Πανεπιστήμιο Κρήτης, Τμήμα Μαθηματικών **Θεωρία Δακτυλίων και Modules (M 222)**

Εξέταση Ιουνίου 2010 **Εξεταστής: Δημήτριος Νταής**

ΑΠΑΝΤΗΣΕΙΣ ΔΟΘΕΝΤΩΝ ΘΕΜΑΤΩΝ

ΘΕΜΑ 1ο Βλ. θεώρημα 2.5.20 (στις σημειώσεις). □

ΘΕΜΑ 2ο Βλ. εδάφια 3.3.1, 3.3.2, 3.3.14 και 3.3.19. □

ΘΕΜΑ 3ο Βλ. θεώρημα 4.1.15. □

ΘΕΜΑ 4ο (i) Βλ. πρόταση 2.3.5. (ii) Βλ. θεώρημα 5.4.21. □

ΘΕΜΑ 5ο Βλ. θεώρημα 5.6.3. □

ΘΕΜΑ 6ο Ας υποθέσουμε ότι υπάρχει κάποιος μεταθετικός δακτύλιος R με μοναδιαίο στοιχείο, με την πολλαπλασιαστική ομάδα των αντιστεψίμων στοιχείων του $(R^\times, \cdot)$ έχουσα τάξη $\left|R^\times\right| = 5$. Επειδή το 5 είναι πρώτος αριθμός, κατά το (iii) (τής δοθείσας σημειώσεως) η $R^\times$ είναι κυκλική ομάδα. Ας υποθέσουμε ότι το $a \in R^\times$ είναι ένας γεννήτορας αυτής. Προφανώς, $a^5 = 1_R$ και $a \neq 1_R$ (διότι η $(R^\times, \cdot)$ είναι μη τετριμμένη) και $R^\times = \{1_R, a, a^2, a^3, a^4\}$. Ως γνωστόν, $0_R \notin R^\times$ και $\{\pm 1_R\} \subseteq R^\times$ (βλ. εδάφιο 1.2.9). Επειδή $(-1_R)^2 = 1_R$, έχουμε $\mathrm{ord}(-1_R) \in \{1, 2\}$ (βάσει τού ορισμού τής τάξεως στοιχείου και τού (i) τής δοθείσας σημειώσεως). Επειδή $\mathrm{ord}(-1_R) \mid 5$ (βλ. το (ii) τής δοθείσας σημειώσεως), έχουμε κατ' ανάγκην $\mathrm{ord}(-1_R) = 1$, οπότε $-1_R = 1_R$ (= το ουδέτερο στοιχείο τής $(R^\times, \cdot)$). Αυτό σημαίνει ότι $2 \cdot 1_R = 0_R$, απ' όπου έπεται ότι $\mathrm{χαρ}(R) = 2$ (βλ. 1.4.2 (iii) και πρόταση 1.4.3). Προκειμένου να καταλήξουμε σε άτοπο, *αρκεί να προσδιορίσουμε κάποιο στοιχείο* $b \in R^\times$ *τής μορφής* $b = 1_R + c(a + 1_R)$, $c \in R^\times \setminus \{1\}$, με $b^k = 1_R$, για κάποιο $k \in \{2, 3, 4\}$. Πράγματι· υποθέτοντας ότι υπάρχει ένα τέτοιο b, θα ισχύει $\mathrm{ord}(b) \mid k$ (βλ. το (i) τής δοθείσας σημειώσεως) και, ως εκ τούτου, $\mathrm{ord}(b) \in \{1, 2, 3, 4\}$. Η περίπτωση όπου $\mathrm{ord}(b) \neq 1$ αποκλείεται, καθόσον τούτο θα αντέφασκε προς το (ii) τής δοθείσας σημειώσεως (αφού $2 \nmid 5$, $3 \nmid 5$ και $4 \nmid 5$). Άρα

$$\begin{aligned} \mathrm{ord}(b) &= 1 \Rightarrow b = 1_R \Rightarrow c(a + 1_R) = 0_R \\ &\Rightarrow a + 1_R = c^{-1}(c(a + 1_R)) = c^{-1} \cdot 0_R = 0_R \\ &\Rightarrow a = -1_R = 1_R, \end{aligned}$$

