Δακτύλιοι και Πρότυπα

Σημειώσεις Παραδόσεων-Χειμερινά εξάμηνα 2018-19 και 2019-20

Κ. Γκότσης

Οι Σημειώσεις αυτές υπόκειται σε διαρκή αναθεώρηση. Πιστεύω ότι κάποια στιγμή θα καταστεί δυνατόν να αποτελέσουν ένα ικανοποιητικό βοήθημα για τους φοιτητές που παρακολουθούν το συγκεκριμένο μάθημα.

Περιεχόμενα

Κεφάλαιο 1

Βασικές Έννοιες στους Δακτυλίους

1.1 Δακτύλιοι-Ιδεώδη

ΟΡΙΣΜΟΣ 1.1. Ένα μη κενό σύνολο R εφοδιασμένο με δύο πράξεις $+ : R\times R \to R$ (πρόσθεση) και $\cdot : R \times R \to R$ (πολλαπλασιασμός) λέγεται **δακτύλιος** αν ισχύουν τα παρακάτω:

1) Το ζεύγος $(R,+)$ είναι αβελιανή ομάδα, δηλαδή ισχύουν τα ακόλουθα:

(i) $\alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma$, για κάθε $\alpha,\beta,\gamma\in R$.

(ii) Υπάρχει (αποδεικνύεται μοναδικό) στοιχείο 0 ή για έμφαση (όταν έχουμε διαφορετικούς δακτυλίους) με 0_R τέτοιο, ώστε $\alpha+0=0+\alpha=\alpha$, για κάθε $\alpha\in R$.

(iii) Για κάθε $\alpha\in R$ υπάρχει (αποδεικνύεται μοναδικό) στοιχείο $-\alpha\in R$ με την ιδιότητα $\alpha+(-\alpha)=(-\alpha)+\alpha=0$.

(iv) $\alpha+\beta=\beta+\alpha$, για κάθε $\alpha,\beta\in R$.

Σχόλιο: Από την ιδιότητα (iv) προκύπτει ότι οι ισότητες $\alpha+0=0+\alpha$ και $\alpha+(-\alpha)=(-\alpha)+\alpha$ στις ιδιότητες (ii) και (iii) είναι περιττές.

2) Το ζεύγος $(R,\cdot)$ είναι ημιομάδα, δηλαδή $\alpha(\beta\gamma)=(\alpha\beta)\gamma$, για κάθε $\alpha,\beta,\gamma\in R$. (Το σύμβολο $\cdot$ του πολλαπλασιασμού συνήθως παραλείπεται).

3) Ισχύουν οι επιμεριστικές ιδιότητες: $\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma$ και $(\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma$, για κάθε $\alpha,\beta,\gamma\in R$.

Για να θυμηθούμε κάποια πράγματα, ας αποδείξουμε πρώτα ότι το μηδενικό στοιχείο είναι μοναδικό. Πράγματι, αν $\tilde{0}$ είναι ένα άλλο μηδενικό στοιχείο, τότε $0+\tilde{0}=\tilde{0}$, γιατί το 0 είναι μηδενικό στοιχείο της πρόσθεσης. Αλλά πάλι $0+\tilde{0}=0$, γιατί το $\tilde{0}$ είναι και αυτό μηδενικό στοιχείο της πρόσθεσης. Τελικώς $\tilde{0}=0+\tilde{0}=0$.
Αν τώρα $\tilde{\alpha}$ είναι ένα άλλο αντίθετο στοιχείο του α, τότε $\tilde{\alpha}=\tilde{\alpha}+0=\tilde{\alpha}+(\alpha+(-\alpha))=$ $=(\tilde{\alpha}+\alpha)+(-\alpha)=0+(-\alpha)=-\alpha$.
Κατά τα γνωστά θέτουμε $\alpha-\beta=\alpha+(-\beta)$. Από τον ορισμό του αντιθέτου προκύπτει επίσης ότι $-(-\alpha)=\alpha$.
Επίσης, $0\cdot\alpha=(0+0)\cdot\alpha=0\cdot\alpha+0\cdot\alpha$. Επομένως $0=0\cdot\alpha+(-(0\cdot\alpha))=(0\cdot\alpha+0\cdot\alpha)+(-(0\cdot\alpha))=$ $=0\cdot\alpha+(0\cdot\alpha+(-(0\cdot\alpha)))=0\cdot\alpha+0=0\cdot\alpha$. Παρόμοια, $\alpha\cdot 0=0$.
Επίσης, $\alpha\beta+(-\alpha)\beta=(\alpha+(-\alpha))\beta=0\cdot\beta=0$. Άρα $(-\alpha)\beta=-\alpha\beta$. Ομοίως $\alpha(-\beta)=-\alpha\beta$.
Ακόμα, αν $\alpha_1,\alpha_2,\ldots,\alpha_k\in R$, τότε $-(\alpha_1+\alpha_2+\cdots+\alpha_k)=(-\alpha_1)+(-\alpha_2)+\cdots+(-\alpha_k)=$ $=-\alpha_1-\alpha_2-\cdots-\alpha_k$. Πράγματι, $\alpha_1+\alpha_2+\cdots+\alpha_k+((-\alpha_1)+(-\alpha_2)+\cdots+(-\alpha_k))=$ $=(\alpha_1+(-\alpha_1))+(\alpha_2+(-\alpha_2))+\cdots+(\alpha_k+(-\alpha_k))=0_R+0_R+\cdots+0_R=0_R$.

ΟΡΙΣΜΟΣ 1.2. (i) Ένας δακτύλιος R λέγεται **μεταθετικός** αν και μόνον αν $\alpha\beta=\beta\alpha$, για κάθε $\alpha,\beta\in R$.

(ii) Ένας δακτύλιος R λέγεται **μοναδιαίος ή δακτύλιος με μονάδα** αν και μόνον αν υπάρχει στοιχείο 1 (ή 1_R για έμφαση) με την ιδιότητα $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$, για κάθε $\alpha \in R$.

ΠΑΡΑΔΕΙΓΜΑ 1.3. (i) Το σύνολο των τετραγωνικών $n \times n$ πινάκων $\mathbb{F}^{n\times n}$ με στοιχεία από ένα σώμα $\mathbb{F}$ και πράξεις τη συνήθη πρόσθεση και πολλαπλασιασμό πινάκων είναι μοναδιαίος δακτύλιος. Αυτός δεν είναι μεταθετικός εν γένει. Για παράδειγμα, στο $\mathbb{Q}^{2\times 2}$ έχουμε

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \neq \begin{pmatrix} 0 & -2 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

(ii) Ο τετριμμένος ή μηδενικός δακτύλιος $\{0\}$ είναι μεταθετικός δακτύλιος με μονάδα. Εδώ έχουμε $0 = 1$. Στα επόμενα θα ασχοληθούμε με μη τετριμμένους δακτυλίους, εκτός εάν άλλως τονίζεται.
(iii) Ο γνωστός μας δακτύλιος $\mathbb{Z}_n$ των ακεραίων modulo n, όπου n θετικός ακέραιος είναι μεταθετικός δακτύλιος με μονάδα. Παρατηρείστε ότι αν $n = 1$, τότε ο $\mathbb{Z}_1$ είναι ο τετριμμένος δακτύλιος.
(iv) Κάθε σώμα είναι (μη τετριμμένος) μεταθετικός δακτύλιος με μονάδα. Ιδιαιτέρως τα γνωστά σώματα $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ είναι μοναδιαίοι μεταθετικοί δακτύλιοι. Αλλά και ο δακτύλιος $\mathbb{Q}[\sqrt{p}] = \{\alpha + \beta\sqrt{p} \mid \alpha, \beta \in \mathbb{Q}\}$, όπου p πρώτος είναι σώμα (γιατί;) και άρα μεταθετικός μοναδιαίος δακτύλιος. Αλλά και ο δακτύλιος $\mathbb{Z}_p$, όπου p πρώτος είναι σώμα.
(v) Ο πολυωνυμικός δακτύλιος $R[x] = \{f(x) = \sum_{i=0}^{n} \alpha_i x^i \mid n \geq 0 \text{ και } \alpha_i \in R, \text{ για κάθε } i = 0, 1, \ldots, n\}$ των πολυωνύμων με συντελεστές από έναν μεταθετικό δακτύλιο R είναι μεταθετικός δακτύλιος. Αν ο R είναι μοναδιαίος, τότε και ο $R[x]$ είναι μοναδιαίος. Ιδιαιτέρως επισημαίνουμε τους δακτυλίους $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$, αλλά και τους δακτυλίους $\mathbb{Z}_n[x]$ κτλ.
(vi) Το σύνολο $2\mathbb{Z}$ των αρτίων ακεραίων είναι μεταθετικός δακτύλιος, αλλά όχι μοναδιαίος. (Γιατί;) Στα επόμενα θα δούμε ότι τέτοιες κατασκευές είναι τα λεγόμενα **ιδεώδη** ενός δακτυλίου.

ΟΡΙΣΜΟΣ 1.4. Σε έναν (μη τετριμμένο) μοναδιαίο δακτύλιο R ένα μη μηδενικό στοιχείο u λέγεται **αντιστρέψιμο** αν και μόνον αν υπάρχει $v \in R$ τέτοιο, ώστε $uv = vu = 1$.

Το αντίστροφο v ενός αντιστρεψίμου στοιχείου είναι **μοναδικό**. Αυτό θα συμβολίζεται με u^{-1}. Πράγματι, έστω $v, v' \in R$ με $uv = vu = 1 = uv' = v'u$. Τότε $v' = v' \cdot 1 = v'(uv) = (v'u)v = = 1 \cdot v = v$.

Το σύνολο των αντιστρεψίμων στοιχείων του R συμβολίζεται με $U(R)$. Είναι σαφές ότι το $U(R)$ αποτελεί ομάδα με πράξη τον πολλαπλασιασμό στο R.

Από τώρα και στο εξής θα αναφερόμαστε σε μεταθετικούς δακτυλίους με μονάδα. Επίσης, όλοι οι δακτύλιοι θεωρούνται μη τετριμμένοι. ($1 \neq 0$).

ΟΡΙΣΜΟΣ 1.5. Έστω $\varnothing \neq I \subseteq R$. Το I λέγεται **ιδεώδες** του δακτυλίου R αν ισχύουν τα ακόλουθα:
(i) Το $(I, +)$ είναι υποομάδα της (αβελιανής) προσθετικής ομάδας $(R, +)$, δηλαδή $0_R \in I$, $x+y \in \in I$, για κάθε $x, y \in I$ και $-x \in I$, για κάθε $x \in I$.
(ii) $rx \in I$, για κάθε $x \in I$ και $r \in R$.
Συμβολισμός: $I \trianglelefteq R$.

Προφανώς το μονοσύνολο $\{0\}$ και ολόκληρος ο δακτύλιος R είναι ιδεώδη του R. Αν το ιδεώδες I του R είναι γνήσιο υποσύνολο του R, τότε αυτό λέγεται **γνήσιο ιδεώδες** (του R).
Συμβολισμός: $I \lhd R$.

ΠΡΟΣΟΧΗ! Ο παραπάνω ορισμός ισχύει **μόνον για μεταθετικούς δακτυλίους**. Σε μη μεταθετικό δακτύλιο μπορεί κανείς να θεωρήσει **αριστερά ή δεξιά ή αμφίπλευρα ιδεώδη**, ανάλογα αν ισχύει η σχέση $rx \in I$, $xr \in I$ και $rx, xr \in I$, για κάθε $x \in I$ και $r \in R$.

ΠΡΟΤΑΣΗ 1.6. **(Εναλλακτικός ορισμός ιδεώδους)** Ένα μη κενό υποσύνολο I ενός μοναδιαίου μεταθετικού δακτυλίου R είναι ιδεώδες αυτού αν και μόνον αν ισχύουν τα εξής:
(i) $x + y \in I$, για κάθε $x, y \in I$ και **(ii)** $rx \in I$, για κάθε $x \in I$ και για κάθε $r \in R$.
ΑΠΟΔΕΙΞΗ: Θα πρέπει να αποδείξουμε είναι ότι το I είναι προσθετική υποομάδα του R.
Παρατηρούμε ότι για κάθε $x \in I$ ισχύει $(-1_R) \cdot x \in I$. Αλλά $(-1_R) \cdot x = -(1_R \cdot x) = -x$. Επίσης, αν $x \in I$, τότε $0_R = x + (-x) \in I$. Άρα το I είναι προσθετική υποομάδα του R και τελειώσαμε. ■

Την παραπάνω μορφή θα χρησιμοποιούμε για να ελέγχουμε αν ένα μη κενό υποσύνολο I του R είναι ιδεώδες αυτού.

ΛΗΜΜΑ 1.7. Η τομή $\bigcap_{\lambda\in\Lambda} I_\lambda$ μιας οικογένειας ιδεωδών του R είναι επίσης ιδεώδες αυτού.
ΑΠΟΔΕΙΞΗ: Έστω $J = \bigcap_{\lambda\in\Lambda} I_\lambda$. Τότε $0_R \in I_\lambda$, για κάθε $\lambda \in \Lambda$. Άρα $0_R \in \bigcap_{\lambda\in\Lambda} I_\lambda = J$. Αν τώρα $x, y \in J$, τότε $x, y \in I_\lambda$, για κάθε $\lambda \in \Lambda$. Άρα $x + y \in I_\lambda$, για κάθε $\lambda \in \Lambda$ και συνεπώς $x + y \in \bigcap_{\lambda\in\Lambda} I_\lambda = J$. Επίσης, αν $r \in R$ και $x \in J$, τότε $x \in I_\lambda$, για κάθε $\lambda \in \Lambda$ και κατά συνέπεια $rx \in I_\lambda$, για κάθε $\lambda \in \Lambda$. Από αυτό προκύπτει ότι $rx \in \bigcap_{\lambda\in\Lambda} I_\lambda = J$. ■

ΠΡΟΤΑΣΗ 1.8. Έστω $X \subseteq R$. Τότε υπάρχει **μοναδικό ελάχιστο ιδεώδες**, το οποίο συμβολίζουμε με (X) και **το οποίο περιέχει το X**.
(i) Αν $X = \varnothing$, τότε το ελάχιστο ιδεώδες που περιέχει το κενό σύνολο είναι το **τετριμμένο** $\{0\}$.
(ii) Αν $X \neq \varnothing$, τότε το (X) αποτελείται από όλους τους πεπερασμένους γραμμικούς συνδυασμούς της μορφής $\sum_{i=1}^{n} r_i x_i$, όπου $n \geq 1$, $r_i \in R$ και $x_i \in X$, για κάθε $i = 1, \ldots, n$.
ΑΠΟΔΕΙΞΗ: Έστω $\{I_\lambda\}_{\lambda\in\Lambda}$ η οικογένεια των ιδεωδών του R που περιέχει το X. Το R ανήκει στην οικογένεια αυτή, άρα η οικογένεια αυτή δεν είναι κενή. Είναι σαφές ότι, με βάση και το προηγούμενο λήμμα, το ιδεώδες $J = \bigcap_{\lambda\in\Lambda} I_\lambda$ είναι το ελάχιστο ιδεώδες που περιέχει το X.
(i) Είναι τετριμμένο, γιατί $\varnothing \subsetneq \{0_R\} \subseteq I_\lambda$, για κάθε $\lambda \in \Lambda$ και το $\{0_R\}$ είναι ιδεώδες του R.
(ii) Προφανώς κάθε γραμμικός συνδυασμός της μορφής $\sum_{i=1}^{n} r_i x_i$, όπου $r_i \in R$ και $x_i \in X$ ανήκει σε κάθε ιδεώδες που περιέχει το X, άρα και στο (X). Αρκεί να δείξουμε ότι το σύνολο A των γραμμικών αυτών συνδυασμών αποτελεί ιδεώδες, το οποίο περιέχει το X.
Έστω $x = \sum_{i=1}^{m} r_i x_i, y = \sum_{j=1}^{n} s_j y_j \in A$ είναι δύο τέτοιοι γραμμικοί συνδυασμοί, $\big(r_i, s_j \in R$ και $x_i, y_j \in X\big)$. Τότε το άθροισμα $x + y = \sum_{i=1}^{m} r_i x_i + \sum_{j=1}^{n} s_j y_j$ είναι ένας τέτοιος γραμμικός συνδυασμός. $\big($Αν για παράδειγμα $x_i = y_j$, για κάποια i, j, τότε $r_i x_i + s_j y_j = (r_i + s_j) x_i\big)$.
Αν $x = \sum_{i=1}^{n} r_i x_i$ είναι ένας τέτοιος γραμμικός συνδυσμός και $r \in R$, τότε $rx = \sum_{i=1}^{n} (r r_i) x_i$. Επομένως $A \trianglelefteq R$ και $A \subseteq (X)$.
Ακόμη, για κάθε $x \in X$ ισχύει $x = 1_R \cdot x$, γραμμικός συδυασμός με έναν όρο. Άρα $X \subseteq A$ και κατά συνέπεια $(X) \subseteq A$. Τελικώς $A = (X)$. ■

ΟΡΙΣΜΟΣ 1.9. Έστω $X = \{x\}$ $\big($μονοσύνολο$\big)$. Τότε το ιδεώδες που παράγεται από το $\{x\}$ λέγεται **κύριο ιδεώδες** και συμβολίζεται με (x). Είναι σαφές ότι $(x) = \{rx \mid r \in R\}$, γι' αυτό

και γράφεται και ως Rx. Γενικότερα, αν $X = \{x_1, x_2, \ldots, x_n\}$, τότε το ιδεώδες που παράγεται από το X συμβολίζεται με $(x_1, x_2, \ldots, x_n)$ ή ισοδύναμα με $Rx_1 + Rx_2 + \cdots + Rx_n$.

ΠΡΟΤΑΣΗ 1.10. Έστω $I_1, I_2, \ldots, I_k$ ιδεώδη του R.
Το **άθροισμα** $I_1 + I_2 + \cdots + I_k = \{x_1 + x_2 + \cdots + x_k \mid x_i \in I_i, \text{ για κάθε } i = 1, 2, \ldots, k\}$ είναι ιδεώδες του R. Αυτό είναι το ιδεώδες που παράγεται από την ένωση $X = I_1 \cup I_2 \cup \cdots \cup I_k$.
ΑΠΟΔΕΙΞΗ: Έστω $x_i, x_i' \in I_i$, για κάθε $i = 1, 2, \ldots, k$. Τότε $(x_1 + x_2 + \cdots + x_k) + (x_1' + x_2' + \cdots + x_k') = (x_1 + x_1') + (x_2 + x_2') + \cdots + (x_k + x_k') \in I_1 + I_2 + \cdots + I_k$, γιατί $x_i + x_i' \in I_i$, για κάθε $i = 1, 2, \ldots, k$.
Επίσης, αν $r \in R$ και $x_i \in I_i$, για κάθε $i = 1, 2, \ldots, k$, τότε $r \cdot (x_1 + x_2 + \cdots + x_k) = = rx_1 + rx_2 + \cdots + rx_k \in I_1 + I_2 + \cdots + I_k$, γιατί $rx_i \in I_i$, για κάθε $i = 1, 2, \ldots, k$.
Επομένως το $I_1 + I_2 + \cdots + I_k$ είναι ιδεώδες το οποίο προφανώς περιέχεται στο ιδεώδες που παράγεται από το $I_1 \cup I_2 \cup \cdots \cup I_k$. $\big($Τα στοιχεία του είναι αθροίσματα στοιχείων του $I_1 \cup I_2 \cup \cdots \cup I_k\big)$. Δηλαδή $I_1 + I_2 + \cdots + I_k \subseteq (I_1 \cup I_2 \cup \cdots \cup I_k)$.
Αντιστρόφως, αν $x \in I_i$, για κάποιο $i \in \{1, 2, \ldots, k\}$, τότε $x = \underset{\cap\, I_1}{0_R} + \underset{\cap\, I_2}{0_R} + \cdots + \underset{\cap\, I_i}{x} + \cdots + \underset{\cap\, I_k}{0_R} \in$
$\in I_1 + I_2 + \cdots + I_k$ και κατά συνέπεια $I_i \subseteq I_1 + I_2 + \cdots + I_k$, για κάθε $i = 1, 2, \ldots, k$. Άρα $I_1 \cup I_2 \cup \cdots \cup I_k \subseteq I_1 + I_2 + \cdots + I_k$ και συνεπώς $(I_1 \cup I_2 \cup \cdots \cup I_k) \subseteq I_1 + I_2 + \cdots + I_k$. ■

ΟΡΙΣΜΟΣ 1.11. Έστω $I_1, I_2, \ldots, I_k$ ιδεώδη του R. Το ιδεώδες-γινόμενο $I_1 I_2 \cdots I_k$ είναι το ιδεώδες που παράγεται από το σύνολο $X = \{x_1 x_2 \cdots x_k \mid x_i \in I_i, \text{ για κάθε } i = 1, 2, \ldots, k\}$.
Αν $I_1 = I_2 = \cdots = I_k = I$ γράφουμε I^k αντί $\underbrace{I \cdot I \cdots I}_{k \text{ φορές}}$.

ΠΡΟΤΑΣΗ 1.12. $I_1 I_2 \cdots I_k \subseteq I_1 \cap I_2 \cap \cdots \cap I_k$.
ΑΠΟΔΕΙΞΗ: Αρκεί να δείξουμε ότι το σύνολο X, όπως ορίστηκε στον προηγούμενο ορισμό περιέχεται στο $I_1 \cap I_2 \cap \cdots \cap I_k$. Έστω $x_1 x_2 \cdots x_k \in X$ $\big($δηλαδή $x_i \in I_i\big)$. Τότε $x_1 x_2 \cdots x_k = = (x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k) x_i \in I_i$, ως πολλαπλάσιο στοιχείου του I_i. Επειδή το i ήταν τυχόν, $x_1 x_2 \cdots x_k \in I_1 \cap I_2 \cap \cdots \cap I_k$. ■

1.2 Ακέραιες Περιοχές-Σώματα

ΟΡΙΣΜΟΣ 1.13. Έστω R μεταθετικός δακτύλιος με μονάδα. Ο R λέγεται **ακέραια περιοχή** (integral domain) ή απλά **περιοχή** (domain) αν και μόνον αν από κάθε σχέση της μορφής $\alpha\beta = 0$ προκύπτει ότι $\alpha = 0$ ή $\beta = 0$.
Ένας μεταθετικός δακτύλιος με μονάδα F λέγεται **σώμα** αν και μόνον αν κάθε μη μηδενικό στοιχείο είναι αντιστρέψιμο. Είναι δηλαδή $U(F) = F \setminus \{0\}$.

Είναι σαφές ότι κάθε σώμα είναι ακέραια περιοχή. Γιατί αν $xy = 0 \in F$, όπου F σώμα και $x \neq 0$, τότε το x είναι αντιστρέψιμο. Επομένως $xy = 0 \Rightarrow x^{-1}xy = 0 \Leftrightarrow 1 \cdot y = 0 \Leftrightarrow y = 0$.
Ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι ακέραια περιοχή. Αλλά δεν είναι σώμα. $\big($Π.χ. $2^{-1} \notin \mathbb{Z}\big)$.
Ακόμη, ο δακτύλιος $\mathbb{Z}_n$ είναι ακέραια περιοχή αν και μόνον αν ο n είναι πρώτος. Στην τελευταία περίπτωση ο $\mathbb{Z}_n$ είναι σώμα, όπως δείχνει και η επόμενη πρόταση.

ΠΡΟΤΑΣΗ 1.14. **(i)** Κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.
(ii) Αν ο R είναι ακέραια περιοχή, τότε και ο πολυωνυμικός δακτύλιος $R[x]$ είναι ακέραια περιοχή.

ΑΠΟΔΕΙΞΗ: (i) Έστω $R = \{\alpha_1 = 0, \alpha_2 = 1, \alpha_3, \ldots, \alpha_n\}$ ακέραια περιοχή. Έστω $\alpha_i \neq 0 \Leftrightarrow$ $\Leftrightarrow i \neq 1$. Ορίζουμε την απεικόνιση $f : R \to R$ με $f(\alpha_j) = \alpha_i\alpha_j$, για κάθε $j = 1, 2, 3, \ldots, n$. Παρατηρούμε ότι αν $f(\alpha_j) = f(\alpha_k)$, τότε $\alpha_i(\alpha_j - \alpha_k) = 0$. Επειδή ο R είναι ακέραια περιοχή, έπεται ότι $\alpha_j = \alpha_k \Leftrightarrow j = k$. Επομένως η f είναι 1-1 και επειδή ο R είναι πεπερασμένο σύνολο, είναι και επί. Άρα υπάρχει j τέτοιο, ώστε $f(\alpha_j) = \alpha_2 = 1 \Leftrightarrow \alpha_i\alpha_j = 1$.
(ii) Έστω $f(x) = \sum_{i=0}^{m} \alpha_i x^i$ και $g(x) = \sum_{i=0}^{n} \beta_i x^i$, όπου m, n μη αρνητικοί ακέραιοι και $\alpha_i, \beta_j \in$ $\in R$, για κάθε $i = 0, 1, \ldots, m$ και $j = 0, 1, \ldots, n$. Υποθέτουμε ότι $f(x) \neq 0$ και $g(x) \neq 0$. Τότε υπάρχουν ελάχιστοι μη αρνητικοί ακέραιοι κ, λ τέτοιοι, ώστε $\alpha_\kappa \neq 0$, $\beta_\lambda \neq 0$ και $\alpha_i = 0$ και $\beta_j = 0$ για κάθε μη αρνητικούς ακεραίους $i < \kappa$ και $j < \lambda$. (Αν υπάρχουν τέτοιοι, γιατί μπορεί $\kappa = 0$ ή $\lambda = 0$). Τότε ο συντελεστής του $x^{\kappa+\lambda}$ στο γινόμενο $f(x)g(x)$ ισούται με $\sum\limits_{\substack{i,j\geq 0 \\ i+j=\kappa+\lambda}} \alpha_i\beta_j$. Στο άθροισμα αυτό αν $i > \kappa$, τότε $j < \lambda$ και επομένως $\beta_j = 0 \Rightarrow \alpha_i\beta_j = 0$. Παρόμοια, αν $j > \lambda$, τότε $i < \kappa \Rightarrow \alpha_i = 0 \Rightarrow \alpha_i\beta_j = 0$. Επομένως $i \leq \kappa$ και $j \leq \lambda$. Λόγω της επιλογής των κ και λ ο μόνος μη μηδενικός όρος στο άθροισμα $\sum_{i+j=\kappa+\lambda} \alpha_i\beta_j$ είναι ο $\alpha_\kappa\beta_\lambda \neq 0$. Επομένως $f(x)g(x) \neq 0$. ■

1.3 Ομομορφισμοί Δακτυλίων

ΟΡΙΣΜΟΣ 1.15. Έστω R και S δύο μεταθετικοί δακτύλιοι με μονάδες 1_R και 1_S αντίστοιχα. Μια απεικόνιση $\varphi : R \to S$ λέγεται **ομομορφισμός δακτυλίων** αν η φ πληροί τα ακόλουθα:
(i) $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$, για κάθε $\alpha, \beta \in R$.
(ii) $\varphi(\alpha \cdot \beta) = \varphi(\alpha) \cdot \varphi(\beta)$, για κάθε $\alpha, \beta \in R$.
(iii) $\varphi(1_R) = 1_S$.

Παρατήρηση: Οι ιδιότητες **(i)** και **(ii)** δεν συνεπάγονται την **(iii)**. Επί παραδείγματι, αν $R = \mathbb{Z}_6$ και $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_6$ με $\varphi(\alpha) = 3\alpha$, για κάθε $\alpha \in \mathbb{Z}_6$, τότε η φ πληροί τις ιδιότητες **(i)** και **(ii)**, αλλά όχι την **(iii)**. Ένα άλλο αντιπαράδειγμα είναι το εξής: Έστω $R = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ ο δακτύλιος όλων των συναρτήσεων από το $\mathbb{R}$ στο $\mathbb{R}$. $\big($Η πρόσθεση και ο πολλαπλασιασμός ορίζονται κατά σημείο ως εξής: $(f + g)(x) = f(x) + g(x)$ και $(f \cdot g)(x) = f(x)g(x)$, για κάθε $x \in \mathbb{R}\big)$. Είναι εύκολο να επαληθεύσει κανείς ότι το σύνολο R είναι δακτύλιος με μηδενικό στοιχείο τη συνάρτηση $\mathbf{0} : \mathbb{R} \to \mathbb{R}$, όπου $\mathbf{0}(x) = 0$, για κάθε $x \in \mathbb{R}$ και μοναδιαίο στοιχείο τη συνάρτηση $\mathbf{1} : \mathbb{R} \to \mathbb{R}$, όπου $\mathbf{1}(x) = 1$, για κάθε $x \in \mathbb{R}$. Αν $\chi_{\mathbb{Q}}$ είναι η χαρακτηριστική συνάρτηση των ρητών, δηλαδή

$$\chi_{\mathbb{Q}}(x) = \begin{cases} 1, & \text{αν } x \in \mathbb{Q} \\ 0, & \text{αν } x \notin \mathbb{Q} \end{cases},$$

τότε $\chi_{\mathbb{Q}}^2 = \chi_{\mathbb{Q}}$ και η απεικόνιση $\varphi : R \to R$ με $\varphi(f) = \chi_{\mathbb{Q}} \cdot f$, για κάθε $f \in R$, πληροί τις ιδιότητες **(i)** και **(ii)**, αλλά όχι την **(iii)**. $\big($Γιατί $\varphi(\mathbf{1}) = \chi_{\mathbb{Q}} \neq \mathbf{1}\big)$.

ΟΡΙΣΜΟΣ 1.16. Έστω R και S δύο μεταθετικοί δακτύλιοι με μονάδες και $\varphi : R \to S$ ομομορφισμός δακτυλίων.
(i) Η φ λέγεται **επιμορφισμός** αν $\varphi(R) = S$.
(ii) Η φ λέγεται **μονομορφισμός** αν η φ είναι 1-1.
(iii) Η φ λέγεται **ισομορφισμός** αν η φ είναι μονομορφισμός και επιμορφισμός ταυτόχρονα. Τότε οι δακτύλιοι R και S λέγονται **ισόμορφοι**. Στην περίπτωση αυτή γράφουμε $R \cong S$.

ΟΡΙΣΜΟΣ 1.17. Έστω R μεταθετικός δακτύλιος με μονάδα. Ένα υποσύνολο S του R λέγεται **υποδακτύλιος** του R αν $0_R, 1_R \in S$ και το σύνολο S είναι δακτύλιος με πράξεις τους περιορισμούς σ' αυτό της πρόσθεσης και του πολλαπλασιασμού του R. Είναι προφανές ότι αν S είναι

ένας υποδακτύλιος του R, τότε η προφανής εμφύτευση $i : S \to R$, με $i(\alpha) = \alpha$, για κάθε $\alpha \in S$ είναι μονομορφισμός.

ΠΡΟΤΑΣΗ 1.18. Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων. Τότε ισχύουν τα εξής:
(i) Η εικόνα $\varphi(R)$ είναι υποδακτύλιος του S.
(ii) Ο **πυρήνας** $\text{Ker}\varphi = \{\alpha \in R \mid \varphi(\alpha) = 0_S\}$ είναι ιδεώδες του R.
(iii) Η φ είναι μονομορφισμός αν και μόνον αν $\text{Ker}\varphi = \{0_R\}$.
ΑΠΟΔΕΙΞΗ: (i) $\varphi(\alpha) + \varphi(\beta) = \varphi(\alpha + \beta) \in \varphi(R)$, για κάθε $\alpha, \beta \in R$.
$\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$. Επομένως $0_S = \varphi(0_R) - \varphi(0_R) = (\varphi(0_R) + \varphi(0_R)) - -\varphi(0_R) = \varphi(0_R) + (\varphi(0_R) - \varphi(0_R)) = \varphi(0_R) + 0_S = \varphi(0_R) \in \varphi(R)$.
$0_S = \varphi(0_R) = \varphi(\alpha + (-\alpha)) = \varphi(\alpha) + \varphi(-\alpha)$. Επομένως $-\varphi(\alpha) = \varphi(-\alpha) \in \varphi(R)$, για κάθε $\alpha \in R$. Συνεπώς $\varphi(\alpha) - \varphi(\beta) = \varphi(\alpha) + \varphi(-\beta) = \varphi(\alpha + (-\beta)) = \varphi(\alpha - \beta) \in \varphi(R)$, για κάθε $\alpha, \beta \in R$.
$\varphi(\alpha)\varphi(\beta) = \varphi(\alpha\beta) \in \varphi(R)$, για κάθε $\alpha, \beta \in R$ και τέλος, $1_S = \varphi(1_R) \in \varphi(R)$.
(ii) Έστω $\alpha, \beta \in \text{Ker}\varphi \Leftrightarrow \varphi(\alpha) = \varphi(\beta) = 0_S$. Τότε $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta) = 0_S + 0_S = 0_S \Rightarrow$ $\Rightarrow \alpha + \beta \in \text{Ker}\varphi$. Επίσης, αν $\alpha \in \text{Ker}\varphi \Leftrightarrow \varphi(\alpha) = 0_S$ και $r \in R$, τότε $\varphi(r\alpha) = \varphi(r)\varphi(\alpha) = = \varphi(r) \cdot 0_S = 0_S$. Επομένως $r\alpha \in \text{Ker}\varphi$.
(iii) Έστω $\varphi : R \to S$ μονομορφισμός. Επειδή $\varphi(0_R) = 0_S$, αν $\alpha \in \text{Ker}\varphi$, τότε $\varphi(\alpha) = 0_S = = \varphi(0_R)$ και άρα $\alpha = 0_R$. Αντιστρόφως, υποθέτουμε ότι $\text{Ker}\varphi = \{0_R\}$. Έστω $\alpha, \beta \in R$ με $\varphi(\alpha) = \varphi(\beta) \Leftrightarrow \varphi(\alpha) - \varphi(\beta) = 0_S \Leftrightarrow \varphi(\alpha - \beta) = 0_S \Leftrightarrow \alpha - \beta \in \text{Ker}\varphi = \{0_R\}$. Άρα $\alpha = \beta$. ■

Συμβολισμός: Η εικόνα $\varphi(R)$ συμβολίζεται με $\text{Im}\boldsymbol{\varphi}$.

1.4 Δακτύλιος-Πηλίκο

ΟΡΙΣΜΟΣ 1.19. Έστω R μεταθετικός δακτύλιος με μονάδα και I ιδεώδες αυτού. Στον R ορίζουμε τη σχέση «$\equiv \mod I$» ως εξής:

$$\alpha \equiv \beta \mod I \Leftrightarrow \alpha - \beta \in I.$$

ΠΡΟΤΑΣΗ 1.20. (i) Η σχέση $\equiv \mod I$ είναι μια σχέση ισοδυναμίας στον R.
(ii) Οι κλάσεις ισοδυναμίας είναι τα σύνολα $\alpha + I = \{\alpha + x \mid x \in I\}$, όπου $\alpha \in R$.
ΑΠΟΔΕΙΞΗ: (i) Ανακλαστική: $\alpha - \alpha = 0_R \in I \Leftrightarrow \alpha \equiv \alpha \mod I$, για κάθε $\alpha \in R$.
Συμμετρική: $\alpha \equiv \beta \mod I \Leftrightarrow \alpha - \beta \in I \Leftrightarrow -(\alpha - \beta) = \beta - \alpha \in I \Leftrightarrow \beta \equiv \alpha \mod I$.
Μεταβατική: Έστω $\alpha \equiv \beta \mod I$ και $\beta \equiv \gamma \mod I$, δηλαδή $\alpha - \beta \in I$ και $\beta - \gamma \in I$. Τότε $\alpha - \gamma = (\alpha - \beta) + (\beta - \gamma) \in I \Rightarrow \alpha \equiv \gamma \mod I$.
(ii) Έστω $\alpha \in R$. Έστω επίσης ότι το $\beta \in R$ ανήκει στην κλάση ισοδυναμίας στην οποία ανήκει το α, δηλαδή $\beta \equiv \alpha \mod I \Leftrightarrow \beta - \alpha \in I$. Θέτουμε $x = \beta - \alpha \in I$. Τότε $\beta = \alpha + x \in \alpha + I$. Αντιστρόφως, έστω $x \in I$. Θέτουμε $\beta = \alpha + x \in \alpha + I$. Τότε $\beta - \alpha = x \in I \Rightarrow \beta \equiv \alpha \mod I$. ■

Προφανώς, επειδή η πρόσθεση είναι μεταθετική, $\alpha + I = I + \alpha = \{x + \alpha \mid x \in I\}$.

Το σύνολο των κλάσεων ισοδυναμίας $\{\alpha + I \mid \alpha \in R\}$ το παριστάνουμε με $\boldsymbol{R/I}$.

Εφοδιάζουμε το R/I με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού, ώστε να καταστήσουμε το R/I μεταθετικό δακτύλιο με μονάδα. (Αν $I = R \Leftrightarrow 1_R \in I$, τότε παίρνουμε τον τετριμμένο δακτύλιο).
Αυτό θα γίνει κατά τα γνωστά, μέσω αντιπροσώπων των κλάσεων ισοδυναμίας.

Ορίζουμε:
$$(\alpha+I)+(\beta+I)=(\alpha+\beta)+I \text{ και}$$
$$(\alpha+I)(\beta+I)=\alpha\beta+I.$$
Θα πρέπει να αποδείξουμε ότι οι πράξεις είναι καλά ορισμένες.
Έστω $\alpha+I=\alpha'+I$ και $\beta+I=\beta'+I$. Οι σχέσεις αυτές είναι ισοδύναμες με τις $\alpha-\alpha'\in I$ και $\beta-\beta'\in I$. Επομένως $(\alpha+\beta)-(\alpha'+\beta')=(\alpha-\alpha')+(\beta-\beta')\in I \Rightarrow (\alpha+\beta)+I=(\alpha'+\beta')+I$, ήτοι η πρόσθεση είναι καλά ορισμένη.
Για τον πολλαπλασιασμό παρατηρούμε ότι $\alpha\beta-\alpha'\beta'=\alpha\beta-\alpha\beta'+\alpha\beta'-\alpha'\beta'=\alpha(\underbrace{\beta-\beta'}_{\in I})+$
$+\beta'(\underbrace{\alpha-\alpha'}_{\in I})\in I+I\subseteq I$. Επομένως $\alpha\beta+I=\alpha'\beta'+I$.

ΠΡΟΤΑΣΗ 1.21. Το σύνολο R/I εφοδιασμένο με τις παραπάνω πράξεις καθίσταται μεταθετικός δακτύλιος με μονάδα. Ο δακτύλιος αυτός λέγεται **δακτύλιος-πηλίκο**.
ΑΠΟΔΕΙΞΗ: (i) Έχουμε: $(\alpha+I)+\big((\beta+I)+(\gamma+I)\big)=(\alpha+I)+\big((\beta+\gamma)+I\big)=\big(\alpha+(\beta+\gamma)\big)+I=$
$=\big((\alpha+\beta)+\gamma\big)+I=\big((\alpha+\beta)+I\big)+(\gamma+I)=\big((\alpha+I)+(\beta+I)\big)+(\gamma+I)$.
(ii) $(\alpha+I)+(\beta+I)=(\alpha+\beta)+I=(\beta+\alpha)+I=(\beta+I)+(\alpha+I)$.
(iii) $(\alpha+I)+I=(\alpha+I)+(0_R+I)=(\alpha+0_R)+I=\alpha+I$. Επομένως $0_{R/I}=I$.
(iv) $(\alpha+I)+((-\alpha)+I)=(\alpha+(-\alpha))+I=0_R+I=I=0_{R/I}$. Επομένως $-(\alpha+I)=-\alpha+I$.
(v) $(\alpha+I)\big((\beta+I)(\gamma+I)\big)=(\alpha+I)(\beta\gamma+I)=\alpha(\beta\gamma)+I=(\alpha\beta)\gamma+I=(\alpha\beta+I)(\gamma+I)=$
$=\big((\alpha+I)(\beta+I)\big)(\gamma+I)$.
(vi) $(\alpha+I)(\beta+I)=\alpha\beta+I=\beta\alpha+I=(\beta+I)(\alpha+I)$.
(vii) $(\alpha+I)\big((\beta+I)+(\gamma+I)\big)=(\alpha+I)\big((\beta+\gamma)+I\big)=\alpha(\beta+\gamma)+I=(\alpha\beta+\alpha\gamma)+I=$
$=(\alpha\beta+I)+(\alpha\gamma+I)=(\alpha+I)(\beta+I)+(\alpha+I)(\gamma+I)$.
(viii) $(\alpha+I)(1_R+I)=\alpha\cdot 1_R+I=\alpha+I$, για κάθε $\alpha\in R$. Επομένως το μοναδιαίο στοιχείο του R/I είναι το $1_{R/I}=1_R+I$. Αν $I=R\Leftrightarrow 1_R\in I$, τότε $1_{R/I}=1_R+I=I=0_{R/I}$, οπότε ο δακτύλιος-πηλίκο $R/I=\{I\}$ είναι ο τετριμμένος. ■

Στα επόμενα θα θεωρήσουμε γνήσια ιδεώδη $I\lhd R$, οπότε ο R/I δεν είναι τετριμμένος.

ΟΡΙΣΜΟΣ 1.22. Η απεικόνιση $p:R\to R/I$ με $p(\alpha)=\alpha+I$, για κάθε $\alpha\in R$ είναι προφανώς επιμορφισμός δακτυλίων. Η p θα λέγεται **φυσικός επιμορφισμός** ή **φυσική προβολή**. Πυρήνας της είναι προφανώς το I.

ΠΡΟΤΑΣΗ 1.23. Έστω $f:R\to S$ ομομορφισμός δακτυλίων. Τότε ισχύει $R/\mathrm{Ker}f\cong \mathrm{Im}f$.
ΑΠΟΔΕΙΞΗ: Ορίζουμε την απεικόνιση $\overline{f}:R/\mathrm{Ker}f\to \mathrm{Im}f$ ως εξής:
$$\overline{f}(r+\mathrm{Ker}f)=f(r),$$
για κάθε $r\in R$. Αν $r+\mathrm{Ker}f=r'+\mathrm{Ker}f$, τότε $r-r'\in\mathrm{Ker}f$ και συνεπώς $f(r-r')=0_S\Leftrightarrow$
$\Leftrightarrow f(r)=f(r')$. Άρα η $\overline{f}$ είναι καλά ορισμένη. Εύκολα προκύπτει ότι η $\overline{f}$ είναι ομομορφισμός δακτυλίων. Επειδή $f(r)=\overline{f}(r+\mathrm{Ker}f)$, η $\overline{f}$ είναι προφανώς επιμορφισμός.
Τώρα, αν $r+\mathrm{Ker}f\in\mathrm{Ker}\overline{f}$, τότε $\overline{f}(r+\mathrm{Ker}f)=0_S\Leftrightarrow f(r)=0_S\Leftrightarrow r\in\mathrm{Ker}f\Leftrightarrow r+\mathrm{Ker}f=$
$=\mathrm{Ker}f=0_{R/\mathrm{Ker}f}$, δηλαδή η $\overline{f}$ είναι και μονομορφισμός, άρα τελικά ισομορφισμός. ■

ΟΡΙΣΜΟΣ 1.24. Ένα γνήσιο ιδεώδες $P\lhd R$ λέγεται **πρώτο ιδεώδες** αν και μόνον αν για κάθε $\alpha,\beta\in R$ ισχύει η ισοδυναμία
$$\alpha\beta\in P\Leftrightarrow\big(\alpha\in P \text{ ή } \beta\in P\big).$$

ΠΡΟΤΑΣΗ 1.25. Το ιδεώδες P είναι πρώτο αν και μόνον αν ο δακτύλιος-πηλίκο R/P είναι ακέραια περιοχή.
ΑΠΟΔΕΙΞΗ: Έστω αρχικά ότι το P είναι πρώτο. Υποθέτουμε ότι $(\alpha+P)(\beta+P)=0_{R/P}=P$. Ισοδύναμα $\alpha\beta+P=P\Leftrightarrow\alpha\beta\in P\underset{P\text{ πρώτο}}{\Leftrightarrow}\big(\alpha\in P\text{ ή }\beta\in P\big)\Leftrightarrow\big(\alpha+P=P=0_{R/P}\text{ ή }\beta+P=$ $=P=0_{R/P}\big)$. Άρα ο δακτύλιος R/P είναι ακέραια περιοχή.
Αντιστρόφως, υποθέτουμε ότι ο R/P είναι ακέραια περιοχή. Έστω $\alpha\beta\in P\Leftrightarrow\alpha\beta+P=P=$ $=0_{R/P}\Leftrightarrow(\alpha+P)(\beta+P)=0_{R/P}\underset{\substack{R/P\text{ ακέραια}\\\text{περιοχή}}}{\Leftrightarrow}\big(\alpha+P=0_{R/P}=P\text{ ή }\beta+P=0_{R/P}=P\big)\Leftrightarrow\big(\alpha\in$ $\in P\text{ ή }\beta\in P\big)$. Επομένως το P είναι πρώτο. ■

ΠΟΡΙΣΜΑ 1.26. Ένας μεταθετικός μοναδιαίος δακτύλιος είναι ακέραια περιοχή αν και μόνον αν το τετριμμένο ιδεώδες $\{0_R\}$ είναι πρώτο.
ΑΠΟΔΕΙΞΗ: Ο $R\cong R/\{0_R\}$ είναι ακέραια περιοχή αν και μόνον αν το $\{0_R\}$ είναι πρώτο, σύμφωνα με την προηγούμενη πρόταση.
Εναλλακτικά, έστω ότι το $\{0_R\}$ είναι πρώτο. Τότε $\alpha\beta=0_R\Leftrightarrow\alpha\beta\in\{0_R\}\underset{\{0_R\}\text{ πρώτο}}{\Leftrightarrow}\big(\alpha\in$ $\in\{0_R\}\text{ ή }\beta\in\{0_R\}\big)\Leftrightarrow\big(\alpha=0_R\text{ ή }\beta=0_R\big)$. Αντιστρόφως, έστω ότι ο R είναι ακέραια περιοχή. Τότε $\alpha\beta\in\{0_R\}\Leftrightarrow\alpha\beta=0_R\Leftrightarrow\big(\alpha=0_R\text{ ή }\beta=0_R\big)\Leftrightarrow\big(\alpha\in\{0_R\}\text{ ή }\beta\in\{0_R\}\big)$, δηλαδή το ιδεώδες $\{0_R\}$ είναι πρώτο. ■

ΟΡΙΣΜΟΣ 1.27. Ένα γνήσιο ιδεώδες $M\lhd R$ λέγεται **μέγιστο ιδεώδες** αν και μόνον αν δεν υπάρχει γνήσιο ιδεώδες M' με $M\subsetneq M'$, δηλαδή το M' να περιέχει γνήσια το M.

ΠΡΟΤΑΣΗ 1.28. Ένα γνήσιο ιδεώδες M του R είναι μέγιστο αν και μόνον αν ο δακτύλιος πηλίκο R/M είναι σώμα.
ΑΠΟΔΕΙΞΗ: Έστω M μέγιστο ιδεώδες του R. $\big($Εφόσον M γνήσιο ιδεώδες, ο δακτύλιος R/M είναι μη τετριμμένος$\big)$. Έστω $\alpha+M\neq0_{R/M}=M\Leftrightarrow\alpha\notin M$. Το ιδεώδες λοιπόν $(\alpha)+M$ περιέχει γνήσια το M και άρα $(\alpha)+M=R$. Επομένως υπάρχουν $r\in R$ και $x\in M$ τέτοια, ώστε $r\alpha+x=1_R$. Κατά συνέπεια $(r\alpha+x)+M=1_R+M=1_{R/M}$.
Αλλά $(r\alpha+x)+M=(r\alpha+M)+(x+M)\underset{x\in M}{=}(r+M)(\alpha+M)+M\underset{M=0_{R/M}}{=}(r+M)(\alpha+M)$.
Επομένως $(r+M)(\alpha+M)=1_{R/M}$, δηλαδή το $\alpha+M$ αντιστρέφεται. Άρα ο R/M είναι σώμα.
Αντιστρόφως, υποθέτουμε ότι ο R/M είναι σώμα. Έστω M' ιδεώδες του R, το οποίο περιέχει γνήσια το M. Τότε υπάρχει $\alpha\in M'\setminus M$. Εφόσον $\alpha\notin M\Leftrightarrow\alpha+M\neq0_{R/M}$, το $\alpha+M$ αντιστρέφεται στον R/M. Άρα υπάρχει $r\in R$ με $(r+M)(\alpha+M)=1_R+M=1_{R/M}\Leftrightarrow$ $\Leftrightarrow r\alpha+M=1_R+M\Leftrightarrow1_R-r\alpha\in M$. Έστω $x=1_R-r\alpha\in M$. Τότε $1_R=r\alpha+x\in M'$. $\big(r\alpha\in M'\text{ και }x\in M\subseteq M'\big)$. Δηλαδή $M'=R$. ■

ΠΟΡΙΣΜΑ 1.29. Κάθε μέγιστο ιδεώδες του R είναι πρώτο.
ΑΠΟΔΕΙΞΗ: Έστω M μέγιστο ιδεώδες. Τότε R/M είναι σώμα και κατά συνέπεια ακέραια περιοχή.
Εναλλακτικά, έστω $\alpha\beta\in M$ με $\alpha\notin M$. Εφόσον M μέγιστο και $\alpha\notin M$, έχουμε $(\alpha)+M=R$. Άρα $r\alpha+x=1_R$, για κάποιο $r\in R$ και $x\in M$. Επομένως $\beta=r\underbrace{\alpha\beta}_{\in M}+\beta x\in M$. ■

Ένας δακτύλιος μπορεί να έχει περισσότερα του ενός μέγιστα ιδεώδη. Για παράδειγμα, κάθε κύριο ιδεώδες του $\mathbb{Z}$ της μορφής (p), όπου p πρώτος εκτός από πρώτο ιδεώδες είναι και μέγιστο. Πράγματι, ο δακτύλιος-πηλίκο $\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}$ είναι πεπερασμένη ακέραια περιοχή και άρα σώμα.

