# Παράρτημα C

# Δακτύλιοι και σώματα

Παρά το γεγονός ότι οι σημειώσεις εστιάζονται στη μελέτη των *ομάδων*, στο ένα ή στο άλλο σημείο συναντούμε ορισμένες αβελιανές (προσθετικές) ομάδες, τα υποκείμενα σύνολα των οποίων εφοδιάζονται κατά τρόπο φυσικό και με μία δεύτερη (πολλαπλασιαστικώς συμβολιζόμενη) εσωτερική (προσεταιριστική) πράξη, μέσω τής οποίας αυτές καθίστανται *δακτύλιοι*. Γι' αυτόν τον λόγο παραθέτουμε εδώ τις πλέον βασικές έννοιες που αφορούν στη δομή τού *δακτυλίου*.

## C.1 ΔΑΚΤΥΛΙΟΙ

**C.1.1 Ορισμός.** Ένας **δακτύλιος** $(R, +, \cdot)$ είναι ένα μη κενό σύνολο $R$ εφοδιασμένο με δύο εσωτερικές πράξεις "$+$" και "$\cdot$", που καλούνται (και συμβολίζονται ως) *πρόσθεση* και *πολλαπλασιασμός*, αντιστοίχως, ούτως ώστε

(i) το ζεύγος $(R, +)$ να είναι μια αβελιανή ομάδα (βλ. 2.1.1),

(ii) το ζεύγος $(R, \cdot)$ να είναι μια ημιομάδα (βλ. 1.3.2 (i)) και

(iii) η "$\cdot$" να είναι τόσον *εξ αριστερών* όσον και *εκ δεξιών επιμεριστική* ως προς την "$+$", δηλαδή για κάθε $a, b$ και $c \in R$ να ισχύει

$$a(b+c) = ab + ac \text{ και } (a+b)c = ac + bc.$$

Το ουδέτερο στοιχείο τής ομάδας $(R, +)$ καλείται **μηδενικό στοιχείο** τού $(R, +, \cdot)$ και σημειώνεται με το $0_R$. Εάν η ημιομάδα $(R, \cdot)$ διαθέτει *μοναδιαίο (=* πολλαπλασιαστικώς ουδέτερο*) στοιχείο* (σημειούμενο ως $1_R$), δηλαδή εάν η $(R, \cdot)$ είναι ένα μονοειδές, τότε και ο $(R, +, \cdot)$ καλείται **δακτύλιος με μοναδιαίο στοιχείο.** Εάν η ημιομάδα $(R, \cdot)$ είναι αβελιανή, τότε λέμε ότι ο $(R, +, \cdot)$ είναι **μεταθετικός δακτύλιος**.

**C.1.2 Σημείωση.** Για λόγους συντομίας, αντί τού $a \cdot b$ θα γράφουμε ως επί το πλείστον $ab$, ενώ όταν θα ομιλούμε για κάποιον «δακτύλιο $R$», θα υπονοούμε τη θεώρηση μιας τριάδας $(R, +, \cdot)$ όπως στον ορισμό C.1.1 χωρίς όμως και να τη σημειώνουμε. Επίσης, εάν $n \in \mathbb{N}$ και εάν τα $a_1,..., a_n$ είναι στοιχεία ενός δακτυλίου $R$, τότε χρησιμοποιούμε ενίοτε τις βραχυγραφίες

$$\sum_{i=1}^{n} a_i := a_1 + \cdots + a_n \quad \text{και} \quad \prod_{i=1}^{n} a_i := a_1 \cdot \cdots \cdot a_n.$$

**C.1.3 Παραδείγματα.** (i) Ως προς τις *συνήθεις* πράξεις προσθέσεως "$+$" και πολλαπλασιασμού "$\cdot$", οι τριάδες $(\mathbb{Z}, +, \cdot)$ , $(\mathbb{Q}, +, \cdot)$ , $(\mathbb{R}, +, \cdot)$ και $(\mathbb{C}, +, \cdot)$ καθίστανται μεταθετικοί δακτύλιοι με μοναδιαίο στοιχείο.

(ii) Ως προς τις πράξεις προσθέσεως "$+$" και πολλαπλασιασμού "$\cdot$" τις εισαχθείσες στην ενότητα B.4 (βλ. (B.51) και B.4.44), η τριάδα $(\mathbb{Z}_m, +, \cdot)$ καθίσταται για κάθε $m \in \mathbb{N}$ μεταθετικός δακτύλιος με μοναδιαίο στοιχείο. (Εν προκειμένω, $0_{\mathbb{Z}_m} = [0]_m$ και $1_{\mathbb{Z}_m} = [1]_m$).

(iii) Το σύνολο $2\mathbb{Z}$ των αρτίων ακεραίων αριθμών, εφοδιαζόμενο με τις *συνήθεις* πράξεις προσθέσεως και πολλαπλασιασμού, αποτελεί μεταθετικό δακτύλιο *χωρίς* μοναδιαίο στοιχείο.

(iv) Εκκινώντας από τον $(\mathbb{Z}, +, \cdot)$ μπορούμε να κατασκευάσουμε έναν άλλο μεταθετικό δακτύλιο με μοναδιαίο στοιχείο $(\mathbb{Z}, \boxplus, \boxdot)$ μέσω των πράξεων

$$a \boxplus b := a + b - 1, \qquad a \boxdot b := a + b - ab\ .$$

Το αξιοπερίεργο εδώ είναι ότι το ουδέτερο στοιχείο αυτού τού δακτυλίου ως προς την πρόσθεση $\boxplus$ είναι το $1$, ενώ το μοναδιαίο στοιχείο ως προς τον πολλαπλασιασμό $\boxdot$ είναι το $0$.

(v) Έστω $X$ ένα μη κενό σύνολο και έστω $R$ ένας δακτύλιος. Τότε το σύνολο των απεικονίσεων $R^X := \{\text{απεικονίσεις } f : X \longrightarrow R\}$ καθίσταται δακτύλιος μέσω των «σημειακών» πράξεων

$$\begin{aligned} f + g : X \longrightarrow R, &\quad x \longmapsto f(x) + g(x) \\ f \cdot g : X \longrightarrow R, &\quad x \longmapsto f(x) \cdot g(x) \end{aligned}$$

Ιδιαιτέρως, εάν $X = \{1,..., n\} \subset \mathbb{N}$, τότε μπορούμε να ταυτίζουμε το $R^X$ με το *καρτεσιανό γινόμενο* $\underbrace{R \times R \times \cdots \times R \times R}_{n \text{ φορές}}$, το οποίο αποκτά τη δομή τού δακτυλίου μέσω των πράξεων

$$(x_1, x_2,..., x_n) + (y_1, y_2,..., y_n) := (x_1 + y_1, x_2 + y_2,..., x_n + y_n)\ ,$$
$$(x_1, x_2,..., x_n) \cdot (y_1, y_2,..., y_n) := (x_1 \cdot y_1, x_2 \cdot y_2,..., x_n \cdot y_n)\ ,$$

με ουδέτερο στοιχείο ως προς την πρόσθεση το $(0_R,..., 0_R)$. Εξάλλου, δοθέντων $n$ αυθαιρέτως επιλεγμένων δακτυλίων $R_1, R_2,..., R_n$ μπορούμε να ορίσουμε τη δομή ενός δακτυλίου επί τού *καρτεσιανού* ή (*εξωτερικού* ) *ευθέος γινομένου* τους

$$\prod_{j=1}^{n} R_j := R_1 \times \cdots \times R_n \tag{C.1}$$

με τις ανάλογες πράξεις κατά παράγοντες. Ο δακτύλιος (C.1) είναι μεταθετικός εάν και μόνον εάν καθένας των παραγόντων του είναι μεταθετικός. Επιπροσθέτως, ο (C.1) έχει μοναδιαίο στοιχείο εάν και μόνον εάν καθένας των παραγόντων του έχει μοναδιαίο στοιχείο. (Μάλιστα, όταν ο (C.1) έχει μοναδιαίο στοιχείο, τότε αυτό είναι το $(1_{R_1},\dots,1_{R_n})$.) Κατ' αναλογίαν, εάν η $(R_j)_{j\in J}$ είναι μια μη κενή οικογένεια δακτυλίων, μπορούμε να ορίσουμε τη δομή δακτυλίου επί τού $\prod\limits_{j\in J} R_j$ μέσω των πράξεων

$$(x_j)_{j\in J} + (y_j)_{j\in J} := (x_j + y_j)_{j\in J},\ (x_j)_{j\in J}\cdot(y_j)_{j\in J} := (x_j\cdot y_j)_{j\in J}.$$

(vi) Εάν το $R$ είναι ένα μονοσύνολο, τότε μπορεί να θεωρηθεί κατά τρόπο τετριμμένο ως δακτύλιος και γι' αυτό ονομάζεται **τετριμμένος δακτύλιος**. Σε αυτήν την περίπτωση έχουμε προφανώς $0_R = 1_R$.

**C.1.4 Πρόταση.** *Έστω $R$ ένας δακτύλιος. Τότε ισχύουν τα εξής:*

(i) $0_R\, a = a\, 0_R = 0_R$, *για όλα τα $a \in R$.*

(ii) $(-a)\, b = a\, (-b) = -(a\, b)$, *για όλα τα $a, b \in R$.*

(iii) $(-a)\, (-b) = a\, b$, *για όλα τα $a, b \in R$.*

(iv) *Για $m, n \in \mathbb{N}$ και για οιαδήποτε στοιχεία $a_1,\dots,a_m, b_1,\dots,b_n$ τού $R$ έχουμε*

$$\left(\sum_{j=1}^{m} a_j\right)\left(\sum_{k=1}^{n} b_k\right) = \sum_{j=1}^{m}\sum_{k=1}^{n} a_j\, b_k\ .$$

(v) *Εάν για οιαδήποτε $a \in R$ και $n \in \mathbb{Z}$ χρησιμοποιήσουμε τη βραχυγραφία*

$$\boxed{na := \begin{cases} \underbrace{a + a + \cdots + a + a}_{n\text{-φορές}}, & \text{όταν}\quad n > 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a) + (-a)}_{(-n)\text{-φορές}}, & \text{όταν}\quad n < 0 \\ 0_R\ , & \text{όταν}\quad n = 0 \end{cases}}$$

*από τη θεωρία των προσθετικών ομάδων, τότε*

$$(na)\, b = a\, (nb) = n(a\, b)$$

*για όλα τα $n \in \mathbb{Z}$ και όλα τα $a, b \in R$.*

(vi) *Εάν ο δακτύλιος $R$ έχει μοναδιαίο στοιχείο και διαθέτει περισσότερα τού ενός στοιχεία, τότε $1_R \neq 0_R$.*

ΑΠΟΔΕΙΞΗ. (i) $0_R\, a = (0_R + 0_R)\, a = 0_R\, a + 0_R\, a \Longrightarrow 0_R\, a = 0_R$. Ομοίως δείχνει κανείς ότι $a\, 0_R = 0_R$.

