q}[x]/<x^2-1>$ είναι ισόμορφοι.

Απάντησεις:

(α′) Λάθος. Θα έπρεπε επιπλέον να έχουμε ότι $a, b \neq 0$.

(β′) Λάθος. Ο δακτύλιος $\mathbb{Z}$ είναι ακεραία περιοχή αλλά όχι σώμα.

(γ′) Σωστό.

(δ′) Λάθος. Δεν είναι καν δακτύλιος διότι δεν είναι κλειστό ως προς την πράξη του πολλαπλάσιασμού $\cdot : i\mathbb{R} \times i\mathbb{R} \to i\mathbb{R}$ μιας και $i \cdot i = -1 \notin i\mathbb{R}$.

(ε′) Σωστό. Ένας τέτοιος πίνακας έχει 4 εγγραφές και για κάθε εγγραφή έχουμε 2 επιλογές, συνολικά $2^4 = 16$ πίνακες.

(ϛ′) Λάθος. Αν ήταν μεταθετικός θα έπρεπε για κάθε $A, B \in M_2(\mathbb{Z}_2)$ να ισχύει $AB = BA$. Για $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ και $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ όμως έχουμε $AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ενώ $BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

(ζ′) Σωστό.

(η′) Σωστό.

(θ′) Λάθος. Έχουμε ότι το $(a+b)(a-b) = a^2 + ba - ab + b^2$ είναι ίσο με $a^2 - b^2$ αν και μόνον αν $ba - ab = 0$ δήλαδή $ab = ba$, δηλαδή αν και μόνον αν ο δακτύλιος είναι μεταθετικός.

(ι′) Σωστό. Έστω $d = $μκδ$(a, b)$, τότε $d \mid a$ και $d \mid b$. Συνεπώς $d \mid am$ και $d \mid bn$ και άρα $d \mid (am + bn)$, δηλαδή $d \mid 1$ και άρα $d = 1$.

(ια′) Λάθος. Κατα αρχήν παρατηρούμε ότι και οι δύο δακτύλιοι είναι μεταθετικοί με μονάδα. Επιπλέον το πολυώνυμο $x^2 + 1$ είναι ανάγωγο επί του $\mathbb{Q}$, διότι είναι δευτέρου βαθμού και οι ρίζες του δεν ανήκουν στο $\mathbb{Q}$. Από την άλλη πλευρά, το πολυώνυμο $x^2 - 1$ δεν είναι ανάγωγο, διότι $x^2 - 1 = (x+1)(x-1) \in \mathbb{Q}[x]$. Σύμφωνα λοιπόν με την άσκηση (3) ο δακτύλιος $\mathbb{Q}[x]/ < x^2 + 1 >$ είναι σώμα ενώ ο $\mathbb{Q}[x]/ < x^2 - 1 >$ όχι και ως εκ τούτου δεν μπορεί να είναι ισόμορφοι.

Άννα Καρασούλου

5. **[Άσκηση 5]** Να βρεθούν τα αντιστρέψιμα στοιχεία του δακτυλίου $M_2(\mathbb{Z}_2)$ των 2×2 πινακων με στοιχεία από το $\mathbb{Z}_2$. Να βρεθούν στοιχεία για την ομάδα αυτή.

Απάντηση: Το σύνολο $M_2(\mathbb{Z}_2)$ των 2×2 πινακων με στοιχεία από το $\mathbb{Z}_2$ έχει 16 στοιχεία, διότι αφού έχουμε πίνακες 2×2 οι θέσεις είναι 4 και σε κάθε θέση μπορούμε να έχουμε $0(mod2)$ ή $1(mod2)$. Τώρα από τη Γραμμική άλγεβρα έχουμε ότι ένας πίνακας είναι αντιστρέψιμος εάν και μόνο εάν η ορίζουσά του είναι διαφορετική από $0(mod2)$

Βρίσκουμε δια αναγραφής τους παρακάτω 6 πίνακες:

$$\begin{pmatrix} 1(mod2) & 0(mod2) \\ 0(mod2) & 1(mod2) \end{pmatrix}$$

$$\begin{pmatrix} 1(mod2) & 1(mod2) \\ 0(mod2) & 1(mod2) \end{pmatrix}$$

$$\begin{pmatrix} 1(mod2) & 0(mod2) \\ 1(mod2) & 1(mod2) \end{pmatrix}$$

$$\begin{pmatrix} 0(mod2) & 1(mod2) \\ 1(mod2) & 0(mod2) \end{pmatrix}$$

$$\begin{pmatrix} 1(mod2) & 1(mod2) \\ 1(mod2) & 0(mod2) \end{pmatrix}$$

$$\begin{pmatrix} 0(mod2) & 1(mod2) \\ 1(mod2) & 1(mod2) \end{pmatrix}$$

Βρισκουμε τα παρακάτω:

(α′) Το σύνολο των 6 πινάκων με πράξη τον πολλαπλασιασμό σχηματίζει ομάδα Γ.

(β′) Η παραπάνω ομάδα δεν είναι αβελιανή

(γ′) Η παραπάνω ομάδα Γ έχει τρία στοιχεία τάξης 2 και 2 στοιχεία τάξης 3

(δ′) Η παραπάνω ομάδα είναι ισόμορφη με την ομάδα μεταθέσεων S_3

Προσεχώς λεπτομέρειες. Καλούνται οι φοιτητές να προσπαθήσουν

Ε.Ράπτης

6. **[Άσκηση 6]** Δείξτε ότι ο δακτύλιος $R = \{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}\}$ με πράξεις την πρόσθεση και τον πολλαπλασιασμό πινάκων είναι ισόμορφος με τον δακτύλιο $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Z}\}$ ο οποίος έχει εφοδιαστεί με τις συνήθεις πράξεις.

Απάντηση: Ορίζουμε $\phi : R \to \mathbb{Z}[\sqrt{2}]$ με $\phi(a+b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$ για κάθε $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Τότε

$$\begin{aligned}\phi((a+b\sqrt{2})+(c+d\sqrt{2})) &= \phi((a+c))+(b+d)\sqrt{2}) \\ &= \begin{pmatrix} a+c & 2(b+d) \\ b+d & a+c \end{pmatrix} \\ &= \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + \begin{pmatrix} c & 2d \\ d & c \end{pmatrix} \\ &= \phi(a+b\sqrt{2}) + \phi(c+d\sqrt{2})\end{aligned}$$

και

$$\begin{aligned}\phi((a+b\sqrt{2})(c+d\sqrt{2})) &= \phi((ac+2bd))+(ad+bc)\sqrt{2}) \\ &= \begin{pmatrix} ac+2bd & 2(ad+bc) \\ ad+bc & ac+2bd \end{pmatrix} \\ &= \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & 2d \\ d & c \end{pmatrix} \\ &= \phi(a+b\sqrt{2})\phi(c+d\sqrt{2}).\end{aligned}$$

Άρα η ϕ είναι ομομορφισμός δακτυλίων με πυρήνα

$$\begin{aligned}ker\phi &= \{a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] : \phi(a+b\sqrt{2}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\} \\ &= \{a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] : \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\} \\ &= \{a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] : a=b=c=d=0\} \\ &= \{0+0\sqrt{2}\}.\end{aligned}$$

Συνεπώς η ϕ είναι 1-1. Μένει να δείξουμε ότι η ϕ είναι επί. Για το λόγο αυτό θεωρούμε έναν τυχαίο πίνακα $A = \begin{pmatrix} x & 2y \\ y & x \end{pmatrix}$ του S και παρατηρούμε ότι το

στοιχείο $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ έχει εικόνα τον Α. Έτσι λοιπόν η ϕ είναι ένας ισομορφισμός δακτυλίων όπως θέλαμε να δείξουμε.

Άννα Καρασούλου

7. **[Άσκηση 7]** Σωστό ή Λάθος;

   (α′) Έστω R το σύνολο των συναρτήσεων από το $\mathbb{R}$ στο $\mathbb{R}$ οι οποίες έχουν παράγωγο κάθε τάξης. Ορίζουμε μια συνάρτηση $\phi : R \to R$ με
   $$\phi(f(x)) = f'(x) \text{ για κάθε } f(x) \in R.$$
   i. Η $\phi : (R, +) \to (R, +)$ είναι ομομορφισμός ομάδων.
   ii. Η $\phi : (R, +, \cdot) \to (R, +, \cdot)$ είναι ομομορφισμός δακτυλίων.

   (β′) Έστω $\phi : R \to S$ ένας ομομορφισμός δακτυλίων και I ένας ιδεώδες του R, τότε το $\phi(I)$ είναι ιδεώδες του S.

   (γ′) Έστω $\phi : R \to S$ ένας ομομορφισμός δακτυλίων και I ένας ιδεώδες του R, τότε το $\phi(I)$ είναι ιδεώδες του $Im\phi$.

   (δ′) Έστω $\phi : R \to S$ ένας ομομορφισμός δακτυλίων και J ένας ιδεώδες του S, τότε το $\phi^{-1}(J)$ είναι ιδεώδες του R.

   (ε′) Το $\mathbb{Q}$ είναι ιδεώδες του $\mathbb{R}$.

   (ϛ′) Οι δακτύλιοι $\mathbb{Z}$ και $\mathbb{Z}/n\mathbb{Z}$ είναι ισόμορφοι.

   (ζ′) Αν R είναι μια ακεραία περιοχή που δεν είναι σώμα και I ένα ιδεώδες του R, τότε το πηλίκο R/I δεν μπορεί να είναι σώμα.

   (η′) Αν R είναι μια ακεραία περιοχή και I ένα ιδεώδες του R, τότε το πηλίκο R/I είναι επίσης ακεραία περιοχή.

   (ϑ′) Αν R είναι ένας μεταθετικός δακτύλιος με μονάδα, που δεν είναι ακεραία περιοχή και I ένα ιδεώδες του R, τότε το πηλίκο R/I δεν μπορεί να είναι ακεραία περιοχή.

   (ι′) Κάθε υποδακτύλιος του $\mathbb{Z} \times \mathbb{Z}$ είναι και ιδεώδες του.

   (ια′) Ένας δακτύλιος R/I είναι μεταθετικός αν και μόνον αν $rs - sr \in I$ για κάθε $r, s \in I$.

Απάντησεις:

(α′) i. Σωστό. Ισχύει ότι

$$\begin{aligned}\phi(f(x) + g(x)) &= \phi((f + g)(x)) \\ &= (f + g)'(x) \\ &= f'(x) + g'(x) \text{ για κάθε } f(x), g(x) \in R.\end{aligned}$$

ii. Λάθος, διότι

$$\begin{aligned}\phi(f(x)\cdot g(x)) &= \phi((f\cdot g)(x))\\ &= (f\cdot g)'(x)\\ &= f'(x)\cdot g(x) + f(x)\cdot g'(x) \text{ για κάθε } f(x), g(x)\in R,\end{aligned}$$

ενώ $\phi(f(x))\cdot\phi(g(x)) = f'(x)\cdot g'(x)$.

(β΄) Λάθος. Θεωρούμε τον ομομορφισμό $\phi : \mathbb{Z}\to\mathbb{Q}$ με $\phi(n) = n$ για κάθε $n\in\mathbb{Z}$. Το $2\mathbb{Z}$ είναι ιδεώδες του $\mathbb{Z}$ αλλά το $\phi(2\mathbb{Z}) = 2\mathbb{Z}$ δεν είναι ιδεώδες του $\mathbb{Q}$. Πράγματι, αν ήταν ιδεώδες θα έπρεπε για κάθε $x\in 2\mathbb{Z}$ και για κάθε $q\in\mathbb{Q}$ να έπεται $qx\in 2\mathbb{Z}$. Για $x = 2$ και $q = \frac{1}{2}$ όμως έχουμε $qx = 1\notin 2\mathbb{Z}$. Άτοπο.

(γ΄) Σωστό. Γνωρίζουμε ότι $Im\phi$ είναι υποδακτύλιος του S. Για να δείξουμε ότι το $\phi(I)$ είναι ιδεώδες του $Im\phi$ αρκεί να δείξουμε ότι $yw, wy\in\phi(I)$ για κάθε $y\in Im\phi$ και για κάθε $w\in\phi(I)$. Έστω λοιπόν $y\in Im\phi$ και $w\in\phi(I)$, τότε υπάρχει ένα $x\in R$ και ένα $a\in I$ ώστε $\phi(x) = y$ και $\phi(a) = w$. Καθώς το I είναι ιδεώδες του R έπεται ότι $xa\in I$ και $ax\in I$. Συνεπώς $yw = \phi(x)\phi(a) = \phi(xa)\in\phi(I)$ και $wy = \phi(a)\phi(x) = \phi(ax)\in\phi(I)$.

(δ΄) Σωστό. Η απόδειξη είναι απλή εφαρμογή των ορισμών.

(ε΄) Λάθος. Αν το $\mathbb{Q}$ ήταν ιδεώδες του $\mathbb{R}$ τότε θα έπρεπε $xq\in\mathbb{Q}$ για κάθε $x\in\mathbb{R}$ και για κάθε $q\in\mathbb{Q}$. Για $x = \frac{\sqrt{2}}{3}$ και $q = 3$ όμως έχουμε $xq = \sqrt{2}\notin\mathbb{Q}$.

(ϛ΄) Σωστό. Ορίζουμε $\phi : \mathbb{Z}\to\mathbb{Z}_n$ με $\phi(a) = a(modn)$ για κάθε $a\in\mathbb{Z}$. Η ϕ είναι καλά ορισμένη. Επιπλέον είναι ομομορφισμός, αφού για κάθε $a, b\in\mathbb{Z}$ έχουμε:

$$\begin{aligned}\phi(a+b) &= (a+b)\ (modn)\\ &= (a\ modn) + (b\ modn)\\ &= \phi(a) + \phi(b)\end{aligned}$$

και

$$\begin{aligned}\phi(ab) &= ab\ (modn)\\ &= (a\ modn)(b\ modn)\\ &= \phi(a)\phi(b).\end{aligned}$$

Η ϕ είναι προφανώς επί και άρα $Im\phi = \mathbb{Z}_n$. Ας υπολογίσουμε και τον

πυρήνα

$$\begin{aligned} ker\phi = \{a \in \mathbb{Z} : \phi(a) = 0 \ mod n\} &= \{a \in \mathbb{Z} : a \ mod n = 0 \ mod n\} \\ &= \{a \in \mathbb{Z} : n \mid a\} \\ &= \{a \in \mathbb{Z} : \exists k \in \mathbb{Z} \text{ με } a = kn\} \\ &= \{kn : k \in \mathbb{Z}\} \\ &=< n > \text{ ή με άλλο συμβολισμό } n\mathbb{Z} \end{aligned}$$

Από το πρώτο θεώρημα ισομορφισμών έχουμε $\mathbb{Z}/n\mathbb{Z} \cong Im\phi = \mathbb{Z}_n$.

(ζ′) Λάθος. Το $\mathbb{Z}$ είναι μια ακεραία περιοχή που δεν είναι σώμα. Το πηλίκο όμως $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$ είναι σώμα.

(η′) Λάθος. Το $\mathbb{Z}$ είναι μια ακεραία περιοχή. Το πηλίκο όμως $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$ δεν είναι.

(ϑ′) Λάθος. Ο δακτύλιος $\mathbb{Z} \times \mathbb{Z}$ είναι μεταθετικός με μονάδα και το πηλίκο $\mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \{0\} \cong \mathbb{Z}$ είναι ακεραία περιοχή.

(ι′) Λάθος. Ο $S = \{(n, n) : n \in \mathbb{N}\}$ είναι υποδακτύλιος (γιατί;) αλλά όχι ιδεώδες αφού $(2, 1)(5, 5) = (10, 5) \notin S$.

(ια′) Σωστό. Ο δακτύλιος R/I είναι μεταθετικός αν και μόνον αν για κάθε $r, s \in R$

$$\begin{aligned} (r + I)(s + I) = (s + I)(r + I) &\Leftrightarrow rs + I = sr + I \\ &\Leftrightarrow rs - sr \in I \end{aligned}$$

Άννα Καρασούλου

8. **[Άσκηση 8]** Αν $n, m \in \mathbb{Z}$ με μκδ$(m, n) = 1$, να δείξετε ότι οι δακτύλιοι $\mathbb{Z}_n \times \mathbb{Z}_m$ και $\mathbb{Z}_{nm}$ είναι ισόμορφοι.

Απάντηση: Ορίζουμε $\phi : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ με

$$\phi(a \mod nm) = (a \mod n \ , \ a \mod m)$$

για κάθε $a \mod nm \in \mathbb{Z}_{nm}$. Θα δείξουμε ότι η ϕ είναι ισομορφισμός.

Η ϕ είναι καλά ορισμένη: Αν $a \mod nm = b \mod nm$, τότε $nm \mid b - a$. Καθώς μκδ$(m, n) = 1$, έπεται ότι $n \mid b - a$ και $m \mid b - a$, ισοδύναμα $a \mod n = b \mod n$ και $a \mod m = b \mod m$.

Η ϕ είναι ομομορφισμός: Πράγματι,

$$\begin{aligned}\phi(a \mod nm + b \mod nm) &= \phi(a+b \mod nm)\\ &= (a+b \mod n\ ,\ a+b \mod m)\\ &= (a \mod n\ ,\ a \mod m) + (b \mod n\ ,\ b \mod m)\\ &= \phi(a \mod nm) + \phi(b \mod nm).\end{aligned}$$

και

$$\begin{aligned}\phi(a \mod nm \cdot b \mod nm) &= \phi(ab \mod nm)\\ &= (ab \mod n\ ,\ ab \mod m)\\ &= (a \mod n\ ,\ a \mod m)(b \mod n\ ,\ b \mod m)\\ &= \phi(a \mod nm)\phi(b \mod nm).\end{aligned}$$

Η ϕ είναι 1-1: Έστω $a \mod nm\ ,\ b \mod nm \in \mathbb{Z}_{nm}$ με

$$\phi(a \mod nm) = \phi(b \mod nm),$$

τότε $(a \mod n\ ,\ a \mod m) = (b \mod n\ ,\ b \mod m)$ που σημαίνει ότι $a = b \mod n$ και $a = b \mod m$. Συνεπώς $n \mid b-a$ και $m \mid b-a$. Καθώς μκδ$(m,n) = 1$, έπεται ότι $nm \mid b-a$ και άρα $a = b \mod n$.

Η ϕ είναι επί: Προφανές αφού είναι 1-1 και τα σύνολα $\mathbb{Z}_n \times \mathbb{Z}_m$ και $\mathbb{Z}_{nm}$ είναι ισοπληθικά.