Αποδεικνύεται, με βάση το συνολοθεωρητικό **Λήμμα του Zörn**, το οποίο είναι ισοδύναμο με το **Αξίωμα Επιλογής**, ότι κάθε μη τετριμμένος δακτύλιος περιέχει μέγιστο ιδεώδες. Τι λέει το Λήμμα του Zörn;

Κατ' αρχάς θα υπενθυμίσουμε κάποια πράγματα από τη Θεωρία Συνόλων[1] ξεκινώντας από τον επόμενο ορισμό:

ΟΡΙΣΜΟΣ 1.30. Ένα μη κενό σύνολο A λέγεται **μερικώς διατεταγμένο σύνολο** (partially ordered set-poset) αν στο A υπάρχει μια σχέση (μερικής) διατάξεως $\preceq$ με τις ακόλουθες ιδιότητες:
(i) $\alpha \preceq \alpha$, για κάθε $\alpha \in A$. (Αυτοπαθής)
(ii) Αν $\alpha \preceq \beta$ και $\beta \preceq \alpha$, τότε $\alpha = \beta$. (Αντισυμμετρική)
(iii) Αν $\alpha \preceq \beta$ και $\beta \preceq \gamma$, τότε $\alpha \preceq \gamma$. (Μεταβατική)

Σημειώνουμε εδώ ότι δύο στοιχεία α και β ενός μερικώς διατεταγμένου συνόλου A μπορεί να μην είναι συγκρίσιμα. Δηλαδή να μην ισχύει καμία από τις σχέσεις $\alpha \preceq \beta$ ή $\beta \preceq \alpha$. Για παράδειγμα, αν $B = \{x, y\}$ είναι ένα σύνολο με δύο στοιχεία και $A = \mathscr{P}(B) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$ το **δυναμοσύνολο** του A, δηλαδή το σύνολο όλων των υποσυνόλων του και $\preceq$ είναι η σχέση $\subseteq$ του περιέχεσθαι, τότε $\{x\} \not\subseteq \{y\}$ και $\{y\} \not\subseteq \{x\}$, δηλαδή τα στοιχεία $\{x\}, \{y\} \in A = \mathscr{P}(B)$ είναι μη συγκρίσιμα. Αντιθέτως $\varnothing \subseteq \{x\} \subseteq \{x, y\} = B$.
Ένα άλλο παράδειγμα είναι το σύνολο $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ των θετικών ακεραίων με τη σχέση «$|$» της διαιρετότητας. Η σχέση «$|$» είναι σχέση μερικής διάταξης. Αλλά $3 \nmid 5$ και $5 \nmid 3$. Άρα οι αριθμοί 3 και 5 είναι μη συγκρίσιμοι. Αλλά $5 \mid 10$, $17 \mid 51$ κτλ.
Από την άλλη μεριά, στο σύνολο $\mathbb{R}$ των πραγματικών αριθμών, για κάθε $x, y \in \mathbb{R}$ ισχύει $x \leq y$ ή $y \leq x$. Λέμε ότι το $\mathbb{R}$, ακριβέστερα το ζεύγος $(\mathbb{R}, \leq)$, είναι **γραμμικά (ή ολικά) διατεταγμένο σύνολο**.
Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο και A' ένα μη κενό υποσύνολό του. Αν υπάρχει $\alpha \in A$ με την ιδιότητα $x \preceq \alpha$, για κάθε $x \in A'$, τότε **το α λέγεται ένα άνω φράγμα του A'** και **το A' άνω φραγμένο από το α**.
Για παράδειγμα, στο σύνολο $\mathbb{Z}^+$ των θετικών ακεραίων κάθε **πεπερασμένο** υποσύνολό του $\{x_1, x_2, \ldots, x_k\}$ είναι άνω φραγμένο ως προς τη σχέση «$|$» της διαιρετότητας από το ελάχιστο κοινό πολλαπλάσιο των στοιχείων του. Αλλά και στο $(\mathbb{R}, \leq)$ το διάστημα $(-1, 1)$ είναι άνω φραγμένο από το 1, αλλά φυσικά και από κάθε αριθμό μεγαλύτερο ή ίσο του 1.
Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο και $\alpha \in A$. **Το α λέγεται μέγιστο στοιχείο του A, αν δεν υπάρχει $\beta \in A$ τέτοιο, ώστε $\alpha \preceq \beta$ και $\alpha \neq \beta$.** Σε ένα μερικώς διατεταγμένο σύνολο μπορεί να μην υπάρχει μέγιστο στοιχείο (για παράδειγμα σε ολόκληρο το $\mathbb{R}$ με τη σχέση $\leq$) ή να υπάρχουν περισσότερα του ενός μέγιστα στοιχεία. Για παράδειγμα, στο σύνολο $A = \{\varnothing, \{1\}, \{2\}, \{1, 2, 3\}, \{1, 2, 4\}\}$ με τη σχέση «$\subseteq$» τα σύνολα-στοιχεία $\{1, 2, 3\}$ και $\{1, 2, 4\}$ είναι μέγιστα στοιχεία. Στο σύνολο των γνησίων ιδεωδών του $\mathbb{Z}$ τα ιδεώδη $p\mathbb{Z}$, όπου p πρώτος, είναι μέγιστα στοιχεία αφού το $\mathbb{Z}_p = \mathbb{Z}\Big/_{p\mathbb{Z}}$ είναι σώματα.
Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο και B ένα μη κενό υποσύνολό του. **Το B λέγεται αλυσίδα του A αν είναι γραμμικά διατεταγμένο ως προς τη σχέση $\preceq$.**

[1] Ο ενδιαφερόμενος αναγνώστης μπορεί να καταφύγει στο κλασικό σύγγραμμα του Paul R. Halmos, *Naive Set Theory* (*Αφελής Θεωρία Συνόλων!*), Undergraduate Texts in Mathematics, Springer-Verlag, Fifth Edition, 1987.

ΛΗΜΜΑ 1.31. (ΛΗΜΜΑ ΤΟΥ ZÖRN) Έστω $(A, \preceq)$ ένα μερικώς διατεταγμένο σύνολο. Αν κάθε αλυσίδα B του A έχει άνω φράγμα στο A, τότε το A έχει ένα τουλάχιστον μέγιστο στοιχείο.

Το λήμμα του Zörn το δεχόμαστε εδώ χωρίς απόδειξη. Θα το εφαρμόσουμε για να αποδείξουμε ότι κάθε μεταθετικός δακτύλιος με μονάδα (μη τετριμμένος) έχει μέγιστο ιδεώδες.

ΠΡΟΤΑΣΗ 1.32. Κάθε μοναδιαίος μεταθετικός δακτύλιος R έχει μέγιστο ιδεώδες.
ΑΠΟΔΕΙΞΗ: Έστω $\mathscr{A}$ το σύνολο των γνήσιων ιδεωδών του R. Προφανώς $\{0_R\} \in \mathscr{A}$. Επομένως $\mathscr{A} \neq \varnothing$. Έστω $\{I_\lambda \mid \lambda \in \Lambda\}$ μια αλυσίδα στο $\mathscr{A}$, την οποία παριστάνουμε υπό μορφή οικογένειας με σύνολο δεικτών Λ. Δηλαδή, για κάθε $\lambda, \lambda' \in \Lambda$ έχουμε $I_\lambda \subseteq I_{\lambda'}$ ή $I_{\lambda'} \subseteq I_\lambda$.
Έστω $J = \bigcup_{\lambda\in\Lambda} I_\lambda$. Αν $x, y \in J$. Τότε υπάρχουν $\lambda_1, \lambda_2 \in \Lambda$ τέτοια, ώστε $x \in I_{\lambda_1}$ και $y \in I_{\lambda_2}$. Αλλά, όπως είπαμε $I_{\lambda_1} \subseteq I_{\lambda_2}$ ή $I_{\lambda_2} \subseteq I_{\lambda_1}$. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $I_{\lambda_1} \subseteq I_{\lambda_2}$. Τότε $x, y \in I_{\lambda_2}$. Επομένως $x + y \in I_{\lambda_2} \subseteq \bigcup_{\lambda\in\Lambda} I_\lambda = J$. Αν τώρα $r \in R$ και $x \in J$, τότε $x \in I_{\lambda_0}$, για κάποιο $\lambda_0 \in \Lambda$. Άρα $rx \in I_{\lambda_0} \subseteq \bigcup_{\lambda\in\Lambda} I_\lambda = J$. Συμπεραίνουμε λοιπόν ότι το J είναι ιδεώδες του R. Είναι επίσης γνήσιο ιδεώδες γιατί, αν $1_R \in J$, τότε $1_R \in I_\lambda$, για κάποιο $\lambda \in \Lambda$, άτοπο γιατί το I_λ είναι γνήσιο ιδεώδες. Κατά συνέπεια το $J = \bigcup_{\lambda\in\Lambda} I_\lambda$ είναι άνω φράγμα στο $\mathscr{A}$ για την οικογένεια (αλυσίδα) ιδεωδών $\{I_\lambda \mid \lambda \in \Lambda\}$. Από το λήμμα του Zörn προκύπτει ότι το σύνολο των γνήσιων ιδεωδών $\mathscr{A}$ έχει μέγιστο στοιχείο. ■

1.5 Σώμα Πηλίκων Ακέραιας Περιοχής

Ερχόμαστε τώρα σε ένα πρόβλημα, το οποίο έχει δημιουργήσει σύγχυση και παρερμηνείες, ακόμα και σε καθηγητές δευτεροβάθμιας εκπαίδευσης. Θα έχετε ίσως παρατηρήσει ότι τα κλάσματα με αριθμητή και παρονομαστή ακεραίους και τα οποία εκφράζουν την ίδια ποσότητα αναφέρονται στα σχολικά βιβλία ως «ισοδύναμα» και όχι ως ίσα. Αυτό είναι **λάθος**. Στο δημοτικό μάθαμε ότι αν κόψουμε ένα μήλο σε 6 ίσα κομμάτια και πάρουμε τα 3, αυτό είναι το ίδιο με το να κόψουμε το μήλο σε δύο ίσα κομμάτια και να πάρουμε το ένα. Δηλαδή έχουμε **ισότητα** των κλασμάτων $\frac{3}{6} = \frac{1}{2}$. Για να μην λέμε ανοησίες περί «ισοδυναμίας», ας ξεκαθαρίσουμε το πράγμα άπαξ δια παντός.
Χάριν απλότητος, εδώ θα γράφουμε 0 αντί 0_R και 1 αντί 1_R.

ΠΡΟΤΑΣΗ 1.33. Έστω R ακέραια περιοχή. (Ας έχουμε στο μυαλό μας το $\mathbb{Z}$). Θέτουμε $R^* = R \setminus \{0\}$. Στο καρτεσιανό γινόμενο $R \times R^*$ ορίζουμε τη σχέση $\approx$ ως εξής:

$$(\alpha, \beta) \approx (\gamma, \delta) \Leftrightarrow \alpha\delta = \gamma\beta \Leftrightarrow \alpha\delta - \gamma\beta = 0.$$

(Θυμηθείτε την ισότητα κλασμάτων). Τότε η σχέση $\approx$ είναι σχέση ισοδυναμίας στο σύνολο $R \times R^*$.
ΑΠΟΔΕΙΞΗ: (i) Ανακλαστική: Για κάθε $(\alpha, \beta) \in R \times R^*$ έχουμε: $(\alpha, \beta) \approx (\alpha, \beta) \Leftrightarrow \alpha\beta = \alpha\beta$, η οποία προφανώς ισχύει.
(ii) Συμμετρική: Έστω $(\alpha, \beta), (\gamma, \delta) \in R \times R^*$. Τότε έχουμε: $(\alpha, \beta) \approx (\gamma, \delta) \Leftrightarrow \alpha\delta = \gamma\beta \Leftrightarrow$ $\Leftrightarrow \gamma\beta = \alpha\delta \Leftrightarrow (\gamma, \delta) \approx (\alpha, \beta)$.
(iii) Μεταβατική: Έστω $(\alpha, \beta), (\gamma, \delta), (\varepsilon, \zeta) \in R \times R^*$ με $(\alpha, \beta) \approx (\gamma, \delta)$ και $(\gamma, \delta) \approx (\varepsilon, \zeta)$. Τότε έχουμε τις σχέσεις: $\alpha\delta = \gamma\beta$ και $\gamma\zeta = \varepsilon\delta$. Επομένως $\alpha\delta\zeta = \gamma\beta\zeta$ και $\gamma\beta\zeta = \beta\varepsilon\delta$. Συνεπώς $\alpha\delta\zeta = \beta\varepsilon\delta \Leftrightarrow \delta(\alpha\zeta - \varepsilon\beta) = 0$. Επειδή η R είναι ακέραια περιοχή και $\delta \neq 0$, έπεται

$\alpha\zeta = \varepsilon\beta \Leftrightarrow (\alpha,\beta) \approx (\varepsilon,\zeta)$. ■

Συμπεραίνουμε λοιπόν ότι η σχέση $\approx$, ως σχέση ισοδυναμίας, **ορίζει μία διαμέριση του συνόλου $R \times R^*$ σε κλάσεις ισοδυναμίας**.

ΟΡΙΣΜΟΣ 1.34. Για κάθε $\alpha \in R$ και $\beta \in R^*$ συμβολίζουμε με
$$\frac{\alpha}{\beta} = \Big\{(\gamma,\delta) \in R \times R^* \mid (\gamma,\delta) \approx (\alpha,\beta)\Big\},$$
την κλάση ισοδυναμίας στην οποία ανήκει το ζεύγος $(\alpha,\beta) \in R \times R^*$.

Η κλάση ισοδυναμίας $\dfrac{\alpha}{\beta}$ λέγεται κλάσμα με αριθμητή α και παρονομαστή β.

Επειδή δύο κλάσεις ισοδυναμίας είτε ταυτίζονται (είναι δηλαδή ίσες) είτε είναι ξένες μεταξύ τους, **δύο κλάσματα είναι ίσα ή δεν είναι ίσα**.

Τα κλάσματα (κλάσεις ισοδυναμίας στο $R \times R^*$) $\dfrac{\alpha}{\beta}$ και $\dfrac{\gamma}{\delta}$ είναι προφανώς ίσα αν και μόνον αν $(\alpha,\beta) \approx (\gamma,\delta) \Leftrightarrow \alpha\delta = \gamma\beta$.

Θέτουμε $\mathbb{K} = (R \times R^*)/\approx$ για το σύνολο των κλάσεων ισοδυναμίας. Στο σύνολο $\mathbb{K}$ ορίζουμε δύο πράξεις: την πρόσθεση, την οποία καταχρηστικά θα εξακολουθήσουμε να τη συμβολίζουμε με το σύμβολο $+$ και τον πολλαπλασιασμό, τον οποίο επίσης καταχρηστικά θα συμβολίζουμε με το σύμβολο $\cdot$
Η λέξη καταχρηστικά αναφέρεται στο γεγονός ότι με τα σύμβολα $+$ και $\cdot$ συμβολίζουμε την πρόσθεση και τον πολλαπλασιασμό στην ακέραια περιοχή R. Θέτουμε λοιπόν:
$$\frac{\alpha}{\beta} + \frac{\gamma}{\delta} = \frac{\alpha\delta + \gamma\beta}{\beta\delta}$$
και
$$\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} = \frac{\alpha\gamma}{\beta\delta}.$$
Τίθεται όμως ένα ερώτημα: για τον ορισμό των πράξεων ανάμεσα στις κλάσεις ισοδυναμίας (κλάσματα) χρησιμοποιήσαμε αντιπροσώπους (α,β) και (γ,δ) των κλάσεων αυτών. Αν αλλάξουμε τους αντιπροσώπους και πάρουμε άλλους αντιπροσώπους (α',β') και (γ',δ') των αντίστοιχων κλάσεων, τότε το αποτέλεσμα, δηλαδή το κλάσμα ή αλλιώς η κλάση ισοδυναμίας θα παραμείνει η ίδια; Η απάντηση στο ερώτημα αυτό είναι καταφατική.

ΠΡΟΤΑΣΗ 1.35. Οι πράξεις $+$ και $\cdot$ που ορίστηκαν στο σύνολο $\mathbb{K} = R \times R^*/\approx$ είναι καλά ορισμένες.

ΑΠΟΔΕΙΞΗ: Θέλουμε να δείξουμε ότι αν $\dfrac{\alpha}{\beta} = \dfrac{\alpha'}{\beta'}$ και $\dfrac{\gamma}{\delta} = \dfrac{\gamma'}{\delta'}$, δηλαδή αν $(\alpha,\beta) \approx (\alpha',\beta')$ και $(\gamma,\delta) \approx (\gamma',\delta')$, τότε $(\alpha\delta+\gamma\beta,\beta\delta) \approx (\alpha'\delta'+\gamma'\beta',\beta'\delta')$ και $(\alpha\gamma,\beta\delta) \approx (\alpha'\gamma',\beta'\delta')$.
Για να αποδείξουμε την πρώτη σχέση αρκεί να δείξουμε ότι $(\alpha\delta+\gamma\beta)\beta'\delta' = (\alpha'\delta'+\gamma'\beta')\beta\delta \Leftrightarrow$
$\Leftrightarrow \alpha\beta'\delta\delta' - \alpha'\beta\delta\delta' + \gamma\delta'\beta\beta' - \gamma'\delta\beta\beta' = 0 \Leftrightarrow \underbrace{(\alpha\beta' - \alpha'\beta)}_{0}\delta\delta' + \underbrace{(\gamma\delta' - \gamma'\delta)}_{0}\beta\beta' = 0.$
Επομένως η πρόσθεση είναι καλά ορισμένη. Για τον πολλαπλασιασμό αρκεί να δείξουμε ότι $\alpha\gamma\beta'\delta' = \alpha'\gamma'\beta\delta \Leftrightarrow \alpha\gamma\beta'\delta' - \alpha'\gamma\beta\delta' = \alpha'\gamma'\beta\delta - \alpha'\gamma\beta\delta' \Leftrightarrow \underbrace{(\alpha\beta' - \alpha'\beta)}_{0}\gamma\delta' = \underbrace{(\gamma'\delta - \gamma\delta')}_{0}\alpha'\beta \Leftrightarrow$
$\Leftrightarrow 0 = 0.$ ■

ΛΗΜΜΑ 1.36. Ισχύουν τα εξής:
(i) $\frac{\alpha}{\beta} = \frac{\alpha\lambda}{\beta\lambda}$, για κάθε $\alpha, \beta, \lambda \in R$ με $\beta\lambda \neq 0$.
(ii) $\frac{\alpha}{\beta} + \frac{\gamma}{\beta} = \frac{\alpha+\gamma}{\beta}$, για κάθε $\alpha, \beta, \gamma \in R$, με $\beta \neq 0$.
(iii) $\frac{0}{\beta} = \frac{0}{1}$, για κάθε $\beta \in R \setminus \{0\}$.
(iv) Αν $\beta \neq 0$, τότε $\frac{\beta}{\beta} = \frac{1}{1} \neq \frac{0}{1}$.

ΑΠΟΔΕΙΞΗ: (i) $\frac{\alpha}{\beta} = \frac{\alpha\lambda}{\beta\lambda} \Leftrightarrow \alpha\beta\lambda = \alpha\lambda\beta$.
(ii) $\frac{\alpha}{\beta} + \frac{\gamma}{\beta} = \frac{\alpha\beta+\gamma\beta}{\beta^2} = \frac{(\alpha+\gamma)\beta}{\beta^2} = \frac{\alpha+\gamma}{\beta}$, σύμφωνα με το **(i)**.
(iii) $\frac{0}{\beta} = \frac{0}{1} \Leftrightarrow 0 \cdot 1 = 0 \cdot \beta \Leftrightarrow 0 = 0$.
(iv) Έστω $\beta \in R \setminus \{0\}$. Τότε $\frac{\beta}{\beta} = \frac{1\cdot\beta}{1\cdot\beta} = \frac{1}{1}$, σύμφωνα με το **(i)**, όπου $\lambda = \beta$. Τέλος, αν $\frac{1}{1} = \frac{0}{1}$, τότε $1 \cdot 1 = 0 \cdot 1 \Leftrightarrow 1 = 0$, άτοπο. ■

ΠΡΟΤΑΣΗ 1.37. Το $(\mathbb{K}, +, \cdot)$ είναι σώμα.

ΑΠΟΔΕΙΞΗ: Ξεκινάμε με μία παρατήρηση. Από το **(iv)** του προηγουμένου λήμματος προκύπτει ότι $0_{\mathbb{K}} = \frac{0}{1} \neq \frac{1}{1} = 1_{\mathbb{K}}$ και συνεπώς το $\mathbb{K}$ δεν είναι ο τετριμμένος δακτύλιος.
(i) Έστω $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta \in R$ με $\beta\delta\zeta \neq 0$. Τότε έχουμε:
$\frac{\alpha}{\beta} + \left(\frac{\gamma}{\delta} + \frac{\varepsilon}{\zeta}\right) = \frac{\alpha}{\beta} + \frac{\gamma\zeta+\varepsilon\delta}{\delta\zeta} = \frac{\alpha\delta\zeta+\beta(\gamma\zeta+\varepsilon\delta)}{\beta\delta\zeta} = \frac{\alpha\delta\zeta+\beta\gamma\zeta+\beta\varepsilon\delta}{\beta\delta\zeta} = \frac{(\alpha\delta+\beta\gamma)\zeta+\beta\varepsilon\delta}{\beta\delta\zeta} =$
$= \frac{\alpha\delta+\beta\gamma}{\beta\delta} + \frac{\varepsilon}{\zeta} = \left(\frac{\alpha}{\beta} + \frac{\gamma}{\delta}\right) + \frac{\varepsilon}{\zeta}$ και η προσεταιριστικότητα της πρόσθεσης αποδείχθηκε.
(ii) Έστω $\alpha, \beta, \gamma, \delta \in R$ με $\beta\delta \neq 0$. Τότε έχουμε: $\frac{\alpha}{\beta} + \frac{\gamma}{\delta} = \frac{\alpha\delta+\gamma\beta}{\beta\delta} = \frac{\gamma\beta+\alpha\delta}{\delta\beta} = \frac{\gamma}{\delta} + \frac{\alpha}{\beta}$ και η μεταθετικότητα της πρόσθεσης αποδείχθηκε.
(iii) Έστω $\alpha, \beta \in R$ με $\beta \neq 0$. Τότε $\frac{\alpha}{\beta} + \frac{0}{1} = \frac{\alpha\cdot 1 + 0\cdot\beta}{\beta\cdot 1} = \frac{\alpha}{\beta}$. Άρα το κλάσμα $\frac{0}{1}$ είναι το μηδενικό στοιχείο της πρόσθεσης.
(iv) Έστω $\alpha, \beta \in R$ με $\beta \neq 0$. Τότε $\frac{\alpha}{\beta} + \frac{-\alpha}{\beta} \underset{\substack{\text{(ii) προηγουμένου}\\ \text{λήμματος}}}{=} \frac{\alpha+(-\alpha)}{\beta} = \frac{0}{\beta} = \frac{0}{1}$, σύμφωνα και με το **(iii)** του προηγουμένου λήμματος. Άρα κάθε κλάσμα έχει αντίθετο.
(v) Έστω $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta \in R$ με $\beta\delta\zeta \neq 0$. Τότε $\frac{\alpha}{\beta} \cdot \left(\frac{\gamma}{\delta} \cdot \frac{\varepsilon}{\zeta}\right) = \frac{\alpha}{\beta} \cdot \frac{\gamma\varepsilon}{\delta\zeta} = \frac{\alpha(\gamma\varepsilon)}{\beta(\delta\zeta)} = \frac{(\alpha\gamma)\varepsilon}{(\beta\delta)\zeta} = \frac{\alpha\gamma}{\beta\delta} \cdot \frac{\varepsilon}{\zeta} =$
$= \left(\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta}\right) \cdot \frac{\varepsilon}{\zeta}$ και η προσεταιριστικότητα του πολλαπλασιασμού αποδείχτηκε.
(vi) Έστω $\alpha, \beta, \gamma, \delta \in R$ με $\beta\delta \neq 0$. Τότε έχουμε: $\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} = \frac{\alpha\gamma}{\beta\delta} = \frac{\gamma\alpha}{\delta\beta} = \frac{\gamma}{\delta} \cdot \frac{\alpha}{\beta}$ και η μεταθετικότητα του πολλαπλασιασμού αποδείχθηκε.
(viii) Για την επιμεριστικότητα του πολλαπλασιασμού ως προς τη διαίρεση αρκεί να αποδείξουμε ότι $\frac{\alpha}{\beta} \cdot \left(\frac{\gamma}{\delta} + \frac{\varepsilon}{\zeta}\right) = \frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta} + \frac{\alpha}{\beta} \cdot \frac{\varepsilon}{\zeta}$, για κάθε $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta \in R$ με $\beta\delta\zeta \neq 0$. Και τούτο λόγω της αντιμεταθετικότητας της πρόσθεσης και του πολλαπλασιασμού.
Έχουμε: $\frac{\alpha}{\beta} \cdot \left(\frac{\gamma}{\delta} + \frac{\varepsilon}{\zeta}\right) = \frac{\alpha}{\beta} \cdot \frac{\gamma\zeta+\delta\varepsilon}{\delta\zeta} = \frac{\alpha(\gamma\zeta+\delta\varepsilon)}{\beta\delta\zeta} = \frac{\alpha\gamma\zeta+\alpha\varepsilon\delta}{\beta\delta\zeta}$. Σύμφωνα με το **(ii)** του

προηγουμένου λήμματος, το τελευταίο ισούται με $\frac{\alpha\gamma\zeta}{\beta\delta\zeta}+\frac{\alpha\varepsilon\delta}{\beta\delta\zeta}$ και αυτό με τη σειρά του, βάσει του **(i)** του προηγουμένου λήμματος, με $\frac{\alpha\gamma}{\beta\delta}+\frac{\alpha\varepsilon}{\beta\zeta}=\frac{\alpha}{\beta}\cdot\frac{\gamma}{\delta}+\frac{\alpha}{\beta}\cdot\frac{\varepsilon}{\zeta}$.

(ix) Το $\frac{1}{1}$ είναι το μοναδιαίο στοιχείο, καθόσον $\frac{\alpha}{\beta}\cdot\frac{1}{1}=\frac{\alpha\cdot 1}{\beta\cdot 1}=\frac{\alpha}{\beta}$, όπου $\alpha,\beta\in R$ με $\beta\neq 0$.

(x) Τα μη μηδενικά στοιχεία του $\mathbb{K}$ είναι τα κλάσματα $\frac{\alpha}{\beta}$, όπου $\alpha\beta\neq 0$. Πράγματι, $\frac{\alpha}{\beta}=\frac{0}{1}\Leftrightarrow \alpha\cdot 1=0\cdot\beta=0$, όπου φυσικά $\beta\neq 0$. Επομένως, αν $\alpha\beta\neq 0$, τότε το κλάσμα $\frac{\alpha}{\beta}$ δεν είναι το μηδενικό. Βάσει του **(i)**, του προηγουμένου λήμματος, έχουμε: $\frac{\alpha}{\beta}\cdot\frac{\beta}{\alpha}=\frac{\alpha\beta}{\alpha\beta}=\frac{1\cdot\alpha\beta}{1\cdot\alpha\beta}=\frac{1}{1}$, δηλαδή κάθε μη μηδενικό κλάσμα αντιστρέφεται. ■

ΠΡΟΤΑΣΗ 1.38. Έστω R ακέραια περιοχή και $\mathbb{K}$ το σώμα πηλίκων της. Τότε υπάρχει μια εμφύτευση (μονομορφισμός δακτυλίων) $\varphi: R\hookrightarrow\mathbb{K}$. Έτσι μπορούμε να θεωρήσουμε την R ως υποδακτύλιο του $\mathbb{K}$.
Επίσης, αν $\frac{\alpha}{\beta}\in\mathbb{K}\ \big(\beta\neq 0\big)$, τότε $\frac{\alpha}{\beta}=\varphi(\alpha)\big(\varphi(\beta)\big)^{-1}$, γεγονός που βρίσκεται σε συμφωνία με τη διαίρεση ενός στοιχείου με ένα μη μηδενικό.

ΑΠΟΔΕΙΞΗ: Θέτουμε $\varphi(\alpha)=\frac{\alpha}{1}$, για κάθε $\alpha\in R$. Τότε $\varphi(\alpha+\beta)=\frac{\alpha+\beta}{1}=\frac{\alpha}{1}+\frac{\beta}{1}=\varphi(\alpha)+\varphi(\beta)$, σύμφωνα και με το **(ii)** του προηγουμένου λήμματος. Επίσης $\varphi(\alpha\beta)=\frac{\alpha\beta}{1}=$ $=\frac{\alpha\cdot\beta}{1\cdot 1}=\frac{\alpha}{1}\cdot\frac{\beta}{1}=\varphi(\alpha)\varphi(\beta)$. Ακόμη, $\varphi(1)=\frac{1}{1}=1_{\mathbb{K}}$. Τέλος, έστω $\alpha\in\mathrm{Ker}\varphi$, δηλαδή $\varphi(\alpha)=\frac{\alpha}{1}=\frac{0}{1}$. Τότε $\alpha=\alpha\cdot 1=0\cdot 1=0$. Άρα η φ είναι μονομορφισμός.
Τέλος, έστω $\beta\neq 0$. Τότε $1_{\mathbb{K}}\underset{\substack{\textbf{(iv)}\ \text{προηγου-}\\ \text{μένου λήμματος}}}{=}\frac{\beta}{\beta}=\frac{\beta}{1}\cdot\frac{1}{\beta}=\varphi(\beta)\cdot\frac{1}{\beta}$. Επομένως $\frac{1}{\beta}=\big(\varphi(\beta)\big)^{-1}$. Κατά συνέπεια, $\frac{\alpha}{\beta}=\frac{\alpha}{1}\cdot\frac{1}{\beta}=\varphi(\alpha)\big(\varphi(\beta)\big)^{-1}$. ■

Το σώμα πηλίκων μιας ακέραιας περιοχής είναι το μικρότερο σώμα που την περιέχει. Πιο συγκεκριμένα:

ΠΡΟΤΑΣΗ 1.39. Έστω R ακέραια περιοχή και $\mathbb{K}$ το σώμα πηλίκων της. Αν $\mathbb{F}$ είναι ένα σώμα και $\tau: R\hookrightarrow\mathbb{F}$ μια εμφύτευση (μονομορφισμός) της R στο $\mathbb{F}$, τότε η τ επεκτείνεται κατά μοναδικό τρόπο σε μια εμφύτευση $\bar{\tau}:\mathbb{K}\hookrightarrow\mathbb{F}$, δηλαδή $\bar{\tau}\circ\varphi=\tau$.

ΑΠΟΔΕΙΞΗ: Μέσω της εμφύτευσης $\varphi: R\hookrightarrow\mathbb{K}$ ταυτίζουμε το $x\in R$ με το $\frac{x}{1}\in\mathbb{K}$. Επομένως θα πρέπει $\bar{\tau}\Big(\frac{x}{1}\Big)=(\bar{\tau}\circ\varphi)(x)=\tau(x)$, για κάθε $x\in R$. Αν $x\neq 0$, τότε θα πρέπει $1_{\mathbb{F}}=\tau(1_R)=$ $=\bar{\tau}(1_{\mathbb{K}})=\bar{\tau}\Big(\frac{1}{1}\Big)=\bar{\tau}\Big(\frac{x}{1}\cdot\frac{1}{x}\Big)=\bar{\tau}\Big(\frac{x}{1}\Big)\bar{\tau}\Big(\frac{1}{x}\Big)=\tau(x)\bar{\tau}\Big(\frac{1}{x}\Big)$. Επομένως $\bar{\tau}\Big(\frac{1}{x}\Big)=\big(\tau(x)\big)^{-1}$.
Κατά συνέπεια θα έχουμε αναγκαστικά $\bar{\tau}\Big(\frac{\alpha}{\beta}\Big)=\bar{\tau}\Big(\frac{\alpha}{1}\cdot\frac{1}{\beta}\Big)=\bar{\tau}\Big(\frac{\alpha}{1}\Big)\bar{\tau}\Big(\frac{1}{\beta}\Big)=\tau(\alpha)\big(\tau(\beta)\big)^{-1}$, όπου φυσικά $\beta\neq 0$.
Ορίζουμε λοιπόν $\bar{\tau}:\mathbb{K}\hookrightarrow\mathbb{F}$ ως εξής: $\bar{\tau}\Big(\frac{\alpha}{\beta}\Big)=\tau(\alpha)\big(\tau(\beta)\big)^{-1}$, για κάθε $\frac{\alpha}{\beta}\in\mathbb{K}$.
Αν $\frac{\alpha}{\beta}=\frac{\gamma}{\delta}$, δηλαδή $\alpha\delta=\gamma\beta$, τότε $\tau(\alpha\delta)=\tau(\gamma\beta)\Leftrightarrow\tau(\alpha)\tau(\delta)=\tau(\gamma)\tau(\beta)\Leftrightarrow\tau(\alpha)\big(\tau(\beta)\big)^{-1}=$

$= \tau(\gamma)\big(\tau(\delta)\big)^{-1}$, δηλαδή η $\bar{\tau}$ είναι καλά ορισμένη.
Τώρα, $\bar{\tau}\Big(\frac{\alpha}{\beta}+\frac{\gamma}{\delta}\Big) = \bar{\tau}\Big(\frac{\alpha\delta+\gamma\beta}{\beta\delta}\Big) = \tau(\alpha\delta+\gamma\beta)\big(\tau(\beta\delta)\big)^{-1} = \big(\tau(\alpha)\tau(\delta)+\tau(\gamma)\tau(\beta)\big)\big(\tau(\beta)\tau(\delta)\big)^{-1} =$
$= \big(\tau(\alpha)\tau(\delta) + \tau(\gamma)\tau(\beta)\big)\big(\tau(\beta)\big)^{-1}\big(\tau(\delta)\big)^{-1} = \tau(\alpha)\cancel{\tau(\delta)}\big(\tau(\beta)\big)^{-1}\cancel{\big(\tau(\delta)\big)^{-1}} + \tau(\gamma)\cancel{\tau(\beta)}\cancel{\big(\tau(\beta)\big)^{-1}}$
$\big(\tau(\delta)\big)^{-1} = \tau(\alpha)\big(\tau(\beta)\big)^{-1} + \tau(\gamma)\big(\tau(\delta)\big)^{-1} = \bar{\tau}\Big(\frac{\alpha}{\beta}\Big) + \bar{\tau}\Big(\frac{\gamma}{\delta}\Big)$,
$\bar{\tau}\Big(\frac{\alpha}{\beta}\cdot\frac{\gamma}{\delta}\Big) = \bar{\tau}\Big(\frac{\alpha\gamma}{\beta\delta}\Big) = \tau(\alpha\gamma)\big(\tau(\beta\delta)\big)^{-1} = \tau(\alpha)\tau(\gamma)\big(\tau(\beta)\big)^{-1}\big(\tau(\delta)\big)^{-1} = \tau(\alpha)\big(\tau(\beta)\big)^{-1}$.
$\tau(\gamma)\big(\tau(\delta)\big)^{-1} = \bar{\tau}\Big(\frac{\alpha}{\beta}\Big)\cdot\bar{\tau}\Big(\frac{\gamma}{\delta}\Big)$ και τέλος $\overline{\tau}\Big(\frac{1}{1}\Big) = \tau(1)\big(\tau(1)\big)^{-1} = 1_{\mathbb{F}}\cdot 1_{\mathbb{F}}^{-1} = 1_{\mathbb{F}}$.
Έστω $\frac{\alpha}{\beta} \in \mathrm{Ker}\bar{\tau}$. Τότε $\bar{\tau}\Big(\frac{\alpha}{\beta}\Big) = \tau(\alpha)\tau(\beta)^{-1} = 0_{\mathbb{K}} \Rightarrow \tau(\alpha) = 0 \underset{\substack{\tau \text{ μονόμορ-}\\ \text{φισμός}}}{\Rightarrow} \alpha = 0 \Rightarrow \frac{\alpha}{\beta} = \frac{0}{\beta} = \frac{0}{1} =$
$= 0_{\mathbb{K}}$. ■

***Άσκηση* 1.1.** Έστω $\mathbb{K}$ σώμα, άρα ακέραια περιοχή. Κατασκευάζουμε το σώμα πηλίκων του $\mathbb{K}$ σύμφωνα με την προηγούμενη κατασκευή. Έστω αυτό το $\mathbb{F}$. Δείξτε ότι, όπως αναμένεται, $\mathbb{F} \cong \mathbb{K}$.

***Άσκηση* 1.2.** Έστω R ένας (μη τετριμμένος μοναδιαίος μεταθετικός) δακτύλιος. Δείξτε ότι ο R είναι σώμα αν και μόνον αν το μηδενικό ιδεώδες $\{0\}$ είναι μέγιστο.

***Άσκηση* 1.3.** Έστω $\mathrm{I} \trianglelefteq R$. Θεωρούμε το υποσύνολο του $I[x]$ του πολυωνυμικού δακτυλίου $R[x]$ με $I[x] = \{\sum_{i=0}^{n}\alpha_i x^i \mid n \geq 0 \text{ και } \alpha_i \in I, \text{ για κάθε } i = 0,\ldots,n\}$.
(i) Δείξτε ότι $I[x] \trianglelefteq R[x]$.
(ii) Δείξτε ότι υπάρχει ισομορφισμός $R[x]\big/_{I[x]} \cong \Big(R\Big/_{I}\Big)[x]$.

Και μια άσκηση από τη μεταθετική άλγεβρα.

***Άσκηση* 1.4.** Έστω R μοναδιαίος μεταθετικός δακτύλιος και I ιδεώδες αυτού. Θεωρούμε το σύνολο J των στοιχείων x με την ιδιότητα $x^n \in I$, για κάποιον θετικό ακέραιο n, ο οποίος εξαρτάται από το x. Δείξτε ότι $J \trianglelefteq R$. Το J λέγεται **ριζικό του** I και συμβολίζεται με $\boldsymbol{\sqrt{I}}$.

Κεφάλαιο 2

Παραγοντοποίηση σε Ακέραιες Περιοχές

2.1 Συντροφικά Στοιχεία-Πρώτα και Ανάγωγα Στοιχεία

ΟΡΙΣΜΟΣ 2.1. Έστω R μοναδιαίος μεταθετικός δακτύλιος. Αν $\alpha, \beta \in R$, θα γράφουμε $\boldsymbol{\alpha \mid \beta}$ και θα λέμε ότι το $\boldsymbol{\alpha}$ **διαιρεί το** $\boldsymbol{\beta}$ **αν και μονον αν υπάρχει** $\boldsymbol{r \in R}$ **τέτοιο, ώστε** $\boldsymbol{\beta = r \cdot \alpha}$.

ΠΡΟΤΑΣΗ 2.2. Ισχύει η ισοδυναμία: $\alpha \mid \beta \Leftrightarrow (\beta) \subseteq (\alpha)$.
ΑΠΟΔΕΙΞΗ: $\alpha \mid \beta \Leftrightarrow \beta = r \cdot \alpha$, για κάποιο $r \in R$, το οποίο είναι ισοδύναμο με το $\beta \in (\alpha) \Leftrightarrow$ $\Leftrightarrow (\beta) \subseteq (\alpha)$. ■

Παρατηρείστε ότι η σχέση του «διαιρείν» αντιστρέφει τη διάταξη των κυρίων ιδεωδών.

ΟΡΙΣΜΟΣ 2.3. Δύο στοιχεία $\alpha, \beta \in R$ λέγονται **συντροφικά** $\big($associated$\big)$ αν και μόνον αν $\alpha \mid \beta$ και $\beta \mid \alpha$, ισοδύναμα $(\alpha) = (\beta)$. Γράφουμε τότε $\alpha \sim \beta$.

ΠΡΟΤΑΣΗ 2.4. Η σχέση $\sim$ είναι σχέση ισοδυναμίας στον δακτύλιο R.
ΑΠΟΔΕΙΞΗ: Άμεση, από την ισοδυναμία $\alpha \sim \beta \Leftrightarrow (\alpha) = (\beta)$. ■

Γενικά, μπορούμε εύκολα να αποδείξουμε ότι σε έναν μοναδιαίο μεταθετικό δακτύλιο R ισχύουν τα εξής:
(i) Αν $\alpha \sim \beta$ και $\beta \mid \gamma$, τότε και $\alpha \mid \gamma$.
(ii) Αν $\alpha \mid \beta$ και $\beta \sim \gamma$, τότε και $\alpha \mid \gamma$.
$\Big($**(i)** Έστω $\alpha \sim \beta$ και $\beta \mid \gamma$. Τότε $\alpha \mid \beta$ και $\beta \mid \gamma$. Άρα $\alpha \mid \gamma$. **(ii)** Έστω $\alpha \mid \beta$ και $\beta \sim \gamma$. Τότε και $\beta \mid \gamma$. Επομένως $\alpha \mid \gamma\Big)$.

ΠΡΟΤΑΣΗ 2.5. Έστω R ακέραια περιοχή και $\alpha, \beta \in R \setminus \{0\}$. Τότε $\alpha \sim \beta$ αν και μόνον αν υπάρχει αντιστρέψιμο στοιχείο $u \in R$ τέτοιο, ώστε $\beta = u\alpha$.
ΑΠΟΔΕΙΞΗ: $\alpha \mid \beta \Leftrightarrow \beta = u\alpha$, για κάποιο $u \in R$. Επίσης, $\beta \mid \alpha \Leftrightarrow \alpha = v\beta$, για κάποιο $v \in R$. Επομένως $\beta = u\alpha = uv\beta \Rightarrow \beta(1 - uv) = 0$. Εφόσον R ακέραια περιοχή και $\beta \neq 0$, έπεται ότι $uv = 1$, δηλαδή το u είναι αντιστρέψιμο με $u^{-1} = v$.
Αντιστρόφως, έστω $\beta = u\alpha$, όπου $u \in R$ αντιστρέψιμο. Τότε $\alpha = u^{-1}\beta$. Επομένως ισχύουν ταυτόχρονα οι σχέσεις $\alpha \mid \beta$ και $\beta \mid \alpha$. Επομένως $\alpha \sim \beta$. ■

ΟΡΙΣΜΟΣ 2.6. Έστω R μοναδιαίος μεταθετικός δακτύλιος. Ένα μη μηδενικό και μη αντιστρέψιμο στοιχείο $p \in R$, δηλαδή $p \in R \setminus \big(U(R) \cup \{0\}\big)$, λέγεται **ανάγωγο** αν και μόνον αν από κάθε σχέση της μορφής $p = \alpha\beta$ προκύπτει ότι κάποιο από τα $\alpha, \beta \in R$ είναι αντιστρέψιμο.

ΠΡΟΤΑΣΗ 2.7. Έστω R ακέραια περιοχή και $p, q \in R$ ανάγωγα. Αν $p \mid q$, τότε τα p και q είναι συντροφικά.
ΑΠΟΔΕΙΞΗ: Έχουμε $p \mid q \Leftrightarrow q = up$, για κάποιο $u \in R$. Επειδή το q είναι ανάγωγο, κάποιο από τα u και p είναι αντιστρέψιμο. Αφού το p είναι ανάγωγο, δεν είναι αντιστρέψιμο. Επομένως το u είναι αντιστρέψιμο και άρα $q = up \sim p$. Το αντίστροφο είναι προφανές. Αν $p \sim q$, τότε $q = up$, για κάποιο αντιστρέψιμο στοιχείο $u \in R$ και $p = u^{-1}q$. Επομένως $p \mid q$ και $q \mid p$. ■

ΟΡΙΣΜΟΣ 2.8. Έστω R μοναδιαίος μεταθετικός δακτύλιος. Ένα μη μηδενικό και μη αντιστρέψιμο στοιχείο $p \in R$ λέγεται **πρώτο** αν από κάθε σχέση της μορφής $p \mid \alpha\beta$, όπου $\alpha, \beta \in R$ προκύπτει ότι $p \mid \alpha$ ή $p \mid \beta$.

ΠΟΡΙΣΜΑ 2.9. Έστω R ακέραια περιοχή και $p \in R \setminus \big(U(R) \cup \{0\}\big)$. Τότε το p είναι πρώτο αν και μόνον αν το κύριο ιδεώδες (p) είναι πρώτο.
ΑΠΟΔΕΙΞΗ: Έστω p πρώτο. Τότε $\alpha\beta \in (p) \Leftrightarrow p \mid \alpha\beta \underset{p \text{ πρώτο}}{\Leftrightarrow} \big(p \mid \alpha \text{ ή } p \mid \beta\big) \Leftrightarrow \big(\alpha \in (p) \text{ ή } \beta \in$ $\in (p)\big)$. Επομένως το (p) είναι πρώτο. Αντιστρόφως, έστω ότι το (p) είναι πρώτο και $p \mid \alpha\beta$, όπου $\alpha, \beta \in R$. Τότε $\alpha\beta \in (p) \underset{(p) \text{ πρώτο}}{\Leftrightarrow} \big(\alpha \in (p) \text{ ή } \beta \in (p)\big) \Leftrightarrow \big(p \mid \alpha \text{ ή } p \mid \beta\big)$. Επομένως το p είναι πρώτο. ■

Στα επόμενα θα ασχοληθούμε μόνον με ακέραιες περιοχές.

ΠΡΟΤΑΣΗ 2.10. Έστω R ακέραια περιοχή και $p \in R \setminus \big(U(R) \cup \{0\}\big)$. Αν το p είναι πρώτο, τότε είναι και ανάγωγο στην R.
ΑΠΟΔΕΙΞΗ: Έστω p πρώτο και $p = \alpha\beta$, όπου $\alpha, \beta \in R$. Τότε $p \mid p = \alpha\beta$ και, επειδή το p είναι πρώτο, θα έχουμε $p \mid \alpha$ ή $p \mid \beta$. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $p \mid \alpha \Leftrightarrow \alpha = up$, για κάποιο $u \in R$. Τότε, $p = \alpha\beta = up\beta \Leftrightarrow p(1 - u\beta) = 0 \underset{\substack{R \text{ ακέραια περιοχή} \\ \text{και } p \neq 0}}{\Leftrightarrow} u\beta = 1 \Rightarrow$

$\Rightarrow \beta$ αντιστρέψιμο. ■

Το αντίστροφο της προηγουμένης πρότασης δεν ισχύει γενικά.

ΠΑΡΑΔΕΙΓΜΑ 2.11. Θεωρούμε την ακέραια περιοχή

$$\mathbb{Z}[\mathrm{i}\sqrt{5}] = \{\alpha + \beta\mathrm{i}\sqrt{5} \mid \alpha, \beta \in \mathbb{Z}\}.$$

Εύκολα μπορεί να δείξει κάποιος ότι ο $\mathbb{Z}[\mathrm{i}\sqrt{5}]$ είναι δακτύλιος ως προς τη συνηθισμένες πράξεις της πρόσθεσης και του πολλαπλασιασμού και είναι επίσης ακέραια περιοχή, αφού περιέχεται στο σώμα $\mathbb{C}$ των μιγαδικών αριθμών.
Έστω $N(\alpha + \beta\mathrm{i}\sqrt{5}) = \alpha^2 + 5\beta^2$, δηλαδή το τετράγωνο του μέτρου του μιγαδικού $\alpha + \beta\mathrm{i}\sqrt{5}$. Άρα, για κάθε $x \in \mathbb{Z}[\mathrm{i}\sqrt{5}]$ έχουμε $N(x) = |x|^2 = x\bar{x}$. Επομένως $N(xy) = |xy|^2 = |x|^2|y|^2 =$ $= N(x)N(y)$.
Ποια είναι τώρα τα αντιστρέψιμα στοιχεία της $\mathbb{Z}[\mathrm{i}\sqrt{5}]$; Έστω $x = \alpha + \beta\mathrm{i}\sqrt{5}$ ένα αντιστρέψιμο στοιχείο. Τότε υπάρχει $y \in \mathbb{Z}[\mathrm{i}\sqrt{5}]$ τέτοιο, ώστε $1 = xy$. Επομένως $1 = N(1) = N(xy) =$ $N(x)N(y)$, όπου $N(x), N(y)$ μη αρνητικοί, άρα εδώ θετικοί ακέραιοι. Συνεπώς $1 = N(x) =$ $\alpha^2 + 5\beta^2$. Αν $\beta \neq 0$, τότε $N(x) = \alpha^2 + 5\beta^2 \geq 5 > 1$. Επομένως $\beta = 0$ και συνεπώς $x = \alpha$ με $\alpha^2 = 1 \Leftrightarrow \alpha = \pm 1$. Είναι επίσης σαφές ότι τα στοιχεία 1, -1 είναι αντιστρέψιμα στο $\mathbb{Z}[\mathrm{i}\sqrt{5}]$. Επομένως τα ± 1, δηλαδή αντιστρέψιμα στοιχεία του $\mathbb{Z}[\mathrm{i}\sqrt{5}]$ είναι ακριβώς αυτά τα στοιχεία x με $N(x) = 1$.
Τώρα, το 2 και το 3 είναι ανάγωγα στοιχεία στην περιοχή $\mathbb{Z}[\mathrm{i}\sqrt{5}]$.
Πράγματι, αν $2 = (\alpha + \beta\mathrm{i}\sqrt{5})(\gamma + \delta\mathrm{i}\sqrt{5})$, όπου $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ και $\alpha + \mathrm{i}\beta\sqrt{5}, \gamma + \delta\mathrm{i}\sqrt{5} \neq \pm 1$,

τότε $4 = N(\alpha + \mathbf{i}\beta\sqrt{5})N(\gamma + \delta\mathbf{i}\sqrt{5}) = (\alpha^2 + 5\beta^2)(\gamma^2 + 5\delta^2)$. Εφόσον $\alpha + \mathbf{i}\beta\sqrt{5}, \gamma + \delta\mathbf{i}\sqrt{5}$ μη αντιστρέψιμα, $N(\alpha + \mathbf{i}\beta\sqrt{5}) > 1$ και $N(\gamma + \delta\mathbf{i}\sqrt{5}) > 1$. Άρα $N(\alpha + \mathbf{i}\beta\sqrt{5}) = N(\gamma + \delta\mathbf{i}\sqrt{5}) = 2$. Αν $\beta \neq 0$, τότε $N(\alpha + \beta\mathbf{i}\sqrt{5}) = \alpha^2 + 5\beta^2 \geq 5 > 2$, άτοπο. Άρα $\beta = 0$ και $2 = \alpha^2$, άτοπο και πάλι. Με την ίδια λογική προκύπτει ότι και το 3 είναι ανάγωγο στην $\mathbb{Z}[\mathbf{i}\sqrt{5}]$.
Παρατηρούμε τώρα ότι $2 \cdot 3 = 6 = (1+\mathbf{i}\sqrt{5})(1-\mathbf{i}\sqrt{5}) \Rightarrow 2 \mid (1+\mathbf{i}\sqrt{5})(1-\mathbf{i}\sqrt{5})$. Αλλά $2 \nmid 1 \pm \mathbf{i}\sqrt{5}$. Σε αντίθετη περίπτωση θα υπήρχε $\kappa + \lambda\mathbf{i}\sqrt{5}$ $\big(\kappa, \lambda \in \mathbb{Z}\big)$ με $1 \pm \mathbf{i}\sqrt{5} = 2(\kappa + \lambda\mathbf{i}\sqrt{5}) = 2\kappa + 2\lambda\mathbf{i}\sqrt{5}$. Αλλά τότε $1 = 2\kappa \Rightarrow 2 \mid 1$, άτοπο.

ΕΦΑΡΜΟΓΗ 2.12. Αν $n \in \mathbb{Z}$ είναι μη τέλειο τετράγωνο, τότε το 2 δεν είναι πρώτο στην περιοχή $\mathbb{Z}[\sqrt{n}] = \{\alpha + \beta\sqrt{n} \mid \alpha, \beta \in \mathbb{Z}\}$.
ΑΠΟΔΕΙΞΗ: Παρατηρούμε ότι $2 \mid n(n-1) = n^2 - n = n^2 - \big(\sqrt{n}\big)^2 = (n + \sqrt{n})(n - \sqrt{n})$. Αν τώρα $2 \mid n \pm \sqrt{n}$, τότε θα υπήρχε $\kappa + \lambda\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$, με $2(\kappa + \lambda\sqrt{n}) = 2\kappa + 2\lambda\sqrt{n} = n \pm \sqrt{n}$. Αλλά τότε $2\lambda = \pm 1$, άτοπο. ■

ΠΡΟΤΑΣΗ 2.13. Έστω R ακέραια περιοχή και $p \in R \setminus \big(U(R) \cup \{0\}\big)$.
(i) Αν το p είναι ανάγωγο και $q \sim p$, τότε και το q είναι ανάγωγο.
(ii) Αν το p είναι πρώτο και $q \sim p$, τότε και το q είναι πρώτο.
ΑΠΟΔΕΙΞΗ: (i) Έστω p ανάγωγο και $q = up$, όπου $u \in U(R)$. Θα δείξουμε ότι και το q είναι ανάγωγο.
Αν $q = \alpha\beta$, τότε $up = \alpha\beta$. Άρα $p = (u^{-1}\alpha)\beta$. Επομένως κάποιο από τα $u^{-1}\alpha, \beta \in R$ είναι αντιστρέψιμο. Αν το β είναι αντιστρέψιμο έχει καλώς. Αλλιώς το $u^{-1}\alpha$ είναι αντιστρέψιμο, οπότε $ru^{-1}\alpha = 1$, για κάποιο $r \in R$. Άρα το α είναι αντιστρέψιμο με αντίστροφο το ru^{-1}.
(ii) Έστω p πρώτο και $q = up$, όπου $u \in U(R)$. Υποθέτουμε ότι $q \mid \alpha\beta$. Επειδή $p \mid q = up$, έπεται ότι $p \mid \alpha\beta \Rightarrow p \mid \alpha$ ή $p \mid \beta$. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $p \mid \alpha$, δηλαδή $\alpha = rp$, για κάποιο $r \in R$. Τότε $\alpha = ru^{-1}(up) = ru^{-1}q \Rightarrow q \mid \alpha$. ■

2.2 Περιοχές Μοναδικής Παραγοντοποίησης

2.2.1 Ανάλυση σε Γινόμενο Ανάγωγων Παραγόντων

ΟΡΙΣΜΟΣ 2.14. Έστω R ακέραια περιοχή. Η R λέγεται **Περιοχή Μοναδικής Παραγοντοποίησης** $\big($Unique Factorization Domain$\big)$ αν και μόνον αν ισχύουν τα παρακάτω:
1) Κάθε μη μηδενικό και μη αντιστρέψιμο στοιχείο $\alpha \in R$ γράφεται ως γινόμενο αναγώγων στοιχείων.
2) Η γραφή ενός τέτοιου α είναι μοναδική, υπό την έννοια ότι αν

$$\alpha = p_1 p_2 \cdots p_\kappa = q_1 q_2 \cdots q_\lambda,$$

όπου p_i, q_j ανάγωγα, για κάθε $i = 1, \ldots, \kappa$ και $j = 1, \ldots, \lambda$, τότε $\kappa = \lambda$ και $\big($αν ανάγκη αλλάζοντας την αρίθμηση των $q_1, \ldots, q_\kappa\big)$ έχουμε $p_i \sim q_i$, για κάθε $i = 1, \ldots, \kappa$.

