Βασική Άλγεβρα
Θέματα Εξετάσεων Ιανουαρίου 2018

1. Δίνεται το σύνολο $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$.

(α) Δείξτε ότι το R είναι υποδακτύλιος του $M_2(\mathbb{Z})$.

(β) Είναι η απεικόνιση $\varphi : R \to \mathbb{Z}$ με $\varphi \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a + b$ ομομορφισμός δακτυλίων;

(γ) Υπάρχει επιμορφισμός δακτυλίων $\psi : R \to \mathbb{Z} \times \mathbb{Z}$;

2. Δίνεται το πολυώνυμο $x^4 + x^2 \in \mathbb{Z}_2[x]$, το κύριο ιδεώδες $I = \langle x^4 + x^2 \rangle \subseteq \mathbb{Z}_2[x]$ και ο δακτύλιος πηλίκο $R = \mathbb{Z}_2[x]/I$.

(α) Υπολογίστε το πλήθος των στοιχείων του δακτυλίου R και την τάξη της ομάδας $U(R)$ των αντιστρέψιμων στοιχείων του.

(β) Αν το πολυώνυμο $f(x) \in \mathbb{Z}_2[x]$ δεν έχει ρίζες στο σώμα $\mathbb{Z}_2$ και $\xi \in R$ είναι η κλάση του $f(x)$ στο πηλίκο, δείξτε ότι υπάρχει θετικός ακέραιος n τέτοιος ώστε $\xi^n = 1 \in R$.

(γ) Αν $\zeta \in R$ είναι η κλάση του πολυωνύμου $g(x) = x^{27} + x^9 + x^3 + 1 \in \mathbb{Z}_2[x]$ στο πηλίκο, δείξτε ότι $\zeta^n \neq 1 \in R$ για κάθε θετικό ακέραιο n.

3. Δίνονται ομάδα G τάξης $|G| \leq 140$ και υποομάδες H και K της G τάξεων $|H| = 8$ και $|K| = 9$.

(α) Υπολογίστε την τάξη της G.

(β) Δείξτε ότι $[G : H \cap K] = [G : H][G : K]$.

(γ) Δείξτε ότι κάθε $x \in G$ μπορεί να γραφεί στη μορφή $x = ab$, με $a \in H$ και $b \in K$.

4. Δίνεται η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & u & 1 & v & 2 & 6 & 4 \end{pmatrix} \in S_8$, όπου $u, v \in \{3, 5\}$. Υποθέτουμε ότι η μετάθεση σ^{2018} είναι γεννήτορας της κυκλικής υποομάδας $\langle \sigma \rangle$ της S_8 που παράγεται από τη σ.

(α) Βρείτε τις τιμές των u και v.

(β) Δείξτε ότι υπάρχει $w \in S_8$ τέτοια ώστε $\sigma^2 = w \sigma w^{-1}$.

(γ) Δείξτε ότι για κάθε αβελιανή ομάδα A και κάθε ομομορφισμό ομάδων $\varphi : S_8 \longrightarrow A$ ισχύει ότι $\langle \sigma \rangle \subseteq \ker(\varphi)$.

Να απαντήσετε σε όλα τα ερωτήματα.
Να δικαιολογήσετε πλήρως τις απαντήσεις σας.
Αθήνα 2/2/2018 – Καλή Επιτυχία

Βασική Άλγεβρα
Θέματα Εξετάσεων Ιανουαρίου 2018
Λύσεις

1. α΄) Θεωρούμε τυχόντα στοιχεία

$$X = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, Y = \begin{pmatrix} m & n \\ 0 & m \end{pmatrix} \in R$$

Αρκεί να δείξουμε ότι $X - Y, XY \in R$.Ισχύει

$$X - Y = \begin{pmatrix} a-m & b-n \\ 0 & a-m \end{pmatrix} \in R$$

και

$$XY = \begin{pmatrix} am & an+bm \\ 0 & am \end{pmatrix} \in R$$

Το ζητούμενο έπεται.

β΄) Έστω ότι ο ϕ είναι ομομορφισμός δακτυλίων.Παρατηρούμε ότι

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \xrightarrow{\phi} 1 \text{ και } \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \xrightarrow{\phi} 0$$

Θα έπρεπε λοιπόν

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 \xrightarrow{\phi} 1^2 = 1$$

Παρόλ΄ αυτά,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \xrightarrow{\phi} 0 \neq 1$$

άτοπο.Συμπεραίνουμε ότι ο ϕ δεν είναι ομομορφισμός δακτυλίων.

