ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΕΞΕΤΑΣΗ ΣΤΟ ΜΑΘΗΜΑ

Αλγεβρα

24 Ιουνίου 2022

1. Έστω $a = (12453)(274)$, $b = (234)(435)$ και
$$c = a^{-492}b^{1823}a^{1914}(a^2ba)^{-2022}$$
μεταθέσεις του S_7. Να τις γράψετε σαν γινόμενο κύκλων ξένων μεταξύ τους, σαν γινόμενο 2-κύκλων, να βρείτε την τάξη τους και να βρείτε αν είναι άρτιες ή περιττές.

2. (i) Να βρεθεί το υπόλοιπο της διαίρεσης $4^{19916} : 13$.
   (ii) Να βρεθεί ο αντίστροφος του 1234 στο $\mathbb{Z}^*_{33349}$

3. Να εξετάσετε ποια από τα παρακάτω είναι ιδεώδη του $\mathbb{Q}[x]$.
   (i) $A = \{f(x) \in \mathbb{Q}[x] \mid f(1) = f(2) = 0\}$
   (ii) $B = \{f(x) \in \mathbb{Q}[x] \mid x^2 - 2x + 1$ διαιρεί το $f(x)\}$
   (iii) $C = \{f(x) \in \mathbb{Q}[x] \mid f(\frac{1}{2}) \in 2\mathbb{Z}\}$

4. Εξετάστε αν η ομάδα $U(\mathbb{Z}_8)$ των αντιστρέψιμων στοιχείων της $\mathbb{Z}_8$ είναι ισομορφική με την $\mathbb{Z}_4$.

5. (i) Έστω $\mathbb{R}$ το σώμα των πραγματικών αριθμών και I το ιδεώδες του $\mathbb{R}[x]$ που παράγεται από το $x^2 + 1$. Δείξτε ότι $\mathbb{R}[x]/I \cong \mathbb{C}$.
   (ii) Κατασκευάστε ένα σώμα με 81 στοιχεία.

ΚΑΛΗ ΕΠΙΤΥΧΙΑ

Β. Μεταφτσής

Ενδεικτικές Λύσεις

1. $a = (12753), b = (235), a^2ba = (12375)$, $492 \equiv 2 \pmod 5$, $1823 \equiv 2 \pmod 3$, $1914 \equiv 4 \pmod 5$, $2022 \equiv 2 \pmod 5$. Άρα πρέπει να υπολογίσω τη μετάθεση

$$c = (12753)^{-2}(235)^2(12753)^4(12375)^{-2} = (35721)^2(235)^2(12753)^4(57321)^2 =$$

$$(37152)(253)(35721)(53172) = (12)(57)$$

Άρα a έχει τάξη 5 είναι άρτια, η b έχει τάξη 3 και είναι άρτια, η c έχει τάξη 2 και είναι άρτια.

2. (i) Παρατηρώ ότι $4^3 = 64 \equiv -1 \pmod{13}$ και $19916 = 3 \cdot 6638 + 2$ και άρα $4^{19916} = (4^3)^{6638} \cdot 4^2 = (-1)^{6638} \cdot 16 \equiv 3 \pmod{13}$.

   (ii) $33349 = (27) cdot 1234 + 31$, $1234 = (39) \cdot 31 + 25$, $31 = 25 + 6$, $25 = (4) \cdot 6 + 1$ και με προς τα πίσω αντικατάσταση έχω $1 = (-199) \cdot 33349 + (5378) \cdot 1234$. Άρα ο αντίστροφος είναι ο 5378.

3. (i) Το A είναι όλα τα πολυώνυμα που έχουν ρίζες τα 1 και 2 άρα είναι όλα τα πολυώνυμα της μορφής $(x-1)(x-2)g(x)$ για κάθε $g(x) \in \mathbb{Q}[x]$. Είναι προφανές ότι είναι ιδεώδες.

   (ii) Το B είναι όλα τα πολυώνυμα της μορφής $(x^2 - 2x + 1)g(x) = (x-1)^2 g(x)$ για κάθε $g(x) \in \mathbb{Q}[x]$. Είναι προφανές ότι είναι ιδεώδες.

   (iii) Το C είναι όλα τα πολυώνυμα για τα οποία $f(\frac{1}{2})$ είναι άρτιος αριθμός. Όμως αν $g(x) = x + 1$ και $f(x) = 4x \in C$ τότε το $f(x)g(x) \notin C$ εφόσον $f(\frac{1}{2})g(\frac{1}{2}) = 2 \cdot \frac{3}{2} = 3 \notin 2\mathbb{Z}$. Άρα το C όχι ιδεώδες.

4. Τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_8$ είναι όλα τα στοιχεία του $\mathbb{Z}_8$ που είναι πρώτα με το 8. Άρα $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$. Μένει να ελέγξω αν είναι κυκλική. Έχω $3 \cdot 3 = 9 \equiv 1 \pmod 8$, $5 \cdot 5 = 25 \equiv 1 \pmod 8$ και $7 \cdot 7 = 49 \equiv 1 \pmod 8$ άρα είναι ισόμορφη με την $\mathbb{Z}_2 \times \mathbb{Z}_2$.

5. (i) Το $x^2 + 1$ είναι ανάγωγο στο $\mathbb{R}$ επομένως το $\mathbb{R}[x]/I$ είναι σώμα και από την θεωρία ξέρω ότι $\mathbb{R}[x]/I = \{a_0 + a_1 x + I \mid a_0, a_1 \in \mathbb{R}\}$. Ορίζουμε $f : \mathbb{R}[x]/I \to \mathbb{C}$ με $f(a_0 + a_1 x + I) = a_0 + a_1 i$. Εύκολα η f είναι επιμορφισμός δακτυλίων και ο πυρήνας είναι το I.

   (ii) Το πολυώνυμο $f(x) = x^4 + x^3 + x^2 + x + 1$ είναι ανάγωγο στο $\mathbb{Z}_3[x]$. Πράγματι, $f(0) = 1, f(1) = 2, f(-1) = 1$. Άρα δεν έχει ρίζες. Επιπλέον, αν

$$x^4 + x^3 + x^2 + x + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

τότε έχω το σύστημα

$$\begin{aligned} a+c &= 1 \\ ac+b+d &= 1 \\ bc+ad &= 1 \\ bd &= 1 \end{aligned}$$

Αν $b = d = 1$ παίρνω τις $ac = 2$ και $a + c = 1$ που είναι αδύνατες. Αν $b = d = -1$ παίρνω τις $a + c = 1$ και $a + c = -1$ που είναι αδύνατες. Άρα το $f(x)$ είναι ανάγωγο στο $\mathbb{Z}_3[x]$ και άρα το $\mathbb{Z}_3[x]/\langle f(x)\rangle$ είναι σώμα με 81 στοιχεία.