Από την προηγούμενη πρόταση συνάγουμε ότι το πλήθος των παραγόντων στην ανάλυση ενός μη μηδενικού και μη αντιστρεψίμου στοιχείου της $\alpha \in R$ εξαρτάται μόνον από το στοιχείο αυτό. Αν λοιπόν $\alpha = p_1 p_2 \cdots p_\kappa$ είναι η ανάλυση του α σε γινόμενο αναγώγων παραγόντων, θέτουμε $\lambda(\alpha) = \kappa$. Αν τέλος το $\alpha \in R$ είναι αντιστρέψιμο, τότε θέτουμε $\lambda(\alpha) = 0$. Είναι σαφές ότι για κάθε $\alpha, \beta \in R \setminus \{0\}$ ισχύει

$$\lambda(\alpha\beta) = \lambda(\alpha) + \lambda(\beta).$$

Πράγματι, αν και το α και το β είναι αντιστρέψιμα, τότε και το γινόμενό τους $\alpha\beta$ είναι αντιστρέψιμο. Άρα $\lambda(\alpha\beta) = 0 = 0 + 0 = \lambda(\alpha) + \lambda(\beta)$. Αν ένα από τα δύο είναι αντιστρέψιμο, π.χ. το α και το β δεν είναι, τότε $\beta = p_1 p_2 \cdots p_\kappa$, όπου p_i ανάγωγο, για κάθε $i = 1, \ldots, \kappa$. Τότε $\alpha\beta = (\alpha p_1)p_2 \cdots p_\kappa$ και το αp_1 είναι ανάγωγο, ως συντροφικό του p_1. Άρα $\lambda(\alpha\beta) = \kappa = 0 + \kappa = = \lambda(\alpha) + \lambda(\beta)$. Τέλος, αν $\alpha = p_1 \cdots p_\mu$ και $\beta = q_1 \cdots q_\nu$ μη αντιστρέψιμα, όπου p_i, q_j ανάγωγα, για κάθε $i = 1, \ldots, \mu$ και $j = 1, \ldots, \nu$, τότε $\lambda(\alpha\beta) = \lambda(p_1 \cdots p_\mu q_1 \cdots q_\nu) = \mu + \nu = \lambda(\alpha) + \lambda(\beta)$. Την τιμή $\lambda(\alpha)$ όπου $\alpha \neq 0_R$, θα την ονομάζουμε **μήκος του α**.

ΠΡΟΤΑΣΗ 2.15. Έστω R περιοχή μοναδικής παραγοντοποίησης. Τότε ισχύουν οι ακόλουθες συνθήκες-κριτήρια:
Κριτήριο 1: Κάθε ανάγωγο στοιχείο $p \in R$ είναι πρώτο.
Κριτήριο 2: Κάθε αύξουσα ακολουθία κυρίων ιδεωδών είναι τελικά σταθερή, δηλαδή αν
$$(\alpha_1) \subseteq (\alpha_2) \subseteq (\alpha_3) \subseteq \ldots,$$
τότε υπάρχει θετικός ακέραιος n τέτοιος, ώστε $(\alpha_n) = (\alpha_{n+1}) = (\alpha_{n+2}) = \cdots$
ΑΠΟΔΕΙΞΗ: Κριτήριο 1: Έστω p ανάγωγο στοιχείο και $\alpha, \beta \in R$ με $p \mid \alpha\beta$.
Αν κάποιο από τα α, β είναι μηδέν, τότε η περίπτωση είναι τετριμμένη. Έστω $\alpha\beta \neq 0$. Τότε υπάρχει $r \in R \setminus \{0\}$ τέτοιο, ώστε $rp = \alpha\beta$. Έστω $x = rp = \alpha\beta$. Παρατηρούμε ότι το p (ή κάποιο συντροφικό του, στην περίπτωση που το r είναι αντιστρέψιμο) εμφανίζεται στην ανάλυση του x σε γινόμενο αναγώγων στοιχείων. Επειδή η R είναι περιοχή μοναδικής παραγοντοποίησης, το p (ή κάποιο συντροφικό του) θα εμφανίζεται και στο δεξιό μέλος της σχέσης $rp = \alpha\beta$, ως αποτέλεσμα της ανάλυσης είτε του α είτε του β σε γινόμενο αναγώγων στοιχείων. Επομένως το p θα διαιρεί είτε το α είτε το β.
Κριτήριο 2: Επειδή $(\alpha_i) \subseteq (\alpha_{i+1}) \Leftrightarrow \alpha_{i+1} \mid \alpha_i$, θα έχουμε έχουμε $\alpha_i = \alpha_{i+1}\beta_{i+1}$, για κάποιο $\beta_{i+1} \neq 0$. Επομένως $\lambda(\alpha_i) = \lambda(\alpha_{i+1}\beta_{i+1}) = \lambda(\alpha_{i+1}) + \lambda(\beta_{i+1}) \geq \lambda(\alpha_{i+1})$, για κάθε $i = 1, 2, \ldots$ Η ακολουθία $\lambda(\alpha_i)$ είναι λοιπόν μια φθίνουσα ακολουθία μη αρνητικών ακεραίων. Αυτή θα έχει ελάχιστο στοιχείο $\lambda(\alpha_n) = \lambda(\alpha_{n+1}) = \lambda(\alpha_{n+2}) = \cdots$ Αλλά για κάθε $i \geq n$ έχουμε $\lambda(\alpha_i) = \lambda(\alpha_{i+1}\beta_{i+1}) = \lambda(\alpha_{i+1}) + \lambda(\beta_{i+1})$, οπότε $\lambda(\beta_{i+1}) = 0$, δηλαδή το β_{i+1} είναι αντιστρέψιμο, για κάθε $i = n, n+1, n+2, \ldots$ και άρα $(\alpha_{i+1}) = (\alpha_i)$, για κάθε $i = n, n+1, n+2, \ldots$ ■

Θα αποδείξουμε ότι ισχύει και το αντίστροφο της προηγούμενης πρότασης. Πιο συγκεκριμένα, έχουμε το επόμενο θεώρημα:

ΘΕΩΡΗΜΑ 2.16. Έστω R ακέραια περιοχή. Τότε η R είναι περιοχή μοναδικής παραγοντοποίησης αν και μόνον αν πληροί τα κριτήρια της προηγούμενης πρότασης:
Κριτήριο 1: Κάθε ανάγωγο στοιχείο $p \in R$ είναι πρώτο.
Κριτήριο 2: Κάθε αύξουσα ακολουθία κυρίων ιδεωδών είναι τελικά σταθερή, δηλαδή αν
$$(\alpha_1) \subseteq (\alpha_2) \subseteq (\alpha_3) \subseteq \ldots,$$
τότε υπάρχει θετικός ακέραιος n τέτοιος, ώστε $(\alpha_n) = (\alpha_{n+1}) = (\alpha_{n+2}) = \cdots$
ΑΠΟΔΕΙΞΗ: Πρώτα θα αποδείξουμε ότι κάθε μη μηδενικό και μη αντιστρέψιμο στοιχείο αναλύεται σε γινόμενο ανάγωγων στοιχείων.
Προχωράμε με απαγωγή σε άτοπο. Έστω $\alpha_0 \in R \setminus \big(U(R) \cup \{0\}\big)$. Το α_0 δεν είναι ανάγωγο γιατί τότε θα αναλυόταν σε γινόμενο αναγώγων με έναν μόνον παράγοντα, τον εαυτό του. Εφόσον το α_0 δεν είναι ανάγωγο, θα υπάρχουν (μη μηδενικά) μη αντιστρέψιμα στοιχεία $\alpha_1, \beta_1 \in R$ τέτοια, ώστε $\alpha_0 = \alpha_1\beta_1$. Αν και το α_1 και το β_1 αναλύονταν σε γινόμενο ανάγωγων στοιχείων, τότε το ίδιο θα συνέβαινε και με το γινόμενό τους α_0. Επομένως κάποιο από αυτά, έστω το α_1 δεν αναλύεται σε γινόμενο αναγώγων στοιχείων. Έχουμε προφανώς $(\alpha_0) \subseteq (\alpha_1)$. Επίσης, επειδή το β_1 δεν είναι αντιστρέψιμο, έπεται ότι $(\alpha_0) \subsetneq (\alpha_1)$. Πράγματι, αν $(\alpha_0) = (\alpha_1)$, τότε

$\alpha_0 \mid \alpha_1$, οπότε $\alpha_1 = \alpha_0\gamma$, για κάποιο $\gamma \neq 0$. Άρα $\alpha_1 = \alpha_0\gamma = \alpha_1\beta_1\gamma \Leftrightarrow \alpha_1(1-\beta_1\gamma) = 0$ και επειδή είμαστε σε ακέραια περιοχή, $\beta_1\gamma = 1$, άτοπο γιατί υποθέσαμε ότι το β_1 δεν είναι αντιστρέψιμο. Εφαρμόζοντας την ίδια επιχειρηματολογία για το α_1 που δεν είναι μηδενικό, δεν είναι αντιστρέψιμο και δεν αναλύεται σε γινόμενο ανάγωγων παραγόντων βρίσκουμε ένα κύριο ιδεώδες (α_2) με $(\alpha_1) \subsetneq (\alpha_2)$. Προχωρώντας κατ' αυτόν τον τρόπο κατασκευάζουμε μια **γνησίως αύξουσα** ακολουθία κυρίων ιδεωδών

$$(\alpha_0) \subsetneq (\alpha_1) \subsetneq (\alpha_2) \subsetneq \cdots$$

Αυτό είναι άτοπο σύμφωνα με το κριτήριο 2.

Έστω $\alpha \in R \setminus \big(U(R) \cup \{0\}\big)$. Τότε $\alpha = p_1 \cdots p_\mu = q_1 \cdots q_\nu$, όπου μ, ν θετικοί ακέραιοι και p_i, q_j ανάγωγα, για κάθε $i = 1, \ldots, \mu$ και $j = 1, \ldots, \nu$. Εφαρμόζουμε επαγωγή επί του μ. Αν $\mu = 1$, τότε και $\nu = 1$, γιατί αλλιώς $p_1 = q_1 \cdots q_\nu$, δηλαδή το ανάγωγο στοιχείο p_1 αναλύεται σε γινόμενο μη μηδενικών και μη αντιστρεψίμων στοιχείων, πράγμα άτοπο. Άρα $\alpha = p_1 = q_1$ και τελειώσαμε σ' αυτήν την περίπτωση. Το ίδιο επιχείρημα προφανώς λειτουργεί αν υποθέσουμε ότι $\nu = 1$.

Έστω τώρα ότι $\mu, \nu \geq 2$ και $\alpha = p_1 p_2 \cdots p_\mu = q_1 q_2 \cdots q_\nu$. Βάσει του κριτηρίου 1, το ανάγωγο στοιχείο p_1 είναι πρώτο και διαιρεί το γινόμενο $q_1 q_2 \cdots q_\nu$. Επομένως διαιρεί κάποιο από τα q_j και χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $p_1 \mid q_1$. Βάσει της πρότασης 2.7, τα p_1 και q_1 είναι συντροφικά, άρα $q_1 = up_1$, όπου u αντιστρέψιμο στην R. Εφόσον η R είναι ακέραια περιοχή, παίρνουμε

$$p_2 \cdots p_\mu = (uq_2) \cdots q_\nu.$$

Βάσει της επαγωγικής υπόθεσης, $\mu - 1 = \nu - 1 \Leftrightarrow \mu = \nu$ και χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $p_2 \sim uq_2 \sim q_2$, $p_3 \sim q_3, \ldots, p_\mu \sim q_\mu$. ■

2.2.2 Μέγιστος Κοινός Διαιρέτης και Ελάχιστο Κοινό Πολλαπλάσιο σε Περιοχή Μοναδικής Παραγοντοποίησης

Παρατήρηση: Σε κάθε περιοχή μοναδικής παραγοντοποίησης R κάθε μη μηδενικό στοιχείο α γράφεται στη μορφή $\alpha = up_1^{r_1} \cdots p_k^{r_k}$, όπου u αντιστρέψιμο και p_i ανάγωγα, **ανά δύο μη συντροφικά** και $r_i \geq 0$, για κάθε $i = 1, \ldots, k$. Τη μορφή αυτή τη χρειαζόμαστε όταν θέλουμε να συγκρίνουμε δύο μη μηδενικά στοιχεία του R.

1) Πώς το πετυχαίνουμε αυτό; Αν για παράδειγμα έχουμε $\alpha = q_1 q_2 \cdots q_\lambda$, τότε **«μαζεύουμε» κατά ομάδες τους συντροφικούς ανάγωγους παράγοντες**. Για παράδειγμα, έστω

$$\alpha = q_1 q_2 q_3 q_4 q_5 q_6,$$

όπου $q_1 \sim q_2 \sim q_4$ και $q_3 \sim q_6$ και επίσης $q_1 \not\sim q_3$, $q_1 \not\sim q_5$ και $q_3 \not\sim q_5$.

Θέτουμε $p_1 = q_1$, $q_2 = u_1 q_1 = u_1 p_1$, $q_4 = u_2 q_1 = u_2 p_1$, $p_2 = q_3$, $q_6 = u_3 q_3 = u_3 p_2$ και $p_3 = q_5$. Τότε $\alpha = p_1(u_1 p_1) p_2 (u_2 p_1) p_3 (u_3 p_2) = \underbrace{(u_1 u_2 u_3)}_{u \text{ αντιστρέψιμο}} p_1^3 p_2^2 p_3 = up_1^3 p_2^2 p_3$.

2) Αν λοιπόν $\alpha = up_1^{r_1} \cdots p_k^{r_k}$, όπου u αντιστρέψιμο και p_i ανάγωγα με $p_i \not\sim p_j$ για $i \neq j$ και $r_1 = r_2 = \cdots = r_k = 0$, τότε $\alpha = u$ αντιστρέψιμο.

2) Γενικά, η απεικόνιση μήκους $\lambda : R \setminus \{0\} \to \{0, 1, 2, 3, \ldots\}$ σε ένα στοιχείο α που το έχουμε γράψει στη μορφή $\alpha = up_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, όπου $p_i \not\sim p_j$ για κάθε ζεύγος δεικτών (i, j) με $i \neq j$, τότε

$$\boxed{\lambda(\alpha) = \sum_{i=1}^{k} r_i.}$$

Αυτό είναι φυσικό γιατί η λ μετράει το πλήθος των ανάγωγων παραγόντων που διαιρούν τον α. Αν στο γινόμενο $\alpha = up_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ κάποιος r_t είναι μηδέν, τότε $p_t^{r_t} = 1$, οπότε ουσιαστικά το

ανάγωγο στοιχείο p_t δεν διαιρεί το α, άρα δεν «μετράει» στο άθροισμα $\sum_{i=1}^{k} r_i$.
3) Δύο ή και περισσότερα μη μηδενικά στοιχεία $\alpha, \beta, \gamma, \ldots \in R$ μπορούμε να τα γράψουμε στη μορφή $\alpha = up_1^{r_1} \cdots p_k^{r_k}$, $\beta = vp_1^{s_1} \cdots p_k^{s_k}$, $\gamma = wp_1^{t_1} \cdots p_k^{t_k}$ κτλ $\big(u, v, w$ αντιστρέψιμα$\big)$, όπου θέτουμε μηδενικό εκθέτη στο ανάγωγο στοιχείο που λείπει από κάποιον από τους α, β, γ κτλ.

ΠΡΟΤΑΣΗ 2.17. Με τις παραπάνω συμβάσεις, έστω $\alpha = up_1^{r_1} \cdots p_k^{r_k}$ και $\beta = vp_1^{s_1} \cdots p_k^{s_k}$ μη μηδενικά στοιχεία της R. $\big(p_i \not\sim p_j$ για $i \neq j\big)$.
Τότε $\alpha \mid \beta \Leftrightarrow r_i \leq s_i$, για κάθε $i = 1, 2, \ldots, k$.
ΑΠΟΔΕΙΞΗ: Έστω ότι $\alpha \mid \beta \Leftrightarrow \beta = \alpha\gamma$, για κάποιο $\gamma \in R \setminus \{0\}$. Τότε έχουμε τη σχέση

$$vp_1^{s_1} \cdots p_k^{s_k} = up_1^{r_1} \cdots p_k^{r_k}\gamma. \qquad \textbf{(1)}$$

Υποθέτουμε ότι $r_i > s_i$, για κάποιο i, π.χ. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $r_1 > s_1$. Τότε επειδή ο R είναι ακέραια περιοχή, ισχύει ο νόμος της διαγραφής στον πολλαπλασιασμό και παίρνουμε

$$vp_2^{s_2} \cdots p_k^{s_k} = up_1^{r_1 - s_1} \cdots p_k^{r_k}\gamma \qquad \textbf{(2)}$$

και $r_1 - s_1 > 0$. Το p_1 εμφανίζεται στο δεξιό μέλος της **(2)**, άρα διαιρεί κάποιο από τα μη συντροφικά του ανάγωγα στοιχεία $p_2, \ldots, p_k$ που εμφανίζονται στο αριστερό μέλος. $\big($Σημειώνουμε ότι το v είναι αντιστρέψιμο άρα δεν διαιρείται από το ανάγωγο-πρώτο $p_1\big)$. Αυτό είναι άτοπο σύμφωνα με την πρόταση 2.7.
Το αντίστροφο είναι προφανές. Έστω ότι $r_i \leq s_i$, για κάθε $i = 1, 2, \ldots, k$. Τότε $\beta = \alpha\gamma$, όπου $\gamma = vu^{-1}p_1^{s_1 - r_1} \cdots p_k^{s_k - r_k}$. ■

ΠΟΡΙΣΜΑ 2.18. Με τις παραπάνω συμβάσεις, έστω $\alpha = up_1^{r_1} \cdots p_k^{r_k}$ και $\beta = vp_1^{s_1} \cdots p_k^{s_k}$ μη μηδενικά στοιχεία της R. Τότε $\alpha \sim \beta \Leftrightarrow r_i = s_i$, για κάθε $i = 1, \ldots, k$.
ΑΠΟΔΕΙΞΗ: Άμεση από την προηγούμενη πρόταση, αφού $\alpha \sim \beta \Leftrightarrow \big(\alpha \mid \beta$ και $\beta \mid \alpha\big) \Leftrightarrow$ $\Leftrightarrow \big(r_i \leq s_i,$ για κάθε $i = 1, \ldots, k$ και $s_i \leq r_i,$ για κάθε $i = 1, \ldots, k\big) \Leftrightarrow r_i = s_i,$ για κάθε $i =$ $= 1, \ldots, k$. ■

ΠΡΟΤΑΣΗ 2.19. Έστω $\alpha = up_1^{r_1} \cdots p_k^{r_k}$ και $\beta = vp_1^{s_1} \cdots p_k^{s_k}$ μη μηδενικά στοιχεία της R, όπως παραπάνω. Τότε υπάρχει μοναδικό ως προς τη συντροφικότητα στοιχείο $\delta \in R \setminus \{0\}$ με τις ακόλουθες ιδιότητες:
(i) $\delta \mid \alpha$ και $\delta \mid \beta$.
(ii) Αν $\delta' \mid \alpha$ και $\delta' \mid \beta$, τότε $\delta' \mid \delta$.
ΑΠΟΔΕΙΞΗ: Θέτουμε $\delta = p_1^{\min\{r_1, s_1\}} \cdots p_k^{\min\{r_k, s_k\}}$. Επειδή $\min\{r_i, s_i\} \leq r_i$ και $\min\{r_i, s_i\} \leq s_i$, για κάθε $i = 1, \ldots, k$, έχουμε $\delta \mid \alpha$ και $\delta \mid \beta$.
Αν $\delta' = wp_1^{t_1} \cdots p_k^{t_k}$ κοινός διαιρέτης των α και β $\big(w$ αντιστρέψιμο και $t_i \geq 0$, για κάθε $i =$ $= 1, \ldots, k\big)$, τότε από την προηγούμενη πρόταση προκύπτει ότι $t_i \leq r_i$ και $t_i \leq s_i$, για κάθε $i = = 1, \ldots, k$. Άρα $t_i \leq \min\{r_i, s_i\}$, για κάθε $i = 1, \ldots, k$, οπότε και πάλι με βάση την προηγούμενη πρόταση $\big($ή είναι προφανές$\big)$ έπεται ότι $\delta' \mid \delta$. Άρα το δ είναι ένας μέγιστος κοινός διαιρέτης των α και β.
Τέλος, το δ είναι μοναδικό ως προς τη συντροφικότητα. Πράγματι, αν δ_1 κοινός διαιρέτης των α και β, ο οποίος διαιρείται από οποιονδήποτε άλλον κοινό διαιρέτη αυτών, τότε $\delta \mid \delta_1$, αλλά $\big($από τον ορισμό του $\delta\big)$ και $\delta_1 \mid \delta$, δηλαδή $\delta_1 \sim \delta$. ■

ΟΡΙΣΜΟΣ 2.20. Ένα στοιχείο δ, το οποίο πληροί τις προϋποθέσεις που αναφέρονται στην προηγούμενη πρόταση θα λέγεται **ένας μέγιστος κοινός διαιρέτης των α και β**.

Τονίζουμε εδώ ότι, σε αντίθεση με ό,τι συνηθίζεται στη Θεωρία Αριθμών, ο μέγιστος κοινός διαιρέτης **δεν είναι μοναδικός**. Όλοι οι μέγιστοι κοινοί διαιρέτες συγκροτούν μια κλάση ως

προς τη συντροφικότητα.
Είναι επίσης προφανές ότι η έννοια του μέγιστου κοινού διαιρέτη γενικεύεται για περισσότερα από δύο στοιχεία της R, εκ των οποίων **ένα τουλάχιστον είναι μη μηδενικό**. Το 0 διαιρείται από οποιοδήποτε στοιχείο της R και επομένως δεν λαμβάνεται υπόψη στον υπολογισμό του μέγιστου κοινού διαιρέτη. Έτσι, λέμε ότι ένας μέγιστος κοινός διαιρέτης των $2^2 \cdot 3 \cdot (-5)$, $-2 \cdot 3^2 \cdot 5^3 \cdot 7$, $2^4 \cdot 5^2 \cdot (-7)$ και του 0 στο $\mathbb{Z}$ είναι το $2 \cdot 5 = 10$ ή το $-2 \cdot 5 = -10$.
Ή, αν $\alpha = up_1^{r_1} \cdots p_k^{r_k}$, $\beta = vp_1^{s_1} \cdots p_k^{s_k}$ και $\gamma = wp_1^{t_1} \cdots p_k^{t_k}$, τότε ένας μέγιστος κοινός διαιρέτης των α, β και γ θα έχει τη μορφή $u' p_1^{\min\{r_1,s_1,t_1\}} \cdots p_k^{\min\{r_k,s_k,t_k\}}$, όπου u' οποιοδήποτε αντιστρέψιμο στοιχείο.
Κατ' αναλογίαν προς το μέγιστο κοινό διαιρέτη ορίζεται το ελάχιστο κοινό πολλαπλάσιο.

ΠΡΟΤΑΣΗ 2.21. Έστω $\alpha = up_1^{r_1} \cdots p_k^{r_k}$ και $\beta = vp_1^{s_1} \cdots p_k^{s_k}$ μη μηδενικά στοιχεία της R, όπως παραπάνω. Τότε υπάρχει μοναδικό ως προς τη συντροφικότητα στοιχείο $\varepsilon \in R \setminus \{0\}$ με τις ακόλουθες ιδιότητες:
(i) $\alpha \mid \varepsilon$ και $\beta \mid \varepsilon$.
(ii) Αν $\alpha \mid \varepsilon'$ και $\beta \mid \varepsilon'$, τότε $\varepsilon \mid \varepsilon'$.
ΑΠΟΔΕΙΞΗ: Η απόδειξη είναι ανάλογη με αυτήν της προηγούμενης πρότασης. Θέτουμε $\varepsilon = p_1^{\max\{r_1,s_1\}} \cdots p_k^{\max\{r_k,s_k\}}$ και προχωράμε κατά τρόπο συμμετρικό. ■

ΟΡΙΣΜΟΣ 2.22. Ένα στοιχείο ε, το οποίο πληροί τις προϋποθέσεις που αναφέρονται στην προηγούμενη πρόταση θα λέγεται **ένα ελάχιστο κοινό πολλαπλάσιο των α και β**.

Όπως με τον μέγιστο κοινό διαιρέτη, έτσι και η έννοια του ελαχίστου κοινού πολλαπλασίου γενικεύεται για περισσότερα από δύο **μη μηδενικά** στοιχεία της R. (Πρέπει όλα τα στοιχεία να είναι μη μηδενικά γιατί το μόνο πολλαπλάσιο του μηδενός είναι το μηδέν). Αν λοιπόν $\alpha = up_1^{r_1} \cdots p_k^{r_k}$, $\beta = vp_1^{s_1} \cdots p_k^{s_k}$ και $\gamma = wp_1^{t_1} \cdots p_k^{t_k}$, τότε ένα ελάχιστο κοινό πολλαπλάσιο των α, β και γ θα έχει τη μορφή $u' p_1^{\max\{r_1,s_1,t_1\}} \cdots p_k^{\max\{r_k,s_k,t_k\}}$, όπου u' οποιοδήποτε αντιστρέψιμο στοιχείο.

2.3 Περιοχές Κυρίων Ιδεωδών

ΟΡΙΣΜΟΣ 2.23. Μια ακέραια περιοχή R λέγεται **περιοχή κυρίων ιδεωδών** (Principal Ideal Domain) αν κάθε ιδεώδες της είναι κύριο.

ΠΡΟΤΑΣΗ 2.24. Κάθε περιοχή κυρίων ιδεωδών είναι περιοχή μοναδικής παραγοντοποίησης.
ΑΠΟΔΕΙΞΗ: Θα αποδείξουμε τα κριτήρια 1 και 2.
Κριτήριο 1: Έστω p ανάγωγο στοιχείο και $p \mid \alpha\beta$. Υποθέτουμε ότι $p \nmid \alpha$. Θεωρούμε το ιδεώδες (p, α) που παράγεται από το p και το α. Αυτό είναι κύριο ιδεώδες της μορφής (u), όπου $u \in R \setminus \{0\}$. Επομένως $u \mid p$, δηλαδή $p = uq$, όπου $q \in R \setminus \{0\}$. Εφόσον το p είναι ανάγωγο, το u είναι αντιστρέψιμο ή συντροφικό του p. Αν $u \sim p$, τότε επειδή $u \mid \alpha$, θα είχαμε $p \mid \alpha$, άτοπο. Επομένως το u είναι αντιστρέψιμο. Συνεπώς $(p, \alpha) = (u) = (1) = R$. Άρα υπάρχουν $x, y \in R$ τέτοια, ώστε $px + \alpha y = 1 \Rightarrow p\beta x + \alpha\beta y = \beta$. Εφόσον $p \mid p\beta x$ και $p \mid \alpha\beta y$, έπεται ότι $p \mid p\beta x + \alpha\beta y = \beta$. Συνεπώς το p είναι πρώτο.
Κριτήριο 2: Έστω $(\alpha_1) \subseteq (\alpha_2) \subseteq (\alpha_3) \subseteq \cdots$ μια αύξουσα ακολουθία κυρίων ιδεωδών. Η ένωση $I = \bigcup_{i=1}^{\infty} (\alpha_i)$ είναι ένα ιδεώδες της R. (Γενικότερα, η ένωση μιας αύξουσας ακολουθίας ιδεωδών είναι επίσης ιδεώδες). Αν $x, y \in I$, τότε υπάρχουν θετικοί ακέραιοι i, j τέτοιοι, ώστε $x \in (\alpha_i)$ και

$y \in (\alpha_j)$. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $i \leq j$. Άρα $(\alpha_i) \subseteq (\alpha_j)$ και επομένως $x, y \in (\alpha_j)$. Συνεπώς $x+y \in (\alpha_j) \subseteq I$. Αν τώρα $x \in I$ και $r \in R$, τότε υπάρχει θετικός ακέραιος i τέτοιος, ώστε $x \in (\alpha_i)$. Επομένως $rx \in (\alpha_i) \subseteq I$.

Τώρα, το ιδεώδες I είναι κύριο της μορφής (β), για κάποιο $\beta \in R$. Επομένως $\beta \in \bigcup_{i=1}^{\infty}(\alpha_i) \Rightarrow \beta \in (\alpha_k)$, για κάποιον θετικό ακέραιο k. Συνεπώς $I = (\beta) \subseteq (\alpha_k) \subseteq (\alpha_{k+1}) \subseteq (\alpha_{k+2}) \subseteq \cdots \subseteq I$. Επομένως $(\alpha_k) = (\alpha_{k+1}) = (\alpha_{k+2}) = \cdots = I$. ■

ΠΡΟΤΑΣΗ 2.25. Έστω $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$, όχι όλα μηδέν, όπου R περιοχή κυρίων ιδεωδών. Τότε ένα στοιχείο $\delta \in R$ είναι ένας μέγιστος κοινός διαιρέτης των $\alpha_1, \alpha_2, \ldots, \alpha_n$ αν και μόνον αν
$$(\delta) = (\alpha_1, \alpha_2, \ldots, \alpha_n).$$
ΑΠΟΔΕΙΞΗ: Υποθέτουμε ότι $(\delta) = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Εφόσον κάποιο α_i δεν είναι μηδέν, τότε και το δ δεν είναι το μηδενικό στοιχείο. Επειδή τώρα $\alpha_i \in (\alpha_1, \alpha_2, \ldots, \alpha_n) = (\delta)$, έχουμε $(\alpha_i) \subseteq (\delta) \Leftrightarrow \delta \mid \alpha_i$, για κάθε $i = 1, \ldots, n$. Επίσης, επειδή $\delta \in (\alpha_1, \alpha_2, \ldots, \alpha_n)$, υπάρχουν $x_1, x_2, \ldots, x_n \in R$ τέτοια, ώστε $\delta = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n$. Αν τώρα δ' είναι ένα μη μηδενικό στοιχείο της R με $\delta' \mid \alpha_i$, για κάθε $i = 1, 2, \ldots, n$, τότε $\delta' \mid x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n = \delta$. Επομένως το δ είναι ένας μέγιστος κοινός διαιρέτης των $\alpha_1, \alpha_2, \ldots, \alpha_n$.
Αντιστρόφως, υποθέτουμε ότι το δ είναι ένας μέγιστος κοινός διαιρέτης των $\alpha_1, \alpha_2, \ldots, \alpha_n$. Θεωρούμε το ιδεώδες $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Επειδή βρισκόμαστε σε περιοχή κυρίων ιδεωδών, το ιδεώδες $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ είναι κύριο. Έστω $(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\delta')$, για κάποιο $\delta' \in R \setminus \{0\}$. Σύμφωνα με την προηγούμενη επιχειρηματολογία και ο δ' είναι ένας μέγιστος κοινός διαιρέτης των $\alpha_1, \alpha_2, \ldots, \alpha_n$. Από τον ορισμό του μέγιστου κοινού διαιρέτη σε μια περιοχή μοναδικής παραγοντοποίησης προκύπτει ότι $\delta \mid \delta'$ και $\delta' \mid \delta$. Επομένως $(\delta) = (\delta') = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. ■

ΛΗΜΜΑ 2.26. Έστω R περιοχή κυρίων ιδεωδών. Αν $\alpha \mid \beta\gamma$ και $(\alpha, \beta) = (1_R)$, τότε $\alpha \mid \gamma$.
ΑΠΟΔΕΙΞΗ: Εφόσον $(\alpha, \beta) = (1_R)$, υπάρχουν $x, y \in R$ τέτοια, ώστε $\alpha x + \beta y = 1_R$. Συνεπώς $\alpha\gamma x + \beta\gamma y = \gamma$ με $\alpha \mid \alpha\gamma x$ και $\alpha \mid (\beta\gamma)y$. Επομένως $\alpha \mid \alpha\gamma x + \beta\gamma y = \gamma$. ■

Το επόμενο πόρισμα είναι πολύ σημαντικό και θα χρησιμοποιηθεί στην απόδειξη του θεωρήματος, το οποίο αφορά τη δομή των πεπερασμένα παραγόμενων προτύπων επί μιας περιοχής κυρίων ιδεωδών.

ΠΟΡΙΣΜΑ 2.27. Αν R περιοχή κυρίων ιδεωδών και $p \in R$ ανάγωγο, τότε το ιδεώδες (p) είναι μέγιστο και άρα ο δακτύλιος $R/(p)$ είναι σώμα.
ΑΠΟΔΕΙΞΗ: Εφόσον R περιοχή μοναδικής παραγοντοποίησης, οι έννοιες του «πρώτου» και «αναγώγου» στοιχείου συμπίπτουν. Επομένως το ιδεώδες (p) είναι πρώτο και άρα ο $R/(p)$ είναι ακέραια περιοχή. Τώρα η διαδικασία της απόδειξης έχει ήδη αναφερθεί στην απόδειξη του Κριτηρίου 1, στην πρόταση 2.24. Έστω ότι το (p) δεν είναι μέγιστο και υπάρχει γνήσιο ιδεώδες I του R με $(p) \subsetneq I$. Τότε υπάρχει $\alpha \in I \setminus (p)$. Θεωρούμε το ιδεώδες $(\alpha, p) = (u)$, για κάποιο $u \in R$. Τότε $u = x\alpha + yp$, για κάποια $x, y \in R$. Επίσης, $u \mid p$ και άρα $p = up'$, για κάποιο $p' \in R$. Αν u όχι αντιστρέψιμο, τότε το p' θα ήταν αντιστρέψιμο, αφού p ανάγωγο. Άρα $u \sim p$ και προφανώς $u \mid \alpha$. Επομένως $p \mid \alpha \Leftrightarrow \alpha \in (p)$, άτοπο. ■

2.4 Ευκλείδειες Περιοχές

2.4.1 Ορισμοί-Βασικές Ιδιότητες

ΟΡΙΣΜΟΣ 2.28. Έστω R ακέραια περιοχή και $N : R \setminus \{0\} \to \{0, 1, 2, \ldots\}$ μια απεικόνιση με τις ακόλουθες ιδιότητες:
(i) Αν $\alpha, \beta \in R \setminus \{0\}$ και $\alpha \mid \beta$, τότε $N(\alpha) \leq N(\beta)$.
(ii) Αν $\alpha, \beta \in R$ και $\beta \neq 0$, τότε υπάρχουν $\pi, \upsilon \in R$ τέτοια, ώστε $\alpha = \beta\pi + \upsilon$, όπου $\upsilon = 0$ ή $N(\upsilon) < N(\beta)$.
Η απεικόνιση $N : R \setminus \{0\} \to \{0, 1, 2, \ldots\}$ λέγεται **ευκλείδεια απεικόνιση**. Η ακέραια περιοχή R λέγεται **ευκλείδειος περιοχή** $\big($Euclidean Domain$\big)$.

Είναι προφανές ότι η σχέση $\alpha = \beta\pi + \upsilon$ γενικεύει τη σχέση της ευκλείδειας διαίρεσης στους ακεραίους.

ΠΑΡΑΔΕΙΓΜΑΤΑ 2.29. (i) $R = \mathbb{Z}$ και $N(x) = |x|$, για κάθε $x \in \mathbb{Z} \setminus \{0\}$. Από την περίπτωση αυτή καθίσταται φανερό ότι **το «πηλίκο» π και το «υπόλοιπο» υ στη σχέση $\alpha = \beta\pi + \upsilon$ δεν είναι κατ᾽ ανάγκην μοναδικά**.
Για παράδειγμα, οι σχέσεις $11 = 3 \cdot 3 + 2$ και $11 = 3 \cdot 4 + (-1)$ με δυνατά πηλίκα τα 3 και 4 και αντίστοιχα υπόλοιπα τα 2 και -1 πληρούν τη συνθήκη (ii) για τη «διαίρεση» $11 : 3$. $\big($Εδώ απαιτούμε $0 \leq |\upsilon| < |\beta|$ και όχι $0 \leq \upsilon < |\beta|$, όπως στην κλασική Θεωρία Αριθμών$\big)$. Η μη μοναδικότητα των π και υ δεν αλλάζει και πολύ τα πράγματα.
(ii) $R = \mathbb{K}[x]$ ο πολυωνυμικός δακτύλιος μιας μεταβλητής επί ενός σώματος $\mathbb{K}$ και ευκλείδεια απεικόνιση το βαθμό $\deg : \mathbb{K}[x] \setminus \{0\} \to \{0, 1, 2, \ldots\}$ των μη μηδενικών πολυωνύμων πληροί τις ιδιότητες (i) και (ii) της ευκλείδειας απεικόνισης. Σημειώνουμε ότι στην περίπτωση $R = \mathbb{K}[x]$ το πηλίκο $\pi(x)$ και το υπόλοιπο $\upsilon(x)$ της διαίρεσης $f(x) : g(x)$, όπου $g(x) \neq 0$ είναι μοναδικά.
(iii) Κάθε σώμα $\mathbb{K}$ είναι ευκλείδειος περιοχή με ευκλείδεια απεικόνιση $N : \mathbb{K} \setminus \{0\} \to \{0\}$.

Το βασικό αποτέλεσμα αυτής της υποπαραγράφου είναι το ακόλουθο:

ΠΡΟΤΑΣΗ 2.30. Κάθε ευκλείδειος περιοχή R είναι περιοχή κυρίων ιδεωδών και άρα περιοχή μοναδικής παραγοντοποίησης.
ΑΠΟΔΕΙΞΗ: Έστω I ιδεώδες της R. Μπορούμε να υποθέσουμε ότι $I \neq (0)$. Από όλα τα μη μηδενικά στοιχεία του I επιλέγουμε ένα στοιχείο α, στο οποίο η N παίρνει την ελάχιστη τιμή $N(\alpha)$. Έστω τώρα $\beta \in I$. Τότε υπάρχουν $\pi, \upsilon \in R$ τέτοια, ώστε $\beta = \alpha\pi + \upsilon$, όπου $\upsilon = 0$ ή $N(\upsilon) < N(\alpha)$. Αν $\upsilon \neq 0$, τότε $\upsilon = \beta - \pi\alpha \in I \setminus \{0\}$ και $N(\upsilon) < N(\alpha)$, άτοπο λόγω της επιλογής του α. Επομένως $\upsilon = 0 \Rightarrow \alpha \mid \beta$. Συνεπώς $I = (\alpha)$. ■

2.4.2 Ο Δακτύλιος $\mathbb{Z}[\mathbf{i}]$ των Ακεραίων του Gauss

ΟΡΙΣΜΟΣ 2.31. Ο Δακτύλιος $\mathbb{Z}[\mathrm{i}]$ των ακεραίων του Gauss είναι το σύνολο

$$\mathbb{Z}[\mathrm{i}] = \{\alpha + \beta\mathrm{i} \mid \alpha, \beta \in \mathbb{Z}\}.$$

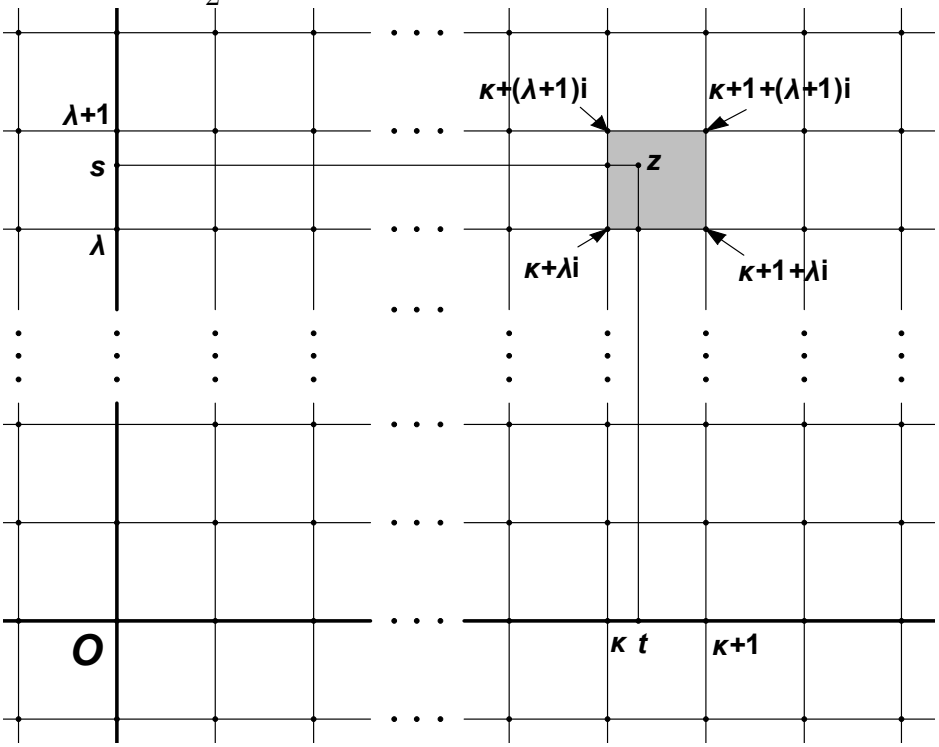
Ο $\mathbb{Z}[\mathrm{i}]$ είναι υποδακτύλιος του σώματος $\mathbb{C}$ των μιγαδικών αριθμών, αφού $0 = 0 + 0\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$, $1 = 1 + 0\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ και $(\alpha + \beta\mathrm{i}) + (\gamma + \delta\mathrm{i}) = (\alpha + \gamma) + (\beta + \delta)\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ και $(\alpha + \beta\mathrm{i}) \cdot (\gamma + \delta\mathrm{i}) = (\alpha\gamma - \beta\delta) + (\alpha\delta + \gamma\beta)\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$, για κάθε $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$.

ΟΡΙΣΜΟΣ 2.32. Ορίζουμε την απεικόνιση $N : \mathbb{Z}[\mathrm{i}] \setminus \{0\} \to \{1, 2, \ldots\}$ με $N(\alpha + \beta\mathrm{i}) = \alpha^2 + \beta^2 = |\alpha + \beta\mathrm{i}|^2$, για κάθε $\alpha, \beta \in \mathbb{Z}$, όπου $\alpha^2 + \beta^2 \neq 0$. $\big($Η περίπτωση $N(x) = 0$ σημαίνει ότι $x = 0\big)$.

Είναι σαφές ότι $N(x) = x\bar{x}$, για κάθε $x \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$. Επομένως $N(xy) = (xy)(\overline{xy}) = x\bar{x} \cdot y\bar{y} =$ $= N(x)N(y)$, για κάθε $x, y \in \mathbb{Z}[\mathrm{i}]$.

ΠΡΟΤΑΣΗ 2.33. Ο δακτύλιος $\mathbb{Z}[\mathrm{i}]$ με την απεικόνιση $N : \mathbb{Z}[\mathrm{i}] \setminus \{0\} \to \{1, 2, \ldots\}$ είναι ευκλείδειος περιοχή.
ΑΠΟΔΕΙΞΗ: (i) Έστω $x, y \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$ με $x \mid y$. Επομένως υπάρχει $z \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$ τέτοιο, ώστε $y = xz$. Επομένως $N(y) = N(x)N(z) \underset{N(z)\geq 1}{\geq} N(x)$.

Έστω τώρα $x, y \in \mathbb{Z}[\mathrm{i}]$ με $y \neq 0$. Θεωρούμε τον μιγαδικό αριθμό $z = \dfrac{x}{y} = t + \mathrm{i}s$, όπου $t, s \in \mathbb{R}$. Η ιδέα είναι ότι ο z κείται σε κάποιο τετράγωνο πλευράς 1 με κορυφές στοιχεία του $\mathbb{Z}[\mathrm{i}]$. Επομένως θα απέχει από μια τουλάχιστον κορυφή απόσταση μικρότερη ή ίση του $\dfrac{\sqrt{2}}{2} < 1$. Έστω $\kappa = \lfloor t \rfloor$ και $\lambda = \lfloor s \rfloor$. Προφανώς $\kappa, \lambda \in \mathbb{Z}$, άρα $\kappa + \lambda\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$. Έχουμε $t \in [\kappa, \kappa + 1)$ διάστημα μήκους 1, και επομένως $t - \kappa \leq \dfrac{1}{2}$ ή $\kappa + 1 - t \leq \dfrac{1}{2}$. Συνεπώς $|t - \kappa'| \leq \dfrac{1}{2}$, όπου κ' κάποιος από τους $\kappa, \kappa + 1$. Ομοίως $|s - \lambda'| \leq \dfrac{1}{2}$, όπου λ' κάποιος από τους $\lambda, \lambda + 1$.



Σχήμα 1

Επομένως $|z - (\kappa' + \lambda'\mathrm{i})|^2 = |(t - \kappa') + (s - \lambda')\mathrm{i}|^2 = (t - \kappa')^2 + (s - \lambda')^2 \leq \dfrac{1}{4} + \dfrac{1}{4} = \dfrac{1}{2} < 1$.
Άρα $|x - y(\kappa' + \lambda'\mathrm{i})|^2 < |y|^2$. Θέτουμε $\pi = \kappa' + \lambda'\mathrm{i}$ και $\upsilon = x - y\pi \in \mathbb{Z}[\mathrm{i}] \Leftrightarrow x = y\pi + \upsilon$. Τότε $|\upsilon|^2 < |y|^2$, οπότε $\upsilon = 0$ ή $N(\upsilon) = |\upsilon|^2 < |y|^2 = N(y)$. ■

ΠΑΡΑΔΕΙΓΜΑΤΑ 2.34. (i) Ας υποθέσουμε ότι θέλουμε να προσδιορίσουμε τους μέγιστους κοινούς διαιρέτες των $3 + 5\mathrm{i}$ και $5 - 4\mathrm{i}$. Παρατηρούμε ότι $N(3 + 5\mathrm{i}) = 3^2 + 5^2 = 34$ και $N(5 - 4\mathrm{i}) =$ $= 25 + 16 = 41 > N(3 + 5\mathrm{i})$. Έχουμε $\dfrac{5 - 4\mathrm{i}}{3 + 5\mathrm{i}} = \dfrac{(5 - 4\mathrm{i})(3 - 5\mathrm{i})}{34} = \dfrac{15 - 20 - (12 + 25)\mathrm{i}}{34} =$

$= -\frac{5}{34} - \frac{37}{34}\mathbf{i}$. Έστω $-\mathbf{i}$ ο πλησιέστερος ακέραιος του Gauss. Θέτουμε $\pi = -\mathbf{i}$ και $\upsilon = 5 - 4\mathbf{i} + \mathbf{i}(3 + 5\mathbf{i}) = -\mathbf{i}$, το οποίο είναι αντιστρέψιμο. Επομένως $(5 - 4\mathbf{i}, 3 + 5\mathbf{i}) = (-\mathbf{i}) = (1) = \mathbb{Z}[\mathbf{i}]$. Άρα οι $3 + 5\mathbf{i}$ και $5 - 4\mathbf{i}$ είναι πρώτοι μεταξύ τους. Μέγιστοι κοινοί διαιρέτες οι $\pm 1, \pm\mathbf{i}$.

(ii) Έστω ότι θέλουμε να βρούμε τους μέγιστους κοινούς διαιρέτες των $86 - 4\mathbf{i}$ και $-33 + 81\mathbf{i}$. Παρατηρούμε ότι $N(86-4\mathbf{i}) = 86^2+4^2 = 7412$ και $N(-33+81\mathbf{i}) = 7650 > N(86-4\mathbf{i})$. Έχουμε: $\frac{-33 + 81\mathbf{i}}{86 - 4\mathbf{i}} = \frac{(86 + 4\mathbf{i})(-33 + 81\mathbf{i})}{86^2 + 4^2} = -\frac{1581}{3706} + \frac{3417}{3706}\mathbf{i} = -0,426\ldots + \mathbf{i} \cdot 0,922\ldots$. Ένα «καλό» πηλίκο είναι λοιπόν το $0 + 1 \cdot \mathbf{i} = \mathbf{i}$. Θέτουμε $\upsilon = -33 + 81\mathbf{i} - \mathbf{i} \cdot (86 - 4\mathbf{i}) = -37 - 5\mathbf{i}$. Επομένως $(-33 + 81\mathbf{i}, 86 - 4\mathbf{i}) = (86 - 4\mathbf{i}, -37 - 5\mathbf{i}) = (86 - 4\mathbf{i}, 37 + 5\mathbf{i})$.

Συνεχίζουμε: $\frac{86 - 4\mathbf{i}}{37 + 5\mathbf{i}} = \frac{(86 - 4\mathbf{i})(37 - 5\mathbf{i})}{37^2 + 5^2} = \frac{3162}{1394} - \frac{578}{1394}\mathbf{i} = 2,268\ldots - \mathbf{i} \cdot 0,414\ldots$ Ένα «καλό» πηλίκο είναι το 2. Θέτουμε $\upsilon_1 = 86 - 4\mathbf{i} - 2(37 + 5\mathbf{i}) = 12 - 14\mathbf{i}$. Επομένως $(86 - 4\mathbf{i}, 37 + 5\mathbf{i}) = (37 + 5\mathbf{i}, 12 - 14\mathbf{i})$. Ακόμη, $\frac{37 + 5\mathbf{i}}{12 - 14\mathbf{i}} = \frac{(37 + 5\mathbf{i})(12 + 14\mathbf{i})}{12^2 + 14^2} = \frac{374}{340} + \frac{578}{340}\mathbf{i} = 1,1 + 1,7 \cdot \mathbf{i}$. Ένα «καλό» πηλίκο είναι ο $1 + 2\mathbf{i}$. Θέτουμε $\upsilon_2 = 37 + 5\mathbf{i} - (1 + 2\mathbf{i})(12 - 14\mathbf{i}) = -3 - 5\mathbf{i}$. Συνεπώς $(37 + 5\mathbf{i}, 12 - 14\mathbf{i}) = (12 - 14\mathbf{i}, -3 - 5\mathbf{i}) = (12 - 14\mathbf{i}, 3 + 5\mathbf{i})$. Ακόμη, $\frac{12 - 14\mathbf{i}}{3 + 5\mathbf{i}} = \frac{(12 - 14\mathbf{i})(3 - 5\mathbf{i})}{34} = -1 - 3\mathbf{i}$. Επομένως $12 - 14\mathbf{i} = -(1 + 3\mathbf{i})(3 + 5\mathbf{i})$. Άρα $(12 - 14\mathbf{i}, 3 + 5\mathbf{i}) = (-(1 + 3\mathbf{i})(3 + 5\mathbf{i}), 3 + 5\mathbf{i}) = (3 + 5\mathbf{i})$.

Επομένως οι μέγιστοι κοινοί διαιρέτες των $86-4\mathbf{i}$ και $-33+81\mathbf{i}$ είναι οι $3+5\mathbf{i}$, $\mathbf{i}(3+5\mathbf{i}) = -5+3\mathbf{i}$, $-3 - 5\mathbf{i}$ και $5 - 3\mathbf{i}$. Αν θελήσουμε να γράψουμε τον μέγιστο κοινό διαιρέτη $3 + 5\mathbf{i}$ ως γραμμικό συνδυασμό των $86-4\mathbf{i}$ και $-33+81\mathbf{i}$, παρατηρούμε ότι $3+5\mathbf{i} = -(37+5\mathbf{i}) + (1+2\mathbf{i})(12-14\mathbf{i}) = -(37 + 5\mathbf{i}) + (1 + 2\mathbf{i})(86 - 4\mathbf{i} - 2(37 + 5\mathbf{i})) = (3 + 4\mathbf{i})(-37 - 5\mathbf{i}) + (1 + 2\mathbf{i})(86 - 4\mathbf{i}) = (3+4\mathbf{i})(-33+81\mathbf{i} - \mathbf{i} \cdot (86-4\mathbf{i})) + (1+2\mathbf{i})(86-4\mathbf{i}) = (3+4\mathbf{i})(-33+81\mathbf{i}) + (5-\mathbf{i})(86-4\mathbf{i})$. ■

Στη συνέχεια θα εντοπίσουμε τα ανάγωγα στοιχεία της ευκλείδειας περιοχής $\mathbb{Z}[\mathbf{i}]$. Ξεκινάμε με κάποιες παρατηρήσεις.