(ii) Προφανώς, $a\, b + a\, (-b) = a\, (b + (-b)) = a\, 0_R = 0_R \Longrightarrow a\, (-b) = -(a\, b)$. Η δεύτερη ισότητα αποδεικνύεται με ανάλογο τρόπο.

(iii) Προφανώς, $(-a)(-b) = -(-a)\, b = -(-(a\, b)) = a\, b$ [ύστερα από διπλή εφαρμογή τής (ii)].

(iv) Θεωρούμε το $m$ ως παγιωμένο και χρησιμοποιούμε μαθηματική επαγωγή ως προς τον $n$. Για $n = 1$ η ανωτέρω ισότητα γράφεται ως

$$(a_1 + \cdots + a_m)\, b_1 = a_1 b_1 + \cdots + a_m b_1$$

και είναι αληθής λόγω τής επιμεριστικής ιδιότητας τού πολλαπλασιασμού τού $R$ ως προς την πρόσθεση. Ας υποθέσουμε ότι, για δοθέντες $m, n$, ισχύει η ισότητα

$$\left(\sum_{j=1}^{m} a_j\right) \left(\sum_{k=1}^{n} b_k\right) = \sum_{j=1}^{m} \sum_{k=1}^{n} a_j\, b_k.$$

Εφαρμόζοντας εκ νέου την επιμεριστική ιδιότητα, σε συνδυασμό με την επαγωγική μας υπόθεση, λαμβάνουμε

$$\begin{aligned} \left(\sum_{j=1}^{m} a_j\right) \left(\sum_{k=1}^{n+1} b_k\right) &= \left(\sum_{j=1}^{m} a_j\right) \left(\sum_{k=1}^{n} b_k + b_{n+1}\right) \\ &= \left(\sum_{j=1}^{m} a_j\right) \left(\sum_{k=1}^{n} b_k\right) + \left(\sum_{j=1}^{m} a_j\right) b_{n+1} \\ &= \sum_{j=1}^{m} \sum_{k=1}^{n} a_j\, b_k + \sum_{j=1}^{m} a_j\, b_{n+1} = \sum_{j=1}^{m} \sum_{k=1}^{n+1} a_j\, b_k. \end{aligned}$$

(v) Τούτο έπεται άμεσα από το (iv).

(vi) Επί τη βάσει τής υποθέσεώς μας, $R \smallsetminus \{0_R\} \neq \varnothing$. Άρα για κάθε $a \in R \smallsetminus \{0_R\}$ έχουμε $1_R a = a$, οπότε $1_R \neq 0_R$. $\square$

**C.1.5 Ορισμός.** Για κάθε στοιχείο $a$ ενός δακτυλίου $R$ και έναν $n \in \mathbb{N}$, θέτουμε

$$\boxed{a^n := \underbrace{a \cdot a \cdot \cdots \cdot a \cdot a}_{n \text{ φορές}}}$$

και $a^0 := 1_R$, όταν ο $R$ διαθέτει μοναδιαίο στοιχείο. Προφανώς $a^m a^n = a^{m+n}$ και $(a^m)^n = a^{mn}$ για όλους τους φυσικούς αριθμούς $m, n$.

**C.1.6 Σημείωση.** Εάν ο $R$ διαθέτει μοναδιαίο στοιχείο και $a, b \in R$ με $ab = ba$, τότε για κάθε $n \in \mathbb{N}$ είναι εύκολο να αποδειχθεί (επαγωγικώς) ο ακόλουθος (γενικευμένος) *διωνυμικός τύπος*:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k}, \tag{C.2}$$

όπου $\binom{n}{k} := \frac{n!}{k!(n-k)!}$.

**C.1.7 Ορισμός.** Ένα μη κενό υποσύνολο $S$ (τού υποκειμένου συνόλου $R$) ενός δακτυλίου $(R, +, \cdot)$ καλείται **υποδακτύλιος** τού $(R, +, \cdot)$ όταν το $S$ είναι κλειστό ως προς αμφότερες τις πράξεις "$+$" και "$\cdot$" και καθίσταται αφ' εαυτού δακτύλιος (ως προς τον περιορισμό των εν λόγω πράξεων επ' αυτού).

**C.1.8 Πρόταση.** *Ένα μη κενό υποσύνολο $S$ ενός δακτυλίου $R$ είναι υποδακτύλιος τού $R$ εάν και μόνον εάν ικανοποιούνται οι ακόλουθες συνθήκες:*

(i) $a - b := a + (-b) \in S$, *για κάθε* $(a, b) \in S \times S$.

(ii) $ab \in S$, *για κάθε* $(a, b) \in S \times S$.

ΑΠΟΔΕΙΞΗ. Εάν το $S$ είναι υποδακτύλιος τού $R$, τότε $-b \in S$ για κάθε $b \in S$ (καθώς η $(S, +)$ είναι υποομάδα τής $(R, +)$). Επομένως, $a - b := a + (-b) \in S$ και $ab \in S$, $\forall\, (a, b) \in S \times S$ (λόγω τού ότι το σύνολο $S$ είναι κλειστό ως προς αμφότερες τις πράξεις "$+$" και "$\cdot$"). Και αντιστρόφως· εάν ικανοποιούνται οι ανωτέρω συνθήκες, τότε $a + (-a) = 0_R \in S$ για κάθε $a \in S$ (λόγω τής (i)), οπότε η $(S, +)$ είναι υποομάδα τής $(R, +)$ (βλ. πρόταση 2.1.16). Το ότι το ζεύγος $(S, \cdot)$ είναι ημιομάδα και το ότι η "$\cdot$" είναι τόσον εξ αριστερών όσον και εκ δεξιών επιμεριστική ως προς την "$+$" *εντός τού* $S$ έπεται από την (ii). □

**C.1.9 Παραδείγματα.** (i) Ο δακτύλιος $\mathbb{Z}$ είναι υποδακτύλιος τού $\mathbb{Q}$, ο $\mathbb{Q}$ υποδακτύλιος τού $\mathbb{R}$ και ο $\mathbb{R}$ είναι υποδακτύλιος τού $\mathbb{C}$. Επίσης, ο $2\mathbb{Z}$ είναι υποδακτύλιος τού $\mathbb{Z}$ και το $\{[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}$ υποδακτύλιος τού $\mathbb{Z}_{10}$.

(ii) Ο *δακτύλιος των ακεραίων τού Gauss* (ή «*γκαουσιανών ακεραίων*»)

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subsetneqq \mathbb{C}$$

με πράξεις τις (συνήθεις πράξεις τού $\mathbb{C}$):

$$\begin{aligned}(a + bi) + (c + di) &:= (a + c) + (b + d)i, \\ (a + bi) \cdot (c + di) &:= (ac - bd) + (ad + bc)i,\end{aligned}$$

όπου $i$ η «φανταστική» μονάδα, είναι (μεταθετικός) υποδακτύλιος τού δακτυλίου των μιγαδικών αριθμών, ενώ περιέχει τον $\mathbb{Z}$ ως υποδακτύλιό του. Γενικότερα, το

$$\mathbb{Z}[\sqrt{m}] := \left\{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\right\} \subsetneqq \mathbb{C},$$

όπου το $m \in \mathbb{Z}$ δεν είναι τέλειο τετράγωνο (δηλαδή $\sqrt{m} \notin \mathbb{Q}$), καθίσταται υποδακτύλιος τού $\mathbb{R}$, όταν $m \in \mathbb{N}$, και υποδακτύλιος τού $\mathbb{C}$, όταν $m \in \mathbb{Z} \smallsetminus \mathbb{N}_0$, καθότι για οιουσδήποτε $a + b\sqrt{m}$, $a' + b'\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$, έχουμε

$$\left\{\begin{array}{l}(a + b\sqrt{m}) - (a' + b'\sqrt{m}) = (a - a') + (b - b')\sqrt{m} \in \mathbb{Z}[\sqrt{m}], \\ \\ (a + b\sqrt{m})\,(a' + b'\sqrt{m}) = (aa' + bmb') + (ab' + ba')\sqrt{m} \in \mathbb{Z}[\sqrt{m}].\end{array}\right.$$

(iii) Κάθε δακτύλιος $R$ έχει πάντοτε ως υποδακτυλίους τον εαυτό του και τον **τετριμμένο υποδακτύλιο** $\{0_R\}$. Ένας υποδακτύλιος $S$ ενός δακτυλίου $R$ με $S \subsetneqq R$ λέγεται **γνήσιος υποδακτύλιος** τού $R$.

**C.1.10 Σημείωση.** Υπάρχουν υποδακτύλιοι $S$ δακτυλίων $R$ που συμπεριφέρονται αρκετά παράξενα όσον αφορά στην ύπαρξη ή μη μοναδιαίου στοιχείου.

(i) Ο $S$ είναι δυνατόν να μην έχει μοναδιαίο στοιχείο, ενώ ο $R$ να έχει, όπως π.χ. συμβαίνει στους $S = 2\mathbb{Z},\ R = \mathbb{Z}$.

(ii) Επίσης, ο $S$ μπορεί να έχει μοναδιαίο στοιχείο, ενώ ο $R$ να μην έχει, όπως π.χ. συμβαίνει στους $S = \{0\} \times \mathbb{R},\ R = 2\mathbb{Z} \times \mathbb{R}$.

(iii) Εάν ο $R$ έχει μοναδιαίο στοιχείο το $1_R$ και $1_R \in S$, τότε $1_R = 1_S$.

(iv) Τέλος, ενδέχεται και οι δυο τους να έχουν μοναδιαία στοιχεία $1_S$ και $1_R$, αντιστοίχως, χωρίς αυτά να είναι ίσα μεταξύ τους. Π.χ., ο $R = \mathbb{Z} \times \mathbb{Z}$ έχει ως μοναδιαίο του στοιχείο το $(1,1)$, ενώ ο υποδακτύλιός του $S = \mathbb{Z} \times \{0\}$ το $(1,0)$.

**C.1.11 Πρόταση.** *Εάν η $(S_j)_{j\in J}$ είναι μια μη κενή οικογένεια υποδακτυλίων ενός δακτυλίου $R$, τότε η τομή $\bigcap_{j\in J} S_j$ αποτελεί έναν υποδακτύλιο τού $R$.*

ΑΠΟΔΕΙΞΗ. Επειδή $0_R \in S_j$ για κάθε $j \in J$, έχουμε $0_R \in \bigcap_{j\in J} S_j$, οπότε η τομή αυτή δεν είναι κενή. Εάν $a, b \in \bigcap_{j\in J} S_j$, τότε

$$[a, b \in S_j,\ \forall j \in J] \Longrightarrow [a - b \in S_j,\ \forall j \in J] \Longrightarrow a - b \in \bigcap_{j\in J} S_j$$

και $[a, b \in S_j,\ \forall j \in J] \Longrightarrow [ab \in S_j,\ \forall j \in J] \Longrightarrow ab \in \bigcap_{j\in J} S_j$. Άρα η $\bigcap_{j\in J} S_j$ είναι όντως ένας υποδακτύλιος τού $R$ (βλ. πρόταση C.1.8). □

**C.1.12 Ορισμός.** Έστω $(R, +, \cdot)$ ένας μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο. Ένα στοιχείο τού $R$ καλείται **αντιστρέψιμο στοιχείο** όταν διαθέτει (κατ' ανάγκην μονοσημάντως ορισμένο[1]) *αντίστροφο στοιχείο* (= συμμετρικό στοιχείο ως προς την πράξη τού πολλαπλασιασμού). Μέσω τού μονοειδούς $(R, \cdot)$ ορίζεται η (πολλαπλασιαστική) **ομάδα** $(R^\times, \cdot)$ **των αντιστρεψίμων στοιχείων τού** $R$. (Βλ. πρόταση 2.1.6.)