πράγμα *άτοπο*, αφού $a \neq 1_R$. Ο προσδιορισμός ενός τέτοιου b γίνεται με *δοκιμές για τις τιμές τού* c, υψώσεις σε κάποια από τις τρεις επιτρεπτές δυνάμεις και χρήση τού γεγονότος ότι ο δακτύλιός μας έχει χαρακτηριστική 2. Επί παραδείγματι, ορίζοντας ως b το $b := 1_R + a^2(a + 1_R)$ (με $c := a^2 \in R^\times \setminus \{1\}$, και χωρίς να γνωρίζουμε *εκ των προτέρων* ότι το εν λόγω b ανήκει στην $R^\times$), λαμβάνουμε (ύστερα από ύψωση στην τρίτη δύναμη)

$$\begin{aligned} b^3 &= \left(1_R + a^2 + a^3\right)^3 = 1_R + 3a^2 + 3a^3 + 3a^4 + 6a^5 + 4a^6 + 3a^7 + 3a^8 + a^9 \\ &= 1_R + a^2 + a^3 + a^4 + a^7 + a^8 + a^9 = 1_R + a^2 + a^3 + a^4 + a^2 + a^3 + a^4 \\ &= 1_R + 2(a^2 + a^3 + a^4) = 1_R. \end{aligned}$$

Επειδή $b^3 = b \cdot b^2 = 1_R$, έχουμε $b \in R^\times$ με $b^{-1} = b^2$. Εδώ αποπερατούται η απόδειξη! □

ΘΕΜΑ 7ο (i) Για κάθε $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ $(a, b \in \mathbb{Z})$ ορίζουμε την επιριπτική απεικόνιση

$$f : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_7, \quad f(a + b\sqrt{-5}) := [a + 4b]_7 .$$

Για οιουσδήποτε $a, b, c, d \in \mathbb{Z}$ έχουμε

$$\begin{aligned} f((a+b\sqrt{-5})+(c+d\sqrt{-5})) &= f((a+c)+(b+d)\sqrt{-5}) = [(a+c)+4(b+d)]_7 \\ &= [a+4b]_7 + [c+4d]_7 \\ &= f(a+b\sqrt{-5}) + f(c+d\sqrt{-5}) \end{aligned}$$

και

$$\begin{aligned} f((a+b\sqrt{-5})(c+d\sqrt{-5})) &= f((ac-5bd)+(ad+bc)\sqrt{-5}) \\ &= [(ac-5bd)+4(ad+bc)]_7 \\ &= [ac-5bd]_7 + [4(ad+bc)]_7 \\ &= [ac]_7 + ([-5]_7 \cdot [bd]_7) + [4(ad+bc)]_7 \\ &= [ac]_7 + ([16]_7 \cdot [bd]_7) + [4(ad+bc)]_7 \\ &= [ac+16bd]_7 + [4(ad+bc)]_7 \\ &= [(ac+16bd)+4(ad+bc)]_7 \\ &= [(a+4b)(c+4d)]_7 \\ &= [a+4b]_7\,[c+4d]_7 \\ &= f(a+b\sqrt{-5})f(c+d\sqrt{-5}), \end{aligned}$$

οπότε η f είναι ένας επιμορφισμός δακτυλίων. Σύμφωνα με το 1ο θεώρημα ισομορφισμών δακτυλίων 3.3.2,

$$\mathbb{Z}[\sqrt{-5}]/\mathrm{Ker}(f) \cong \mathbb{Z}_7.$$

Επειδή $f(7) = [7+4\cdot 0]_7 = [7]_7 = [0]_7$ και $f(4-\sqrt{-5}) = [4+4\cdot(-1)]_7 = [0]_7$, έχουμε

$$7 \in \mathrm{Ker}(f),\ 4-\sqrt{-5} \in \mathrm{Ker}(f) \Rightarrow \langle 7, 4-\sqrt{-5}\rangle \subseteq \mathrm{Ker}(f).$$

Και αντιστρόφως· για τυχόν $a+b\sqrt{-5} \in \mathrm{Ker}(f)$ $(a, b \in \mathbb{Z})$ έχουμε $7 \mid a+4b$, οπότε

$$a+b\sqrt{-5} = 7\left(\frac{a+4b}{7}\right) - \left(4-\sqrt{-5}\right)b,$$

απ' όπου έπεται και ο αντίστροφος εγκλεισμός $\mathrm{Ker}(f) \subseteq \langle 7, 4-\sqrt{-5}\rangle$. □