Παρατήρηση. Το πλήθος των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_{nm}$ είναι ίσο με το πλήθος των αντιστρέψιμων στοιχείων του $\mathbb{Z}_n \times \mathbb{Z}_m$. Λόγω της πολλαπλασιαστικότητας της συναρτησης του *Euler* έχουμε όμως ότι το πλήθος των αντιστρέψιμων στοιχείων του $\mathbb{Z}_n \times \mathbb{Z}_m$ είναι το γινόμενο του πλήθους των αντιστρέψιμων στοιχείων του $\mathbb{Z}_n$ επί του πλήθους των αντιστρέψιμων στοιχείων του $\mathbb{Z}_m$, συμβολικά

$$|U(\mathbb{Z}_{nm})| = |U(\mathbb{Z}_n)||U(\mathbb{Z}_m)|.$$

Κωνσταντίνος Λέντζος

9. **[Άσκηση 9]** Έστω R δακτύλιος και I ένα ιδεώδες του. Να δείξετε ότι

$$R[x]/I[x] \cong (R/I)[x].$$

Απάντηση: Ορίζουμε μια συνάρτηση $\phi : R[x] \to (R/I)[x]$ με

$$\phi(a_n x^n + \cdots + a_1 x + a_0) = (a_n + I)x^n + \cdots + (a_1 + I)x + (a_0 + I)$$

Μπορούμε επίσης να θεωρήσουμε τον φυσικό επιμορφισμό $\pi : R \to R/I$ όπου

$$\pi(r) = r + I, \text{ για κάθε } r \in R.$$

Τότε

$$\phi(a_n x^n + \cdots + a_1 x + a_0) = \pi(a_n)x^n + \cdots + \pi(a_1)x_1 + \pi(a_0).$$

Η ϕ είναι ομομορφισμός: Έστω $f(x) = a_n x^n + \cdots + a_1 x + a_0$ και $g(x) = b_n x^n + \cdots + a_1 x + a_0 \in R[x]$. Τα πολυώνυμα δεν έχουν απαραίτητα τον ίδιο βαθμό, αλλά μπορούμε εισάγοντας μερικούς μηδενικούς συντελεστές να υποθέσουμε ότι έχουν την παραπάνω μορφή. Υπολογίζουμε

$$\begin{aligned}
\phi(f(x) + g(x)) &= \phi((f+g)(x)) \\
&= \phi((a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0)) \\
&= \pi(a_n + b_n)x^n + \cdots + \pi(a_1 + b_1)x + \pi(a_0 + b_0) \\
&= [\pi(a_n) + \pi(b_n)]x^n + \cdots + [\pi(a_1) + \pi(b_1)]x + [\pi(a_0) + \pi(b_0)] \\
&= [\pi(a_n)x^n + \cdots + \pi(a_1)x + \pi(a_0)] + [\pi(b_n)x^n + \cdots + \pi(b_1)x + \pi(b_0)] \\
&= \phi(a_n x^n + \cdots + a_1 x + a_0) + \phi(b_n x^n + \cdots + b_1 x + b_0) \\
&= \phi(f(x)) + \phi(g(x)).
\end{aligned}$$

$$\begin{aligned}
\phi(f(x)g(x)) &= \phi((a_n b_n)x^n + \cdots + (a_1 b_0 + a_0 b_1)x + (a_0 b_0)) \\
&= \pi(a_n b_n)x^n + \cdots + \pi(a_1 b_0 + a_0 b_1)x + \pi(a_0 b_0) \\
&= \pi(a_n)\pi(b_n)x^n + \cdots + [\pi(a_1)\pi(b_0) + \pi(a_0)\pi(b_1)]x + \pi(a_0)\pi(b_0) \\
&= [\pi(a_n)x^n + \cdots + \pi(a_1)x + \pi(a_0)][\pi(b_n)x^n + \cdots + \pi(b_1)x + \pi(b_0)] \\
&= \phi(f(x))\phi(g(x)).
\end{aligned}$$

Η ϕ είναι επί: Αρκεί να δείξουμε ότι για κάθε

$$(a_n + I)x^n + \cdots + (a_1 + I)x + (a_0 + I) \in (R/I)[x],$$

υπάρχει πολυώνυμο $f(x) \in R[x]$ ώστε

$$\phi(f(x)) = (a_n + I)x^n + \cdots + (a_1 + I)x + (a_0 + I).$$

Έύκολα φαίνεται ότι για $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ έχουμε το επιθυμητό και άρα $Im\phi = (R/I)[x]$.

Ισχυριζόμαστε ότι $ker\phi = I[x]$: Υπολογίζουμε

$$\begin{aligned} ker\phi &= \{f(x) \in R[x] : \phi(f(x)) = 0 \in (R/I)[x]\} \\ &= \{f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x] : a_i \in I \ \forall i\} \\ &= I[x] \end{aligned}$$

Σημείωση. Το $I[x]$ είναι ιδεώδες του $R[x]$ ως πυρήνας του ομομορφισμού ϕ.

Από το πρώτο θεώρημα ισομορφισμών έχουμε

$$R[x]/I[x] \cong Im\phi = (R/I)[x].$$

Κωνσταντίνος Λέντζος

10. [**Άσκηση 10**] Δίνεται το ιδεώδες

$$I = \{f(x) \in \mathbb{R}[x] : f(1) = f(2) = 0\} \trianglelefteq \mathbb{R}[x]$$

Δείξτε ότι $\mathbb{R}[x]/I \cong \mathbb{R} \times \mathbb{R}$.

Απάντηση: Το ιδεώδες I περιέχει όλα τα πολυώνυμα με πραγματικούς συντελεστές, τα οποία έχουν ως ρίζες το 1 και το 2. Συνεπώς ένα πολυώνυμο $f(x)$ ανήκει στο I αν και μόνον αν $(x-1) \mid f(x)$ και $(x-2) \mid f(x)$. Τα πολυώνυμα $x-1$ και $x-2$ όμως είναι πρώτα μεταξύ τους και άρα $f(x) \in I$ αν και μόνον αν $(x-1)(x-2) \mid f(x)$, δηλαδή αν και μόνον αν υπάρχει κάποιο $a(x) \in \mathbb{R}[x]$ ώστε $f(x) = a(x)(x-1)(x-2)$. Έτσι λοιπόν

$$I = < (x-1)(x-2) > = < x^2 - 3x + 2 >.$$

Οπότε ισοδύναμα θα μπορούσε η άσκηση να ζητάει να δείξουμε ότι

$$\mathbb{R}[x]/ < x^2 - 3x + 2 > \cong \mathbb{R} \times \mathbb{R}.$$

Θεωρούμε $\phi : \mathbb{R}[x] \to \mathbb{R} \times \mathbb{R}$ με

$$\phi(f(x)) = (f(1), f(2)) \text{ για κάθε } f(x) \in \mathbb{R}[x].$$

Η ϕ είναι καλά ορισμένη: Είναι προφανές.

Η ϕ είναι ομομορφισμός: Έστω $f(x), g(x) \in \mathbb{R}[x]$. Υπολογίζουμε

$$\begin{aligned}\phi(f(x)+g(x)) &= \phi((f+g)(x)) \\ &= ((f+g)(1),(f+g)(2)) \\ &= (f(1)+g(1), f(2)+g(2)) \\ &= (f(1),f(2))+(g(1),g(2)) \\ &= \phi(f(x))+\phi(g(x)).\end{aligned}$$

Επίσης

$$\begin{aligned}\phi(f(x)g(x)) &= \phi((fg)(x)) \\ &= ((fg)(1),(fg)(2)) \\ &= (f(1)g(1), f(2)g(2)) \\ &= (f(1),f(2))(g(1),g(2)) \\ &= \phi(f(x))\phi(g(x)).\end{aligned}$$

Η ϕ είναι επί: Αρκεί για κάθε $(a,b) \in \mathbb{R}\times\mathbb{R}$ να βρούμε ένα πολυώνυμο $f(x) \in \mathbb{R}[x]$ ώστε $\phi(f(x)) = (a,b)$ ή ισοδύναμα $f(1) = a$ και $f(2) = b$. Για

$$f(x) = (x-1)b + (2-x)a \in \mathbb{R}[x]$$

έχουμε το επιθυμητό και άρα $Im\phi = \mathbb{R}\times\mathbb{R}$.

$ker\phi = I$: Υπολογίζουμε

$$\begin{aligned}ker\phi &= \{f(x) \in \mathbb{R}[x] : \phi(f(x)) = (0,0) \in \mathbb{R}\times\mathbb{R}\} \\ &= \{f(x) \in \mathbb{R}[x] : (f(1),f(2)) = (0,0)\} \\ &= \{f(x) \in \mathbb{R}[x] : f(1) = 0, f(2) = 0\} \\ &= I.\end{aligned}$$

Από το πρώτο θεώρημα ισομορφισμών έχουμε

$$\mathbb{R}[x]/I \cong Im\phi = \mathbb{R}\times\mathbb{R}.$$

Άννα Καρασούλου

11. **[Άσκηση 11]** Για κάθε $m,n \in \mathbb{Z}$ ισχύει $\mathbb{Z}_{nm}/ < n > \cong \mathbb{Z}_n$

Απάντηση: Ορίζουμε $\phi : \mathbb{Z}_{nm} \to \mathbb{Z}_n$ με

$$\phi(a \mod nm) = a \mod n.$$

Η ϕ είναι καλά ορισμένη: Αν υποθέσουμε ότι

$$a \mod nm = b \mod nm,$$

τότε $nm \mid b - a$ και άρα υπάρχει κάποιο $k \in \mathbb{Z}$ ώστε $b - a = knm$. Έτσι $n \mid b - a$ που σημαίνει ότι $a \mod n = b \mod n$.

Η ϕ είναι ομομορφισμός: Για κάθε $a \mod nm$, $b \mod mn \in \mathbb{Z}_{nm}$ έχουμε

$$\begin{aligned}\phi(a \mod nm + b \mod nm) &= \phi(a + b \mod nm)\\ &= a + b \mod n\\ &= a \mod n + b \mod n\\ &= \phi(a \mod nm) + \phi(b \mod nm)\end{aligned}$$

$$\begin{aligned}\phi(a \mod nm \cdot b \mod nm) &= \phi(ab \mod nm)\\ &= ab \mod n\\ &= (a \mod n) \cdot (b \mod n)\\ &= \phi(a \mod nm) \cdot \phi(b \mod nm)\end{aligned}$$

Η ϕ είναι επί: Αρκεί να δείξουμε ότι για κάθε $y \mod n \in \mathbb{Z}_n$ υπάρχει $x \mod nm \in \mathbb{Z}_{nm}$ ώστε $\phi(x \mod nm) = y \mod n$. Θεωρώντας $x \mod mn = y \mod mn$ έχουμε το επιθυμητό και άρα $Im\phi = \mathbb{Z}_n$.

$ker\phi =< n >$: Υπολογίζουμε

$$\begin{aligned}ker\phi &= \{a \mod nm \in \mathbb{Z}_{nm} : \phi(a \mod nm) = 0 \mod n\}\\ &= \{a \mod nm \in \mathbb{Z}_{nm} : a \mod n = 0 \mod n\}\\ &= \{a \mod nm \in \mathbb{Z}_{nm} : n \mid a\}\\ &= \{a \mod nm \in \mathbb{Z}_{nm} : \exists k \in \mathbb{Z} \text{ με } a = kn\}\\ &= \{kn \mod nm \in \mathbb{Z}_{nm} : k \in \mathbb{Z}\}\\ &= < n > \trianglelefteq \mathbb{Z}_{nm}.\end{aligned}$$

Από το πρώτο θεώρημα ισομορφισμών έχουμε

$$\mathbb{Z}_{nm}/ < n > \cong Im\phi = \mathbb{Z}_n.$$

Άννα Καρασούλου

12. [**Άσκηση 12**] Δείξτε ότι

$$\mathbb{Z} \times \mathbb{Z}/(< n > \times < m >) \cong \mathbb{Z}_n \times \mathbb{Z}_m.$$

Απάντηση: Ορίζουμε $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_n \times \mathbb{Z}_m$ με

$$\phi(a, b) = (a \mod n \ , \ b \mod m \text{ για κάθε } (a, b) \in \mathbb{Z} \times \mathbb{Z}.$$

Η ϕ είναι καλά ορισμένη: Αν υποθέσουμε ότι $a_1 = a_2$ και ότι $b_1 = b_2$, τότε προφανώς

$$a_1 \mod n \ = \ a_2 \mod n$$

και

$$b_1 \mod m \ = \ b_2 \mod n$$

και άρα $\phi(a_1, b_1) = \phi(a_2, b_2)$.

Η ϕ είναι ομομορφισμός: Για κάθε $(a_1, b_1), (a_2, b_2) \in \mathbb{Z} \times \mathbb{Z}$ έχουμε

$$\begin{aligned}
\phi((a_1, b_1) + (a_2, b_2)) &= \phi((a_1 + a_2, b_1 + b_2)) \\
&= (a_1 + a_2 \mod n \ , \ b_1 + b_2 \mod m) \\
&= (a_1 \mod n \ , \ b_1 \mod m) + (a_2 \mod n \ , \ b_2 \mod m) \\
&= \phi(a_1, b_1) + \phi(a_2, b_2)
\end{aligned}$$

$$\begin{aligned}
\phi((a_1, b_1)(a_2, b_2)) &= \phi((a_1 a_2, b_1 b_2)) \\
&= (a_1 a_2 \mod n \ , \ b_1 b_2 \mod m) \\
&= (a_1 \mod n \ , \ b_1 \mod m)(a_2 \mod n \ , \ b_2 \mod m) \\
&= \phi(a_1, b_1)\phi(a_2, b_2)
\end{aligned}$$

Η ϕ είναι επί: Αρκεί να δείξουμε ότι για κάθε $(x \mod n \ , \ y \mod m) \in \mathbb{Z}_n \times \mathbb{Z}_m$ υπάρχει $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ ώστε $\phi(a, b) = (x \mod n \ , \ y \mod m)$. Θεωρώντας για $(a, b) = (x, y)$ έχουμε το επιθυμητό και άρα $Im\phi = \mathbb{Z}_n \times \mathbb{Z}_m$.

$ker\phi =< n > \times < m >$: Υπολογίζουμε

$$
\begin{aligned}
ker\phi &= \{(a,b) \in \mathbb{Z}\times\mathbb{Z} : \phi(a,b) = (0 \mod n\ ,\ 0 \mod m)\} \\
&= \{(a,b) \in \mathbb{Z}\times\mathbb{Z} : (a \mod n\ ,\ b \mod m) = (0 \mod n\ ,\ 0 \mod m)\} \\
&= \{a \mod nm \in \mathbb{Z}_{nm} : n \mid a \text{ και } m \mid b\} \\
&= \{a \mod nm \in \mathbb{Z}_{nm} : \exists k,l \in \mathbb{Z} \text{ με } a = kn \text{ και } b = lm\} \\
&= \{(kn, lm) \in \mathbb{Z}\times\mathbb{Z} : k,l \in \mathbb{Z}\} \\
&= < n > \times < m > .
\end{aligned}
$$

Από το πρώτο θεώρημα ισομορφισμών έχουμε

$$\mathbb{Z}\times\mathbb{Z}/(< n > \times < m >) \cong Im\phi = \mathbb{Z}_n \times \mathbb{Z}_m.$$

Κωνσταντίνος Λέντζος

13. **[Άσκηση 13]** Να αποδειχθεί ότι :

   (α′) $a \cdot b = 0 \Leftrightarrow a = 0$ ή $b = 0, a, b \in \mathbb{Z}$.

   (β′) Ισχύει το ίδιο αν: $[a], [b] \in \mathbb{Z}_6$;

   Απάντηση:

   (α′) Θα το αποδείξουμε με απαγωγή σε άτοπο. Έστω ότι είναι $a \cdot b = 0$ και $a \neq 0$ και $b \neq 0$ τότε από θα ισχύει ακριβώς ένα από τα εξής:

$$
\begin{aligned}
a < 0, b < 0 &\Rightarrow a \cdot b > 0 \\
a < 0, b > 0 &\Rightarrow a \cdot b < 0 \\
a > 0, b > 0 &\Rightarrow a \cdot b > 0 \\
a > 0, b < 0 &\Rightarrow a \cdot b < 0
\end{aligned}
$$

   Δηλαδή γενικά θα είναι : $a \cdot b \neq 0$, άτοπο! Ομοίως και το αντίστροφο.

   (β′) Αν $[a], [b] \in \mathbb{Z}_6$, τότε

$$[2] \cdot [3] = [6] = [0].$$

   Πώς ονομάζεται ένας δακτύλιος με την ιδιότητα Ι;

Σωτήρης Δ. Χασάπης

14. **[Άσκηση 14]**

(α′) Δείξτε ότι το $x-2$ διαιρεί το $f(x)=x^{23}+3x^{12}+6x+1$ στο $\mathbb{Z}_{11}[x]$.

(β′) Δείξτε ότι το $(x-1)(x-2)$ διαιρεί το $f(x)=x^{23}+3x^{12}+6x+1$ στο $\mathbb{Z}_{11}[x]$.

Απάντηση:

(α′) Γνωρίζουμε ότι το πολυώνυμο $(x-2)$ διαιρεί το $f(x)$ αν και μόνο αν το 2 είναι ρίζα του $f(x)$, δηλαδή $f(2)=0 \mod 11$, ισοδύναμα

$$2^{23}+3\cdot 2^{12}+6\cdot 2+1=0 \mod 11.$$

Ο 11 είναι πρώτος και άρα $\phi(11)=11-1=10$, όπου ϕ η συνάρτηση του Euler. Επιπλέον μκδ$(2,11)=1$ και συνεπώς από το θεώρημα του Euler παίρνουμε ότι $2^{\phi(11)}=1 \mod 11$ ή ισοδύναμα $2^{10}=1 \mod 11$. Ας υπολογίσουμε τώρα κάθε προσθεταίο του $f(2)$ ξεχωριστά:

$$2^{23}=(2^{10})^2\cdot 2^3 \mod 11 = 1\cdot 8 \mod 11 = 8 \mod 11 \qquad (1)$$

$$\begin{aligned} 3\cdot 2^{12} &= 3\cdot(2^{10})\cdot 2^2 && \mod 11\\ &= 3\cdot 1\cdot 2^2 && \mod 11\\ &= 3\cdot 4 && \mod 11\\ &= 12 && \mod 11\\ &= 1 && \mod 11 \end{aligned} \qquad (2)$$

$$6\cdot 2 \mod 11 = 12 \mod 11 = 1 \mod 11 \qquad (3)$$

Από τις (1),(2) και (3) έχουμε ότι

$$\begin{aligned} f(2)=2^{23}+3\cdot 2^{12}+6\cdot 2+1 &= (8+1+1+1) && \mod 11\\ &= 11 && \mod 11\\ &= 0 && \mod 11 \end{aligned}$$

και άρα το $(x-2)$ διαιρεί το $f(x)$.

(β′) Κατα αρχήν παρατηρούμε ότι το πολυώνυμο $(x-1)$ διαιρεί το $f(x)$ αφού $f(1)=0$, πράγματι

$$\begin{aligned} f(1) &= 1^{23}+3\cdot 1^{12}+6\cdot 1+1 && \mod 11\\ &= 11 && \mod 11\\ &= 0 && \mod 11 \end{aligned}$$

Εφόσον το $(x-1)$ διαιρεί το $f(x)$ και από προηγούμενο ερώτημα το $(x-2)$ διαιρεί επίσης το $f(x)$, παίρνουμε ότι

$$(x-1)\cdot(x-2) \mid f(x),$$

αφού μκδ$(x-1, x-2) = 1$.

Μηλίγκου Κωνσταντίνα

15. **[Άσκηση 15]** Θεωρούμε τον δακτύλιο $R = \{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R}\}$ και το ιδεώδες αυτού $I = \{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R}\}$. Να δείξετε ότι ο αντίστοιχος δακτύλιος πηλίκο R/I είναι σώμα.

Απάντηση: Ορίζουμε $\phi : R \to \mathbb{R}$ με

$$\phi(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}) = a, \text{ για κάθε } \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R.$$

Η ϕ είναι καλά ορισμένη: Αν υποθέσουμε ότι $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix} \in R$

$$\text{με } \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix},$$

τότε $a = a'$ και συνεπώς

$$\phi(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}) = \phi(\begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix})$$

Η ϕ είναι ομομορφισμός: Για κάθε $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix} \in R$ έχουμε

$$\begin{aligned} \phi(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix}) &= \phi(\begin{pmatrix} a+a' & b+b' \\ 0 & a+a' \end{pmatrix}) \\ &= a + a' \\ &= \phi(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}) + \phi(\begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix}) \end{aligned}$$

$$\begin{aligned} \phi(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix}) &= \phi(\begin{pmatrix} aa' & ab'+ba' \\ 0 & aa' \end{pmatrix}) \\ &= aa' \\ &= \phi(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix})\phi(\begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix}) \end{aligned}$$

Η ϕ είναι επί: Αρκεί να δείξουμε ότι για κάθε $y \in \mathbb{R}$ υπάρχει πίνακας

$$A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R$$

ώστε $\phi(A) = y$. Θεωρώντας για $A = \begin{pmatrix} y & 2008 \\ 0 & y \end{pmatrix}$ έχουμε το επιθυμητό και άρα $Im\phi = \mathbb{R}$.

$\underline{ker\phi = I}$: Υπολογίζουμε

$$ker\phi = \{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R : \phi(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = 0 \in \mathbb{R}\}$$

$$= \{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R : a = 0\}$$

$$= \{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R}\}$$

$$= I$$

Από το πρώτο θεώρημα ισομορφισμών έχουμε

$$R/ker\phi = R/I \cong Im\phi = \mathbb{R}.$$

Έτσι ο δακτύλιος R/I είναι σώμα αφού είναι ισόμορφος με το σώμα $\mathbb{R}$.