**C.1.13 Σημείωση.** (i) Προφανώς, $\{\pm 1_R\} \subseteq R^\times$.

(ii) Η $R^\times$ είναι δυνατόν να είναι αβελιανή ακόμη και όταν ο $R$ δεν είναι μεταθετικός.

(iii) Άλλοτε η $R^\times$ έχει *πεπερασμένη* τάξη, όπως στην περίπτωση θεωρήσεως τού δακτυλίου $R = \mathbb{Z}_m$, $m \geq 2$, με

$$\mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \mid 1 \leq k \leq m-1,\ \text{μκδ}\,(k, m) = 1\}$$

και $|\mathbb{Z}_m^\times| = \phi(m)$, όπου $\phi$ η συνάρτηση φι τού Euler (βλ. B.4.43, B.4.15), και άλλοτε *άπειρη*. Επί παραδείγματι, η

$$\mathbb{Z}[\sqrt{2}]^\times = \left\{\pm(1+\sqrt{2})^k \mid k \in \mathbb{Z}\right\}$$

[1] Βλ. πρόταση 1.2.13.

είναι άπειρη αριθμήσιμη. (Για ένα άλλο παράδειγμα δακτυλίου με άπειρη *υπεραριθμήσιμη* ομάδα αντιστρεψίμων στοιχείων βλ. εδάφιο D.2.20 (ii).)

(iv) Εάν ο $R$ είναι ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και $a, b \in R$, τότε $[a \in R^{\times}$ και $b \in R^{\times}] \iff ab \in R^{\times}$. Πράγματι· η συνεπαγωγή "$\Rightarrow$" είναι προφανής (λόγω τής κλειστότητας τής πολλαπλασιαστικής πράξεως τής ομάδας $(R^{\times}, \cdot)$). Και αντιστρόφως· εάν $ab \in R^{\times}$, τότε υπάρχει μονοσημάντως ορισμένο στοιχείο $c \in R^{\times}$, τέτοιο ώστε να ισχύει $(ab)c = 1_R$. Επειδή $(ab)c = a(bc) = b(ac)$, τα $a$ και $b$ είναι αντιστρέψιμα στοιχεία τού $R$ (με το $a$ έχον ως αντίστροφό του το $bc$ και με το $b$ έχον αντίστροφό του το $ac$). Άρα και η "$\Leftarrow$" είναι αληθής. Γενικότερα, για οιονδήποτε φυσικό αριθμό $n \geq 2$ και για οιαδήποτε στοιχεία $a_1, ..., a_n$ τού $R$ έχουμε $[a_i \in R^{\times}, \forall i \in \{1, ..., n\}] \iff \prod_{i=1}^{n} a_i \in R^{\times}$.

(v) Εάν ο $S$ είναι ένας μη τετριμμένος υποδακτύλιος (με μοναδιαίο στοιχείο $1_S$) ενός δακτυλίου $R$ με μοναδιαίο στοιχείο $1_R = 1_S$, τότε $S^{\times} \subseteq R^{\times} \cap S$, χωρίς να αποκλείεται ο εγκλεισμός να είναι αυστηρός. Επί παραδείγματι, όταν $R = \mathbb{R}$ και $S = \mathbb{Z}$, τότε $2 \in R^{\times} = \mathbb{R} \smallsetminus \{0\}$ αλλά $2 \notin S^{\times} = \{\pm 1\}$.

► **Ομομορφισμοί δακτυλίων**. Πρόκειται για απεικονίσεις μεταξύ δακτυλίων που είναι ομομορφισμοί ομάδων (ως προς τις προσθετικές τους πράξεις) και *ταυτοχρόνως* μεταφέρουν κατά «δομοθεωρητικώς επιτρεπτό» τρόπο *και* τις πολλαπλασιαστικές τους πράξεις.

**C.1.14 Ορισμός.** Εάν οι $(R_1, +_1, \cdot_1)$ και $(R_2, +_2, \cdot_2)$ είναι δυο δακτύλιοι και

$$f : R_1 \longrightarrow R_2$$

μια απεικόνιση, τότε η $f$ καλείται **ομομορφισμός (δακτυλίων)** όταν[2]

$$\boxed{f(a +_1 b) = f(a) +_2 f(b)} \quad \text{και} \quad \boxed{f(a \cdot_1 b) = f(a) \cdot_2 f(b)}$$

για όλα τα $a, b \in R$. (Προφανώς, $f(0_{R_1}) = 0_{R_2}$.)

Ένας ομομορφισμός δακτυλίων $f : R_1 \longrightarrow R_2$ ονομάζεται **μονομορφισμός** και, αντιστοίχως, **επιμορφισμός/ισομορφισμός (δακτυλίων)** όταν η απεικόνιση $f$ είναι ενριπτική και, αντιστοίχως, επιρριπτική/αμφιρριπτική.

**C.1.15 Παραδείγματα.** (i) Έστω $m$ ένας φυσικός αριθμός. Ορίζουμε την απεικόνιση $f : \mathbb{Z} \longrightarrow \mathbb{Z}_m, n \longmapsto [n]_m$. Είναι εύκολο να αποδειχθεί ότι η $f$ είναι ένας επιμορφισμός δακτυλίων.

(ii) Η απεικόνιση $f : \mathbb{Z} \longrightarrow 2\,\mathbb{Z}$ η οριζομένη μέσω τού τύπου $f(n) := 2n$ *δεν είναι* ομομορφισμός δακτυλίων, παρότι *είναι* ισομορφισμός μεταξύ των αντιστοίχων προσθετικών ομάδων!

[2] Απλούστευση συμβολισμού: Κατά κανόνα (για λόγους συντομίας) οι δείκτες 1, 2 *παραλείπονται* στον συμβολισμό των πράξεων.

(iii) Έστω $(2\,\mathbb{Z}, +, *)$ ο δακτύλιος ο αποτελούμενος από τους αρτίους ακεραίους με τη συνήθη πρόσθεση και τον ακόλουθο «τροποποιημένο» πολλαπλασιασμό:

$$m * n := \frac{m \cdot n}{2}\ .$$

Τότε η $f : \mathbb{Z} \longrightarrow 2\,\mathbb{Z}$ η οριζομένη μέσω τού τύπου $f\,(n) := 2n$ (όπως στο (ii)) αποτελεί *ισομορφισμό δακτυλίων.*

(iv) Η *μηδενική απεικόνιση* $f : R_1 \longrightarrow R_2$ μεταξύ δυο δακτυλίων $R_1$ και $R_2$, όπου $f(a) = 0_{R_2}$ για κάθε $a \in R_1$, είναι ένας ομομορφισμός δακτυλίων (ο λεγόμενος *μηδενικός ομομορφισμός*). Σημειωτέον ότι όταν κανείς εκ των $R, S$ δεν είναι τετριμμένος, ο μηδενικός ομομορφισμός δεν είναι ούτε ενριπτικός ούτε επιρριπτικός.

**C.1.16 Πρόταση.** *Ένας ομομορφισμός δακτυλίων $f : R_1 \longrightarrow R_2$ έχει τις εξής ιδιότητες:*

(i) *Εάν ο $S_1$ είναι ένας υποδακτύλιος τού $R_1$, τότε η εικόνα του $f\,(S_1)$ μέσω τής $f$ είναι ένας υποδακτύλιος τού $R_2$.*

(ii) *Εάν ο $S_2$ είναι ένας υποδακτύλιος τού $R_2$, τότε η αντίστροφή του εικόνα $f^{-1}\,(S_2)$ μέσω τής $f$ είναι ένας υποδακτύλιος τού $R_1$.*

(iii) *Εάν ο $R_1$ είναι ένας δακτύλιος με μοναδιαίο στοιχείο, τότε και ο $f(R_1)$ είναι δακτύλιος με μοναδιαίο στοιχείο, και μάλιστα ισχύει η ισότητα $f\,(1_{R_1}) = 1_{f(R_1)}$.*

ΑΠΟΔΕΙΞΗ. (i) Εάν $b_1, b_2 \in f(S_1)$, τότε υπάρχουν $a_1, a_2 \in S_1$, τέτοια ώστε να ισχύει $f(a_1) = b_1$ και $f(a_2) = b_2$. Επειδή ο $S_1$ είναι ένας υποδακτύλιος τού $R_1$,

$$\left.\begin{array}{r} a_1 - a_2 \in S_1, \\ a_1 a_2 \in S_1 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} b_1 - b_2 = f(a_1) - f(a_2) = f(a_1 - a_2) \in f(S_1), \\ b_1 b_2 = f(a_1) f(a_2) = f(a_1 a_2) \in f(S_1), \end{array}\right.$$

οπότε η εικόνα $f(S_1)$ τού $S_1$ μέσω τής $f$ είναι όντως ένας υποδακτύλιος τού $R_2$.

(ii) Εάν $a_1, a_2 \in f^{-1}(S_2)$, τότε $f(a_1) \in S_2$ και $f(a_2) \in S_2$. Κι επειδή ο $S_2$ είναι υποδακτύλιος τού $R_2$,

$$\left.\begin{array}{r} f(a_1 - a_2) = f(a_1) - f(a_2) \in S_2, \\ f(a_1 a_2) = f(a_1) f(a_2) \in S_2 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} a_1 - a_2 \in f^{-1}(S_2), \\ a_1 a_2 \in f^{-1}(S_2), \end{array}\right.$$

ήτοι *και* η αντίστροφή του εικόνα $f^{-1}\,(S_2)$ μέσω τής $f$ είναι ένας υποδακτύλιος τού δακτυλίου $R_1$.