γ΄) Έστω ότι υπάρχει τέτοιος επιμορφισμός.Οι δακτύλιοι $R, \mathbb{Z} \times \mathbb{Z}$ έχουν μοναδιαία στοιχεία τα

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ και } (1,1)$$

αντίστοιχα,επομένως,αφού ο ψ είναι επιμορφισμός,θα πρέπει να ισχύει

$$\psi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = (1,1)$$

Έστω ότι

$$\psi\left(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right) = (x,y) \in \mathbb{Z} \times \mathbb{Z}$$

Όπως είδαμε και παραπάνω,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

οπότε,αφού ο ψ είναι ομομορφισμός,θα πρέπει $(x,y)^2 = (0,0) \Rightarrow x = y = 0$.Θεωρούμε τώρα τυχόν

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

Παρατηρούμε ότι ισχύει

$$X = aI_2 + b\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

άρα $\psi(X) = a\psi(I_2) + b \cdot 0 = (a,a)$.Τότε όμως $\operatorname{Im}\psi \subseteqq \{(a,a) : a \in \mathbb{Z}\} \subsetneqq \mathbb{Z} \times \mathbb{Z}$,άτοπο.Συνεπώς,δεν υπάρχει τέτοιος επιμορφισμός.

2. α΄) Το πλήθος των στοιχείων του R είναι ίσο με το πλήθος των δυνατών υπολοίπων στη διαίρεση με το $x^4 + x^2$ στο σώμα $\mathbb{Z}_2$.Αύτα είναι όλα τα πολυώνυμα βαθμού το πολύ 3 με συντελεστές από το $\mathbb{Z}_2$.Αυτά όμως είναι σε πλήθος $2 \cdot 2 \cdot 2 \cdot 2 = 16$,άρα ο R έχει 16 στοιχεία.Παρατηρούμε ότι,αφού δουλεύουμε στο $\mathbb{Z}_2$,ισχύει $x^4 + x^2 = x^4 - x^2 = x^2(x-1)(x+1) = x^2(x-1)^2$.Τα αντιστρέψιμα στοιχεία του R είναι όλα τα $p(x) \in \mathbb{Z}_2[x]$ που είναι τέτοια ώστε $\mu\kappa\delta(p(x), x^4 + x^2) = 1$.Αφού το $x^4 + x^2$ έχει τελικά ρίζες όλα τα στοιχεία του $\mathbb{Z}_2$,θα πρέπει το p να μην έχει καμία ρίζα.
   - $\deg(p) = 0$.Το μοναδικό δεκτό πολυώνυμο είναι το $p(x) = 1$.
   - $\deg(p) = 1$.Τα πιθανά πολυώνυμα είναι τα $x, x+1$.Κανένα δεν είναι αποδεκτό.
   - $\deg(p) = 2$.Υπάρχουν τα πολυώνυμα $x^2, x^2+1, x^2+x, x^2+x+1$.Αποδεκτό μόνο το $p(x) = x^2+x+1$,καθώς τα άλλα έχουν ριζες στο $\mathbb{Z}_2$.
   - $\deg(p) = 3$.Πιθανά πολυώνυμα είναι μόνο αυτά που έχουν σταθερό όρο ίσο με 1,καθώς τα υπόλοιπα έχουν ρίζα το 0.Αυτά είναι τα $x^3+1, x^3+x+1, x^3+x^2+1, x^3+x^2+x+1$.Αποδεκτά είναι τα $p(x) = x^3+x+1, q(x) = x^3+x^2+1$.

   Από τα παραπάνω,συμπεραίνουμε ότι ο δακτύλιος R έχει 4 αντιστρέψιμα στοιχεία.

   β΄) Έστω $p(x)$ το υπόλοιπο της διαίρεσης του $f(x)$ με το $x^4 + x^2$ και

$$f(x) = (x^4 + x^2) \cdot \pi(x) + p(x)$$

η ταυτότητα της ευκλείδειας διαίρεσης στο $\mathbb{Z}_2$.Αφού το x^4+x^2 έχει ρίζα κάθε στοιχείο του $\mathbb{Z}_2$,από τη σχέση αυτή συμπεραίνουμε ότι το $p(x)$ επίσης δεν έχει ρίζες.Σύμφωνα λοιπόν με το παραπάνω ερώτημα,$p(x)+I \in U(R) \Rightarrow \xi \in U(R)$ και $p(x) \in \{1, x^2+x+1, x^3+x+1, x^3+x^2+1\}$.
• $p(x)=1$.Το ζητούμενο σε αυτήν την περίπτωση είναι προφάνες.
• $p(x)=x^2+x+1$.Τότε,

$$\xi^2 = p^2(x)+I = x^4+x^2+1+2x^3+2x^2+2x+I = x^4+x^2+1+I = 1+I$$

άρα $\xi^2=1$.
• $p(x)=x^3+x+1$.Τότε

$$\xi^2 = p^2(x)+I = x^6+x^2+1+I = x^2(x^4+1)+1+I = x^2(x-1)^4+1+I = 1+I$$

άρα $\xi^2=1$.
• $p(x)=x^3+x^2+1$.Τότε

$$\xi^2 = p^2(x)+I = x^6+x^4+1+I = x^4(x^2+1)+1+I = x^4(x-1)^2+1+I = 1+I$$

άρα $\xi^2=1$. Σε κάθε περίπτωση λοιπόν το ζητούμενο ισχύει.