Κωνσταντίνος Λέντζος

16. **[Άσκηση 16]**

Θεωρούμε τον δακτύλιο $R = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R}\}$ και το ιδεώδες αυτού $I = \{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R}\}$. Να δείξετε ότι ο αντίστοιχος δακτύλιος πηλίκο R/I είναι ισόμορφος με τον $\mathbb{R} \times \mathbb{R}$.

Απάντηση: Ορίζουμε $\phi : R \to \mathbb{R} \times \mathbb{R}$ με

$$\phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) = (a, c), \text{ για κάθε } \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R.$$

Η ϕ είναι καλά ορισμένη: Αν υποθέσουμε ότι $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \in R$

$$\text{με } \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix},$$

τότε $a = a'$, $c = c'$ και άρα $(a, a') = (c, c')$ που σημαίνει ότι

$$\phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) = \phi(\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix})$$

Η ϕ είναι ομομορφισμός: Για κάθε $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \in R$ έχουμε

$$\begin{aligned} \phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}) &= \phi(\begin{pmatrix} a+a' & b+b' \\ 0 & c+c' \end{pmatrix}) \\ &= (a+a', c+c') \\ &= (a, c) + (a', c') \\ &= \phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) + \phi(\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}) \end{aligned}$$

$$\begin{aligned} \phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}) &= \phi(\begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix}) \\ &= (aa', cc') \\ &= (a, c) \cdot (a', c') \\ &= \phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix})\phi(\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}) \end{aligned}$$

Η ϕ είναι επί: Αρκεί να δείξουμε ότι για κάθε $(x, y) \in \mathbb{R} \times \mathbb{R}$ υπάρχει πίνακας

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R$$

ώστε $\phi(A) = (x, y)$. Θεωρώντας για $A = \begin{pmatrix} x & 2008 \\ 0 & y \end{pmatrix}$ έχουμε το επιθυμητό και άρα $Im\phi = \mathbb{R} \times \mathbb{R}$.

$ker\phi = I$: Υπολογίζουμε

$$ker\phi = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R : \phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (0,0)\}$$

$$= \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in R : (a,c) = (0,0)\}$$

$$= \{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{R}\}$$

$$= I$$

Από το πρώτο θεώρημα ισομορφισμών έχουμε

$$R/ker\phi = R/I \cong Im\phi = \mathbb{R} \times \mathbb{R}.$$

Σημείωση. Ο δακτύλιος $\mathbb{R} \times \mathbb{R}$ δεν είναι ακεραία περιοχή διότι αν ήταν θα έπρεπε για κάθε $(x,y),(x',y') \in \mathbb{R} \times \mathbb{R}$ με $(x,y) \cdot (x',y') = (0,0)$ να συνεπάγεται $(x,y) = (0,0)$ ή $(x',y') = (0,0)$. Για τα στοιχεία όμως $(1,0)$ και $(0,1)$ έχουμε

$$(1,0) \cdot (0,1) = (1 \cdot 0, 0 \cdot 1) = (0,0),$$

αλλά ούτε $(1,0) = (0,0)$, ούτε $(0,1)=(0,0)$. Έτσι ο δακτύλιος $R/I \cong \mathbb{R} \times \mathbb{R}$ δεν είναι ακεραία περιοχή και ως εκ τούτου δεν είναι και σώμα.

Κωνσταντίνος Λέντζος

17. **[Άσκηση 17]**

Έστω ο δακτύλιος των πινάκων $(\mathbb{R}^{2\times 2}, +, \cdot)$. Να βρεθούν τα ιδεώδη του.

Απάντηση: Την απάντηση θα τη βρείτε στο βίντεο εδώ ή εδώ

Σχόλια Σε προηγούμενες ασκήσεις θεωρούσαμε ως δακτυλίους όχι $(\mathbb{R}^{2\times 2}, +, \cdot)$ αλλά κάποιους υποδακτυλίους Δείτε επίσης και το σχόλιο στο τέλος του βίντεο σχετικά με ομομορφισμούς δακτυλίων της μορφής $(\mathbb{R}^{2\times 2}, +, \cdot) \longrightarrow R$. Εδώ ο πυρήνας του ομομορφισμού έχει δύο επιλογές και έτσι στην πραγματικότητα έχουμε δύο ομομορφισμούς. Σκεφθείτε αν έχουμε παρόμοια κατάσταση για άλλους δακτυλίους

Ευάγγελος Ράπτης

18. **[Άσκηση 18]** Να βρεθούν σώματα F, E και ομομορφισμός $\phi : F \to E$ ώστε ο ϕ να μην είναι 1-1.

Απάντηση: Καλούνται οι φοιτητές να συμμετάσχουν μέσω του συνδέσμου "κουβέντα" της ηλεκτρονικής τάξης.

Προσεχώς λεπτομέρειες!

Άννα Καρασούλου

19. **[Άσκηση 19]** Θεωρούμε το σύνολο των θετικών ρητών, έστω G και το εφοδιάζουμε με μία πράξη

$$* : G \times G \to G$$

που ορίζεται ως εξής:

$$a * b = \frac{ab}{2}.$$

Να δειχθεί ότι το σύνολο των θετικών ρητών εφοδιασμένο με την παραπάνω πράξη είναι ομάδα. Ποιο είναι το ουδέτερο στοιχείο της ομάδας αυτής;

Απάντηση: Καλούνται οι φοιτητές να συμμετάσχουν μέσω του συνδέσμου "κουβέντα" της ηλεκτρονικής τάξης.

Προσεχώς λεπτομέρειες!

Άννα Καρασούλου

20. **[Άσκηση 20]** Έστω R μια ακεραία περιοχή και $a \in R$. Να δείξετε ότι

$$< a >=< ua >, \text{ για κάθε } u \in U(R).$$

Με $U(R)$ συμβολίζουμε τα αντιστρέψιμα στοιχεία του δακτυλίου R.

Απάντηση: Έστω u ένα αντιστρέψιμο στοιχείο του R. Θα δείξουμε τους δύο εγκλεισμούς.

$\underline{< a > \subseteq < ua >}$: Αρκεί να δείξουμε ότι $a \in < ua >$, δηλαδή αρκεί να δείξουμε ότι υπάρχει $r \in R$ ώστε $a = r(ua)$. Το u είναι αντριστρέψιμο στοιχείο και συνεπώς θεωρώντας για $r = u^{-1}$ έχουμε το επιθυμητό.

$\underline{< ua > \subseteq < a >}$: Αρκεί να δείξουμε ότι $ua \in < a >$, δηλαδή αρκεί να δείξουμε ότι υπάρχει $r \in R$ ώστε $ua = ra$. Για $r = u$ έχουμε το επιθυμητό.

Κωνσταντίνος Λέντζος

21. **[Άσκηση 21]** Έστω R ένας μεταθετικός δακτύλιος με μονάδα, $a \in U(R)$ και $r \in R$ με την ιδιότητα να υπάρχει ένα $n \in \mathbb{N}$ ώστε $r^n = 0$. Δείξτε ότι το στοιχείο $1 - r$ είναι αντιστρέψιμο.

Απάντηση: Από υπόθεση υπάρχει ένα $n \in \mathbb{N}$ ώστε $r^n = 0$ και άρα

$$1 = 1 - r^n = (1 - r)(1 + r + ... + r^{n-1})$$

Έτσι το $1 - r$ είναι αντιστρέψιμο και μάλιστα

$$(1 - r)^{-1} = 1 + r + ... + r^{n-1}.$$

Κωνσταντίνος Λέντζος

22. **[Άσκηση 22]** Τι μορφή έχουν οι υποδακτύλιοι του $\mathbb{Z}$;

Απάντηση: Εύκολα επιβεβαιώνουμε ότι για κάθε n το υποσύνολο $n\mathbb{Z} \subseteq \mathbb{Z}$ αποτελεί υποδακτύλιο του $\mathbb{Z}$ (γιατί;). Εστω τώρα S ένας υποδακτυλιος του $\mathbb{Z}$. Θα δείξουμε ότι ο S είναι της μορφής $n\mathbb{Z}$ για κάποιο n. Καθώς το S είναι υποδακτύλιος παρατηρούμε ότι για κάθε $w \in S$, έχουμε ότι και το $-w \in S$,

αλλά και το $w + w \in S$. Επαγωγικα λοιπόν δειχνουμε οτι κάθε πολλαπλάσιο του w ανήκει στο S. Θέτουμε $n \in S$, τον ελάχιστο φυσικό αριθμό που περιέχεται στο S. Σύμφωνα με τα παραπάνω $n\mathbb{Z} \subseteq S$. Θα δείξουμε τον άλλον εγκλεισμό τώρα. Έστω $m \in S$ τυχαίο, τότε από την ταυτότητα της διαίρεσης στο $\mathbb{Z}$, έχουμε ότι υπάρχουν $q, r \in \mathbb{Z}$ με

$$m = qn + r \text{ και } 0 \leq r < n.$$

Όπως είπαμε παραπάνω καθώς $n \in S$ έπεται ότι και κάθε πολλαπλάσιο του n θα ανήκει στο S, ειδικότερα το $qn \in S$. Καθώς ο S είναι υποδακτύλιος έπεται ότι $r = m - qn \in S$. Από την ανισότητα $0 \leq r < n$ και τον ορισμό του n, ως τον ελάχιστο φυσικό που περιέχεται στον S, παίρνουμε ότι $r = 0$ και άρα $m = qn \in n\mathbb{Z}$ όπως θέλαμε.

Άννα Καρασούλου

23. [**Άσκηση 23**] Να αποδείξετε ότι τα ιδεώδη του δακτυλίου $\mathbb{Z}$ είναι της μορφής $n\mathbb{Z}$.

Απάντηση: Έστω I ένα μη μηδενικό ιδεώδες του $\mathbb{Z}$ και $n \in I$ ο ελάχιστος μη μηδενικός φυσικός αριθμός που περιέχεται στο I. Θα αποδείξουμε ότι $I = n\mathbb{Z}$. Θα δείξουμε τους δύο εγκλεισμούς.

($\supseteq$) Έχουμε ότι $n \in I$ και καθώς το I είναι ιδεώδες έπεται ότι $an \in I$ για κάθε $a \in \mathbb{Z}$. Συνεπώς $n\mathbb{Z} \subseteq I$.

($\subseteq$) Έστω $m \in I$. Από την ταυτότητα της διαίρεσης στο $\mathbb{Z}$, έχουμε ότι υπάρχουν $q, r \in \mathbb{Z}$ με

$$m = qn + r \text{ και } 0 \leq r < n.$$

Έτσι $r = m - qn \in I$, διότι το I είναι ιδεώδες. Από την ανισότητα $0 \leq r < n$ και τον ορισμό του n, ως τον ελάχιστο φυσικό που περιέχεται στο I, παίρνουμε ότι $r = 0$ και άρα $m = qn \in n\mathbb{Z}$ όπως θέλαμε.

Άννα Καρασούλου

24. [**Άσκηση 24**] Αν F είναι ένα σώμα, τι μορφή έχουν τα ιδεώδη του δακτυλίου $F[x]$;

Απάντηση: Η απόδειξη είναι όμοια με αυτή της άσκησης 23. Προσπαθήστε την!

Άννα Καρασούλου

25. **[Άσκηση 25]** Τι μορφή έχουν τα ιδεώδη του δακτυλίου $\mathbb{Z} \times \mathbb{Z}$;

Απάντηση: Θα δείξουμε ότι τα ιδεώδη του $\mathbb{Z} \times \mathbb{Z}$ είναι της μορφής $n\mathbb{Z} \times m\mathbb{Z}$. Είναι εύκολο να επιβεβαιώσουμε ότι το $n\mathbb{Z} \times m\mathbb{Z}$ είναι ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$ (γιατί;). Έστω τώρα A ένα ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$. Θα δείξουμε ότι το A είναι της μορφής $n\mathbb{Z} \times m\mathbb{Z}$ για κάποιους n, m. Θεωρούμε τις απεικονίσεις $f_1, f_2 : A\mathbb{Z}$ με

$$f_1(x, y) = x \text{ για κάθε } (x, y) \in A$$

και

$$f_2(x, y) = y \text{ για κάθε } (x, y) \in A.$$

Παρατηρούμε ότι $A = f_1(A) \times f_2(A)$. Ισχυριζόμαστε ότι το $f_1(A)$ είναι ιδεώδες του $\mathbb{Z}$. Πράγματι το $f_1(A)$ είναι ένα μη κενό υποσύνολο του $\mathbb{Z}$. Για να δείξουμε ότι είναι ιδεώδες, θεωρούμε $x_1, x_2 \in f_1(A)$ και $r \in \mathbb{Z}$ και θα τσεκάρουμε ότι $x_1 - x_2 \in f_1(A)$ και $rx_1 = x_1 r \in f_1(A)$.

Για να δείξουμε ότι $x_1 - x_2 \in f_1(A)$ αρκεί να βρούμε ένα $(w_1, w_2) \in \mathbb{Z} \times \mathbb{Z}$ ώστε $f_1(w_1, w_2) = x_1 - x_2$. Παρατηρούμε ότι για $(w_1, w_2) = (x_1 - x_1, 0)$ έχουμε το επιθυμητό.

Για να δείξουμε τώρα ότι $rx_1 \in f_1(A)$ αρκεί να βρούμε ένα $(w_1, w_2) \in \mathbb{Z} \times \mathbb{Z}$ ώστε $f_1(w_1, w_2) = rx_1$. Παρατηρούμε ότι για $(w_1, w_2) = (rx_1, 0)$ έχουμε το επιθυμητό.

Όμοια δείχνουμε ότι το $f_2(A)$ είναι ιδεώδες του $\mathbb{Z}$. Γνωρίζουμε όμως τι μορφή έχουν τα ιδεώδη του $\mathbb{Z}$. Συνεπώς υπάρχουν n, m ώστε $f_1(A) = n\mathbb{Z}$ και $f_2(A) = m\mathbb{Z}$ και έτσι $A = n\mathbb{Z} \times m\mathbb{Z}$ οπως θέλαμε.

Σημείωση. Το παραπάνω επιχείρημα δεν δουλεύει για υποδακτυλίους. Πράγματι το υποσύνολο

$$\{(r, r) : r \in \mathbb{Z}\}$$

είναι ένας υποδακτύλιος του $\mathbb{Z}\times\mathbb{Z}$ αλλά δεν είναι της μορφής $S_1\times S_2$, όπου S_1 και S_2 υποδακτύλιοι του $\mathbb{Z}$. Ας μην ξεχνάμε τι μορφή έχουν οι υποδακτύλιοι του $\mathbb{Z}$ (βλ. άσκηση 22). Το παραπάνω σύνολο αποτελεί επίσης παράδειγμα υποδακτυλίου το οποίο δεν είναι ιδεώδες, σε αντίθεση με τον δακτύλιο $\mathbb{Z}$ στον οποίον είδαμε ότι κάθε υποδακτύλιος είναι και ιδεώδες.

Ενδιαφέρον ερώτημα: Τι μορφή έχουν τα ιδεώδη των παρακάτω δακτυλίων; $\mathbb{R}\times\mathbb{R}$, $\mathbb{Q}\times\mathbb{Q}$, $\mathbb{C}\times\mathbb{C}$ και $\mathbb{Z}_7\times\mathbb{Z}_7$

Άννα Καρασούλου

26. **[Άσκηση 26]** Αν R και S είναι δύο μεταθετικοί δακτύλιοι με μονάδα, προσδιορίστε την μορφή των ιδεωδών του δακτυλίου $R\times S$.

Απάντηση: Η απόδειξη είναι όμοια με αυτή της άσκησης 25. Προσπαθήστε την! Δείξτε δηλαδή ότι κάθε ιδεώδες του $R\times S$ είναι της μορφής $I\times J$ για κάποιο I ιδεώδες του R και για κάποιο J ιδεώδες του S.

Ενδιαφέρον ερώτημα: Που χρησιμοποιήθηκε στην απόδειξη ότι οι δακτύλιοι R και S έχουν μονάδα;

Άννα Καρασούλου

27. **[Άσκηση 27]** Να βρεθεί παράδειγμα μεταθετικού δακτυλίου με μονάδα και υποδακτυλίου του, ο οποίος να έχει μονάδα αλλά να είναι διαφορετική από αυτή του δακτυλίου.

Απάντηση: Ο δακτύλιος $\mathbb{Z}\times\mathbb{Z}$ είναι μεταθετικός και τον ρόλο της μονάδας παίζει το στοιχείο $(1,1)\in\mathbb{Z}\times\mathbb{Z}$. Μπορούμε πολύ εύκολα να επιβεβαιώσουμε ότι το υποσύνολο $\mathbb{Z}\times 0$ είναι υποδακτύλιος με μονάδα το $(1,0)$.

Άννα Καρασούλου

28. **[Άσκηση 28]** Ένα στοιχείο $[a]\in\mathbb{Z}_m$ είναι αντιστρέψιμο αν και μόνον αν $\text{μκδ}(a,m)=1$.

Απάντηση: ($\Rightarrow$) Έστω ότι το $[a]$ είναι αντιστρέψιμο, τότε υπάρχει $[b]\in\mathbb{Z}_m$ ώστε $[a][b]=[1]$ και άρα $m\mid ab-1$, που σημαίνει ότι υπάρχει κάποιος $n\in\mathbb{Z}$ ώστε $ab=mn+1$ ή $ab+m(-n)=1$. Από το δέκατο υποερώτημα όμως της άσκησης 4 έπεται ότι $\text{μκδ}(a,m)=1$.

($\Leftarrow$) Έστω ότι μκδ$(a, m) = 1$. Θα δείξουμε ότι το στοιχείο $[a]$ είναι αντιστρέψιμο στον δακτύλιο $\mathbb{Z}_m$. Από υπόθεση υπάρχουν $x, y \in \mathbb{Z}$ ώστε $ax + my = 1$ και έτσι

$$\begin{aligned}[ax + my] = [1] &\Rightarrow [ax] + [my] = [1] \\ &\Rightarrow [a][x] + [m][y] = [1] \\ &\Rightarrow [a][x] + [0][y] = [1] \\ &\Rightarrow [a][x] = [1]\end{aligned}$$

και άρα το $[a]$ είναι αντιστρέψιμο.

Σημείωση: Η παραπάνω απόδειξη περιέχει έναν πρακτικό τρόπο υπολογισμού του αντιστρόφου (εφόσον αυτός υπάρχει) του $[a]$. Ας δούμε ένα παράδειγμα. Να βρεθεί ο αντίστροφος του $[4]$ στο $\mathbb{Z}_7$. Χρησιμοποιώντας τον ευκλείδειο αλγόριθμο έχουμε

$$\begin{aligned}\mu\kappa\delta(7, 4) &= \mu\kappa\delta(4, 3) \\ &= \mu\kappa\delta(3, 1) \\ &= 1\end{aligned}$$

και άρα το $[4]$ είναι αντιστρέψιμο στον δακτύλιο $\mathbb{Z}_7$. Καθώς μκδ$(7, 4) = 1$, υπάρχουν $x, y \in \mathbb{Z}$ ώστε $7x + 4y = 1$. Για να προσδιορίσουμε τα x και y εργαζόμαστε ως εξής:

Γράφουμε κατά αρχήν τις ευκλείδειες διαιρέσεις που κάναμε για να υπολογίσουμε τον μέγιστο κοινό διαιρέτη.

$$\begin{aligned}7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 1 \cdot 3 + 0\end{aligned}$$

Λύνουμε τις δύο πρώτες ως προς το υπόλοιπο τους και αντικαθιστούμε την πρώτη στη δεύτερη.

$$\begin{aligned}1 &= 4 - 1 \cdot 3 \\ &= 4 - 1 \cdot (7 - 1 \cdot 4) \\ &= 4 - 1 \cdot 7 + 1 \cdot 4 \\ &= 2 \cdot 4 - 1 \cdot 7\end{aligned}$$

και άρα $x = -1$, $y = 2$. Για να βρούμε τον αντίστροφο του $[4]$ στο $\mathbb{Z}_7$ εργαζόμαστε όπως στην απόδειξη της άσκησης, δηλαδή

$$\begin{aligned}[2 \cdot 4 - 1 \cdot 7] = [1] &\Rightarrow [2 \cdot 4] + [-1 \cdot 7] = [1] \\ &\Rightarrow [2][4] - [7] = [1] \\ &\Rightarrow [2][4] - [0] = [1] \\ &\Rightarrow [2][4] = [1]\end{aligned}$$

Συνεπώς ο αντίστροφος του [4] στον δακτύλιο $\mathbb{Z}_7$ είναι το [2].

