ΑΠΑΝΤΗΣΕΙΣ ΔΟΘΕΝΤΩΝ ΘΕΜΑΤΩΝ

ΘΕΜΑΤΑ 1-5 Οι αποδείξεις είχαν παρουσιασθεί στις παραδόσεις. □

ΘΕΜΑ 6ο (i) Εξ υποθέσεως,

$$\left.\begin{array}{r} p \mid n^2+3 \\ p \mid (n+1)^2+3 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \exists k \in \mathbb{Z} : n^2+3 = kp \\ \exists l \in \mathbb{Z} : (n+1)^2+3 = lp \end{array}\right\}.$$

Από τον ευκλείδειο αλγόριθμο τής διαιρέσεως

$$\exists!(p,r) \in \mathbb{Z}\times\mathbb{Z} : n = qp + r, \ \text{ όπου } \ 0 \leq r < p.$$

Επομένως,

$$r^2+3 = (n-qp)^2+3 = n^2+3+(qp)^2-2nqp = pw,$$

όπου $w := k + q^2p - 2nq$. Επιπροσθέτως,

$$(r+1)^2+3 = ((n+1)-qp)^2+3 = (n+1)^2+3+(qp)^2-2(n+1)qp = pz,$$

όπου $z := l + q^2p - 2(n+1)q$. Αυτό σημαίνει ότι

$$p(z-w) = ((r+1)^2+3) - (r^2+3) = 2r+1 \geq 1.$$

Εξ αυτού έπεται ότι $1 \leq 2r+1 = p(z-w) \leq 2p-1$, διότι $r \leq p-1$. Παρατηρούμε ότι $z-w=1$ (διότι εάν υποθέταμε ότι $z-w \geq 2$, θα καταλήγαμε σε άτοπο: $2p \leq p(z-w) \leq 2p-1$). Συνεπώς,

$$p = 2r+1 \Rightarrow [r = \tfrac{p-1}{2} \ \text{ και } \ r+1 = \tfrac{p+1}{2}]$$

και, ως εκ τούτου,

$$\left\{\begin{array}{l} pw = r^2+3 = (\frac{p-1}{2})^2+3 = \frac{1}{4}(p^2-2p+13) \\ pz = (r+1)^2+3 = (\frac{p+1}{2})^2+3 = \frac{1}{4}(p^2+2p+13) \end{array}\right\},$$

απ' όπου έπεται ότι

$$4p(z+w) = (p^2+2p+13)+(p^2-2p+13) = 2(p^2+13)$$
$$\Longrightarrow 13 = p\,(2(z+w)-p)\,.$$

Επειδή ο p είναι πρώτος, η τελευταία ισότητα δίδει $2(z+w)-p=1$ και $p=13$, οπότε

$$\left.\begin{array}{r} 2(z+w)-13 = 1 \Rightarrow z+w = 7 \\ z-w = 1 \end{array}\right\} \Longrightarrow [w=3, z=4 \ \text{ και } \ r = \tfrac{13-1}{2} = 6].$$

Προφανώς, $6^2+3 = 39 = 3\cdot 13$ και $7^2+3 = 52 = 4\cdot 13$. Επίσης, είναι πρόδηλο ότι μαζί με την τιμή $n=r=6$ **και** όλες (οι εμφανώς *απειροπληθείς*) τιμές $n = 6+13u$, $u \in \mathbb{Z}$, ικανοποιούν τις συνθήκες διαιρετότητας

$$13 \mid n^2+3 \ \text{ και } \ 13 \mid (n+1)^2+3.$$

(ii) Ο συντελεστής "3" μας υποδεικνύει το πώς μπορούμε να εργασθούμε με αναγωγή mod 3 και «εις άτοπον απαγωγή». Εάν υπήρχαν ακέραιοι αριθμοί x, y, τέτοιοι ώστε να ισχύει η ισότητα $x^2-3y^2 = 989$, τότε, επειδή έχουμε $989 = 329\cdot 3+2$, θα έπρεπε να ισχύει

$$\left[x^2-3y^2\right]_3 = \left[x^2\right]_3 - [3]_3\left[y^2\right]_3 = \left[x^2\right]_3 - [0]_3\left[y^2\right]_3 = \left[x^2\right]_3 = [989]_3 = [2]_3\,,$$

δηλαδή να υπάρχει λύση τής $([x]_3)^2 = [2]_3$ εντός τού $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$. Τούτο όμως είναι αδύνατο, καθότι $([0]_3)^2 = [0]_3$, $([1]_3)^2 = [1]_3$ και $([2]_3)^2 = \left[2^2\right]_3 = [4]_3 = [1]_3$. □