γ΄) Έστω ότι υπάρχει τέτοιος ακέραιος n.Τότε,το $g(x)+I$ είναι αντιστρέψιμο στοιχείο του δακτυλίου R.Αυτό όμως δεν ισχύει.Πράγματι,$g(1)=0$,οπότε $x-1 \mid g(x) \Rightarrow \mu\kappa\delta(g(x), x^4+x^2) \neq 1$.Άρα,$\zeta^n \neq 1$ για κάθε $n \in \mathbb{N}$.

3. α΄) Αφού $|H|=8$,συμπεραίνουμε ότι $8 \mid |G|$.Ομοίως,$9 \mid |G|$.Αφού $\mu\kappa\delta(8,9)=1$,έπεται ότι $8 \cdot 9 \mid |G| \Rightarrow 72 \mid |G|$.Γνωρίζουμε επιπλέον ότι $|G| \leq 140$,άρα αναγκαστικά $|G|=72$.

β΄) Η $H \cap K$ είναι υποομάδα των K, H,άρα,σύμφωνα με το θεώρημα του Lagrange,η τάξη της θα πρέπει να διαιρεί την τάξη και των δύο.Με λίγα λόγια,$|H \cap K| \mid 9$ και $|H \cap K| \mid 8$,από όπου έπεται ότι $|H \cap K|=1$.Σύμφωνα λοιπόν με το θεώρημα του Lagrange,

$$[G : H \cap K] = \frac{|G|}{|H \cap K|} = 72 \ , \ [G:K] = \frac{|G|}{|K|} = 8 \ , \ [G:H] = \frac{|G|}{|H|} = 9$$

Το ζητούμενο έπεται.

γ΄) Θεωρούμε όλα τα γινόμενα της μορφής hk όπου $h \in H, k \in K$.Αυτά είναι σε πλήθος $8 \cdot 9 = 72$ (κάποια από τα οποία πιθανόν να είναι ίσα μεταξύ τους).Θα αποδείξουμε ότι αυτά τα γινόμενα είναι διαφορετικά ανά δύο.Έστω ότι $h_1k_1 = h_2k_2$.Τότε,$h_2^{-1}h_1 = k_2k_1^{-1}$.Όμως,$h_2^{-1}h_1 \in H$, $k_2k_1^{-1} \in K$,και έχουμε ήδη δει παραπάνω ότι $H \cap K = \{1\}$.Από αυτά συμπεραίνουμε ότι $h_2^{-1}h_1 = k_2k_1^{-1} = 1 \Rightarrow h_1 = h_2$ και $k_1 = k_2$ όπως θέλαμε.Αν λοιπόν $A = \{hk : h \in H, k \in K\}$,τότε $|A| = 72$.Ταυτόχρονα όμως,$A \subseteq G$ και $|G| = 72 = |A|$,από όπου προκύπτει ότι $G = A$.Άρα,για κάθε $x \in G$,υπάρχουν $a \in H, b \in K$,τέτοια ώστε $x = ab$,όπως θέλαμε.

4. α΄) Ισχύει $\sigma = (1\ 8\ 4)(2\ 7\ 6)(3\ 5)$ ή $\sigma = (1\ 8\ 4)(2\ 7\ 6)$,άρα $o(\sigma) = 6$ ή $o(\sigma) = 3$.Επίσης,$2018 = 6 \cdot 336 + 2$ άρα,δεδομένου ότι $\sigma^6 = i$,έπεται ότι $\sigma^{2018} = \sigma^2$.Αφού

ο σ^2 είναι γεννήτορας της $\langle\sigma\rangle$,συμπεραίνουμε ότι μκδ$(o(\sigma), 2) = 1 \Rightarrow o(\sigma) = 3$.Συνεπώς,$u = 3, v = 5$.

β΄) Γνωρίζουμε από τη θεωρία πως υπάρχει τέτοια μετάθεση αν και μόνο αν οι σ, σ^2 έχουν τον ίδιο τύπο.Αρκεί λοιπόν να δείξουμε ότι οι σ, σ^2 έχουν τον ίδιο τύπο.Ο τύπος της σ είναι $(1, 1, 3, 3)$.Επιπλέον,παρατηρούμε ότι

$$\sigma^2 = (3)(5)(1\ 4\ 8)(2\ 6\ 7)$$

άρα ο τύπος της σ^2 είναι επίσης $(1, 1, 3, 3)$,και το ζητούμενο έπεται.

γ΄) Θα αποδείξουμε ότι $\phi(\sigma) = 1$.Τότε,$\phi\left(\sigma^k\right) = 1^k = 1$ για κάθε ακέραιο k,το οποίο είναι το ζητούμενο.Έχουμε

$$\phi\left(\sigma^2\right) = \phi\left(w\sigma w^{-1}\right) = \phi(w)\phi(\sigma)\phi\left(w^{-1}\right) = \phi(\sigma)$$

όπου η τελευταία ισότητα προέκυψε επειδή η A είναι αβελιανή.Συνεπώς,

$$\phi\left(\sigma^2\right) = \phi(\sigma) \Rightarrow \phi(\sigma)^2 = \phi(\sigma) \Rightarrow \phi(\sigma) = 1$$

το οποίο είναι το ζητούμενο.