(ii) Ας υποθέσουμε ότι υπάρχει κάποιος ισομορφισμός δακτυλίων $\vartheta : \mathbb{Z}[\mathsf{X}] \longrightarrow \mathbb{Q}[\mathsf{X}]$. Επειδή έχουμε προφανώς $\vartheta(1) \in \mathbb{Q}[\mathsf{X}] \Rightarrow \frac{1}{2}\vartheta(1) \in \mathbb{Q}[\mathsf{X}]$ και επειδή η απεικόνιση f είναι επιρριπτική, υπάρχει κάποιο $f(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$, τέτοιο ώστε να ισχύει η ισότητα $\vartheta(f(\mathsf{X})) = \frac{1}{2}\vartheta(1)$. Επομένως,

$$\vartheta(2f(\mathsf{X})) = \vartheta(f(\mathsf{X})+f(\mathsf{X})) = \vartheta(f(\mathsf{X})) + \vartheta(f(\mathsf{X})) = \frac{1}{2}\vartheta(1) + \frac{1}{2}\vartheta(1) = \vartheta(1).$$

Επειδή η απεικόνιση είναι ενριπτική, έχουμε $2f(\mathsf{X}) = 1$. Εάν

$$f(\mathsf{X}) = \sum_{i=0}^{m} a_i \mathsf{X}^i \in \mathbb{Z}[\mathsf{X}],$$

τότε $2a_0 = 1 \Rightarrow a_0 = \frac{1}{2} \in \mathbb{Q} \smallsetminus \mathbb{Z}$. Άτοπο! □

<u>ΘΕΜΑ 8ο</u> (α) (i)⇒(ii) Εάν $n \in \mathbb{Z}\smallsetminus\{0\}$ και $I_n = \langle f(\mathsf{X})\rangle$, για κάποιο $f(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$, τότε υπάρχουν πολυώνυμα $g(\mathsf{X}), h(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$, τέτοια ώστε να ισχύουν οι ισότητες $n = f(\mathsf{X})g(\mathsf{X})$ και $\mathsf{X} = f(\mathsf{X})h(\mathsf{X})$. Επειδή ο $\mathbb{Z}$ και, κατ' επέκτασιν και ο $\mathbb{Z}[\mathsf{X}]$, είναι ακεραία περιοχή, έχουμε

$$0 = \deg(f(\mathsf{X})g(\mathsf{X})) = \deg(f(\mathsf{X})) + \deg(g(\mathsf{X})) \Rightarrow \deg(f(\mathsf{X})) = \deg(g(\mathsf{X})) = 0$$

(βλ. πρόταση 1.3.9), οπότε $f(\mathsf{X}) = a \in \mathbb{Z}\smallsetminus\{0\}$. Επιπροσθέτως,

$$1 = \deg(f(\mathsf{X})h(\mathsf{X})) = \deg(f(\mathsf{X})) + \deg(h(\mathsf{X})) = \deg(h(\mathsf{X})),$$

οπότε $\exists b, c \in \mathbb{Z} : h(\mathsf{X}) = b\mathsf{X} + c$. Κατά συνέπειαν,

$$\mathsf{X} = f(\mathsf{X})h(\mathsf{X}) \Rightarrow \mathsf{X} = a(b\mathsf{X} + c) \Rightarrow ab = 1, c = 0 \Rightarrow a \in \mathbb{Z}^{\times} = \{\pm 1\}.$$

Από την άλλη μεριά, $f(\mathsf{X}) \in I_n := \langle n, \mathsf{X} \rangle$, οπότε $\exists \theta_1(\mathsf{X}), \theta_2(\mathsf{X}) \in \mathbb{Z}[\mathsf{X}]$:

$$f(\mathsf{X}) = n\theta_1(\mathsf{X}) + \mathsf{X}\theta_2(\mathsf{X}) \Rightarrow \theta_2(\mathsf{X}) = 0_{\mathbb{Z}[\mathsf{X}]},\ \theta_1(\mathsf{X}) = d \in \mathbb{Z}.$$

Άρα $\{\pm 1\} \ni a = f(\mathsf{X}) = nd \Rightarrow n, d \in \{\pm 1\}$.

(ii)⇒(i) Εάν $n = 0$, τότε $I_n = \langle \mathsf{X} \rangle$. Εάν $n \in \{\pm 1\}$, τότε $I_n = \mathbb{Z}[\mathsf{X}]$. Άρα σε αμφότερες τις περιπτώσεις το I_n είναι κύριο ιδεώδες τού $\mathbb{Z}[\mathsf{X}]$. □

(β) Έστω $n \in \mathbb{N},\ n \geq 2$. Θεωρούμε τους επιμορφισμούς δακτυλίων

$$\mathbb{Z}[\mathsf{X}] \ni \sum_{i=0}^{m} a_i \mathsf{X}^i \overset{\beta}{\longmapsto} a_0 \in \mathbb{Z},\ \ \mathbb{Z} \ni k \overset{\gamma}{\longmapsto} [k]_n \in \mathbb{Z}_n.$$