Παρατήρηση 1η: Τα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\mathbf{i}]$ είναι τα $\{-1, 1, \mathbf{i}, -\mathbf{i}\}$ και είναι ακριβώς αυτά τα $x \in \mathbb{Z}[\mathbf{i}]$ με $N(x) = 1$.

Πράγματι, αν $x = \alpha + \beta\mathbf{i}$ αντιστρέψιμο με αντίστροφο το $y \in \mathbb{Z}[\mathbf{i}]$, τότε $1 = xy \Rightarrow 1 = N(1) = N(xy) = N(x)N(y)$, γιατί $N(x) = |x|^2 = x\bar{x}$. Άρα $N(x) = 1 \Leftrightarrow \alpha^2 + \beta^2 = 1 \Rightarrow \big((\alpha = \pm 1 \text{ και } \beta = 0) \text{ ή } (\alpha = 0 \text{ και } \beta = \pm 1)\big)$.

Παρατήρηση 2η: Αν $N(y) = p$, όπου p ακέραιος πρώτος, τότε το y είναι ανάγωγο στο $\mathbb{Z}[\mathbf{i}]$.

Πράγματι, αν $y = zw$, τότε $p = N(y) = N(z)N(w)$. Επομένως, εφόσον ο p είναι πρώτος, κάποιος από τους θετικούς ακεραίους $N(z), N(w)$ είναι μονάδα και βάσει της προηγούμενης παρατήρησης το αντίστοιχο στοιχείο αντιστρέφεται.

Παρατήρηση 3η: Αν το y είναι ανάγωγο στοιχείο στο $\mathbb{Z}[\mathbf{i}]$, τότε και το συζυγές του $\bar{y}$ είναι επίσης ανάγωγο στο $\mathbb{Z}[\mathbf{i}]$.

Πράγματι, αν $\bar{y} = zw$, τότε $y = \bar{z}\bar{w}$ και επειδή το y είναι ανάγωγο στοιχείο, κάποιος από τους $\bar{z}, \bar{w}$ αντιστρέφεται και επομένως και ο συζυγής αυτού $\big($το z ή το $w\big)$ αντιστρέφεται.

(i) Ας προσπαθήσουμε πρώτα να εντοπίσουμε τα ανάγωγα στοιχεία του $\mathbb{Z}[\mathbf{i}]$, τα οποία **είναι συντροφικά προς κάποιον ακέραιο**. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι ένα τέτοιο ανάγωγο στοιχείο θα είναι ένας θετικός ακέραιος p. Ο p αναγκαστικά θα είναι πρώτος, γιατί αλλιώς θα γραφόταν ως γινόμενο δύο θετικών ακεραίων μεγαλύτερων της μονάδας, άρα κανένα απ' αυτά δεν θα ήταν αντιστρέψιμο. $\big($Βλέπε 1^{η} παρατήρηση$\big)$.

Αν ο p γραφόταν ως άθροισμα δύο τετραγώνων $p = \alpha^2 + \beta^2$, τότε κανείς από τους $\alpha, \beta \in \mathbb{Z}$ δεν

θα ήταν μηδέν. Αλλιώς ο p θα ήταν τέλειο τετράγωνο ακεραίου. Αλλά τότε $p = (\alpha + \beta\mathrm{i})(\alpha - \beta\mathrm{i})$ και $N(\alpha \pm \beta\mathrm{i}) = \alpha^2 + \beta^2 = p$ πρώτος. Με βάση την 2^{η} παρατήρηση, τα στοιχεία $\alpha \pm \beta\mathrm{i}$ θα ήταν ανάγωγα στο $\mathbb{Z}[\mathrm{i}]$. Επομένως ο p ως γινόμενο δύο αναγώγων στοιχείων δεν θα ήταν ανάγωγο στοιχείο του $\mathbb{Z}[\mathrm{i}]$. Άρα ο p δεν γράφεται ως άθροισμα δύο τετραγώνων.
Αντιστρόφως, έστω ότι ο p δεν γράφεται ως άθροισμα δύο τετραγώνων. Υποθέτουμε ότι $p = = (\alpha+\beta\mathrm{i})(\gamma+\delta\mathrm{i})$, όπου $\alpha+\beta\mathrm{i}, \gamma+\delta\mathrm{i}$ μη αντιστρέψιμα στοιχεία στο $\mathbb{Z}[\mathrm{i}]$. Συνεπώς $N(\alpha+\beta\mathrm{i}) > 1$ και $N(\gamma + \delta\mathrm{i}) > 1$. Αλλά τότε $p^2 = N(p) = N((\alpha + \beta\mathrm{i})(\gamma + \delta\mathrm{i})) = N(\alpha + \beta\mathrm{i})N(\gamma + \delta\mathrm{i})$. Εφόσον οι ακέραιοι $N(\alpha+\beta\mathrm{i})$, $N(\gamma+\delta\mathrm{i})$ είναι μεγαλύτεροι της μονάδας, αναγκαστικά $p = N(\alpha+\beta\mathrm{i}) = = N(\gamma + \delta\mathrm{i})$, δηλαδή $p = \alpha^2 + \beta^2 = \gamma^2 + \delta^2$, άτοπο γιατί υποθέσαμε ότι ο p δεν γράφεται ως άθροισμα τετραγώνων.
Συμπέρασμα: Οι πρώτοι p που δεν γράφονται ως άθροισμα τετραγώνων, αλλά και τα συντροφικά τους $-p, \mathrm{i}p, -\mathrm{i}p$ είναι ανάγωγα στοιχεία του $\mathbb{Z}[\mathrm{i}]$.
(ii) Τώρα, ας προσπαθήσουμε να εντοπίσουμε τα ανάγωγα στοιχεία του $\mathbb{Z}[\mathrm{i}]$, τα οποία **δεν είναι συντροφικά προς κάποιον ακέραιο**. Ένα τέτοιο στοιχείο q θα είναι της μορφής $q = \alpha + \beta\mathrm{i}$, όπου $\alpha\beta \neq 0$. Πράγματι, αν κάποιος από τους $\alpha, \beta \in \mathbb{Z}$ ήταν μηδέν, τότε το q θα ήταν συντροφικό είτε προς τον $\alpha \in \mathbb{Z}$ (για $\beta = 0$) είτε προς τον $\beta \in \mathbb{Z}$ (για $\alpha = 0$).
Από την 3^{η} παρατήρηση προκύπτει ότι και το στοιχείο $\bar{q} = \alpha - \beta\mathrm{i}$ είναι επίσης ανάγωγο στο $\mathbb{Z}[\mathrm{i}]$. Τότε όμως $q\bar{q} = (\alpha + \beta\mathrm{i})(\alpha - \beta\mathrm{i}) = \alpha^2 + \beta^2$, ένας θετικός ακέραιος.
Αν ο $\alpha^2 + \beta^2$ δεν ήταν πρώτος, τότε $\alpha^2 + \beta^2 = \kappa\lambda$, όπου κ, λ θετικοί ακέραιοι μεγαλύτεροι της μονάδας.
Έχουμε λοιπόν τη σχέση $(\alpha + \beta\mathrm{i})(\alpha - \beta\mathrm{i}) = \kappa\lambda$. Στο αριστερό μέλος έχουμε το γινόμενο **δύο αναγώγων στοιχείων**. Στο δεξιό μέλος έχουμε το γινόμενο δύο μη αντιστρεψίμων στοιχείων. $\big($Βλέπε παρατήρηση $1^{\eta}\big)$. Αν κάποιος από τους κ, λ δεν ήταν ανάγωγο στοιχείο στο $\mathbb{Z}[\mathrm{i}]$, τότε αυτός θα αναλυόταν σε γινόμενο δύο τουλάχιστον αναγώγων στοιχείων. Επομένως στο δεξιό μέλος θα είχαμε ένα γινόμενο **τουλάχιστον τριών αναγώγων στοιχείων**. Άτοπο, γιατί βρισκόμαστε σε περιοχή μοναδικής παραγοντοποίησης. Συμπεραίνουμε λοιπόν ότι τα κ, λ είναι ανάγωγα στο $\mathbb{Z}[\mathrm{i}]$, δηλαδή ανήκουν στην περίπτωση **(i)**. Επειδή βρισκόμαστε σε περιοχή μοναδικής παραγοντοποίησης, θα πρέπει $\kappa \sim \alpha + \beta\mathrm{i} = q$ ή $\lambda \sim \alpha + \beta\mathrm{i} = q$. Αυτό είναι άτοπο γιατί υποθέσαμε ότι το $q = \alpha + \beta\mathrm{i}$ δεν είναι συντροφικό με κάποιον ακέραιο.
Συμπέρασμα: Ο αριθμός $N(q) = N(\alpha + \beta\mathrm{i}) = \alpha^2 + \beta^2$ είναι πρώτος. Το αντίστροφο είναι προφανές. $\big($Βλέπε παρατήρηση $2^{\eta}\big)$. Αν ο $p = \alpha^2 + \beta^2$ είναι πρώτος, τότε ο $\alpha + \beta\mathrm{i}$ $\big($αλλά και ο $\alpha - \beta\mathrm{i}\big)$ είναι ανάγωγα στοιχεία στο $\mathbb{Z}[\mathrm{i}]$. Γιατί $N(\alpha \pm \beta\mathrm{i}) = \alpha^2 + \beta^2 = p$.
Τελικό συμπέρασμα: Τα ανάγωγα στοιχεία του $\mathbb{Z}[\mathrm{i}]$ είναι:
(i) Τα στοιχεία της μορφής $\pm p$, $\pm\mathrm{i}p$, όπου p πρώτος ακέραιος που δεν γράφεται σαν άθροισμα τετραγώνων.
(ii) Τα στοιχεία της μορφής $\alpha + \beta\mathrm{i}$, όπου $\alpha^2 + \beta^2$ πρώτος ακέραιος.

Τώρα, αν θέλουμε να προχωρήσουμε το πράγμα λίγο περισσότερο θα μπορούσαμε να βρούμε τους πρώτους των περιπτώσεων **(i)** και **(ii)**.
Θα ακολουθήσουμε στοιχειώδη μέθοδο, η οποία στηρίζεται σε βασικές γνώσεις Θεωρίας Αριθμών. Έστω p πρώτος που γράφεται ως άθροισμα τετραγώνων, εκτός από το $2 = 1^2 + 1^2$, άρα p περιττός.

1) Ξεκινάμε με το **θεώρημα του Wilson:** Έστω $p > 1$. Τότε ο p είναι πρώτος αν και μόνον αν
$$(p-1)! \equiv -1 \mod p.$$
ΑΠΟΔΕΙΞΗ: Αρχικώς θα αποδείξουμε ότι αν $(p-1)! \equiv -1 \mod p$, τότε ο p είναι πρώτος. Ας

υποθέσουμε λοιπόν ότι ο p είναι σύνθετος και $(p-1)! \equiv -1 \mod p$. Ο p ως σύνθετος θα έχει έναν γνήσιο διαιρέτη n, δηλαδή $1 < n < p$. Τότε $n \leq p-1$ και επομένως $n \mid (p-1)!$. Εφόσον όμως $p \mid (p-1)!+1$ και $n \mid p$, έπεται $n \mid (p-1)!+1$. Επομένως θα ίσχυαν ταυτόχρονα οι σχέσεις $n \mid (p-1)!$ και $n \mid (p-1)!+1$. Από αυτές προκύπτει ότι $n \mid (p-1)!+1-(p-1)! = 1$, δηλαδή $n = 1$, άτοπο.
Αντιστρόφως, υποθέτουμε ότι ο p είναι πρώτος. Θα δείξουμε ότι $p \mid (p-1)!+1$. Για $p = 2$ η σχέση αυτή ισχύει. Επομένως μπορούμε να υποθέσουμε ότι ο p είναι περιττός.
Έστω $\alpha \in \{1, 2, \ldots, p-1\}$. Προφανώς $(\alpha, p) = 1$ και άρα η ισοτιμία $\alpha x \equiv 1 \mod p$ έχει μοναδική λύση modulo p. (Τον **αντίστροφο** του α στο $\mathbb{Z}_p$). Έστω $\alpha' \in \{1, 2, \ldots, p-1\}$ η μοναδική λύση της ισοτιμίας αυτής.
Ποιος είναι τώρα ο αντίστροφος του α' modulo p; Επειδή $\alpha\alpha' \equiv 1 \mod p \Leftrightarrow \alpha'\alpha \equiv 1 \mod p$, ο αντίστροφος $\alpha'' := (\alpha')'$ του α' modulo p αναγκαστικά είναι ο α. (Ο αντίστροφος modulo p εξ ορισμού είναι μοναδικός).
Οι αριθμοί λοιπόν $1, 2, 3, \ldots, p-1$ χωρίζονται εν γένει σε ξένα ζευγάρια-δισύνολα $\{\alpha, \alpha'\}$ αντιστρόφων modulo p. Είναι δυνατόν κάποιος από τους $1, 2, \ldots, p-1$ να είναι αντίστροφος του εαυτού του; Δηλαδή $\alpha^2 \equiv 1 \mod p$; Αυτό είναι ισοδύναμο με τη σχέση $p \mid \alpha^2 - 1 = (\alpha-1)(\alpha+1) \Leftrightarrow \big(p \mid \alpha-1$ ή $p \mid \alpha+1\big) \Leftrightarrow \big(\alpha \equiv 1 \mod p$ ή $\alpha \equiv -1 \equiv p-1 \mod p\big)$. Επειδή δε οι αριθμοί $1, 2, \ldots, p-1$ είναι ανισοϋπόλοιποι modulo p, οι δυνατές περιπτώσεις είναι δύο: $\alpha = 1$ και $\alpha = p-1$.
Συμπερασματικά, οι αριθμοί $2, 3, \ldots, p-2$ χωρίζονται σε ξένα ζευγάρια αντιστρόφων και κατά συνέπεια το γινόμενό τους είναι ισοϋπόλοιπο 1 modulo p. Ο αριθμός 1 δεν αλλάζει το γινόμενο, άρα το $(p-2)!$ είναι ισοϋπόλοιπο modulo p με το 1. Επομένως $(p-1)! = (p-2)!(p-1) \equiv 1 \cdot (p-1) = p-1 \equiv -1 \mod p$. ■

Ένα δεύτερο αποτέλεσμα που θα χρειαστούμε είναι το ακόλουθο:

2) Έστω p περιττός πρώτος. Αν $q = \dfrac{p-1}{2}$, τότε δείξτε $(q!)^2 + (-1)^q \equiv 0 \mod p$. Συμπεράνατε ότι αν $p \equiv 1 \mod 4$, τότε $(q!)^2 \equiv -1 \mod p$.
ΑΠΟΔΕΙΞΗ: Από το θεώρημα του Wilson έχουμε $(p-1)! + 1 \equiv 0 \mod p$. Παρατηρούμε ότι $-k \equiv p-k \mod p$, για κάθε $k = 1, 2, \ldots, \dfrac{p-1}{2}$. Επομένως

$$\begin{aligned} -1 &\equiv p-1 \mod p \\ -2 &\equiv p-2 \mod p \\ -3 &\equiv p-3 \mod p \\ &\vdots \\ -\frac{p-1}{2} &\equiv p - \frac{p-1}{2} = \frac{p+1}{2} \mod p \end{aligned}$$

Άρα

$$\begin{aligned} (p-1)! &= \Big(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\Big) \cdot \Big(\frac{p+1}{2} \cdot \frac{p+3}{2} \cdots (p-1)\Big) \equiv \\ &\equiv \Big(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\Big) \cdot \Big(\Big(-\frac{p-1}{2}\Big) \cdot \Big(-\frac{p-3}{2}\Big) \cdots (-3) \cdot (-2) \cdot (-1)\Big) = \\ &= \Big(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\Big)^2 (-1)^{\frac{p-1}{2}} = (q!)^2 (-1)^q \mod p \end{aligned}$$

.
Επομένως $(q!)^2(-1)^q + 1 \equiv 0 \mod p \Leftrightarrow (q!)^2 \equiv (-1)^{q+1} \mod p$.

Τώρα, αν $p \equiv 1 \mod 4 \Leftrightarrow 2 \Big| \dfrac{p-1}{2} = q \Leftrightarrow 2 \nmid q+1 \Leftrightarrow (-1)^{q+1} = -1$.
Επομένως $(q!)^2 \equiv -1 \mod p$. ■

Το τελευταίο αποτέλεσμα είναι μια «πονηρή» άσκηση, η τελευταία στο κεφάλαιο για τις ισοτιμίες στο βιβλίο του (ελληνικής καταγωγής) Tom M. Apostol, *Introduction to Analytic Number Theory*. (Tom M. Apostol-Θωμάς Αποστολόπουλος).

3) Έστω p περιττός πρώτος και $(\alpha, p) = 1$. Τότε υπάρχουν ακέραιοι x, y τέτοιοι, ώστε $\alpha x \equiv y \mod p$, με $0 < x < \sqrt{p}$ και $0 < |y| < \sqrt{p}$.
Τη λέω «πονηρή» γιατί κάποτε την έλυσα (το πιθανότερο είναι ότι πίστευα ότι την έλυσα) χρησιμοποιώντας την αρχή του περιστερώνα. Όταν την ξαναείδα έδωσα την ακόλουθη λύση:
ΑΠΟΔΕΙΞΗ: Αρχικώς υποθέτουμε ότι $\alpha > 0$. Επειδή ο p δεν είναι τέλειο τετράγωνο, $\lfloor \sqrt{p} \rfloor < \sqrt{p}$. Έστω $k = \lfloor \sqrt{p} \rfloor$. Για κάθε $\lambda \in \{1, 2, \ldots, k\}$ υπάρχει **μοναδικό** $z_\lambda \in \{1, 2, 3, \ldots, p-1\}$ τέτοιο ώστε $\alpha\lambda \equiv z_\lambda \mod p$. Για το σκοπό αυτό αρκεί να δείξουμε ότι οι ακέραιοι z_λ, ισοδύναμα οι ακέραιοι $\alpha\lambda$, όπου $\lambda \in \{1, 2, \ldots, k\}$ είναι ανά δύο ανισοϋπόλοιποι modulo p. Πράγματι, έστω $\alpha\lambda \equiv \alpha\lambda' \mod p$. Τότε επειδή $(\alpha, p) = 1$, παίρνουμε $\lambda \equiv \lambda' \mod p$ και εφόσον $\lambda, \lambda' < p$, έπεται ότι $\lambda = \lambda'$. Έστω $0 < z_{\lambda_1} < z_{\lambda_2} < \cdots < z_{\lambda_k} < p$ η διάταξη των z_λ κατ' αύξον μέγεθος, όπου $\lambda_1, \lambda_2, \ldots, \lambda_k$ μια μετάθεση των $1, 2, \ldots, k$. Διακρίνουμε τρεις περιπτώσεις:
1η περίπτωση: Για κάποιο $\lambda \in \{1, 2, \ldots, k\}$ έχουμε $z_\lambda < \sqrt{p}$. Τότε θέτουμε $x = \lambda$ και $y = z_\lambda$. Επομένως στις επόμενες δύο περιπτώσεις υποθέτουμε ότι $z_\lambda \geq \sqrt{p}$ και επειδή ο $\sqrt{p}$ είναι άρρητος, αυτό είναι ισοδύναμο με $z_\lambda > \sqrt{p} \Leftrightarrow z_\lambda \geq \lfloor \sqrt{p} \rfloor + 1 = k + 1$, για κάθε $\lambda \in \{1, 2, \ldots, k\}$.
2η περίπτωση: $z_{\lambda_{i+1}} < z_{\lambda_i} + \sqrt{p}$, για κάποιο $i \in \{1, 2, \ldots, k-1\}$. Τότε $0 < z_{\lambda_{i+1}} - z_{\lambda_i} < \sqrt{p}$. Επομένως $\alpha(\lambda_{i+1} - \lambda_i) \equiv z_{\lambda_{i+1}} - z_{\lambda_i} \mod p$. Αν $\lambda_{i+1} > \lambda_i$, τότε θέτουμε $0 < x = \lambda_{i+1} - \lambda_i < \sqrt{p}$ και $0 < y = z_{\lambda_{i+1}} - z_{\lambda_i} < \sqrt{p}$ ενώ, αν $\lambda_{i+1} < \lambda_i$, τότε θέτουμε $0 < x = \lambda_i - \lambda_{i+1} < \sqrt{p}$ και $y = z_{\lambda_i} - z_{\lambda_{i+1}}$ με $0 < |y| = |z_{\lambda_i} - z_{\lambda_{i+1}}| = z_{\lambda_{i+1}} - z_{\lambda_i} < \sqrt{p}$.
3η περίπτωση: $z_{\lambda_{i+1}} \geq z_{\lambda_i} + \sqrt{p} \Leftrightarrow z_{\lambda_{i+1}} \geq z_{\lambda_i} + k + 1$, για κάθε $i \in \{1, 2, \ldots, k-1\}$. (Επειδή ο $\sqrt{p}$ είναι άρρητος και οι z_{λ_i}, $z_{\lambda_{i+1}}$ ακέραιοι). Από τις σχέσεις

$$\begin{aligned} z_{\lambda_2} &\geq z_{\lambda_1} + k + 1 \\ z_{\lambda_3} &\geq z_{\lambda_2} + k + 1 \\ &\vdots \\ z_{\lambda_k} &\geq z_{\lambda_{k-1}} + k + 1 \end{aligned}$$

προκύπτει ότι $p > z_{\lambda_k} \geq z_{\lambda_1} + (k-1)(k+1) \geq k + 1 + k^2 - 1 = k^2 + k$. (Έχουμε υποθέσει ότι $z_\lambda \geq \lfloor \sqrt{p} \rfloor + 1 = k + 1$, για κάθε $\lambda \in \{1, 2, \ldots, k\}$). Τότε $0 < p - z_{\lambda_k} \leq p - k^2 - k$. Θα δείξουμε ότι $p - k^2 - k < \sqrt{p} \Leftrightarrow p < k^2 + k + \sqrt{p}$. Έχουμε:
$k^2 = (\lfloor \sqrt{p} \rfloor)^2 > (\sqrt{p} - 1)^2 = p + 1 - 2\sqrt{p}$, $k = \lfloor \sqrt{p} \rfloor > \sqrt{p} - 1$ και επομένως $k^2 + k + \sqrt{p} > p + 1 - 2\sqrt{p} + \sqrt{p} - 1 + \sqrt{p} = p$, δηλαδή αυτό που θέλαμε. Άρα $0 < p - z_{\lambda_k} \leq p - k^2 - k < \sqrt{p}$. Τώρα, $\alpha\lambda_k \equiv z_{\lambda_k} \equiv z_{\lambda_k} - p \mod p$. Θέτουμε $x = \lambda_k$ και $y = z_{\lambda_k} - p$. Τότε $0 < x < \sqrt{p}$ και $0 < |y| = |z_{\lambda_k} - p| = p - z_{\lambda_k} < \sqrt{p}$.
Απομένει η περίπτωση $\alpha < 0$. Αλλά τότε υπάρχουν ακέραιοι x και y με $-\alpha x \equiv y \mod p$, όπου $0 < x < \sqrt{p}$ και $0 < |y| < \sqrt{p}$. Συνεπώς $\alpha x \equiv -y \mod p$, με $0 < x < \sqrt{p}$ και $0 < |-y| = |y| < \sqrt{p}$. ■

ΣΥΜΠΕΡΑΣΜΑ: Έστω p περιττός πρώτος. Τα επόμενα είναι ισοδύναμα:
(i) Υπάρχει ακέραιος α τέτοιος, ώστε $\alpha^2 \equiv -1 \mod p$.

(ii) Ο p γράφεται σαν άθροισμα δύο τετραγώνων.
(iii) $p \equiv 1 \mod 4$.
ΑΠΟΔΕΙΞΗ: (i)⇒(ii) Έστω $\alpha \in \mathbb{Z}$ με $\alpha^2 \equiv -1 \mod p$. Από το προηγούμενο λήμμα προκύπτει ότι υπάρχουν ακέραιοι x και y τέτοιοι, ώστε $0 < x < \sqrt{p}$, $0 < |y| < \sqrt{p}$ και $\alpha x \equiv y \mod p$. Επομένως $\alpha^2 x^2 \equiv y^2 \mod p \Leftrightarrow -x^2 \equiv y^2 \mod p \Leftrightarrow p \mid x^2 + y^2$. Άρα $p \leq x^2 + y^2 < < (\sqrt{p})^2 + (\sqrt{p})^2 = 2p$. Επομένως $p = x^2 + y^2$.
(ii)⇒(iii) Έστω $p = x^2 + y^2$, όπου x, y ακέραιοι. Αν οι x, y ήσαν και οι δύο άρτιοι ή και οι δύο περιττοί, τότε ο p θα ήταν άρτιος. Άρα ο ένας π.χ. ο x είναι περιττός και ο y άρτιος. Έστω $x = 2m + 1$ και $y = 2n$. Τότε $p = x^2 + y^2 = 4(m^2 + m + n^2) + 1 \equiv 1 \mod 4$.
(iii)⇒(i) Έστω $p \equiv 1 \mod 4$. Από το πρώτο αποτέλεσμα που δείξαμε, για $\alpha = q!$, όπου $q = \dfrac{p-1}{2}$, έχουμε $\alpha^2 = (q!)^2 \equiv -1 \mod p$. ■

Σύμφωνα με το προηγούμενο συμπέρασμα η ικανή και αναγκαία συνθήκη για να γράφεται ένας περιττός πρώτος p ως άθροισμα δύο τετραγώνων είναι η $p \equiv 1 \mod 4$.
Επομένως τα ανάγωγα στοιχεία στον δακτύλιο $\mathbb{Z}[\mathrm{i}]$ της περίπτωσης **(ii)** είναι τα $(1 \pm \mathrm{i}), (-1 \pm \mathrm{i})$ που αντιστοιχούν στο $2 = 1^2 + 1^2$ και τα $\alpha + \beta\mathrm{i}$ με $\alpha^2 + \beta^2 = p$ πρώτος, με $p \equiv 1 \mod 4$. Άρα τα ανάγωγα στοιχεία της περιπτώσεως **(i)** είναι της μορφής $\pm p, \pm \mathrm{i}p$, όπου $p \in \mathbb{Z}$ περιττός πρώτος, με $p \equiv 3 \mod 4$.

Σύμφωνα με το προηγούμενο συμπέρασμα η ικανή και αναγκαία συνθήκη για να γράφεται ένας περιττός πρώτος p ως άθροισμα δύο τετραγώνων είναι η $p \equiv 1 \mod 4$. Στην επόμενη πρόταση θα αποδείξουμε ότι η μορφή αυτή είναι μοναδική.

ΠΡΟΤΑΣΗ 2.35. Έστω p περιττός πρώτος με $p \equiv 1 \mod 4$. Έστω α, β, γ, δ θετικοί ακέραιοι με $\alpha^2 + \beta^2 = \gamma^2 + \delta^2 = p$. Τότε $\alpha = \gamma$ και $\beta = \delta$ ή $\alpha = \delta$ και $\beta = \gamma$.
ΑΠΟΔΕΙΞΗ: Προφανώς $(\alpha, \beta) = 1$, γιατί $0 < (\alpha, \beta) < p$ και $(\alpha, \beta) \mid p$. Ανάλογα έχουμε $(\gamma, \delta) = 1$.
Παρατηρούμε ότι $(\alpha\gamma + \beta\delta)(\alpha\delta + \beta\gamma) = (\alpha^2 + \beta^2)\gamma\delta + (\gamma^2 + \delta^2)\alpha\beta = p(\alpha\beta + \gamma\delta)$.
Κατά συνέπεια $p \mid \alpha\gamma + \beta\delta$ ή $p \mid \alpha\delta + \beta\gamma$.
Έστω ότι $p \mid \alpha\gamma + \beta\delta$, δηλαδή $\alpha\gamma + \beta\delta = kp$, όπου k θετικός ακέραιος. (Όλοι οι εμφανιζόμενοι αριθμοί είναι θετικοί). Έχουμε:

$$p^2 = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2) = (\alpha\gamma + \beta\delta)^2 + (\alpha\delta - \beta\gamma)^2 = k^2p^2 + (\alpha\delta - \beta\gamma)^2$$

και επειδή $k > 0$, θα πρέπει αναγκαστικά $k = 1$ και $\alpha\delta - \beta\gamma = 0 \Leftrightarrow \alpha\delta = \beta\gamma$. Συνεπώς $\alpha \mid \beta\gamma$ και επειδή $(\alpha, \beta) = 1$, $\alpha \mid \gamma$, δηλαδή $\gamma = \lambda\alpha$, για κάποιον θετικό ακέραιο λ. Αλλά τότε και $\delta = \lambda\beta$. Επομένως $p = \gamma^2 + \delta^2 = \lambda^2(\alpha^2 + \beta^2) = \lambda^2 p$. Συμπεραίνουμε ότι $\lambda = 1$ και κατά συνέπεια $\gamma = \alpha$ και $\delta = \beta$.
Έστω τώρα ότι $p \mid \alpha\delta + \beta\gamma$, δηλαδή $\alpha\delta + \beta\gamma = rp$, όπου r θετικός ακέραιος. Έχουμε:

$$p^2 = (\alpha^2 + \beta^2)(\gamma^2 + \delta^2) = (\alpha\gamma - \beta\delta)^2 + (\alpha\delta + \beta\gamma)^2 = (\alpha\gamma - \beta\delta)^2 + r^2p^2.$$

Προχωρώντας όπως προηγουμένως συνάγουμε ότι $\gamma = \beta$ και $\delta = \alpha$. ■

ΠΑΡΑΔΕΙΓΜΑ 2.36. Να αναλύσετε στο $\mathbb{Z}[\mathrm{i}]$ τους παρακάτω αριθμούς σε γινόμενο πρώτων παραγόντων:
(i) $-7 - 28\mathrm{i}$, **(ii)** $-45 - 163\mathrm{i}$ και **(iii)** $11 - 231\mathrm{i}$.
ΛΥΣΗ: (i) Παρατηρούμε ότι $7 \equiv 3 \mod 4$ και συνεπώς το 7 είναι πρώτος στον $\mathbb{Z}[\mathrm{i}]$. Επίσης, $-7 - 28\mathrm{i} = (-7) \cdot (1 + 4\mathrm{i})$ και $1^2 + 4^2 = 17 \equiv 1 \mod 4$. Επομένως ο $1 + 4\mathrm{i}$ είναι πρώτος στον $\mathbb{Z}[\mathrm{i}]$. Κατά συνέπεια η σχέση $-7 - 28\mathrm{i} = (-7) \cdot (1 + 4\mathrm{i})$ είναι μια ανάλυση του $-7 - 28\mathrm{i}$ σε γινόμενο

πρώτων παραγόντων.
(ii) Παρατηρούμε ότι $N(-45-163\mathrm{i}) = 45^2+163^2 = 28594 = 2\cdot 17\cdot 29^2$. Έχουμε $2 = (1+\mathrm{i})(1-\mathrm{i})$ και $17 \equiv 29 \equiv 1 \mod 4$ και $17 = 1^2+4^2$ και $29 = 2^2+5^2$. Επίσης, $\dfrac{-45-163\mathrm{i}}{2+5\mathrm{i}} = \dfrac{(-45-163\mathrm{i})(2-5\mathrm{i})}{(2+5\mathrm{i})(2-5\mathrm{i})} = \dfrac{-905-101\mathrm{i}}{29} \notin \mathbb{Z}[\mathrm{i}]$, ενώ $\dfrac{-45-163\mathrm{i}}{(2-5\mathrm{i})^2} = \dfrac{(-45-163\mathrm{i})(2+5\mathrm{i})^2}{(2-5\mathrm{i})^2(2+5\mathrm{i})^2} = \dfrac{4205+2523\mathrm{i}}{29^2} = 5+3\mathrm{i}$. Ακόμη $\dfrac{5+3\mathrm{i}}{4+\mathrm{i}} = \dfrac{(5+3\mathrm{i})(4-\mathrm{i})}{(4+\mathrm{i})(4-\mathrm{i})} = \dfrac{23+7\mathrm{i}}{17} \notin \mathbb{Z}[\mathrm{i}]$, ενώ $\dfrac{5+3\mathrm{i}}{4-\mathrm{i}} = \dfrac{(5+3\mathrm{i})(4+\mathrm{i})}{(4-\mathrm{i})(4+\mathrm{i})} = \dfrac{17+17\mathrm{i}}{17} = 1+\mathrm{i}$. Άρα μια ανάλυση του $-45-163\mathrm{i}$ σε γινόμενο ανάγωγων παραγόντων είναι $-45-163\mathrm{i} = (1+\mathrm{i})(4-\mathrm{i})(2-5\mathrm{i})^2$.
(iii) Παρατηρούμε ότι $N(11-231\mathrm{i}) = 11^2+231^2 = 53482 = 2\cdot 11^2\cdot 13\cdot 17$. Προφανώς $11 \equiv 3 \mod 4$. Επομένως $11 \mid 11-231\mathrm{i}$. Πράγματι, $\dfrac{11-231\mathrm{i}}{11} = 1-21\mathrm{i}$. Επειδή $17 \equiv 1 \mod 4$, θα έχουμε $17 = 1^2+4^2 = (1+4\mathrm{i})(1-4\mathrm{i})$ και άρα $1+4\mathrm{i} \mid 1-21\mathrm{i}$ ή $1-4\mathrm{i} \mid 1-21\mathrm{i}$. Παρατηρούμε ότι $\dfrac{1-21\mathrm{i}}{1+4\mathrm{i}} = \dfrac{(1-21\mathrm{i})(1-4\mathrm{i})}{17} = \dfrac{-83-25\mathrm{i}}{17} \notin \mathbb{Z}[\mathrm{i}]$, γιατί $17 \nmid 25$, αλλά $\dfrac{1-21\mathrm{i}}{1-4\mathrm{i}} = \dfrac{(1-21\mathrm{i})(1+4\mathrm{i})}{17} = \dfrac{85-17\mathrm{i}}{17} = 5-\mathrm{i}$. Επίσης, $13 = (2+3\mathrm{i})(2-3\mathrm{i})$, άρα $2+3\mathrm{i} \mid 5-\mathrm{i}$ ή $2-3\mathrm{i} \mid 5-\mathrm{i}$. Παρατηρούμε ότι $\dfrac{5-\mathrm{i}}{2+3\mathrm{i}} = \dfrac{(5-\mathrm{i})(2-3\mathrm{i})}{13} = \dfrac{7-17\mathrm{i}}{13} \notin \mathbb{Z}[\mathrm{i}]$, ενώ $\dfrac{5-\mathrm{i}}{2-3\mathrm{i}} = \dfrac{(5-\mathrm{i})(2+3\mathrm{i})}{13} = \dfrac{13+13\mathrm{i}}{13} = 1+\mathrm{i}$. Κατά συνέπεια $11-231\mathrm{i} = (1+\mathrm{i})(2-3\mathrm{i})(1-4\mathrm{i})\cdot 11$. ■

Στη συνέχεια θα δώσουμε μια απόδειξη για το πλήθος των στοιχείων του δακτυλίου-πηλίκο $\mathbb{Z}[\mathrm{i}]\Big/(\alpha+\beta\mathrm{i})$, όπου $(\alpha+\beta\mathrm{i})$ το (κύριο) ιδεώδες που παράγεται από το στοιχείο $\alpha+\beta\mathrm{i} \in \mathbb{Z}[\mathrm{i}]\setminus\{0\}$.

ΛΗΜΜΑ 2.37. Αν $\alpha+\beta\mathrm{i} \in \mathbb{Z}[\mathrm{i}]\setminus\{0\}$, τότε ο δακτύλιος $\mathbb{Z}[\mathrm{i}]\Big/(\alpha+\beta\mathrm{i})$ περιέχει πεπερασμένο το πλήθος στοιχεία.
ΑΠΟΔΕΙΞΗ: Έστω $x+y\mathrm{i}+(\alpha+\beta\mathrm{i}) \in \mathbb{Z}[\mathrm{i}]\Big/(\alpha+\beta\mathrm{i})$. Αν $\upsilon = \kappa+\lambda\mathrm{i}$ είναι ένα υπόλοιπο της διαίρεσης $(x+y\mathrm{i}) : (\alpha+\beta\mathrm{i})$, τότε $\big(\upsilon = 0 \Leftrightarrow \kappa = \lambda = 0\big)$ ή $N(\upsilon) = \kappa^2+\lambda^2 < N(\alpha+\beta\mathrm{i}) = \alpha^2+\beta^2$. Επίσης $x+y\mathrm{i}+(\alpha+\beta\mathrm{i}) = \kappa+\lambda\mathrm{i}+(\alpha+\beta\mathrm{i})$. Αλλά λόγω της σχέσης $\kappa^2+\lambda^2 < \alpha^2+\beta^2$, οι δυνατές επιλογές για τα κ και λ είναι πεπερασμένες. ■

Ας συμβολίσουμε με $n(r)$ το πλήθος των κλάσεων ισοδυναμίας modulo r, όπου $r \in \mathbb{Z}[\mathrm{i}]\setminus\{0\}$, δηλαδή $n(r) = \Big|\mathbb{Z}[\mathrm{i}]\Big/(r)\Big|$.

ΛΗΜΜΑ 2.38. Έστω $r \in \mathbb{Z}[\mathrm{i}]\setminus\{0\}$. Τότε το πλήθος των κλάσεων ισοδυναμίας modulo r ισούται με το πλήθος των κλάσεων ισοδυναμίας modulo $\overline{r}$, δηλαδή $n(r) = n(\overline{r})$.
ΑΠΟΔΕΙΞΗ: Έστω $s,t \in \mathbb{Z}[\mathrm{i}]$. Τότε $s \equiv t \mod r \Leftrightarrow s = t+\lambda r$, για κάποιο $\lambda \in \mathbb{Z}[\mathrm{i}]$, ισοδύναμα $\overline{s} = \overline{t}+\overline{\lambda}\,\overline{r}$, ισοδύναμα $\overline{s} \equiv \overline{t} \mod \overline{r}$. ■

ΛΗΜΜΑ 2.39. Έστω $r_1, r_2 \in \mathbb{Z}[\mathrm{i}]\setminus\{0\}$. Τότε το πλήθος των κλάσεων ισοδυναμίας modulo r_1r_2 ισούται με το γινόμενο του πλήθους των κλάσεων ισοδυναμίας modulo r_1 επί το πλήθος των κλάσεων ισοδυναμίας modulo r_2. Με άλλα λόγια $n(r_1r_2) = n(r_1)n(r_2)$.
ΑΠΟΔΕΙΞΗ: Έστω $t_1, t_2, \ldots, t_{n(r_1)}$ και $s_1, s_2, \ldots, s_{n(r_2)}$ αντιπρόσωποι των κλάσεων ισοδυναμίας modulo r_1 και modulo r_2 αντίστοιχα. Θεωρούμε τα $n(r_1)n(r_2)$ στοιχεία $t_\kappa + s_\lambda r_1$, όπου $\kappa =$

$= 1, \ldots, n(r_1)$ και $\lambda = 1 \ldots, n(r_2)$. Έστω $t_\kappa + s_\lambda r_1 \equiv t_{\kappa_0} + s_{\lambda_0} r_1 \mod (r_1 r_2)$. Τότε $r_1 \mid t_\kappa - t_{\kappa_0}$ και επομένως $\kappa = \kappa_0$. Κατά συνέπεια $s_\lambda r_1 \equiv s_{\lambda_0} r_1 \mod (r_1 r_2) \underset{r_1 \neq 0}{\Leftrightarrow} s_\lambda \equiv s_{\lambda_0} \mod r_2$ και άρα $\lambda = \lambda_0$. Τώρα, έστω $x \in \mathbb{Z}[\mathrm{i}]$. Τότε $x \equiv t_\kappa \mod r_1$, για κάποιο $\kappa = 1, \ldots, n(r_1)$, δηλαδή $x = t_\kappa + y r_1$, όπου $y \in \mathbb{Z}[\mathrm{i}]$. Τώρα $y \equiv s_\lambda \mod r_2$ και συνεπώς $y = s_\lambda + \mu r_2$, όπου $\mu \in \mathbb{Z}[\mathrm{i}]$. Επομένως $x = t_\kappa + (s_\lambda + \mu r_2) r_1 = t_\kappa + s_\lambda r_1 + \mu r_1 r_2 \equiv t_\kappa + s_\lambda r_1 \mod (r_1 r_2)$. ■

ΛΗΜΜΑ 2.40. Έστω r θετικός ακέραιος. Τότε $n(r) = r^2$.
ΑΠΟΔΕΙΞΗ: Θεωρούμε τους r^2 μιγαδικούς $\kappa + \mathrm{i}\lambda$, όπου $\kappa, \lambda \in \{0, 1, \ldots, r-1\}$. Αν $\kappa + \mathrm{i}\lambda \equiv \equiv \kappa_0 + \mathrm{i}\lambda_0 \mod r$, τότε $\kappa + \mathrm{i}\lambda = \kappa_0 + \mathrm{i}\lambda_0 + (\mu + \mathrm{i}\nu) r$, για κάποιους $\mu, \nu \in \mathbb{Z}$ και επομένως $\kappa - \kappa_0 + (\lambda - \lambda_0)\mathrm{i} = \mu r + \mathrm{i}\nu r$. Συνεπώς $\kappa - \kappa_0 = \mu r$ και $\lambda - \lambda_0 = \nu r$, άρα $r \mid \kappa - \kappa_0$ και $r \mid \lambda - \lambda_0$, ήτοι $\kappa \equiv \kappa_0 \mod r$ και $\lambda \equiv \lambda_0 \mod r$. Συνεπώς $\kappa = \kappa_0$ και $\lambda = \lambda_0$.
Έστω τώρα $x = s + \mathrm{i}t \in \mathbb{Z}[\mathrm{i}]$. Αν κ είναι το υπόλοιπο της διαίρεσης $s : r$ και λ το υπόλοιπο της διαίρεσης $t : r$, τότε $x = \pi_1 r + \kappa + (\pi_2 r + \lambda)\mathrm{i} = \kappa + \lambda\mathrm{i} + (\pi_1 + \pi_2) r$, όπου π_1, π_2 τα πηλίκα των αντίστοιχων διαιρέσεων. Προφανώς $x \equiv \kappa + \lambda\mathrm{i} \mod r$. ■

ΠΡΟΤΑΣΗ 2.41. $n(\alpha + \beta\mathrm{i}) = N(\alpha + \beta\mathrm{i}) = \alpha^2 + \beta^2$.
ΑΠΟΔΕΙΞΗ: Από το λήμμα 2.38 έχουμε $n(\alpha + \beta\mathrm{i}) = n(\alpha - \beta\mathrm{i})$. Επίσης από το λήμμα 2.39 έχουμε $n(\alpha^2 + \beta^2) = n((\alpha + \beta\mathrm{i})(\alpha - \beta\mathrm{i})) = n(\alpha + \beta\mathrm{i}) n(\alpha - \beta\mathrm{i}) = n(\alpha + \beta\mathrm{i})^2$. Τέλος, από το λήμμα 2.40 έχουμε $n(\alpha^2 + \beta^2) = (\alpha^2 + \beta^2)^2$. Άρα $n(\alpha + \beta\mathrm{i})^2 = (\alpha^2 + \beta^2)^2$ και κατά συνέπεια $n(\alpha + \beta\mathrm{i}) = \alpha^2 + \beta^2 = N(\alpha + \beta\mathrm{i})$, δηλαδή $\left| \mathbb{Z}[\mathrm{i}] \Big/ (\alpha + \beta\mathrm{i}) \right| = \alpha^2 + \beta^2$. ■

2.5 Ο Πολυωνυμικός Δακτύλιος $R[x]$, όπου R Περιοχή Μοναδικής Παραγοντοποίησης

Στόχος μας είναι να αποδείξουμε το επόμενο θεώρημα:

ΘΕΩΡΗΜΑ 2.42. Έστω R περιοχή μοναδικής παραγοντοποίησης. Τότε και ο δακτύλιος $R[x]$ των πολυωνύμων με συντελεστές από το R είναι επίσης περιοχή μοναδικής παραγοντοποίησης.

Κατ' αρχάς σημειώνουμε ότι $R \subseteq R[x] \subseteq \mathbb{K}[x]$, όπου $\mathbb{K}$ το σώμα πηλίκων της R. Για να αποδείξουμε το θεώρημα αυτό θα ακολουθήσουμε μια σειρά από βήματα-λήμματα.

ΛΗΜΜΑ 2.43. Τα ανάγωγα στοιχεία της R παραμένουν ανάγωγα στην περιοχή $R[x]$. Συνεπώς τα μη αντιστρέψιμα στοιχεία της R παραμένουν μη αντιστρέψιμα και στην $R[x]$.
ΑΠΟΔΕΙΞΗ: Έστω $p \in R$ ανάγωγο. Υποθέτουμε ότι $p = f(x)g(x)$, όπου $f(x), g(x) \in R[x]$. Προφανώς $0 = \deg p = \deg(f(x)g(x)) = \deg f(x) + \deg g(x)$ και $\deg f(x), \deg g(x) \geq 0$. Επομένως $\deg f(x) = \deg g(x) = 0$, δηλαδή $f(x), g(x) \in R$ σταθερά πολυώνυμα. Έστω $f(x) = \alpha$ και $g(x) = \beta$. Η σχέση $p = \alpha\beta$ στο R συνεπάγεται ότι κάποιο από τα $\alpha, \beta \in R$ είναι αντιστρέψιμο $\big($και το άλλο συντροφικό με το $p\big)$. ■

ΟΡΙΣΜΟΣ 2.44. Ένα πολυώνυμο $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n \in R[x]$ $\big(\alpha_i \in R\big)$ λέγεται **πρωταρχικό** αν το 1 είναι ένας μέγιστος κοινός διαιρέτης των συντελεστών του α_i, $i = 0, 1, \ldots, n$.

Παρατήρηση: $\big($Ίσως χαζή, αλλά χρήσιμη$\big)$. Αν δ είναι ένας μέγιστος κοινός διαιρέτης των συντελεστών $\alpha_i \in R$ του πολυωνύμου $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n$, τότε προφανώς $\alpha_i = \delta\beta_i$, για κάθε $i = 0, 1, \ldots, n$ και το πολυώνυμο $g(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \cdots + \beta_n x^n$ με $f(x) = \delta g(x)$ είναι πρωταρχικό. Πράγματι, αν u είναι ένας μέγιστος κοινός διαιρέτης των

$\beta_0, \beta_1, \beta_2, \ldots, \beta_n$, τότε $\beta_i = u\gamma_i$, για κάθε i $\big(\gamma_i \in R\big)$ και άρα $\alpha_i = \delta\beta_i = \delta u\gamma_i$, για κάθε i. Άρα $\delta u \mid \alpha_i$, για κάθε i και άρα το δu είναι κοινός διαιρέτης των $\alpha_0, \alpha_1, \ldots, \alpha_n$ και από τον ορισμό του μέγιστου κοινού διαιρέτη, $\delta u \mid \delta \Leftrightarrow \delta = \delta ur$, $r \in R$. Συνεπώς $\delta(1-ur) = 0 \underset{\delta \neq 0_R}{\Leftrightarrow} ur = 1$, δηλαδή το u είναι αντιστρέψιμο και άρα το $g(x)$ είναι πρωταρχικό.

ΛΗΜΜΑ 2.45. Έστω $f(x), g(x) \in R[x]$ πρωταρχικά και $\alpha, \beta \in R \setminus \{0\}$. Αν $\alpha f(x) = \beta g(x)$, τότε $\alpha \sim \beta$.
ΑΠΟΔΕΙΞΗ: Εφαρμόζουμε επαγωγή επί του $\lambda(\alpha) + \lambda(\beta)$, όπου $\lambda(x)$ το μήκος του $x \in R \setminus \{0\}$. Αν $\lambda(\alpha)+\lambda(\beta) = 0 \Leftrightarrow \lambda(\alpha) = \lambda(\beta) = 0$, τα στοιχεία α και β είναι αντιστρέψιμα, άρα συντροφικά. Έστω p ανάγωγος διαιρέτης του α. Τότε $p \mid \beta g(x) \Leftrightarrow p \cdot h(x) = \beta g(x)$, με $h(x) \in R[x]$. Είναι σαφές ότι $\deg h(x) = \deg(p \cdot h(x)) = \deg(\beta g(x)) = \deg g(x)$. Αν $g(x) = b_0 + b_1 x + \cdots + b_m x^m$, τότε $h(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_m x^m$ και $\beta g(x) = \beta b_0 + \beta b_1 x + \cdots + \beta b_m x^m$, όπου $\gamma_i, b_i \in R$, για κάθε $i = 0, 1, \ldots, m$. Άρα $p\gamma_i = \beta b_i \Rightarrow p \mid \beta b_i$, για κάθε $i = 0, 1, \ldots, m$. Επειδή το $g(x)$ είναι πρωταρχικό, υπάρχει κάποιος συντελεστής b_k με $p \nmid b_k$. Εφόσον R περιοχή μοναδικής παραγοντοποίησης, το p είναι πρώτο. Επειδή δε $p \mid \beta b_k$ και $p \nmid b_k$, έπεται ότι $p \mid \beta$. Επομένως $\alpha = p\alpha'$ και $\beta = p\beta'$ με $\lambda(\alpha') = \lambda(\alpha) - 1$ και $\lambda(\beta') = \lambda(\beta) - 1$. Επίσης $p\alpha' f(x) = p\beta' g(x) \underset{\substack{R[x] \text{ ακέραια} \\ \text{περιοχή}}}{\Leftrightarrow} \alpha' f(x) = \beta' g(x)$.
Με βάση το επαγωγικό βήμα, $\alpha' \sim \beta' \Rightarrow p\alpha' \sim p\beta' \Leftrightarrow \alpha \sim \beta$. ■

ΛΗΜΜΑ 2.46. $\big($**ΛΗΜΜΑ του GAUSS**$\big)$**:** Το γινόμενο δύο ή περισσοτέρων πρωταρχικών πολυωνύμων είναι πρωταρχικό.
ΑΠΟΔΕΙΞΗ: Έστω $f(x), g(x) \in R[x]$ πρωταρχικά με $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_m x^m$ και $g(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \cdots + \beta_n x^n$. Υποθέτουμε ότι το $f(x)g(x)$ δεν είναι πρωταρχικό. Τότε, αν $f(x)g(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{m+n} x^{m+n}$, θα υπάρχει ανάγωγο στοιχείο p με $p \mid c_i$, για κάθε $i = 0, 1, \ldots, m+n$. Έστω κ και λ οι ελάχιστοι δείκτες με $p \nmid \alpha_\kappa$ και $p \nmid \beta_\lambda$. Τότε $p \mid \alpha_i$ για κάθε $i < \kappa$ και $p \mid \beta_j$ για κάθε $j < \lambda$. $\big($Αν φυσικά υπάρχουν τέτοια i και j, δηλαδή όταν $\kappa > 0$ ή $\lambda > 0\big)$. Τότε $\kappa \leq m$ και $\lambda \leq n$. Θεωρούμε τον συντελεστή $c_{\kappa+\lambda}$ του $f(x)g(x)$. Παρατηρούμε ότι $c_{\kappa+\lambda} = \sum_{i<\kappa} \alpha_i \beta_{\kappa+\lambda-i} + \sum_{j<\lambda} \alpha_{\kappa+\lambda-j}\beta_j + \alpha_\kappa \beta_\lambda$. Επειδή $p \mid \alpha_i$ και $p \mid \beta_j$, για κάθε $i < \kappa$ και $j < \lambda$, έπεται ότι $p \mid \sum_{i<\kappa} \alpha_i \beta_{\kappa+\lambda-i}$ και $p \mid \sum_{j<\lambda} \alpha_{\kappa+\lambda-j}\beta_j$. Όμως $p \mid c_{\kappa+\lambda}$. Επομένως $p \mid \alpha_\kappa \beta_\lambda$. Αλλά το p είναι πρώτο στην R και $p \nmid \alpha_\kappa$ και $p \nmid \beta_\lambda$, άτοπο. Συμπέρασμα: τέτοιο p δεν υπάρχει και συνεπώς το $f(x)g(x)$ είναι πρωταρχικό.
Η απόδειξη ολοκληρώνεται με επαγωγή επί του πλήθους των πρωταρχικών πολυωνύμων. ■

ΛΗΜΜΑ 2.47. Αν $f(x) \in R[x]$ μη σταθερό πολυώνυμο και $f(x)$ ανάγωγο στην $R[x]$, τότε το $f(x)$ είναι πρωταρχικό $\big($στην $R[x]\big)$ και ανάγωγο στην $\mathbb{K}[x]$.
ΑΠΟΔΕΙΞΗ: Έστω u ένας μέγιστος κοινός διαιρέτης των συντελεστών του $f(x)$ στην $R[x]$. Τότε $f(x) = u \cdot g(x)$, όπου $g(x)$ πρωταρχικό. Αν το u δεν ήταν αντιστρέψιμο στην $R \subseteq R[x]$, επειδή το $g(x)$ $\big($ως μη σταθερό πολυώνυμο$\big)$ δεν είναι αντιστρέψιμο στην $R[x]$, τότε το $f(x) = u \cdot g(x)$ θα ήταν γινόμενο δύο μη αντιστρεψίμων στοιχείων της $R[x]$, άρα όχι ανάγωγο. Συνεπώς το u είναι αντιστρέψιμο στην R. Άρα το $f(x)$ είναι πρωταρχικό στην $R[x]$.
Τώρα, τα μη αντιστρέψιμα στοιχεία στην ευκλείδεια περιοχή $\mathbb{K}[x]$ είναι το 0 και τα μη σταθερά πολυώνυμα. Αν λοιπόν το $f(x)$ δεν ήταν ανάγωγο στο $\mathbb{K}[x]$, τότε θα υπήρχαν μη σταθερά πολυώνυμα $f_1(x), f_2(x) \in \mathbb{K}[x]$ τέτοια, ώστε $f(x) = f_1(x)f_2(x)$. Έστω ε_i το ελάχιστο κοινό πολλαπλάσιο των παρονομαστών των συντελεστών του $f_i(x)$ $\big(i = 1, 2\big)$ και d_i ο μέγιστος κοινός διαιρέτης των συντελεστών του $\varepsilon_i f_i(x) \in R[x]$ $\big(i = 1, 2\big)$. Τότε $\varepsilon_i f_i(x) = d_i g_i(x)$, όπου $g_i(x) \in R[x]$ πρωταρχικό, για κάθε $i = 1, 2$. Επομένως $\varepsilon_1\varepsilon_2 f(x) = d_1 d_2 g_1(x) g_2(x)$. Το πολυώνυμο $f(x)$ είναι πρωταρχικό, καθώς και το γινόμενο $g_1(x)g_2(x)$. $\big($Βλέπε λήμμα του Gauss$\big)$.