(iii) Έστω $b$ τυχόν στοιχείο τού $f(R_1)$. Τότε υπάρχει ένα $a \in R_1$, τέτοιο ώστε να ισχύει η ισότητα $f(a) = b$. Άρα

$$f(1_{R_1}) f(a) = f(1_{R_1} a) = f(a), \quad f(a) f(1_{R_1}) = f(a 1_{R_1}) = f(a),$$

οπότε ο $f(R_1)$ είναι δακτύλιος με μοναδιαίο στοιχείο και $f\,(1_{R_1}) = 1_{f(R_1)}$. □

► **Πολυωνυμικοί δακτύλιοι**. Δοθέντος ενός δακτυλίου $R$ με μοναδιαίο στοιχείο θεωρούμε το σύνολο $R^{\mathbb{N}_0}$ των ακολουθιών $(a_0, a_1, a_2, \ldots\ldots)$ με $a_i \in R$, $i = 0, 1, 2, \ldots$, καθώς και το σύνολο $R^{(\mathbb{N}_0)}$ των ακολουθιών $(a_0, a_1, a_2, \ldots\ldots)$ με $a_i \in R$, $i = 0, 1, 2, \ldots$, για τις οποίες υπάρχουν *το πολύ πεπερασμένου πλήθους* $a_i$ που είναι διάφορα τού $0_R$. Κάθε στοιχείο $\psi$ τού $R^{(\mathbb{N}_0)}$ γράφεται υπό τη μορφή

$$\psi = (a_0, a_1, a_2, ..., a_n, 0_R, 0_R, ...)$$

για κάποιον ακέραιο αριθμό $n \geq 0$. Προφανώς, δυο στοιχεία

$$\psi = (a_0, a_1, a_2, ..., a_n, ...), \ \ \chi = (b_0, b_1, b_2, ..., b_n, ...)$$

τού $R^{\mathbb{N}_0}$ είναι ίσα ($\psi = \chi$) όταν $a_i = b_i, \forall i \in \mathbb{N}_0$. Επί τού $R^{\mathbb{N}_0}$ ορίζουμε πράξεις *προσθέσεως* και *πολλαπλασιασμού* ως ακολούθως:

$$\left| \begin{array}{lcl} (a_0, a_1, a_2, ...) + (b_0, b_1, b_2, ...) & := & (a_0 + b_0, a_1 + b_1, a_2 + b_2, ...), \\ \\ (a_0, a_1, a_2, ...) \cdot (b_0, b_1, b_2, ...) & := & (c_0, c_1, c_2, ...), \end{array} \right.$$

όπου

$$c_m := \sum_{i+j=m} a_i b_j = a_0 b_m + a_1 b_{m-1} + \cdots + a_m b_0, \ \forall m \in \mathbb{N}_0. \tag{C.3}$$

Η τριάδα $(R^{\mathbb{N}_0}, +, \cdot)$ αποτελεί έναν δακτύλιο με μηδενικό του στοιχείο το $(0_R, 0_R, ...)$ και μοναδιαίο του στοιχείο το $(1_R, 0_R, 0_R, ...)$ και η τριάδα $(R^{(\mathbb{N}_0)}, +, \cdot)$ έναν υποδακτύλιο τού $(R^{\mathbb{N}_0}, +, \cdot)$ (με μοναδιαίο στοιχείο του το $(1_R, 0_R, 0_R, ...)$). Επίσης, *ταυτίζοντας* κάθε $a \in R$ με το $(a, 0_R, 0_R, ...)$ έχουμε τη δυνατότητα θεωρήσεως τού $R$ ως έναν υποδακτύλιο τού $(R^{(\mathbb{N}_0)}, +, \cdot)$. Εισάγοντας ένα νέο σύμβολο

$$\mathsf{X} := (0_R, 1_R, 0_R, 0_R, ...)$$

παρατηρούμε ότι, βάσει των ως άνω πράξεων,

$$\mathsf{X}^2 = (0_R, 0_R, 1_R, 0_R, 0_R, ...) \, , \ \mathsf{X}^3 = (0_R, 0_R, 0_R, 1_R, 0_R, 0_R, ...)$$

και, γενικότερα, $\mathsf{X}^n = (0_R, 0_R, ..., 0_R, \underbrace{\ 1_R\ }_{n+1 \text{ θέση}}, 0_R, 0_R, ...), \ \forall n \in \mathbb{N}_0$. Επίσης, λόγω τής ανωτέρω ταυτίσεως, για κάθε $a \in R$ λαμβάνουμε

$$a\mathsf{X}^n = (0_R, 0_R, ..., 0_R, \underbrace{\ a\ }_{n+1 \text{ θέση}}, 0_R, 0_R, ...), \ \forall n \in \mathbb{N}_0.$$

Εάν το $(a_0, a_1, a_2, ...)$ είναι τυχόν στοιχείο τού δακτυλίου $R^{(\mathbb{N}_0)}$, όπου $a_i = 0_R$, για κάθε $i \geq n$, για κάποιον παγιωμένο $n \in \mathbb{N}_0$, τότε μπορούμε να γράψουμε

$$(a_0, a_1, a_2, ..., a_n, 0_R, 0_R, ...) = a_0 + a_1\mathsf{X} + a_2\mathsf{X} + \cdots + a_n\mathsf{X}^n =: \sum_{i=0}^{n} a_i \mathsf{X}^i.$$

**C.1.17 Ορισμός.** Ο δακτύλιος $R^{(\mathbb{N}_0)}$ συμβολίζεται συνήθως ως $R\,[\mathsf{X}]$ και καλείται **δακτύλιος πολυωνύμων** (ή **πολυωνυμικός δακτύλιος**) μιας **απροσδιορίστου** $\mathsf{X}$ με συντελεστές ειλημμένους από τον $R$. Τα στοιχεία του ονομάζονται **πολυώνυμα** και σημειώνονται ως $\psi(\mathsf{X}), \chi(\mathsf{X}), ..$ κ.λπ., ενώ τα εκάστοτε αναγραφόμενα $a_0, a_1, a_2, ...$ ονομάζονται **συντελεστές** των πολυωνύμων.

**C.1.18 Παρατήρηση.** Βάσει τού ορισμού τού πολλαπλασιασμού πολυωνύμων είναι σαφές ότι ο δακτύλιος $R[\mathsf{X}]$ είναι μεταθετικός εάν και μόνον εάν ο ίδιος ο $R$ είναι μεταθετικός.

**C.1.19 Σημείωση.** Εκ των ανωτέρω συμπεραίνουμε ότι δυο πολυώνυμα

$$\psi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]\ ,\ \ \chi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}]$$

είναι **ίσα** ($\psi(\mathsf{X}) = \chi(\mathsf{X})$) εάν και μόνον εάν *είτε* αμφότερα είναι ίσα με το $0_{R[\mathsf{X}]}$ *είτε*

$$\max\{\, i \in \{0,...,n\} |\, a_i \neq 0_R\} = \max\{\, j \in \{0,...,m\} |\, b_j \neq 0_R\}\ \ (=: k)$$

και $a_i = b_i,\ \ \forall i \in \{0,...,k\}$.

**C.1.20 Ορισμός.** Εάν $\psi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}] \smallsetminus \{0_{R[\mathsf{X}]}\}$ και $a_n \neq 0_R$, τότε λέμε ότι ο αριθμός $\deg(\psi(\mathsf{X})) := n$ είναι **ο βαθμός** τού πολυωνύμου $\psi(\mathsf{X})$, το $a_0$ **ο σταθερός όρος** τού $\psi(\mathsf{X})$ και ο $\mathrm{LC}(\psi(\mathsf{X})) := a_n$ ο **επικεφαλής συντελεστής** (ή ο **μεγιστοβάθμιος συντελεστής**) τού $\psi(\mathsf{X})$. Στην περίπτωση όπου $\psi(\mathsf{X})$ είναι το **μηδενικό πολυώνυμο** $0_{R[\mathsf{X}]}$, θέτουμε εξ ορισμού $\deg(\psi(\mathsf{X})) := -\infty$, υπό τον όρο ότι θεσπίζουμε τη σύμβαση[3]: $-\infty < n,\ \ \forall n \in \mathbb{N}_0$. Κατ' αυτόν τον τρόπο ο βαθμός των πολυωνύμων μπορεί να εκληφθεί ως μια απεικόνιση

$$\deg : R[\mathsf{X}] \longrightarrow \mathbb{N}_0 \cup \{-\infty\}\,.$$

Ένα πολυώνυμο $\psi(\mathsf{X}) \in R[\mathsf{X}]$ λέγεται **σταθερό πολυώνυμο** όταν $\deg(\psi(\mathsf{X})) \leq 0$.

**C.1.21 Πρόταση.** *Έστω $R$ ένας δακτύλιος με μοναδιαίο στοιχείο. Για οιαδήποτε πολυώνυμα $\psi(\mathsf{X}), \chi(\mathsf{X}) \in R[\mathsf{X}]$ ισχύουν τα εξής:*

(i) $\deg(\psi(\mathsf{X}) + \chi(\mathsf{X})) \leq \max\{\deg(\psi(\mathsf{X})), \deg(\chi(\mathsf{X}))\}$.

(ii) $\deg(\psi(\mathsf{X}) \cdot \chi(\mathsf{X})) \leq \deg(\psi(\mathsf{X})) + \deg(\chi(\mathsf{X}))$.

(iii) *Εάν* $\deg(\psi(\mathsf{X})) \neq \deg(\chi(\mathsf{X}))$, *τότε*

$$\deg(\psi(\mathsf{X}) + \chi(\mathsf{X})) = \max\{\deg(\psi(\mathsf{X}))\,,\ \deg(\chi(\mathsf{X}))\}.$$

(iv) *Εάν* $\mathrm{LC}(\psi(\mathsf{X}))\cdot \mathrm{LC}(\chi(\mathsf{X})) \neq 0_R$, *τότε*

$$\deg(\psi(\mathsf{X}) \cdot \chi(\mathsf{X})) = \deg(\psi(\mathsf{X})) + \deg(\chi(\mathsf{X})).$$

ΑΠΟΔΕΙΞΗ. Εάν τουλάχιστον ένα εκ των $\psi(\mathsf{X}), \chi(\mathsf{X})$ είναι το μηδενικό πολυώνυμο, τότε τα (i)-(iii) είναι προφανώς αληθή. Ας υποθέσουμε ότι

$$\psi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in R[\mathsf{X}]\ ,\ a_n \neq 0_R,\quad \chi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in R[\mathsf{X}],\ \ b_m \neq 0_R,$$

[3]Επίσης, στο $\mathbb{N}_0 \cup \{-\infty\}$ θέτουμε $(-\infty) + (-\infty) := -\infty$, $(-\infty) \cdot (-\infty) := -\infty$ και $(-\infty) + n := n$, $(-\infty) \cdot n := -\infty$, $\forall n \in \mathbb{N}_0$.