ΘΕΜΑ 7ο Έστω $G := \langle a, b\rangle$ η υποομάδα τής $\mathfrak{S}_8$ η παραγόμενη από τα στοιχεία

$$a := [1\,2\,3\,4] \circ [5\,6\,7\,8] \quad \text{και} \quad b := [1\,5\,3\,7] \circ [2\,8\,4\,6].$$

Επειδή οι 4-κύκλοι [1 2 3 4] και [5 6 7 8] (και αντιστοίχως, οι 4-κύκλοι [1 5 3 7] και [2 8 4 6]) είναι ξένοι μεταξύ τους, οφείλουν να μετατίθενται αμοιβαίως. Αυτό σημαίνει ότι

$$a^i = [1\,2\,3\,4]^i \circ [5\,6\,7\,8]^i \quad \text{και} \quad b^j := [1\,5\,3\,7]^j \circ [2\,8\,4\,6]^j, \ \forall (i,j) \in \mathbb{Z}^2.$$

Επειδή κάθε 4-κύκλος έχει τάξη 4, λαμβάνουμε

$$G = \left\{ a^i \circ b^j, b^j \circ a^i \,\middle|\, 0 \leq i, j \leq 3 \right\}.$$

Εν συνεχεία, παρατηρούμε ότι

$$\begin{array}{ll} a = [1\,2\,3\,4] \circ [5\,6\,7\,8], & b = [1\,5\,3\,7] \circ [2\,8\,4\,6], \\ a^2 = [1\,3] \circ [2\,4] \circ [5\,7] \circ [6\,8], & b^2 = [1\,3] \circ [5\,7] \circ [2\,4] \circ [8\,6], \\ a^3 = [1\,4\,3\,2] \circ [5\,8\,7\,6], & b^3 = [1\,7\,3\,5] \circ [2\,6\,4\,8], \\ a \circ b = [1\,8\,3\,6] \circ [2\,7\,4\,5], & b \circ a = [1\,6\,3\,8] \circ [2\,5\,4\,7], \\ (ab)^2 = [1\,3] \circ [8\,6] \circ [2\,4] \circ [7\,5], & (ab)^3 = [1\,6\,3\,8] \circ [2\,5\,4\,7], \end{array}$$

με $a^2 = b^2 = (a \circ b)^2$ και $(a \circ b)^3 = b \circ a$, οπότε $a^2 \circ b^2 = \mathrm{id} = b^2 \circ a^2$ και

$$\begin{array}{ll} a \circ b^2 = a^3 = b^2 \circ a, & a \circ b^3 = a^3 \circ b = b^3 \circ a^3 = b \circ a, \\ a^2 \circ b = b^3 = b \circ a^2, & a^3 \circ b^3 = b \circ a^3 = b^3 \circ a = a \circ b, \\ a^3 \circ b^2 = a = b^2 \circ a^3, & a^2 \circ b^3 = b = b^3 \circ a^2. \end{array}$$

Κατά συνέπειαν,

$$G = \left\{ \mathrm{id}, a, a^2 (= b^2), a^3, b, b^3, ab, ba \right\} \Rightarrow |G| = 8$$

και ορμώμενοι από τον πίνακα τής πράξεως

$\cdot$	$\mathbf{I}$	$-\mathbf{I}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
$\mathbf{I}$	$\mathbf{I}$	$-\mathbf{I}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
$-\mathbf{I}$	$-\mathbf{I}$	$\mathbf{I}$	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{i}$	$-\mathbf{I}$	$\mathbf{I}$	$\mathbf{k}$	$-\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$
$-\mathbf{i}$	$-\mathbf{i}$	$\mathbf{i}$	$\mathbf{I}$	$-\mathbf{I}$	$-\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{k}$	$\mathbf{k}$	$-\mathbf{I}$	$\mathbf{I}$	$\mathbf{i}$	$-\mathbf{i}$
$-\mathbf{j}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$	$\mathbf{I}$	$-\mathbf{I}$	$-\mathbf{i}$	$\mathbf{i}$
$\mathbf{k}$	$\mathbf{k}$	$-\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{i}$	$\mathbf{i}$	$-\mathbf{I}$	$\mathbf{I}$
$-\mathbf{k}$	$-\mathbf{k}$	$\mathbf{k}$	$-\mathbf{j}$	$\mathbf{j}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{I}$	$-\mathbf{I}$

τής ομάδας $\mathbf{Q} = \{\pm \mathbf{I}_2, \pm \mathbf{i}, \pm\, \mathbf{j}, \pm \mathbf{k}\}$ των τετρανίων, όπου

$$\mathbf{I} = \mathbf{I}_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \mathbf{j} := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{k} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