Η σύνθεσή τους $\gamma \circ \beta : \mathbb{Z}[\mathsf{X}] \longrightarrow \mathbb{Z}_n$ είναι ένας επιμορφισμός δακτυλίων έχων ως πυρήνα του το ιδεώδες

$$\begin{aligned}
\mathrm{Ker}(\gamma \circ \beta) &= \left\{ \sum_{i=0}^{m} a_i \mathsf{X}^i \in \mathbb{Z}[\mathsf{X}] \,\middle|\, [a_0]_n = [0]_n \right\} \\
&= \left\{ \sum_{i=0}^{m} a_i \mathsf{X}^i \in \mathbb{Z}[\mathsf{X}] \,\middle|\, n \mid a_0 \right\} \\
&= \left\{ nk + \mathsf{X}\left(\sum_{i=1}^{m} a_i \mathsf{X}^{i-1} \right) \in \mathbb{Z}[\mathsf{X}] \,\middle|\, k \in \mathbb{Z} \right\} \\
&= \langle n, \mathsf{X} \rangle =: I_n.
\end{aligned}$$

Σύμφωνα με το 1ο θεώρημα ισομορφισμών δακτυλίων 3.3.2,

$$\mathbb{Z}[\mathsf{X}]/I_n \cong \mathbb{Z}_n.$$

(i)⇒(ii) Εάν το I_n είναι μεγιστικό ιδεώδες τού $\mathbb{Z}\,[\mathsf{X}]$, τότε το I_n είναι πρώτο ιδεώδες τού $\mathbb{Z}\,[\mathsf{X}]$, διότι ο $\mathbb{Z}\,[\mathsf{X}]$ είναι μεταθετικός δακτύλιος με μοναδιαίο στοιχείο (βλ. θεώρημα 2.5.22).

(ii)⇒(iii) Εάν το I_n είναι πρώτο ιδεώδες τού $\mathbb{Z}\,[\mathsf{X}]$, τότε ο πηλικοδακτύλιος $\mathbb{Z}[\mathsf{X}]/I_n$ και, κατ' επέκτασιν, και ο $\mathbb{Z}_n$ είναι ακεραία περιοχή (βλ. θεώρημα 2.6.4 και πόρισμα 3.1.10 (i)). Άρα ο n είναι πρώτος αριθμός επί τη βάσει τού πορίσματος 1.2.27.

(iii)⇒(i) Εάν ο n είναι πρώτος αριθμός, τότε ο $\mathbb{Z}_n$ και , κατ' επέκτασιν, και ο πηλικοδακτύλιος $\mathbb{Z}[\mathsf{X}]/I_n$ είναι σώμα (βλ. πόρισμα 1.2.27. και πόρισμα 3.1.10 (iii)). Άρα το ιδεώδες I_n είναι μεγιστικό ιδεώδες τού $\mathbb{Z}\,[\mathsf{X}]$ επί τη βάσει τού (ii) τού πορίσματος 2.6.5. □

<u>ΘΕΜΑ 9ο</u> (i) Ας υποθέσουμε ότι το $a + b\sqrt{-6},\ a, b \in \mathbb{Z}$, είναι ένας *γνήσιος* διαιρέτης τού 2 (και αντιστοίχως, τού 5) εντός τής $\mathbb{Z}[\sqrt{-6}]$. Από τα (iii), (vi) και (vii) τής προτάσεως 5.2.39 έπεται ότι

$$\left.\begin{aligned} \mathbf{N}\left(a + b\sqrt{-6}\right) \mid \mathbf{N}(2) = 4 \\ \mathbf{N}\left(a + b\sqrt{-6}\right) \neq \pm 1 \\ \mathbf{N}\left(a + b\sqrt{-6}\right) \neq \mathbf{N}(2) = 4 \end{aligned}\right\} \Longrightarrow \mathbf{N}\left(a + b\sqrt{-6}\right) = 2,$$

και αντιστοίχως,

$$\left.\begin{aligned} \mathbf{N}\left(a + b\sqrt{-6}\right) \mid \mathbf{N}(5) = 25 \\ \mathbf{N}\left(a + b\sqrt{-6}\right) \neq \pm 1 \\ \mathbf{N}\left(a + b\sqrt{-6}\right) \neq \mathbf{N}(5) = 25 \end{aligned}\right\} \Longrightarrow \mathbf{N}\left(a + b\sqrt{-6}\right) = 5,$$

οπότε $a^2 + 6b^2 = 2$ (και αντιστοίχως, $a^2 + 6b^2 = 5$). Αυτές οι διοφαντικές εξισώσεις δεν επιδέχονται ακέραιες λύσεις. Άρα το 2 (και αντιστοίχως, το 5) δεν διαθέτει γνήσιους διαιρέτες, οπότε είναι ανάγωγο

