Αριστοτελειο Πανεπιστημιο Θεσσαλονικης
Τμημα Μαθηματικων

Αλγεβρικές Δομές ΙΙ

Τελική Εξέταση – 10 Φεβρουαρίου 2017

Διάρκεια εξέτασης 2 ώρες και 30 λεπτά

1. Έστω ότι $R = \mathbb{Z}_3[x]$.

(α΄) Να αποδείξετε ότι ο R είναι περιοχή κυρίων ιδεωδών, δηλ. ότι είναι ακεραία περιοχή και ότι κάθε ιδεώδες του R είναι ίσο με $\{p(x)f(x) : \ f(x) \in R\}$ για κάποιο $p(x) \in R$.

Απάντηση Έστω $f(x) = \sum a_i x^i$, $g(x) = \sum b_j x^j$ δύο μη μηδενικά στοιχεία του R, βαθμού m και n αντίστοιχα (δηλ. $a_n, b_m \neq 0$). Τότε $f(x)g(x) = \sum_{t=0}^{m+n} (\sum a_j b_{t-j}) x^t$ και αφού $a_m b_n \neq 0$, συμπεραίνουμε ότι $f(x)g(x) \neq 0$. Επομένως ο R είναι ακεραία περιοχή. Το μηδενικό ιδεώδες είναι κύριο αφού παράγεται από το μηδενικό πολυώνυμο. Αν I είναι κάποιο μη μηδενικό ιδεώδες του R, τότε υπάρχει $p(x) \in I$ τέτοιο ώστε ο $\deg p(x)$ να είναι ελάχιστος των βαθμών των μη μηδενικών στοιχείων του I. Έστω $h(x) \in I$. Από το Θεώρημα Διαίρεσης, υπάρχουν $f(x), r(x) \in R$, τέτοια ώστε $h(x) = p(x)f(x) + r(x)$, όπου $\deg r(x) < \deg p(x)$, ή $r(x) = 0$. Όμως $r(x) = h(x) - p(x)f(x) \in I$ (αφού $h(x), p(x)f(x) \in I$). Αν λοιπόν υποθέσουμε ότι $r(x) \neq 0$, καταλήγουμε σε άτοπο εξαιτίας του βαθμού του $r(x)$ και της επιλογής του $p(x)$. Επομένως $r(x) = 0$ και $h(x) = p(x)f(x)$. Αποδείξαμε, λοιπόν, ότι $I \subset \{p(x)f(x) : \ f(x) \in R\} = \langle p(x) \rangle$. Ο αντίστροφος εγκλεισμός είναι άμεσος και άρα $I = \langle p(x) \rangle$.

(β΄) Να αποδείξετε ότι το ιδεώδες $J = \langle x^2 + x + 2 \rangle$ είναι μέγιστο στον R και να βρείτε όλα τα πρώτα ιδεώδη που περιέχονται στο J. Στη συνέχεια να βρείτε (αν υπάρχει) ένα μη πρώτο ιδεώδες που περιέχεται στο J.

Απάντηση Για να δείξουμε ότι το J είναι μέγιστο, αρκεί να δείξουμε ότι το $p(x) = x^2 + x + 2$ είναι ανάγωγο, ισοδύναμα, ότι δεν έχει ρίζα στο $\mathbb{Z}_3$. Πράγματι $p(0) = 2$, $p(1) = 1$ και $p(2) = 1$. Άρα το J είναι μέγιστο. Το $\{0\} \subset J$ είναι ιδεώδες και είναι πρώτο, αφού $\mathbb{Z}_3[x]$ είναι ακεραία περιοχή.

Έστω $I = \langle q(x) \rangle$ ένα μη μηδενικό πρώτο ιδεώδες τέτοιο ώστε $I \subset J$. Αφού J πρώτο, το $q(x)$ είναι ανάγωγο. Αφού $q(x) \in I$, προκύπτει ότι $q(x) = p(x)f(x)$, για κάποιο $f(x) \in R$. Αφού, όμως, το $q(x)$ είναι ανάγωγο, συμπεραίνουμε ότι το $f(x)$ είναι αντιστρέψιμο, δηλ. $f(x) = \pm 1$, άρα $q(x) = \pm p(x)$ και $I = J$. Κατά συνέπεια τα πρώτα ιδεώδη που είναι υποσύνολα του J είναι δύο: το μηδενικό ιδεώδες και το J.

Έστω τώρα $J_1 = \langle xp(x) \rangle$. Τότε $J_1 \subsetneq J$ και το J_1 ΔΕΝ είναι πρώτο ιδεώδες (παρατηρείστε επίσης ότι $xp(x)$ δεν είναι ανάγωγο).