Από το λήμμα 2.45 συνάγουμε ότι $\varepsilon_1\varepsilon_2 \sim d_1d_2$. Επομένως $f(x) = ug_1(x)g_2(x)$, όπου u αντιστρέψιμο στο R, δηλαδή το $f(x)$ θα ήταν ίσο με ένα γινόμενο δύο μη σταθερών και άρα μη αντιστρεψίμων στην $R[x]$ πολυωνύμων. Των $ug_1(x)$ και $g_2(x)$. Αυτό είναι άτοπο γιατί το $f(x)$ είναι ανάγωγο στο $R[x]$. ■

Ισχύει και το αντίστροφο:

ΠΡΟΤΑΣΗ 2.48. Έστω $f(x) \in R[x]$ μη σταθερό πολυώνυμο. Αν το $f(x)$ είναι πρωταρχικό στην $R[x]$ και ανάγωγο στην $\mathbb{K}[x]$, τότε είναι ανάγωγο στην $R[x]$.
ΑΠΟΔΕΙΞΗ: Έστω $f(x) = f_1(x)f_2(x)$ με $f_1(x), f_2(x) \in R[x]$. Αν και τα δύο πολυώνυμα $f_1(x), f_2(x)$ ήταν μη σταθερά στην $R[x]$, άρα και στην $\mathbb{K}[x]$, τότε θα ήσαν μη αντιστρέψιμα στην $\mathbb{K}[x]$, άρα το $f(x) = f_1(x)f_2(x)$ δεν θα ήταν ανάγωγο στην $\mathbb{K}[x]$, άτοπο. Άρα κάποιο από τα δύο, έστω το $f_1(x)$ είναι σταθερό, δηλαδή $f_1(x) = r \in R$. Αν το r δεν ήταν αντιστρέψιμο στην R, τότε θα είχε έναν ανάγωγο διαιρέτη $p \in R$. Επειδή $f(x) = f_1(x)f_2(x) = rf_2(x)$ και $p \mid r$, το p θα διαιρούσε όλους τους συντελεστές του $f(x)$. Αυτό είναι άτοπο, γιατί το $f(x)$ είναι πρωταρχικό στην $R[x]$. Συνεπώς το $r = f_1(x)$ είναι αντιστρέψιμο στην $R[x]$. ■

ΣΥΜΠΕΡΑΣΜΑ: Τα ανάγωγα στοιχεία της $R[x]$ είναι:
1) Τα ανάγωγα στοιχεία της R και
2) τα μη σταθερά πολυώνυμα της $R[x]$, τα οποία είναι πρωταρχικά στην $R[x]$ και ανάγωγα στην $\mathbb{K}[x]$.

ΠΡΟΤΑΣΗ 2.49. Κάθε μη μηδενικό και μη αντιστρέψιμο στοιχείο της $R[x]$ αναλύεται σε γινόμενο αναγώγων στοιχείων της $R[x]$.
ΑΠΟΔΕΙΞΗ: Αν $f(x) = r \in R$, τότε αυτό προκύπτει από το γεγονός ότι η R είναι περιοχή μοναδικής παραγοντοποίησης.
Έστω λοιπόν ότι το $f(x) \in R[x]$ είναι μη σταθερό πολυώνυμο. Αν δ είναι ένας μέγιστος κοινός διαιρέτης των συντελεστών του $f(x)$, τότε $f(x) = \delta g(x)$, όπου $g(x) \in R[x]$ πρωταρχικό. Το $g(x)$ αναλύεται στο $\mathbb{K}[x]$ σε γινόμενο αναγώγων $\big($άρα μη σταθερών$\big)$ πολυωνύμων $g_1(x), g_2(x), \ldots, g_k(x) \in \mathbb{K}[x]$. Όπως προηγουμένως, θέτουμε ε_i για το ελάχιστο κοινό πολλαπλάσιο των παρονομαστών των συντελεστών του $g_i(x)$ και έστω d_i ένας μέγιστος κοινός διαιρέτης των συντελεστών του $\varepsilon_i g_i(x) \in R[x]$, για κάθε $i = 1, \ldots, k$. Άρα $\varepsilon_i g_i(x) = d_i h_i(x)$, όπου $h_i(x)$ πρωταρχικό, για κάθε $i = 1, \ldots, k$. Επειδή δε $h_i(x) \sim g_i(x)$ $\big($στην $\mathbb{K}[x]\big)$, το $h_i(x)$ είναι και ανάγωγο στην $\mathbb{K}[x]$, άρα είναι ανάγωγο στην $R[x]$. Επομένως $\varepsilon_1 \cdots \varepsilon_k \delta \cdot g(x) = d_1 \cdots d_k h_1(x) \cdots h_k(x)$. Το $g(x)$ και το $h_1(x) \cdots h_k(x)$ $\big($λήμμα του Gauss$\big)$ είναι πρωταρχικά. Επομένως $d_1 \cdots d_k \sim \varepsilon_1 \cdots \varepsilon_k \delta \Leftrightarrow d_1 \cdots d_k = \varepsilon_1 \cdots \varepsilon_k \delta \cdot u$, όπου u αντιστρέψιμο στο R. Άρα $g(x) = u \cdot h_1(x) \cdots h_k(x) \Rightarrow f(x) = \delta g(x) = \delta' h_1(x) \cdots h_k(x)$, όπου $\delta' = \delta u \sim \delta$. Τέλος, αν αναλύσουμε το δ' $\big($στην περίπτωση που δεν είναι αντιστρέψιμο$\big)$ σε γινόμενο αναγώγων στοιχείων του R $\big($που όπως είπαμε είναι ανάγωγα και στο $R[x]\big)$, πετυχαίνουμε μιαν ανάλυση του $f(x)$ σε γινόμενο αναγώγων στοιχείων του $R[x]$. ■

ΠΡΟΤΑΣΗ 2.50. Η ανάλυση ενός $f(x) \in R[x]$ σε γινόμενο αναγώγων στοιχείων είναι μοναδική, $\big($αν αγνοήσουμε τη διάταξη των ανάγωγων παραγόντων$\big)$.
ΑΠΟΔΕΙΞΗ: Η περίπτωση που $f(x) = r \in R$ προκύπτει άμεσα από το γεγονός ότι η R είναι περιοχή μοναδικής παραγοντοποίησης. Γι' αυτό υποθέτουμε ότι $f(x) \in R[x]$ είναι μη σταθερό πολυώνυμο.
Έστω $f(x) = p_1 \cdots p_\kappa h_1(x) \cdots h_\mu(x) = q_1 \cdots q_\lambda \bar{h}_1(x) \cdots \bar{h}_\nu(x)$, όπου p_i, q_j ανάγωγα στο R και

$h_i(x), \bar{h}_j(x)$ ανάγωγα στο $R[x]$, δηλαδή πρωταρχικά στο $R[x]$ και ανάγωγα στο $\mathbb{K}[x]$. Σύμφωνα με το λήμμα του Gauss τα γινόμενα $h_1(x)\cdots h_\mu(x)$ και $\bar{h}_1(x)\cdots\bar{h}_\nu(x)$ είναι πρωταρχικά. Επομένως, με βάση το λήμμα 2.45, έχουμε $p_1\cdots p_\kappa \sim q_1\cdots q_\lambda$ και επειδή η R είναι περιοχή μοναδικής παραγοντοποίησης, $\kappa=\lambda$ και χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $p_i\sim q_i$, για κάθε $i=1,\ldots,\kappa$. Άρα $q_i=u_ip_i$, όπου u_i αντιστρέψιμο στην R, για κάθε $i=1,\ldots,\kappa$. Θέτουμε $u=u_1\cdots u_\kappa$ και παίρνουμε $h_1(x)\cdots h_\mu(x)=u\bar{h}_1(x)\cdots\bar{h}_\nu(x)=$ $=(u\bar{h}_1(x))\bar{h}_2(x)\cdots\bar{h}_\nu(x)$, με u αντιστρέψιμο στο R.
Τώρα, τα $h_1(x),\ldots,h_\mu(x)$ και $u\bar{h}_1(x),\bar{h}_2(x),\ldots,\bar{h}_\nu(x)$ είναι ανάγωγα στο $\mathbb{K}[x]$, άρα $\mu=\nu$ και χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι τα $h_1(x)$, $h_2(x),\ldots$, $h_\mu(x)$ είναι συντροφικά (στην $\mathbb{K}[x]$ όμως που είναι ευκλείδειος περιοχή!), με τα $u\bar{h}_1(x)$, $\bar{h}_2(x),\ldots$, $\bar{h}_\mu(x)$, αντίστοιχα. Επομένως υπάρχουν αντιστρέψιμα (μη μηδενικά) στοιχεία $\dfrac{\alpha_i}{\beta_i}\in\mathbb{K}$ $(\alpha_i,\beta_i\in R\backslash\{0\})$ τέτοια, ώστε $h_1(x)=\dfrac{\alpha_1}{\beta_1}\cdot u\bar{h}_1(x)$, $h_2(x)=\dfrac{\alpha_2}{\beta_2}\cdot\bar{h}_2(x),\ldots,h_\mu(x)=\dfrac{\alpha_\mu}{\beta_\mu}\cdot\bar{h}_\mu(x)$. Άρα $\beta_1h_1(x)=$ $=u\alpha_1\bar{h}_1(x)$, $\beta_2h_2(x)=\alpha_2\bar{h}_2(x),\ldots$, $\beta_\mu h_\mu(x)=\alpha_\mu\bar{h}_\mu(x)$. Επειδή τα $h_1(x),h_2(x),\ldots,h_\mu(x)$ και $\bar{h}_1(x),\bar{h}_2(x),\ldots,\bar{h}_\mu(x)$ είναι πρωταρχικά στο $R[x]$, από το λήμμα 2.45 παίρνουμε ότι $\beta_1\sim$ $\sim u\alpha_1\sim\alpha_1$, $\beta_2\sim\alpha_2,\ldots,\beta_\mu\sim\alpha_\mu$. Επομένως $u\alpha_1=v_1\beta_1,\alpha_2=v_2\beta_2,\ldots,\alpha_\mu=v_\mu\beta_\mu$, όπου v_i αντιστρέψιμο στην R, για κάθε $i=1,2,\ldots,\mu$. Συνεπώς $h_1(x)=v_1\bar{h}_1(x),h_2(x)=$ $=v_2\bar{h}_2(x),\ldots,h_\mu(x)=v_\mu\bar{h}_\mu(x)$, δηλαδή $h_i(x)\sim\bar{h}_i(x)$, για κάθε $i=1,2,\ldots,\mu$. ■

Από τα παραπάνω έπεται ότι η απόδειξη του θεωρήματος 2.42 είναι πλήρης.

ΠΟΡΙΣΜΑ 2.51. Αν R περιοχή μοναδικής παραγοντοποίησης, τότε και ο πολυωνυμικός δακτύλιος $R[x_1,x_2,\ldots,x_n]$ στις n μεταβλητές είναι περιοχή μοναδικής παραγοντοποίησης.
ΑΠΟΔΕΙΞΗ: Το αποτέλεσμα προκύπτει με επαγωγή επί του n, αφού $R[x_1,x_2]=R[x_1][x_2]$, $R[x_1,x_2,x_3]=R[x_1,x_2][x_3]$ κ.ο.κ. ■

Ακόμα και αν η R είναι περιοχή κυρίων ιδεωδών, η $R[x]$ δεν είναι απαραίτητα περιοχή κυρίων ιδεωδών. Ένα τέτοιο παράδειγμα είναι $R=\mathbb{Z}$. Το $\mathbb{Z}$ είναι κάτι περισσότερο. Είναι ευκλείδειος περιοχή. Αλλά το $\mathbb{Z}[x]$ δεν είναι περιοχή κυρίων ιδεωδών, όπως δείχνει το επόμενο παράδειγμα:

ΠΑΡΑΔΕΙΓΜΑ 2.52. Θεωρούμε το ιδεώδες $(2,x)$ της $\mathbb{Z}[x]$ που παράγεται από το 2 και το x. Τότε το $(2,x)$ δεν είναι κύριο.
ΑΠΟΔΕΙΞΗ: Αν το ιδεώδες $(2,x)$ ήταν κύριο, θα παραγόταν από ένα πολυώνυμο $f(x)\in\mathbb{Z}[x]$. Επομένως $2=f(x)g(x)$, όπου $g(x)\in\mathbb{Z}[x]$ και, συγκρίνοντας τους βαθμούς των πολυωνύμων, παίρνουμε $\deg f(x)=\deg g(x)=0$, άρα $f(x)=\kappa\in\mathbb{Z}$. Αλλά τότε $x=h(x)\kappa$, για κάποιο $h(x)\in\mathbb{Z}[x]$. Συγκρίνοντας βαθμούς παίρνουμε ότι $\deg h(x)=1$, άρα $h(x)=\alpha x+\beta$, με $\alpha,\beta\in\mathbb{Z}$. Επομένως $x=\kappa\alpha x+\kappa\beta \underset{\kappa\neq0}{\Rightarrow} \beta=0$ και $\kappa\alpha=1$, δηλαδή το κ είναι αντιστρέψιμο και συνεπώς $(2,x)=(\kappa)=\mathbb{Z}=(1)$. Αλλά τότε θα υπήρχαν πολυώνυμα $\varphi(x),\tau(x)\in\mathbb{Z}[x]$ με $1=\varphi(x)\cdot2+\tau(x)\cdot x=2\varphi(0)\underset{\varphi(0)\in\mathbb{Z}}{\Rightarrow}2\mid1$, άτοπο. ■

Τέλος, υπάρχει περιοχή κυρίων ιδεωδών, η οποία δεν είναι ευκλείδειος περιοχή. Μια τέτοια είναι η $\mathbb{Z}\Big[\dfrac{1+\mathrm{i}\sqrt{19}}{2}\Big]$.

*2.6 Παράδειγμα Περιοχής Κυρίων Ιδεωδών, η οποία δεν είναι Ευκλείδειος Περιοχή

Στην παράγραφο αυτή αντιγράφουμε (με κάποιες επιπλέον επεξηγήσεις) το άρθρο του R. J. Wilson $\big($http://www.maths.qmul.ac.uk/~raw/MTH5100/PIDnotED.pdf$\big)$, το οποίο αποτελεί απλούστευση του άρθρου του Oscar A. Cámpoli: *A principal ideal domain that is not a Euclidean domain*, Amer. Math. Monthly, vol. 95 no. 9 (Nov. 1988), 868-871.

ΠΡΟΤΑΣΗ 2.53. Η $R = \mathbb{Z}\Big[\dfrac{1+\mathrm{i}\sqrt{19}}{2}\Big]$ είναι περιοχή κυρίων ιδεωδών, αλλά όχι ευκλείδειος περιοχή.

ΑΠΟΔΕΙΞΗ: Ισχυρισμός 1ος: Έστω $\vartheta = \frac{1}{2}(1+\mathrm{i}\sqrt{19})$. Τότε $R = \{x+y\vartheta \mid x,y \in \mathbb{Z}\}$. Επίσης, $x+y\vartheta = x'+y'\vartheta \Leftrightarrow (x=x' \text{ και } y=y')$.

Απόδειξη ισχυρισμού: Παρατηρούμε ότι $\vartheta^2 = \frac{1}{4}(1-19+2\mathrm{i}\sqrt{19}) = \frac{1}{4}(-18+2\mathrm{i}\sqrt{19}) = \frac{1}{4}(-20+ +2+2\mathrm{i}\sqrt{19}) = -5+\frac{1}{2}(1+\mathrm{i}\sqrt{19}) = \vartheta - 5$. Επομένως $(\alpha+\beta\vartheta)(\gamma+\delta\vartheta) = \alpha\gamma+\beta\delta\vartheta^2+ +(\alpha\delta+\beta\gamma)\vartheta = (\alpha\gamma-5\beta\delta)+(\alpha\delta+\beta\gamma+\beta\delta)\vartheta \in \{x+y\vartheta \mid x,y\in\mathbb{Z}\}$, για κάθε $\alpha,\beta,\gamma,\delta \in \mathbb{Z}$. Επομένως το σύνολο $\{x+y\vartheta \mid x,y\in\mathbb{Z}\}$ είναι κλειστό ως προς τον πολλαπλασιασμό και προφανώς κλειστό ως προς την πρόσθεση. Περιέχει προφανώς τα στοιχεία $0 = 0+0\cdot\vartheta$ και $1 = 1+0\cdot\vartheta$ καθώς και το αντίθετο $-x-y\vartheta$ οποιουδήποτε στοιχείου $x+y\vartheta$ αυτού. Άρα είναι υποδακτύλιος του $\mathbb{C}$ και μάλιστα ο ελάχιστος υποδακτύλιος που περιέχει $\big($το $\mathbb{Z}\big)$ και το ϑ. Άρα $\{x+y\vartheta \mid x,y\in\mathbb{Z}\} = \mathbb{Z}[\vartheta] = R$.

Έστω τώρα $x+y\vartheta = x'+y'\vartheta$, όπου $x,x',y,y' \in \mathbb{Z}$. Αν $y \neq y'$, τότε $\vartheta = \dfrac{x-x'}{y'-y} \in \mathbb{Q} \subseteq \mathbb{R}$, άτοπο. Επομένως $y = y'$, οπότε και $x = x'$.

Ισχυρισμός 2ος: Τα μόνα αντιστρέψιμα στοιχεία του R είναι τα -1 και 1 και είναι ακριβώς αυτά που έχουν μιγαδικό μέτρο ίσο με 1. Επίσης τα στοιχεία 2 και 3 είναι ανάγωγα στο R.

Απόδειξη ισχυρισμού: Παρατηρούμε ότι $\overline{\vartheta} = \frac{1}{2}(1-\mathrm{i}\sqrt{19}) = 1-\frac{1}{2}(1+\mathrm{i}\sqrt{19}) = 1-\vartheta$.

Με $N(x) = |x|^2 = x\overline{x}$ θα συμβολίζουμε ως συνήθως το τετράγωνο του μέτρου ενός μιγαδικού x. Αν $x = \alpha+\beta\vartheta \in R$, τότε $N(x) = (\alpha+\beta\vartheta)\overline{(\alpha+\beta\vartheta)} = (\alpha+\beta\vartheta)(\alpha+\beta\overline{\vartheta}) = (\alpha+\beta\vartheta)((\alpha+\beta)-\beta\vartheta) = = \alpha(\alpha+\beta)+5\beta^2 = \frac{1}{2}((\alpha+\beta)^2+\alpha^2+9\beta^2)$. Αν λοιπόν $x = \alpha+\beta\vartheta$ $\big(\alpha,\beta\in\mathbb{Z}\big)$ αντιστρέψιμο στο R και $xy = 1$, τότε $1 = N(1) = N(x)N(y)$. Επομένως $N(x) = \frac{1}{2}((\alpha+\beta)^2+\alpha^2+9\beta^2) = 1 \Leftrightarrow \Leftrightarrow (\alpha+\beta)^2+\alpha^2+9\beta^2 = 2$. Αν $\beta \neq 0$, τότε $(\alpha+\beta)^2+\alpha^2+9\beta^2 \geq 9\beta^2 \geq 9 > 2$, άτοπο. Άρα $\beta = 0$ και $x = \alpha \in \mathbb{Z}$. Αλλά τότε $N(x) = \frac{1}{2}(2\alpha^2) = \alpha^2 \Rightarrow \alpha = \pm 1$. Προφανώς τα στοιχεία ± 1 είναι αντιστρέψιμα στο R.

Τώρα, τα στοιχεία 2 και 3 είναι ανάγωγα στο R. Πράγματι, έστω $2 = xy$, όπου $x,y \in R$. Τότε $4 = N(2) = N(x)N(y)$. Αν κανένα από τα x,y δεν ήταν αντιστρέψιμο, τότε $N(x), N(y) > 1$, άρα $N(x) = N(y) = 2$. Έστω $x = \alpha+\beta\vartheta$. Όπως προηγουμένως, $\frac{1}{2}((\alpha+\beta)^2+\alpha^2+9\beta^2) = 2 \Leftrightarrow \Leftrightarrow (\alpha+\beta)^2+\alpha^2+9\beta^2 = 4$. Αν $\beta \neq 0$, τότε $(\alpha+\beta)^2+\alpha^2+9\beta^2 \geq 9\beta^2 \geq 9 > 4$, άτοπο. Επομένως $\beta = 0$ και $x = \alpha \in \mathbb{Z}$. Αλλά τότε $2 = N(x) = \frac{1}{2}(2\alpha^2) = \alpha^2$, άτοπο γιατί το 2 δεν είναι τέλειο τετράγωνο στο $\mathbb{Z}$.

Έστω $3 = xy$, όπου κανένα από τα x,y δεν είναι αντιστρέψιμο. Τότε $9 = N(3) = N(x)N(y)$ και άρα $N(x) = N(y) = 3$. Έστω $x = \alpha+\beta\vartheta$. Όπως προηγουμένως, $\frac{1}{2}((\alpha+\beta)^2+\alpha^2+9\beta^2) = 3 \Leftrightarrow \Leftrightarrow (\alpha+\beta)^2+\alpha^2+9\beta^2 = 6$. Αν $\beta \neq 0$, τότε $(\alpha+\beta)^2+\alpha^2+9\beta^2 \geq 9\beta^2 \geq 9 > 6$, άτοπο. Επομένως $\beta = 0$ και $x = \alpha \in \mathbb{Z}$. Αλλά τότε $3 = N(x) = \frac{1}{2}(2\alpha^2) = \alpha^2$, άτοπο γιατί το 3 δεν είναι τέλειο τετράγωνο στο $\mathbb{Z}$.

Ισχυρισμός 3ος: Η R δεν είναι ευκλείδειος περιοχή.

Απόδειξη ισχυρισμού: Έστω $\tilde{N} : R\setminus\{0\} \to \{0,1,2,\ldots\}$ ευκλείδεια απεικόνιση. Επιλέγουμε

ένα $x \in R \setminus (\{0\} \cup U(R))$ με $\tilde{N}(x)$ το ελάχιστο δυνατό. Διαιρούμε το 2 με το x και παίρνουμε

$$2 = x\pi + \upsilon,$$

όπου $\pi, \upsilon \in R$ και $\upsilon = 0$ ή $\tilde{N}(\upsilon) < \tilde{N}(x)$. Επειδή το $x \in R \setminus (\{0\} \cup U(R))$ έχει την ελάχιστη τιμή $\tilde{N}(x)$, αυτό σημαίνει ότι είτε υ αντιστρέψιμο είτε $\upsilon = 0$, δηλαδή $\upsilon = 0, 1$ ή -1. Αν $\upsilon = 0$, τότε $x \mid 2$ και εφόσον το x δεν είναι αντιστρέψιμο και το 2 ανάγωγο, έπεται ότι $x \sim 2$, δηλαδή $x = \pm 2$. Αν $\upsilon = -1$, τότε $x\pi = 3 \Rightarrow x \mid 3$ και εφόσον το x δεν είναι αντιστρέψιμο και το 3 ανάγωγο, έπεται ότι $x \sim 3$, δηλαδή $x = \pm 3$. Η περίπτωση $\upsilon = 1$ αποκλείεται γιατί τότε, $x\pi = 1$, ήτοι x αντιστρέψιμο.

Συμπέρασμα: $x = \pm 2, \pm 3$. Μετά διαιρούμε το $\vartheta = \frac{1}{2}(1 + \mathrm{i}\sqrt{19})$ με το $x = \pm 2, \pm 3$ και παίρνουμε

$$\vartheta = x\pi' + \upsilon',$$

όπου $\upsilon' = 0$ ή $\tilde{N}(\upsilon') < \tilde{N}(x)$. Λόγω της επιλογής του x θα έχουμε, όπως προηγουμένως $\upsilon' = 0, 1$ ή -1. Επομένως το $x = \pm 2, \pm 3$ θα διαιρεί είτε το ϑ είτε το $\vartheta - 1$ είτε το $\vartheta + 1$. Αλλά τότε θα υπήρχε σε κάθε περίπτωση $\alpha + \beta\vartheta \in R$ τέτοιο, ώστε $\pm 2\alpha \pm 2\beta\vartheta = \vartheta$ ή $\pm 2\alpha + 1 \pm 2\beta\vartheta = \vartheta$ ή $\pm 2\alpha - 1 \pm 2\beta\vartheta = \vartheta$ ή $\pm 3\alpha \pm 3\beta\vartheta = \vartheta$ ή $\pm 3\alpha + 1 \pm 3\beta\vartheta = \vartheta$ ή $\pm 3\alpha - 1 \pm 3\beta\vartheta = \vartheta$. Όλες οι περιπτώσεις αποκλείονται λόγω του δεύτερου σκέλους του $1^{\text{ου}}$ ισχυρισμού. Ο R δεν είναι λοιπόν ευκλείδειος περιοχή.

Ισχυρισμός $4^{\text{ος}}$: Η R είναι περιοχή κυρίων ιδεωδών.

Απόδειξη ισχυρισμού: Έστω $\mathrm{I} \neq \{0\}$ ένα ιδεώδες του R. Επιλέγουμε ένα $s \in \mathrm{I} \setminus \{0\}$ με το μικρότερο μιγαδικό μέτρο. Ένα τέτοιο $s = \alpha + \beta\vartheta$ $\big(\alpha, \beta \in \mathbb{Z}\big)$ υπάρχει, αφού θα αντιστοιχεί στη μικρότερη τιμή του $N(s) = \frac{1}{2}((\alpha + \beta)^2 + \alpha^2 + 9\beta^2)$ που είναι θετικό ακέραιο πολλαπλάσιο του $\frac{1}{2}$. Θα αποδείξουμε ότι $\mathrm{I} = Rs$. Υποθέτουμε λοιπόν ότι $\mathrm{I} \supsetneq Rb$ και έστω $t \in \mathrm{I} \setminus Rs$.

Η στρατηγική είναι η ακόλουθη: Θα αποδείξουμε ότι υπάρχουν $r, r' \in R$ τέτοια, ώστε $0 < < |rt - r's| < |s|$. Αυτό οδηγεί σε άτοπο γιατί το $rt - r's$ θα ανήκει στο $\in \mathrm{I} \setminus \{0\}$ και θα έχει μιγαδικό μέτρο μικρότερο από το ελάχιστο δυνατό.

Κατ' αρχάς παρατηρούμε ότι το φανταστικό μέρος ενός $\alpha + \beta\vartheta = \frac{1}{2}(2\alpha + \beta) + \frac{1}{2}\beta\mathrm{i}\sqrt{19} \in R$ $\big(\alpha, \beta \in \mathbb{Z}\big)$ είναι $\frac{1}{2}\beta\sqrt{19}$. Αν $x + y\mathrm{i}$ $\big(x, y \in \mathbb{R}\big)$ είναι τυχόν μιγαδικός, τότε μπορούμε να αφαιρέσουμε κατάλληλο $r_0 = \alpha + \beta\vartheta \in R$ από τον $x + y\mathrm{i}$ έτσι, ώστε το φανταστικό μέρος $y - \frac{1}{2}\beta\sqrt{19}$ της διαφοράς $x + y\mathrm{i} - r_0$ να βρίσκεται στο διάστημα $\big[-\frac{1}{4}\sqrt{19}, \frac{1}{4}\sqrt{19}\big]$, δηλαδή να έχει απόλυτη τιμή μικρότερη ή ίση του $\frac{1}{4}\sqrt{19}$. Θα πρέπει το $\beta \in \mathbb{Z}$ να επιλεγεί κατάλληλα, ώστε $\big|y - \frac{1}{2}\beta\sqrt{19}\big| = \big|\frac{1}{2}\beta\sqrt{19} - y\big| \leq \frac{1}{4}\sqrt{19} \Leftrightarrow \left|\beta - \frac{2y}{\sqrt{19}}\right| \leq \frac{1}{2}$. Ένας τέτοιος ακέραιος β υπάρχει για κάθε πραγματικό y. Είναι είτε ο $\big\lfloor \frac{2y}{\sqrt{19}} \big\rfloor$ είτε ο $\big\lfloor \frac{2y}{\sqrt{19}} \big\rfloor + 1$. $\big(\lfloor x \rfloor$ το ακέραιο μέρος του $x \in \mathbb{R}\big)$.

Θεωρούμε τώρα τον μιγαδικό $t/s = x + y\mathrm{i}$ $\big(x, y \in \mathbb{R}\big)$. Σύμφωνα με τα προηγούμενα, μπορούμε να αφαιρέσουμε από τον t/s κατάλληλο $r_0 \in R$ έτσι, ώστε το φανταστικό μέρος του $t/s - r_0$ να βρίσκεται στο διάστημα $\big[-\frac{1}{4}\sqrt{19}, \frac{1}{4}\sqrt{19}\big]$. Λόγω της σχέσης $\frac{1}{2}\sqrt{3} < \frac{1}{4}\sqrt{19} \Leftrightarrow 12 < 19$ εξετάζουμε πρώτα την περίπτωση κατά την οποία το φανταστικό μέρος του $t/s - r_0$ βρίσκεται στο διάστημα $\big(-\frac{1}{2}\sqrt{3}, \frac{1}{2}\sqrt{3}\big)$. Τώρα, το πραγματικό μέρος του $t/s - r_0$ απέχει από έναν ακέραιο $\kappa \in \mathbb{Z} \subseteq \mathbb{Z}[\vartheta]$ απόσταση μικρότερη ή ίση του $\frac{1}{2}$. Επομένως το πραγματικό μέρος του $t/s - r_0 - \kappa$ έχει απόλυτη τιμή μικρότερη ή ίση του $\frac{1}{2}$, ενώ το φανταστικό του εξακολουθεί να βρίσκεται στο διάστημα $\big(-\frac{1}{2}\sqrt{3}, \frac{1}{2}\sqrt{3}\big)$. Έστω $r' = r_0 + \kappa \in \mathbb{Z}[\vartheta]$. Τότε $|t/s - r'|^2 < \frac{1}{4} + \frac{3}{4} = 1 \Leftrightarrow |t - r's| < |s|$. Αλλά $r's \in Rs \subseteq \mathrm{I}$ και $t \in \mathrm{I} \setminus Rs$. Επομένως $t - r's \in \mathrm{I} \setminus Rs \subseteq \mathrm{I} \setminus \{0\}$, άρα $0 < |t - r's|$. Τελικώς $0 < |t - r's| < |s|$, άτοπο.

Η επόμενη περίπτωση είναι αυτή κατά την οποία το φανταστικό μέρος του $t/s - r_0$ βρίσκεται στο διάστημα $\big[\frac{1}{2}\sqrt{3}, \frac{1}{4}\sqrt{19}\big]$. Τότε $\mathrm{Im}(2t/s - 2r_0 - \vartheta) = 2\mathrm{Im}(t/s - r_0) - \frac{\sqrt{19}}{2} \in \left(\frac{2\sqrt{3} - \sqrt{19}}{2}, 0\right]$.

Αλλά $\sqrt{19} < \sqrt{27} = 3\sqrt{3}$ και επομένως $-\sqrt{3} < 2\sqrt{3} - \sqrt{19} \Leftrightarrow -\frac{1}{2}\sqrt{3} < \frac{2\sqrt{3}-\sqrt{19}}{2}$. Επομένως $|\mathrm{Im}(2t/s - 2r_0 - \vartheta)| < \frac{1}{2}\sqrt{3}$. Σύμφωνα με την προηγούμενη περίπτωση, υπάρχει $\kappa \in \mathbb{Z}$ τέτοιο, ώστε $|\mathrm{Re}(2t/s - 2r_0 - \vartheta) - \kappa| = |\mathrm{Re}(2t/s - 2r_0 - \vartheta - \kappa)| \leq \frac{1}{2}$. Θέτουμε $r = 2$ και $r' = 2r_0 - \vartheta - \kappa$. Τότε $|rt/s - r'| < 1 \Leftrightarrow |rt - r's| < |s|$. Όλα καλά για να οδηγηθούμε σε άτοπο, εκτός από ένα σημείο: Ξέρουμε σίγουρα ότι $rt - r's \neq 0$; Αν έχουμε αποτύχει και εφόσον $r = 2$, θα πρέπει $0 = 2t/s = r' = 2r_0 - \vartheta - \kappa \Leftrightarrow t/s = r_0 - \frac{1}{2}\vartheta - \frac{1}{2}\kappa$.
Αν $\kappa = 2\kappa'$ άρτιος, τότε $t/s = r_0 - \kappa' - \frac{1}{2}\vartheta = r_0 - \overline{\vartheta} - \kappa' + \frac{1}{2}\vartheta = r_1 + \frac{1}{2}\vartheta$, όπου $r_1 = r_0 - \vartheta - \kappa' \in R$. Τότε $\overline{\vartheta}t/s = r_1\overline{\vartheta} + \frac{1}{2}|\vartheta|^2 = r_1\overline{\vartheta} + \frac{5}{2} = r_1\overline{\vartheta} + 2 + \frac{1}{2}$ και $\overline{\vartheta} = 1 - \vartheta \in R$. Θέτουμε $r'' = r_1\overline{\vartheta} + 2 \in R$. Τότε $|\overline{\vartheta}t/s - r''| = \frac{1}{2} \Leftrightarrow |\overline{\vartheta}t - r''s| = \frac{1}{2}|s|$, θετικό και μικρότερο του $|s|$, άτοπο.
Αν $\kappa = 2\kappa' + 1$ περιττός, τότε $t/s = r_0 - \kappa' - \frac{1}{2} - \frac{1}{2}\vartheta = r_0 - \kappa' - 1 + \frac{1}{2} - \frac{1}{2}\vartheta = r_0 - \kappa' - 1 + \frac{1}{2}\overline{\vartheta} = r_1 + \frac{1}{2}\overline{\vartheta}$, όπου τώρα $r_1 = r_0 - \kappa' - 1 \in R$. Επομένως $\vartheta t/s = r_1\vartheta + \frac{5}{2} = r_1\vartheta + 2 + \frac{1}{2}$. Τώρα θέτουμε $r'' = r_1\vartheta + 2$. Και πάλι $\vartheta t/s - r'' = \frac{1}{2} \Rightarrow |\vartheta t - r''s| = \frac{1}{2}|s|$, άτοπο.
Απομένει η περίπτωση κατά την οποία το φανταστικό μέρος του $t/s - r_0$ βρίσκεται στο διάστημα $\left[-\frac{1}{4}\sqrt{19}, -\frac{1}{2}\sqrt{3}\right]$, η οποία είναι συμμετρική της $\left[\frac{1}{2}\sqrt{3}, \frac{1}{4}\sqrt{19}\right]$. Πράγματι, μπορούμε να επαναλάβουμε τους προηγούμενους συλλογισμούς (με κάποια, όχι βέβαια αναγκαία, τροποποίηση στο συμβολισμό) για τον μιγαδικό $r_0 - t/s$ και τελειώσαμε. ■

***Άσκηση* 2.1.** Να αποδείξετε ότι ο δακτύλιος $\mathbb{Z}[\sqrt{10}] = \{\alpha + \beta\sqrt{10} \mid \alpha, \beta \in \mathbb{Z}\}$ δεν είναι περιοχή μοναδικής παραγοντοποίησης.

Κεφάλαιο 3

Πρότυπα

3.1 Ορισμοί-Παραδείγματα

Η έννοια του προτύπου επί ενός δακτυλίου αποτελεί φυσική γενίκευση της έννοιας του διανυσματικού χώρου επί ενός σώματος. Πολλές από τις ιδιότητες των διανυσματικών χώρων επεκτείνονται στα πρότυπα, ενώ άλλες όχι.
Επαναλαμβάνουμε ότι εργαζόμαστε με μοναδιαίους μεταθετικούς δακτυλίους.

ΟΡΙΣΜΟΣ 3.1. Έστω R μοναδιαίος μεταθετικός δακτύλιος και M ένα μη κενό σύνολο. Το M λέγεται ***R*-πρότυπο** $\big(R\text{-module}\big)$ αν και μόνον αν ισχύουν τα παρακάτω:
Το M είναι εφοδιασμένο με μια πράξη, την **πρόσθεση** $+ : M \times M \to M/(x, y) \mapsto x + y$ και έναν **εξωτερικό (βαθμωτό) πολλαπλασιασμό** $\cdot : R \times M \to M/(r, x) \mapsto rx$, $\big($το σύμβολο $\cdot$ συνήθως παραλείπεται$\big)$ με τις εξής ιδιότητες:
(i) Το ζεύγος $(M, +)$ είναι αβελιανή ομάδα. Το μηδενικό στοιχείο του συμβολίζεται με 0_M ή, αν δεν υπάρχει φόβος συγχύσεως, απλά με 0.
(ii) Ο εξωτερικός πολλαπλασιασμός πληροί τις ακόλουθες ιδιότητες:
α) $r(x + y) = rx + ry$, για κάθε $r \in R$ και για κάθε $x, y \in M$.
β) $(r + s)x = rx + sy$, για κάθε $r, s \in R$ και για κάθε $x \in M$.
γ) $(rs)x = r(sx)$, για κάθε $r, s \in R$ και για κάθε $x \in M$.
δ) $1_R \cdot x = x$, για κάθε $x \in M$.

Τα παραδείγματα **3.2.(iii)** και **3.2.(iv)** αποτελούν την «καρδιά» του μαθήματος.

ΠΑΡΑΔΕΙΓΜΑΤΑ 3.2. (i) Κάθε διανυσματικός χώρος V επί ενός σώματος $\mathbb{K}$ είναι προφανώς ένα $\mathbb{K}$-πρότυπο.
(ii) Αν R είναι ένας μοναδιαίος μεταθετικός δακτύλιος, τότε ο R είναι ένα R-πρότυπο. Ο βαθμωτός πολλαπλασιασμός είναι ο συνήθης πολλαπλασιασμός του δακτυλίου R. Γενικότερα, **κάθε ιδεώδες *I* του *R* είναι ένα *R*-πρότυπο**. Αυτό προκύπτει από τον ορισμό του ιδεώδους.
(iii) Κάθε αβελιανή ομάδα $(M, +)$ μπορεί να θεωρηθεί ως $\mathbb{Z}$-πρότυπο και αντίστροφα. Ορίζουμε τον βαθμωτό πολλαπλασιασμό $\cdot : \mathbb{Z} \times M \to M/(k, x) \mapsto kx$ ως εξής:

$$kx = \begin{cases} \underbrace{x + x + \cdots + x}_{k \text{ φορές}}, & \text{αν } k > 0, \\ 0_M, & \text{αν } k = 0, \\ \underbrace{-x - x - \cdots - x}_{|k| = -k \text{ φορές}}, & \text{αν } k < 0. \end{cases}$$

Είναι μια εύκολη, αλλά ανιαρή και γεμάτη υποπεριπτώσεις άσκηση (αλλά συστήνω να την κάνετε) για να επαληθεύσει κανείς ότι ισχύουν οι ιδιότητες **α)**-**δ)** του προηγούμενου ορισμού.
Οι έννοιες λοιπόν της αβελιανής ομάδας και του $\mathbb{Z}$-προτύπου ταυτίζονται. Στα επόμενα η ταύτιση αυτή θα θεωρείται δεδομένη, χωρίς κάποια ιδιαίτερη αναφορά.
(iv) Έστω V διανυσματικός χώρος επί ενός σώματος $\mathbb{K}$ και $\alpha : V \to V$ μια $\mathbb{K}$-γραμμική απεικόνιση. Ως γνωστόν, μια τέτοια απεικόνιση λέγεται ενδομορφισμός του V. Θέτουμε $\alpha^0 = 1_V$, ο ταυτοτικός ενδομορφισμός του V και $\alpha^n = \underbrace{\alpha \circ \alpha \circ \cdots \circ \alpha}_{n \text{ φορές}}$, όπου n θετικός ακέραιος. Αν $f(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in \mathbb{K}[x]$, τότε θέτουμε

$$f(\alpha) = b_n\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 1_V : V \to V.$$

Θεωρούμε τον V ως ένα $\mathbb{K}[x]$-πρότυπο με βαθμωτό πολλαπλασιασμό

$$(f(x), v) \mapsto f(x)v := f(\alpha)(v), \text{ για κάθε } f(x) \in \mathbb{K}[x] \text{ και } v \in V.$$

Επαληθεύουμε εν τάχει τις ιδιότητες α)-δ) του ορισμού.
α) $f(x)(v_1 + v_2) = f(\alpha)(v_1 + v_2) \underset{f(\alpha)\ \text{γραμμική}}{=} f(\alpha)(v_1) + f(\alpha)(v_2) = f(x)v_1 + f(x)v_2$, για κάθε $f(x) \in \mathbb{K}[x]$ και $v_1, v_2 \in V$.
β) $(f(x)+g(x))v = (f(\alpha)+g(\alpha))(v) = f(\alpha)(v)+g(\alpha)(v) = f(x)v+g(x)v$, για κάθε $f(x), g(x) \in \in \mathbb{K}[x]$ και $v \in V$.
γ) $(f(x)g(x))v = (f(\alpha) \circ g(\alpha))(v) = f(\alpha)(g(\alpha)(v)) = f(\alpha)(g(x)v) = f(x)(g(x)v)$, για κάθε $f(x), g(x) \in \mathbb{K}[x]$ και $v \in V$.
δ) $1_{\mathbb{K}[x]} \cdot v = 1_V(v) = v$, για κάθε $v \in V$.
(v) Έστω $\varphi : R \to S$ ομομορφισμός μοναδιαίων μεταθετικών δακτυλίων. Έστω M ένα S-πρότυπο. Τότε το M καθίσταται R-πρότυπο με βαθμωτό πολλαπλασιασμό $r \cdot x = \varphi(r)x$, για κάθε $r \in R$ και $x \in M$. (Συμπληρώστε τις λεπτομέρειες).

ΠΡΟΤΑΣΗ 3.3. (**ΤΡΕΙΣ ΣΤΟΙΧΕΙΩΔΕΙΣ ΙΔΙΟΤΗΤΕΣ ΕΝΟΣ ΠΡΟΤΥΠΟΥ**) Έστω M ένα R-πρότυπο. Τότε ισχύουν τα ακόλουθα:
(i) $0_R \cdot x = 0_M$, για κάθε $x \in M$.
(ii) $r \cdot 0_M = 0_M$, για κάθε $r \in R$.
(iii) $(-r)x = r(-x) = -rx$, για κάθε $r \in R$ και $x \in M$.
ΑΠΟΔΕΙΞΗ: (i) $0_R \cdot x = (0_R + 0_R)x = 0_R \cdot x + 0_R \cdot x$. Επομένως $0_M = 0_R \cdot x + (-0_R \cdot x) = = (0_R \cdot x + 0_R \cdot x) + (-0_R \cdot x) = 0_R \cdot x + (0_R \cdot x + (-0_R \cdot x)) = 0_R \cdot x + 0_M = 0_R \cdot x$.
(ii) $r \cdot 0_M = r(0_M + 0_M) = r \cdot 0_M + r \cdot 0_M$.
Επομένως $0_M = r \cdot 0_M + (-r \cdot 0_M) = (r \cdot 0_M + r \cdot 0_M) + (-r \cdot 0_M) = r \cdot 0_M + (r \cdot 0_M + (-r \cdot 0_M)) = = r \cdot 0_M + 0_M = r \cdot 0_M$.
(iii) $rx + (-r)x = (r + (-r))x = 0_R \cdot x = 0_M$. Άρα $(-r)x = -rx$. Παρόμοια, $rx + r(-x) = = r(x + (-x)) = r \cdot 0_M = 0_M$. Επομένως $r(-x) = -rx$. ■

3.2 Υποπρότυπα-Πηλίκο Προτύπων

ΟΡΙΣΜΟΣ 3.4. Έστω M ένα R-πρότυπο και N μη κενό υποσύνολο του M. Το N λέγεται **υποπρότυπο του M** αν είναι ένα R-πρότυπο με πράξεις τους περιορισμούς της πρόσθεσης και του βαθμωτού πολλαπλασιασμού στο $N \times N$ και $R \times N$ αντίστοιχα. Γράφουμε $N \leqslant M$.
Πιο αναλυτικά, το N είναι υποπρότυπο του M αν και μόνον αν:
(i) $x + y \in N$, για κάθε $x, y \in N$.
(ii) $-y \in N$, για κάθε $y \in N$.
(iii) $0_M \in N$.

(iv) $rx \in N$, για κάθε $r \in R$ και $x \in N$.

Παρατήρηση: Οι ιδιότητες **(i)**, **(ii)** και **(iii)** λένε ότι το ζεύγος $(N,+)$ είναι υποομάδα της αβελιανής ομάδας $(M,+)$. Η ιδιότητα **(iii)** είναι περιττή γιατί προκύπτει από τις **(i)** και **(ii)**. Πράγματι, αν $x \in N$, τότε από την **(ii)** προκύπτει ότι και $-x \in N$. Τέλος, από την **(i)** προκύπτει ότι $0_M = x + (-x) \in N$.
Μάλιστα, επειδή εργαζόμαστε σε μοναδιαίο μεταθετικό δακτύλιο, οι συνθήκες **(ii)** και **(iii)** είναι περιττές, όπως μας λέει η επόμενη πρόταση.

ΠΡΟΤΑΣΗ 3.5. Έστω M ένα R-πρότυπο και N ένα μη κενό υποσύνολο αυτού. Τότε $N \leqslant M$ αν και μόνον αν ισχύουν τα ακόλουθα:
(i) $x + y \in N$, για κάθε $x, y \in N$.
(ii) $rx \in N$, για κάθε $r \in R$ και $x \in N$.
ΑΠΟΔΕΙΞΗ: Αν $x \in N$, τότε από την ιδιότητα **(ii)** προκύπτει ότι $-x = (-1_R)x \in N$. Εφόσον τώρα $-x \in N$ για κάθε $x \in N$, από την ιδιότητα **(i)** προκύπτει ότι $0_M = x + (-x) \in N$. ■

ΠΡΟΤΑΣΗ 3.6. **(i)** Έστω $X \subseteq M$. Τότε υπάρχει ελάχιστο ως προς τη σχέση $\subseteq$ του «περιέχεσθαι» υποπρότυπο του M, το οποίο περιέχει το X. Το υποπρότυπο αυτό συμβολίζεται με (X).
(ii) Το (X) είναι η τομή όλων των υποπροτύπων που περιέχουν το X.
(iii) Αν $X = \varnothing$, τότε $(X) = \{0_M\}$, το **τετριμμένο υποπρότυπο**. Αν $X \neq \varnothing$, τότε το (X) αποτελείται από όλους τους πεπερασμένους R-γραμμικούς συνδυασμούς $\sum_{i=1}^{n} r_i x_i$, για όλους τους θετικούς ακεραίους n, με $r_i \in R$ και $x_i \in X$, για κάθε $i = 1, \ldots, n$.
ΑΠΟΔΕΙΞΗ: Έστω $\mathscr{A}$ η συλλογή όλων των υποπροτύπων του M που περιέχουν το X. Προφανώς $M \in \mathscr{A}$ και συνεπώς $\mathscr{A} \neq \varnothing$. Επειδή $0_M \in N$, για κάθε υποπρότυπο $N \in \mathscr{A}$, η τομή $\bigcap_{N \in \mathscr{A}} N$ δεν είναι κενή $\big($περιέχει το $0_M\big)$. Αν $x, y \in \bigcap_{N \in \mathscr{A}} N$, τότε $x, y \in N$, για κάθε υποπρότυπο $N \in \mathscr{A}$ και κατά συνέπεια $x + y \in N$, για κάθε υποπρότυπο $N \in \mathscr{A}$. Άρα $x + y \in \bigcap_{N \in \mathscr{A}} N$. Ομοίως, αν $r \in R$ και $x \in \bigcap_{N \in \mathscr{A}} N$, τότε $x \in N$, για κάθε υποπρότυπο $N \in \mathscr{A}$ και κατά συνέπεια και $rx \in N$, για κάθε υποπρότυπο $N \in \mathscr{A}$. Επομένως $rx \in \bigcap_{N \in \mathscr{A}} N$. Επομένως η τομή $\bigcap_{N \in \mathscr{A}} N$ είναι ένα υποπρότυπο που περιέχει το X και φυσικά είναι το ελάχιστο.
Τώρα, αν $X = \varnothing$, τότε το $X = \varnothing$ περιέχεται οπουδήποτε, άρα περιέχεται και στο ελάχιστο υποπρότυπο του M, το τετριμμένο $\{0_M\}$. Συνεπώς $(\varnothing) = \{0_M\}$.
Τέλος, το (X) $\big($ως πρότυπο$\big)$ περιέχει όλους τους R-γραμμικούς συνδυασμούς των στοιχείων του. Ιδιαιτέρως των στοιχείων του που ανήκουν στο X. Είναι το σύνολο A των γραμμικών αυτών συνδυασμών υποπρότυπο του M; Αν η απάντηση είναι καταφατική, τότε αυτό θα είναι το (X), αφού $X \subseteq A \subseteq (X)$. $\big($Η σχέση $X \subseteq A$ προκύπτει απ' το γεγονός ότι $x = 1_R \cdot x$, για κάθε $x \in X$-γραμμικός συνδυασμός με έναν όρο$\big)$. Παρατηρούμε ότι το άθροισμα $\sum_{i=1}^{m} r_i x_i + \sum_{j=1}^{n} s_j y_j$, όπου $r_i, s_j \in R$ και $x_i, y_j \in X$ είναι ένας R-γραμμικός συνδυασμός στοιχείων του X. Πράγματι, αν θέσουμε $x'_i = x_i$, $r'_i = r_i$, για κάθε $i = 1, \ldots, m$ και $x'_{j+m} = y_j$ και $r'_{j+m} = s_j$, για κάθε $j = 1, \ldots, n$, τότε το άθροισμα $\sum_{i=1}^{m} r_i x_i + \sum_{j=1}^{n} s_j y_j$ γράφεται ως $\sum_{i=1}^{m+n} r'_i x'_i$. Κανείς δεν μας απαγορεύει τα στοιχεία του X να επαναλαμβάνονται σ' έναν γραμμικό συνδυασμό περισσότερες από μία φορές. Αν δεν το θέλουμε αυτό, αρκεί να βγάλουμε κοινό παράγοντα π.χ. το στοιχείο $x_i = y_j$ με συντελεστή τον $r_i + s_j$. Έστω τώρα $\sum_{i=1}^{m} r_i x_i$ ένας R-γραμμικός συνδυασμός στοιχείων του X και $r \in R$. Τότε $r \cdot \sum_{i=1}^{m} r_i x_i = \sum_{i=1}^{m} (r r_i) x_i$, ένας R-γραμμικός συνδυασμός στοιχείων του X. ■

ΟΡΙΣΜΟΣ 3.7. Το υποπρότυπο (X) του M που ορίστηκε στην προηγούμενη πρόταση λέγεται **το υποπρότυπο που παράγεται από το X**. Τα στοιχεία του X λέγονται **γεννήτορες** του υποπροτύπου (X). Αν το X είναι πεπερασμένο, π.χ. $X = \{x_1, \ldots, x_n\}$, τότε γράφουμε $(x_1, \ldots, x_n)$ αντί $(\{x_1, \ldots, x_n\})$ και το $N = (X)$ λέγεται **πεπερασμένα παραγόμενο**. Ιδιαιτέρως αν το $X = \{x\}$ είναι μονοσύνολο, τότε το υποπρότυπο (x) λέγεται **κυκλικό**. Αυτό αποτελείται από όλα τα πολλαπλάσια του x, δηλαδή $(x) = \{rx \mid r \in R\}$. Γι' αυτό και το συμβολίζουμε και με Rx. Επίσης, αν $X = \varnothing$, τότε θεωρούμε ότι $\boldsymbol{(\varnothing) = \{0_M\}}$, όπως προαναφέραμε.