και ας ορίσουμε $a_i := 0_R$ για κάθε $i > n$ και $b_j := 0_R$ για κάθε $j > m$.
(i) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n \geq m$. Τότε

$$\psi(\mathsf{X}) + \chi(\mathsf{X}) = \sum_{i=0}^{n} (a_i + b_i)\,\mathsf{X}^i, \tag{C.4}$$

οπότε $\deg(\psi(\mathsf{X}) + \chi(\mathsf{X})) \leq n = \max\{\deg(\psi(\mathsf{X})), \deg(\chi(\mathsf{X}))\}$.
(ii) Βάσει τής (C.3) το γινόμενο των δύο πολυωνύμων μπορεί να γραφεί ως

$$\psi(\mathsf{X}) \cdot \chi(\mathsf{X}) = \sum_{k \geq 0} \left( \sum_{i=0}^{k} a_i b_{k-i} \right) \mathsf{X}^k,$$

όπου

$$\sum_{i=0}^{k} a_i b_{k-i} = \begin{cases} a_n b_m, & \text{όταν } k = n + m \\ \sum\limits_{i=0}^{n} a_i b_{k-i} + \sum\limits_{i=n+1}^{k} a_i b_{k-i} = 0_R, & \text{όταν } k \geq n + m + 1 \end{cases} \tag{C.5}$$

Κατά συνέπειαν, $\deg(\psi(\mathsf{X}) \cdot \chi(\mathsf{X})) \leq n + m = \deg(\psi(\mathsf{X})) + \deg(\chi(\mathsf{X}))$.
(iii) Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $n > m$. Τότε έχουμε $a_n + b_n = a_n \neq 0_R$ και από την (C.4) έπεται ότι

$$\deg(\psi(\mathsf{X}) + \chi(\mathsf{X})) = n = \max\{\deg(\psi(\mathsf{X})),\ \deg(\chi(\mathsf{X}))\}.$$

(iv) Επειδή $a_n b_m = \mathrm{LC}(\psi(\mathsf{X}))\cdot \mathrm{LC}(\chi(\mathsf{X})) \neq 0_R$, από την ισότητα (C.5) λαμβάνουμε $\deg(\psi(\mathsf{X}) \cdot \chi(\mathsf{X})) = \deg(\psi(\mathsf{X})) + \deg(\chi(\mathsf{X}))$. □

**C.1.22 Παραδείγματα.** Σημειωτέον ότι οι ανωτέρω ανισοϊσότητες μπορούν πράγματι να ισχύουν και ως αυστηρές ανισότητες.
(i) Εάν $\psi(\mathsf{X}) = 2\mathsf{X} + 1$, $\chi(\mathsf{X}) = -2\mathsf{X} + 1 \in \mathbb{Z}[\mathsf{X}]$, τότε

$$0 = \deg(\psi(\mathsf{X}) + \chi(\mathsf{X})) < \max\{\deg(\psi(\mathsf{X})), \deg(\chi(\mathsf{X}))\} = 1.$$

(ii) Εάν $\psi(\mathsf{X}) = [2]_4\,\mathsf{X} + [1]_4$, $\chi(\mathsf{X}) = [-2]_4\,\mathsf{X} + [1]_4 \in \mathbb{Z}_4[\mathsf{X}]$, τότε

$$\psi(\mathsf{X}) \cdot \chi(\mathsf{X}) = [-4]_4\,\mathsf{X}^2 + [1]_4 = [1]_4\,,$$

που σημαίνει ότι $0 = \deg(\psi(\mathsf{X}) \cdot \chi(\mathsf{X})) < \deg(\psi(\mathsf{X})) + \deg(\chi(\mathsf{X})) = 2$.

## C.2 ΑΚΕΡΑΙΕΣ ΠΕΡΙΟΧΕΣ ΚΑΙ ΣΩΜΑΤΑ

**C.2.1 Ορισμός.** Έστω $R$ ένας μεταθετικός μη τετριμμένος δακτύλιος. Ένα στοιχείο $a \in R \diagdown \{0_R\}$ καλείται **μηδενοδιαιρέτης** όταν υπάρχει ένα $b \in R \diagdown \{0_R\}$, τέτοιο ώστε $ba = 0_R$.

**C.2.2 Παράδειγμα.** Τα στοιχεία $[2]_6, [3]_6$ τού δακτυλίου $\mathbb{Z}_6$ είναι μηδενοδιαιρέτες, διότι $[2]_6 \cdot [3]_6 = [3]_6 \cdot [2]_6 = [0]_6 = 0_{\mathbb{Z}_6}$.

**C.2.3 Ορισμός.** Κάθε μεταθετικός μη τετριμμένος δακτύλιος $R$ με μοναδιαίο στοιχείο, ο οποίος δεν διαθέτει κανέναν μηδενοδιαιρέτη, καλείται **ακεραία περιοχή.**

**C.2.4 Παραδείγματα.** (i) Ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι ακεραία περιοχή, διότι εάν το γινόμενο δύο ακεραίων αριθμών ισούται με $0$, τότε τουλάχιστον ένας εξ αυτών οφείλει να είναι το $0$.

(ii) Ο δακτύλιος $\mathbb{Z}_6$ είναι μεταθετικός, μη τετριμμένος δακτύλιος με μοναδιαίο στοιχείο, αλλά δεν είναι ακεραία περιοχή. (Βλ. παράδειγμα C.2.2).

**C.2.5 Πρόταση.** *Έστω $f : R_1 \longrightarrow R_2$ ένας ομομορφισμός δακτυλίων.*

(i) *Εάν ο $R_1$ είναι μεταθετικός, τότε και ο $f(R_1)$ είναι μεταθετικός.*

(ii) *Εάν ο $R_1$ είναι ένας δακτύλιος με μοναδιαίο στοιχείο, ο $f$ μη μηδενικός ομομορφισμός και ο $R_2$ ακεραία περιοχή, τότε $f\left(1_{R_1}\right) = 1_{R_2}$.*

(iii) *Εάν ο $f$ είναι μονομορφισμός και ο $R_1$ ακεραία περιοχή, τότε και ο $f(R_1)$ είναι ακεραία περιοχή.*

Αποδειξη. (i) Προφανώς, για κάθε $a, b \in R_1$, έχουμε

$$f(a)f(b) = f(ab) = f(ba) = f(b)f(a).$$

(ii) Επειδή -εξ υποθέσεως- ο $f$ δεν είναι ο μηδενικός ομομορφισμός, θα υπάρχει ένα $a \in R_1$, τέτοιο ώστε να ισχύει $f(a) \neq 0_{R_2}$. Εξ αυτού έπεται ότι

$$f(a) \cdot 1_{R_2} = f(a) = f(a \cdot 1_{R_1}) = f(a)f(1_{R_1}) \Longrightarrow f(a)\left(f\left(1_{R_1}\right) - 1_{R_2}\right) = 0_{R_2}.$$

Επειδή ο $R_2$ ακεραία περιοχή, λαμβάνουμε $f\left(1_{R_1}\right) = 1_{R_2}$.

(iii) Έστω ότι ο $f$ είναι μονομορφισμός και ο $R_1$ ακεραία περιοχή. Προφανώς, επειδή $1_{R_1} \neq 0_{R_1}$, το $f(1_{R_1}) = 1_{f(R_1)}$ είναι διάφορο τού $f(0_{R_1}) = 0_{R_1}$. Εάν υποθέσουμε ότι $f(a), f(b) \in f(R_1)$, για κάποια $a, b \in R_1$, τέτοια ώστε να ισχύει

$$f(a)f(b) = 0_{f(R_1)} \Longleftrightarrow f(ab) = 0_{f(R_1)} = f\left(0_{R_1}\right),$$

τότε $ab = 0_{R_1}$, οπότε είτε $a = 0_{R_1}$ είτε $b = 0_{R_1}$. Συνεπώς, είτε $f(a) = 0_{f(R_1)}$ είτε $f(b) = 0_{f(R_1)}$. Άρα *και* ο $f(R_1)$ είναι ακεραία περιοχή. $\square$

**C.2.6 Ορισμός.** (i) Ένας μεταθετικός δακτύλιος $(F, +, \cdot)$ με μοναδιαίο στοιχείο καλείται **σώμα** όταν κάθε μη μηδενικό στοιχείο τού $F$ (ήτοι κάθε στοιχείο ανήκον στο $F \smallsetminus \{0_F\}$) διαθέτει αντίστροφο (= «συμμετρικό» ως προς την πράξη τού πολλαπλασιασμού). Εν τοιαύτη περιπτώσει, $F^{\times} = F \smallsetminus \{0_F\}$. (Σημειωτέον ότι το υποκείμενο σύνολο ενός σώματος διαθέτει περισσότερα τού ενός στοιχεία.)

(ii) Εάν το $(F, +, \cdot)$ είναι ένα σώμα και το $F'$ ένας υποδακτύλιος αυτού με μοναδιαίο στοιχείο του το $1_{F'} = 1_F$, ο οποίος συμβαίνει να είναι σώμα ως προς τις ίδιες πράξεις, τότε το $F'$ καλείται **υπόσωμα** τού $F$.

**C.2.7 Παραδείγματα.** (i) Ο δακτύλιος $\mathbb{Z}$ των ακεραίων δεν είναι σώμα (παρότι είναι ακεραία περιοχή), διότι οι ακέραιοι $n \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$ δεν διαθέτουν αντίστροφα στοιχεία.

(ii) Οι δακτύλιοι $\mathbb{Q}, \mathbb{R}$ και $\mathbb{C}$ των ρητών, των πραγματικών και των μιγαδικών αριθμών (ως προς τις συνήθεις πράξεις προσθέσεως και πολλαπλασιασμού) είναι σώματα, και μάλιστα το $\mathbb{Q}$ είναι υπόσωμα τού $\mathbb{R}$ και το $\mathbb{R}$ υπόσωμα τού $\mathbb{C}$.

**C.2.8 Πρόταση.** (i) *Κάθε σώμα είναι ακεραία περιοχή.*

(ii) *Κάθε πεπερασμένη ακεραία περιοχή είναι σώμα.*

ΑΠΟΔΕΙΞΗ. (i) Έστω $F$ ένα σώμα. Εάν $a \in F \smallsetminus \{0_F\}$ και εάν υποθέσουμε ότι υφίσταται κάποιο $b \in F$, τέτοιο ώστε να ισχύει $ab = 0_F$, τότε

$$a^{-1}(ab) = a^{-1} \cdot 0_F = 0_F \Rightarrow 0_F = a^{-1}(ab) = (a^{-1}a)b = 1_F \cdot b = b,$$

οπότε το $F$ δεν διαθέτει κανέναν μηδενοδιαιρέτη και είναι, ως εκ τούτου, ακεραία περιοχή.