(γ΄) Να αποδείξετε ότι $\langle x^3, x^2 + x + 2 \rangle = R$ και να βρείτε ένα στοιχείο $g(x) + J$ του R/J, τέτοιο ώστε $(g(x) + J)(x^3 + J) = 1 + J$.

Απάντηση Έστω $h(x) = x^3$ και $f(x) = x^2 + x + 2$. Εφαρμόζουμε τον Ευκλείδειο αλγόριθμο.

- $h(x) = f(x)(x - 1) + (-x + 2)$
- $f(x) = (-x + 2)(-x) + 2$

Άρα

$$2 = f(x) + (-x + 2)x = f(x) - [h(x) - f(x)(x - 1)]x = f(x)(x^2 - x + 1) - h(x)x$$

και

$$1 = \frac{1}{2} f(x)(x^2 - x + 1) - \frac{1}{2} h(x)x.$$

Επομένως

$$1 \in \langle h(x), f(x) \rangle \Rightarrow \langle x^3, x^2 + x + 2 \rangle = R.$$

Έστω $g(x) = (-1/2)x$. Αφού $\frac{1}{2}f(x)(x^2 - x + 1) \in J$ και $1 = \frac{1}{2}f(x)(x^2 - x + 1) - g(x)x^3$ συμπεραίνουμε ότι
$$1 + J = (-g(x) + J)(x^3 + J).$$

(δ') Να αποδείξετε ότι ο $|R/J| = 9$, να βρείτε την χαρακτηριστική του R και να βρείτε το σώμα κλασμάτων του R/J.

Απάντηση Έστω $g(x) + J$ τυχαίο στοιχείο του R/J. Από το Θεώρημα Διαίρεσης, υπάρχουν $f(x), r(x) \in R$, τέτοια ώστε $g(x) = f(x) + r(x)$, όπου $\deg r(x) < \deg p(x)$, ή $r(x) = 0$. Επομένως $r(x) = a_0 + a_1x$, με $a_i \in \mathbb{Z}_3$. Αφού $g(x) - r(x) \in J$, προκύπτει ότι $g(x) + J = r(x) + J$. Άρα

$$R/J = \{0 + J, 1 + J, 2 + J, x + J, (1 + x) + J, (2 + x) + J, 2x + J, (1 + 2x) + J, (2 + 2x) + J\}.$$

Αφού $3 \cdot \bar{1} = \bar{0}$, η χαρακτηριστική του R είναι 3.

Το R/J είναι σώμα, αφού το J είναι μέγιστο. Άρα το σώμα κλασμάτων του R/J είναι το ίδιο το J.

2. Έστω $R = \mathbb{C}[x, y]$.

(α') Να αποδείξετε ότι το σύνολο $I = \{f(x, y) : \ f(0, y) = 0\}$ είναι ιδεώδες του R. Να βρείτε 3 στοιχεία που ανήκουν στο I.

Απάντηση Αφού $0 \in I$, το I είναι μη κενό σύνολο. Έστω $g(x, y), f(x, y) \in I$, δηλ. $f(0, y) = 0$ και $g(0, y) = 0$. Τότε $h(0, y) = g(0, y) - f(0, y) = 0$ και άρα $h(x, y) = g(x, y) - f(x, y) \in I$. Επομένως το $(I, +)$ είναι προσθετική υποομάδα του R. Έστω $q(x, y) \in R$ και $g(x, y) \in I$. Τότε $h(0, y) = q(0, y)g(0, y) = q(0, y) \cdot 0 = 0$ και άρα $h(x, y) = q(x, y)g(x, y) \in I$. Επομένως το I είναι ιδεώδες του R (αφού ο R είναι αντιμεταθετικός δακτύλιος, αρκεί να ελέγθουμε το γινόμενο $q(x, y)g(x, y)$). Τρία στοιχεία του I είναι τα $0, x, xy \in I$.

(β') Να αποδείξετε ότι το I είναι πρώτο ιδεώδες. Να βρείτε ένα ιδεώδες J που να περιέχει γνήσια το I και να συμπεράνετε ότι το I δεν είναι μέγιστο ιδεώδες.