Ας δούμε και μια εφαρμογή του προηγουμένου.

Εφαρμογή: Να βρεθούν όλοι οι ακέραιοι x τέτοιοι ώστε $8x = 5 \mod 11$. Εργαζόμενοι στο $\mathbb{Z}_{11}$ έχουμε $[8x] = [5]$, δηλαδή

$$[8][x] = [5]. \tag{4}$$

Επειδή

$$\begin{aligned} \mu\kappa\delta(11,8) &= \mu\kappa\delta(8,3) \\ &= \mu\kappa\delta(3,2) \\ &= \mu\kappa\delta(2,1) \\ &= 1 \end{aligned}$$

έχουμε ότι το [8] είναι αντιστρέψιμο στο $\mathbb{Z}_{11}$. Ας υπολογίσουμε τον αντίστροφό του! Γράφουμε τις ευκλείδειες διαιρέσεις που κάναμε για να βρούμε τον μκδ(11,8)

$$\begin{aligned} 11 &= 1 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

και θα υπολογίσουμε τα $x, y \in \mathbb{Z}$ ώστε 1=μκδ(11,8)=$11x + 8y$. Για το λόγο αυτό λύνουμε τις τρεις πρώτες σχέσεις ως προς το υπόλοιπό τους:

$$\begin{aligned} 3 &= 11 - 1 \cdot 8 \\ 2 &= 8 - 2 \cdot 3 \\ 1 &= 3 - 1 \cdot 2 \end{aligned}$$

Υπολογίζουμε

$$\begin{aligned} 1 = 3 - 1 \cdot 2 &= 3 - 1 \cdot (8 - 2 \cdot 3) && \text{(αντικαταστήσαμε το 2 από την δεύτερη σχέση)} \\ &= 3 - 1 \cdot 8 + 2 \cdot 3 \\ &= 3 \cdot 3 - 1 \cdot 8 \\ &= 3 \cdot (11 - 1 \cdot 8) - 1 \cdot 8 && \text{(αντικαταστήσαμε το 3 από την πρώτη σχέση)} \\ &= 3 \cdot 11 - 3 \cdot 8 - 1 \cdot 8 \\ &= 3 \cdot 11 - 4 \cdot 8 \end{aligned}$$

και άρα $x = 3$, $y = -4$. Για να βρούμε τώρα τον αντίστροφο του $[8]$ εργαζόμαστε όπως στην απόδειξη της άσκησης.

$$\begin{aligned}
[3 \cdot 11 - 4 \cdot 8] = [1] &\Rightarrow [3 \cdot 11] + [-4 \cdot 8] = [1] \\
&\Rightarrow [3][11] + [-4][8] = [1] \\
&\Rightarrow [3][0] + [-4][8] = [1] \\
&\Rightarrow [-4][8] = [1] \\
&\Rightarrow [7][8] = [1] \qquad\qquad (\text{αφού } -4 = 7 \mod 11)
\end{aligned}$$

Πολλαπλασιάζοντας την σχέση (4) με τον αντίστροφο του $[8]$, που είναι το $[7]$ παίρνουμε ότι

$$[x] = [7][5] = [2]$$

και συνεπώς τα ζητούμενα $x \in \mathbb{Z}$ είναι αυτά τα οποία αν διαιρεθούν με το 11 δίνουν υπόλοιπο 2, δηλαδή οι ακέραιοι της μορφής:

$$x = 11\xi + 2, \;\; \xi \in \mathbb{Z}.$$

Παρόμοια άσκηση: Να βρεθούν όλοι οι ακέραιοι x τέτοιοι ώστε $8x = 11 \mod 15$.

(Απάντηση: $x = 15\xi + 7, \;\; \xi \in \mathbb{Z}$)

Κωνσταντίνος Λέντζος

29. **[Άσκηση 29]** Να δείξετε ότι ο δακτύλιος $\mathbb{Z}_m$ είναι σώμα αν και μόνον αν ο m είναι πρώτος.

Απάντηση: Αν ο m είναι πρώτος τότε προφανώς κάθε μη μηδενικό στοιχείο $[a]$ είναι αντιστρέψιμο, αφού $\mu\kappa\delta(a, m) = 1$. Αντίστροφα, αν υποθέσουμε ότι ο δακτύλιος $\mathbb{Z}_m$ είναι σώμα και ότι ο m δεν είναι πρώτος, τότε θα υπήρχαν ακέραιοι $1 < a, b < m$ ώστε $m = ab$ συνεπάγεται $[0] = [m] = [ab] = [a][b]$, χωρίς $[a] = 0$ ή $[b] = 0$. Άτοπο, αφού ο $\mathbb{Z}_m$ είναι σώμα και ειδικότερα ακεραία περιοχή.

Κωνσταντίνος Λέντζος

30. **[Άσκηση 30]** Να κατασκευαστεί σώμα με

(α′) 2 στοιχεία

(β′) 3 στοιχεία

(γ′) 4 στοιχεία

(δ′) 5 στοιχεία

(ε′) 7 στοιχεία

(ϛ′) 8 στοιχεία

(ζ′) 9 στοιχεία

(η′) 25 στοιχεία

(ϑ′) 27 στοιχεία

(ι′) 73 στοιχεία

Απάντηση:

(α′) Όπως είδαμε παραπάνω ο δακτύλιος $\mathbb{Z}_m$ είναι σώμα αν και μόνον αν ο m είναι πρώτος. Έτσι ένα σώμα με δύο στοιχεία είναι το $\mathbb{Z}_2$.

(β′) Ένα σώμα με 3 στοιχεία είναι το $\mathbb{Z}_3$.

(γ′) Αναζητούμε τώρα ένα σώμα με 4 στοιχεία. Προσοχή! Ο $\mathbb{Z}_4$ δεν είναι σώμα!! Μάλιστα δεν είναι καν ακεραία περιοχή,

$$\text{αφού } [2][2] = [0] \text{ και } [2] \neq [0].$$

Για να βρούμε ένα σώμα με 4 στοιχεία, θεωρούμε τον δακτύλιο $\mathbb{Z}_2[x]$ και το πολυώνυμο

$$f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x].$$

Το $f(x)$ είναι ανάγωγο στον $\mathbb{Z}_2[x]$. Πράγματι, το $f(x)$ είναι βαθμού 2 και οι ρίζες του δεν ανήκουν στο $\mathbb{Z}_2$, αφού

$$f(0) = 0^2 + 0 + 1 = 1 \neq 0 \mod 2 \text{ και}$$

$$f(1) = 1^2 + 1 + 1 = 3 = 1 \neq 0 \mod 2.$$

Από την άσκηση λοιπόν 3 έχουμε ότι ο δακτύλιος

$$\mathbb{Z}_2[x]/ < x^2 + x + 1 >$$

είναι σώμα. Θέτουμε $I =< x^2 + x + 1 >$, τότε ένα στοιχείο του $\mathbb{Z}_2[x]/ < x^2 + x + 1 >$ είναι της μορφής $g(x) + I$ με $g(x)$ κάποιο πολυώνυμο του $\mathbb{Z}_2[x]$. Από την ταυτότητα της διαίρεσης στο $\mathbb{Z}_2[x]$, υπάρχουν $q(x), r(x)\mathbb{Z}_2[x]$ ώστε

$$g(x) = q(x)(x^2 + x + 1) + r(x) \text{ και}$$

$$0 \leq deg(r(x)) < deg(x^2 + x + 1) = 2.$$

Έτσι το πολυώνυμο $r(x)$ είναι βαθμού το πολύ 1 και ως εκ τούτου έχει τη μορφή

$$r(x) = ax + b \text{ για κάποια } a, b \in \mathbb{Z}_2.$$

Παρατηρούμε ότι

$$\begin{aligned} g(x) + I &= [q(x)(x^2 + x + 1) + r(x)] + I \\ &= [q(x)(x^2 + x + 1) + I] + (r(x) + I) \\ &= (0 + I) + (r(x) + I) \qquad (\text{αφού } I =< x^2 + x + 1 >) \\ &= r(x) + I \\ &= (ax + b) + I \end{aligned}$$

Έτσι το τυχαίο στοιχείο $g(x) + I$ του δακτυλίου πηλίκου είναι της μορφής $(ax + b) + I$ για κάποια $a, b \in \mathbb{Z}_2$. Πόσα στοιχεία έχει ο δακτύλιος $\mathbb{Z}_2[x]/ < x^2 + x + 1 >$; Έχει τόσα στοιχεία, όσα και πολυώνυμα της μορφής $ax + b$ με $a, b \in \mathbb{Z}_2 = \{[0], [1]\}$, δηλαδή 4 στοιχεία, διότι έχουμε δύο επιλογές για το a (ή $[0]$ ή $[1]$) και άλλες δύο για το b. Συνολικά $2^2 = 4$ επιλογές.

Αν θέλουμε να αναγράψουμε τα στοιχεία του $\mathbb{Z}_2[x]/ < x^2 + x + 1 >$, τότε αυτά είναι:

0+I

1+I

$x + I$

$(x + 1) + I$

Έτσι λοιπόν κατασκευάσαμε ένα σώμα με 4 στοιχεία.

(δ΄) Ένα σώμα με 5 στοιχεία είναι το $\mathbb{Z}_5$.

(ε΄) Ένα σώμα με 7 στοιχεία είναι το $\mathbb{Z}_7$.

(ϛ΄) Θα κατασκευάσουμε ένα σώμα με 8 στοιχεία. θεωρούμε τον δακτύλιο $\mathbb{Z}_2[x]$ και το πολυώνυμο

$$f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x].$$

Το $f(x)$ είναι ανάγωγο στον $\mathbb{Z}_2[x]$. Πράγματι, το $f(x)$ είναι βαθμού 3 και οι ρίζες του δεν ανήκουν στο $\mathbb{Z}_2$, αφού

$$f(0) = 0^3 + 0 + 1 = 1 \neq 0 \mod 2$$

$$f(1) = 1^3 + 1 + 1 = 3 = 1 \neq 0 \mod 2$$

Από την άσκηση λοιπόν 3 έχουμε ότι ο δακτύλιος

$$\mathbb{Z}_2[x]/ < x^3 + x + 1 >$$

είναι σώμα. Θέτουμε $I =< x^3 + x + 1 >$, τότε ένα στοιχείο του $\mathbb{Z}_2[x]/ < x^3 + x + 1 >$ είναι της μορφής $g(x) + I$ με $g(x)$ κάποιο πολυώνυμο του $\mathbb{Z}_2[x]$. Από την ταυτότητα της διαίρεσης στο $\mathbb{Z}_2[x]$, υπάρχουν $q(x), r(x)\mathbb{Z}_2[x]$ ώστε

$$g(x) = q(x)(x^3 + x^2 + x + 2) + r(x) \text{ και}$$

$$0 \leq deg(r(x)) < deg(x^3 + x + 1) = 3.$$

Έτσι το πολυώνυμο $r(x)$ είναι βαθμού το πολύ 2 και ως εκ τούτου έχει τη μορφή

$$r(x) = ax^2 + bx + c \text{ για κάποια } a, b, c \in \mathbb{Z}_2.$$

Παρατηρούμε ότι

$$\begin{aligned} g(x) + I &= [q(x)(x^3 + x + 1) + r(x)] + I \\ &= [q(x)(x^3 + x + 1) + I] + (r(x) + I) \\ &= (0 + I) + (r(x) + I) && (\text{αφού } I =< x^3 + x + 1 >) \\ &= r(x) + I \\ &= (ax^2 + bx + c) + I \end{aligned}$$

Έτσι το τυχαίο στοιχείο $g(x)+I$ του δακτυλίου πηλίκου είναι της μορφής $(ax^2+bx+c)+I$ για κάποια $a, b, c \in \mathbb{Z}_2$. Πόσα στοιχεία έχει ο δακτύλιος $\mathbb{Z}_2[x]/ < x^3 + x + 1 >$; Έχει τόσα στοιχεία, όσα και πολυώνυμα της μορφής $ax^2 + bx + c$ με $a, b, c \in \mathbb{Z}_2 = \{[0], [1]\}$, δηλαδή 8 στοιχεία, διότι έχουμε δύο επιλογές για το a (ή $[0]$ ή $[1]$), δύο για το b και άλλες δύο για το c. Συνολικά $2^3 = 8$ επιλογές. Έτσι λοιπόν κατασκευάσαμε ένα σώμα με 8 στοιχεία.

(ζ′) Θα κατασκευάσουμε ένα σώμα με 9 στοιχεία. θεωρούμε τον δακτύλιο $\mathbb{Z}_3[x]$ και το πολυώνυμο

$$f(x) = x^2 + 1 \in \mathbb{Z}_3[x].$$

Το $f(x)$ είναι ανάγωγο στον $\mathbb{Z}_3[x]$. Πράγματι, το $f(x)$ είναι βαθμού 2 και οι ρίζες του δεν ανήκουν στο $\mathbb{Z}_2$, αφού

$$\begin{aligned} f(0) &= 0^2 + 1 = 1 \neq 0 && \mod 3 \\ f(1) &= 1^2 + 1 = 2 \neq 0 && \mod 3 \\ f(2) &= 2^2 + 1 = 5 = 2 \neq 0 && \mod 3 \end{aligned}$$

Από την άσκηση λοιπόν 3 έχουμε ότι ο δακτύλιος

$$\mathbb{Z}_3[x]/ < x^2 + 1 >$$

είναι σώμα. Θέτουμε $I =< x^2 + 1 >$, τότε ένα στοιχείο του $\mathbb{Z}_3[x]/ < x^2 + 1 >$ είναι της μορφής $g(x) + I$ με $g(x)$ κάποιο πολυώνυμο του $\mathbb{Z}_3[x]$. Από την ταυτότητα της διαίρεσης στο $\mathbb{Z}_3[x]$, υπάρχουν $q(x), r(x)\mathbb{Z}_3[x]$ ώστε

$$g(x) = q(x)(x^2 + x + 1) + r(x) \text{ και}$$

$$0 \leq deg(r(x)) < deg(x^2 + 1) = 2.$$

Έτσι το πολυώνυμο $r(x)$ είναι βαθμού το πολύ 1 και ως εκ τούτου έχει τη μορφή

$$r(x) = ax + b \text{ για κάποια } a, b \in \mathbb{Z}_3.$$

Παρατηρούμε ότι

$$\begin{aligned} g(x) + I &= [q(x)(x^2 + 1) + r(x)] + I \\ &= [q(x)(x^2 + 1) + I] + (r(x) + I) \\ &= (0 + I) + (r(x) + I) \qquad (\text{αφού } I =< x^2 + 1 >) \\ &= r(x) + I \\ &= (ax + b) + I \end{aligned}$$

Έτσι το τυχαίο στοιχείο $g(x) + I$ του δακτυλίου πηλίκου είναι της μορφής $(ax + b) + I$ για κάποια $a, b \in \mathbb{Z}_3$. Πόσα στοιχεία έχει ο δακτύλιος $\mathbb{Z}_3[x]/ < x^2 + 1 >$; Έχει τόσα στοιχεία, όσα και πολυώνυμα της μορφής $ax + b$ με $a, b \in \mathbb{Z}_3 = \{[0], [1], [2]\}$, δηλαδή 9 στοιχεία, διότι έχουμε τρεις επιλογές για το a (ή [0] ή [1] ή [2]) και άλλες τρεις για το b. Συνολικά $3^2 = 9$ επιλογές.

Αν θέλουμε να αναγράψουμε τα στοιχεία του $\mathbb{Z}_2[x]/ < x^2 + 1 >$, τότε αυτά είναι:

0+I

1+I

2+I

$x + I$

$2x + I$

$(x + 1) + I$

$(x+2)+I$

$(2x+1)+I$

$(2x+2)$+I

Έτσι λοιπόν κατασκευάσαμε ένα σώμα με 9 στοιχεία.

(η΄) Θα κατασκευάσουμε ένα σώμα με 25 στοιχεία. θεωρούμε τον δακτύλιο $\mathbb{Z}_5[x]$ και το πολυώνυμο

$$f(x) = x^2 + x + 1 \in \mathbb{Z}_5[x].$$

Το $f(x)$ είναι ανάγωγο στον $\mathbb{Z}_5[x]$. Πράγματι, το $f(x)$ είναι βαθμού 2 και οι ρίζες του δεν ανήκουν στο $\mathbb{Z}_5$, αφού

$$\begin{aligned}
f(0) &= 0^2 + 0 + 1 = 1 \neq 0 && \mod 5\\
f(1) &= 1^2 + 1 + 1 = 3 \neq 0 && \mod 5\\
f(2) &= 2^2 + 2 + 1 = 7 = 2 \neq 0 && \mod 5\\
f(3) &= 3^2 + 3 + 1 = 13 = 3 \neq 0 && \mod 5\\
f(4) &= 4^2 + 4 + 1 = 21 = 1 \neq 0 && \mod 5
\end{aligned}$$

Από την άσκηση λοιπόν 3 έχουμε ότι ο δακτύλιος

$$\mathbb{Z}_3[x]/ < x^2 + x + 1 >$$

είναι σώμα. Θέτουμε $I =< x^2 + x + 1 >$, τότε ένα στοιχείο του $\mathbb{Z}_5[x]/ < x^2 + x + 1 >$ είναι της μορφής $g(x) + I$ με $g(x)$ κάποιο πολυώνυμο του $\mathbb{Z}_5[x]$. Από την ταυτότητα της διαίρεσης στο $\mathbb{Z}_5[x]$, υπάρχουν $q(x), r(x)\mathbb{Z}_5[x]$ ώστε

$$g(x) = q(x)(x^2 + x + 1) + r(x) \text{ και}$$

$$0 \leq deg(r(x)) < deg(x^2 + x + 1) = 2.$$

Έτσι το πολυώνυμο $r(x)$ είναι βαθμού το πολύ 1 και ως εκ τούτου έχει τη μορφή

$$r(x) = ax + b \text{ για κάποια } a, b \in \mathbb{Z}_5.$$

Παρατηρούμε ότι

$$\begin{aligned}
g(x) + I &= [q(x)(x^2 + x + 1) + r(x)] + I\\
&= [q(x)(x^2 + x + 1) + I] + (r(x) + I)\\
&= (0 + I) + (r(x) + I) && (\text{αφού } I =< x^2 + x + 1 >)\\
&= r(x) + I\\
&= (ax + b) + I
\end{aligned}$$

Έτσι το τυχαίο στοιχείο $g(x)+I$ του δακτυλίου πηλίκου είναι της μορφής $(ax+b)+I$ για κάποια $a,b \in \mathbb{Z}_5$. Πόσα στοιχεία έχει ο δακτύλιος $\mathbb{Z}_5[x]/ < x^2+x+1 >$; Έχει τόσα στοιχεία, όσα και πολυώνυμα της μορφής $ax+b$ με $a,b \in \mathbb{Z}_5 = \{[0],[1],[2],[3],[4]\}$, δηλαδή 25 στοιχεία, διότι έχουμε πέντε επιλογές για το a (ή $[0]$ ή $[1]$ ή $[2]$ ή $[3]$ ή $[4]$) και άλλες πέντε για το b. Συνολικά $5^2 = 25$ επιλογές. Έτσι λοιπόν κατασκευάσαμε ένα σώμα με 25 στοιχεία.