στοιχείο (βλ. το (viii) τής προτάσεως 5.3.4). Κατ' αναλογίαν, εάν το $a+b\sqrt{-6},\ a,b\in\mathbb{Z}$, είναι ένας *γνήσιος* διαιρέτης τού $2-\sqrt{-6}$, τότε

$$\left.\begin{array}{r} \mathbf{N}\left(a+b\sqrt{-6}\right)\mid \mathbf{N}(2-\sqrt{-6})=10 \\ \mathbf{N}\left(a+b\sqrt{-6}\right)\neq \pm 1 \\ \mathbf{N}\left(a+b\sqrt{-6}\right)\neq \mathbf{N}(2-\sqrt{-6})=10 \end{array}\right\}\Longrightarrow \mathbf{N}\left(a+b\sqrt{-6}\right)\in\{2,5\},$$

ήτοι κάτι που (όπως έχουμε ήδη αποδείξει) είναι αδύνατο. Άρα *και* το $2-\sqrt{-6}$ είναι ανάγωγο στοιχείο τής $\mathbb{Z}[\sqrt{-6}]$. Από την άλλη μεριά, έχουμε $2\mid 6=(i\sqrt{6})(-i\sqrt{6})$ αλλά $2\nmid \pm i\sqrt{6}$, οπότε το 2 δεν είναι πρώτο. Κατ' αναλογίαν, το 5 είναι διαιρέτης τού $(2+\sqrt{-6})(2-\sqrt{-6})$ αλλά $5\nmid 2\pm\sqrt{-6}$ και το $2-\sqrt{-6}$ είναι διαιρέτης τού $2\cdot 5$ αλλά $2-\sqrt{-6}\nmid 2$ και $2-\sqrt{-6}\nmid 5$. Άρα τα $2,5,2-\sqrt{-6}$ είναι πρώτα στοιχεία τής $\mathbb{Z}[\sqrt{-6}]$.

(ii) Έστω $d\in \text{ΜΚΔ}_{\mathbb{Z}[\sqrt{-6}]}(5,2+\sqrt{-6})$. Τότε (λαμβανομένου υπ' όψιν τού (i)) έχουμε

$$\left.\begin{array}{r} d\mid 5\Rightarrow \mathbf{N}\left(d\right)\mid \mathbf{N}(5)=25 \\ d\mid 2+\sqrt{-6}\Rightarrow \mathbf{N}\left(d\right)\mid \mathbf{N}(2+\sqrt{-6})=10 \\ \mathbf{N}\left(d\right)\mid \text{μκδ}(10,25)=5 \end{array}\right\}\Longrightarrow \mathbf{N}\left(d\right)=1.$$

Όμως τούτο σημαίνει ότι $d\in\{\pm 1\}\Rightarrow 1\in \text{ΜΚΔ}_{\mathbb{Z}[\sqrt{-6}]}(5,2+\sqrt{-6})$. Από την άλλη μεριά,

$$\left\langle 5,2+\sqrt{-6}\right\rangle\subsetneqq\mathbb{Z}[\sqrt{-6}]\Rightarrow 1\notin\left\langle 5,2+\sqrt{-6}\right\rangle.$$

(iii) Ας υποθέσουμε ότι $\text{ΜΚΔ}_{\mathbb{Z}[\sqrt{-6}]}(10,4+2\sqrt{-6})\neq\varnothing$ και ότι $d\in\text{ΜΚΔ}_{\mathbb{Z}[\sqrt{-6}]}(10,4+2\sqrt{-6})$. Τότε

$$\left.\begin{array}{r} d\mid 10\Rightarrow \mathbf{N}\left(d\right)\mid \mathbf{N}(10)=100 \\ d\mid 4+2\sqrt{-6}\Rightarrow \mathbf{N}\left(d\right)\mid \mathbf{N}(4+2\sqrt{-6})=40 \end{array}\right\}\Longrightarrow \mathbf{N}\left(d\right)\mid \text{μκδ}(100,40)=20.$$

Επειδή $2\mid 10$ και $2\mid 4+2\sqrt{-6}$ έχουμε $2\mid d$ (βλ. 5.2.9). Κατ' αναλογίαν, επειδή $2+\sqrt{-6}\mid 10$ και $2+\sqrt{-6}\mid 4+2\sqrt{-6}$ έχουμε $2+\sqrt{-6}\mid d$. Επομένως,

$$\left.\begin{array}{r} \mathbf{N}\left(2\right)=4\mid \mathbf{N}\left(d\right) \\ \mathbf{N}(2+\sqrt{-6})=10\mid \mathbf{N}\left(d\right) \\ \mathbf{N}\left(d\right)\geq 1,\ \mathbf{N}\left(d\right)\mid 20 \end{array}\right\}\Longrightarrow \mathbf{N}\left(d\right)=20.$$