Απάντηση Θα αποδείξουμε πρώτα ότι $I = \langle x \rangle$. Πράγματι, $x \in I$ και άρα $\langle x \rangle \subset I$. Για τον αντίστροφο εγκλεισμό, έστω $f(x, y) = \sum a_{i,j}x^iy^j \in I$. Τότε $f(0, y) = \sum a_{0,j}y^j = 0$ είναι το μηδενικό πολυώνυμο στον $\mathbb{C}[y]$ και άρα $a_{0,j} = 0$, $j \geq 0$. Επομένως

$$f(x, y) = \sum_{i>0} a_{i,0}x^i = x\left(\sum_{i>0} a_{i,0}x^{i-1}\right) \in \langle x \rangle \Rightarrow I \subset \langle x \rangle.$$

Εναλλακτικά, παρατηρούμε ότι $I = \ker\phi$, όπου $\phi : \mathbb{C}[x, y] \to \mathbb{C}[y]$, $f(x, y) \mapsto f(0, y)$ είναι ο ομομορφισμός εκτίμησης και ότι ϕ είναι επιμορφισμός. Άρα $\mathbb{C}[x, y]/\ker\phi \cong \mathbb{C}[y]$ και κατά συνέπεια $\ker\phi$ είναι πρώτο ιδεώδες.

Αφού $y \notin I$, $I \subsetneq \langle x, y \rangle$. Αφού $\langle x, y \rangle$ είναι γνήσιο ιδεώδες του R, το I δεν είναι μέγιστο.

3. Να αποδείξετε ότι κάθε πεπερασμένη ακεραία περιοχή είναι σώμα.

4. Να βρείτε τους ανάγωγους παράγοντες του $x^6 - 8$ στον $\mathbb{Q}[x]$, στον $\mathbb{R}[x]$ και στον $\mathbb{C}[x]$.

Απάντηση Σημειώνουμε ότι

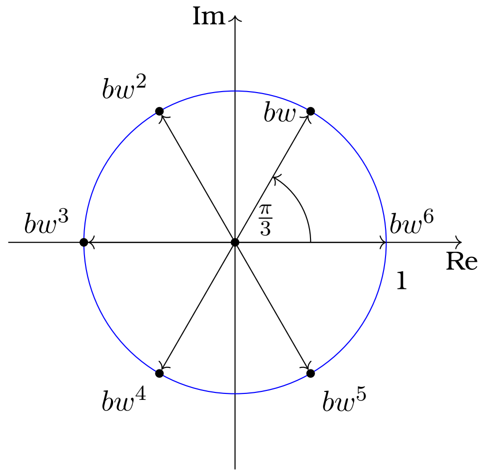
$$x^6 - 8 = (x^3 - 2\sqrt{2})(x^3 + 2\sqrt{2}) = (x - \sqrt[6]{8})(x^2 + \sqrt[6]{8}x + \sqrt[6]{8^2})(x + \sqrt[6]{8})(x^2 - \sqrt[6]{8}x + \sqrt[6]{8^2}),$$

δηλαδή
$$x^6 - 8 = (x - \sqrt[6]{8})(x + \sqrt[6]{8})(x^2 + \sqrt{2}x + 2)(x^2 - \sqrt{2}x + 2).$$

Οι δευτεροβάθμιοι παράγοντες είναι ανάγωγα πολυώνυμα στον $\mathbb{R}[x]$, αφού δεν έχουν ρίζες στον $\mathbb{R}$ (έλεγχος διακρίνουσας). Άρα το παραπάνω είναι η ανάλυση του x^6-8 σε ανάγωγους παράγοτνες στον $\mathbb{R}[x]$.

Για να βρούμε την ανάγωγη ανάλυση στον $\mathbb{C}[x]$, βρίσκουμε τις ρίζες των δευτεροβάθμιων παραγόντων. Εναλλακτικά, μπορούμε εύκολα να προσδιορίσουμε τις 6 μιγαδικές ρίζες του $f(x)=x^6-8$ στον μοναδιαίο κύκλο. Έστω $\omega = e^{2\pi i/6} = e^{\pi i/3} = \frac{1}{2}+i\frac{3}{2}$ και $b=\sqrt[6]{8}$. Παρατηρούμε, ότι $\omega^3=-1$. Οι ρίζες του $f(x)$ είναι:

$$b\omega, b\omega^2, -b, b\omega^4, b\omega^5, b.$$



Σχήμα 1:

Το $f(x)$ έχει 6 ανάγωγους παράγοντες στον $\mathbb{C}[x]$:

$$f(x) = (x-b\omega)(x-b\omega^2)(x+b)(x-b\omega^4)(x-b\omega^5)(x-b).$$

Εάν είξαμε θεκινήσει με την ανάλυση του x^6-8 στον $\mathbb{C}[x]$, για να βρούμε την ανάλυση του x^6-8 στον $\mathbb{R}[x]$, θα παρατηρούσαμε ότι δύο από τους παράγοντες ανήκουνς στον $\mathbb{R}[x]$. Επίσης $\bar{\omega}=\omega^5$ και $\overline{\omega^2}=\omega^3$, άρα

$$(x-b\omega)(x-b\omega^5) = x^2-2bRe(\omega)+b^2 = x^2-\sqrt{2}x+2$$

και

$$(x-b\omega^2)(x-b\omega^4) = x^2-2bRe(\omega^2)+b^2 = x^2+\sqrt{2}x+2.$$

Για τους ανάγωγους παράγοντες στον $\mathbb{Q}[x]$, παρατηρούμε ότι $(x-b)(x+b)=x^2-b^2=x^2-2\in\mathbb{Q}[x]$ και είναι ανάγωγο στον $\mathbb{Q}[x]$. Αφού

$$x^6-8 = (x^2-2)(x^4+2x^2+4)$$

μένει να αποφασίσουμε αν x^4+2x^2+4 είναι ανάγωγο στον $\mathbb{Q}[x]$. Οι ρίζες του x^4+2x^2+4 δεν είναι στο $\mathbb{Q}$, άρα αν το x^4+2x^2+4 δεν είναι ανάγωγο, τότε $x^4+2x^2+4=h_1(x)h_2(x)$ στον $\mathbb{Q}[x]$, όπου $\deg h_i(x)=2$, για $i=1,2$. Από την ανάγωγη ανάλυση του x^4+2x^2+4 στον $\mathbb{R}[x]$, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $h_1(x)=c(x^2+\sqrt{2}x+2)$, για κάποιο $c\in\mathbb{R}$. Έτσι αν $h_1(x)=a_2x^2+a_1x+a_0$, τότε $c\cdot 1=a_2$ (άρα c είναι ρητός), $c\sqrt{2}=a_1$ και $c\cdot 2=a_0$. Αφού $\sqrt{2}\notin\mathbb{Q}$ και $\sqrt{2}=a_2/c$ καταλήγουμε σε άτοπο. Επομένως στον $\mathbb{Q}[x]$, το $f(x)$ έχει την παρακάτω ανάλυση σε ανάγωγους παράγοντες:

$$f(x) = (x^2-2)(x^4+2x^2+4).$$

5. Έστω $R = M_{2\times 2}(\mathbb{C})$. Να βρείτε όλα τα αριστερά ιδεώδη του R που περιέχουν τον πίνακα $\begin{pmatrix}1 & -1\\ 1 & -1\end{pmatrix}$.

Απάντηση Έστω $A = \begin{pmatrix}1 & -1\\ 1 & -1\end{pmatrix}$. Το σύνολο $I = \{CA: \ C \in R\}$ περιέχει το A (για $C = I_2$) και είναι αριστερό ιδεώδες του R. Πράγματι, αν $C_1A, C_2A \in I$, τότε $C_1A - C_2A = (C_1 - C_2)A \in I$. Επίσης αν $D \in R$, τότε $D(CA) = (DC)A \in R$. Είναι φανερό ότι το I είναι το *ελάχιστο* αριστερό ιδεώδες που περιέχει τον A, με την έννοια ότι αν J είναι αριστερό ιδεώδες και $A \in J$, τότε $I \subset J$. Παίρνοντας το γινόμενα CA, για $C = (c_{ij})$, βλέπουμε ότι

$$I = \left\{\begin{pmatrix}r & -r\\ t & -t\end{pmatrix} : r, t \in \mathbb{C}\right\}.$$

Έστω τώρα J ένα ιδεώδες που περιέχει τον A, τέτοιο ώστε $I \subsetneqq J$. Έστω $C \in J \setminus I$. Αν ο C είναι αντιστρέψιμος πίνακας, τότε $J = R$. Αν ο C δεν είναι αντιστρέψιμος, τότε $\operatorname{rank} C = 1$ (αφού $C \neq 0$). Έστω

$$C = \begin{pmatrix}a & b\\ ta & tb\end{pmatrix}, \text{ όπου } b \neq (-a), t \in \mathbb{C}.$$

Τότε

$$\begin{pmatrix}1 & 0\\ -t & 1\end{pmatrix} C = \begin{pmatrix}a & b\\ 0 & 0\end{pmatrix} \in J \Rightarrow \begin{pmatrix}0 & b+a\\ 0 & 0\end{pmatrix} = \begin{pmatrix}a & b\\ 0 & 0\end{pmatrix} - \begin{pmatrix}a & -a\\ 0 & 0\end{pmatrix} \in J \Rightarrow \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} \in J \Rightarrow \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} \in J.$$