(ϑ′) Θα κατασκευάσουμε ένα σώμα με 27 στοιχεία. ϑεωρούμε τον δακτύλιο $\mathbb{Z}_3[x]$ και το πολυώνυμο

$$f(x) = x^3 + x^2 + x + 2 \in \mathbb{Z}_3[x].$$

Το $f(x)$ είναι ανάγωγο στον $\mathbb{Z}_3[x]$. Πράγματι, το $f(x)$ είναι βαθμού 3 και οι ρίζες του δεν ανήκουν στο $\mathbb{Z}_5$, αφού

$$\begin{aligned} f(0) &= 0^3+0^2+0+2 = 2 \neq 0 && \mod 3 \\ f(1) &= 1^3+1^2+1+2 = 5 = 2 \neq 0 && \mod 3 \\ f(2) &= 2^3+2^2+2+2 = 16 = 1 \neq 0 && \mod 3 \end{aligned}$$

Από την άσκηση λοιπόν 3 έχουμε ότι ο δακτύλιος

$$\mathbb{Z}_3[x]/ < x^3+x^2+x+2 >$$

είναι σώμα. Θέτουμε $I =< x^3+x^2+x+2 >$, τότε ένα στοιχείο του $\mathbb{Z}_3[x]/ < x^3+x^2+x+2 >$ είναι της μορφής $g(x)+I$ με $g(x)$ κάποιο πολυώνυμο του $\mathbb{Z}_3[x]$. Από την ταυτότητα της διαίρεσης στο $\mathbb{Z}_3[x]$, υπάρχουν $q(x), r(x)\mathbb{Z}_3[x]$ ώστε

$$g(x) = q(x)(x^3+x^2+x+2) + r(x) \text{ και}$$

$$0 \leq deg(r(x)) < deg(x^3+x^2+x+2) = 3.$$

Έτσι το πολυώνυμο $r(x)$ είναι βαθμού το πολύ 2 και ως εκ τούτου έχει τη μορφή

$$r(x) = ax^2+bx+c \text{ για κάποια } a,b,c \in \mathbb{Z}_3.$$

Παρατηρούμε ότι

$$\begin{aligned} g(x)+I &= [q(x)(x^3+x^2+x+2)+r(x)]+I \\ &= [q(x)(x^3+x^2+x+2)+I]+(r(x)+I) \\ &= (0+I)+(r(x)+I) && (\text{αφού } I =< x^3+x^2+x+2 >) \\ &= r(x)+I \\ &= (ax^2+bx+c)+I \end{aligned}$$

Έτσι το τυχαίο στοιχείο $g(x)+I$ του δακτυλίου πηλίκου είναι της μορφής $(ax^2+bx+c)+I$ για κάποια $a, b, c \in \mathbb{Z}_3$. Πόσα στοιχεία έχει ο δακτύλιος $\mathbb{Z}_3[x]/ < x^3+x^2+x+2 >$; Έχει τόσα στοιχεία, όσα και πολυώνυμα της μορφής ax^2+bx+c με $a, b, c \in \mathbb{Z}_3 = \{[0], [1], [2]\}$, δηλαδή 27 στοιχεία, διότι έχουμε τρεις επιλογές για το a (ή $[0]$ ή $[1]$ ή $[2]$), άλλες τρεις για το b και άλλες τρεις για το c. Συνολικά $3^3 = 27$ επιλογές. Έτσι λοιπόν κατασκευάσαμε ένα σώμα με 27 στοιχεία.

(ι΄) Ένα σώμα με 73 στοιχεία είναι το $\mathbb{Z}_{73}$, διότι ο 73 είναι πρώτος.

Σχόλια.

- Σώμα με ένα στοιχείο δεν υπάρχει. Θυμηθείτε στον ορισμό ενός σώματος F την απαίτηση να υπάρχει το ουδέτερο στοιχείο της πρόσθεσης 0_F και η μονάδα 1_R και αυτά να είναι διακεκριμμένα, δηλαδή $0_F \neq 1_F$. Συνεπώς ένα σώμα δεν μπορεί να έχει λιγότερα από δύο στοιχεία.
- Αποδεικνύεται ότι πεπερασμένα σώματα υπάρχουν μόνο με πλήθος στοιχείων δυνάμεις πρώτων. Για παράδειγμα δεν υπάρχει σώμα με 10 ή 12 στοιχεία. Στην πράξη για να κατασκευάσουμε ένα σώμα που έχει p^k στοιχεία, συνήθως βρίσκουμε ένα ανάγωγο πολυώνυμο $f(x) \in \mathbb{Z}_p$ βαθμού k (αυτό δεν είναι πάντα εύκολο) και εν συνεχεία αποδεικνύουμε όπως κάναμε παραπάνω ότι ο δακτύλιος $\mathbb{Z}_p[x]/ < f(x) >$ είναι σώμα.
- Σε ένα σώμα κάθε μη μηδενικό στοιχείο είναι αντιστρέψιμο. Ας πάρουμε για παράδειγμα τον δακτύλιο

$$\mathbb{Z}_2[x]/ < x^3 + x^2 + 1 >,$$

ο οποίος είναι σώμα με 8 στοιχεία (μπορείτε για εξάσκηση να το επιβεβαιώσετε). Να βρεθεί ο αντίστροφος του στοιχείου $(x+1)+I$, όπου $I =< x^3 + x^2 + 1 >$.

Θυμηθείτε πως εργαστήκαμε στη σημείωση μετά την άσκηση 28.

- Ένα άλλο σώμα με 9 στοιχεία είναι το $\mathbb{Z}[i]/3\mathbb{Z}[i]$, αλλά δεν θα μας απασχολήσει.
- Κάποιος γράφει: "*Θεωρώ τον δακτύλιο* $\mathbb{Z}_3[x]$ *και το πολυώνυμο* x^2+x+1. *Θέτω* $I =< x^2+x+1 >$ *Κάθε στοιχείο του δακτυλίου πηλίκου* $\mathbb{Z}_3[x]/ < x^2+x+1 >$ *είναι της μορφής* $(ax+b)+I$ *για κάποια* $a, b \in \mathbb{Z}_3$, *διότι το πολυώνυμο* $x^2+x+1 \in \mathbb{Z}_3[x]$ *είναι βαθμού 2. Έτσι το* $\mathbb{Z}_3[x]/I$ *έχει 9 στοιχεία και με αυτό τον τρόπο κατασκευάσαμε ένα σώμα με 9 στοιχεία.*"

Είναι σωστός ο παραπάνω συλλογισμός; Η συζήτηση συνεχίζεται στον σύνδεσμο "κουβέντα" της ηλεκτρονικής τάξης.

Κωνσταντίνος Λέντζος

31. [**Άσκηση 31**] Δώστε μερικά παραδείγματα σωμάτων με άπειρα το πλήθος στοιχεία.

Απάντηση: Καλούνται οι φοιτητές να συμμετάσχουν μέσω του συνδέσμου "κουβέντα" της ηλεκτρονικής τάξης.

Προσεχώς λεπτομέρειες!

Κωνσταντίνος Λέντζος

32. [**Άσκηση 32**] Δείξτε ότι ένα σώμα έχει μόνο δύο ιδεώδη, το μηδενικό και τον εαυτό του.

Απάντηση: Κάθε δακτύλιος έχει σίγουρα δύο ιδεώδη, το μηδενικό $\{0\}$ και τον εαυτό του. Έστω τώρα F ένα σώμα, τότε το F θα έχει ως ιδεώδη σίγουρα το $\{0\}$ και τον εαυτό F. Θα δείξουμε ότι δεν έχει άλλα. Για το λόγο αυτό θεωρούμε I ένα μη μηδενικό ιδεώδες του και θα δείξουμε ότι το I αναγκαστικά ισούται με το F. Το I ως μη μηδενικό θα περιέχει τουλάχιστον ένα μη μηδενικό στοιχείο a. Το F όμως είναι σώμα και σύνεπως κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο, ειδικότερα το a είναι αντιστρέψιμο. Έστω $r \in F$ ο αντίστροφος του a. Καθώς το I είναι ιδεώδες, από τον ορισμού ενός ιδεώδους έχουμε ότι $ra \in I$. Όμως $ra = 1$ και έτσι

$$1 \in I.$$

Δείξαμε λοιπόν ότι η μονάδα του σώματος ανήκει στο I. Στη συνέχεια θα δείξουμε ότι και κάθε άλλο στοιχείο του F ανήκει στο I. Έστω $w \in F$ τυχαίο, τότε καθώς το I είναι ιδεώδες, από τον ορισμό ενός ιδεώδους, έπεται ότι $w = w \cdot 1 \in I$ και τελειώσαμε.

Άννα Καρασούλου

33. [**Άσκηση 33**] Αν ένας δακτύλιος έχει μόνο δύο ιδεώδη έπεται ότι είναι σώμα;

Απάντηση: Αυτό δεν είναι γενικά σωστό. Είδαμε στην απόδειξη της άσκησης 17 ότι ο δακτύλιος των πινάκων 2×2 με στοιχεία από το $\mathbb{R}$, τον οποίον συμβολίζουμε με $\mathbb{R}^{2\times 2}$ έχει μόνο δύο ιδεώδη, το μηδενικό και τον εαυτό του. Παρ'όλα αυτά δεν είναι σώμα, αφού δεν είναι μεταθετικός. Πραγματι αν θεωρήσουμε τους πίνακες

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ και } B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

τότε

$$AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ ενώ } BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

δηλαδή $AB \neq BA$.

Άννα Καρασούλου

34. **[Άσκηση 34]** Βρείτε τα ιδεώδη των παρακάτω δακτυλίων:

(α′) $\mathbb{Z}_3$

(β′) $\mathbb{Z}_4$

(γ′) $\mathbb{Z}_5$

(δ′) $\mathbb{Z}_6$

Απάντηση:

(α′) Ο δακτύλιος $\mathbb{Z}_3$ είναι σώμα και συμφωνα με την άσκηση 32 τα μόνα ιδεώδη του είναι το $\{[0]\}$ και ο εαυτός του.

(β′) Προσπαθήστε να δείξετε μόνοι σας ότι τα ιδεώδη του $\mathbb{Z}_4$ είναι τα εξής: $\{0\}, \{[0], [2]\}$ και $\mathbb{Z}_4$.

(γ′) Ο δακτύλιος $\mathbb{Z}_5$ είναι σώμα και συμφωνα με την άσκηση 32 τα μόνα ιδεώδη του είναι το $\{[0]\}$ και ο εαυτός του.

(δ′) Ένα ιδεώδες περιέχει πάντα το μηδενικό στοιχείο του δακτυλίου. Συνεπώς ιδεώδη με ένα στοιχείο είναι μόνο το $\{[0]\}$.

Ιδεώδη με δύο στοιχεία: Ένα ιδεώδες I με δύο στοιχεία θα περιέχει σίγουρα το $[0]$ και ένα άλλο στοιχείο. Αν περιείχε το $[1]$ τότε θα έπρεπε να περιείχε και το $[1]+[1] = [2]$ (καθώς επίσης και το $[2]+[1] = [3]$) και συνεπώς θα είχε περισσότερα από δύο στοιχεία. Άτοπο. Άρα το $[1]$ δεν μπορεί να το έχει. Αν υποθέσουμε ότι περιέχει το $[2]$ τότε θα έπρεπε να περιέχει και το $[2] + [2] = [4]$. Άτοπο γιατί σε αυτή την περίπτωση θα έχει τρία στοιχεία. Άρα ούτε το $[2]$ μπορεί να το έχει. Αν το I περιέχει το $[3]$, τότε θα δείξουμε ότι το υποσύνολο $\{[0], [3]\}$ είναι ιδεώδες του $\mathbb{Z}_6$.

Πράγματι, η διαφορά δύο οποιοδήποτε στοιχείων του $\{[0],[3]\}$ σε αυτή την περίπτωση ανήκει στο $\{[0],[3]\}$, αφού

$$\begin{aligned}[0]-[0]=[0]&\in\{[0],[3]\}\\ [3]-[0]=[3]&\in\{[0],[3]\}\\ [0]-[3]=[-3]=[3]&\in\{[0],[3]\}\\ [3]-[3]=[0]&\in\{[0],[3]\}.\end{aligned}$$

Επιπλέον αν $[a]\in\mathbb{Z}_6$ τότε $[a][0]=[0]\in\{[0],[3]\}$ και $[a][3]\in\{[0],[3]\}$. Πράγματι,

$$\begin{aligned}[1][3]=&[3]\in\{[0],[3]\}\\ [2][3]=&[6]=[0]\in\{[0],[3]\}\\ [3][3]=&[9]=[3]\in\{[0],[3]\}\\ [4][3]=&[12]=[0]\in\{[0],[3]\}\\ [5][3]=&[15]=[3]\in\{[0],[3]\}\end{aligned}$$

Έτσι λοιπόν το $\{[0],[3]\}$ είνα ένα ιδεώδες. Συνεχίζουμε μήπως βρούμε και άλλο ιδεώδες με δύο στοιχεία. Αν υποθέσουμε ότι το I περιέχει το $[4]$ τότε θα πρέπει να περιέχει και το $[4]+[4]=[8]=[2]$ και συνεπώς θα είχε περισσότερα από δύο στοιχεία. Άτοπο. Άρα το $[4]$ δεν μπορεί να το έχει. Αν υποθέσουμε τέλος ότι το I περιέχει το $[5]$ τότε θα πρέπει να περιέχει και το $[5]+[5]=[10]=[4]$ και συνεπώς θα είχε περισσότερα από δύο στοιχεία. Άτοπο. Άρα ούτε το $[5]$ δεν μπορεί να έχει.

Ιδεώδη με τρία στοιχεία: Έστω I ένα ιδεώδες με τρία στοιχεία, τότε το I θα περιέχει σίγουρα το $[0]$ και φυσικά άλλα δύο στοιχεία. Αν το I περιέχει το $[1]$, τότε θα έπρεπε να περιέχει και το $[1]+[1]=[2]$ καθώς επίσης και το $[2]+[1]=[3]$ και συνεπώς θα είχε περισσότερα από δύο στοιχεία. Άτοπο. Άρα το $[1]$ δεν μπορεί να το έχει. Αν υποθέσουμε ότι περιέχει το $[2]$, τοτε θα πρέπει να περιέχει και το $[2]+[2]=[4]$. Θα δείξουμε ότι το υποσύνολο $\{[0],[2],[4]\}$ αποτελεί ιδεώδες του $\mathbb{Z}_6$. Πράγματι, η διαφορά δύο οποιοδήποτε στοιχείων του $\{[0],[2],[4]\}$, ανήκει στο

$\{[0],[2],[4]\}$, αφού

$$\begin{array}{lcl}
[0]-[0]=[0] & \in & \{[0],[2],[4]\} \\
[0]-[2]=[-2]=[4] & \in & \{[0],[2],[4]\} \\
[0]-[4]=[-4]=[2] & \in & \{[0],[2],[4]\} \\
[2]-[0]=[2] & \in & \{[0],[2],[4]\} \\
[2]-[2]=[0] & \in & \{[0],[2],[4]\} \\
[2]-[4]=[-2]=[4] & \in & \{[0],[2],[4]\} \\
[4]-[0]=[4] & \in & \{[0],[2],[4]\} \\
[4]-[2]=[2] & \in & \{[0],[2],[4]\} \\
[4]-[4]=[0] & \in & \{[0],[2],[4]\}
\end{array}$$

Επιπλέον αν $[a] \in \mathbb{Z}_6$ τότε $[a][0]=[0] \in \{[0],[2],[4]\}$, $[a][2] \in \{[0],[2],[4]\}$ και $[a][4] \in \{[0],[2],[4]\}$. Πράγματι,

$$\begin{aligned}
[1][2]=[2] &\in \{[0],[2],[4]\} \\
[2][2]=[4] &\in \{[0],[2],[4]\} \\
[3][2]=[6]=[0] &\in \{[0],[2],[4]\} \\
[4][2]=[8]=[2] &\in \{[0],[2],[4]\} \\
[5][2]=[10]=[4] &\in \{[0],[2],[4]\}
\end{aligned}$$

και

$$\begin{aligned}
[1][4]=[4] &\in \{[0],[2],[4]\} \\
[2][4]=[8]=[2] &\in \{[0],[2],[4]\} \\
[3][4]=[12]=[0] &\in \{[0],[2],[4]\} \\
[4][4]=[16]=[4] &\in \{[0],[2],[4]\} \\
[5][4]=[20]=[2] &\in \{[0],[2],[4]\}
\end{aligned}$$

Έτσι λοιπόν το $\{[0],[2],[4]\}$ είνα ένα ιδεώδες. Συνεχίζουμε μήπως βρούμε και άλλο ιδεώδες με τρία στοιχεία. Αν υποθέσουμε ότι το I περιέχει το $[4]$ τότε θα πρέπει να περιέχει και το $[2]$ και όπως δείξαμε πριν το υποσύνολο $\{[0],[2],[4]\}$ είναι ιδεώδες. Αν υποθέσουμε τέλος ότι το I περιέχει το $[5]$ τότε θα πρέπει να περιέχει και το $[5]+[5]=[10]=[4]$. Αν όμως περιέχει το $[4]$ θα πρέπει να περιέχει και το $[2][4]=[8]=[2]$ και συνεπώς θα είχε περισσότερα από δύο στοιχεία. Άτοπο. Άρα το $[5]$ δεν μπορεί να το έχει.

Ιδεώδη με τέσσερα στοιχεία: Ιδεώδη με τέσσερα στοιχεία δεν υπάρχουν διότι για ένα ιδεώδες $(I,+,\cdot)$ του δακτυλίου $(\mathbb{Z}_6,+,\cdot)$ παρατηρούμε ότι το $(I,+)$ αποτελεί υποομάδα της $(\mathbb{Z}_6,+)$. Η ομάδα όμως $(\mathbb{Z}_6,+)$ έχει έξι στοιχεία και συνεπώς από το θεώρημα Lagrange δεν μπορεί να έχει υποομάδα με τέσσερα στοιχεία!

Ιδεώδη με πέντε στοιχεία: Ιδεώδη με πέντε στοιχεία δεν υπάρχουν διότι για ένα ιδεώδες $(I,+,\cdot)$ του δακτυλίου $(\mathbb{Z}_6,+,\cdot)$ παρατηρούμε ότι το $(I,+)$ αποτελεί υποομάδα της $(\mathbb{Z}_6,+)$. Η ομάδα όμως $(\mathbb{Z}_6,+)$ έχει έξι στοιχεία και συνεπώς από το θεώρημα Lagrange δεν μπορεί να έχει υποομάδα με πέντε στοιχεία!

Ιδεώδη με έξι στοιχεία: Είναι μόνο το $\mathbb{Z}_6$.

Συμπερασματικά τα ιδεώδη του $\mathbb{Z}_6$ είναι τα εξής: $\{0\},\{[0],[3]\},\{[0],[2],[4]\}$ και $\mathbb{Z}_6$.

Παρόμοια Άσκηση: Να βρεθούν τα ιδεώδη των δακτυλίων $\mathbb{Z}_7,\mathbb{Z}_8,\mathbb{Z}_9,\mathbb{Q},\mathbb{R}$ και $\mathbb{C}$.

Άννα Καρασούλου

35. **[Άσκηση 35]**

Πόσα ιδεώδη έχει ο δακτύλιος $\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\times 11\mathbb{Z}$;

Απάντηση: Από την άσκηση 12 έχουμε ότι

$$\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\times 11\mathbb{Z}\cong\mathbb{Z}_6\times\mathbb{Z}_{11}.$$

Παρατηρούμε ότι καθώς ο 11 είναι πρώτος, ο δακτύλιος $\mathbb{Z}_{11}$ είναι σώμα και συνεπώς από την άσκηση 32 έπεται ότι έχει ακριβώς δύο ιδεώδη. Από την άλλη είδαμε στην άσκηση 34 ότι ο δακτύλιος $\mathbb{Z}_6$ έχει 4 ιδεώδη. Συνεπώς από την άσκηση 26 έπεται ότι ο δακτύλιος

$$\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}\times 11\mathbb{Z}$$

έχει ακριβώς $4\cdot 2=8$ ιδεώδη.

Άννα Καρασούλου

36. **[Άσκηση 36]**

Θεωρούμε τον δακτύλιο $\mathbb{Q}[x]/ < x^3+3x+5 >$. Να βρεθεί ο αντίστροφος του $(2x+I)$.