με

$$\mathbf{I}_2 = \mathbf{j}^4 = \mathbf{k}^4, \ -\mathbf{I}_2 = \mathbf{j}^2 = \mathbf{k}^2, \ \mathbf{i} = \mathbf{jk},$$

$$-\mathbf{i} = \mathbf{kj} = -\mathbf{jk}, \ -\mathbf{j} = \mathbf{j}^3, \ -\mathbf{k} = \mathbf{k}^3,$$

διαπιστώνουμε άμεσα ότι η απεικόνιση $\mathbf{Q} \longrightarrow G$,

$$\begin{array}{llll} \mathbf{I}_2 \longmapsto & \mathrm{id}, & -\mathbf{I}_2 \longmapsto a^2\ (= b^2), \\ \mathbf{i} \longmapsto & b^3, & -\mathbf{i} \longmapsto b, \\ \mathbf{j} \longmapsto & ba, & -\mathbf{j} \longmapsto ab, \\ \mathbf{k} \longmapsto & a, & -\mathbf{k} \longmapsto a^3, \end{array}$$

αποτελεί ισομορφισμό ομάδων. Άρα $G \cong \mathbf{Q}$. □

ΘΕΜΑ 8ο (i) Εάν $x \in R$ είναι ένα μηδενοδύναμο στοιχείο, τότε υπάρχει $k \in \mathbb{N} : x^k = 0_R$ και το $1_R + x$ είναι αντιστρέψιμο με

$$(1_R + x)^{-1} = \sum_{j=0}^{k} (-1)^j x^j.$$

Πράγματι· πολλαπλασιάζοντας εκ δεξιών το $1_R + x$ με το ανωτέρω άθροισμα λαμβάνουμε

$$\begin{aligned} (1_R + x)\left(\sum_{j=0}^{k} (-1)^j x^j\right) &= \sum_{j=0}^{k} (-1)^j x^j + \sum_{j=0}^{k} (-1)^j x^{j+1} \\ &= 1_R + \sum_{j=1}^{k} (-1)^j x^j + \sum_{j=0}^{k-1} (-1)^j x^{j+1} + (-1)^j \underbrace{x^{k+1}}_{=0_R} \\ &= 1_R + \sum_{j=0}^{k-1} (-1)^{j+1} x^{j+1} + \sum_{j=0}^{k-1} (-1)^j x^{j+1} \\ &= 1_R + \sum_{j=0}^{k-1} \underbrace{((-1)^{j+1} + (-1)^j)}_{=0} x^{j+1} = 1_R. \end{aligned}$$

Παρομοίως αποδεικνύεται και η ισότητα $\left(\sum_{j=0}^{k} (-1)^j x^j\right)(1_R + x) = 1_R$. □

Εισαγωγικά σχόλια για τα (ii) *και* (iii). Εάν $a, b \in R$ με $ab = ba$, τότε

$$(a \pm b)^{p^n} = a^{p^n} + \sum_{j=1}^{p^n - 1} (\pm 1)^j \binom{p^n}{j} a^{p^n - j} b^j + b^{p^n} = a^{p^n} + b^{p^n}, \tag{1}$$

διότι για κάθε $j \in \{1, ..., p^n - 1\}$ έχουμε

$$\left.\begin{array}{r} \binom{p^n}{j} = \frac{p^n (p^n - 1) \cdots (p^n - j + 1)}{j!} \Rightarrow p^n \mid j! \binom{p^n}{j} \\ p^n \nmid j! \end{array}\right\} \Rightarrow p^n \mid \binom{p^n}{j}.$$

Επιπροσθέτως, αποδεικνύεται άμεσα (μέσω μαθηματικής επαγωγής) ότι

$$(a \pm b)^{(p^n)^\nu} = a^{(p^n)^\nu} \pm b^{(p^n)^\nu},\ \forall \nu \in \mathbb{N}. \tag{2}$$

(Προσοχή! Μη συγχέετε τις ανωτέρω ισότητες (1) και (2) με εκείνες που παρουσιάσαμε στις παραδόσεις, *παρά το γεγονός* ότι οι αποδείξεις είναι παρόμοιες. Εδώ ο R έχει χαρακτηριστική p^n, όπου n *τυχών* φυσικός αριθμός, ενώ δεν προϋποτίθεται ότι είναι μεταθετικός ή ακεραία περιοχή.)