Εάν $d=x+y\sqrt{-6},\ x,y\in\mathbb{Z}$, τότε $x^2+6y^2=20$. Προφανώς, $|x|\leq 4$ και $|y|\leq 1$ Από τον πίνακα όλων των δυνατών τιμών λαμβάνουμε

$\lvert x\rvert$	$\lvert y\rvert$	x^2+6y^2
0	0	0
0	1	6
1	0	1
1	1	7
2	0	4

$\lvert x\rvert$	$\lvert y\rvert$	x^2+6y^2
2	1	10
3	0	9
3	1	15
4	0	16
4	1	22

οπότε η $x^2+6y^2=20$ δεν διαθέτει κανένα ζεύγος $(x,y)\in\mathbb{Z}^2$ ως λύση της. Άτοπο!

(iv) Το στοιχείο 10 μπορεί να γραφεί ως εξής

$$10=2\cdot 5=(2+\sqrt{-6})(2-\sqrt{-6}),$$

όπου

$$2\underset{\text{συν.}}{\not\sim}2\pm\sqrt{-6},\ 5\underset{\text{συν.}}{\not\sim}2\pm\sqrt{-6},$$

όπως διαπιστώνεται άμεσα (με απλές πράξεις). □

ΘΕΜΑ 10ο (α) Δίδονται τα εξής ιδεώδη τού δακτυλίου $\mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$:

(i)	$\langle \mathsf{X}_1^2 \rangle$,	(iv)	$\langle \mathsf{X}_1^2 - 1 \rangle$,
(ii)	$\langle \mathsf{X}_1 - 2, \mathsf{X}_2 - 3 \rangle$,	(v)	$\langle \mathsf{X}_1 + \mathsf{X}_2 \rangle$,
(iii)	$\langle \mathsf{X}_1^2 + 1 \rangle$,	(vi)	$\langle \mathsf{X}_1 \mathsf{X}_2 \rangle$.

Θα εξετάσουμε ποια εξ αυτών είναι πρώτα και ποια μεγιστικά. Επειδή ο δακτύλιος $\mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$ είναι μεταθετικός, ένα ιδεώδες $\mathfrak{p} \subsetneqq \mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$ είναι πρώτο εάν και μόνον εάν ισχύει η συνεπαγωγή

$$[f(\mathsf{X}_1, \mathsf{X}_2)g(\mathsf{X}_1, \mathsf{X}_2) \in \mathfrak{p} \Longrightarrow \text{είτε } \ f(\mathsf{X}_1, \mathsf{X}_2) \in \mathfrak{p} \ \text{ είτε } \ g(\mathsf{X}_1, \mathsf{X}_2) \in \mathfrak{p}],$$

για οιαδήποτε $f(\mathsf{X}_1, \mathsf{X}_2), g(\mathsf{X}_1, \mathsf{X}_2) \in \mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$ (βλ. πρόταση 2.5.2). Επιπροσθέτως, επειδή ο $\mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$ είναι δακτύλιος με μοναδιαίο στοιχείο, κάθε μεγιστικό ιδεώδες του είναι κατ' ανάγκην πρώτο (βλ. θεώρημα 2.5.22).

(i) Επειδή $\mathsf{X}_1^2 = \mathsf{X}_1 \cdot \mathsf{X}_1 \in \langle \mathsf{X}_1^2 \rangle$ αλλά $\mathsf{X}_1 \notin \langle \mathsf{X}_1^2 \rangle$, το $\langle \mathsf{X}_1^2 \rangle$ δεν είναι ούτε πρώτο ούτε μεγιστικό ιδεώδες.

(ii) Εάν ορίσουμε τον ομομορφισμό δακτυλίων

$$\vartheta : \mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2] \longrightarrow \mathbb{Q}, \ \ f(\mathsf{X}_1, \mathsf{X}_2) \longmapsto f(2, 3),$$

παρατηρούμε ότι ο ϑ είναι επιμορφισμός. (Για κάθε $\lambda \in \mathbb{Q}$, υπάρχει ένα πολυώνυμο

$$f_\lambda(\mathsf{X}_1, \mathsf{X}_2) := (\mathsf{X}_1 - 2) + (\mathsf{X}_2 - 3) + \lambda,$$