Ομοίως

$$\begin{pmatrix}b+a & 0\\ 0 & 0\end{pmatrix} = \begin{pmatrix}a & b\\ 0 & 0\end{pmatrix} + \begin{pmatrix}b & -b\\ 0 & 0\end{pmatrix} \in J \Rightarrow \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} \in J.$$

Επομένως

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} \in J \Rightarrow J = R.$$

6. Να αποδείξετε ότι $\phi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $m \mapsto (m + 2\mathbb{Z}, m + 5\mathbb{Z})$ είναι ομομορφισμός δακτυλίων. Στη συνέχεια να αποδείξετε ότι είναι επιμορφισμός και ότι $\ker \phi = 10\mathbb{Z}$. Να συμπεράνετε ότι $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Απάντηση Αφού

$$\phi(m+n) = ((m+n) + 2\mathbb{Z}, (m+n) + 5\mathbb{Z}) = ((m + 2\mathbb{Z}) + (n + 2\mathbb{Z}), (m + 5\mathbb{Z}) + (n + 5\mathbb{Z})) =$$

$$(m + 2\mathbb{Z}, m + 5\mathbb{Z}) + (n + 2\mathbb{Z}, n + 5\mathbb{Z}) = \phi(m) + \phi(m)$$

και

$$\phi(m \cdot n) = ((m \cdot n) + 2\mathbb{Z}, (m \cdot n) + 5\mathbb{Z}) = ((m + 2\mathbb{Z}) \cdot (n + 2\mathbb{Z}), (m + 5\mathbb{Z}) \cdot (n + 5\mathbb{Z})) =$$

$$(m + 2\mathbb{Z}, m + 5\mathbb{Z}) \cdot (n + 2\mathbb{Z}, n + 5\mathbb{Z}) = \phi(m) \cdot \phi(m)$$

Έστω $(r + 2\mathbb{Z}, s + 5\mathbb{Z})$ τυχαίο στοιχείο του $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Θα βρούμε $m \in \mathbb{Z}$, τέτοιο ώστε $m \equiv r \mod 2$ και ταυτόχρονα $m \equiv s \mod 5$. Θέλουμε, λοιπόν, να βρούμε κ και λ, τέτοια ώστε $m = r + 2\kappa$ και $m = s + 5\lambda$. Ισοδύναμα, τα κ και λ πρέπει να ικανοποιούν $r + 2\kappa = s + 5\lambda \Leftrightarrow r - s = 5\lambda - 2\kappa$. Η εξίσωση αυτή με σταθερά το $r - s$ και αγνώστους τα κ και λ, έχει λύση (θυμηθείτε ότι μκδ$(2, 5) = 1$), για παράδειγμα $\lambda = r - s$ και $\kappa = 2(r - s)$. Άρα $m = s + 5(r - s)$ είναι τέτοιο ώστε $m \mapsto (r + 2\mathbb{Z}, s + 5\mathbb{Z})$. Αποδείξαμε λοιπόν ότι ο ϕ είναι επί.

Στη συνέχεια θα αποδείξουμε ότι $\ker \phi = 10\mathbb{Z}$. Το μηδενικό στοιχείο του $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ είναι το $(\bar{0}, \bar{0}) = (2\mathbb{Z}, 5\mathbb{Z})$. Αν $m = 10\kappa$, τότε $\phi(m) = (10\kappa + 2\mathbb{Z}, 10\kappa + 5\mathbb{Z}) = (2\mathbb{Z}, 5\mathbb{Z})$. Επομένως

$10\mathbb{Z} \subset \ker\phi$. Για τον αντίστροφο εγκλεισμό, έστω $m \in \ker\phi$. Αφού $(m+2\mathbb{Z}, m+5\mathbb{Z}) = (\bar{0}, \bar{0}) = (2\mathbb{Z}, 5\mathbb{Z})$, αυτό σημαίνει ότι $m \in 2\mathbb{Z}$ και $m \in 5\mathbb{Z}$, και άρα $m \in 10\mathbb{Z}$. Κατά συνέπεια $\ker\phi \subset 10\mathbb{Z}$. Αφού ισχύουν οι εγλεισμοί και προς τις δύο κατευθύνσεις,προκύπτει ότι $\ker\phi \subset 10\mathbb{Z}$.

Το τελικό συμπέρασμα είναι συνέπεια του Πρώτου θεωρήματος ισομορφίας δακτυλίων: $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.