(ii) "$\Rightarrow$" Εάν το $1_R - r$ είναι μηδενοδύναμο, τότε και το $r - 1_R$ είναι μηδενοδύναμο, οπότε (μέσω εφαρμογής τού (i) για $x := r - 1_R$)

$$(r - 1_R) + 1_R = r \in R^\times.$$

Εξ ορισμού, υπάρχει κάποιος $m \in \mathbb{N}$, τέτοιος ώστε να ισχύει $(1_R - r)^m = 0_R$. Εξετάζουμε δύο ενδεχόμενα χωριστά.

Περίπτωση πρώτη. Εάν $p^n \geq m$, τότε

$$0_R = (1_R - r)^m \Rightarrow 0_R = (1_R - r)^m (1_R - r)^{p^n - m} = (1_R - r)^{p^n} = 1_R - r^{p^n},$$

όπου η τελευταία ισότητα έπεται από την (1), διότι τα r και 1_R είναι αμοιβαίως μετατιθέμενα. Επομένως,

$$r^{p^n} = 1_R \Rightarrow \mathrm{ord}(r) \mid p^n \Rightarrow [\exists k \in \{0,1,...,n\} : \mathrm{ord}(a) = p^k].$$

Περίπτωση δεύτερη. Εάν $m > p^n$, επιλέγουμε *αρκούντως μεγάλον* $\nu \in \mathbb{N}$, ήτοι $\nu > \log_{p^n}(m)$, ούτως ώστε να ισχύει $(p^n)^\nu > m$. Προφανώς,

$$0_R = (1_R - r)^m \Rightarrow 0_R = (1_R - r)^m (1_R - r)^{(p^n)^\nu - m} = (1_R - r)^{(p^n)^\nu} = 1_R - r^{(p^n)^\nu},$$

όπου η τελευταία ισότητα έπεται από την (2), διότι τα r και 1_R είναι αμοιβαίως μετατιθέμενα. Επομένως,

$$r^{(p^n)^\nu} = 1_R \Rightarrow \mathrm{ord}(r) \mid p^{n\nu} \Rightarrow [\exists l \in \{0,1,...,n\nu\} : \mathrm{ord}(a) = p^l].$$

"$\Leftarrow$" Υποθέτουμε ότι $r \in R^\times$ και $\mathrm{ord}(r) = p^s$ για κάποιον $s \in \mathbb{N}_0$. Εξετάζουμε και πάλι δύο ενδεχόμενα χωριστά.

Περίπτωση πρώτη. Εάν $s \leq n$, τότε

$$(1_R - r)^{p^n} \underset{(1)}{=} 1_R - r^{p^n} = 1_R - \left(r^{p^s}\right)^{p^{n-s}} = 1_R - (1_R)^{p^{n-s}} = 0_R$$

$$\Rightarrow 1_R - r \in \mathrm{Nil}\,(R)\,.$$

Περίπτωση δεύτερη. Εάν $s > n$, τότε για οιονδήποτε $\nu \in \mathbb{N}$ με $\nu > \frac{s}{n}$ έχουμε $n\nu > s$ και

$$(1_R - r)^{(p^n)^\nu} \underset{(2)}{=} 1_R - r^{(p^n)^\nu} = 1_R - \left(r^{p^s}\right)^{p^{n\nu-s}} = 1_R - (1_R)^{p^{n\nu-s}} = 0_R,$$

οπότε $1_R - r \in \mathrm{Nil}(R)$. □

(iii) Προφανώς, μκδ$(p^n, \mathrm{ord}(a)) = p^k$ για κάποιον $k \in \mathbb{N}_0$, $k \leq n$. Επειδή

$$p^k \mid \mathrm{ord}(a) \Longrightarrow [\exists l \in \mathbb{N} : \mathrm{ord}(a) = p^k l \text{ με } p \nmid l],$$

θέτοντας $b := a^l$ λαμβάνουμε $b^{p^k} = 1_R$. Εν συνεχεία παρατηρούμε ότι

$$(1_R - b)^{p^n} = 1_R - b^{p^n} = 1_R - (b^{p^k})^{p^{n-k}} = 1_R - (1_R)^{p^{n-k}} = 0_R$$

$$\Rightarrow 1_R - b \in \mathrm{Nil}\,(R) = \{0_R\} \Rightarrow b = a^l = 1_R \Rightarrow \mathrm{ord}(a) \mid l,$$

απ' όπου έπεται ότι $p^k l = \mathrm{ord}(a) \leq l \Rightarrow p^k \leq 1 \Rightarrow k = 0$. Η συνεπαγωγή

$$\text{μκδ}(p^n, \mathrm{ord}(a)) = 1 \Rightarrow \text{μκδ}(p, \mathrm{ord}\,(a)) = 1$$