για το οποίο ισχύει $\vartheta\left(f_\lambda(\mathsf{X}_1, \mathsf{X}_2)\right) = \lambda$). Χρησιμοποιώντας το 1ο θεώρημα ισομορφισμών δακτυλίων 3.3.2 σχηματίζουμε έναν ισομορφισμό

$$\mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2] \,/\, \mathrm{Ker}(\vartheta) \cong \mathbb{Q}.$$

Ο εγκλεισμός

$$\langle \mathsf{X}_1 - 2, \mathsf{X}_2 - 3 \rangle \subseteq \mathrm{Ker}(\vartheta) = \{\, f(\mathsf{X}_1, \mathsf{X}_2) \in \mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2] \mid f(2, 3) = 0 \,\}$$

είναι προφανής. Ο αντίστροφος εγκλεισμός "$\supseteq$" έπεται από το ότι κάθε

$$f(\mathsf{X}_1, \mathsf{X}_2) = \sum_{i,j} a_{ij} \mathsf{X}_1^i \mathsf{X}_2^j \in \mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$$

με $f(2, 3) = 0$ μπορεί να γραφεί ως

$$f(\mathsf{X}_1, \mathsf{X}_2) = \sum_{i,j} a_{ij} (2 + \mathsf{X}_1 - 2)^i (3 + \mathsf{X}_2 - 3)^j$$

$$= \sum_{i,j} a_{ij} \left[\sum_{k=0}^{i} \tbinom{i}{k} 2^k (\mathsf{X}_1 - 2)^{i-k} \right] \left[\sum_{l=0}^{j} \tbinom{j}{l} 3^l (\mathsf{X}_2 - 3)^{j-l} \right]$$

ήτοι ως αθροίσματα ρητών αριθμών πολλαπλασιαζομένων με δυνάμεις των $\mathsf{X}_1 - 2$ και $\mathsf{X}_2 - 3$. Επειδή το $\mathbb{Q}$ είναι σώμα, ο πηλικοδακτύλιος $\mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2] \,/\, \langle \mathsf{X}_1 - 2, \mathsf{X}_2 - 3 \rangle$ είναι ωσαύτως σώμα και το ιδεώδες $\langle \mathsf{X}_1 - 2, \mathsf{X}_2 - 3 \rangle$ μεγιστικό (και, κατ' επέκτασιν, πρώτο), βλ. πόρισμα 1.2.27. και πόρισμα 3.1.10 (iii).

(iii) Επειδή το $\mathsf{X}_1^2 + 1$ είναι ανάγωγο πολυώνυμο στον $\mathbb{Q}[\mathsf{X}_1]$, το $\langle \mathsf{X}_1^2 + 1 \rangle$ είναι πρώτο ιδεώδες (τόσον τού $\mathbb{Q}[\mathsf{X}_1]$ όσον και τού[1] $\mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$), αλλά δεν είναι μεγιστικό ιδεώδες, καθότι, π.χ.,

$$\langle \mathsf{X}_1^2 + 1 \rangle \subsetneqq \langle \mathsf{X}_1^2 + 1, \mathsf{X}_2 - 3 \rangle \subsetneqq \mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2].$$

(iv) Επειδή $\mathsf{X}_1^2 - 1 = (\mathsf{X}_1 - 1)(\mathsf{X}_1 + 1)$, το $\mathsf{X}_1^2 - 1$ δεν είναι ανάγωγο, οπότε το $\langle \mathsf{X}_1^2 - 1 \rangle$ δεν είναι ούτε πρώτο ούτε μεγιστικό ιδεώδες.

[1] Τόσον ο $\mathbb{Q}[\mathsf{X}_1]$ όσον και ο $\mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$ είναι Π.Μ.Π., οπότε κάθε ανάγωγο στοιχείο τους είναι και πρώτο στοιχείο (το οποίο παράγει ένα πρώτο ιδεώδες, βλ. θεώρημα 5.6.3 και πρόταση 5.3.4. (i)).

(v) Το $\mathsf{X}_1 + \mathsf{X}_2$ είναι ανάγωγο πολυώνυμο και, ως εκ τούτου, πρώτο στοιχείο τού $\mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2]$, οπότε το $\langle \mathsf{X}_1 + \mathsf{X}_2 \rangle$ είναι πρώτο ιδεώδες. Ωστόσο, το $\langle \mathsf{X}_1 + \mathsf{X}_2 \rangle$ δεν είναι μεγιστικό, διότι π.χ.

$$\langle \mathsf{X}_1 + \mathsf{X}_2 \rangle \subsetneqq \langle \mathsf{X}_1, \mathsf{X}_2 \rangle \subsetneqq \mathbb{Q}[\mathsf{X}_1, \mathsf{X}_2].$$