ΠΑΡΑΔΕΙΓΜΑ 3.8. Ο ίδιος ο δακτύλιος R είναι R-πρότυπο με βαθμωτό πολλαπλασιασμό τον συνήθη πολλαπλασιασμό του R. **Τα υποπρότυπα του R είναι ακριβώς τα ιδεώδη του**.

ΠΡΟΤΑΣΗ 3.9. Έστω $M_1, M_2, \ldots, M_k$ υποπρότυπα ενός R-προτύπου M. Τότε το άθροισμα
$$M_1 + M_2 + \cdots + M_k = \{x_1 + x_2 + \cdots + x_k \mid x_i \in M_i, \text{ για κάθε } i = 1, 2, \ldots, k\}$$
είναι υποπρότυπο του M και μάλιστα είναι το ελάχιστο υποπρότυπο που περιέχει το σύνολο
$$M_1 \cup M_2 \cup \cdots \cup M_k.$$
ΑΠΟΔΕΙΞΗ: Θα χρησιμοποιήσουμε τον συμβολισμό $\sum_{i=1}^{k} M_i = M_1 + M_2 + \cdots + M_k$. Έστω λοιπόν $\sum_{i=1}^{k} x_i, \sum_{i=1}^{k} x_i' \in \sum_{i=1}^{k} M_i$, όπου $x_i, x_i' \in M_i$, για κάθε $i = 1, 2, \ldots, k$ και $r \in R$.
Τότε $\sum_{i=1}^{k} x_i + \sum_{i=1}^{k} x_i' = \sum_{i=1}^{k} (x_i + x_i') \in \sum_{i=1}^{k} M_i$, αφού $x_i + x_i' \in M_i$, για κάθε $i = 1, 2, \ldots, k$.
Επίσης $r \sum_{i=1}^{k} x_i = \sum_{i=1}^{k} rx_i \in \sum_{i=1}^{k} M_i$, αφού $rx_i \in M_i$, για κάθε $i = 1, 2, \ldots, k$.
Τέλος, το υποπρότυπο $(M_1 \cup M_2 \cup \cdots \cup M_k)$ που παράγεται από την ένωση των M_i θα περιέχει κάθε στοιχείο x_i του M_i, άρα θα περιέχει και όλα τα αθροίσματα $x_1 + x_2 + \cdots + x_k$, όπου $x_i \in M_i$, για κάθε $i = 1, 2, \ldots, k$. Εφόσον τα αθροίσματα αυτά συγκροτούν υποπρότυπο, θα έχουμε $(M_1 \cup M_2 \cup \cdots \cup M_k) \supseteq M_1 + M_2 + \cdots + M_k$.
Απ' την άλλη μεριά για κάθε i, αν $x_i \in M_i$, τότε
$$x_i = 0_M + 0_M + \cdots + \underset{\substack{\uparrow \\ i \text{ θέση}}}{x_i} + \cdots + 0_M \in M_1 + M_2 + \cdots + M_k$$
και άρα $M_1 \cup M_2 \cup \cdots \cup M_k \subseteq M_1 + M_2 + \cdots + M_k \Rightarrow (M_1 \cup M_2 \cup \cdots \cup M_k) \subseteq M_1 + M_2 + \cdots + M_k$. ■

Κατ' αναλογίαν προς την έννοια του δακτυλίου-πηλίκο ορίζεται και η έννοια του προτύπου-πηλίκο.

ΠΡΟΤΑΣΗ 3.10. Έστω M ένα R-πρότυπο και N υποπρότυπο του M. Στο M ορίζουμε τη σχέση
$$x \equiv y \mod N \Leftrightarrow x - y \in N.$$
Τότε η σχέση $(\equiv \mod N)$ είναι σχέση ισοδυναμίας στο M. Το σύνολο των κλάσεων ισοδυναμίας συμβολίζεται με $M \Big/ N$ ή με $\dfrac{M}{N}$, ή ελλείψει χώρου, με M/N.
ΑΠΟΔΕΙΞΗ: (i) $x - x = 0_M \in N \Leftrightarrow x \equiv x \mod N$ (Ανακλαστική).
(ii) $x \equiv y \mod N \Leftrightarrow x - y \in N \Leftrightarrow y - x = -(x - y) \in N \Leftrightarrow y \equiv x \mod N$ (Συμμετρική).
(iii) Έστω $x \equiv y \mod N$ και $y \equiv z \mod N$. Αυτό σημαίνει ότι $x - y \in N$ και $y - z \in N$. Επομένως $x - z = (x - y) + (y - z) \in N \Rightarrow x \equiv z \mod N$ (Μεταβατική). ■

ΠΡΟΤΑΣΗ 3.11. Έστω $x \in M$. Η κλάση ισοδυναμίας modulo N στην οποία ανήκει το x είναι το σύνολο $x + N = \{x + y \mid y \in N\}$.
ΑΠΟΔΕΙΞΗ: Έστω $x' \equiv x \mod N \Leftrightarrow x' - x \in N$. Θέτουμε $y = x' - x \in N$. Τότε $x' = x + y \in \in x + N$. Αντιστρόφως, έστω $x + y \in x + N \Leftrightarrow y \in N$. Τότε $x + y - x = y \in N \Leftrightarrow x + y \equiv x \mod N$. ■

ΠΡΟΤΑΣΗ 3.12. Στο σύνολο $M/N = \{x+N \mid x \in M\}$ των κλάσεων ισοδυναμίας ορίζουμε δύο πράξεις: $\big($**Πρόσθεση**$\big)$ $+ : M/N \times M/N \to M/N$ με $(x+N)+(y+N) = (x+y)+N$, για κάθε $x, y \in M$ και
$\big($**Βαθμωτό πολλαπλασιασμό**$\big)$ $\cdot : R \times M/N \to M/N$ με $r(x+N) = (rx)+N$, για κάθε $r \in R$ και $x \in M$.
Τότε το σύνολο M/N καθίσταται R-πρότυπο με μηδενικό στοιχείο $0_{M/N} = N$.
ΑΠΟΔΕΙΞΗ: Αρχικώς θα αποδείξουμε ότι οι πράξεις της πρόσθεσης και του βαθμωτού πολλαπλασιασμού είναι καλά ορισμένες. Έστω λοιπόν $x+N = x'+N$ και $y+N = y'+N$. Αυτό σημαίνει ότι $x-x', y-y' \in N$. Επομένως $(x+y)-(x'+y') = (x-x')+(y-y') \in N$. Κατά συνέπεια $(x+y)+N = (x'+y')+N$ και η πρόσθεση είναι καλά ορισμένη.
Έστω τώρα $x+N = x'+N$ και $r \in R$. Επομένως $x-x' \in N \Rightarrow rx-rx' = r(x-x') \in N$. Άρα $rx+N = rx'+N$ και ο βαθμωτός πολλαπλασιασμός είναι καλά ορισμένος. Τα υπόλοιπα είναι θέμα ρουτίνας.
1) $(x+N)+((y+N)+(z+N)) = (x+N)+((y+z)+N) = x+(y+z)+N = (x+y)+z+N =$
$= ((x+y)+N)+(z+N) = ((x+N)+(y+N))+(z+N)$ $\big($Προσεταιριστικότητα της πρόσθεσης$\big)$.
2) $(x+N)+(y+N) = (x+y)+N = (y+x)+N = (y+N)+(x+N)$ $\big($Μεταθετικότητα της πρόσθεσης$\big)$.
3) $(x+N)+N = (x+N)+(0_M+N) = (x+0_M)+N = x+N$ $\big($Ύπαρξη μηδενικού στοιχείου $0_{M/N} = N\big)$.
4) $(x+N)+(-x+N) = (x+(-x))+N = 0_M+N = N = 0_{M/N}$ $\big($Ύπαρξη αντιθέτου στοιχείου$\big)$.
5) $r((x+N)+(y+N)) = r((x+y)+N) = r(x+y)+N = (rx+ry)+N = (rx+N)+(ry+N) =$
$= r(x+N)+r(y+N)$ $\big($Επιμεριστικότητα 1$\big)$.
6) $(r+s)(x+N) = (r+s)x+N = (rx+sx)+N = (rx+N)+(sx+N) = r(x+N)+s(x+N)$
$\big($Επιμεριστικότητα 2$\big)$.
7) $(rs)(x+N) = (rs)x+N = r(sx)+N = r(sx+N) = r(s(x+N))$ $\big($Προσεταιριστικότητα βαθμωτού πολλαπλασιασμού$\big)$.
8) $1_R(x+N) = (1_R \cdot x)+N = x+N$ $\big($Δράση μοναδιαίου στοιχείου$\big)$. ■

ΜΙΑ ΣΗΜΑΝΤΙΚΗ ΠΑΡΑΤΗΡΗΣΗ: Έστω $N \leqslant M$ και $K \leqslant M$ με $N \subseteq K$. $\big($Άρα $N \leqslant K\big)$. Τότε κάθε κλάση ισοδυναμίας στο M modulo N, η οποία τέμνει το K, περιέχεται εξ ολοκλήρου στο K. Πράγματι, έστω $(x+N) \cap K \neq \varnothing$ και $y \in (x+N) \cap K$. Τότε $y+N = x+N \subseteq M$. Άρα $x-y \in N \subseteq K$ και $y \in K$. Τότε $x = (x-y)+y \in K$. Επομένως οι κλάσεις ισοδυναμίας modulo N που περιέχουν στοιχεία του K ορίζουν μια διαμέριση του K. Οι κλάσεις αυτές είναι οι κλάσεις του περιορισμού της ισοδυναμίας $\big(\equiv \mod N\big)$ στο K. Το σύνολό τους είναι το K/N, το οποίο είναι λοιπόν υποσύνολο του M/N. Στο K/N μπορούμε να ορίσουμε τις πράξεις της πρόσθεσης και του βαθμωτού πολλαπλασιασμού και να καταστήσουμε το K/N ένα R-πρότυπο. Επειδή δε $K/N \subseteq M/N$, μπορούμε **να θεωρήσουμε ότι το K/N είναι υποπρότυπο του M/N**.
Δύο ακραίες περιπτώσεις: 1) Αν $N = M$, τότε η σχέση $x \equiv y \mod M \Leftrightarrow x-y \in M$ μας λέει ότι όλα τα στοιχεία του M είναι ισοδύναμα modulo M. Επομένως το πρότυπο M/M περιέχει μία μόνο κλάση ισοδυναμίας και κατά συνέπεια το πρότυπο M/M είναι το τετριμμένο $\{0_{M/M}\} = \{M\}$.
2) Αν $N = \{0_M\}$, τότε η σχέση $x \equiv y \mod \{0_M\} \Leftrightarrow x-y = 0_M \Leftrightarrow x = y$ ταυτίζεται με την ισότητα στο M. Κάθε στοιχείο του M αποτελεί μια κλάση ισοδυναμίας. Άρα το $M/\{0_M\}$ αποτελείται από τα μονοσύνολα $\{x\}$, όπου $x \in M$. Σ' αυτή την περίπτωση, όπως θα δούμε στη συνέχεια, τα πρότυπα $M/\{0_M\}$ και M είναι **ισόμορφα**.

3.3 Ομομορφισμοί Προτύπων-Θεωρήματα Ισομορφισμών

ΟΡΙΣΜΟΣ 3.13. Έστω A και B δύο R-πρότυπα και $\varphi : A \to B$ μια απεικόνιση. Η φ λέγεται **ομομορφισμός R-προτύπων** ή **R-ομομορφισμός** αν και μόνον αν ισχύουν τα εξής:
(i) $\varphi(x+y) = \varphi(x) + \varphi(y)$, για κάθε $x, y \in A$.
(ii) $\varphi(rx) = r\varphi(x)$, για κάθε $r \in R$ και $x \in A$.
Η **εικόνα** $\varphi(A) \subseteq B$ συμβολίζεται με $\mathrm{Im}\varphi$.
Ο **πυρήνας** $\mathrm{Ker}\varphi$ είναι το σύνολο $\{x \in A \mid \varphi(x) = 0_B\}$.
Αν η φ είναι επί $\big(\mathrm{Im}\varphi = B\big)$, τότε η φ λέγεται **επιμορφισμός**.
Αν η φ είναι 1-1, τότε η φ λέγεται **μονομορφισμός**.
Τέλος αν η φ είναι 1-1 και επί $\big($μονομορφισμός και επιμορφισμός$\big)$, τότε η φ λέγεται **ισομορφισμός**.
Σε αυτήν την περίπτωση **τα A και B λέγονται ισόμορφα R-πρότυπα**. Τότε γράφουμε $A \underset{R}{\cong} B$ ή απλά $A \cong B$.
Είναι σαφές ότι η αντίστροφη απεικόνιση $\varphi^{-1} : B \to A$ ενός ισομορφισμού είναι επίσης ισομορφισμός.

ΠΡΟΤΑΣΗ 3.14. **(i)** Η εικόνα $\mathrm{Im}\varphi$ είναι υποπρότυπο του B. Γενικότερα, αν $C \leqslant A$, τότε $\varphi(C) \leqslant B$.
(ii) Ο πυρήνας $\mathrm{Ker}\varphi = \varphi^{-1}(\{0_B\})$ είναι υποπρότυπο του A. Γενικότερα, αν $D \leqslant B$, τότε $\varphi^{-1}(D) \leqslant A$.
(iii) Η φ είναι μονομορφισμός αν και μόνον αν $\mathrm{Ker}\varphi = \{0_A\}$.
ΑΠΟΔΕΙΞΗ: (i) Έστω $\beta_1, \beta_2 \in \varphi(C)$. Τότε υπάρχουν $c_1, c_2 \in C$ τέτοια, ώστε $\beta_1 = \varphi(c_1)$ και $\beta_2 = \varphi(c_2)$. Επομένως $\beta_1 + \beta_2 = \varphi(c_1) + \varphi(c_2) = \varphi(c_1 + c_2) \in \varphi(C)$, αφού $c_1 + c_2 \in C \leqslant A$. Έστω τώρα $\beta \in \varphi(C)$ και $r \in R$. Τότε $\beta = \varphi(c)$, για κάποιο $c \in C$. Άρα $r\beta = r\varphi(c) = \varphi(rc) \in \in \varphi(C)$, αφού $rc \in C \leqslant A$.
(ii) Έστω $\alpha_1, \alpha_2 \in \varphi^{-1}(D)$, δηλαδή $\varphi(\alpha_1), \varphi(\alpha_2) \in D$. Τότε $\varphi(\alpha_1 + \alpha_2) = \varphi(\alpha_1) + \varphi(\alpha_2) \in D$, δηλαδή $\alpha_1 + \alpha_2 \in \varphi^{-1}(D)$. Έστω $\alpha \in \varphi^{-1}(D) \Leftrightarrow \varphi(\alpha) \in D$ και $r \in R$. Τότε $\varphi(r\alpha) = r\varphi(\alpha) \in D$. Άρα $r\alpha \in \varphi^{-1}(D)$.
(iii) Έστω $\mathrm{Ker}\varphi = \{0_A\}$. Υποθέτουμε ότι $\varphi(\alpha_1) = \varphi(\alpha_2)$, για κάποια $\alpha_1, \alpha_2 \in A$.
Τότε $\varphi(\alpha_1 - \alpha_2) = \varphi(\alpha_1) - \varphi(\alpha_2) = 0_B \Rightarrow \alpha_1 - \alpha_2 \in \mathrm{Ker}\varphi = \{0_A\}$, δηλαδή $\alpha_1 = \alpha_2$. Άρα η φ είναι μονομορφισμός.
Αντιστρόφως, έστω ότι η φ είναι μονομορφισμός. Τότε επειδή $\varphi(0_A) = 0_B$, θα είχαμε $\varphi(\alpha) = = \varphi(0_A)$, για κάθε στοιχείο α του $\mathrm{Ker}\varphi$ και επειδή η φ είναι μονομορφισμός, αναγκαστικά $\alpha = 0_A$. ■

ΠΡΟΤΑΣΗ 3.15. Έστω M ένα R-πρότυπο και $N \leqslant M$. Θεωρούμε την απεικόνιση
$$p : M \to M/N, \text{ όπου } p(x) = x + N, \text{ για κάθε } x \in M.$$
(i) Η p είναι ένας επιμορφισμός R-προτύπων, ο οποίος καλείται **φυσικός επιμορφισμός** ή **φυσική προβολή**. Πυρήνας της p είναι το N.
(ii) Έστω $\mathscr{A}$ το σύνολο των υποπροτύπων του M, τα οποία περιέχουν το N και $\mathscr{B}$ το σύνολο των υποπροτύπων του M/N. Η απεικόνιση $T : \mathscr{A} \to \mathscr{B}$ με $T(L) = p(L) = L/N$ είναι μια αμφιμονοσήμαντη αντιστοιχία $\big($1-1 και επί$\big)$.
ΑΠΟΔΕΙΞΗ: (i) $p(x+y) = (x+y) + N = (x+N) + (y+N) = p(x) + p(y)$ και αν $r \in R$, τότε $p(rx) = rx + N = r(x+N) = rp(x)$. Άρα η p είναι R-ομομορφισμός. Η p είναι προφανώς επί. Επίσης, $x \in \mathrm{Ker}p \Leftrightarrow p(x) = x + N = N = 0_{M/N} \Leftrightarrow x \in N$.
(ii) Αν $N \leqslant L \leqslant M$, τότε σύμφωνα και με την παρατήρηση στο τέλος της προηγούμενης

παραγράφου, $T(L) = p(L) = \{x + N \mid x \in L\} = L/N$.
Αντιστρόφως, έστω $\bar{L}$ υποπρότυπο του M/N. Εφόσον p επιμορφισμός και $0_{M/N} \in \bar{L}$, έπεται ότι το υποπρότυπο $L := p^{-1}(\bar{L}) = \{x \in M \mid x + N \in \bar{L}\}$ (βλέπε και **(ii)** προηγούμενης πρότασης) περιέχει το $p^{-1}(\{0_{M/N}\}) = \text{Ker}p = N$. Επειδή η p είναι επί, $T(L) = p(L) = p(p^{-1}(\bar{L})) = \bar{L}$. Αν $N \leqslant L' \leqslant M$ με $T(L) = T(L')$, δηλαδή $p(L) = \{x + N \mid x \in L\} = \{x + N \mid x \in L'\} = p(L')$, τότε θα έχουμε: $x \in L \Rightarrow x + N \in p(L) = p(L') \Rightarrow x + N = x' + N$, για κάποιο $x' \in L'$. Επομένως $x - x' \in N \leqslant L' \Rightarrow x = (x - x') + x' \in L'$. Άρα $L \leqslant L'$. Ομοίως $L' \leqslant L$. Άρα $L = L'$. ■

ΘΕΩΡΗΜΑ 3.16. 1ο ΘΕΩΡΗΜΑ ΙΣΟΜΟΡΦΙΣΜΩΝ: Έστω M και N δύο R-πρότυπα και $\varphi : M \to N$ ένας R-ομομορφισμός. Τότε ισχύει

$$M/\text{Ker}\varphi \cong \text{Im}\varphi.$$

ΑΠΟΔΕΙΞΗ: Ορίζουμε την απεικόνιση $\bar{\varphi} : M/\text{Ker}\varphi \to \text{Im}\varphi$ βάσει του τύπου

$$\bar{\varphi}(x + \text{Ker}\varphi) = \varphi(x), \text{ για κάθε } x \in M.$$

1) Η $\bar{\varphi}$ είναι καλά ορισμένη. Έστω $x + \text{Ker}\varphi = y + \text{Ker}\varphi \Leftrightarrow x - y \in \text{Ker}\varphi \Leftrightarrow \varphi(x) - \varphi(y) = \varphi(x - y) = 0_N \Leftrightarrow \varphi(x) = \varphi(y)$.
2) Η $\bar{\varphi}$ είναι R-γραμμική. Πράγματι, $\bar{\varphi}((x+\text{Ker}\varphi)+(y+\text{Ker}\varphi)) = \bar{\varphi}(x+y+\text{Ker}\varphi) = \varphi(x+y) = \varphi(x) + \varphi(y) = \bar{\varphi}(x + \text{Ker}\varphi) + \bar{\varphi}(y + \text{Ker}\varphi)$ και
$\bar{\varphi}(r(x + \text{Ker}\varphi)) = \bar{\varphi}(rx + \text{Ker}\varphi) = \varphi(rx) = r\varphi(x) = r\bar{\varphi}(x + \text{Ker}\varphi)$.
3) Η $\bar{\varphi}$ είναι προφανώς επί γιατί $\text{Im}\varphi \ni \varphi(x) = \bar{\varphi}(x + \text{Ker}\varphi)$, για κάθε $x \in M$.
4) $\text{Ker}\bar{\varphi} = \{0_{M/\text{Ker}\varphi}\}$. Πράγματι, έστω $x + \text{Ker}\varphi \in \text{Ker}\bar{\varphi}$. Τότε $\varphi(x) = \bar{\varphi}(x + \text{Ker}\varphi) = 0_N$. Συνεπώς $x \in \text{Ker}\varphi \Leftrightarrow x + \text{Ker}\varphi = \text{Ker}\varphi = 0_{M/\text{Ker}\varphi}$.
Από τα προηγούμενα προκύπτει ότι η φ είναι R-ισομορφισμός. ■

ΘΕΩΡΗΜΑ 3.17. 2ο ΘΕΩΡΗΜΑ ΙΣΟΜΟΡΦΙΣΜΩΝ: Έστω K και L δύο υποπρότυπα ενός R-προτύπου M. Τότε

$$K + L\Big/_K \cong L\Big/_{K \cap L} \qquad \text{και} \qquad K + L\Big/_L \cong K\Big/_{K \cap L}$$

ΑΠΟΔΕΙΞΗ: Θα αποδείξουμε την πρώτη σχέση. Επειδή $L \leqslant K + L$, θεωρούμε την εμφύτευση (μονομορφισμό) $i : L \hookrightarrow K + L$ με $i(y) = y$, για κάθε $y \in L$. Στη συνέχεια θεωρούμε την φυσική προβολή $p : K + L \to K + L\Big/_K$. Έστω $\varphi = p \circ i : L \to K + L\Big/_K$.

1) Ένα στοιχείο του $K + L\Big/_K$ είναι της μορφής $x + y + K$, όπου $x \in K$ και $y \in L$. Αλλά τότε $x + y + K = (x + K) + (y + K) \underset{x \in K}{=} K + (y + K) = y + K = (p \circ i)(y) = \varphi(y)$. Επομένως η $\varphi = p \circ i$ είναι επί.
2) Έστω $y \in \text{Ker}\varphi$. Τότε $K = 0_{K+L/K} = \varphi(y) = y + K$. Άρα $y \in K$ και επειδή $y \in L$, έπεται ότι $y \in K \cap L$. Αντιστρόφως, έστω $y \in K \cap L \subseteq K$. Τότε $\varphi(y) = y + K \underset{y \in K}{=} K = 0_{K+L/K}$, δηλαδή $y \in \text{Ker}\varphi$. Επομένως $\text{Ker}\varphi = K \cap L$.
Από το 1ο θεώρημα ισομορφισμών παίρνουμε ότι

$$K + L\Big/_K = \text{Im}\varphi \cong L\Big/_{\text{Ker}\varphi} = L\Big/_{K \cap L}$$ ■

ΘΕΩΡΗΜΑ 3.18. 3ο ΘΕΩΡΗΜΑ ΙΣΟΜΟΡΦΙΣΜΩΝ: Έστω K, L, M τρία R-πρότυπα με $K \leqslant L \leqslant M$. Τότε ισχύει:

$$M\Big/_L \cong M\Big/_K \Big/ L\Big/_K$$

ΑΠΟΔΕΙΞΗ: Θεωρούμε την απεικόνιση $\varphi : M\Big/_K \to M\Big/_L$ με $\varphi(x + K) = x + L$, για κάθε

$x \in M$. Η φ είναι καλά ορισμένη γιατί αν $x + K = x' + K$, τότε $x - x' \in K \leqslant L$. Επομένως $x + L = x' + L$. Η γραμμικότητα είναι προφανής. $\big(\varphi\big((x + K) + (x' + K)\big) = \varphi(x + x' + K) = = x + x' + L = (x + L) + (x' + L) = \varphi(x + K) + \varphi(x' + K)$ και $\varphi(r(x + K)) = \varphi(rx + K) = = rx + L = r(x + L) = r\varphi(x + K)\big)$. Η φ είναι επί γιατί $x + L = \varphi(x + K)$, για κάθε $x \in M$. Τώρα, όσον αφορά τον πυρήνα: $x + K \in \text{Ker}\varphi \Leftrightarrow \varphi(x + K) = 0_{M/L} = L \Leftrightarrow x + L = L \Leftrightarrow x \in \in L \Leftrightarrow x+K \in L/K$. Επομένως $\text{Ker}\varphi = L/K$ και το αποτέλεσμα προκύπτει από το 1ο θεώρημα ισομορφισμών. ■

3.4 Ευθέα Αθροίσματα Προτύπων και Δακτυλίων

ΟΡΙΣΜΟΣ 3.19. Έστω $M_1, M_2, \ldots, M_k$ υποπρότυπα ενός προτύπου M. Λέμε ότι **το M είναι το εσωτερικό ευθύ άθροισμα των $M_1, M_2, \ldots, M_k$** και γράφουμε

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$$

αν και μόνον αν ισχύουν τα επόμενα:

(i) Το M παράγεται $\big($είναι το άθροισμα$\big)$ των υποπροτύπων $M_1, M_2, \ldots, M_k$, δηλαδή

$$M = \textstyle\sum_{i=1}^{k} M_i \quad .$$

(ii) Για κάθε $i = 1, 2, \ldots, k$ η τομή $M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_k) = M_i \cap \sum_{j\neq i} M_j$ είναι το τετριμμένο $\big($μηδενικό$\big)$ υποπρότυπο.

ΠΡΟΤΑΣΗ 3.20. $\big($Εναλλακτικός ορισμός του εσωτερικού ευθέος αθροίσματος$\big)$
Έστω M_1, M_2, $\ldots, M_k$ υποπρότυπα ενός προτύπου M. Τότε το M είναι το εσωτερικό ευθύ άθροισμα των M_i αν και μόνον αν ισχύει το εξής:
Κάθε στοιχείο x του M γράφεται **μονοσήμαντα** στη μορφή $x = x_1 + x_2 + \cdots + x_k$, όπου $x_i \in M_i$, για κάθε $i = 1, 2, \ldots, k$.

ΑΠΟΔΕΙΞΗ: Έστω ότι ισχύουν οι υποθέσεις της πρότασης. Από το γεγονός ότι κάθε στοιχείο του M γράφεται σαν άθροισμα στοιχείων των M_i προκύπτει ότι $M = \sum_{i=1}^{k} M_i$. Έστω τώρα $y \in M_i \cap \sum_{j\neq i} M_j$. Τότε $y = x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_k \Leftrightarrow 0_M = x_1 + \cdots + x_{i-1} + (-y) + +x_{i+1} + \cdots + x_k$. Αλλά $0_M = 0_M + 0_M + \cdots + 0_M$. Από τη μοναδικότητα της γραφής προκύπτει ότι $-y = 0_M \Leftrightarrow y = 0_M$. Άρα $M_i \cap \sum_{j\neq i} M_j = \{0_M\}$.

Αντιστρόφως, έστω ότι ισχύουν οι υποθέσεις του προηγούμενου ορισμού. Εφόσον $M = \sum_{i=1}^{k} M_i$, κάθε στοιχείο $x \in M$ γράφεται στη μορφή $x = x_1 + x_2 + \cdots + x_k$, όπου $x_i \in M_i$, για κάθε $i = 1, 2, \ldots, k$. Αν το x γραφόταν και στη μορφή $x = x'_1 + x'_2 + \cdots + x'_k$, όπου $x'_i \in M_i$, για κάθε $i = 1, 2, \ldots, k$, τότε θα είχαμε $x_1 + x_2 + \cdots + x_k = x'_1 + x'_2 + \cdots + x'_k$. Τότε για κάθε $i = 1, 2, \ldots, k$ παίρνουμε τη σχέση
$x_i - x'_i = (x'_1 - x_1) + \cdots + (x'_{i-1} - x_{i-1}) + (x'_{i+1} - x_{i+1}) + \cdots + (x'_k - x_k) \in M_i \cap \sum_{j\neq i} M_j = \{0\}$.
Άρα $x_i = x'_i$, για κάθε $i = 1, 2, \ldots, k$. ■

Από τον ορισμό του ευθέος αθροίσματος υποπροτύπων ενός προτύπου M προκύπτει ότι η διάταξη $\{M_1, M_2, \ldots, M_k\}$ δεν παίζει κανέναν ρόλο. Δηλαδή, αν $\sigma \in S_k$ $\big($μετάθεση των k συμβόλων$\big)$, τότε

$$M_1 \oplus M_2 \oplus \cdots \oplus M_k = M_{\sigma(1)} \oplus M_{\sigma(2)} \oplus \cdots \oplus M_{\sigma(k)}.$$

Πολλές φορές χρησιμοποιούμε τον συμβολισμό $\bigoplus_{i=1}^{k} M_i$ αντί του $M_1 \oplus M_2 \oplus \cdots \oplus M_k$.

Αν τώρα έχουμε k R-πρότυπα, M_1, M_2,...,M_k, **τα οποία δεν είναι κατ' ανάγκην υποπρότυπα**

ενός προτύπου M, μπορούμε να ορίσουμε μεταξύ τους κάποιο είδος ευθέος αθροίσματος;

ΟΡΙΣΜΟΣ 3.21. Έστω M_1, M_2,...,M_k R-πρότυπα. Θέτουμε $M = M_1 \times M_2 \times \cdots \times M_k$ για το καρτεσιανό γινόμενό τους. Εφοδιάζουμε το M με τις κατά σημείον πράξεις:

$$(x_1, x_2, \ldots, x_k) + (y_1, y_2, \ldots, y_k) = (x_1 + y_1, x_2 + y_2, \ldots, x_k + y_k)$$

και

$$r \cdot (x_1, x_2, \ldots, x_k) = (rx_1, rx_2, \ldots, rx_k).$$

Τότε εύκολα διαπιστώνει κανείς ότι το $M = M_1 \times M_2 \times \cdots \times M_k$ καθίσταται R-πρότυπο. Το μηδενικό του στοιχείο είναι το $(0_{M_1}, 0_{M_2}, \ldots, 0_{M_k})$. Το πρότυπο αυτό λέγεται **εξωτερικό ευθύ άθροισμα** (ή γινόμενο) **των $M_1, M_2, \ldots, M_k$**.

ΠΡΟΤΑΣΗ 3.22. Έστω M_1, M_2, $\ldots$, M_k υποπρότυπα ενός προτύπου M με

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_k.$$

Τότε υπάρχει ισομορφισμός

$$M_1 \times M_2 \times \cdots \times M_k \cong M_1 \oplus M_2 \oplus \cdots \oplus M_k = M.$$

ΑΠΟΔΕΙΞΗ: Έστω $\varphi : M_1 \times M_2 \times \cdots \times M_k \to M_1 \oplus M_2 \oplus \cdots \oplus M_k$ με

$$\varphi(x_1, x_2, \ldots, x_k) = x_1 + x_2 + \cdots + x_k.$$

Επειδή κάθε στοιχείο του M παριστάνεται μοναδικά ως άθροισμα $x_1 + x_2 + \cdots + x_k$, η φ είναι επί. Προφανώς είναι R-γραμμική. Έστω $(x_1, x_2, \ldots, x_k) \in \mathrm{Ker}\varphi$. Τότε $x_1 + x_2 + \cdots + x_k = 0_M = 0_M + 0_M + \cdots + 0_M$. Επειδή κάθε στοιχείο του M παριστάνεται μοναδικά ως άθροισμα στοιχείων των M_i, έπεται ότι $x_1 = x_2 = \cdots = x_k = 0_M$, άρα $(x_1, x_2, \ldots, x_k) = (0_M, 0_M, \ldots, 0_M)$, το οποίο είναι το μηδενικό στοιχείο του $M_1 \times M_2 \times \cdots \times M_k$. ■

Το εξωτερικό ευθύ άθροισμα των R-προτύπων M_1, M_2, $\ldots$, M_k μπορεί να παρασταθεί ως εσωτερικό ευθύ άθροισμα ισομόρφων αντιγράφων των M_i.

Έστω M_1, M_2, $\ldots$, M_k R-πρότυπα. Για κάθε $i = 1, 2, \ldots, k$ ορίζουμε στο εξωτερικό ευθύ άθροισμα $M_1 \times M_2 \times \cdots \times M_k$

$$\overline{M}_i = \{(0_{M_1}, 0_{M_2}, \ldots, 0_{M_{i-1}}, \underset{\substack{\uparrow \\ i \text{ θέση}}}{x}, 0_{M_{i+1}}, \ldots, 0_{M_k}) \mid x \in M_i\}.$$

Το $\overline{M}_i$ είναι προφανώς υποπρότυπο του $M_1 \times M_2 \times \cdots \times M_k$.

Τώρα, η απεικόνιση $\varphi_i : M_i \to \overline{M}_i$ με $\varphi_i(x) = (0_{M_1}, 0_{M_2}, \ldots, 0_{M_{i-1}}, \underset{\substack{\uparrow \\ i \text{ θέση}}}{x}, 0_{M_{i+1}}, \ldots, 0_{M_k})$, για κάθε $x \in M_i$ είναι προφανώς ισομορφισμός R-προτύπων.

ΠΡΟΤΑΣΗ 3.23. Σύμφωνα με τους παραπάνω συμβολισμούς

$$M_1 \times M_2 \times \cdots \times M_k = \overline{M}_1 \oplus \overline{M}_2 \oplus \cdots \oplus \overline{M}_k.$$

ΑΠΟΔΕΙΞΗ: Η απόδειξη είναι άμεση, αφού το τυχόν στοιχείο $(x_1, x_2, \ldots, x_k)$ του $M_1 \times M_2 \times \cdots \times M_k$ γράφεται μονοσήμαντα στη μορφή

$$(x_1, x_2, \ldots, x_k) = (x_1, 0_{M_2}, \ldots, 0_{M_k}) + (0_{M_1}, x_2, \ldots, 0_{M_k}) + \cdots + (0_{M_1}, 0_{M_2}, \ldots, x_k).$$ ■

Από τα παραπάνω καθίσταται φανερό ότι οι συμβολισμοί $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ και $M_1 \times M_2 \times \cdots \times M_k$ είναι (ως προς ισομορφισμό) ισοδύναμοι και θα χρησιμοποιούνται αμφότεροι στα επόμενα, ανάλογα με το ποιος είναι ο προσφορότερος στο εκάστοτε πρόβλημα. Ακόμα και στην περίπτωση που τα πρότυπα $M_1, M_2, \ldots, M_k$ δεν είναι υποπρότυπα ενός προτύπου M, μπορούμε να χρησιμοποιούμε τον συμβολισμό $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ υπονοώντας σαφώς το ευθύ άθροισμα $\overline{M}_1 \oplus \overline{M}_2 \oplus \cdots \oplus \overline{M}_k$ των ισομόρφων αντιγράφων των $M_1, M_2, \ldots, M_k$.

Στην ειδική περίπτωση που το R-πρότυπο είναι ο ίδιος ο δακτύλιος R, τότε τα υποπρότυπά

του είναι τα ιδεώδη του. Έστω R μοναδιαίος μεταθετικός δακτύλιος και $S_1, S_2, \ldots, S_k$ μη μηδενικά ιδεώδη του R. Θα γράφουμε $R = S_1 \oplus S_2 \oplus \cdots \oplus S_k$ αν ο R (ως R-πρότυπο) είναι το ευθύ άθροισμα των $S_1, S_2, \ldots, S_k$ (ως R-υποπρότυπα).

ΠΡΟΤΑΣΗ 3.24. Έστω $R = S_1 \oplus S_2 \oplus \cdots \oplus S_k$, όπου $S_1, S_2, \ldots, S_k$ μη μηδενικά ιδεώδη του R. Τότε ισχύουν τα εξής:
(i) $S_iS_j = S_i \cap S_j = \{0\}$, για $i \neq j$.
(ii) $1_R = e_1 + e_2 + \cdots + e_k$, $e_i^2 = e_i \in S_i$, για κάθε i και $e_ie_j = 0$, για $i \neq j$.
(iii) Κάθε ιδεώδες S_i είναι μοναδιαίος μεταθετικός δακτύλιος. Το μοναδιαίο στοιχείο του είναι το e_i.
ΑΠΟΔΕΙΞΗ: (i) $S_iS_j \subseteq RS_j \subseteq S_j$. Ομοίως $S_iS_j \subseteq S_iR \subseteq S_i$. Επομένως $S_iS_j \subseteq S_i \cap S_j = \{0\}$, γιατί το άθροισμα $S_1 \oplus S_2 \oplus \cdots \oplus S_k$ είναι ευθύ.
(ii) Έστω $1_R = e_1 + e_2 + \cdots + e_k$, όπου $e_i \in S_i$, για κάθε $i = 1, 2, \ldots, k$. Τότε $e_i = 1_R \cdot e_i = (e_1+e_2+\cdots+e_k)e_i = e_1e_i+e_2e_i+\cdots+e_{i-1}e_i+e_i^2+e_{i+1}e_i+\cdots+e_ke_i$. Αλλά $e_je_i \in S_jS_i = \{0\}$, για κάθε $j \neq i$. Επομένως και $e_i^2 = e_i$, για κάθε $i = 1, 2, \ldots, k$.
(iii) Το ότι κάθε ιδεώδες S_i είναι μεταθετικός δακτύλιος το ξέρουμε. Τώρα, αν $x \in S_i$, τότε $x = 1_R \cdot x = (e_1 + e_2 + \cdots + e_k)x = e_1x + e_2x + \cdots + e_kx$. Για $j \neq i$ έχουμε $e_jx \in S_jS_i = \{0\}$. Άρα $e_jx = 0$, για κάθε $j \neq i$. Συνεπώς $x = e_ix$. Άρα, εφόσον $S_i \neq \{0\}$, $e_i \neq 0$ και το e_i είναι το μοναδιαίο στοιχείο του δακτυλίου S_i. ■

ΟΡΙΣΜΟΣ 3.25. Αν ισχύουν οι συνθήκες της προηγούμενης πρότασης, τότε λέμε ότι **ο R είναι το εσωτερικό ευθύ άθροισμα των δακτυλίων $S_1, S_2, \ldots, S_k$**.

ΟΡΙΣΜΟΣ 3.26. Έστω $R_1, R_2, \ldots, R_k$ είναι μοναδιαίοι μεταθετικοί δακτύλιοι, τότε θέτουμε
$$R = R_1 \times R_2 \times \cdots \times R_k.$$
Ο R γίνεται μοναδιαίος μεταθετικός δακτύλιος με πράξεις
$$(r_1, r_2, \ldots, r_k) + (s_1, s_2, \ldots, s_k) = (r_1 + s_1, r_2 + s_2, \ldots, r_k + s_k) \text{ (πρόσθεση)}$$
και
$$(r_1, r_2, \ldots, r_k) \cdot (s_1, s_2, \ldots, s_k) = (r_1s_1, r_2s_2, \ldots, r_ks_k) \text{ (πολλαπλασιασμός)}.$$
Το μηδενικό στοιχείο του R είναι το $0_R = (0_{R_1}, 0_{R_2}, \ldots, 0_{R_k})$ και το μοναδιαίο το $1_R = (1_{R_1}, 1_{R_2}, \ldots, 1_{R_k})$.
Ο δακτύλιος $R = R_1 \times R_2 \times \cdots \times R_k$ λέγεται **εξωτερικό ευθύ άθροισμα των δακτυλίων $R_1, R_2, \ldots, R_k$**.

Όπως συμβαίνει με τα πρότυπα, έτσι και με τους δακτυλίους, το εξωτερικό ευθύ άθροισμα των δακτυλίων $R_1, R_2, \ldots, R_k$ μπορεί να παρασταθεί ως εσωτερικό ευθύ άθροισμα ισόμορφων αντιγράφων (ως προς ισομορφισμό δακτυλίων) των R_i.
Θέτουμε $\overline{R}_i = \{(0_{R_1}, 0_{R_2}, \ldots, 0_{R_{i-1}}, \underset{\substack{\uparrow \\ i \text{ θέση}}}{r}, 0_{R_{i+1}}, \ldots, 0_{R_k}) \mid r \in R_i\}$. Το $\overline{R}_i$ είναι ιδεώδες του R, αφού
$$(0_{R_1}, 0_{R_2}, \ldots, 0_{R_{i-1}}, r_1, 0_{R_{i+1}}, \ldots, 0_{R_k}) + (0_{R_1}, 0_{R_2}, \ldots, 0_{R_{i-1}}, r_2, 0_{R_{i+1}}, \ldots, 0_{R_k}) = (0_{R_1}, 0_{R_2}, \ldots, 0_{R_{i-1}}, r_1 + r_2, 0_{R_{i+1}}, \ldots, 0_{R_k})$$
και
$$(s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_k) \cdot (0_{R_1}, 0_{R_2}, \ldots, 0_{R_{i-1}}, r, 0_{R_{i+1}}, \ldots, 0_{R_k}) = (0_{R_1}, 0_{R_2}, \ldots, 0_{R_{i-1}}, s_ir, 0_{R_{i+1}}, \ldots, 0_{R_k}) \in \overline{R}_i.$$
Θεωρούμε την απεικόνιση $\varphi_i : R_i \to \overline{R}_i$ με $\varphi_i(r) = (0_{R_1}, 0_{R_2}, \ldots, 0_{R_{i-1}}, \underset{\substack{\uparrow \\ i \text{ θέση}}}{r}, 0_{R_{i+1}}, \ldots, 0_{R_k})$, για κάθε $i = 1, 2, \ldots, k$. Εύκολα επαληθεύει κανείς ότι η φ_i είναι ισομορφισμός δακτυλίων. Είναι σαφές ότι $R = \overline{R}_1 \oplus \overline{R}_2 \oplus \cdots \oplus \overline{R}_k$, δηλαδή ο R είναι ευθύ άθροισμα ισομόρφων αντιγράφων των δακτυλίων R_i, τα οποία (ισόμορφα αντίγραφα) είναι ιδεώδη του.

ΠΡΟΤΑΣΗ 3.27. Έστω $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$, όπου $k \geq 3$ και $1 \leq \lambda < k$. Τότε
$$M = \big(M_1 \oplus \cdots \oplus M_\lambda\big) \bigoplus \big(M_{\lambda+1} \oplus \cdots \oplus M_k\big).$$
ΑΠΟΔΕΙΞΗ: Κατ' αρχάς τα αθροίσματα $M_1 + \cdots + M_\lambda$ και $M_{\lambda+1} + \cdots + M_k$ είναι ευθέα. Αυτό προκύπτει απ' το γεγονός ότι $M_i \bigcap \left(\sum\limits_{\substack{1 \leq j \leq \lambda \\ j \neq i}} M_j \right) \subseteq M_i \bigcap \left(\sum\limits_{\substack{1 \leq j \leq k \\ j \neq i}} M_j \right) = \{0\}$ και παρόμοια για το δεύτερο άθροισμα. Έστω $x \in M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$. Τότε υπάρχουν μοναδικά $x_i \in M_i$ τέτοια, ώστε $x = x_1 + \cdots + x_\lambda + x_{\lambda+1} + \cdots + x_k$. Έστω $x' = x_1 + \cdots + x_\lambda$ και $x'' = x_{\lambda+1} + \cdots + x_k$. Τότε $x = x' + x''$, όπου $x' \in M_1 \oplus \cdots \oplus M_\lambda$ και $x'' \in M_{\lambda+1} \oplus \cdots \oplus M_k$. Επομένως $M = \big(M_1 \oplus \cdots \oplus M_\lambda\big) + \big(M_{\lambda+1} \oplus \cdots \oplus M_k\big)$.
Αρκεί να αποδείξουμε ότι $\big(M_1 \oplus \cdots \oplus M_\lambda\big) \bigcap \big(M_{\lambda+1} \oplus \cdots \oplus M_k\big) = \{0\}$. Έστω λοιπόν $x \in$ $\in \big(M_1 \oplus \cdots \oplus M_\lambda\big) \bigcap \big(M_{\lambda+1} \oplus \cdots \oplus M_k\big)$. Εφόσον $x \in M_1 \oplus \cdots \oplus M_\lambda$, υπάρχουν μοναδικά $x_1 \in M_1$, $x_2 \in M_2$,...,$x_\lambda \in M_\lambda$ τέτοια, ώστε $x = x_1 + \cdots + x_\lambda$. Ομοίως, υπάρχουν μοναδικά $x_{\lambda+1} \in M_{\lambda+1}, \ldots, x_k \in M_k$ τέτοια, ώστε $x = x_{\lambda+1} + \cdots + x_k$. Επομένως $0 = \underbrace{0 + 0 + \cdots + 0}_{k \text{ φορές}} =$
$= x_1 + \cdots + x_\lambda + (-x_{\lambda+1}) + \cdots + (-x_k)$ με $x_1 \in M_1, \ldots, x_\lambda \in M_\lambda, -x_{\lambda+1} \in M_{\lambda+1}, \ldots, -x_k \in$ $\in M_k$. Επειδή το άθροισμα $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ είναι ευθύ, έπεται ότι $x_1 = x_2 = \cdots = x_\lambda =$ $= 0\big(= -x_{\lambda+1} = \cdots = -x_k\big)$. Άρα $x = x_1 + \cdots + x_\lambda = 0$. ■

ΠΡΟΤΑΣΗ 3.28. Έστω $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$ και κάποιο από τα $M_1, \ldots, M_k$, έστω το M_i είναι το μηδενικό πρότυπο. Τότε $M = M_1 \oplus M_2 \oplus \cdots \oplus M_{i-1} \oplus M_{i+1} \oplus \cdots \oplus M_k$.
ΑΠΟΔΕΙΞΗ: Άμεση, αφού κάθε στοιχείο $x \in M$ γράφεται κατά τρόπο μοναδικό στη μορφή $x = x_1 + \cdots + x_{i-1} + 0_M + x_{i+1} + \cdots + x_k = x_1 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_k$, όπου $x_j \in M_j$, για $j \neq i$ και $0_M \in M_i = \{0_M\}$. ■

Το υποπρότυπο N ενός ευθέος αθροίσματος υποπροτύπων $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$ δεν είναι αναγκαστικά ευθύ άθροισμα υποπροτύπων $N = N_1 \oplus \cdots \oplus N_k$, όπου $N_i \leqslant M_i$, για κάθε $i = 1, \ldots, k$. Πάρτε για παράδειγμα $R = \mathbb{R}$ και $M = \mathbb{R}^2$. Προφανώς $\mathbb{R}^2 = V_1 \oplus V_2$, όπου $V_1 = \{(x, 0) \mid x \in \mathbb{R}\}$ και $V_2 = \{(0, x) \mid x \in \mathbb{R}\}$. Θεωρείστε το υποπρότυπο $\big($διανυσματικό υπόχωρο$\big)$ $N = \{(x, x) \mid x \in \mathbb{R}\}$. Επειδή $N \cap V_1 = N \cap V_2 = \{(0, 0)\}$, το N δεν διασπάται σε ευθύ άθροισμα υποχώρων των V_1 και V_2.

ΠΡΟΤΑΣΗ 3.29. Έστω $M = M_1 \oplus \cdots \oplus M_k$ και $N \leqslant M$ με $N = N_1 \oplus \cdots \oplus N_k$, όπου $N_i \leqslant M_i$, για κάθε $i = 1, \ldots, k$. Τότε
$$M \Big/ N \;\cong\; M_1 \Big/ N_1 \times \cdots \times M_k \Big/ N_k$$
ή αλλιώς
$$M_1 \times M_2 \times \cdots \times M_k \Big/ N_1 \times N_2 \times \cdots \times N_k \;\cong\; M_1 \Big/ N_1 \times M_2 \Big/ N_2 \times \cdots \times M_k \Big/ N_k$$
ΑΠΟΔΕΙΞΗ: Ορίζουμε την απεικόνιση $\varphi : M \to M_1 \Big/ N_1 \times \cdots \times M_k \Big/ N_k$ ως εξής: Κάθε στοιχείο x του M γράφεται μονοσήμαντα στη μορφή $x = x_1 + \cdots + x_k$, όπου $x_i \in M_i$, για κάθε $i = 1, \ldots, k$. Θέτουμε $\varphi(x) = \varphi(x_1 + \cdots + x_k) = (x_1 + N_1, \ldots, x_k + N_k) \in M_1 \Big/ N_1 \times \cdots \times$ $\times M_k \Big/ N_k$. Επειδή το x γράφεται μονοσήμαντα στη μορφή $x_1 + \cdots + x_k$, η φ είναι καλά ορισμένη. Είναι R-γραμμική, όπως εύκολα κανείς μπορεί να διαπιστώσει. Αν τώρα $x_i \in M_i$, για κάθε $i = 1, \ldots, k$, τότε $(x_1 + N_1, \ldots, x_k + N_k) = \varphi(x_1 + \cdots + x_k)$. Επομένως η φ είναι επί. Απομένει ο πυρήνας της. Έστω $x = x_1 + \cdots + x_k \in \mathrm{Ker}\varphi$, όπου $x_i \in M_i$, για κάθε $i = 1, \ldots, k$. Τότε $\varphi(x_1 + \cdots + x_k) = (x_1 + N_1, \ldots, x_k + N_k) = (0_{M_1/N_1}, \ldots, 0_{M_k/N_k}) = (N_1, \ldots, N_k)$, ισοδύναμα $x_i \in N_i$, για κάθε $i = 1, \ldots, k$. Δηλαδή $x = x_1 + \cdots + x_k \in N_1 \oplus \cdots \oplus N_k = N$. Επομένως

$\mathrm{Ker}\varphi = N$ και το αποτέλεσμα προκύπτει από το 1ο θεώρημα ισομορφισμών. Επομένως η φ επάγεται έναν ισομοφισμό $\overline{\varphi}: M\Big/_N \to M_1\Big/_{N_1} \times\cdots\times M_k\Big/_{N_k}$ με $\overline{\varphi}(x_1+x_2+\cdots+x_k+N) = (x_1+N_1, x_2+N_2, \ldots, x_k+N_k)$.
Στην περίπτωση που έχουμε $M_1\times M_2\times\cdots\times M_k\Big/_{N_1\times N_2\times\cdots\times N_k}$ η παραπάνω απόδειξη είναι παρόμοια: Ορίζουμε την $\varphi: M_1\times M_2\times\cdots\times M_k \to M_1\Big/_{N_1}\times\cdots\times M_k\Big/_{N_k}$ με $\varphi(x_1, x_2, \ldots, x_k) = \big(x_1+N_1, x_2+N_2, \ldots, x_k+N_k\big)$ και προχωράμε παρόμοια όπως προηγουμένως. ■

Μέσω της ταύτισης $x+N_i = (0_{M_1/N_1}, \ldots, 0_{M_{i-1}/N_{i-1}}, x+N_i, 0_{M_{i+1}/N_{i+1}}, \ldots, 0_{M_k/N_k})$, όπου $x\in M_i$, για κάθε $i = 1, 2, \ldots, k$, μπορούμε να γράψουμε

$$M_1\oplus+\cdots+\oplus M_k\Big/_{N_1\oplus+\cdots+\oplus N_k} \cong M_1\Big/_{N_1}\oplus\cdots\oplus M_k\Big/_{N_k},$$

όπου το τυχόν στοιχείο στο δεύτερο μέλος της παραπάνω σχέσης γράφεται

$$(x_1+N_1)+(x_2+N_2)+\cdots+(x_k+N_k)$$

με πρόσθεση $\big((x_1+N_1)+(x_2+N_2)+\cdots+(x_k+N_k)\big)+\big((y_1+N_1)+(y_2+N_2)+\cdots+(y_k+N_k)\big) = (x_1+y_1+N_1)+(x_2+y_2+N_2)+\cdots+(x_k+y_k+N_k)$ και βαθμωτό πολλαπλασιασμό $r\cdot\big((x_1+N_1)+(x_2+N_2)+\cdots+(x_k+N_k)\big) = (rx_1+N_1)+(rx_2+N_2)+\cdots+(rx_k+N_k)$, όπου $x_i, y_i\in M_i$, για κάθε $i = 1, 2, \ldots, k$ και $r\in R$.