είναι προφανής. □

<u>ΘΕΜΑ 9ο</u> (i) Εάν $z = x + iy \in \mathbb{C}\ (x, y \in \mathbb{R})$ είναι μια θέση μηδενισμού τού $\mathsf{X}^2 - \xi \in \mathbb{C}\,[\mathsf{X}]$, τότε

$$x^2 - y^2 + (2xy)i = z^2 = \xi = \xi_1 + \xi_2 i,$$

απ' όπου έπεται ότι

$$\begin{aligned} x^2 - y^2 &= \xi_1, &(1)\\ 2xy &= \xi_2, &(2)\\ \left(x^2+y^2\right)^2 &= \left(x^2-y^2\right)^2 + 4x^2y^2 = r^2 = \xi_1^2 + \xi_2^2. &(3) \end{aligned}$$

Η (3) δίδει $x^2 + y^2 \in \{\pm r\}$. Επειδή $x^2 + y^2 \geq 0$ και $-r \leq 0$, έχουμε $x^2 + y^2 = -r$ εάν και μόνον εάν $x = y = r = 0$. Εάν $r \neq 0$ ($\Leftrightarrow \xi \neq 0$), τότε $x^2 + y^2 = r$ και μέσω τής (1) λαμβάνουμε

$$\left.\begin{array}{l} x^2 = \frac{1}{2}(r + \xi_1) \\ y^2 = \frac{1}{2}(r - \xi_1) \end{array}\right\} \Rightarrow \left\{\begin{array}{l} x \in \left\{\pm\sqrt{\frac{1}{2}(r+\xi_1)}\right\} \\ y \in \left\{\pm\sqrt{\frac{1}{2}(r-\xi_1)}\right\} \end{array}\right\},$$

οπότε η (2) δίδει $\operatorname{sign}(\xi_2) = \operatorname{sign}(2xy) = \operatorname{sign}(xy)$ και

$$z \in \left\{ \sqrt{\tfrac{1}{2}(r+\xi_1)} + i\operatorname{sign}(\xi_2)\sqrt{\tfrac{1}{2}(r-\xi_1)}, -\sqrt{\tfrac{1}{2}(r+\xi_1)} - i\operatorname{sign}(\xi_2)\sqrt{\tfrac{1}{2}(r-\xi_1)} \right\}.$$

Κατά συνέπειαν, $\{\, z \in \mathbb{C} \,|\, z^2 - \xi = 0 \} = \{z_1, z_2\}$, όπου $z_2 = -z_1$ και

$$z_1 := \sqrt{\tfrac{1}{2}(r+\xi_1)} + i\operatorname{sign}(\xi_2)\sqrt{\tfrac{1}{2}(r-\xi_1)}.$$

(ii) Έστω $\varphi(\mathsf{X}) := a\mathsf{X}^2 + b\mathsf{X} + c \in \mathbb{C}[\mathsf{X}]$, όπου $a \neq 0$, και έστω $D := b^2 - 4ac$. Εάν w είναι ένα στοιχείο τού συνόλου $\{\, \zeta \in \mathbb{C} \,|\, \zeta^2 - D = 0 \}$, τότε, κατά το (i), $\{\, \zeta \in \mathbb{C} \,|\, \zeta^2 - D = 0 \} = \{\pm w\}$ και το $\{\, z \in \mathbb{C} \,|\, \varphi(z) = 0 \}$ απαρτίζεται από εκείνους τους μιγαδικούς αριθμούς z για τους οποίους ισχύει

$$\begin{aligned} 0 &= a(z^2 + \tfrac{b}{a}z + \tfrac{c}{a}) = a(z^2 + 2\left(\tfrac{b}{2a}\right)z + \tfrac{b^2}{4a^2} - \tfrac{b^2}{4a^2} + \tfrac{c}{a}) \\ &= a\left(\left(z + \tfrac{b}{2a}\right)^2 - \tfrac{D}{4a^2}\right) = a\left(\left(z + \tfrac{b}{2a}\right)^2 - \tfrac{w^2}{4a^2}\right) \\ &= a\left((z + \tfrac{b}{2a}) - \tfrac{w}{2a}\right)\left((z + \tfrac{b}{2a}) + \tfrac{w}{2a}\right). \end{aligned}$$

Επομένως,

$$\{\, z \in \mathbb{C} \,|\, \varphi(z) = 0 \} = \left\{ \tfrac{-b+w}{2a}, \tfrac{-b-w}{2a} \right\}.$$