(ii) Έστω $R$ μια ακεραία περιοχή με πεπερασμένο πλήθος στοιχείων και έστω τυχόν $a \in R \smallsetminus \{0_R\}$. Αρκεί να αποδείξουμε ότι το $a$ διαθέτει αντίστροφο στοιχείο. Εάν $a = 1_R$, τότε αυτό είναι προφανές (διότι το $a$ θα έχει τον εαυτό του ως αντίστροφο στοιχείο). Εάν $a \neq 1_R$, τότε θεωρούμε την ακολουθία στοιχείων τού $R$:

$$a, a^2, a^3, \ldots, a^n, a^{n+1}, \ldots$$

Επειδή το σύνολο $R$ είναι πεπερασμένο, θα υπάρχουν κατ' ανάγκην $i, j \in \mathbb{N}, i > j$, με $a^i = a^j$. Από τον ορισμό τής ακεραίας περιοχής έπεται ότι

$$\left.\begin{array}{r} a^{i-j}a^j - a^j = \left(a^{i-j} - 1_R\right) a^j = 0_R \\ a \neq 0_R \Rightarrow a^j \neq 0_R \end{array}\right\} \Longrightarrow a^{i-j} = 1_R.$$

Επειδή, εξ υποθέσεως, $a \neq 1_R$, έχουμε $i - j \geq 2$, οπότε το $a^{i-j-1}$ είναι αντίστροφο στοιχείο τού $a$. $\square$

**C.2.9 Πόρισμα.** *Οι ακόλουθες συνθήκες για τον δακτύλιο $\mathbb{Z}_m$, $m \geq 2$, είναι ισοδύναμες:*

(i) *Ο $m$ είναι πρώτος αριθμός.*

(ii) *Ο $\mathbb{Z}_m$ είναι μια ακεραία περιοχή.*

(iii) *Ο $\mathbb{Z}_m$ αποτελεί ένα σώμα.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii): Εάν ο $m$ είναι πρώτος αριθμός, $k \in \mathbb{Z}$ με $m \nmid k$ (ή, ισοδυνάμως, $[k]_m \neq [0]_m$) και εάν υποθέσουμε ότι υφίσταται κάποιος $l \in \mathbb{Z}$, τέτοιος ώστε να ισχύει $[k]_m [l]_m = [0]_m$, τότε

$$\left.\begin{array}{r} [kl]_m = [0]_m \Rightarrow m \mid kl \\ m \nmid k,\ m \text{ πρώτος αριθμός} \end{array}\right\} \underset{\text{B.3.5}}{\Longrightarrow} m \mid l \Longrightarrow [l]_m = [0]_m\,,$$

οπότε ο δακτύλιος $\mathbb{Z}_m$ δεν διαθέτει κανέναν μηδενοδιαιρέτη και είναι, ως εκ τούτου, ακεραία περιοχή.

(ii)⇒(i): Ας υποθέσουμε ότι ο $m$ είναι σύνθετος αριθμός, δηλαδή ότι γράφεται ως γινόμενο $m = kl$ δύο άλλων ακεραίων $k, l$, όπου $1 < k, l < m$. Αυτό θα σήμαινε ότι $[m]_m = [0]_m = [k]_m\, [l]_m$ με $k \neq 0$ και $l \neq 0$, πράγμα που αντίκειται στην (ii).

(ii)⇔(iii): Τούτο έπεται άμεσα από την πρόταση C.2.8. □

**C.2.10 Ορισμός.** Έστω $F$ ένα σώμα. Ας υποθέσουμε ότι υπάρχει (τουλάχιστον) ένας $m \in \mathbb{N}$ με την ιδιότητα

$$(m \cdot 1_F =)\ \underbrace{1_F + \cdots + 1_F}_{m \text{ φορές}} = 0_F.$$

Εάν ο $n \in \mathbb{N}$ είναι ο *ελάχιστος* φυσικός αριθμός με αυτήν την ιδιότητα, τότε ο $n$ λέγεται **χαρακτηριστική** τού $F$. Εάν δεν υπάρχει κανένας $m \in \mathbb{N}$ με την ανωτέρω ιδιότητα, τότε λέμε ότι το $F$ έχει **χαρακτηριστική** $0$. Η χαρακτηριστική ενός σώματος $F$ συμβολίζεται ως $\text{χαρ}(F)$.

**C.2.11 Παρατήρηση.** Εάν ένα σώμα $F$ έχει χαρακτηριστική $\neq 0$, τότε $\text{χαρ}(F) > 1$ (διότι $1_F \neq 0_F$).

**C.2.12 Πρόταση.** *Η χαρακτηριστική ενός σώματος είναι είτε $0$ είτε ένας πρώτος αριθμός.*

ΑΠΟΔΕΙΞΗ. Έστω $F$ τυχόν σώμα. Εάν υποθέσουμε ότι $\text{χαρ}(F) = n \neq 0$, τότε $n \geq 2$, οπότε υφίσταται κάποιος πρώτος διαιρέτης $p$ τού $n$ (βλ. B.3.2). Άρα $\exists k \in \mathbb{N} : n = pk$. Προφανώς, $1 \leq k < n$ και

$$0_F = n \cdot 1_F = \underbrace{1_F + \cdots + 1_F}_{n \text{ φορές}} = (\underbrace{1_F + \cdots + 1_F}_{p \text{ φορές}})(\underbrace{1_F + \cdots + 1_F}_{k \text{ φορές}}) = (p \cdot 1_F)(k \cdot 1_F).$$

Αυτό σημαίνει ότι *είτε* $p \cdot 1_F = 0_F$ *είτε* $k \cdot 1_F = 0_F$. Από τον ορισμό C.2.10 τού $n$ (ως τού *ελαχίστου* φυσικού αριθμού με την ανωτέρω ιδιότητα) έπεται ότι $n = p$ *και* $k = 1$. □

**C.2.13 Παραδείγματα.** (i) $\text{χαρ}(\mathbb{Q}) = \text{χαρ}(\mathbb{R}) = \text{χαρ}(\mathbb{C}) = 0$.

(ii) $\text{χαρ}(\mathbb{Z}_p) = p$ για κάθε πρώτο αριθμό $p$.

**C.2.14 Πρόταση.** *Εάν $F$ είναι ένα σώμα με χαρακτηριστική κάποιον πρώτο αριθμό $p$, τότε*

$$(a+b)^p = a^p + b^p,\ \forall (a,b) \in F \times F. \tag{C.6}$$

ΑΠΟΔΕΙΞΗ. Για οιοδήποτε ζεύγος $(a,b) \in F \times F$ ο διωνυμικός τύπος (C.2) δίδει

$$(a+b)^p = a^p + \sum_{j=1}^{p-1} \binom{p}{j} a^j b^{p-j} + b^p.$$

Επειδή $p \mid \binom{p}{j}$, ήτοι $\exists k_j \in \mathbb{N} : \binom{p}{j} = pk_j$ (βλ. B.4.10), έχουμε

$$\begin{aligned} \binom{p}{j} a^j b^{p-j} &= (pk_j)\, a^j b^{p-j} = ((pk_j) \cdot 1_F)\, a^j b^{p-j} \\ &= (\underbrace{(p \cdot 1_F)}_{=0_F}(k_j \cdot 1_F))a^j b^{p-j} = 0_F \end{aligned} \tag{C.7}$$

για κάθε $j \in \{1, ..., p-1\}$. Άρα η (C.6) προκύπτει από τις ισότητες (C.7). □

**C.2.15 Θεώρημα.** **(Ταξινόμηση πεπερασμένων σωμάτων «μέχρις ισομορφισμού».)**
(i) *Εάν $F$ είναι ένα πεπερασμένο σώμα, τότε ισχύει κατ' ανάγκην* $\mathrm{card}(F) = q$, *όπου* $q = p^\nu$, *$p$ κάποιος πρώτος αριθμός και* $\nu \in \mathbb{N}$.

(ii) *Για κάθε αριθμό $q$ αυτής τής μορφής υφίσταται κάποιο σώμα*[4] *με πληθικό αριθμό $q$.*

(iii) *Δυο σώματα $F_1$ και $F_2$, για τα οποία ισχύει* $\mathrm{card}(F_1) = \mathrm{card}(F_2) = q$, *είναι κατ' ανάγκην ισόμορφα.*

**C.2.16 Σημείωση.** (i) Το μοναδικό (μέχρις ισομορφισμού σωμάτων) σώμα με πληθικό αριθμό $q = p^\nu$ συμβολίζεται συνήθως ως $\mathbb{F}_q$ (ή ως $\mathrm{GF}(q)$).

(ii) Για κάθε πρώτο αριθμό $p$, το σώμα $\mathbb{F}_p$ (και κάθε άλλο σώμα με πληθικό αριθμό $p$) είναι ισόμορφο με το σώμα $\mathbb{Z}_p$.

(iii) Ομαδοθεωρητικές αποδείξεις τού (i) τού θεωρήματος C.2.15 και των (i) και (ii) τού θεωρήματος C.2.17 (που ακολουθεί) δίδονται στα πορίσματα 5.7.6, 9.1.15 και 9.1.35, αντιστοίχως. Οι αποδείξεις των (ii) και (iii) τού θεωρήματος C.2.15, καθώς και των (iii) και (iv) τού θεωρήματος C.2.17, παρουσιάζονται στα μαθήματα «Εφαρμοσμένη Άλγεβρα» και «Θεωρία Σωμάτων».

(iv) Το $\mathbb{F}_q$ (και κάθε άλλο σώμα με πληθικό αριθμό $q = p^\nu$) έχει χαρακτηριστική $p$. Σημειωτέον ότι υπάρχουν και *απειροπληθή* σώματα έχοντα ως χαρακτηριστική τους έναν πρώτο αριθμό $p$, όπως, π.χ., είναι *το σώμα των ρητών συναρτήσεων*

$$\mathbb{Z}_p(\mathsf{X}) := \left\{ \frac{\psi(\mathsf{X})}{\chi(\mathsf{X})} \,\middle|\, \psi(\mathsf{X}) \in \mathbb{Z}_p[\mathsf{X}], \chi(\mathsf{X}) \in \mathbb{Z}_p[\mathsf{X}] \smallsetminus \{0_{\mathbb{Z}_p[\mathsf{X}]}\} \right\}$$

υπεράνω τού σώματος $\mathbb{Z}_p$ (ως προς τις *συνήθεις* πράξεις[5]).

**C.2.17 Θεώρημα.** (i) *Η προσθετική ομάδα* $(\mathbb{F}_q, +), q = p^\nu$, *είναι ισόμορφη τής*

$$\underbrace{\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p}_{\nu \text{ φορές}}.$$

(ii) *Η πολλαπλασιαστική ομάδα* $(\mathbb{F}_q^\times, \cdot)$, $q = p^\nu$, *είναι κυκλική τάξεως* $q - 1$.

[4]Πρόκειται για το «σώμα διασπάσεως» τού πολυωνύμου $\mathsf{X}^q - \mathsf{X}$ υπεράνω τού σώματος $\mathbb{Z}_p$ (όπου $q = p^\nu$), γνωστό και ως **σώμα Galois** τάξεως $q$. Βλ. π.χ. J.J. Rotman: *Θεωρία Galois*, (σε μετάφραση Ν. Μαρμαρίδη), εκδόσεις Leader Books, Αθήνα 2000, θεώρημα 33, σελ. 42, και πόρισμα 53, σελ. 67.

[5] $\frac{\psi_1(\mathsf{X})}{\chi_1(\mathsf{X})} + \frac{\psi_2(\mathsf{X})}{\chi_2(\mathsf{X})} := \frac{\psi_1(\mathsf{X})\chi_2(\mathsf{X}) + \psi_2(\mathsf{X})\chi_1(\mathsf{X})}{\chi_1(\mathsf{X})\chi_2(\mathsf{X})}$, $\frac{\psi_1(\mathsf{X})}{\chi_1(\mathsf{X})} \cdot \frac{\psi_2(\mathsf{X})}{\chi_2(\mathsf{X})} := \frac{\psi_1(\mathsf{X})\psi_2(\mathsf{X})}{\chi_1(\mathsf{X})\chi_2(\mathsf{X})}$.