ΠΟΡΙΣΜΑ 3.30. Έστω $M = M_1\oplus\cdots\oplus M_k$. Τότε, αν $i\in\{1, \ldots, k\}$ ισχύει ότι

$$M\Big/_{M_i} = M_1\oplus\cdots\oplus M_k\Big/_{M_i} \cong M_1\oplus\cdots\oplus M_{i-1}\oplus M_{i+1}\oplus\cdots\oplus M_k$$

ΑΠΟΔΕΙΞΗ: Βάσει του φυσικού ισομορφισμού $M_1\oplus\cdots\oplus M_k\cong M_1\times\cdots\times M_k$, όπου το M_i ταυτίζεται με το $\overline{M}_i = \{0_M\}\times\cdots\times M_i\times\cdots\times\{0_M\}$ και της προηγούμενης πρότασης, έχουμε:

$$M\Big/_{M_i} = M_1\times\cdots\times M_k\Big/_{\overline{M}_i} = M_1\times\cdots\times M_i\times\cdots\times M_k\Big/_{\{0_M\}\times\cdots\times M_i\times\cdots\times\{0_M\}}$$
$$\cong M_1\Big/_{\{0_M\}}\times\cdots\times M_{i-1}\Big/_{\{0_M\}}\times M_i\Big/_{M_i}\times M_{i+1}\Big/_{\{0_M\}}\times\cdots\times M_k\Big/_{\{0_M\}}\cong$$
$$\cong M_1\times\cdots\times M_{i-1}\times\{0_M\}\times M_{i+1}\times\cdots\times M_k\cong M_1\times\cdots\times M_{i-1}\times M_{i+1}\times\cdots\times M_k.$$

Μια πιο φυσιολογική απόδειξη βέβαια, χωρίς να στηρίζεται στην προηγούμενη πρόταση είναι η ακόλουθη: Ορίζουμε την απεικόνιση
$\varphi: M = M_1\oplus\cdots\oplus M_{i-1}\oplus M_i\oplus M_{i+1}\oplus\cdots\oplus M_k \to M_1\oplus\cdots\oplus M_{i-1}\oplus M_{i+1}\oplus\cdots\oplus M_k$ κατά τον προφανή τρόπο: $x_1+\cdots+x_{i-1}+x_i+x_{i+1}+\cdots+x_k \overset{\varphi}{\mapsto} x_1+\cdots+x_{i-1}+x_{i+1}+\cdots+x_k$, όπου $x_i\in M_i$, για κάθε $i = 1, \ldots, k$. Η φ είναι προφανώς R-γραμμική και επί. Πυρήνας της είναι προφανώς το M_i. ■

Χρησιμοποιώντας την πρόταση 3.27 και το γεγονός ότι το ευθύ άθροισμα δεν εξαρτάται από τη σειρά αναγραφής των υποπροτύπων συνάγουμε το ακόλουθο πόρισμα:

ΠΟΡΙΣΜΑ 3.31. Αν $1\le\lambda_1<\lambda_2<\cdots<\lambda_t\le k$, όπου $1\le t\le k$, τότε

$$M_1\oplus M_2\oplus\cdots\oplus M_k\Big/_{M_{\lambda_1}\oplus\cdots\oplus M_{\lambda_t}} \cong \bigoplus_{\substack{j\neq\lambda_i\\ \text{για κάθε } i=1,\ldots,t}} M_j$$

ΑΠΟΔΕΙΞΗ: Επειδή $M_1\oplus M_2\oplus\cdots\oplus M_k = M_{\sigma(1)}\oplus M_{\sigma(2)}\oplus\cdots\oplus M_{\sigma(k)}$ για κάθε μετάθεση σ των δεικτών $1, 2, \ldots, k$ μπορούμε να υποθέσουμε ότι $\lambda_i = i$, για κάθε $i = 1, 2, \ldots, t$. Αρκεί λοιπόν να δείξουμε ότι

$$M_1\oplus M_2\oplus\cdots\oplus M_t\oplus M_{t+1}\oplus\cdots\oplus M_k\Big/_{M_1\oplus\cdots\oplus M_t} \cong M_{t+1}\oplus M_{t+2}\oplus\cdots\oplus M_k$$

Αλλά με βάση την πρόταση 3.27 έχουμε

$$M_1 \oplus M_2 \oplus \cdots \oplus M_k = \big(M_1 \oplus M_2 \oplus \cdots \oplus M_t\big) \bigoplus \big(M_{t+1} \oplus \cdots \oplus M_k\big).$$

Εφαρμόζουμε τώρα το προηγούμενο πόρισμα και παίρνουμε

$$M_1 \oplus M_2 \oplus \cdots \oplus M_t \oplus M_{t+1} \oplus \cdots \oplus M_k \Big/ M_1 \oplus \cdots \oplus M_t =$$

$$= \big(M_1 \oplus M_2 \oplus \cdots \oplus M_t\big) \bigoplus \big(M_{t+1} \oplus \cdots \oplus M_k\big) \Big/ M_1 \oplus M_2 \oplus \cdots \oplus M_t \cong$$

$\cong M_{t+1} \oplus \cdots \oplus M_k$. ■

ΠΡΟΤΑΣΗ 3.32. **(ΚΙΝΕΖΙΚΟ ΘΕΩΡΗΜΑ ΥΠΟΛΟΙΠΩΝ):** Έστω R ένας μοναδιαίος μεταθετικός δακτύλιος και I, J ιδεώδη του. Υποθέτουμε ότι $R = I + J$. Τότε

(i) $I \cap J = IJ$.

(ii) Υπάρχει ισομορφισμός δακτυλίων $R/I \cap J \cong R/I \times R/J$.

(iii) Τα παραπάνω αποτελέσματα γενικεύονται επαγωγικά ως εξής:

Έστω $I_1, I_2, \ldots, I_k$ ιδεώδη του R με $k \geq 2$. Υποθέτουμε ότι $I_i + I_j = R$, για κάθε $i \neq j$. Τότε

α) $I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k$ και

β) $R/I_1 \cap I_2 \cap \cdots \cap I_k \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k$.

ΑΠΟΔΕΙΞΗ: (i) Προφανώς $IJ \subseteq I \cap J$. Έστω τώρα $\alpha \in I \cap J$. Επειδή $I + J = R$, υπάρχουν $x \in I$ και $y \in J$ τέτοια, ώστε $1_R = x + y$. Επομένως $\alpha = 1_R \cdot \alpha = (x + y)\alpha = x\alpha + y\alpha$. Αλλά $x \in I$ και $\alpha \in I \cap J \subseteq J$. Επομένως $x\alpha \in IJ$. Ομοίως, $y \in J$ και $\alpha \in I \cap J \subseteq I$. Επομένως $y\alpha \in JI = IJ$. Συμπεραίνουμε ότι $\alpha = x\alpha + y\alpha \in IJ$.

(ii) Ορίζουμε την απεικόνιση $\varphi : R/I \cap J \to R/I \times R/J$ με

$$\varphi(r + I \cap J) = (r + I, r + J), \text{ για κάθε } r \in R.$$

1) Η φ είναι καλά ορισμένη. Πράγματι, έστω $r + I \cap J = r' + I \cap J \Leftrightarrow r - r' \in I \cap J$. Τότε $r - r' \in I$ και $r - r' \in J$. Άρα $r + I = r' + I$ και $r + J = r' + J$, δηλαδή $(r + I, r + J) = (r' + I, r' + J)$.

2) Είναι σαφές ότι η φ είναι ομομορφισμός μοναδιαίων μεταθετικών δακτυλίων. (Ο δακτύλιος $R/I \times R/J$ είναι το εξωτερικό ευθύ άθροισμα των δακτυλίων R/I και R/J).

3) Έστω $(r + I, s + J) \in R/I \times R/J$. Θέτουμε $r' = yr + xs$, όπου $x + y = 1_R$, όπως προηγουμένως. Τότε $r' + I = yr + xs + I \underset{x \in I}{=} yr + I \underset{x \in I}{=} xr + yr + I = (x + y)r + I = 1_R \cdot r + I = r + I$ και $r' + J = yr + xs + J \underset{y \in J}{=} xs + J \underset{y \in J}{=} xs + ys + J = (x + y)s + J = 1_R \cdot s + J = s + J$. Επομένως $(r + I, s + J) = (r' + I, r' + J) = \varphi(r' + I \cap J)$. Επομένως η φ είναι επιμορφισμός.

4) Έστω $r + I \cap J \in \text{Ker}\varphi$. Ισοδύναμα $(r + I, r + I) = (0_{R/I}, 0_{R/J}) = (I, J)$. Ισοδύναμα $r + I = I \Leftrightarrow r \in I$ και $r + J = J \Leftrightarrow r \in J$, δηλαδή $r \in I \cap J \Leftrightarrow r + I \cap J = 0_{R/I \cap J}$. Άρα η φ είναι μονομορφισμός.

(iii) Υποθέτουμε ότι τα αποτελέσματα ισχύουν για $k \geq 2$ ιδεώδη. Έστω λοιπόν $I_1, I_2, \ldots, I_k, I_{k+1}$ ιδεώδη με $I_i + I_j = R$, για κάθε $i \neq j$. Αποδεικνύουμε πρώτα επαγωγικά ότι αν $\alpha_1, \alpha_2, \ldots, \alpha_n \in \in I$, όπου I ιδεώδες του R, τότε $(1 - \alpha_1)(1 - \alpha_2) \cdots (1 - \alpha_n) = 1 - \beta$, όπου $\beta \in I$. Για $n = 1$ είναι προφανές. Έστω ότι $(1 - \alpha_1)(1 - \alpha_2) \cdots (1 - \alpha_n) = 1 - \beta$, για κάποιο $\beta \in I$. Τότε $(1 - \alpha_1)(1 - \alpha_2) \cdots (1 - \alpha_n)(1 - \alpha_{n+1}) = (1 - \beta)(1 - \alpha_{n+1}) = 1 - (\beta + \alpha_{n+1} - \beta\alpha_{n+1})$, όπου προφανώς $\beta' = \beta + \alpha_{n+1} - \beta\alpha_{n+1} \in I$.

Τώρα, από κάθε σχέση της μορφής $I_i + I_{k+1} = R$, για $i = 1, 2, \ldots, k$ παίρνουμε $x_i + \alpha_i = 1$, όπου $x_i \in I_i$ και $\alpha_i \in I_{k+1}$. Ισοδύναμα, έχουμε τις σχέσεις:

$$x_1 = 1 - \alpha_1$$
$$x_2 = 1 - \alpha_2$$
$$\vdots$$
$$x_k = 1 - \alpha_k$$

Πολλαπλασιάζοντας κατά μέλη και με βάση την προηγούμενη επαγωγική απόδειξη συνάγουμε ότι $x_1x_2\cdots x_k = 1-\beta$, όπου $\beta \in I_{k+1}$. Αλλά $x_1x_2\cdots x_k \in I_1I_2\cdots I_k = I_1 \cap I_2 \cap \cdots \cap I_k$, βάσει της επαγωγικής υπόθεσης. Επειδή $x_1x_2\cdots x_k + \beta = 1$, έπεται ότι $I_1 \cap \cdots \cap I_k \cap I_{k+1} = = (I_1 \cap \cdots \cap I_k) \cap I_{k+1} = (I_1 \cdots I_k) \cap I_{k+1} = (I_1 \cdots I_k)I_{k+1} = I_1 \cdots I_kI_{k+1}$ και υπάρχει ισομορφισμός δακτυλίων

$$R\Big/_{I_1 \cap \cdots \cap I_k \cap I_{k+1}} \cong R\Big/_{I_1 \cap \cdots \cap I_k} \times R\Big/_{I_{k+1}} \underset{\substack{\text{επαγωγική}\\ \text{υπόθεση}}}{\cong} R\Big/_{I_1} \times \cdots \times R\Big/_{I_k} \times R\Big/_{I_{k+1}}.$$

■

Η παραπάνω γενικευμένη μορφή του κινεζικού θεωρήματος υπολοίπων είναι προφανώς εμπνευσμένη από την κλασική μορφή του θεωρήματος στη στοιχειώδη Θεωρία Αριθμών. Εκεί δουλεύουμε στο $\mathbb{Z}$ που είναι ευκλείδειος περιοχή, άρα περιοχή κυρίων ιδεωδών. Δύο θετικοί ακέραιοι $m, n \in \mathbb{Z}$ είναι πρώτοι μεταξύ τους αν και μόνον αν υπάρχουν ακέραιοι x, y τέτοιοι, ώστε $mx + ny = 1$. Αυτό είναι ισοδύναμο με το να πούμε ότι το άθροισμα των ιδεωδών (m) και (n) ισούται με $\mathbb{Z}$. Το ότι το σύστημα

$$\begin{cases} x \equiv \alpha_1 \mod m_1 \\ x \equiv \alpha_2 \mod m_2 \\ \quad \vdots \\ x_k \equiv \alpha_k \mod m_k \end{cases}$$

έχει μοναδική λύση modulo $m_1m_2\cdots m_k$, όπου $(m_i, m_j) = 1 \Leftrightarrow (m_i) + (m_j) = \mathbb{Z}$, για κάθε $i \neq j$ και για κάθε k-άδα ακεραίων $\alpha_1, \alpha_2, \ldots, \alpha_k$ σημαίνει ότι υπάρχει ισομορφισμός

$$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k} = \mathbb{Z}\Big/_{m_1\mathbb{Z}} \times \mathbb{Z}\Big/_{m_2\mathbb{Z}} \times \cdots \times \mathbb{Z}\Big/_{m_k\mathbb{Z}} \cong \mathbb{Z}\Big/_{m_1\mathbb{Z} \cap m_2\mathbb{Z} \cap \cdots \cap m_k\mathbb{Z}} =$$
$$= \mathbb{Z}\Big/_{(m_1)(m_2)\cdots(m_k)} = \mathbb{Z}_{m_1m_2\cdots m_k}.$$

ΟΡΙΣΜΟΣ 3.33. Έστω I ιδεώδες ενός μοναδιαίου μεταθετικού δακτυλίου και M ένα R-πρότυπο. Το IM είναι το υποπρότυπο του M που παράγεται από όλα τα στοιχεία sx, όπου $s \in I$ και $x \in M$.

ΠΡΟΤΑΣΗ 3.34. Έστω I ιδεώδες ενός μοναδιαίου μεταθετικού δακτυλίου και M ένα R-πρότυπο. Το IM αποτελείται από όλους τους πεπερασμένους γραμμικούς συνδυασμούς της μορφής $\sum_{i=1}^{n} s_ix_i$, όπου n θετικός ακέραιος και $s_i \in I$ και $x_i \in M$, για κάθε $i = 1, \ldots, n$.
ΑΠΟΔΕΙΞΗ: Αρκεί να επαληθεύσουμε ότι το άθροισμα $\sum_{i=1}^{m} r_ix_i + \sum_{j=1}^{n} s_jy_j = \sum_{i=1}^{m+n} r'_ix'_i$, όπου $r'_i = r_i \in I$, $x'_i = x_i \in M$, για κάθε $i = 1, \ldots, m$ και $r'_{i+1} = s_i \in I$ και $x'_{i+1} = y_i \in M$, για κάθε $i = 1, \ldots, n$ και το γινόμενο $r \cdot \sum_{i=1}^{m} r_ix_i = \sum_{i=1}^{m}(rr_i)x_i$, όπου $r \in R$ και $r_i \in I$, για κάθε $i = 1, \ldots, m$ είναι τέτοιοι γραμμικοί συνδυασμοί, το οποίο όπως δείξαμε ισχύει. ■

ΠΡΟΤΑΣΗ 3.35. (i) Έστω I γνήσιο ιδεώδες ενός μοναδιαίου μεταθετικού δακτυλίου και M ένα R-πρότυπο. Το R-πρότυπο πηλίκο $M/_{IM}$ γίνεται κατά τον προφανή τρόπο ένα $R/_I$-πρότυπο. Ιδιαιτέρως, **αν το I είναι μέγιστο ιδεώδες του R, τότε το $M/_{IM}$ είναι ένας**

R/I **-διανυσματικός χώρος**. (Βλέπε πρόταση 1.26).
(ii) Αν M, N είναι R-πρότυπα, I ένα γνήσιο ιδεώδες του R και $f : M \to N$ ένας R-ομομορφισμός, τότε ο f επάγεται έναν R/I -ομομορφισμό $\bar{f} : M/IM \to N/IN$ με
$$\bar{f}(x + IM) = f(x) + IN, \text{ για κάθε } x \in M.$$
Ιδιαιτέρως, αν ο f είναι R-επιμορφισμός, τότε και ο $\bar{f}$ είναι R/I -επιμορφισμός. Αν ο f είναι R-ισομορφισμός, τότε και ο $\bar{f}$ είναι R/I -ισομορφισμός.
ΑΠΟΔΕΙΞΗ: (i) Η πρόσθεση στο M/IM είναι καλά ορισμένη. Όσον αφορά τον βαθμωτό πολλαπλασιασμό, ορίζουμε $(r+I)(x+IM) = rx+IM$. Ο βαθμωτός πολλαπλασιασμός είναι καλά ορισμένος, αφού αν $r + I = r' + I \Leftrightarrow r - r' \in I$ και $x + IM = x' + IM \Leftrightarrow x - x' \in IM$, τότε $rx - r'x' = \underbrace{(r - r')}_{\in I}x + r'(x - x') \in IM + (RI)M \subseteq IM + IM \subseteq IM$.
1) $(r + I)\big((x + IM) + (y + IM)\big) = (r + I)(x + y + IM) = r(x + y) + IM = rx + ry + IM =$
$= (rx + IM) + (ry + IM) = (r + I)(x + IM) + (r + I)(y + IM)$,
2) $\big((r + I) + (r' + I)\big)(x + IM) = (r + r' + I)(x + IM) = (r + r')x + IM = rx + r'x + IM =$
$= (rx + IM) + (r'x + IM) = (r + I)(x + IM) + (r' + I)(x + IM)$,
3) $(r_1 + I)\big((r_2 + I)(x + IM)\big) = (r_1 + I)(r_2x + IM) = r_1(r_2x) + IM = (r_1r_2)x + IM =$
$= (r_1r_2 + I)(x + IM) = \big((r_1 + I)(r_2 + I)\big)(x + IM)$ και
4) $(1_R + I)(x + IM) = 1_R \cdot x + IM = x + IM$.
(ii) Έστω $x + IM = x' + IM \Leftrightarrow x - x' \in IM$. Τότε $f(x) - f(x') = f(x - x') \in f(IM) \subseteq$
$\subseteq If(M) \subseteq IN$. Επομένως $f(x) + IN = f(x') + IN$. Άρα η $\bar{f}$ είναι καλά ορισμένη.
1) $\bar{f}\big((x + IM) + (y + IM)\big) = \bar{f}((x + y) + IM) = f(x + y) + IN = f(x) + f(y) + IN =$
$= (f(x) + IN) + (f(y) + IN) = \bar{f}(x + IM) + \bar{f}(y + IM)$,
2) $\bar{f}\big((r + I)(x + IM)\big) = \bar{f}(rx + IM) = f(rx) + IN = rf(x) + IN = (r + I)\big(f(x) + IN\big) =$
$= (r + I)\bar{f}(x + IM)$. Επομένως η $\bar{f}$ είναι R/I -ομομορφισμός.
Έστω ότι η $f : M \to N$ είναι επιμορφισμός. Αν $y + IN \in N/IN$, τότε $y = f(x)$, για κάποιο $x \in M$. Επομένως $y + IN = f(x) + IN = \bar{f}(x + IM)$ και η $\bar{f}$ είναι επί.
Έστω ότι η f είναι R-ισομορφισμός. Τότε η f είναι επί. Υποθέτουμε ότι $x + IM \in \text{Ker}\bar{f}$. Τότε $f(x) \in IN$ και συνεπώς $f(x) = \sum_{i=1}^{k} s_iy_i$, όπου $s_i \in I$ και $y_i \in N$, για κάθε $i = 1, \ldots, k$. Εφόσον η f είναι επί, υπάρχουν $x_1, \ldots, x_k \in M$ τέτοια, ώστε $y_i = f(x_i)$, για κάθε $i = 1, \ldots, k$. Προφανώς $\sum_{i=1}^{k} s_ix_i \in IM$. Επομένως $f(x - \sum_{i=1}^{k} s_ix_i) = f(x) - \sum_{i=1}^{k} s_if(x_i) = \sum_{i=1}^{k} s_iy_i -$
$- \sum_{i=1}^{k} s_iy_i = 0_N$. Επειδή η f είναι R-ισομορφισμός, έπεται ότι $x = \sum_{i=1}^{k} s_ix_i \in IM \Leftrightarrow$
$\Leftrightarrow x + IM = IM = 0_{M/IM}$. ■

3.5 Ελεύθερα Πρότυπα

ΟΡΙΣΜΟΣ 3.36. Έστω M ένα R-πρότυπο και $x \in M$. **Ο μηδενιστής $Ann_R(x)$ του x** είναι το υποσύνολο του R που μηδενίζει το x, δηλαδή
$$Ann_R(x) = \{r \in R \mid rx = 0_M\}.$$
Γενικότερα, **ο μηδενιστής (*annihilator*) $Ann_R(X)$ ενός μη κενού υποσυνόλου X του M** είναι το σύνολο
$$Ann_R(X) = \{r \in R \mid rx = 0_M, \text{ για κάθε } x \in X\}.$$
Αν $X = M$, τότε μιλάμε για τον μηδενιστή $Ann_R(M)$ όλου του προτύπου M.

Είναι σαφές ότι $Ann_R(X) = \bigcap_{x \in X} Ann_R(x)$. Όταν ο δακτύλιος R είναι δεδομένος, μπορούμε

να γράφουμε απλά $Ann(X)$ αντί $Ann_R(X)$.

ΠΡΟΤΑΣΗ 3.37. Ο μηδενιστής $Ann(X)$ ενός μη κενού υποσυνόλου X του M είναι ιδεώδες του R.
ΑΠΟΔΕΙΞΗ: Έστω $r_1, r_2 \in Ann(X)$, δηλαδή $r_1x = r_2x = 0_M$, για κάθε $x \in X$. Τότε $(r_1+r_2)x = = r_1x + r_2x = 0_M + 0_M = 0_M$, για κάθε $x \in X$, ήτοι $r_1 + r_2 \in Ann(X)$.
Τώρα, αν $r \in Ann(X)$ και $r' \in R$, τότε $(r'r)x = r'(rx) = r'0_M = 0_M$, για κάθε $x \in X$, δηλαδή $r'r \in Ann(X)$. ■

Υπενθυμίζουμε ότι ένα R-πρότυπο λέγεται κυκλικό αν παράγεται από ένα στοιχείο του x και συμβολίζεται με Rx ή (x). (Βλέπε ορισμό 3.7). Αν (x) ένα κυκλικό R-πρότυπο, τότε είναι σαφές ότι η απεικόνιση $g : R \to (x) = Rx$ με $g(r) = rx$ είναι R-επιμορφισμός με πυρήνα τον μηδενιστή $Ann(x)$ του x. Από το 1ο θεώρημα ισομορφισμών προκύπτει ότι $(x) \cong {}^{R}\!\Big/_{Ann(x)}$.

ΠΡΟΤΑΣΗ 3.38. Δύο κυκλικά πρότυπα (x) και (y) είναι ισόμορφα αν και μόνον αν
$$Ann(x) = Ann(y).$$
ΑΠΟΔΕΙΞΗ: Σύμφωνα με τα παραπάνω, αρκεί να δείξουμε ότι ${}^{R}\!\Big/_{I} \cong {}^{R}\!\Big/_{J}$ (ως R-πρότυπα), για δύο ιδεώδη I και J του R, αν και μόνον αν $I = J$.
Έστω λοιπόν ότι ${}^{R}\!\Big/_{I} \cong {}^{R}\!\Big/_{J}$. (Το αντίστροφο είναι προφανές). Έστω επίσης
$$\varphi : {}^{R}\!\Big/_{I} \to {}^{R}\!\Big/_{J}$$
ο αντίστοιχος R-ισομορφισμός. Υποθέτουμε ότι $r \notin I \Leftrightarrow r + I \neq 0_{R/I}$. Τότε και $\varphi(r + I) \neq \neq 0_{R/J} = J$. Αν $\varphi(1_R + I) = s + J$, τότε $\varphi(r + I) = \varphi(r(1_R + I)) = r\varphi(1_R + I) = rs + J$. Αν $r \in J$, τότε $rs \in J \Leftrightarrow rs + J = 0_{R/J} = J$, δηλαδή $\varphi(r + I) = 0_{R/J}$, αντίφαση. Επομένως $r \notin J$. Παρόμοια, μέσω της $\varphi^{-1} : {}^{R}\!\Big/_{J} \to {}^{R}\!\Big/_{I}$ προκύπτει ότι αν $r \notin J$, τότε και $r \notin I$. ■

ΟΡΙΣΜΟΣ 3.39. Έστω M ένα R-πρότυπο και $X \subseteq M$. Το X λέγεται ***R*-γραμμικώς εξαρτημένο (απλά γραμμικά εξαρτημένο)** αν υπάρχουν πεπερασμένα το πλήθος στοιχεία του $x_1, x_2, \ldots, x_k$, διαφορετικά ανά δύο, όπου k θετικός ακέραιος και $r_1, r_2, \ldots, r_k \in R$, **όχι όλα μηδέν**, τέτοια ώστε
$$r_1x_1 + r_2x_2 + \cdots + r_kx_k = 0_M.$$
Σε αντίθετη περίπτωση το X λέγεται **γραμμικώς ανεξάρτητο**.

ΠΑΡΑΤΗΡΗΣΕΙΣ: 1) ΠΡΟΣΟΧΗ! Με βάση τον προηγούμενο ορισμό, **το ∅ είναι γραμμικώς ανεξάρτητο**. Αν δεν ήταν, **θα υπήρχαν (;)** $x_1, \ldots, x_k \in \varnothing$ και $r_1, r_2, \ldots, r_k \in R$ τέτοια, ώστε... **Υπάρχουν $x_1, \ldots, x_k \in \varnothing$;** Προφανώς όχι. Το $\varnothing$ είναι λοιπόν γραμμικώς ανεξάρτητο, ενώ το $\{0_M\}$, επίσης προφανώς, δεν είναι.
2) Από τον ορισμό προκύπτει ότι αν $X = \{x_1, x_2, \ldots, x_k\} \neq \varnothing$ είναι ένα μη κενό πεπερασμένο γραμμικώς ανεξάρτητο σύνολο (με $x_i \neq x_j$, για $i \neq j$), τότε από κάθε σχέση της μορφής
$$\boldsymbol{r_1x_1 + r_2x_2 + \cdots + r_kx_k = 0_M}$$
συνάγουμε ότι $\boldsymbol{r_1 = r_2 = \cdots = r_k = 0_R}$. Τότε τα στοιχεία του $x_1, x_2, \ldots, x_k$ λέγονται R-γραμμικώς ανεξάρτητα ή απλά γραμμικώς ανεξάρτητα.

Εμείς θα ασχοληθούμε με πεπερασμένα παραγόμενα R-πρότυπα. (Βλέπε ορισμό 3.7).

ΠΡΟΤΑΣΗ 3.40. Έστω M ένα R-πρότυπο και $\{e_1, e_2, \ldots, e_k\}$ ένα μη κενό υποσύνολο του M με k ακριβώς στοιχεία, όπου k θετικός ακέραιος. (Δηλαδή $e_i \neq e_j$, για $i \neq j$). Τα επόμενα είναι

ισοδύναμα:
(i) Τα $e_1, e_2, \ldots, e_k$ είναι γραμμικώς ανεξάρτητα και παράγουν το M.
(ii) $M = (e_1) \oplus (e_2) \oplus \cdots (e_k)$ και $Ann(e_i) = \{0_R\}$, για κάθε $i = 1, 2, \ldots, k$.
(iii) Για κάθε $x \in M$ υπάρχουν **μοναδικά** $r_1, r_2, \ldots, r_k \in R$ τέτοια, ώστε

$$x = r_1e_1 + r_2e_2 + \cdots + r_ke_k.$$

ΑΠΟΔΕΙΞΗ: (i) ⇒ (ii) Προφανώς $M = \sum_{i=1}^{k}(e_i) = \sum_{i=1}^{k} Re_i$, από την υπόθεση.
Έστω $y \in (e_i) \bigcap \sum_{j\neq i}(e_j)$. Τότε $y \in (e_i) \Leftrightarrow y = re_i$, για κάποιο $r \in R$. Από την άλλη μεριά, $y \in \bigcap \sum_{j\neq i}(e_j) \Rightarrow y = \sum_{j\neq i} r_je_j$, για κάποια $r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_k \in R$. Επομένως έχουμε τη σχέση

$$re_i = r_1e_1 + \cdots + r_{i-1}e_{i-1} + r_{i+1}e_{i+1} + \cdots + r_ke_k \Leftrightarrow$$
$$r_1e_1 + \cdots + r_{i-1}e_{i-1} + \boldsymbol{(-r)e_i} + r_{i+1}e_{i+1} + \cdots + r_ke_k = 0_M.$$

Επειδή τα $e_1, e_2, \ldots, e_k$ είναι γραμμικώς ανεξάρτητα θα έχουμε $r_1 = \cdots = r_{i-1} = -r = r_{i+1} = = \cdots = r_k = 0_R$. Αλλά $-r = 0_R \Leftrightarrow r = 0_R \Rightarrow y = re_i = 0_Re_i = 0_M$.
Τώρα, αν $r \in Ann(e_i) \Leftrightarrow re_i = 0_M$, τότε $0_M = 0_Re_1 + \cdots + 0_Re_{i-1} + \boldsymbol{re_i} + 0_Re_{i+1} + \cdots + 0_Re_k$ και από τη γραμμική ανεξαρτησία των $e_1, \ldots, e_k$ προκύπτει ότι $r = 0_R$.
(ii) ⇒ (iii) Έστω $x \in M = Re_1 \oplus Re_2 \oplus \cdots \oplus Re_k$. Τότε $x = r_1e_1 + r_2e_2 + \cdots + r_ke_k$, για κάποια $r_1, r_2, \ldots, r_k \in R$. Έστω ότι $x = s_1e_1 + s_2e_2 + \cdots + s_ke_k$, για κάποια $s_1, s_2, \ldots, s_k \in R$. Θα δείξουμε ότι $s_i = r_i$, για κάθε $i = 1, 2, \ldots, k$. Προφανώς έχουμε
$(r_1 - s_1)e_1 + \cdots + (r_{i-1} - s_{i-1})e_{i-1} + (r_i - s_i)e_i + (r_{i+1} - s_{i+1})e_{i+1} + \cdots + (r_k - s_k)e_k = 0_M \Leftrightarrow$
$\Leftrightarrow (s_i - r_i)e_i = (r_1 - s_1)e_1 + \cdots + (r_{i-1} - s_{i-1})e_{i-1} + (r_{i+1} - s_{i+1})e_{i+1} + \cdots + (r_k - s_k)e_k \in$
$\in (e_i) \bigcap \sum_{j\neq i}(e_j) = \{0_M\}$, γιατί το άθροισμα $\sum_{t=1}^{k}(e_t)$ είναι ευθύ. Συνεπώς $s_i - r_i \in Ann(e_i) =$
$= \{0_R\} \Leftrightarrow s_i = r_i$.
(iii) ⇒ (i) Εφόσον κάθε στοιχείο του M γράφεται στη μορφή $r_1e_1 + r_2e_2 + \cdots + r_ke_k$, όπου $r_i \in R$, για κάθε $i = 1, 2, \ldots, k$, τα $e_1, e_2, \ldots, e_k$ παράγουν το M.
Αν $r_1e_1 + r_2e_2 + \cdots + r_ke_k = 0_M = 0_R \cdot e_1 + 0_R \cdot e_2 + \cdots + 0_R \cdot e_k$, τότε από τη **μοναδικότητα** των συντελεστών r_i προκύπτει ότι $r_i = 0_R$, για κάθε $i = 1, 2, \ldots, k$. ■

ΟΡΙΣΜΟΣ 3.41. Έστω M ένα R-πρότυπο και $e_1, e_2, \ldots, e_k$ (k θετικός ακέραιος) στοιχεία του M που πληρούν τις ισοδύναμες συνθήκες της προηγούμενης πρότασης. Τότε το M λέγεται **ελεύθερο R-πρότυπο με βάση το σύνολο $\{e_1, e_2, \ldots, e_k\}$**. **Το τετριμμένο-μηδενικό πρότυπο θεωρείται ελεύθερο με βάση το κενό σύνολο**. Συνήθως ένα ελεύθερο R-πρότυπο συμβολίζεται με το γράμμα F, ίσως από τη λέξη «free».

ΠΡΟΤΑΣΗ 3.42. Ένα ελεύθερο R-πρότυπο F με βάση $\{e'_1, e'_2, \ldots, e'_k\}$ είναι ισόμορφο με το $R^k = \{(r_1, r_2, \ldots, r_k) \mid r_i \in R, \text{ για κάθε } i = 1, 2, \ldots, k\}$.
ΑΠΟΔΕΙΞΗ: Έστω $\varphi : R^k \to F$ με $\varphi(r_1, r_2, \ldots, r_k) = r_1e'_1 + r_2e'_2 + \cdots + r_ke'_k$. Η φ είναι προφανώς R-γραμμική και επί, αφού κάθε στοιχείο του F γράφεται (κατά μοναδικό τρόπο) ως R-γραμμικός συνδυασμός των $e'_1, e'_2, \ldots, e'_k$.
Έστω $(r_1, r_2, \ldots, r_k) \in \text{Ker}\varphi$. Τότε $r_1e'_1 + r_2e'_2 + \cdots + r_ke'_k = 0_F$. Επειδή τα $e'_1, e'_2, \ldots, e'_k$ είναι γραμμικά ανεξάρτητα, συμπεραίνουμε ότι $r_1 = r_2 = \cdots = r_k = 0_R \Leftrightarrow (r_1, r_2, \ldots, r_k) = = (0_R, 0_R, \ldots, 0_R) = 0_{R^k}$. ■

Σημειώνουμε ότι $\varphi(e_i) = e'_i$, για κάθε $i = 1, 2, \ldots, k$, όπου $e_1 = (1_R, 0_R, 0_R, \ldots, 0_R)$, $e_2 = = (0_R, 1_R, 0_R, \ldots, 0_R)$,…,$e_k = (0_R, 0_R, 0_R, \ldots, 1_R)$ η συνήθης βάση του R^k.

ΠΟΡΙΣΜΑ 3.43. Έστω F, F' δύο ελεύθερα R-πρότυπα με βάσεις $\{v_1, v_2, \ldots, v_m\}$ και $\{u_1, u_2, , \ldots, u_n\}$ αντίστοιχα. Τότε $F \cong F'$ αν και μόνον αν $R^m \cong R^n$. ■

ΛΗΜΜΑ 3.44. Έστω m θετικός ακέραιος. Αν I είναι ιδεώδες του R, τότε $IR^m = I^{(m)}$, όπου
$$I^{(m)} = \underbrace{I \times I \times \cdots \times I}_{m \text{ φορές}} = \{(s_1, s_2, \ldots, s_m) \mid s_i \in I, \text{ για κάθε } i = 1, 2, \ldots, m\}.$$
Αν I είναι μέγιστο ιδεώδες του R, $\big($αποδείξαμε ότι υπάρχει τέτοιο μέγιστο ιδεώδες-πρόταση 1.30$\big)$, τότε το $R^m\big/_{IR^m} = R^m\big/_{I^{(m)}}$ καθίσταται $\mathbb{K}$-διανυσματικός χώρος διάστασης m, όπου $\mathbb{K} = R\big/_I$.
ΑΠΟΔΕΙΞΗ: Έστω I ένα ιδεώδες του δακτυλίου R. Θεωρούμε το R-υποπρότυπο IR^m. Το υποπρότυπο αυτό είναι το $I^{(m)} = \{(s_1, s_2, \ldots, s_m) \mid s_i \in I, \text{ για κάθε } i = 1, 2, \ldots, m\}$. Πράγματι, τα στοιχεία του IR^m παράγονται από στοιχεία της μορφής sx, όπου $s \in I$ και $x = (r_1, r_2, \ldots, r_m) \in \in R^m$. Αλλά $sx = s(r_1, r_2, \ldots, r_m) = (sr_1, sr_2, \ldots, sr_m) = (s_1, s_2, \ldots, s_m)$, όπου $s_i = sr_i \in I$, για κάθε $i = 1, 2, \ldots, m$. Επομένως $sx \in I^{(m)}$, για κάθε $s \in I$ και $x \in R^m$ και συνεπώς $IR^m \subseteq I^{(m)}$.
Αντιστρόφως, κάθε στοιχείο $(s_1, s_2, \ldots, s_m) = s_1(1_R, 0_R, 0_R, \ldots, 0_R) + s_2(0_R, 1_R, 0_R, \ldots, 0_R) + + \cdots + s_m(0_R, 0_R, 0_R, \ldots, 1_R)$ του $I^{(m)}$ είναι στοιχείο του IR^m.
Έστω I μέγιστο ιδεώδες του R. Σύμφωνα με την πρόταση 3.35 το πρότυπο-πηλίκο $R^m\big/_{IR^m} = = R^m\big/_{I^{(m)}}$ καθίσταται $\mathbb{K} = R\big/_I$ -διανυσματικός χώρος. Σύμφωνα τώρα με την πρόταση 3.29 υπάρχει R-ισομορφισμός $\overline{\varphi}$
$$R^m\big/_{IR^m} = R^m\big/_{I^{(m)}} = \overbrace{R \times R \times \cdots \times R}^{m \text{ φορές}} \Big/ \underbrace{I \times I \times \cdots \times I}_{m \text{ φορές}} \xrightarrow{\overline{\varphi}} \underbrace{R\big/_I \times R\big/_I \times \cdots \times R\big/_I}_{m \text{ φορές}} =$$
$= \underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{m \text{ φορές}} = \mathbb{K}^m$. Ο $\overline{\varphi}$ είναι στην πραγματικότητα ισομορφισμός $\mathbb{K} = R\big/_I$ -διανυσματικών χώρων. Πράγματι, $\overline{\varphi}\big((r + I)\big((r_1, r_2, \ldots, r_m) + I^{(m)}\big)\big) = \overline{\varphi}\big(r(r_1, r_2, \ldots, r_m) + I^{(m)}\big) = = \overline{\varphi}\big((rr_1, rr_2, \ldots, rr_m) + I^{(m)}\big) = (rr_1 + I, rr_2 + I, \ldots, rr_m + I) = (r + I)(r_1 + I, r_2 + I, \ldots, r_m + I) = = (r + I)\overline{\varphi}\big((r_1, r_2, \ldots, r_m) + I^{(m)}\big)$. ■

Σημείωση: Χρησιμοποιούμε τον συμβολισμό $I^{(m)}$ αντί του I^m για το ιδεώδες $\underbrace{I \times I \cdots \times I}_{m \text{ φορές}}$ του R^m για να μην υπάρξει σύγχυση με το ιδεώδες $\underbrace{I \cdot I \cdots I}_{m \text{ φορές}}$.

ΠΟΡΙΣΜΑ 3.45. Έστω m, n θετικοί ακέραιοι. Τότε $R^m \cong R^n$ αν και μόνον αν $m = n$.
ΑΠΟΔΕΙΞΗ: Αν $m = n$ δεν έχουμε τίποτα να αποδείξουμε. Έστω $R^m \cong R^n$. Από το **(ii)** της πρότασης 3.35 ο ισομορφισμός αυτός επάγεται έναν ισομορφισμό των $\mathbb{K} = R\big/_I$-διανυσματικών χώρων $R^m\big/_{IR^m}$ και $R^n\big/_{IR^n}$, διαστάσεων m και n αντίστοιχα. Επομένως $m = n$. ■

ΠΟΡΙΣΜΑ 3.46. Έστω F ένα ελεύθερο R-πρότυπο με βάση $\{e_1, e_2, \ldots, e_m\}$. Τότε το πλήθος m των στοιχείων της βάσης του είναι σταθερό, δηλαδή ανεξάρτητο από τη συγκεκριμένη βάση.
ΑΠΟΔΕΙΞΗ: Σύμφωνα με την πρόταση 3.42 το F είναι ισόμορφο με το R^m. Αν το F είχε και μια άλλη βάση $\{u_1, u_2, \ldots, u_n\}$ με πλήθος στοιχείων n, τότε θα είχαμε επίσης $F \cong R^n$. Επομένως $R^m \cong F \cong R^n \Rightarrow m = n$. ■

ΟΡΙΣΜΟΣ 3.47. Το πλήθος των στοιχείων της βάσης ενός ελεύθερου R-προτύπου F $\big($η βάση

είναι πεπερασμένο σύνολο) ονομάζεται **βαθμός του F** και συμβολίζεται με **$\mathbf{rank}_R F$** ή απλά με $\mathrm{rank}F$. **Ως βαθμό του μηδενικού προτύπου ορίζουμε το μηδέν**.

ΠΡΟΤΑΣΗ 3.48. Έστω F και F' ελεύθερα R-πρότυπα με $\mathrm{rank}F = m$ και $\mathrm{rank}F' = n$. Τότε το $F \oplus F'$ είναι ελεύθερο με $\mathrm{rank}(F \oplus F') = m + n$.
ΑΠΟΔΕΙΞΗ: Αν κάποιο από τα F, F' είναι μηδενικό, η περίπτωση είναι τετριμμένη. Έστω $\{u_1, u_2, \ldots, u_m\}$ μια βάση του F και $\{v_1, v_2, \ldots, v_n\}$ μια βάση του F'. Θα δείξουμε ότι το σύνολο $\{u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n\}$ είναι μια βάση του $F \oplus F'$. Το ότι τα $u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_n$ παράγουν το $F \oplus F'$ είναι προφανές. Αρκεί να δείξουμε ότι είναι γραμμικά ανεξάρτητα. Έστω λοιπόν $r_1u_1 + r_2u_2 + \cdots + r_mu_m + s_1v_1 + s_2v_2 + \cdots + s_nv_n = 0_{F\oplus F'}$. Τότε $r_1u_1 + r_2u_2 + \cdots + r_mu_m = -(s_1v_1 + s_2v_2 + \cdots + s_nv_n) \in F \cap F' = \{0\}$. Επομένως $r_1u_1 + r_2u_2 + \cdots + r_mu_m = 0$ και $s_1v_1 + s_2v_2 + \cdots + s_nv_n = 0$. Το αποτέλεσμα προκύπτει από τη γραμμική ανεξαρτησία των $u_1, u_2, \ldots, u_m$ και των $v_1, v_2, \ldots, v_n$. ■

Το καίριας σημασίας πόρισμα 3.45 αποδεικνύεται στοιχειωδώς με χρήση πινάκων! Ας δούμε την απόδειξη:

2η ΑΠΟΔΕΙΞΗ ΤΟΥ ΠΟΡΙΣΜΑΤΟΣ 3.45: Υποθέτουμε ότι $R^m \cong R^n$, όπου R μοναδιαίος μεταθετικός δακτύλιος και m, n θετικοί ακέραιοι. Θα αποδείξουμε ότι $m = n$. Υποθέτουμε ότι $m \neq n$. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $m > n$. Έστω $\{e_1 = = (1_R, 0_R, \ldots, 0_R), e_2 = (0_R, 1_R, \ldots, 0_R), \ldots, e_m = (0_R, 0_R, \ldots, 1_R)\}$ και $\{e'_1 = (1_R, 0_R, \ldots, 0_R), e'_2 = (0_R, 1_R, \ldots, 0_R), \ldots, e'_n = (0_R, 0_R, \ldots, 1_R)\}$ οι συνήθεις βάσεις των R^m και R^n αντίστοιχα. Αν $f : R^m \to R^n$ ο ισομορφισμός μεταξύ των R^m και R^n και $f^{-1} : R^n \to R^m$ ο αντίστροφός του, τότε θα έχουμε:

$$f(e_j) = \sum_{i=1}^{n} \alpha_{ij} e'_i$$

και

$$f^{-1}(e'_j) = \sum_{i=1}^{m} \beta_{ij} e_i,$$

όπου $\alpha_{ij} \in R$, για κάθε $j = 1, \ldots, m$ και $i = 1, \ldots, n$ και $\beta_{ij} \in R$, για κάθε $j = 1, \ldots, n$ και $i = 1, \ldots, m$. Επομένως $f^{-1} \circ f = \mathbf{1}_{R^m}$. Δηλαδή $\sum_{s=1}^{n} \beta_{is}\alpha_{sj} = \delta_{ij}$, για κάθε $i, j \in \{1, 2, \ldots, m\}$, όπου δ_{ij} τα δέλτα του Kronecker. Σε πινακική μορφή αυτό γράφεται $BA = I_m$, όπου

$$B = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} \\ \vdots & \vdots & & \vdots \\ \beta_{n1} & \beta_{n2} & \cdots & \beta_{nn} \\ \vdots & \vdots & & \vdots \\ \beta_{m1} & \beta_{m2} & \cdots & \beta_{mn} \end{pmatrix} \text{ και } A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} & \cdots & \alpha_{1m} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} & \cdots & \alpha_{2m} \\ \vdots & \vdots & & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} & \cdots & \alpha_{nm} \end{pmatrix}.$$

Αυτή η σχέση είναι ισοδύναμη με τη σχέση $B'A' = I_m$, όπου οι $m \times m$ πίνακες B' και A' είναι οι ακόλουθοι:

$$B' = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} & \overbrace{0} & \overbrace{0} & \overbrace{\cdots} & \overbrace{0} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \beta_{n1} & \beta_{n2} & \cdots & \beta_{nn} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \beta_{m1} & \beta_{m2} & \cdots & \beta_{mn} & 0 & 0 & \cdots & 0 \end{pmatrix} \overbrace{\quad}^{m-n \text{ στήλες}}$$

και

$$A' = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} & \cdots & \alpha_{1m} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} & \cdots & \alpha_{2m} \\ \vdots & \vdots & & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} & \cdots & \alpha_{nm} \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}\right\} \begin{matrix} m-n \\ \text{γραμμές} \end{matrix}$$

Επειδή $B'A' = I_m$, έπεται ότι οι ορίζουσες $\det(B')$ και $\det(A')$ είναι αντιστρέψιμα στοιχεία του R και επομένως οι πίνακες B' και A' αντιστρέφονται στο R και $B' = A'^{-1}$. Αλλά $\det(A') = \det(B') = 0$, γιατί οι $m-n$ τελευταίες γραμμές του A' και οι $m-n$ τελευταίες στήλες του B' είναι μηδενικές. Άτοπο.

Στη συνέχεια θα ασχοληθούμε με ορισμένα βασικά αποτελέσματα, απαραίτητα για το κεφάλαιο που θα ακολουθήσει.

ΠΡΟΤΑΣΗ 3.49. Κάθε πεπερασμένα παραγόμενο R-πρότυπο είναι επιμορφική εικόνα ενός ελεύθερου προτύπου.

ΑΠΟΔΕΙΞΗ: Έστω $M = \sum_{i=1}^{k} Rm_i$, όπου $m_i \in M$, για κάθε $i = 1, 2, \ldots, k$. Θεωρούμε το ελεύθερο R-πρότυπο $R^k = \underbrace{R \oplus R \oplus \cdots \oplus R}_{k \text{ φορές}}$ με τη συνήθη βάση $\{e_1, e_2, \ldots, e_k\}$. Ορίζουμε τον ομομορφισμό $f : R^k \to M$ με $f(e_i) = m_i$, για κάθε $i = 1, 2, \ldots, k$. Πιο συγκεκριμένα, $f(r_1, r_2, \ldots, r_k) = r_1m_1 + r_2m_2 + \cdots + r_km_k$. Εύκολα μπορεί να δείξει κανείς ότι η f είναι R-ομομορφισμός. Είναι επί γιατί κάθε στοιχείο του M γράφεται στη μορφή $r_1m_1 + r_2m_2 + \cdots + r_km_k = f(r_1, r_2, \ldots, r_k)$, όπου $r_i \in R$, για κάθε $i = 1, 2, \ldots, k$. ■

ΠΡΟΤΑΣΗ 3.50. Έστω $f : M \to F$ επιμορφισμός R-προτύπων, όπου F ελεύθερο βαθμού k. Τότε $M = \text{Ker}f \oplus F'$, όπου F' υποπρότυπο του M, ισόμορφο προς το F.

ΑΠΟΔΕΙΞΗ: Έστω $\{u_1, u_2, \ldots, u_k\}$ μια βάση του F. Επειδή η f είναι επιμορφισμός, υπάρχουν $m_1, m_2, \ldots, m_k \in M$ με $f(m_i) = u_i$, για κάθε $i = 1, 2, \ldots, k$. Έστω $F' \leqslant M$ το υποπρότυπο του M που παράγεται από τα $m_1, m_2, \ldots, m_k$, δηλαδή $F' = \sum_{i=1}^{k} Rm_i$. Με βάση την πρόταση 3.40, για να δείξουμε ότι το F' είναι ελεύθερο, αρκεί να δείξουμε ότι τα $m_1, m_2, \ldots, m_k$ είναι γραμμικώς ανεξάρτητα. Πράγματι, αν $r_1m_1 + r_2m_2 + \cdots + r_km_k = 0_M$, τότε $f(r_1m_1 + r_2m_2 + \cdots + r_km_k) = f(0_M) = 0_F \Leftrightarrow r_1f(m_1) + r_2f(m_2) + \cdots + r_kf(m_k) = 0_F \Leftrightarrow r_1u_1 + r_2u_2 + \cdots + r_ku_k = 0_F$ και επειδή τα $u_1, u_2, \ldots, u_k$ αποτελούν βάση του ελεύθερου προτύπου F, έπεται ότι $r_1 = r_2 = \cdots = r_k = 0_R$.

Έστω $x \in M$. Τότε $f(x) = \sum_{i=1}^{k} r_iu_i \in F$, για κάποια $r_1, r_2, \ldots, r_k \in R$. Αλλά $\sum_{i=1}^{k} r_iu_i = \sum_{i=1}^{k} r_if(m_i) = f(\sum_{i=1}^{k} r_im_i)$. Θέτουμε $y = \sum_{i=1}^{k} r_im_i \in F'$. Τότε $f(x) = f(y) \Leftrightarrow x - y \in \text{Ker}f$. Επομένως $x = (x - y) + y \in \text{Ker}f + F'$.

Απομένει να δείξουμε ότι $\text{Ker}f \cap F' = \{0_M\}$. Έστω λοιπόν $y = \sum_{i=1}^{k} r_im_i \in \text{Ker}f \cap F'$. Τότε $0_F = f(y) = \sum_{i=1}^{k} r_if(m_i) = \sum_{i=1}^{k} r_iu_i$ και επειδή τα $u_1, u_2, \ldots, u_k$ είναι γραμμικώς ανεξάρτητα, παίρνουμε $r_1 = r_2 = \cdots = r_k = 0_R$. Επομένως $y = \sum_{i=1}^{k} r_im_i = 0_M$. ■

Το επόμενο αποτέλεσμα αφορά περιοχές κυρίων ιδεωδών με τις οποίες θα ασχοληθούμε στο επόμενο κεφάλαιο.