(iii) Έστω $\rho \in \mathbb{Z} : |\rho| \leq 4$. Τότε $\rho \in \{0, \pm1, \pm2, \pm3, \pm4\}$. Επειδή

$$\begin{aligned} &\psi(0) = -4\sqrt{2} + 4i \neq 0, \\ &\psi(-1) = -5(\sqrt{2} - \sqrt{3} - 1) + 30i \neq 0,\ \psi(1) = -3(\sqrt{2} + \sqrt{3} + 1) - 12i \neq 0 \\ &\psi(-2) = -6(\sqrt{2} + 2\sqrt{3} + 4) + 66i \neq 0,\ \psi(2) = -2(\sqrt{2} + 2\sqrt{3} + 4) - 18i \neq 0 \\ &\psi(-3) = -7(\sqrt{2} - 3\sqrt{3} + 9) + 112i \neq 0,\ \psi(3) = -\sqrt{2} - 3\sqrt{3} - 9 - 14i \neq 0 \\ &\psi(-4) = -8(\sqrt{2} - 4\sqrt{3} + 16) + 168i \neq 0,\ \psi(4) = 0, \end{aligned}$$

έχουμε $\{\rho \in \mathbb{Z} : |\rho| \leq 4 \text{ και } \psi(\rho) = 0\} = \{4\} \Rightarrow \mathsf{X} - 4 \mid \psi(\mathsf{X})$. Εκτελώντας την ευκλείδεια διαίρεση λαμβάνουμε

$$\psi(\mathsf{X}) = (\mathsf{X} - 4)(\mathsf{X}^2 + (\sqrt{3} + 5i)\mathsf{X} + \sqrt{2} - i).$$

Επειδή το τριώνυμο $\mathsf{X}^2 + (\sqrt{3} + 5i)\mathsf{X} + \sqrt{2} - i$ έχει διακρίνουσα

$$(\sqrt{3} + 5i)^2 - 4(\sqrt{2} - i) = -22 - 4\sqrt{2} + \left(4 + 10\sqrt{3}\right)i$$

μέτρου $\left(-22 - 4\sqrt{2}\right)^2 + \left(4 + 10\sqrt{3}\right)^2 = 832 + 176\sqrt{2} + 80\sqrt{3}$ και (σύμφωνα με το (i)) έχουμε

$$\left\{ \zeta \in \mathbb{C} \,|\, \zeta^2 - (-22 - 4\sqrt{2} + \left(4 + 10\sqrt{3}\right)i) = 0 \right\} = \{\pm w\},$$

όπου

$$\begin{aligned} w &:= \sqrt{\tfrac{1}{2}(810 + 172\sqrt{2} + 80\sqrt{3})} + i\sqrt{\tfrac{1}{2}(854 + 180\sqrt{2} + 80\sqrt{3})} \\ &= \sqrt{405 + 86\sqrt{2} + 40\sqrt{3}} + i\sqrt{427 + 90\sqrt{2} + 40\sqrt{3}}, \end{aligned}$$

οι θέσεις μηδενισμού του (σύμφωνα με το (ii)) είναι οι

$$z_{1,2} := \tfrac{1}{2}\left(-(\sqrt{3} + 5i) \pm \left(\sqrt{405 + 86\sqrt{2} + 40\sqrt{3}} + i\sqrt{427 + 90\sqrt{2} + 40\sqrt{3}}\right)\right).$$

Άρα η

$$\psi(\mathsf{X}) = (\mathsf{X} - 4)(\mathsf{X} - z_1)(\mathsf{X} - z_2)$$

είναι η ζητούμενη αποσύνθεση τού $\psi(\mathsf{X})$ σε ανάγωγα πολυώνυμα υπεράνω τού σώματος $\mathbb{C}$. $\square$

ΘΕΜΑ 10ο Από τον ευκλείδειο αλγόριθμο διαιρέσεως πολυωνύμων λαμβάνουμε

$$\begin{aligned}\varphi_1(\mathsf{X}) &= (\mathsf{X}-a)\,\varpi_1(\mathsf{X})+\upsilon_1(\mathsf{X}), &(1)\\ \varphi_2(\mathsf{X}) &= (\mathsf{X}-b)\,\varpi_2(\mathsf{X})+\upsilon_2(\mathsf{X}), &(2)\\ \varphi_1(\mathsf{X})\varphi_2(\mathsf{X}) &= (\mathsf{X}-a)\,(\mathsf{X}-b)\,\varpi(\mathsf{X})+\upsilon(\mathsf{X}). &(3)\end{aligned}$$