Απάντηση: Θέτουμε

$$I =< x^3+3x+5 >= \{h(x)(x^3+3x+5) : h(x) \in \mathbb{Q}[x]\}.$$

Παρατηρούμε ότι

$$2x \notin I \Leftrightarrow 2x+I \neq 0+I$$

και άρα έχει νόημα να αναζητήσουμε τον αντίστροφό του. Εν συνεχεία υπολογίζουμε τον μκδ$(x^3+3x+5, 2x)$. Έκτελούμε την διαίρεση του x^3+3x+5 με το $2x$

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

και γράφουμε την ταυτότητα της διαίρεσης:

$$x^3+3x+5 = 2x(\frac{1}{2}x^2+\frac{3}{2})+5 \qquad (*)$$

Έτσι

$$\begin{aligned} \mu\kappa\delta(x^3+3x+5, 2x) &= \mu\kappa\delta(2x, 5) \\ &= 1 \end{aligned}$$

Θα βρούμε πολυώνυμα $a(x), b(x) \in \mathbb{Q}[x]$ ώστε

$$a(x)(x^3+3x+5)+b(x)(2x) = 1.$$

Από την σχέση $(*)$ έχουμε ότι

$$x^3+3x+5+(-\tfrac{1}{2}x^2-\tfrac{3}{2})2x = 5$$

ή ισοδύναμα

$$\tfrac{1}{5}(x^3+3x+5)+(-\tfrac{1}{10}x^2-\tfrac{3}{10})2x = 1$$

Θεωρώντας την τελευταία σχέση στο δακτύλιο $\mathbb{Q}[x]/I$ παίρνουμε ότι

$$\Big(\tfrac{1}{5}(x^3+3x+5)+I\Big)+\Big((-\tfrac{1}{10}x^2-\tfrac{3}{10})2x+I\Big)=1+I$$

και καθώς $\frac{1}{5}(x^3+3x+5)+I=0+I$, έχουμε

$$(-\tfrac{1}{10}x^2-\tfrac{3}{10})2x+I=1+I$$

ή ισοδύναμα

$$\Big(-\tfrac{1}{10}x^2-\tfrac{3}{10})+I\Big)\Big(2x+I\Big)=1+I$$

Συνεπώς $(2x+I)^{-1}=(-\frac{1}{10}x^2-\frac{3}{10})+I$.

Άννα Καρασούλου

37. [**Άσκηση 37**] Έστω m,n δύο θετικοί ακέραιοι. Θέτουμε $d=$μκδ(m,n) και $e=$εκπ(m,n). Δείξτε τις παρακάτω ισότητες ιδεωδών στο $\mathbb{Z}$.

(α') $< m > + < n >=< d >$

(β') $< m > \cap < n >=< e >$

(γ') $< m >< n >=< mn >$

Απάντηση: Θυμηθείτε ότι αν I,J είναι δύο ιδεώδη ενός δακτυλίου R, τότε τα υποσύνολα $I\cap J$, $I+J$ και IJ του R που ορίζονται ως εξής:

$$\begin{aligned} I\cap J &= \{a\in R : a\in I \ \text{ και } \ a\in J\}\\ I+J &= \{a+b\in R : a\in I \ \text{ και } \ b\in J\}\\ IJ &= \{a_1b_1+\ldots+a_nb_n : a_i\in I, b_i\in J, n\geq 1\}\end{aligned}$$

είναι ιδεώδη του δακτύλιου R. Επίσης το σύνολο $\{ab : a\in I, b\in J\}$ δεν είναι γενικό ίσο με το IJ. Υπάρχουν μάλιστα παραδείγματα που το σύνολο αυτό δεν είναι καν ιδεώδες. Αν θεωρήσουμε για παράδειγμα τον δακτύλιο $\mathbb{Q}[x_1,x_2,x_3,x_4]$ και τα ιδεώδη αυτού

$$I=< x_1,x_2 >$$

$$J=< x_3,x_4 >$$

τότε αν το σύνολο $\{ab : a\in I, b\in J\}$ ήταν ιδεώδες θα έπρεπε

$$u_1 + u_2 \in \{ab : a \in I, b \in J\} \text{ για κάθε } u_1, u_2 \in \{ab : a \in I, b \in J\}.$$

Αν θεωρήσουμε όμως για $u_1 = x_1x_3$ και για $u_2 = x_2x_4$, τότε

$$u_1 + u_2 = x_1x_3 + x_2x_4 \notin \{ab : a \in I, b \in J\},$$

άτοπο. Για το λόγο αυτό να θυμόμαστε ότι το σύνολο IJ ορίζεται να είναι το

$$IJ = \{a_1b_1 + ... + a_nb_n : a_i \in I, b_i \in J, n \geq 1\} \trianglelefteq R$$

και όχι το $\{ab : a \in I, b \in J\}$.

(α′) Θα δείξουμε τους δύο εγκλεισμούς.

($\subseteq$) Έστω $a \in < m > + < n >$, τότε το a γράφεται ώς $a = mx + ny$ για κάποιους ακεραίους x και y. Ο d ως μέγιστος κοινός διαιρέτης των m και n, διαιρεί κάθε γραμμικό συνδυασμό τους και συνεπώς διαιρεί τον a, δηλαδή

$$d \mid a \Rightarrow \exists k \in \mathbb{Z} \text{ ώστε } a = kd$$

και έτσι $a \in < d >$.

($\supseteq$) Έστω τώρα ότι $a \in < d >$ και άρα υπάρχει κάποιο $k \in \mathbb{Z}$ ώστε $a = kd$. Ο d ως μέγιστος κοινός διαιρέτης των m και n είναι γραμμικός συνδυασμός τους, δηλαδή υπάρχουν $x, y \in \mathbb{Z}$ ώστε $d = mx + ny$ και έτσι

$$\begin{aligned} a = kd &= k(mx + ny) \\ &= kmx + kny \\ &= (km)x + (kn)y \in < m > + < n > \end{aligned}$$

(β′) Θα δείξουμε πάλι τους δύο εγκλεισμούς.

($\subseteq$) Έστω $a \in < m > \cap < n >$, τότε $a \in < m >$ και $a \in < n >$. Υπάρχουν λοιπόν $k, l \in \mathbb{Z}$ ώστε $a = km$ και $a = ln$. Έτσι το a είναι ένα κοινό πολλαπλάσιο των m και n. Το e ως το ελάχιστο κοινό τους πολλαπλάσιο έχει την ιδιότητα να διαιρεί κάθε άλλο. Ειδικότερα $e \mid a$ και άρα υπάρχει κάποιο $r \in \mathbb{Z}$ ώστε $a = re$. Συνεπώς $a \in < e >$.

($\supseteq$) Έστω τώρα ότι $a \in < e >$ και άρα υπάρχει κάποιο $k \in \mathbb{Z}$ ώστε $a = ke$. Το e είναι ένα κοινό πολλαπλάσιο των n και m, δηλαδή είναι

ένα πολλαπλάσιο του n και ένα πολλαπλάσιο του m. Συνεπώς $e = xm$ και $e = yn$ για κάποιους ακέραιους x, y. Έτσι

$$\begin{aligned} a = ke &= k(xm) \\ &= (kx)m \in < m > \end{aligned}$$

και

$$\begin{aligned} a = ke &= k(yn) \\ &= (ky)n \in < n > \end{aligned}$$

Συνεπώς $a \in < m > \cap < n >$.

(γ΄) Θα δείξουμε πάλι τους δύο εγκλεισμούς.

($\subseteq$) Έστω $w \in < m >< n >$, τότε υπάρχουν $a_1, ..., a_t \in < m >$ και $b_1, ..., b_t \in < n >$ ώστε

$$w = a_1b_1 + ... + a_tb_t.$$

Καθώς $a_1, ..., a_t \in < m >$, υπάρχουν $k_1, ..., k_t \in \mathbb{Z}$ ώστε

$$a_1 = k_1m$$

$$\dots$$

$$a_n = k_tm$$

Όμοια καθώς $b_1, ..., b_t \in < n >$, υπάρχουν $l_1, ..., l_t \in \mathbb{Z}$ ώστε

$$b_1 = l_1n$$

$$\dots$$

$$b_t = l_tn$$

Έτσι

$$\begin{aligned} w = a_1b_1 + ... + a_tb_t &= k_1ml_1n + ... + k_tml_tn \\ &= (k_1l_1)mn + ... + (k_tl_t)mn \\ &= (k_1l_1 + ... + k_tl_t)mn \end{aligned}$$

και άρα $w \in < mn >$.

($\supseteq$) Έστω $w \in < mn >$ τότε υπάρχει $x \in \mathbb{Z}$ ώστε $w = x(mn)$. Συνεπώς

$$\begin{aligned} w &= x(mn) \\ &= (xm)n \end{aligned}$$

κάθως $xm \in < m >$ και $n \in < n >$, γράψαμε το w ως πεπερασμένο άθροισμα (με έναν προσθεταίο) γινομένων στοιχείων του $< m >$ με στοιχεία του $< n >$ και άρα $w \in < m >< n >$.

38. [**Άσκηση 38**] Εξετάστε αν τα παρακάτω σύνολα είναι ιδεώδη του $\mathbb{Q}[x]$.

(α′) $A = \{f(x) \in \mathbb{Q}[x] : f(0) = 0\}$

(β′) $B = \{f(x) \in \mathbb{Q}[x] : f(0) = 1\}$

(γ′) $C = \{f(x) \in \mathbb{Q}[x] : f(\frac{1}{2}) = 0\}$

(δ′) $D = \{f(x) \in \mathbb{Q}[x] : f(\frac{1}{2}) \in 2\mathbb{Z}\}$

(ε′) $E = \{f(x) \in \mathbb{Q}[x] : f(1) = f(2) = 0\}$

(ϛ′) $F = \{f(x) \in \mathbb{Q}[x] : x^2 - 2x + 1 \mid f(x)\}$

Απάντηση: Ας θυμηθούμε τον ορισμό του ιδεώδους:

Ορισμός. Έστω R ένας δακτύλιος. Ένα μη κενό υποσύνολο I του R ονομάζεται ιδεώδες του R αν για κάθε $a, b \in I$ και $r \in R$, ισχύει $a - b \in I$ και $ar \in I$.

(α′) Κατ'αρχήν το σύνολο A είναι μη κενό αφού $x \in A$ και επιπλέον $A \subseteq \mathbb{Q}[x]$. Θεωρούμε τώρα δύο τυχαία στοιχεία $f(x), g(x) \in A$, τότε $f(0) = 0$ και $g(0) = 0$. Παρατηρούμε ότι $(f - g)(0) = f(0) - g(0) = 0 - 0 = 0$ και έτσι λοιπόν το στοιχείο $f(x) - g(x)$ ανήκει στο σύνολο A. Έστω τώρα ένα τυχαίο στοιχείο $r(x)$ του $\mathbb{Q}[x]$. Παρατηρούμε ότι $r(0)f(0) = r(0)0 = 0$ και έτσι το στοιχείο $r(x)f(x)$ ανήκει στο A. Συμερασμαστικά το A είναι ιδεώδες του δακτυλίου $\mathbb{Q}[x]$. Μια άλλη απάντηση θα μπορούσε να ήταν η εξής. Παρατηρούμε ότι το A περιέχει όλα τα πολυώνυμα με ρητούς συντελεστές, τα οποία έχουν ρίζα το 0. Γνωρίζουμε όμως από τη θεωρία ότι ένα πολυώνυμο $f(x)$ έχει ρίζα το 0 αν και μόνον αν $x \mid f(x)$ και έτσι το σύνολο A δύναται να περιγραφεί ως

$$\begin{aligned} A &= \{f(x) \in \mathbb{Q}[x] : x \mid f(x)\} \\ &= \{f(x) \in \mathbb{Q}[x] : \exists a(x) \in \mathbb{Q}[x] \text{ με } f(x) = xa(x)\} \\ &= \{xa(x) : a(x) \in \mathbb{Q}[x]\}. \end{aligned}$$

Θεωρούμε τώρα δύο τυχαία στοιχεία $f(x), g(x) \in A$, τότε υπάρχουν $a(x), b(x) \in \mathbb{Q}[x]$ ώστε $f(x) = xa(x)$ και $g(x) = xb(x)$. Παρατηρούμε ότι $f(x) - g(x) = xa(x) - xb(x) = x(a(x) - b(x)) \in A$. Επίσης, αν $r(x) \in \mathbb{Q}[x]$, τότε $f(x)r(x) = xa(x)r(x) = x(a(x)r(x)) \in A$ και συνεπώς το A είναι ιδεώδες του $\mathbb{Q}[x]$.

(β′) Το σύνολο B είναι μη κενό αφού $x + 1 \in B$. Θεωρούμε τα πολυώνυμα $f(x) = x + 1$ και $g(x) = x + 1$, τα οποία ανήκουν στο B. Αν το B ήταν ιδεώδες θα έπρεπε η διαφορά οποιονδήποτε δύο παλυωνύμων του

Β να ανήκει πάλι στο Β. Έτσι λοιπόν αν το Β ήταν ιδεώδες θα έπρέπε το $f(x)-g(x)$ να ανήκει στο Β. Όμως το πολυώνυμο $f(x)-g(x)$ είναι το μηδενικό, το οποίο δεν ανήκει στο Β. Άτοπο. Συνεπώς το Β δεν αποτελεί ιδεώδες του δακτυλίου $\mathbb{Q}[x]$.

(γ′) Το σύνολο C είναι μη κενό, αφού $2x-1 \in C$. Παρατηρούμε ότι το C περιέχει όλα τα πολυώνυμα με ρητούς συντελεστές τα οποία έχουν ρίζα το $\frac{1}{2}$. Γνωρίζουμε όμως από τη θεωρία ότι ένα πολυώνυμο $f(x)$ έχει ρίζα το $\frac{1}{2}$ αν και μόνον αν $x-\frac{1}{2} \mid f(x)$ και έτσι το σύνολο C δύναται να περιγραφεί ως

$$\begin{aligned} C &= \{f(x) \in \mathbb{Q}[x] : x-\frac{1}{2} \mid f(x)\} \\ &= \{f(x) \in \mathbb{Q}[x] : \exists a(x) \in \mathbb{Q}[x] \text{ με } f(x) = (x-\frac{1}{2})a(x)\} \\ &= \{(x-\frac{1}{2})a(x) : a(x) \in \mathbb{Q}[x]\}. \end{aligned}$$

Θεωρούμε τώρα δύο τυχαία στοιχεία $f(x), g(x) \in A$, τότε υπάρχουν $a(x), b(x) \in \mathbb{Q}[x]$ ώστε $f(x) = (x-\frac{1}{2})a(x)$ και $g(x) = (x-\frac{1}{2})b(x)$. Παρατηρούμε ότι $f(x)-g(x) = (x-\frac{1}{2})a(x)-(x-\frac{1}{2})b(x) = (x-\frac{1}{2})(a(x)-b(x)) \in C$. Επίσης, αν $r(x) \in \mathbb{Q}[x]$, τότε $f(x)r(x) = (x-\frac{1}{2})a(x)r(x) = (x-\frac{1}{2})(a(x)r(x)) \in C$ και συνεπώς το C είναι ιδεώδες του $\mathbb{Q}[x]$.

(δ′) Το σύνολο D δεν αποτελεί ιδεώδες. Πράγματι, αν ήταν ιδεώδες του $\mathbb{Q}[x]$ θα έπρεπε για κάθε $f(x) \in D$ και για κάθε $r(x) \in \mathbb{Q}[x]$ να ισχύει $r(x)f(x) \in D$. Παρατηρούμε όμως ότι για $f(x) = 2x+1$, έχουμε ότι $f(x) \in D$, μιας και $f(\frac{1}{2}) = 2 \in 2\mathbb{Z}$. Απο την άλλη για $r(x) = x \in \mathbb{Q}[x]$, έχουμε ότι $r(x)f(x) = 2x^2+x \notin D$, αφού $r(\frac{1}{2})f(\frac{1}{2}) = 1 \notin 2\mathbb{Z}$.

(ε′) Το σύνολο E είναι μη κενό, αφού $(x-1)(x-2) = x^2-3x+2 \in E$. Παρατηρούμε ότι το E περιέχει όλα τα πολυώνυμα με ρητούς συντελεστές τα οποία έχουν ρίζα και το 1 και το 2. Γνωρίζουμε όμως από τη θεωρία ότι ένα πολυώνυμο $f(x)$ έχει ρίζα το 1 αν και μόνον αν $x-1 \mid f(x)$ και έχει ρίζα το 2 αν και μόνον $x-2 \mid f(x)$. Έτσι λοιπόν $f(x) \in E$ αν και μόνον αν τα $x-1, x-2$ διαιρούν το $f(x)$, αν και μόνον αν $(x-1)(x-2) \mid f(x)$, δηλαδή αν και μόνον αν $x^2-3x+2 \mid f(x)$, αν και μόνον αν υπάρχει $a(x) \in \mathbb{Q}[x]$ ώστε $f(x) = a(x)(x^2-3x+2)$ Έτσι λοπόν $E = \{a(x)(x^2-3x+2) : a(x) \in \mathbb{Q}[x]\}$. Συνεχίστε όπως στα προηγούμενα ερωτήματα για να δείξετε ότι το Ε είναι πράγματι ένα ιδεώδες του $\mathbb{Q}[x]$.

(ϛ′) Αφήνεται ως άσκηση. Για οποιαδήποτε απορία μη διστάσετε να τη διατυπώσετε στο σύνδεσμο κουβέντα της ηλεκτρονικής τάξης.

Άννα Καρασούλου

39. **[Άσκηση 39]** Να εξετάσετε αν αληθεύουν οι παρακάτω συνεπαγωγές:

(α′) R ακεραία περιοχή $\Rightarrow R[x]$ ακεραία περιοχή.

(β′) R σώμα $\Rightarrow R[x]$ σώμα.

Απάντηση: Καλούνται οι φοιτητές να συμμετάσχουν μέσω της ηλεκτρονικής τάξης.

Άννα Καρασούλου

40. **[Άσκηση 40]** Δείξτε ότι η απεικόνιση $f : \mathbb{Z}_4 \to \mathbb{Z}_{10}$ με $f([x]_4) = [5x]_{10}$ είναι ένας ομομορφισμός δακτυλίων.

Κωνσταντίνος Λέντζος

41. **[Άσκηση 41]** Δείξτε ότι κάθε μη μηδενικός ομομορφισμούς δακτυλίων $\mathbb{R} \to \mathbb{R}$ είναι πάντα μονομορφισμός.

Απάντηση: Έστω $\phi : \mathbb{R} \to \mathbb{R}$ ένας μη μηδενικός ομομορφισμός δακτυλίων. Θέτουμε $K = ker\phi$. Γνωρίζουμε ότι ο πηρύνας ενός ομομορφισμό είναι ιδεώδες του πεδίου ορισμού, δηλαδή του $\mathbb{R}$. Το $\mathbb{R}$ όμως όπως και κάθε άλλο σώμα έχει δύο μόνο ιδεώδη τον εαυτό του και το μηδενικό. Έστω ότι $K = \mathbb{R}$, τότε από τον ορισμό του πηρύνα έχουμε $\phi(x) = 0$ για κάθε $x \in \mathbb{R}$. Άτοπο διότι ο ϕ επλέχθηκε ως μη μηδενικός. Έτσι αναγκαστικά λαμβάνουμε ότι $K = \{0\}$, που σημαίνει ότι ο ϕ είναι 1-1 όπως θέλαμε.

Κωνσταντίνος Λέντζος

42. **[Άσκηση 42]** Έστω $M_2(\mathbb{Z})$ το σύνολο των 2×2 πινάκων με στοιχεία ακεραίους. Να δείξετε ότι το $M_2(\mathbb{Z})$ εφοδιασμένο με τις συνήθεις πράξεις της πρόσθεσης και πολλαπλασιασμού πινάκων που μάθαμε στη γραμμική άλγεβρα είναι ένας δακτύλιος. Είναι μεταθετικός ή όχι; Έχει μονάδα; Ποιά είναι τα αντιστρέψιμα στοιχεία του; Είναι ακεραία περιοχή; Είναι σώμα;

Κωνσταντίνος Λέντζος

43. **[Άσκηση 43]**

(α′) Να βρέθει μεταθετικός δακτύλιος R με μονάδα, 1_R και υποδακτύλιός του S , ο οποίος να μην έχει μονάδα.

(β′) Να βρεθεί παράδειγμα πεπερασμένου μη μεταθετικού δακτυλίου.