(iii) *Η ομάδα αυτομορφισμών* $\mathrm{Aut}(\mathbb{F}_q^{\times})$ *τής* $(\mathbb{F}_q^{\times}, \cdot)$, $q = p^{\nu}$, *είναι κυκλική ομάδα τάξεως* $\nu$ *που παράγεται από τον λεγόμενο «αυτομορφισμό τού Frobenius»*:

$$\mathbb{F}_q^{\times} \longrightarrow \mathbb{F}_q^{\times},\ x \longmapsto x^p.$$

(iv) *Το σώμα* $(\mathbb{F}_{q_1}, +, \cdot)$, *όπου* $q_1 = p_1^{\nu_1}$, *αποτελεί υπόσωμα τού* $(\mathbb{F}_{q_2}, +, \cdot)$, *όπου* $q_2 = p_2^{\nu_2}$, *εάν και μόνον εάν* $p_1 = p_2$ *και* $\nu_1 \mid \nu_2$.

► **Πολυώνυμα με συντελεστές ειλημμένους από σώμα**. Έστω $F$ τυχόν σώμα.

**C.2.18 Πρόταση.** *Ο πολυωνυμικός δακτύλιος* $F[\mathsf{X}]$ *είναι ακεραία περιοχή.*

ΑΠΟΔΕΙΞΗ. Εάν $\psi(\mathsf{X}), \chi(\mathsf{X}) \in F[\mathsf{X}] \smallsetminus \{0_{F[\mathsf{X}]}\}$, όπου

$$\psi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in F[\mathsf{X}]\ ,\ a_n \neq 0_F, \quad \chi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j \in F[\mathsf{X}],\ \ b_m \neq 0_F,$$

$(n, m \in \mathbb{N}_0)$, τότε $a_n b_m \neq 0_F$, διότι το $F$ (σύμφωνα με το (i) τής προτάσεως C.2.8) δεν διαθέτει μηδενοδιαιρέτες. Από το (iv) τής προτάσεως C.1.21 λαμβάνουμε

$$\deg(\psi(\mathsf{X})\chi(\mathsf{X})) = \deg(\psi(\mathsf{X})) + \deg(\chi(\mathsf{X})) \in \mathbb{N}_0$$

και, ως εκ τούτου, $\psi(\mathsf{X})\chi(\mathsf{X}) \neq 0_{F[\mathsf{X}]}$. Άρα και ο δακτύλιος $F[\mathsf{X}]$ δεν έχει μηδενοδιαιρέτες. □

Η *ταυτότητα διαιρέσεως* η ισχύουσα στον δακτύλιο $\mathbb{Z}$ των ακεραίων (βλ. B.1.6) γενικεύεται και για τα στοιχεία τής ακεραίας περιοχής $F[\mathsf{X}]$.

**C.2.19 Θεώρημα. (Ταυτότητα διαιρέσεως)** *Δοθέντων δυο πολυωνύμων*

$$\psi(\mathsf{X}) \in F[\mathsf{X}],\ \ \chi(\mathsf{X}) \in F[\mathsf{X}] \smallsetminus \{0_{F[\mathsf{X}]}\},$$

*υπάρχει ένα ζεύγος* ***μονοσημάντως ορισμένων*** *πολυωνύμων* $\varpi(\mathsf{X}), \upsilon(\mathsf{X}) \in F[\mathsf{X}]$, *ούτως ώστε να ισχύει*[6]

$$\boxed{\psi(\mathsf{X}) = \varpi(\mathsf{X})\chi(\mathsf{X}) + \upsilon(\mathsf{X}), \quad \deg(\upsilon(\mathsf{X})) < \deg(\chi(\mathsf{X}))\,.} \tag{C.8}$$

ΑΠΟΔΕΙΞΗ. **Βήμα 1ο**. *Ύπαρξη των* $\varpi(\mathsf{X}), \upsilon(\mathsf{X})$. Εάν $\deg(\psi(\mathsf{X})) < \deg(\chi(\mathsf{X}))$, τότε θέτουμε

$$\varpi(\mathsf{X}) := 0_{F[\mathsf{X}]},\ \ \upsilon(\mathsf{X}) := \psi(\mathsf{X}).$$

Στην περίπτωση όπου $\deg(\psi(\mathsf{X})) =: n \geq m := \deg(\chi(\mathsf{X})) \geq 0$ και

$$\psi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i,\ \chi(\mathsf{X}) = \sum_{j=0}^{m} b_j \mathsf{X}^j\ \ (a_n \neq 0_F, b_m \neq 0_F),$$

χρησιμοποιούμε μαθηματική επαγωγή ως προς τον βαθμό $n$ τού $\psi(\mathsf{X})$. Εάν $n = 0$, τότε $m = 0$ και

$$\psi(\mathsf{X}) = a_0,\ \ \chi(\mathsf{X}) = b_0 \neq 0_F,$$

οπότε αρκεί να θέσουμε $\varpi(\mathsf{X}) := a_0 b_0^{-1}$ και $\upsilon(\mathsf{X}) := 0_{F[\mathsf{X}]}$. Ας υποθέσουμε τώρα ότι $n \geq 1$ και ότι ο ισχυρισμός (που αφορά μόνον στην *ύπαρξη* τού εν λόγω ζεύγους πολυωνύμων) είναι αληθής για κάθε πολυώνυμο ανήκον στον $F[\mathsf{X}]$ και έχον βαθμό $< n$. Το πολυώνυμο

$$\widetilde{\psi}(\mathsf{X}) := \psi(\mathsf{X}) - (a_n b_m^{-1})\mathsf{X}^{n-m}\chi(\mathsf{X}) = \sum_{i=0}^{n-1} a_i \mathsf{X}^i - \sum_{j=0}^{m-1} (a_n b_m^{-1}) b_j \mathsf{X}^{n-m+j} \in F[\mathsf{X}]$$

έχει βαθμό $\leq n-1$. Κατά την επαγωγική μας υπόθεση υπάρχουν πολυώνυμα $\widetilde{\varpi}(\mathsf{X})$, $\widetilde{\upsilon}(\mathsf{X}) \in F[\mathsf{X}]$, ούτως ώστε να ισχύει

$$\widetilde{\psi}(\mathsf{X}) = \widetilde{\varpi}(\mathsf{X})\chi(\mathsf{X}) + \widetilde{\upsilon}(\mathsf{X}), \quad \deg(\widetilde{\upsilon}(\mathsf{X})) < \deg(\chi(\mathsf{X})).$$

Επειδή $\psi(\mathsf{X}) = \left((a_n b_m^{-1})\mathsf{X}^{n-m} + \widetilde{\varpi}(\mathsf{X})\right)\chi(\mathsf{X}) + \widetilde{\upsilon}(\mathsf{X})$, αρκεί να θέσουμε

$$\varpi(\mathsf{X}) := (a_n b_m^{-1})\mathsf{X}^{n-m} + \widetilde{\varpi}(\mathsf{X}), \ \ \upsilon(\mathsf{X}) := \widetilde{\upsilon}(\mathsf{X}).$$

**Βήμα 2ο**. *Μοναδικότητα των* $\varpi(\mathsf{X}), \upsilon(\mathsf{X})$. Έστω ότι η συνθήκη (C.8) ικανοποιείται από δύο ζεύγη πολυωνύμων $\varpi_1(\mathsf{X}), \upsilon_1(\mathsf{X})$ και $\varpi_2(\mathsf{X}), \upsilon_2(\mathsf{X})$:

$$\begin{aligned} \psi(\mathsf{X}) &= \varpi_1(\mathsf{X})\chi(\mathsf{X}) + \upsilon_1(\mathsf{X}), \quad \deg(\upsilon_1(\mathsf{X})) < \deg(\chi(\mathsf{X})), \\ \psi(\mathsf{X}) &= \varpi_2(\mathsf{X})\chi(\mathsf{X}) + \upsilon_2(\mathsf{X}), \quad \deg(\upsilon_2(\mathsf{X})) < \deg(\chi(\mathsf{X})). \end{aligned}$$

Τότε $0_{F[\mathsf{X}]} = \psi(\mathsf{X}) - \psi(\mathsf{X}) = (\varpi_1(\mathsf{X}) - \varpi_2(\mathsf{X}))\chi(\mathsf{X}) + (\upsilon_1(\mathsf{X}) - \upsilon_2(\mathsf{X}))$, οπότε

$$(\varpi_1(\mathsf{X}) - \varpi_2(\mathsf{X}))\chi(\mathsf{X}) = \upsilon_1(\mathsf{X}) - \upsilon_2(\mathsf{X}).$$

Εάν ίσχυε $\varpi_1(\mathsf{X}) \neq \varpi_2(\mathsf{X})$, τότε θα είχαμε

$$\deg(\chi(\mathsf{X})) \leq \deg((\varpi_1(\mathsf{X}) - \varpi_2(\mathsf{X}))\chi(\mathsf{X})) = \deg(\upsilon_1(\mathsf{X}) - \upsilon_2(\mathsf{X})) < \deg(\chi(\mathsf{X})).$$

Άτοπο! Συνεπώς, $\varpi_1(\mathsf{X}) = \varpi_2(\mathsf{X})$ και, ως εκ τούτου, $\upsilon_1(\mathsf{X}) = \upsilon_2(\mathsf{X})$. □

**C.2.20 Ορισμός.** Το πολυώνυμο $\varpi(\mathsf{X})$ στην (C.8) ονομάζεται **πηλίκο** και το $\upsilon(\mathsf{X})$ **υπόλοιπο** τής διαιρέσεως τού $\psi(\mathsf{X})$ διά τού $\chi(\mathsf{X})$. Όταν $\upsilon(\mathsf{X}) = 0_{F[\mathsf{X}]}$, λέμε ότι το $\chi(\mathsf{X})$ **διαιρεί** (επακριβώς) το $\psi(\mathsf{X})$ ή ότι το $\chi(\mathsf{X})$ είναι **διαιρέτης** τού $\psi(\mathsf{X})$ ή ότι το $\psi(\mathsf{X})$ είναι (πολυωνυμικό) **πολλαπλάσιο** τού $\chi(\mathsf{X})$. (Εν τοιαύτη περιπτώσει χρησιμοποιείται ο συμβολισμός: $\chi(\mathsf{X}) \mid \psi(\mathsf{X})$).

**C.2.21 Παρατήρηση.** Εάν $\chi(\mathsf{X}) \mid \psi(\mathsf{X})$ και $\psi(\mathsf{X}) \neq 0_{F[\mathsf{X}]}$, τότε προφανώς $\deg(\chi(\mathsf{X})) \leq \deg(\psi(\mathsf{X}))$.