(vi) Επειδή $\mathsf{X}_1\mathsf{X}_2 \in \langle \mathsf{X}_1\mathsf{X}_2 \rangle$ αλλά $\mathsf{X}_1 \notin \langle \mathsf{X}_1\mathsf{X}_2 \rangle$ και $\mathsf{X}_2 \notin \langle \mathsf{X}_1\mathsf{X}_2 \rangle$, το $\langle \mathsf{X}_1\mathsf{X}_2 \rangle$ δεν είναι ούτε πρώτο ούτε μεγιστικό ιδεώδες. □

(β) Δίδονται τα εξής στοιχεία τού δακτυλίου $\mathbb{Z}_2[\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3]$:

$$\begin{aligned} &\text{(i)} \quad f(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3) := \mathsf{X}_1^2 + \mathsf{X}_2^2 + \mathsf{X}_3^2, \\ &\text{(ii)} \quad g(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3) := \mathsf{X}_1\mathsf{X}_2 + \mathsf{X}_2\mathsf{X}_3 + \mathsf{X}_3\mathsf{X}_1. \end{aligned}$$

Θα εξετάσουμε ποια εξ αυτών είναι ανάγωγα.

(i) Επειδή

$$f(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3) = (\mathsf{X}_1 + \mathsf{X}_2 + \mathsf{X}_3)^2,$$

με το $\mathsf{X}_1 + \mathsf{X}_2 + \mathsf{X}_3$ μη σταθερό πολυώνυμο, το $f(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$ δεν είναι ανάγωγο.

(ii) Ας υποθέσουμε ότι το $g(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$ γράφεται ως γινόμενο δύο μη σταθερών πολυωνύμων $h_1(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$ και $h_2(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3) \in \mathbb{Z}_2[\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3]$. Επειδή το $g(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$ δεν περιέχει καμία μεταβλητή υψωμένη σε κάποια δύναμη ≥ 2 και ο σταθερός του όρος είναι $= 0$, τα $h_1(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$ και $h_2(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$ δεν μπορούν να περιέχουν μη μηδενικούς σταθερούς όρους, ούτε όρους που περιλαμβάνουν περισσότερες τής μίας μεταβλητής, ούτε όρους που περιλαμβάνουν μία μεταβλητή υψωμένη σε κάποια δύναμη ≥ 2. Κατά συνέπειαν, τα $h_1(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$ και $h_2(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$ είναι τής μορφής

$$\begin{aligned} h_1(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3) &= [a_1]_2 \mathsf{X}_1 + [a_2]_2 \mathsf{X}_2 + [a_3]_2 \mathsf{X}_3, \\ h_2(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3) &= [b_1]_2 \mathsf{X}_1 + [b_2]_2 \mathsf{X}_2 + [b_3]_2 \mathsf{X}_3, \end{aligned}$$

για κάποιους $a_1, a_2, a_3, b_1, b_2, b_3 \in \{0, 1\}$. Από την ισότητα

$$\mathsf{X}_1\mathsf{X}_2 + \mathsf{X}_2\mathsf{X}_3 + \mathsf{X}_3\mathsf{X}_1 = h_1(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3) h_2(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$$

έπεται ότι

$$\begin{gathered} [a_1]_2 [b_1]_2 = [a_2]_2 [b_2]_2 = [a_3]_2 [b_3]_2 = [0]_2, \\ [a_1]_2 [b_2]_2 + [a_2]_2 [b_1]_2 = [1]_2, \\ [a_1]_2 [b_3]_2 + [a_3]_2 [b_1]_2 = [1]_2, \\ [a_2]_2 [b_3]_2 + [a_3]_2 [b_2]_2 = [1]_2. \end{gathered}$$

Βάσει των πρώτων συνθηκών, είτε $a_j = 0$ είτε $b_j = 0$, για κάθε $j \in \{1, 2, 3\}$. Ας υποθέσουμε ότι $a_1 = 0$. Τότε $a_2 = a_3 = b_1 = 1$, οπότε $b_2 = b_3 = 0$, πράγμα άτοπο λόγω τής τελευταίας ισότητας. Παρομοίως καταλήγουμε σε άτοπο υποθέτοντας ότι $a_2 = 0$ ή $a_3 = 0$. Κατ' αναλογίαν, καταλήγουμε σε άτοπο υποθέτοντας ότι ένας εκ των b_1, b_2, b_3 είναι $= 0$. Άρα το $g(\mathsf{X}_1, \mathsf{X}_2, \mathsf{X}_3)$ είναι ανάγωγο πολυώνυμο. □