(γ′) Να βρεθεί παράδειγμα άπειρου μη μεταθετικού δακτυλίου, ο οποίος να μην έχει μονάδα.

Απάντηση:

(α′) Ο δακτύλιος $\mathbb{Z}$ είναι μεταθετικός με μονάδα. Ο υποδακτύλιος του όμως $2\mathbb{Z}$ δεν έχει μονάδα (γιατί;).

(β′) Ένας πεπερασμένος μη μεταθετικός δακτυλιος είναι ο $M_2(\mathbb{Z}_3)$ (γιατί;).

(γ′) Ο δακτύλιος $M_2(2\mathbb{Z})$ είναι ένας απειρος μη μεταθετικός δακτύλιος που δεν έχει μονάδα (γιατί;).

Σχόλιο. Θυμηθείτε επίσης την άσκηση (27).

Κωνσταντίνος Λέντζος

44. **[Άσκηση 44]**

Έστω $S = \{a + bi : a, b \in 2\mathbb{Z}\}$. Δείξτε ότι ο S είναι ένας υποδακτύλιος του $Z[i]$, αλλά όχι ιδεώδες του.

Κωνσταντίνος Λέντζος

45. **[Άσκηση 45]** Αν ένα πολυώνυμο με ρητούς συντελεστές έχει ως ρίζα του το $\sqrt{2}$, να δείξετε ότι έχει και το $-\sqrt{2}$.

Απάντηση: Θεωρούμε την απεικόνιση $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{2}]$ με

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

Η ϕ είναι ομομορφισμός: Θεωρούμε $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ και έχουμε

$$\begin{aligned}\phi((a + b\sqrt{2}) + (c + d\sqrt{2})) &= \phi((a + c) + (b + d)\sqrt{2}) \\ &= (a + c) - (b + d)\sqrt{2} \\ &= (a - b\sqrt{2}) + (c - d\sqrt{2}) \\ &= \phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2})\end{aligned}$$

$$\begin{aligned}\phi((a + b\sqrt{2}) \cdot (c + d\sqrt{2})) &= \phi(ac + 2bd) + (ad + bc)\sqrt{2}) \\ &= (ac + 2bd) - (ad + bc)\sqrt{2}) \\ &= (a - b\sqrt{2}) \cdot (c - d\sqrt{2}) \\ &= \phi(a + b\sqrt{2}) \cdot \phi(c + d\sqrt{2})\end{aligned}$$

Η ϕ είναι επί: Έστω $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Θα δείξουμε ότι υπάρχει $x + y\sqrt{2}$ ώστε

$$\phi(x + y\sqrt{2}) = a + b\sqrt{2}.$$

Για $x + y\sqrt{2} = a - b\sqrt{2}$ έχουμε το επιθυμητό. Πράγματι, $\phi(x + y\sqrt{2}) = \phi(a - b\sqrt{2}) = a + b\sqrt{2}$.

Η ϕ είναι 1-1: Ας υπολογίσουμε τον πηρύνα της.

$$\begin{aligned} ker\phi &= \{a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}] : \phi(a + b\sqrt{2}) = 0 + 0\sqrt{2}\} \\ &= \{a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}] : a - b\sqrt{2}) = 0 + 0\sqrt{2}\} \\ &= \{0 + 0\sqrt{2}\} \end{aligned}$$

Έτσι λοιπόν η ϕ είναι ένας ισομορφισμός. Θεωρούμε τώρα μια άλλη απεικόνιση

$$F : \mathbb{Q}[\sqrt{2}][x] \to \mathbb{Q}[\sqrt{2}][x] \text{ με}$$

$$F(a_n x^n + ... + a_1 x + a_0) = \phi(a_n)x^n + ... + \phi(a_1)x + \phi(a_0).$$

Με $\mathbb{Q}[\sqrt{2}][x]$ συμβολίζουμε τα πολυώνυμα σε μια μεταβλητή των οποίων οι συντελεστές ανήκουν στο $\mathbb{Q}[\sqrt{2}]$. Παρατηρούμε ότι $\phi(g(x)) = g(x)$ για κάθε $g(x) \in \mathbb{Q}[x]$. Επίσης για κάθε $g(x) \in \mathbb{Q}[x]$ και $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ έχουμε ότι

$$F(g(a + b\sqrt{2})) = g(F(a + b\sqrt{2})).$$

Έστω τώρα $g(x) \in \mathbb{Q}[x]$, το οποίο έχει ρίζα το $\sqrt{2}$. Για $a + b\sqrt{2} = \sqrt{2}$ στην παραπάνω σχέση παίρνουμε

$$0 = F(0) = F(g(\sqrt{2})) = g(F(\sqrt{2})) = g(-\sqrt{2})$$

και άρα το $g(x)$ έχει και το $-\sqrt{2}$ ρίζα του.

Παρόμοια άσκηση. Δείξτε ότι αν ένα πολυώνυμο με ακεραίους συντελεστές έχει ως ρίζα του τον αριθμό $1 + \sqrt{3}$, τότε έχει και τον $1 - \sqrt{3}$.

Άννα Καρασούλου

46. **[Άσκηση 46]**

Δείξτε ότι ο δακτύλιος πηλίκο $\mathbb{Q}[x]/ < x^2 - 2 >$ είναι ισόμορφος με τον

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Απάντηση: Θέτουμε $I =< x^2 - 2 >$. Θα εφαρμόσουμε το πρώτο θεώρημα ισομορφισμών για δακτυλίους. Για το λόγο αυτό ορίζουμε $\phi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$ με $\phi(f(x)) = f(\sqrt{2})$. Η ϕ είναι καλά ορισμένη (γιατί;).

Η ϕ είναι ομομορφισμός: Θεωρούμε $f(x), g(x) \in \mathbb{Q}[x]$ και έχουμε

$$\begin{aligned}\phi(f(x) + g(x)) &= \phi((f+g)(x)) \\ &= (f+g)(\sqrt{2}) \\ &= f(\sqrt{2}) + g(\sqrt{2}) \\ &= \phi(f(x)) + \phi(g(x))\end{aligned}$$

$$\begin{aligned}\phi(f(x) \cdot g(x)) &= \phi((f \cdot g)(x)) \\ &= (f \cdot g)(\sqrt{2}) \\ &= f(\sqrt{2}) \cdot g(\sqrt{2}) \\ &= \phi(f(x)) \cdot \phi(g(x))\end{aligned}$$

Η ϕ είναι επί: Έστω $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ ένα τυχαίο στοιχείο. Θα πρέπει να δείξουμε ότι υπάρχει $f(x) \in \mathbb{Q}[x]$ έτσι ώστε

$\phi(f(x)) = a + b\sqrt{2}$.

Παρατηρούμε ότι για $f(x) = a + bx \in \mathbb{Q}[x]$ έχουμε το επιθυμητό. Πράγματι $\phi(f(x)) = \phi(a + bx) = a + b\sqrt{2}$.

Ισχύει $ker\phi = I$: Θα δείξουμε τους δύο εγκλεισμούς. ($\subseteq$) Έστω $f(x) \in \mathbb{Q}[x]$ με $f(x) \in ker\phi$, τότε $\phi(f(x)) = 0 + 0\sqrt{2}$. Ισοδύναμα $f(\sqrt{2}) = 0 + 0\sqrt{2}$. Το πολυώνυμο $f(x)$ έχει ρητούς συντελεστές και ρίζα το $\sqrt{2}$ από την άσκηση 45 επεται ότι έχει ρίζα και το $-\sqrt{2}$. Έτσι

$$x - \sqrt{2} \mid f(x) \quad \text{και} \quad x + \sqrt{2} \mid f(x).$$

Καθώς τα πολυώνυμα $x - \sqrt{2}$ και $x + \sqrt{2}$ είναι σχετικά πρώτα έπεται ότι $(x - \sqrt{2})(x + \sqrt{2}) \mid f(x)$. Συνεπάγεται $x^2 - 2 \mid f(x)$, που σημαίνει ότι υπάρχει κάποιο $\pi(x) \in \mathbb{Q}[x]$ ώστε $f(x) = (x^2 - 2)\pi(x)$. Συνεπώς

$$f(x) \in < x^2 - 2 >= I.$$

($\supseteq$) Έστω $f(x) \in I =< x^2 - 2 >$, τότε υπάρχει $a(x) \in \mathbb{Q}[x]$ ώστε $f(x) = a(x)(x^2 - 2)$. Υπολογίζουμε $\phi(f(x)) = f(\sqrt{2}) = a(\sqrt{2}) \cdot 0 = 0$ και άρα $f(x) \in ker\phi$ όπως θέλαμε.

Συνεπως από το πρώτο θεώρημα ισομορφισμών έχουμε ότι

$$\mathbb{Q}[x]/ < x^2 - 2 >= \mathbb{Q}[x]/ker\phi \cong Im\phi = \mathbb{Q}[\sqrt{2}].$$

Παρόμοια άσκηση: Δείξτε ότι ο δακτύλιος πηλίκο $\mathbb{Q}[x]/ < x^2 - 3 >$ είναι ισόμορφος με τον $\mathbb{Q}[\sqrt{3}]$.

Άννα Καρασούλου

47. **[Άσκηση 47]**

Εξετάστε αν οι δακτύλιοι $\mathbb{Q}[x]/ < x^2 - 1 >$ και $\mathbb{Q} \times \mathbb{Q}$ είναι ισόμορφοι.

Απάντηση: Θέτουμε $I =< x^2 - 1 >$. Θα εφαρμόσουμε το πρώτο θεώρημα ισομορφισμών για δακτυλίους. Για το λόγο αυτό ορίζουμε $\phi : \mathbb{Q}[x] \to \mathbb{Q} \times \mathbb{Q}$ με $\phi(f(x)) = (f(1), f(-1))$. Η ϕ είναι προφανώς καλά ορισμένη.

Η ϕ είναι ομομορφισμός: Θεωρούμε $f(x), g(x) \in \mathbb{Q}[x]$ και έχουμε

$$\begin{aligned}
\phi(f(x) + g(x)) &= \phi((f+g)(x)) \\
&= ((f+g)(1), (f+g)(-1)) \\
&= (f(1) + g(1), f(-1) + g(-1)) \\
&= (f(1), f(-1)) + (g(1), g(-1)) \\
&= \phi(f(x)) + \phi(g(x))
\end{aligned}$$

$$\begin{aligned}
\phi(f(x) \cdot g(x)) &= \phi((f \cdot g)(x)) \\
&= ((f \cdot g)(1), (f \cdot g)(-1)) \\
&= (f(1) \cdot g(1), f(-1) \cdot g(-1)) \\
&= (f(1), f(-1)) \cdot (g(1), g(-1)) \\
&= \phi(f(x)) \cdot \phi(g(x))
\end{aligned}$$

Η ϕ είναι επί: Έστω $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ ένα τυχαίο στοιχείο. Θα πρέπει να δείξουμε ότι υπάρχει $f(x) \in \mathbb{Q}[x]$ έτσι ώστε $\phi(f(x)) = (a, b)$. Ισοδύναμα

$$(f(1), f(-1)) = (a, b).$$

Παρατηρούμε ότι για $f(x) = \frac{a-b}{2}x + \frac{a+b}{2} \in \mathbb{Q}[x]$ έχουμε το επιθυμητό. Πράγματι

$$\begin{aligned}\phi(f(x)) &= (f(1), f(-1)) \\ &= \left(\frac{a-b}{2} + \frac{a+b}{2}\ ,\ \frac{b-a}{2} + \frac{a+b}{2}\right) \\ &= (a, b).\end{aligned}$$

Ισχύει $ker\phi = I$: Θα δείξουμε τους δύο εγκλεισμούς. ($\subseteq$) Έστω $f(x) \in \mathbb{Q}[x]$ με $f(x) \in ker\phi$, τότε $\phi(f(x)) = (0, 0)$. Ισοδύναμα $(f(1), f(-1)) = (0, 0)$ ή ισοδύναμα

$$f(1) = 0 \text{ και } f(-1) = 0,$$

που σημαίνει ότι και το 1 και το -1 είναι ρίζες του $f(x)$. Έτσι

$$x - 1 \mid f(x) \quad \text{και} \quad x + 1 \mid f(x).$$

Καθώς τα πολυώνυμα $x - 1$ και $x + 1$ είναι σχετικά πρώτα έπεται ότι

$$(x - 1)(x + 1) \mid f(x).$$

Συνεπάγεται $x^2 - 1 \mid f(x)$, που σημαίνει ότι υπάρχει κάποιο $\pi(x) \in \mathbb{Q}[x]$ ώστε $f(x) = (x^2 - 1)\pi(x)$. Συνεπώς

$$f(x) \in < x^2 - 1 >= I.$$

($\supseteq$) Έστω $f(x) \in I =< x^2 - 1 >$, τότε υπάρχει $a(x) \in \mathbb{Q}[x]$ ώστε $f(x) = a(x)(x^2 - 1)$. Υπολογίζουμε

$$\begin{aligned}\phi(f(x)) &= (f(1), f(-1)) \\ &= (a(1)0, a(-1)0 \\ &= (0, 0)\end{aligned}$$

και άρα $f(x) \in ker\phi$ όπως θέλαμε.

Συνεπως από το πρώτο θεώρημα ισομορφισμών έχουμε ότι

$$\mathbb{Q}[x]/ < x^2 - 1 >= \mathbb{Q}[x]/ker\phi \cong Im\phi = \mathbb{Q} \times \mathbb{Q}.$$

48. **[Άσκηση 48]**

Εξετάστε αν οι δακτύλιοι $\mathbb{Q}[x]/ < x^2 - 5x + 6 >$ και $\mathbb{Q} \times \mathbb{Q}$ είναι ισόμορφοι.

Απάντηση: Θέτουμε $I =< x^2 - 5x + 6 >$. Θα εφαρμόσουμε το πρώτο θεώρημα ισομορφισμών για δακτυλίους. Για το λόγο αυτό ορίζουμε

$$\phi : \mathbb{Q}[x] \to \mathbb{Q} \times \mathbb{Q}$$

με

$$\phi(f(x)) = (f(2), f(3)).$$

Η ϕ είναι προφανώς καλά ορισμένη.

Η ϕ είναι ομομορφισμός: Θεωρούμε $f(x), g(x) \in \mathbb{Q}[x]$ και έχουμε

$$\begin{aligned}
\phi(f(x) + g(x)) &= \phi((f + g)(x)) \\
&= ((f + g)(2), (f + g)(3)) \\
&= (f(2) + g(2), f(3) + g(3)) \\
&= (f(2), f(3)) + (g(2), g(3) \\
&= \phi(f(x)) + \phi(g(x))
\end{aligned}$$

$$\begin{aligned}
\phi(f(x) \cdot g(x)) &= \phi((f \cdot g)(x)) \\
&= ((f \cdot g)(2), (f \cdot g)(3)) \\
&= (f(2) \cdot g(2), f(3) \cdot g(3)) \\
&= (f(2), f(3)) \cdot (g(2), g(3)) \\
&= \phi(f(x)) \cdot \phi(g(x))
\end{aligned}$$

Η ϕ είναι επί: Έστω $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ ένα τυχαίο στοιχείο. Θα πρέπει να δείξουμε ότι υπάρχει $f(x) \in \mathbb{Q}[x]$ έτσι ώστε $\phi(f(x)) = (a, b)$. Ισοδύναμα $(f(2), f(3)) = (a, b)$. Παρατηρούμε ότι για

$$f(x) = (b - a)x + 3a - 2b \in \mathbb{Q}[x]$$

έχουμε το επιθυμητό. Πράγματι $\phi(f(x)) = (f(2), f(3)) = ((b - a)2 + 3a - 2b, (b - a)3 + 3a - 2b) = (a, b)$.

Ισχύει $ker\phi = I$: Θα δείξουμε τους δύο εγκλεισμούς. ($\subseteq$) Έστω $f(x) \in \mathbb{Q}[x]$ με $f(x) \in ker\phi$, τότε $\phi(f(x)) = (0, 0)$. Ισοδύναμα $(f(2), f(3)) = (0, 0)$ ή ισοδύναμα

$$f(2) = 0 \text{ και } f(3) = 0,$$

που σημαίνει ότι και το 2 και το 3 είναι ρίζες του $f(x)$. Έτσι

$$x - 2 \mid f(x) \quad \text{και} \quad x - 3 \mid f(x).$$

Καθώς τα πολυώνυμα $x - 2$ και $x - 3$ είναι σχετικά πρώτα έπεται ότι

$$(x - 2)(x - 3) \mid f(x).$$

Συνεπάγεται $x^2 - 5x + 6 \mid f(x)$, που σημαίνει ότι υπάρχει κάποιο $\pi(x) \in \mathbb{Q}[x]$ ώστε $f(x) = (x^2 - 5x + 6)\pi(x)$. Συνεπώς

$$f(x) \in < x^2 - 5x + 6 >= I.$$

($\supseteq$) Έστω $f(x) \in I =< x^2 - 5x + 6 >$, τότε υπάρχει $a(x) \in \mathbb{Q}[x]$ ώστε

$$f(x) = a(x)(x^2 - 5x + 6).$$

Υπολογίζουμε $\phi(f(x)) = (f(2), f(3)) = (a(2)0, a(3)0) = (0, 0)$ και άρα $f(x) \in ker\phi$ όπως θέλαμε.

Συνεπως από το πρώτο θεώρημα ισομορφισμών έχουμε ότι

$$\mathbb{Q}[x]/ < x^2 - 5x + 6 >= \mathbb{Q}[x]/ker\phi \cong Im\phi = \mathbb{Q} \times \mathbb{Q}.$$

Άννα Καρασούλου

49. **[Άσκηση 49]**

Δείξτε ότι ο δακτύλιος πηλίκο $\mathbb{Q}[x]/ < x^2 + 1 >$ είναι ισόμορφος με τον

$$\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}.$$

Απάντηση: Θέτουμε $I =< x^2 + 1 >$. Θα εφαρμόσουμε το πρώτο θεώρημα ισομορφισμών για δακτυλίους. Για το λόγο αυτό ορίζουμε $\phi : \mathbb{Q}[x] \to \mathbb{Q}[i]$ με

$$\phi(f(x)) = f(i).$$

Η ϕ είναι καλά ορισμένη (γιατί;).

Η ϕ είναι ομομορφισμός: Θεωρούμε $f(x), g(x) \in \mathbb{Q}[x]$ και έχουμε

$$\begin{aligned}\phi(f(x)+g(x)) &= \phi((f+g)(x)) \\ &= (f+g)(i) \\ &= f(i)+g(i) \\ &= \phi(f(x))+\phi(g(x))\end{aligned}$$

$$\begin{aligned}\phi(f(x)\cdot g(x)) &= \phi((f\cdot g)(x)) \\ &= (f\cdot g)(i) \\ &= f(i)\cdot g(i) \\ &= \phi(f(x))\cdot\phi(g(x))\end{aligned}$$

Η ϕ είναι επί: Έστω $a+bi \in \mathbb{Q}[i]$ ένα τυχαίο στοιχείο. Θα πρέπει να δείξουμε ότι υπάρχει $f(x) \in \mathbb{Q}[x]$ έτσι ώστε $\phi(f(x)) = a+bi$. Παρατηρούμε ότι για $f(x) = a+bx \in \mathbb{Q}[x]$ έχουμε το επιθυμητό. Πράγματι

$$\phi(f(x)) = \phi(a+bx) = a+bi.$$

Ισχύει $ker\phi = I$: Θα δείξουμε τους δύο εγκλεισμούς. ($\subseteq$) Έστω $f(x) \in \mathbb{Q}[x]$ με $f(x) \in ker\phi$, τότε $\phi(f(x)) = 0+0i$. Ισοδύναμα $f(i) = 0+0i$. Το πολυώνυμο $f(x)$ έχει ρητούς συντελεστές και ρίζα το i και άρα έχει ρίζα και το συζηγή μιγαδικό $-i$. Έτσι

$$x-i \mid f(x) \quad \text{και} \quad x+i \mid f(x).$$

Καθώς τα πολυώνυμα $x-i$ και $x+i$ είναι σχετικά πρώτα έπεται ότι

$$(x-i)(x+i) \mid f(x).$$

Συνεπάγεται $x^2+1 \mid f(x)$, που σημαίνει ότι υπάρχει κάποιο $\pi(x) \in \mathbb{Q}[x]$ ώστε $f(x) = (x^2+1)\pi(x)$. Συνεπώς

$$f(x) \in < x^2+1 > = I.$$

($\supseteq$) Έστω $f(x) \in I = < x^2+1 >$, τότε υπάρχει $a(x) \in \mathbb{Q}[x]$ ώστε $f(x) = a(x)(x^2+1)$. Υπολογίζουμε $\phi(f(x)) = f(i) = a(i)\cdot 0 = 0$ και άρα $f(x) \in ker\phi$ όπως θέλαμε.