Επειδή $\deg(\upsilon(\mathsf{X}))\leq 1$, το $\upsilon(\mathsf{X})$ θα γράφεται υπό τη μορφή

$$\upsilon(\mathsf{X})=\kappa\mathsf{X}+\lambda,\ \text{ για κατάλληλους } \kappa,\lambda\in\mathbb{C}.$$

(i) Κατόπιν αποτιμήσεως τής (3) για $\mathsf{X}=a$ και $\mathsf{X}=b$ λαμβάνουμε

$$\left.\begin{cases}\varphi_1(a)\varphi_2(a)=\upsilon(a)=\kappa a+\lambda\\ \varphi_1(b)\varphi_2(b)=\upsilon(b)=\kappa b+\lambda\end{cases}\right\}\Leftrightarrow\begin{pmatrix}a&1\\b&1\end{pmatrix}\begin{pmatrix}\kappa\\ \lambda\end{pmatrix}=\begin{pmatrix}\varphi_1(a)\varphi_2(a)\\ \varphi_1(b)\varphi_2(b)\end{pmatrix}. \tag{4}$$

Επειδή $a\neq b$, το σύστημα (4) ως προς κ και λ διαθέτει μία και μόνον λύση:

$$\begin{aligned}\begin{pmatrix}\kappa\\ \lambda\end{pmatrix}&=\begin{pmatrix}a&1\\b&1\end{pmatrix}^{-1}\begin{pmatrix}\varphi_1(a)\varphi_2(a)\\ \varphi_1(b)\varphi_2(b)\end{pmatrix}\\ &=\frac{1}{\det\begin{pmatrix}a&1\\b&1\end{pmatrix}}\begin{pmatrix}1&-1\\-b&a\end{pmatrix}\begin{pmatrix}\varphi_1(a)\varphi_2(a)\\ \varphi_1(b)\varphi_2(b)\end{pmatrix}\\ &=\tfrac{1}{a-b}\begin{pmatrix}\varphi_1(a)\varphi_2(a)-\varphi_1(b)\varphi_2(b)\\ a\varphi_1(b)\varphi_2(b)-b\varphi_1(a)\varphi_2(a)\end{pmatrix}.\end{aligned}$$

Κατά συνέπειαν, το υπόλοιπο $\upsilon(\mathsf{X})$ εκφράζεται ως εξής:

$$\upsilon(\mathsf{X})=\frac{\varphi_1(a)\varphi_2(a)-\varphi_1(b)\varphi_2(b)}{a-b}\mathsf{X}+\frac{a\varphi_1(b)\varphi_2(b)-b\varphi_1(a)\varphi_2(a)}{a-b} \tag{5}$$

συναρτήσει των $a,b,\varphi_1(a),\varphi_2(a),\varphi_1(b),\varphi_2(b)$.

(ii) Επειδή $\deg(\upsilon_1(\mathsf{X}))\leq 0$ και $\deg(\upsilon_2(\mathsf{X}))\leq 0$, αμφότερα τα $\upsilon_1(\mathsf{X})$ και $\upsilon_2(\mathsf{X})$ είναι *σταθερά* πολυώνυμα. Από τις (1) και (2) για $\mathsf{X}=a$ και $\mathsf{X}=b$, αντιστοίχως, λαμβάνουμε

$$\upsilon_1(\mathsf{X})=\varphi_1(a),\ \ \upsilon_2(\mathsf{X})=\varphi_2(b).$$

Επομένως,

$$\begin{aligned}\varphi_1(b) &= (b-a)\,\varpi_1(b)+\varphi_1(a), &(6)\\ \varphi_2(a) &= (a-b)\,\varpi_2(a)+\varphi_2(b). &(7)\end{aligned}$$

Οι (6), (7) δίδουν μέσω τής (5)

$$\begin{aligned}\upsilon(\mathsf{X}) &= \frac{\varphi_1(a)\left((a-b)\,\varpi_2(a)+\varphi_2(b)\right)-\left((b-a)\,\varpi_1(b)+\varphi_1(a)\right)\varphi_2(b)}{a-b}\mathsf{X}\\ &\quad+\frac{a\left((b-a)\,\varpi_1(b)+\varphi_1(a)\right)\varphi_2(b)-b\varphi_1(a)\left((a-b)\,\varpi_2(a)+\varphi_2(b)\right)}{a-b}\\ &= \varphi_1(a)\varpi_2(a)\mathsf{X}+\frac{\varphi_1(a)\varphi_2(b)}{a-b}\mathsf{X}+\varphi_2(b)\varpi_1(b)\mathsf{X}-\frac{\varphi_1(a)\varphi_2(b)}{a-b}\mathsf{X}\\ &\quad-a\varphi_2(b)\varpi_1(b)+\frac{a\varphi_2(b)\varphi_1(a)}{a-b}-b\varphi_1(a)\varpi_2(a)-\frac{b\varphi_1(a)\varphi_2(b)}{a-b},\end{aligned}$$