**C.2.22 Ορισμός.** Για οιοδήποτε στοιχείο $\lambda \in F$ ορίζεται η **συνάρτηση** $\mathfrak{y}_\lambda$ **πολυωνυμικής αποτιμήσεως στο** $\lambda$ ως εξής:

$$F[\mathsf{X}] \ni \sum_{i=0}^{n} a_i \mathsf{X}^i = \psi(\mathsf{X}) \xmapsto{\mathfrak{y}_\lambda} \mathfrak{y}_\lambda(\psi(\mathsf{X})) := \psi(\lambda) := \sum_{i=0}^{n} a_i \lambda^i \in F.$$

**C.2.23 Σημείωση.** Στο σχολείο είθισται να αντιμετωπίζουμε τα πολυώνυμα ως συνήθεις «συναρτήσεις» (επειδή εκεί γίνεται κυρίως χρήση των σωμάτων $\mathbb{Q}$ και $\mathbb{R}$). Ωστόσο, όταν κανείς θεωρεί *τυχόντα* σώματα $F$, πρέπει να γνωρίζει ότι κάτι τέτοιο *δεν* αληθεύει εν γένει. Εάν

$$\psi(\mathsf{X}) = \sum_{i=0}^{n} a_i \mathsf{X}^i \in F[\mathsf{X}],$$

τότε η **συνάρτηση η επαγομένη από το** $\psi(\mathsf{X})$ είναι η

$$\mathfrak{v}_{\psi(\mathsf{X})} : F \longrightarrow F, \quad \lambda \longmapsto \mathfrak{v}_{\psi(\mathsf{X})}(\lambda) := \mathfrak{y}_\lambda(\psi(\mathsf{X})) = \psi(\lambda) = \sum_{i=0}^{n} a_i \lambda^i.$$

Μέσω αυτής ορίζεται ο ομομορφισμός δακτυλίων

$$F[\mathsf{X}] \longrightarrow F^F, \quad \psi(\mathsf{X}) \longmapsto \mathfrak{v}_{\psi(\mathsf{X})},$$

που δεν είναι κατ' ανάγκην μονομορφισμός δακτυλίων! Επί παραδείγματι, εάν $F = \mathbb{Z}_3$ και $\psi(\mathsf{X}) = \mathsf{X} + \mathsf{X}^3$, $\chi(\mathsf{X}) = [2]_3\, \mathsf{X}$, τότε τα $\psi(\mathsf{X})$ και $\chi(\mathsf{X})$ -ως πολυώνυμα- είναι διαφορετικά, ενώ

$$\begin{aligned}
\mathfrak{v}_{\psi(\mathsf{X})}([0]_3) &= [0]_3 = \mathfrak{v}_{\chi(\mathsf{X})}([0]_3),\\
\mathfrak{v}_{\psi(\mathsf{X})}([1]_3) &= [2]_3 = \mathfrak{v}_{\chi(\mathsf{X})}([1]_3),\\
\mathfrak{v}_{\psi(\mathsf{X})}([2]_3) &= [1]_3 = \mathfrak{v}_{\chi(\mathsf{X})}([2]_3),
\end{aligned}$$

πράγμα που σημαίνει ότι $\mathfrak{v}_{\psi(\mathsf{X})} = \mathfrak{v}_{\chi(\mathsf{X})}$. (Μια ικανή συνθήκη για να είναι ο ως άνω ομομορφισμός δακτυλίων *μονομορφισμός* δίδεται στο πόρισμα C.2.29.)

**C.2.24 Ορισμός.** Έστω $F$ ένα σώμα και έστω $\psi(\mathsf{X}) \in F[\mathsf{X}]$. Ένα στοιχείο $\lambda \in F$ ονομάζεται **θέση μηδενισμού**[7] (ή **σημείο μηδενισμού**) τού πολυωνύμου $\psi(\mathsf{X})$ όταν $\mathfrak{y}_\lambda(\psi(\mathsf{X}))) := \psi(\lambda) = 0_F$, δηλαδή όταν η τιμή τού $\psi(\mathsf{X})$ για $\mathsf{X} = \lambda$ είναι το μηδενικό στοιχείο.

**C.2.25 Πρόταση.** *Εάν $\lambda \in F$ και $\psi(\mathsf{X}) \in F[\mathsf{X}]$, τότε ισχύουν τα εξής:*

(i) *Το υπόλοιπο τής διαιρέσεως τού $\psi(\mathsf{X})$ διά τού $\mathsf{X} - \lambda$ ισούται με το $\psi(\lambda)$.*

(ii) *Το $\lambda$ είναι μια θέση μηδενισμού τού $\psi(\mathsf{X})$ εντός τού $F$ εάν και μόνον εάν*

$$\mathsf{X} - \lambda \mid \psi(\mathsf{X}).$$

ΑΠΟΔΕΙΞΗ. (i) Σύμφωνα με το θεώρημα C.2.19 υπάρχουν μονοσημάντως ορισμένα πολυώνυμα $\varpi(\mathsf{X})$ και $\upsilon(\mathsf{X}) \in F[\mathsf{X}]$, τέτοια ώστε να ισχύει

$$\psi(\mathsf{X}) = (\mathsf{X} - \lambda)\varpi(\mathsf{X}) + \upsilon(\mathsf{X}), \ \ \deg(\upsilon(\mathsf{X})) < \deg(\mathsf{X} - \lambda) = 1.$$

[7]Εδώ, χρησιμοποιούμε τον όρο *θέση μηδενισμού* ακολουθώντας τή γερμανική ορολογία, η οποία, εν προκειμένω, είναι περισσότερο ακριβής απ' ό,τι η αγγλική· ο διαχωρισμός τού όρου Nullstelle από τον όρο Wurzel (αγγλ. *root*, ελλ. *ρίζα*) είναι επιβεβλημένη, καθότι ένα μιγαδικό πολυώνυμο $\psi(\mathsf{X}) \in \mathbb{C}[\mathsf{X}]$ μπορεί να μηδενίζεται όταν $\mathsf{X} = \lambda \in \mathbb{C}$, χωρίς, ωστόσο, το $\lambda$ να προκύπτει από επίλυση τής εξισώσεως $\psi(\mathsf{X}) = 0$ μέσω αποκλειστικής χρήσεως *ριζικών*. (Από την άλλη όμως μεριά, ονομάζουμε, π.χ., τις θέσεις μηδενισμού τής εξισώσεως $\mathsf{X}^\nu = 1$ $\nu$-οστές *ρίζες τής μονάδας*.)

Επομένως, $\upsilon(\mathsf{X}) = a \in F$, οπότε

$$a = \psi(\mathsf{X}) - (\mathsf{X} - \lambda)\varpi(\mathsf{X}) \Longrightarrow a = \psi(\lambda).$$

(ii) Το $\lambda$ είναι μια θέση μηδενισμού τού $\psi(\mathsf{X})$ (εντός τού $F$) εάν και μόνον εάν το υπόλοιπο τής διαιρέσεως τού $\psi(\mathsf{X})$ διά τού $\mathsf{X} - \lambda$ είναι το $0_{F[\mathsf{X}]}$, πράγμα που σημαίνει ότι $\mathsf{X} - \lambda \mid \psi(\mathsf{X})$. □

**C.2.26 Πόρισμα.** *Εάν τα στοιχεία* $\lambda_1,\ldots,\lambda_k \in F$ $(k \in \mathbb{N})$ *είναι* $k$ *σαφώς διακεκριμένες θέσεις μηδενισμού ενός πολυωνύμου* $\psi\,(\mathsf{X}) \in F[\mathsf{X}]$, *τότε*

$$(\mathsf{X} - \lambda_1)\,(\mathsf{X} - \lambda_2)\cdots(\mathsf{X} - \lambda_k) \mid \psi(\mathsf{X}).$$

ΑΠΟΔΕΙΞΗ. Όταν $k = 1$, αυτό είναι αληθές λόγω τής προτάσεως C.2.25. Θα εργασθούμε με τη βοήθεια τής μαθηματικής επαγωγής. Υποθέτουμε ότι ο ισχυρισμός είναι αληθής για $k - 1$ θέσεις μηδενισμού, οπότε

$$\psi(\mathsf{X}) = (\mathsf{X} - \lambda_1)\,(\mathsf{X} - \lambda_2)\cdots(\mathsf{X} - \lambda_{k-1})\,\chi(\mathsf{X})$$

για κάποιο $\chi(\mathsf{X}) \in F[\mathsf{X}]$. Κατόπιν αποτιμήσεως των δύο μελών τής ανωτέρω ισότητας για $\mathsf{X} = \lambda_k$ λαμβάνουμε

$$0_F = \psi(\lambda_k) = (\lambda_k - \lambda_1)\,(\lambda_k - \lambda_2)\cdots(\lambda_k - \lambda_{k-1})\,\chi(\lambda_k),$$

απ' όπου προκύπτει ότι $\chi(\lambda_k) = 0_F$ (λόγω τής αρχικής υποθέσεώς μας). Άρα το $\mathsf{X} - \lambda_k$ διαιρεί το πολυώνυμο $\chi(\mathsf{X})$, οπότε ο ισχυρισμός είναι εμφανώς αληθής και για $k$ θέσεις μηδενισμού. □

**C.2.27 Πόρισμα.** *Κάθε πολυώνυμο* $\psi\,(\mathsf{X}) \in F[\mathsf{X}] \smallsetminus \{0_{F[\mathsf{X}]}\}$ *διαθέτει (συνολικώς) το πολύ* $\deg(\psi(\mathsf{X}))$ *θέσεις μηδενισμού εντός τού* $F$.

ΑΠΟΔΕΙΞΗ. Έπεται από το πόρισμα C.2.26 και την παρατήρηση C.2.21. □

**C.2.28 Πόρισμα.** *Εάν ένα πολυώνυμο* $\psi(\mathsf{X}) \in F[\mathsf{X}]$ *διαθέτει εντός τού* $F$ *θέσεις μηδενισμού, το πλήθος των οποίων υπερβαίνει τον βαθμό του, τότε το* $\psi(\mathsf{X})$ *είναι το μηδενικό πολυώνυμο.*

**C.2.29 Πόρισμα.** *Εάν το (υποκείμενο σύνολο ενός σώματος)* $F$ *είναι απειροσύνολο, τότε η*

$$F\,[\mathsf{X}] \longrightarrow F^F, \quad \psi(\mathsf{X}) \longmapsto \mathfrak{v}_{\psi(\mathsf{X})},$$

*(βλ.* C.2.23) *αποτελεί έναν μονομορφισμό δακτυλίων.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε τυχόντα πολυώνυμα $\psi(\mathsf{X}), \chi(\mathsf{X}) \in F[\mathsf{X}]$ και τις αντίστοιχες συναρτήσεις $\mathfrak{v}_{\psi(\mathsf{X})}$ και $\mathfrak{v}_{\chi(\mathsf{X})}$. Εάν ισχύει $\mathfrak{v}_{\psi(\mathsf{X})} = \mathfrak{v}_{\chi(\mathsf{X})}$, τότε η διαφορά $\psi(\mathsf{X}) - \chi(\mathsf{X})$ έχει ως θέσεις μηδενισμού της όλα τα στοιχεία τού (υποκειμένου συνόλου τού) $F$. Συνεπώς, δυνάμει τού πορίσματος C.2.28 έχουμε $\psi(\mathsf{X}) - \chi(\mathsf{X}) = 0_{F[\mathsf{X}]}$, ήτοι $\psi(\mathsf{X}) = \chi(\mathsf{X})$. □