Συνεπως από το πρώτο θεώρημα ισομορφισμών έχουμε ότι

$$\mathbb{Q}[x]/ < x^2+1 >= \mathbb{Q}[x]/ker\phi \cong Im\phi = \mathbb{Q}[i].$$

Άννα Καρασούλου

50. **[Άσκηση 50]**

Εξετάστε αν οι δακτύλιοι $\mathbb{Q}[x]/ < x^2-2 >$ και $\mathbb{Q}[x]/ < x^2-3 >$ είναι ισόμορφοι.

Απάντηση: Από την άσκηση (46) έχουμε ότι

$$\mathbb{Q}[x]/ < x^2-2 > \cong \mathbb{Q}[\sqrt{2}] \text{ και } \mathbb{Q}[x]/ < x^2-3 > \cong \mathbb{Q}[\sqrt{3}].$$

Θα δείξουμε ότι οι δακτύλιοι $\mathbb{Q}[\sqrt{2}]$ και $\mathbb{Q}[\sqrt{3}]$ δεν είναι ισόμορφοι και συνεπώς ούτε οι αρχικοί δακτύλιοι είναι ισόμορφοι. **Προς άτοπο** υποθέτουμε ότι

$$\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[\sqrt{3}].$$

Μπορείτε να συνεχίσετε;;

προσεχώς λεπτομέρειες...

Άννα Καρασούλου

51. **[Άσκηση 51]**

Δείξτε ότι το πολυώνυμο $f(x) = x^2+3x+2$ έχει 4 το πλήθος ρίζες στο $\mathbb{Z}_6$.

Απάντηση: Πράγματι

$f(1) = 1^2+3\cdot 1+2 = 0$

$f(2) = 2^2+3\cdot 2+2 = 0$

$f(4) = 4^2+3\cdot 4+2 = 0$

$f(5) = 5^2+3\cdot 5+2 = 0$

Σχόλιο: Γνωρίζουμε ότι ένα πολυώνυμο δεν μπορεί να έχει περισσότερες ρίζες από τον βαθμό του. Τι συμβαίνει εδώ; Η συζήτηση συνεχίζεται στο σύνδεσμο κουβέντα της ηλεκτρονικής τάξης!

Κωνσταντίνος Λέντζος

52. **[Άσκηση 52]** Να βρεθεί το τελευταίο ψηφίο του αριθμού $3^{220355} + 7^{220355}$.

Απάντηση: Το τελευταίο ψηφίο του παραπάνω αριθμού είναι το υπόλοιπο της διαίρεσης του αριθμού αυτού με το 10. Συνεπώς ζητείται

$$3^{220355} + 7^{220355} \mod 10.$$

Υπολογίζουμε πρώτα το $3^{220355} \mod 10$. Παρατηρούμε ότι ο μκδ$(3, 10) = 1$ και συνεπώς από το θεώρημα *Euler* έχουμε ότι

$$3^{\phi(10)} = 1 \mod 10.$$

Επιπλέον καθώς $\phi(10) = 4$ παίρνουμε ότι $3^4 = 1 \mod 10$. Γράφουμε

$$\begin{aligned} 3^{220355} &= 3^{55088\cdot 4+3} && \mod 10 \\ &= 3^{55088\cdot 4} \cdot 3^3 && \mod 10 \\ &= (3^4)^{5508} \cdot 3^3 && \mod 10 \\ &= 1^{5508} \cdot 3^3 && \mod 10 \\ &= 3^3 && \mod 10 \\ &= 7 && \mod 10 \end{aligned}$$

Εν συνεχεία υπολογίζουμε το $7^{220355} \mod 10$. Παρατηρούμε ότι ο μκδ$(7, 10) = 1$ και συνεπώς από το θεώρημα *Euler* έχουμε ότι

$$7^{\phi(10)} = 1 \mod 10.$$

Επιπλέον καθώς $\phi(10) = 4$ παίρνουμε ότι $7^4 = 1 \mod 10$. Γράφουμε

$$\begin{aligned} 7^{220355} &= 7^{55088\cdot 4+3} && \mod 10 \\ &= 7^{55088\cdot 4} \cdot 7^3 && \mod 10 \\ &= (7^4)^{5508} \cdot 7^3 && \mod 10 \\ &= 1^{5508} \cdot 7^3 && \mod 10 \\ &= 7^3 && \mod 10 \\ &= 343 && \mod 10 \\ &= 3 && \mod 10 \end{aligned}$$

Τελικά

$$\begin{aligned} 3^{220355} + 7^{220355} &= 7 + 3 && \mod 10 \\ &= 0 && \mod 10 \end{aligned}$$

Άννα Καρασούλου

53. **[Άσκηση 53]** Να βρεθούν τα τελευταία δύο ψηφία του αριθμού 7^{123}.

Απάντηση: Ζητείται να υπολογίσουμε το $7^{123} \mod 100$. Παρατηρούμε ότι μκδ$(7, 100) = 1$ και συνεπώς από το θεώρημα *Euler* έχουμε ότι

$$7^{\phi(100)} = 1 \mod 100.$$

Όμως $\phi(100) = 100(1-\frac{1}{2})(1-\frac{1}{5}) = 40$ και άρα $7^{40} = 1 \mod 100$. Γράφουμε

$$\begin{aligned} 7^{123} &= 7^{40\cdot 3+3} && \mod 100 \\ &= 7^{40\cdot 3} \cdot 7^3 && \mod 100 \\ &= (7^{40})^3 \cdot 7^3 && \mod 100 \\ &= 1^3 \cdot 7^3 && \mod 100 \\ &= 7^3 && \mod 100 \\ &= 343 && \mod 100 \\ &= 43 && \mod 100 \end{aligned}$$

Άννα Καρασούλου

54. **[Άσκηση 54]** Δείξτε ότι κάθε σώμα είναι και ακεραία περιοχή.

Απάντηση: Θυμηθείτε πρώτα τους αντίστοιχους ορισμούς. Θεωρούμε F ένα σώμα και $a, b \in F$ δύο στοιχεία του με $a \neq 0$ και $ab = 0$. Τότε πολλαπλασιάζοντας με a^{-1} από αριστερά παίρνουμε $b = 0$ και άρα το F είναι ακεραία περιοχή.

Κωνσταντίνος Λέντζος

55. **[Άσκηση 55]**

- Δείξτε ότι το στοιχείο $2x + 1$ του δακτυλίου $\mathbb{Z}_4[x]$ είναι αντιστρέψιμο.
- Έστω p ένας πρώτος αριθμός. Υπάρχουν μη σταθερά πολυώνυμα στοιχεία του δακτυλίου $\mathbb{Z}_p[x]$, τα οποία είναι αντιστρέψιμα ;
- Βρείτε ένα πολυώνυμο με ακεραίους συντελεστές το οποιό να έχει ως ρίζες του τους αριθμούς $\frac{1}{2}$ και $-\frac{1}{3}$.

Απάντηση:

- Παρατρούμε ότι $(2x+1)(2x+1) = 4x^2+4x+1 = 1$ και άρα $(2x+1)^{-1} = 2x + 1$.

- Όχι δεν υπάρχουν. Μπορείτε να εξηγήσετε γιατί;
- Αρχικά σκεφτόμαστε το πολυώνυμο $(x-\frac{1}{2})(x+\frac{1}{3})$ το οποίο δεν έχει ακεραίους ομώς συντελεστές. Έτσι καταλήγουμε στο $(6x-3)(6x+2) = 36x^2-6x-6 \in \mathbb{Z}[x]$.

Άννα Καρασούλου

56. **[Άσκηση 56]** Θεωρούμε τον δακτύλιο $\mathbb{Z}[x]$ και τον ομομορφισμό δακτυλίων

$$\phi : \mathbb{Z}[x] \to \mathbb{Z}_2 \times \mathbb{Z}_9$$

που ορίζεται ως εξής:

$$\phi(a_n x^n + ... + a_1 x + a_0) = (a_0 \mod 2\ ,\ a_0 \mod 9).$$

Να βρεθεί ο πυρήνας του ομομορφισμού. Να βρεθεί επίσης πολυώνυμο $f(x) \in \mathbb{Z}[x]$ ώστε $\phi(f(x)) = \phi(x^2+3)$ και $f(0) \neq 3$.

Απάντηση: Η άσκηση θεωρεί ως δεδομένο ότι η απεικόνιση ϕ είναι πράγματι ομομορφισμός δακτυλίων. Αν δεν το ανέφερε θα έπρεπε να το αποδείξουμε. Μπορείτε να το δοκιμάσετε για εξάσκηση. Ας βρούμε τώρα τον πυρήνα του. Ο πυρήνας αποτελείται από όλα τα πολυώνυμα με ακεραίους συντελεστές που απεικονίζονται μέσω του ϕ στο $(0 \mod 2\ ,\ 0 \mod 9)$. Έτσι αν

$$a_n x^n + ... + a_1 x + a_0$$

είναι ένα πολυώνυμο του πυρήνα, τότε ο σταθερός του όρος ικανοποιεί τις σχέσεις:

$$a_0 = 0 \mod 2 \textbf{ και } a_0 = 0 \mod 9.$$

Οδηγούμαστε στο συμπέρασμα ότι και το 2 και το 9 διαιρεί το a_0. Συνεπώς το 18 διαιρεί το a_0 αφού μκδ$(2,9) = 1$. Από την άλλη μεριά αν το 18 διαιρεί το a_0, τότε εύκολα καταλήγουμε στο συμπέρασμα ότι το πολυώνυμο βρίσκεται στον πυρήνα. Τελικά

$$ker\phi = \{a_n x^n + ... + a_1 x + a_0 \in \mathbb{Z}[x] : 18 | a_0\}.$$

Για το δεύτερο ερώτημα τώρα έχουμε $\phi(x^2+3) = (3 \mod 2\ ,\ 3 \mod 9)$. Αναζητούμε ακέραιο a_0 με

$$3 \mod 2 = a_0 \mod 2 = 1 \mod 2$$

και

$$3 \mod 9 = a_0 \mod 9.$$

Άρα $2|a_0 - 3$ και $9|a_0 - 3$, δηλαδή $18|a_0 - 3$, που σημαίνει υπάρχει $\lambda \in \mathbb{Z}$ ώστε

$$a_0 = 3 + 18\lambda.$$

Το συμπέρασμα είναι ότι τα πολυώνυμα $f(x) \in \mathbb{Z}[x]$ με $\phi(f(x)) = \phi(x^2 + 3)$ είναι τα πολυώνυμα με ακεραίους συντελεστές, ο σταθερός όρος των οποίων είναι της μορφής $3 + 18\lambda$ για κάποιο $\lambda \in \mathbb{Z}$. Βέβαια έχουμε και την απαίτηση να ισχύει $f(0) \neq 3$. Αρκεί για αυτό να διαλέξουμε $\lambda \neq 0$. Η απάντηση λοιπόν σε αυτή την ερώτηση είναι ότι το ζητούμενο πολυώνυμο $f(x)$ είναι ένα οποιοδήποτε πολυώνυμο με ακεραίους συντελεστές και με σταθερό όρο της μορφής $3 + 18\lambda$ για κάποιο μη μηδενικό ακέραιο λ.

Άννα Καρασούλου

57. **[Άσκηση 57]** Θέματα εξετάσεων Φεβρουαρίου 2010

(α′) **Θέμα 1 Ομάδα Α**

Για κάθε μία από τις ακόλουθες προτάσεις, αποφανθείτε αν είναι σωστή ή λάθος. Οι απαντήσεις σας πρέπει να είναι πλήρως δικαιολογημένες.

i. Ο δακτύλιος $(\mathbb{Z}_{32}, +, \cdot)$ και ο δακτύλιος $(\mathbb{Z}_{60}, +, \cdot)$ έχουν το ίδιο πλήθος αντιστρεψίμων στοιχείων

ii. Η απεικόνιση $\phi : \mathbb{C} \longrightarrow \mathbb{R}$ με $\phi(\alpha + \beta i) = \alpha$ για $\alpha, \beta \in \mathbb{R}$ είναι ομομορφισμός δακτυλίων

iii. Η ένωση δύο οποιονδήποτε ιδεωδών του δακτυλίου $\mathbb{Z}[x]$ είναι ιδεώδες του ιδίου δακτυλίου $\mathbb{Z}[x]$

iv. Δεν υπάρχει στοιχείο της συμμετρικής ομάδας S_5 το οποίο να έχει τάξη μεγαλύτερη του 5

v. Η τομή δύο οποιονδήποτε κυκλικών υποομάδων μιας ομάδας G είναι επίσης κυκλική υποομάδα της G

vi. Υπάρχει μοναδικό ανάγωγο πολυώνυμο $f(x) \in \mathbb{Z}_2[x]$ τέτοιο ώστε $f(1) = 0$

(β′) **Θέμα 1 Ομάδα Β**

Για κάθε μία από τις ακόλουθες προτάσεις, αποφανθείτε αν είναι σωστή ή λάθος. Οι απαντήσεις σας πρέπει να είναι πλήρως δικαιολογημένες.

i. Ο δακτύλιος $(\mathbb{Z}_{64}, +, \cdot)$ και ο δακτύλιος $(\mathbb{Z}_{120}, +, \cdot)$ έχουν το ίδιο πλήθος αντιστρεψίμων στοιχείων

ii. Η ένωση δύο οποιονδήποτε ιδεωδών του δακτυλίου $\mathbb{R}[x]$ είναι ιδεώδες του ιδίου δακτυλίου $\mathbb{R}[x]$

iii. Η τομή δύο οποιονδήποτε άπειρων υποομάδων μιας άπειρης κυκλικής ομάδας έχει άπειρο πλήθος στοιχείων.

iv. Δεν υπάρχει στοιχείο της συμμετρικής ομάδας S_7 το οποίο να έχει τάξη μεγαλύτερη του 7

v. Υπάρχει μοναδικό ανάγωγο πολυώνυμο $f(x) \in \mathbb{Z}_2[x]$ τέτοιο ώστε $f(1) = 0$

vi. Η απεικόνιση $\phi : \mathbb{C} \longrightarrow \mathbb{R}$ με $\phi(\alpha + \beta i) = \beta$ για $\alpha, \beta \in \mathbb{R}$ είναι ομομορφισμός δακτυλίων

(γ′) **Θέμα 2 Ομάδα Α**

Δίνεται το πολυώνυμο $g(x) = x^2+x+1 \in \mathbb{Z}_3[x]$ και ο δακτύλιος -πηλίκο $\frac{\mathbb{Z}_3[x]}{<g(x)>}$

i. Να αναλύσετε το $g(x)$ σε γινόμενο αναγώγων πολυωνύμων του $\mathbb{Z}_3[x]$

ii. Πόσα στοιχεία έχει ο δακτύλιος R;

iii. Να δείξετε ότι το $-x+ < g(x) >$ είναι αντιστρέψιμο στοιχείο του R και να υπολογίσετε την τάξη του στοιχείου αυτού στην ομάδα $U(R)$ των αντιστρεψίμων στοιχείων του R.

(δ′) **Θέμα 2 Ομάδα Β**

Δίνεται το πολυώνυμο $g(x) = x^2-x+1 \in \mathbb{Z}_3[x]$ και ο δακτύλιος -πηλίκο $\frac{\mathbb{Z}_3[x]}{<g(x)>}$

i. Να αναλύσετε το $g(x)$ σε γινόμενο αναγώγων πολυωνύμων του $\mathbb{Z}_3[x]$

ii. Πόσα στοιχεία έχει ο δακτύλιος R;

iii. Να δείξετε ότι το $x+ < g(x) >$ είναι αντιστρέψιμο στοιχείο του R και να υπολογίσετε την τάξη του στοιχείου αυτού στην ομάδα $U(R)$ των αντιστρεψίμων στοιχείων του R.

(ε′) **Θέμα 3 Ομάδα Α**

Δίνονται τα πολυώνυμα $f(x) = x^4 - 1$ και $g(x) = x^9 - 1$ του $\mathbb{C}[x]$

i. Να υπολογίσετε τον Μέγιστο Κοινό Διαιρέτη $d(x)$ των $f(x)$ και $g(x)$ και να βρείτε πολυώνυμα $\lambda(x), \mu(x) \in \mathbb{C}[x]$, τέτοια ώστε $d(x) = \lambda(x)f(x) + \mu(x)g(x)$

ii. Να βρείτε πολυώνυμα $\alpha(x), \beta(x) \in \mathbb{C}[x]$ τέτοια ώστε $x^{2010} - 1 = \alpha(x)f(x) + \beta(x)g(x)$.

iii. Να δείξετε ότι το σύνολο G των μιγαδικών ριζών του $g(x)$ αποτελεί ομάδα με πράξη τον πολλαπλασιασμό των μιγαδικών αριθμών

iv. Να υπολογίσετε την τάξη της ομάδας G και να δείξετε ότι έχει μία τουλάχιστον υποομάδα διαφορετική από τις υποομάδες $\{1\}$ και G

(ϛ′) **Θέμα 3 Ομάδα Β**

Δίνονται τα πολυώνυμα $f(x) = x(x^4 - 1)$ και $g(x) = x^9 - 1$ του $\mathbb{C}[x]$

i. Να υπολογίσετε τον Μέγιστο Κοινό Διαιρέτη $d(x)$ των $f(x)$ και $g(x)$ και να βρείτε πολυώνυμα $\lambda(x), \mu(x) \in \mathbb{C}[x]$, τέτοια ώστε $d(x) = \lambda(x)f(x) + \mu(x)g(x)$

ii. Να βρείτε πολυώνυμα $\alpha(x), \beta(x) \in \mathbb{C}[x]$ τέτοια ώστε $x^{2010} - 1 = \alpha(x)f(x) + \beta(x)g(x)$.

iii. Να δείξετε ότι το σύνολο G των μιγαδικών ριζών του $g(x)$ αποτελεί ομάδα με πράξη τον πολλαπλασιασμό των μιγαδικών αριθμών

iv. Να υπολογίσετε την τάξη της ομάδας G και να δείξετε ότι έχει μία τουλάχιστον υποομάδα διαφορετική από τις υποομάδες $\{1\}$ και G

(ζ′) **Θέμα 4 Ομάδα Α**

Δίνεται η κυκλική μετάθεση $\tau = (123456789\ 10) \in S_{10}$

i. Γράψτε τις μεταθέσεις τ^2 και τ^5 ως γινόμενα ξένων κύκλων.

ii. Ποιές από τις μεταθέσεις τ^κ για $\kappa \in \{1, 2, 3, \cdots, 10\}$ έχουν τάξη ίση με 5;

iii. Να αποφανθείτε εάν η μετάθεση τ είναι άρτια ή περιττή και να δείξετε ότι δεν υπάρχει μετάθεση $\sigma \in S_{10}$ τέτοια ώστε $\sigma^2 = \tau$

(η′) **Θέμα 4 Ομάδα Β**

Δίνεται η κυκλική μετάθεση $\tau = (123456789\ 10) \in S_{10}$

i. Γράψτε τις μεταθέσεις τ^2 και τ^5 ως γινόμενα ξένων κύκλων.

ii. Ποιές από τις μεταθέσεις τ^κ για $\kappa \in \{1, 2, 3, \cdots, 10\}$ έχουν τάξη ίση με 5;

iii. Να αποφανθείτε εάν η μετάθεση τ είναι άρτια ή περιττή και να δείξετε ότι δεν υπάρχει μετάθεση $\sigma \in S_{10}$ τέτοια ώστε $\sigma^2 = \tau$

Τελευταία ενημέρωση: 4 Δεκεμβρίου 2013