οπότε

$$\upsilon(\mathsf{X})=\varphi_1(a)\varpi_2(a)\,(\mathsf{X}-b)+\varphi_2(b)\varpi_1(b)\,(\mathsf{X}-a)+\varphi_1(a)\varphi_2(b)$$

είναι η ζητούμενη έκφραση τού $\upsilon(\mathsf{X})$ συναρτήσει των $a, b, \varphi_1(a), \varpi_2(a), \varphi_2(b), \varpi_1(b)$.

Στην περίπτωση κατά την οποία

$$\begin{aligned}\varphi_1(\mathsf{X}) &= \mathsf{X}^2 + \left(3 - \sqrt{5} + 3i\right)\mathsf{X} + \left(8 - 3\sqrt{5}\right) + 9i, \\ \varphi_2(\mathsf{X}) &= \mathsf{X}^3 - i\mathsf{X}^2 + \mathsf{X} + 7\end{aligned}$$

και $a = \sqrt{5} - 3i$, $b = i$, έχουμε

$$\begin{aligned}\varphi_1(a) &= \left(\sqrt{5} - 3i\right)^2 + \left(3 - \sqrt{5} + 3i\right)\left(\sqrt{5} - 3i\right) + \left(8 - 3\sqrt{5}\right) + 9i = 8, \\ \varphi_1(b) &= i^2 + \left(3 - \sqrt{5} + 3i\right)i + \left(8 - 3\sqrt{5}\right) + 9i \\ &= 4 - 3\sqrt{5} + \left(12 - \sqrt{5}\right)i, \\ \varphi_2(a) &= \left(\sqrt{5} - 3i\right)^3 - i\left(\sqrt{5} - 3i\right)^2 + \left(\sqrt{5} - 3i\right) + 7 \\ &= 7 - 27\sqrt{5} - 17i \\ \varphi_2(b) &= i^3 - i(i^2) + i + 7 = 7 + i,\end{aligned}$$

οπότε

$$\begin{aligned}\tfrac{\varphi_1(a)\varphi_2(a) - \varphi_1(b)\varphi_2(b)}{a-b} &= \tfrac{8\left(7-27\sqrt{5}-17i\right) - \left(4-3\sqrt{5}+\left(12-\sqrt{5}\right)i\right)(7+i)}{\sqrt{5}-4i} \\ = \tfrac{40-196\sqrt{5}+\left(-224+10\sqrt{5}\right)i}{\sqrt{5}-4i} &= \tfrac{\left(40-196\sqrt{5}+\left(-224+10\sqrt{5}\right)i\right)\left(\sqrt{5}+4i\right)}{\left(\sqrt{5}-4i\right)\left(\sqrt{5}+4i\right)} \\ = \tfrac{\left(40-196\sqrt{5}+\left(-224+10\sqrt{5}\right)i\right)\left(\sqrt{5}+4i\right)}{21} &= \tfrac{-84+\left(210-1008\sqrt{5}\right)i}{21} = -4 + (10 - 48\sqrt{5})i\end{aligned}$$

και

$$\begin{aligned}\tfrac{a\varphi_1(b)\varphi_2(b) - b\varphi_1(a)\varphi_2(a)}{a-b} &= \tfrac{\left(\sqrt{5}-3i\right)\left(4-3\sqrt{5}+\left(12-\sqrt{5}\right)i\right)(7+i) - i8\left(7-27\sqrt{5}-17i\right)}{\sqrt{5}-4i} \\ = \tfrac{-14\sqrt{5}+28+i\left(364\sqrt{5}-154\right)}{\sqrt{5}-4i} &= \tfrac{\left(-14\sqrt{5}+28+i\left(364\sqrt{5}-154\right)\right)\left(\sqrt{5}+4i\right)}{\left(\sqrt{5}-4i\right)\left(\sqrt{5}+4i\right)} \\ = \tfrac{546-1428\sqrt{5}+\left(-210\sqrt{5}+1932\right)i}{21} &= 26 - 68\sqrt{5} + (92 - 10\sqrt{5})i.\end{aligned}$$

Εν κατακλείδι,

$$\upsilon(\mathsf{X}) = \left(-4 + (10 - 48\sqrt{5})i\right)\mathsf{X} + 26 - 68\sqrt{5} + (92 - 10\sqrt{5})i,$$

κάτι που αποπερατώνει τους υπολογισμούς μας.