ΠΡΟΤΑΣΗ 3.51. Έστω R περιοχή κυρίων ιδεωδών και F ένα ελεύθερο R-πρότυπο, με $\text{rank}_R F =$

$= k$. Τότε κάθε υποπρότυπο F' του F είναι ελεύθερο με rank$F' \leq$ rank$F$.
ΑΠΟΔΕΙΞΗ: Η περίπτωση $F = \{0\}$ είναι τετριμμένη. Έστω rank$F = 1$. Τότε $F = Ru$ με $Ann(u) = \{0_R\}$. Έστω I $= \{r \in R \mid ru \in F'\}$. Εύκολα μπορεί να δείξει κανείς ότι το I είναι ιδεώδες του R. Επειδή η R είναι περιοχή κυρίων ιδεωδών, I $= (\delta)$, για κάποιο $\delta \in R$. Αν $\delta = 0$, τότε $F' =$ I$u = (0_R)u = \{0_F\}$ και rank$\{0_F\} = 0 < 1 =$ rank$F$. Αν $\delta \neq 0_R$, τότε $F' = (\delta)u = R(\delta u)$. Επίσης $\delta u \neq 0_F$, γιατί το $\{u\}$ είναι γραμμικά ανεξάρτητο. Έστω $w = \delta u$.
Ορίζουμε την απεικόνιση $f : F = Ru \to F' = Rw = R(\delta u)$ με $f(ru) = rw$. Η f είναι R-γραμμική και μάλιστα επιμορφισμός, από τον ορισμό του δ. Αν τώρα $r \in$ Ker$f$, τότε $rw = r(\delta u) = (r\delta)u = 0_F$ και επειδή το $\{u\}$ είναι γραμμικώς ανεξάρτητο, $r\delta = 0_R$. Αλλά η R είναι ακέραια περιοχή και $\delta \neq 0_R$, οπότε $r = 0_R \Rightarrow ru = 0_F$. Επομένως Ker$f = \{0_F\}$ και κατά συνέπεια $F \cong F'$. Συνεπώς το F' είναι ελεύθερο βαθμού 1.
Υποθέτουμε ότι κάθε υποπρότυπο F' ενός ελεύθερου προτύπου F βαθμού $< k$, όπου k θετικός ακέραιος, είναι ελεύθερο με rank$F' \leq$ rank$F$. Υποθέτουμε τώρα ότι $F' \leqslant F$, όπου F ελεύθερο με rank$F = k$. Επίσης, μπορούμε να υποθέσουμε ότι $k \geq 2$, γιατί για την περίπτωση $k = 1$ δείχθηκε προηγουμένως. Έστω λοιπόν $\{u_1, u_2, \ldots, u_k\}$ μια βάση του F. Έστω $F_1 = Ru_2 \oplus Ru_3 \oplus \cdots \oplus Ru_k$. Το F_1 είναι ελεύθερο βαθμού $k-1$. Με βάση την επαγωγική υπόθεση, το $F' \cap F_1$ είναι ελεύθερο βαθμού $\leq k-1$.
Ορίζουμε τώρα την απεικόνιση $\varphi : F' \to Ru_1$ ως εξής: Κάθε στοιχείο του F', ως στοιχείο του F, γράφεται μονοσήμαντα στη μορφή $r_1u_1 + r_2u_2 + \cdots + r_ku_k$. Θέτουμε $\varphi(r_1u_1 + r_2u_2 + \cdots + r_ku_k) = = r_1u_1 \in Ru_1$. Εύκολα δείχνει κανείς ότι η φ είναι R-γραμμική. Αν Im$\varphi = \{0_F\}$, τότε λόγω του ότι $Ann(u_1) = \{0_R\}$, έπεται ότι $F' \leqslant F_1$, ήτοι $F' = F' \cap F_1$ ελεύθερο βαθμού $\leq k-1$.
Αν Im$\varphi \neq \{0_F\}$, τότε επειδή το Ru_1 είναι ελεύθερο βαθμού 1, και το Imφ θα είναι ελεύθερο βαθμού 1, όπως δείξαμε στην περίπτωση $k = 1$. Άρα η φ επάγεται έναν R-**επιμορφισμό** $\overline{\varphi} : F' \to$ Imφ. Επειδή το Imφ είναι ελεύθερο, σύμφωνα με την προηγούμενη πρόταση υπάρχει υποπρότυπο $\overline{F} \cong$ Imφ $\big($άρα rank$\overline{F} = 1\big)$ του F' τέτοιο, ώστε $F' = \overline{F} \oplus$ Ker$\overline{\varphi}$. Τώρα Ker$\overline{\varphi} = F' \cap F_1$. Επομένως το F' είναι ελεύθερο, ως ευθύ άθροισμα ελεύθερων υποπροτύπων και rank$F' =$ rank(Im$\overline{\varphi}$) + rank$(F' \cap F_1) \leq 1 + k - 1 = k =$ rank$F$. ■

ΠΟΡΙΣΜΑ 3.52. Έστω R περιοχή κυρίων ιδεωδών. Αν M είναι ένα πεπερασμένα παραγόμενο πρότυπο, τότε και κάθε υποπρότυπό του είναι πεπερασμένα παραγόμενο.
ΑΠΟΔΕΙΞΗ: Έστω $f : F \to M$ ένας R-επιμορφισμός, όπου F ελεύθερο με rank$F = k$ θετικός ακέραιος. $\big($Πρόταση 3.49$\big)$. Αν $N \leqslant M$, τότε το $f^{-1}(N)$ είναι υποπρότυπο του ελεύθερου προτύπου F, άρα βάσει της προηγούμενης πρότασης είναι ελεύθερο με rank$f^{-1}(N) \leq k$. Επειδή η f είναι επιμορφισμός, $N = f(f^{-1}(N))$, δηλαδή επιμορφική εικόνα ενός πεπερασμένα παραγόμενου προτύπου. Άρα πεπερασμένα παραγόμενο. ■

Ως πόρισμα παίρνουμε επίσης το ακόλουθο θεμελιώδες θεώρημα:

ΘΕΩΡΗΜΑ 3.53. Κάθε πεπερασμένα παραγόμενο πρότυπο επί μιας περιοχής κυρίων ιδεωδών είναι ισόμορφο με το πηλίκο δύο $\big($πεπερασμένα παραγόμενων$\big)$ ελεύθερων προτύπων.
ΑΠΟΔΕΙΞΗ: Έστω M πεπερασμένα παραγόμενο R-πρότυπο, όπου R περιοχή κυρίων ιδεωδών. Ξέρουμε $\big($πρόταση 3.49$\big)$ ότι το M είναι επιμορφική εικόνα ενός ελεύθερου προτύπου F. Έστω $\varphi : F \to M$ ο επιμορφισμός αυτός. Τότε $M \cong {}^{F}\!/_{\text{Ker}\varphi}$. Από την πρόταση 3.51 το Ker$\varphi = = F'$ είναι ελεύθερο με rank$F' \leq$ rank$F$. Επομένως το M είναι ισόμορφο με το πηλίκο δύο ελεύθερων R-προτύπων. ■

3.6 Γραμμικές Απεικονίσεις Ελεύθερων Προτύπων και Πίνακες

Ας θυμηθούμε κάποια πράγματα από τη Γραμμική Άλγεβρα. Υπενθυμίζουμε ότι για συντομία πολλές φορές θα γράφουμε $\bigoplus_{i=1}^{n} M_i$ αντί $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

ΠΡΟΤΑΣΗ 3.54. Έστω R μοναδιαίος μεταθετικός δακτύλιος.
(i) Έστω $F = Ru_1 \oplus Ru_2 \oplus \cdots \oplus Ru_m$ και $F' = Rv_1 \oplus Rv_2 \oplus \cdots \oplus Rv_n$ δύο ελεύθερα R-πρότυπα με διατεταγμένες βάσεις $\hat{u} = (u_1, u_2, \ldots, u_m)$ και $\hat{v} = (v_1, v_2, \ldots, v_n)$ αντίστοιχα. Τότε υπάρχει μια αμφιμονοσήμαντη αντιστοιχία $\big($1-1 και επί$\big)$
$$\mathrm{Hom}_R(F, F') \longleftrightarrow R^{n\times m},$$
ανάμεσα στο σύνολο $\mathrm{Hom}_R(F, F')$ των R-γραμμικών απεικονίσεων $f : F \to F'$ και των πινάκων $A = (\alpha_{ij}) \in R^{n\times m}$, $\big(n$ γραμμές και m στήλες$\big)$ βάσει του τύπου
$$f(u_j) = \sum_{i=1}^{n} \alpha_{ij} v_i,$$
για κάθε $j = 1, 2, \ldots, m$. Ο πίνακας A που αντιστοιχεί στην απεικόνιση f, βάσει της παραπάνω αντιστοιχίας, θα συμβολίζεται με $(f \mid \hat{u}, \hat{v})$.
(ii) Έστω $F = \bigoplus_{i=1}^{m} Ru_i$, $F' = \bigoplus_{i=1}^{n} Rv_i$ και $F'' = \bigoplus_{i=1}^{k} Rw_i$ τρία ελεύθερα πρότυπα με διατεταγμένες βάσεις $\hat{u} = (u_1, u_2, \ldots, u_m)$, $\hat{v} = (v_1, v_2, \ldots, v_n)$ και $\hat{w} = (w_1, w_2, \ldots, w_k)$.
Αν $A = (\alpha_{ij}) = (f \mid \hat{u}, \hat{v}) \in R^{n\times m}$ και $B = (\beta_{ij}) = (g \mid \hat{v}, \hat{w}) \in R^{k\times n}$, τότε $(g \circ f \mid \hat{u}, \hat{w}) = BA \in$ $\in R^{k\times m}$.
(iii) Έστω F ένα ελεύθερο R-πρότυπο με διατεταγμένη βάση $\hat{u} = (u_1, u_2, \ldots, u_n)$, την οποία θεωρούμε σταθερή. Τότε υπάρχει μια αμφιμονοσήμαντη αντιστοιχία ανάμεσα στο σύνολο των διατεταγμένων βάσεων $\hat{u'} = (u'_1, u'_2, \ldots, u'_n)$ και των αντιστρεψίμων $n \times n$ πινάκων από το $R^{n\times n}$, η οποία δίνεται από τη σχέση:
$$A = (\alpha_{ij}) = (\mathbf{1}_F \mid \hat{u}, \hat{u'}).$$
Ιδιαιτέρως $(\mathbf{1}_F \mid \hat{u}, \hat{u}) = I_n$, ο ταυτοτικός πίνακας.
ΑΠΟΔΕΙΞΗ: (i) Έστω $f : F \to F'$ μια R-γραμμική απεικόνιση. Τότε $f(u_j) = \sum_{i=1}^{n} \alpha_{ij} v_i$, όπου $\alpha_{ij} \in R$, για κάθε $i = 1, 2, \ldots, n$ και $j = 1, 2, \ldots, m$. Προφανώς ο πίνακας $A = (\alpha_{ij})$ ανήκει στο $R^{n\times m}$.
Αντιστρόφως, έστω $A = (\alpha_{ij}) \in R^{n\times m}$. Ορίζουμε την απεικόνιση $f : F \to F'$ με
$$f(r_1u_1 + r_2u_2 + \cdots + r_mu_m) = \big(\textstyle\sum_{j=1}^{m} r_j\alpha_{1j}\big)v_1 + \big(\sum_{j=1}^{m} r_j\alpha_{2j}\big)v_2 + \cdots + \big(\sum_{j=1}^{m} r_j\alpha_{nj}\big)v_n,$$
για κάθε $r_1, r_2, \ldots, r_m \in R$. Εύκολα επαληθεύεται ότι η f είναι R-γραμμική. Παρατηρούμε ότι
$$f(u_j) \underset{\substack{r_j=1\\ \text{και } r_{j'}=0\\ \text{για } j'\neq j}}{=} \alpha_{1j}v_1 + \alpha_{2j}v_2 + \cdots + \alpha_{nj}v_n = \textstyle\sum_{i=1}^{n} \alpha_{ij}v_i.$$
(ii) Εξ ορισμού $f(u_j) = \sum_{s=1}^{n} \alpha_{sj}v_s$ και $g(v_s) = \sum_{i=1}^{k} \beta_{is}w_i$. Έστω $\gamma_{ij} = \sum_{s=1}^{n} \beta_{is}\alpha_{sj}$ το (i, j)-στοιχείο του πίνακα BA, όπου $i = 1, 2, \ldots, k$ και $j = 1, 2, \ldots, n$.
Τότε $(g \circ f)(u_j) = g(f(u_j)) = g\big(\sum_{s=1}^{n} \alpha_{sj}v_s\big) = \sum_{s=1}^{n} \alpha_{sj}g(v_s) = \sum_{s=1}^{n} \alpha_{sj} \sum_{i=1}^{k} \beta_{is}w_i =$ $= \sum_{i=1}^{k} \big(\sum_{s=1}^{n} \beta_{is}\alpha_{sj}\big)w_i = \sum_{i=1}^{k} \gamma_{ij}w_i$.
(iii) Αν $\hat{u'} = (u'_1, u'_2, \ldots, u'_n)$ είναι μια διατεταγμένη βάση του F και $A = (\alpha_{ij}) = (\mathbf{1}_F \mid \hat{u}, \hat{u'})$, τότε ο A είναι αντιστρέψιμος με αντίστροφο τον πίνακα $B = (\beta_{ij}) = (\mathbf{1}_F \mid \hat{u'}, \hat{u})$.
Αντιστρόφως, ας υποθέσουμε ότι $A = (\alpha_{ij})$ είναι ένας αντιστρέψιμος $n \times n$ πίνακας και $B =$

$= (\beta_{ij}) = A^{-1}$. Θέτουμε

$$u'_j = \sum_{i=1}^n \beta_{ij} u_i, \qquad (1)$$

για κάθε $j = 1, 2, \ldots, n$. Τότε η n-άδα $(u'_1, u'_2, \ldots, u'_n)$ είναι μια διατεταγμένη βάση του F. Πράγματι:

α) Τα $u'_1, u'_2, \ldots, u'_n$ παράγουν το F.

Επιλέγουμε $k \in \{1, 2, \ldots, n\}$ και αφού πολλαπλασιάσουμε την (1) με α_{jk}, αθροίζουμε ως προς j.

Παίρνουμε $\sum_{j=1}^n \alpha_{jk} u'_j = \sum_{j=1}^n \alpha_{jk} \sum_{i=1}^n \beta_{ij} u_i = \sum_{i=1}^n \big(\sum_{j=1}^n \beta_{ij} \alpha_{jk} \big) u_i$.

Αλλά $BA = I_n$, οπότε $\sum_{j=1}^n \beta_{ij} \alpha_{jk} = \delta_{ik}$, το δέλτα του Kronecker. Επομένως

$$\sum_{j=1}^n \alpha_{jk} u'_j = \sum_{i=1}^n \delta_{ik} u_i = u_k,$$

δηλαδή τα $u'_1, u'_2, \ldots, u'_n$ παράγουν τους γεννήτορες $u_1, u_2, \ldots, u_n$ του F, άρα και το F.

β) Τα $u'_1, u'_2, \ldots, u'_n$ είναι R-γραμμικώς ανεξάρτητα.

Έστω $\sum_{j=1}^n r_j u'_j = 0_F$, όπου $r_1, r_2, \ldots, r_n \in R$, δηλαδή

$$\sum_{j=1}^n r_j \sum_{i=1}^n \beta_{ij} u_i = 0_F \Leftrightarrow \sum_{i=1}^n \big(\sum_{j=1}^n r_j \beta_{ij} \big) u_i = 0_F.$$

Επειδή τα $u_1, u_2, \ldots, u_n$ είναι γραμμικώς ανεξάρτητα, παίρνουμε $\sum_{j=1}^n r_j \beta_{ij} = 0_R$, για κάθε $i = 1, 2, \ldots, n$.

Πολλαπλασιάζουμε την τελευταία σχέση με α_{ki} και αθροίζουμε ως προς i. Παίρνουμε

$\sum_{i=1}^n \alpha_{ki} \sum_{j=1}^n r_j \beta_{ij} = 0_R \Leftrightarrow \sum_{j=1}^n r_j \big(\sum_{i=1}^n \alpha_{ki} \beta_{ij} \big) = 0_R \Leftrightarrow \sum_{j=1}^n r_j \delta_{kj} = 0_R \Leftrightarrow r_k = 0_R$, για κάθε $k = 1, 2, \ldots, n$. ■

Υπενθυμίζουμε ότι δύο πίνακες $A, B \in R^{n \times m}$ λέγονται **ισοδύναμοι** αν υπάρχουν αντιστρέψιμοι (στον R) πίνακες $X \in R^{n \times n}$ και $Y \in R^{m \times m}$ τέτοιοι, ώστε $A = XBY$. Η σχέση της ισοδυναμίας πινάκων είναι όντως σχέση ισοδυναμίας (υπό την κλασική έννοια). Πράγματι:
$A = I_n A I_m$ (ανακλαστική), $B = XAY \Leftrightarrow A = X^{-1} B Y^{-1}$ (συμμετρική) και αν $B = XAY$ και $\Gamma = X' B Y'$, τότε $\Gamma = (X'X) A (YY')$ (μεταβατική).

ΠΟΡΙΣΜΑ 3.55. Έστω $F = \bigoplus_{i=1}^m Ru_i$ και $F' = \bigoplus_{i=1}^m Rv_i$ δύο ελεύθερα πρότυπα με βάσεις $\hat{u} = (u_1, \ldots, u_m)$ και $\hat{v} = (v_1, \ldots, v_n)$ αντίστοιχα. Έστω επίσης $f : F \to F'$ μια γραμμική απεικόνιση και $A = (f \mid \hat{u}, \hat{v}) \in R^{n \times m}$.

Τότε υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των ζευγών $(\hat{u}', \hat{v}')$ των βάσεων $\hat{u}'$ και $\hat{v}'$ των F και F' αντίστοιχα και των ισοδυνάμων προς τον A πινάκων στο $R^{n \times m}$.

ΑΠΟΔΕΙΞΗ: Έστω $B = XAY$, όπου $X \in R^{n \times n}$ και $Y \in R^{m \times m}$ αντιστρέψιμοι στο R. Με βάση το **(iii)** της προηγούμενης πρότασης $X = (\mathbf{1}_{F'} \mid \hat{v}, \hat{v}')$ και $Y^{-1} = (\mathbf{1}_F \mid \hat{u}, \hat{u}') = (\mathbf{1}_F \mid \hat{u}', \hat{u})^{-1} \Leftrightarrow$
$\Leftrightarrow Y = (\mathbf{1}_F \mid \hat{u}', \hat{u})$, όπου $\hat{u}' = (u'_1, \ldots, u'_m)$ και $\hat{v}' = (v'_1, \ldots, v'_n)$ δύο νέες βάσεις των F και F' αντίστοιχα. Τότε $B = XAY = (\mathbf{1}_{F'} \mid \hat{v}, \hat{v}')(f \mid \hat{u}, \hat{v})(\mathbf{1}_F \mid \hat{u}', \hat{u}) = (\mathbf{1}_{F'} \circ f \circ \mathbf{1}_F \mid \hat{u}', \hat{v}') =$
$= (f \mid \hat{u}', \hat{v}')$.

Αντιστρόφως, $(f \mid \hat{u}', \hat{v}') = (\mathbf{1}_{F'} \mid \hat{v}, \hat{v}')(f \mid \hat{u}, \hat{v})(\mathbf{1}_F \mid \hat{v}', \hat{v}) = XAY$, όπου $X = (\mathbf{1}_{F'} \mid \hat{v}, \hat{v}')$ και $Y = (\mathbf{1}_F \mid \hat{v}', \hat{v})$. ■

Τίθεται λοιπόν το ερώτημα: Υπάρχουν κατάλληλες βάσεις $\hat{u}'$ και $\hat{v}'$ των F και F' αντίστοιχα έτσι, ώστε ο πίνακας $B = (f \mid \hat{u}', \hat{v}')$ να έχει όσο το δυνατόν απλούστερη μορφή; Η απάντηση είναι καταφατική και συγκεκριμένα ο πίνακας αυτός μπορεί να τεθεί σε διαγώνια μορφή, ακόμα

και αν $m \neq n$. Με αυτό το θέμα θα ασχοληθούμε στο επόμενο κεφάλαιο.

Κεφάλαιο 4

Ανάλυση Πεπερασμένα Παραγόμενων Προτύπων επί μιας Περιοχής Κυρίων Ιδεωδών σε Ευθέα Αθροίσματα Κυκλικών Υποπροτύπων

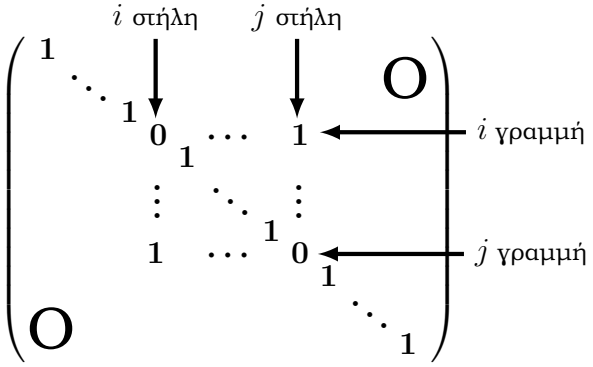
4.1 Ο Αλγόριθμος του Smith

Ας υποθέσουμε ότι μας δίνεται ο πίνακας $\begin{pmatrix} 42 & 16 & 20 \\ 10 & 10 & 6 \end{pmatrix}$. Τίθεται το ερώτημα: Μπορούμε με στοιχειώδεις μετασχηματισμούς γραμμών και στηλών να φέρουμε τον πίνακα αυτόν στην μορφή $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \end{pmatrix}$, όπου $\alpha, \beta \in \mathbb{Z}$ με $\alpha \mid \beta$;
Γενικότερα, θα μπορούσαμε με στοιχειώδεις μετασχηματισμούς να φέρουμε έναν οποιονδήποτε $n \times m$ πίνακα στη διαγώνια μορφή

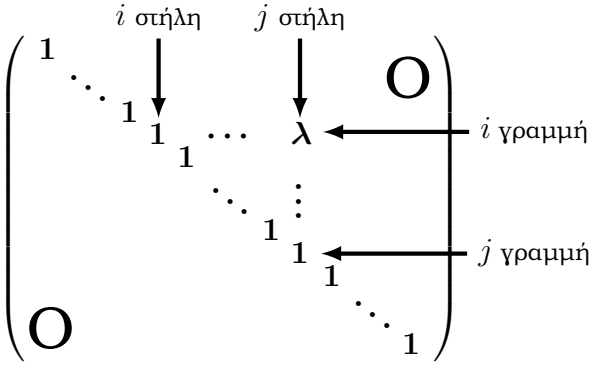
$$\begin{pmatrix} \delta_1 & & & \\ & \delta_2 & & \\ & & \ddots & \\ & & & \delta_\kappa \end{pmatrix},$$

όπου $\kappa = \min\{m, n\}$ και $\delta_i \mid \delta_{i+1}$, για κάθε $i = 1, 2, \ldots, \kappa - 1$;
Κατ' αρχάς ας ξεκαθαρίσουμε τι εννοούμε με τον όρο «στοιχειώδης μετασχηματισμός». Οι στοιχειώδεις μετασχηματισμοί που θα αναφέρουμε ισχύουν σε οποιονδήποτε μεταθετικό δακτύλιο.

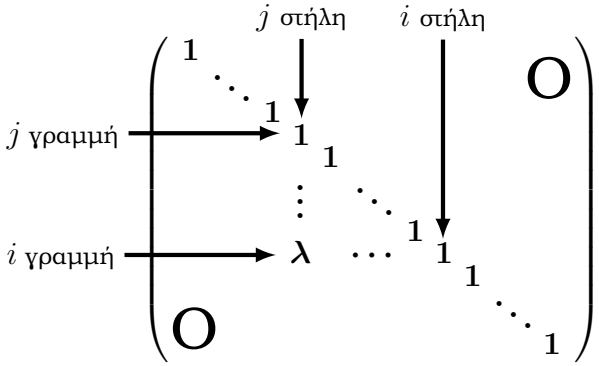
(i) Έστω ο πίνακας $F_{ij} =$



Αν πολλαπλασιάσουμε έναν πίνακα A από δεξιά με κατάλληλο F_{ij}, θα εναλλάξουμε τις στήλες i και j του A. Ενώ ο $F_{ij}A$ προκύπτει με εναλλαγή των γραμμών i και j του A.

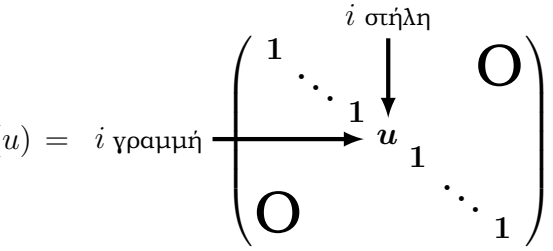
(ii) Έστω ο πίνακας $H_{ij}(\lambda) =$ 

, αν $i < j$

και $H_{ij}(\lambda) = H_{ji}(\lambda)^T =$ 

, αν $j < i$.

Τότε ο πίνακας $AH_{ij}(\lambda)$ προκύπτει αν προσθέσουμε στην j στήλη του A την i στήλη αυτού πολλαπλασιασμένη επί λ, ενώ ο $H_{ij}(\lambda)A$ προκύπτει αν προσθέσουμε στην i γραμμή την j γραμμή πολλαπλασιασμένη επί λ.

(iii) Έστω ο πίνακας $G_i(u) =$ 

, όπου u αντιστρέψιμο στοιχείο. Τότε ο $G_i(u)A$ προκύπτει από τον A αν πολλαπλασιάσουμε την i γραμμή επί u, ενώ ο $AG_i(u)$ προκύπτει αν πολλαπλασιάσουμε την i στήλη επί u.

Προφανώς $\det(F_{ij}) = -1$, $\det(H_{ij}(\lambda)) = 1$ και $\det(G_i(u)) = u$. Άρα όλοι οι παραπάνω πίνακες είναι αντιστρέψιμοι στο R. Σε μια ευκλείδεια περιοχή οι μετασχηματισμοί αυτοί είναι αρκετοί για να φέρουν έναν πίνακα $m \times n$ στη μορφή $\begin{pmatrix} \delta_1 & & & \\ & \delta_2 & & \\ & & \ddots & \\ & & & \delta_\kappa \end{pmatrix}$, όπου $\kappa = \min\{m, n\}$ και $\delta_i \mid \delta_{i+1}$, για κάθε $i = 1, 2, \ldots, \kappa - 1$.

ΠΑΡΑΔΕΙΓΜΑΤΑ 4.1. (i) Ας δούμε πώς δουλεύει η μέθοδος αυτή στον πίνακα $\begin{pmatrix} 42 & 16 & 20 \\ 10 & 10 & 6 \end{pmatrix}$.

Έχουμε:

$$\begin{pmatrix} 42 & 16 & 20 \\ 10 & 10 & 6 \end{pmatrix} \overset{\Gamma_1 \leftrightarrow \Gamma_2}{\longrightarrow} \begin{pmatrix} 10 & 10 & 6 \\ 42 & 16 & 20 \end{pmatrix} \overset{\Sigma_1 \leftrightarrow \Sigma_3}{\longrightarrow} \begin{pmatrix} 6 & 10 & 10 \\ 20 & 16 & 42 \end{pmatrix} \overset{\Sigma_2 \to \Sigma_2 - 2\Sigma_1}{\longrightarrow} \begin{pmatrix} 6 & -2 & 10 \\ 20 & -24 & 42 \end{pmatrix} \overset{\Sigma_1 \leftrightarrow \Sigma_2}{\longrightarrow}$$

$\overset{\Sigma_1\leftrightarrow\Sigma_2}{\longrightarrow}\begin{pmatrix}-2&6&10\\-24&20&42\end{pmatrix}\overset{\Sigma_2\to\Sigma_2+3\Sigma_1}{\longrightarrow}\begin{pmatrix}-2&0&10\\-24&-52&42\end{pmatrix}\overset{\Sigma_3\to\Sigma_3+5\Sigma_1}{\longrightarrow}\begin{pmatrix}-2&0&0\\-24&-52&-78\end{pmatrix}\overset{\Gamma_1\to-\Gamma_1}{\longrightarrow}$
$\overset{\Gamma_1\to-\Gamma_1}{\longrightarrow}\begin{pmatrix}2&0&0\\-24&-52&-78\end{pmatrix}\overset{\Gamma_2\to\Gamma_2+12\Gamma_1}{\longrightarrow}\begin{pmatrix}2&0&0\\0&-52&-78\end{pmatrix}\overset{\Gamma_2\to-\Gamma_2}{\longrightarrow}\begin{pmatrix}2&0&0\\0&52&78\end{pmatrix}\overset{\Sigma_2\to\Sigma_2-\Sigma_3}{\longrightarrow}$
$\overset{\Sigma_2\to\Sigma_2-\Sigma_3}{\longrightarrow}\begin{pmatrix}2&0&0\\0&-26&78\end{pmatrix}\overset{\Sigma_3\to\Sigma_3+3\Sigma_2}{\longrightarrow}\begin{pmatrix}2&0&0\\0&-26&0\end{pmatrix}\overset{\Gamma_2\to-\Gamma_2}{\longrightarrow}\begin{pmatrix}2&0&0\\0&26&0\end{pmatrix}.$

Ας βρούμε τώρα τους πίνακες X και Y για τους οποίους $X\begin{pmatrix}42&16&20\\10&10&6\end{pmatrix}Y=\begin{pmatrix}2&0&0\\0&26&0\end{pmatrix}$.
Προφανώς $X=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}1&0\\12&1\end{pmatrix}\begin{pmatrix}-1&0\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}1&0\\12&1\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}=$
$=\begin{pmatrix}0&-1\\1&-12\end{pmatrix}$ και
$Y=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}\begin{pmatrix}1&-2&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&3&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&5\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&-1&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&3\\0&0&1\end{pmatrix}=$
$=\begin{pmatrix}0&-1&-2\\1&-2&-1\\-2&5&5\end{pmatrix}.$

(ii) Ας δούμε τώρα ένα άλλο παράδειγμα: $\begin{pmatrix}-4&-6&7\\2&2&4\\6&6&15\end{pmatrix}$. Από τα στοιχεία του πίνακα μπορούμε να επιλέξουμε ένα με τη μικρότερη δυνατή απόλυτη τιμή και να το βάλουμε στην $(1,1)$-θέση. Αντ' αυτού, θα προσθέσουμε τη δεύτερη στήλη στην τρίτη για να βγει μονάδα.
$\begin{pmatrix}-4&-6&7\\2&2&4\\6&6&15\end{pmatrix}\overset{\Sigma_3\to\Sigma_3+\Sigma_2}{\longrightarrow}\begin{pmatrix}-4&-6&1\\2&2&6\\6&6&21\end{pmatrix}\overset{\Sigma_1\leftrightarrow\Sigma_3}{\longrightarrow}\begin{pmatrix}1&-6&-4\\6&2&2\\21&6&6\end{pmatrix}\overset{\Sigma_2\to\Sigma_2+6\Sigma_1}{\longrightarrow}\begin{pmatrix}1&0&-4\\6&38&2\\21&132&6\end{pmatrix}$
$\overset{\Sigma_3\to\Sigma_3+4\Sigma_1}{\longrightarrow}\begin{pmatrix}1&0&0\\6&38&26\\21&132&90\end{pmatrix}\overset{\Gamma_2\to\Gamma_2-6\Gamma_1}{\longrightarrow}\begin{pmatrix}1&0&0\\0&38&26\\21&132&90\end{pmatrix}\overset{\Gamma_3\to\Gamma_3-21\Gamma_1}{\longrightarrow}\begin{pmatrix}1&0&0\\0&38&26\\0&132&90\end{pmatrix}\overset{\Sigma_2\to\Sigma_2-\Sigma_3}{\longrightarrow}$
$\longrightarrow\begin{pmatrix}1&0&0\\0&12&26\\0&42&90\end{pmatrix}\overset{\Sigma_3\to\Sigma_3-2\Sigma_2}{\longrightarrow}\begin{pmatrix}1&0&0\\0&12&2\\0&42&6\end{pmatrix}\overset{\Sigma_3\leftrightarrow\Sigma_2}{\longrightarrow}\begin{pmatrix}1&0&0\\0&2&12\\0&6&42\end{pmatrix}\overset{\Sigma_3\to\Sigma_3-6\Sigma_2}{\longrightarrow}\begin{pmatrix}1&0&0\\0&2&0\\0&6&6\end{pmatrix}\overset{\Sigma_2\to\Sigma_2-\Sigma_3}{\longrightarrow}$
$\longrightarrow\begin{pmatrix}1&0&0\\0&2&0\\0&0&6\end{pmatrix}$. Αν X και Y είναι 3×3 πίνακες με $X\begin{pmatrix}-4&-6&7\\2&2&4\\6&6&15\end{pmatrix}Y=\begin{pmatrix}1&0&0\\0&2&0\\0&0&6\end{pmatrix}$, τότε
$X=\begin{pmatrix}1&0&0\\0&1&0\\-21&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\-6&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0\\-6&1&0\\-21&0&1\end{pmatrix}$ και
$Y=\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}\begin{pmatrix}1&6&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&4\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&-1&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&-2\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$
$\begin{pmatrix}1&0&0\\0&1&-6\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&-1&1\end{pmatrix}=\begin{pmatrix}0&22&-19\\1&-17&15\\1&-2&2\end{pmatrix}.$

(iii) Ένα άλλο παράδειγμα από τους ακεραίους του Gauss. Εδώ $R=\mathbb{Z}[\mathrm{i}]$. Έχουμε τον πίνα-

κα $\begin{pmatrix} 2 & 1+\mathbf{i} & 1-\mathbf{i} \\ 8+6\mathbf{i} & -4 & 0 \end{pmatrix}$. Τα στοιχεία $1 \pm \mathbf{i}$ έχουν τη μικρότερη ευκλείδεια νόρμα (και είναι ανάγωγα στο $\mathbb{Z}[\mathbf{i}]$). Έχουμε:

$$\begin{pmatrix} 2 & 1+\mathbf{i} & 1-\mathbf{i} \\ 8+6\mathbf{i} & -4 & 0 \end{pmatrix} \overset{\Sigma_2 \leftrightarrow \Sigma_1}{\longrightarrow} \begin{pmatrix} 1+\mathbf{i} & 2 & 1-\mathbf{i} \\ -4 & 8+6\mathbf{i} & 0 \end{pmatrix} \overset{\Sigma_2 \to \Sigma_2-(1-\mathbf{i})\Sigma_1}{\longrightarrow} \begin{pmatrix} 1+\mathbf{i} & 0 & 1-\mathbf{i} \\ -4 & 12+2\mathbf{i} & 0 \end{pmatrix}$$
$$\overset{\Sigma_3 \to \Sigma_3+\mathbf{i}\Sigma_1}{\longrightarrow} \begin{pmatrix} 1+\mathbf{i} & 0 & 0 \\ -4 & 12+2\mathbf{i} & -4\mathbf{i} \end{pmatrix} \overset{\Gamma_2 \to \Gamma_2+2(1-\mathbf{i})\Gamma_1}{\longrightarrow} \begin{pmatrix} 1+\mathbf{i} & 0 & 0 \\ 0 & 12+2\mathbf{i} & -4\mathbf{i} \end{pmatrix} \overset{\Sigma_2 \to \Sigma_2-3\mathbf{i}\Sigma_3}{\longrightarrow}$$
$$\begin{pmatrix} 1+\mathbf{i} & 0 & 0 \\ 0 & 2\mathbf{i} & -4\mathbf{i} \end{pmatrix} \overset{\Sigma_3 \to \Sigma_3+2\Sigma_2}{\longrightarrow} \begin{pmatrix} 1+\mathbf{i} & 0 & 0 \\ 0 & 2\mathbf{i} & 0 \end{pmatrix} \overset{\Gamma_2 \to -\mathbf{i}\Gamma_2}{\longrightarrow} \begin{pmatrix} 1+\mathbf{i} & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 1+\mathbf{i} & 0 & 0 \\ 0 & (1+\mathbf{i})(1-\mathbf{i}) & 0 \end{pmatrix}.$$

Τώρα οι πίνακες X και Y είναι: $X = \begin{pmatrix} 1 & 0 \\ 0 & -\mathbf{i} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2(1-\mathbf{i}) & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -2-2\mathbf{i} & -\mathbf{i} \end{pmatrix}$ και

$$Y = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1+\mathbf{i} & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \mathbf{i} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -3\mathbf{i} & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2+\mathbf{i} & 4+3\mathbf{i} \\ 0 & -3\mathbf{i} & 1-6\mathbf{i} \end{pmatrix}.$$

(iv) Το R μπορεί να είναι ο πολυωνυμικός δακτύλιος πάνω από ένα σώμα. Ας εξετάσουμε την περίπτωση που $R = \mathbb{Q}[x]$ και ο πίνακάς μας είναι ο

$$\begin{pmatrix} 1-x & 1+x & x \\ x & 1-x & 1 \\ 1+x & 2x & 1 \end{pmatrix}$$

Επειδή το 1 διαιρεί τα πάντα, φέρουμε το $(2,3)$-στοιχείο στη θέση $(1,1)$. Έχουμε λοιπόν:

$$\begin{pmatrix} 1-x & 1+x & x \\ x & 1-x & 1 \\ 1+x & 2x & 1 \end{pmatrix} \overset{\Gamma_1 \leftrightarrow \Gamma_2}{\longrightarrow} \begin{pmatrix} x & 1-x & 1 \\ 1-x & 1+x & x \\ 1+x & 2x & 1 \end{pmatrix} \overset{\Sigma_1 \leftrightarrow \Sigma_3}{\longrightarrow} \begin{pmatrix} 1 & 1-x & x \\ x & 1+x & 1-x \\ 1 & 2x & 1+x \end{pmatrix} \overset{\Sigma_2 \to \Sigma_2-(1-x)\Sigma_1}{\longrightarrow}$$
$$\longrightarrow \begin{pmatrix} 1 & 0 & x \\ x & x^2+1 & 1-x \\ 1 & 3x-1 & 1+x \end{pmatrix} \overset{\Sigma_3 \to \Sigma_3-x\Sigma_1}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ x & x^2+1 & -x^2-x+1 \\ 1 & 3x-1 & 1 \end{pmatrix} \overset{\Gamma_2 \to \Gamma_2-x\Gamma_1}{\longrightarrow}$$
$$\longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^2+1 & -x^2-x+1 \\ 1 & 3x-1 & 1 \end{pmatrix} \overset{\Gamma_3 \to \Gamma_3-\Gamma_1}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x^2+1 & -x^2-x+1 \\ 0 & 3x-1 & 1 \end{pmatrix} \overset{\Gamma_2 \leftrightarrow \Gamma_3}{\longrightarrow}$$
$$\longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3x-1 & 1 \\ 0 & x^2+1 & -x^2-x+1 \end{pmatrix} \overset{\Sigma_2 \leftrightarrow \Sigma_3}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 3x-1 \\ 0 & -x^2-x+1 & x^2+1 \end{pmatrix} \overset{\Sigma_3 \to \Sigma_3-(3x-1)\Sigma_2}{\longrightarrow}$$
$$\longrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -x^2-x+1 & 3x^3+3x^2-4x+2 \end{pmatrix} \overset{\Gamma_3 \to \Gamma_3+(x^2+x-1)\Gamma_2}{\longrightarrow} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3x^3+3x^2-4x+2 \end{pmatrix}$$

Τώρα οι πίνακες X και Y είναι: $X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x^2+x-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -x & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & -x^2-2x+1 & x^2+x-1 \end{pmatrix}$ και

$$Y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & x-1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1-3x \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1-3x \\ 0 & 0 & 1 \\ 1 & -x & 3x^2-1 \end{pmatrix}$$

Ας δούμε τη γενική μέθοδο. Έστω R **περιοχή κυρίων ιδεωδών**. Υπενθυμίζουμε ότι

$$\lambda : R \setminus \{0_R\} \to \{0, 1, 2, \ldots\}$$

είναι η συνάρτηση που δίνει το πλήθος των ανάγωγων παραγόντων ενός μη μηδενικού στοιχείου. (Το μήκος του). Ένα στοιχείο $u \in R \setminus \{0_R\}$ είναι αντιστρέψιμο αν και μόνον αν $\lambda(u) = 0$. Επίσης, αν $\alpha, \beta \neq 0_R$ με $\alpha \mid \beta$, τότε $\lambda(\alpha) \leq \lambda(\beta)$. Ισότητα θα έχουμε στην τελευταία σχέση αν και μόνον αν τα στοιχεία α και β είναι συντροφικά, δηλαδή $\alpha \mid \beta$ και $\beta \mid \alpha$. Πράγματι, έχουμε αποδείξει ότι αν $\alpha = up_1^{r_1} \cdots p_k^{r_k}$ και $\beta = vp_1^{s_1} \cdots p_k^{s_k}$, όπου u, v αντιστρέψιμα, $p_1, \ldots, p_k$ ανάγωγα στοιχεία διαφορετικά ανά δύο και $r_i, s_i \geq 0$, για κάθε $i = 1, \ldots, k$, τότε $\alpha \mid \beta$ αν και μόνον αν $r_i \leq s_i$, για κάθε $i = 1, \ldots, k$. Ενδέχεται κάποιοι εκθέτες r_i να είναι μηδέν. Αν κάποιος s_i είναι μηδέν, τότε αφού $0 \leq r_i \leq s_i$, αναγκαστικά και $r_i = 0$. Οπότε η χρήση του ανάγωγου στοιχείου p_i είναι περιττή, αλλά όχι εσφαλμένη, αφού δεν επηρεάζει το τελικό αποτέλεσμα. Σε κάθε περίπτωση $\lambda(\alpha) = \sum_{i=1}^{k} r_i$ και $\lambda(\beta) = \sum_{i=1}^{k} s_i$. Αν λοιπόν $\sum_{i=1}^{k} r_i = \lambda(\alpha) = \lambda(\beta) = \sum_{i=1}^{k} s_i$, τότε αφού $r_i \leq s_i$, για κάθε $i = 1, \ldots, k$, θα έχουμε $r_i = s_i$, για κάθε $i = 1, \ldots, k$. Επομένως $\alpha = up_1^{r_1} \cdots p_k^{r_k} = up_1^{s_1} \cdots p_k^{s_k} = uv^{-1}vp_1^{s_1} \cdots p_k^{s_k} = uv^{-1}\beta$ και άρα $\alpha \sim \beta$.

Έστω $A = (\alpha_{ij})$ ένας $n \times m$ πίνακας με στοιχεία από το R.
Ο πρώτος και κύριος στόχος μας είναι να μετατρέψουμε τον πίνακα A σε ισοδύναμο της μορφής

$$\left(\begin{array}{c|ccc} \delta_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \boldsymbol{C} & \\ 0 & & & \end{array}\right), \qquad \textbf{(1)}$$

όπου το δ_1 διαιρεί κάθε στοιχείο του πίνακα C. Αν ο A είναι ο μηδενικός πίνακας δεν έχουμε να κάνουμε τίποτα. Υποθέτουμε λοιπόν ότι ο A είναι μη μηδενικός.

ΛΗΜΜΑ 4.2. Έστω $A = (\alpha_{ij})$ ένας $n \times m$ πίνακας με στοιχεία από το R. Τότε υπάρχουν αντιστρέψιμοι πίνακες $X \in R^{n \times n}$ και $Y \in R^{m \times m}$ τέτοιοι, ώστε ο πίνακας $B = XAY$ θα έχει την προηγούμενη μορφή **(1)**.
ΑΠΟΔΕΙΞΗ: Εφαρμόζουμε επαγωγή επί του ελαχίστου μήκους $\lambda(A) = \min\{\lambda(\alpha_{ij}) \mid i = = 1, \ldots, n,\ j = 1, \ldots, m$ και $\alpha_{ij} \neq 0\}$ των μη μηδενικών στοιχείων του A. Αν $\lambda(A) = 0$, δηλαδή υπάρχει στοιχείο α_{ts} με $\lambda(\alpha_{ts}) = 0$, τότε το α_{ts} θα είναι αντιστρέψιμο και άρα θα διαιρεί όλα τα υπόλοιπα στοιχεία του A. Γενικότερα, αν ο A έχει ένα στοιχείο α_{ts} που διαιρεί όλα τα υπόλοιπα α_{ij}, τότε το φέρνουμε στην $(1,1)$-θέση με μεταθέσεις γραμμών και στηλών. Αυτό γίνεται με πολλαπλασιαμό από δεξιά ή αριστερά με πίνακες του τύπου F_{ij} που είναι αντιστρέψιμοι. Άρα ο πίνακας που θα προκύψει είναι ισοδύναμος με τον αρχικό πίνακα A. Μπορούμε λοιπόν να υποθέσουμε ευθύς εξαρχής ότι το στοιχείο ελαχίστου μήκους είναι το α_{11}. Στην περίπτωση αυτή αφαιρούμε από όλες τις στήλες $\Sigma_2, \Sigma_3, \ldots, \Sigma_m$ κατάλληλα πολλαπλάσια της πρώτης στήλης Σ_1, για παράδειγμα αν $\alpha_{12} = \lambda\alpha_{11}$, τότε αφαιρούμε από τη δεύτερη στήλη την πρώτη πολλαπλασιασμένη επί λ. Έτσι μηδενίζουμε όλα τα στοιχεία (πλην του α_{11}) της πρώτης γραμμής. Στη συνέχεια εφαρμόζουμε την ίδια μέθοδο και στις γραμμές, δηλαδή αφαιρούμε από όλες τις γραμμές $\Gamma_2, \Gamma_3, \ldots, \Gamma_n$ κατάλληλα πολλαπλάσια της πρώτης γραμμής Γ_1 και μηδενίζουμε έτσι όλα τα στοιχεία (πλην του α_{11}) της πρώτης στήλης. Θα πάρουμε τη μορφή **(1)**, όπου τα στοιχεία του πίνακα C είναι γραμμικοί συνδυαμοί στοιχείων του A και άρα διαιρούνται όλα με το α_{11}. Θέτουμε $\delta_1 = \alpha_{11}$ και τελειώσαμε.
Υποθέτουμε λοιπόν ότι $\lambda(A) = k > 0$ και $\lambda(\alpha_{ts}) = k$. Επίσης υποθέτουμε ότι το α_{ts} δεν διαιρεί όλα τα υπόλοιπα στοιχεία του A, γιατί τότε η περίπτωση αυτή ανάγεται στην προηγούμενη.
Όπως προηγουμένως, μπορούμε να φέρουμε το στοιχείο α_{ts} στην $(1,1)$-θέση και άρα υποθέτουμε ευθύς εξ αρχής ότι $\alpha_{ts} = \alpha_{11}$.

Περίπτωση 1η: Αν το α_{11} δεν διαιρεί κάποιο α_{1j}, με $j>1$, τότε με αντιμετάθεση της 2ης και της j-στης στήλης φέρουμε το στοιχείο α_{1j} στην $(1,2)$-θέση. Επομένως μπορούμε να υποθέσουμε ότι το στοιχείο α_{1j} είναι το α_{12}. Έστω β_{11} ένας μέγιστος κοινός διαιρέτης των α_{11} και α_{12}, δηλαδή $(\beta_{11})=(\alpha_{11},\alpha_{12})$. Αν $\lambda(\beta_{11})=\lambda(\alpha_{11})$, τότε επειδή $\beta_{11}\mid\alpha_{11}$, θα είχαμε σύμφωνα με την προηγηθέντα ότι $\alpha_{11}\sim\beta_{11}\mid\alpha_{12}$ και άρα $\alpha_{11}\mid\alpha_{12}$, άτοπο. Επομένως $\lambda(\beta_{11})<\lambda(\alpha_{11})$. Προφανώς $\alpha_{11}=y_1\beta_{11}$ και $\alpha_{12}=y_2\beta_{11}$, για κατάλληλα $y_1,y_2\in R$. Επίσης, επειδή $(\beta_{11})=(\alpha_{11},\alpha_{12})$, θα έχουμε $\alpha_{11}x_1+\alpha_{12}x_2=\beta_{11}$, για κατάλληλα $x_1,x_2\in R$ και επομένως $y_1\beta_{11}x_1+y_2\beta_{11}x_2=\beta_{11}$. Το β_{11} δεν είναι μηδέν γιατί αλλιώς θα είχαμε και $\alpha_{11}=y_1\beta_{11}=0$. Επομένως παίρνουμε $y_1x_1+y_2x_2=1$.
Πολλαπλασιάζουμε από δεξιά τον πίνακα A με τον πίνακα

$$P=\begin{pmatrix} x_1 & -y_2 & & \\ x_2 & y_1 & & \\ & & 1 & \\ & & & \ddots \\ & \boldsymbol{O} & & & 1 \end{pmatrix}$$

Η ορίζουσα του P είναι $\det\begin{pmatrix} x_1 & -y_2 \\ x_2 & y_1 \end{pmatrix}=x_1y_1+x_2y_2=1$, άρα ο P είναι αντιστρέψιμος στο $R^{m\times m}$.
Το $(1,1)$-στοιχείο του νέου πίνακα AP είναι το $\alpha_{11}x_1+\alpha_{12}x_2=\beta_{11}$ (και το $(1,2)$-στοιχείο του νέου πίνακα είναι το $\alpha_{11}(-y_2)+\alpha_{12}y_1=-y_1\beta_{11}y_2+y_2\beta_{11}y_1=0$, αλλά αυτό είναι δευτερεύον). Το σημαντικό είναι ότι $\lambda(AP)\le\lambda(\beta_{11})<\lambda(\alpha_{11})=\lambda(A)$. Επαγωγή στο $k=\lambda(A)$ και τελειώσαμε. (Ακριβέστερα επαναλαμβάνουμε τη διαδικασία).
Περίπτωση 2η: Έστω ότι το α_{11} διαιρεί κάθε στοιχείο α_{1j} της πρώτης γραμμής, δηλαδή $\alpha_{1j}=r_{1j}\alpha_{11}$, για κάθε $j=2,\dots,n$. Αν το α_{11} δεν διαιρεί κάποιο στοιχείο της πρώτης στήλης, τότε με δυϊκούς συλλογισμούς, υποθέτουμε όπως με την πρώτη γραμμή ότι το στοιχείο αυτό είναι το α_{21}, θέτουμε ως β_{11} τέτοιο, ώστε $(\beta_{11})=(\alpha_{11},\alpha_{21})$. Όπως προηγουμένως, $\lambda(\beta_{11})<\lambda(\alpha_{11})$, $\alpha_{11}=y_1\beta_{11}$, $\alpha_{21}=y_2\beta_{11}$ και $\alpha_{11}x_1+\alpha_{21}x_2=\beta_{11}$, όπου $x_1,x_2,y_1,y_2\in R$. Έτσι, $y_1x_1+y_2x_2=1$. Η διαφορά είναι ότι τώρα πολλαπλασιάζουμε από αριστερά με τον πίνακα

$$Q=\begin{pmatrix} x_1 & x_2 & & \\ -y_2 & y_1 & & \\ & & 1 & \\ & & & \ddots \\ & \boldsymbol{O} & & & 1 \end{pmatrix}$$

του οποίου η ορίζουσα είναι $\det\begin{pmatrix} x_1 & x_2 \\ -y_2 & y_1 \end{pmatrix}=x_1y_1+x_2y_2=1$, άρα ο Q είναι αντιστρέψιμος στο $R^{n\times n}$. Ξανά επαγωγή στο $k=\lambda(A)$ και τελειώσαμε.
Περίπτωση 3η: Έστω ότι το α_{11} διαιρεί όλα τα στοιχεία της πρώτης γραμμής, αλλά και όλα τα στοιχεία της πρώτης στήλης. Προφανώς μπορούμε να αφαιρέσουμε από κάθε στήλη (πλην της πρώτης) πολλαπλάσια της πρώτης στήλης (στοιχειώδεις μετασχηματισμοί) και να μηδενίσουμε όλα (πλην του α_{11}) τα στοιχεία της πρώτης γραμμής. Στη συνέχεια κάνουμε το ίδιο, αφαιρώντας από κάθε γραμμή (πλην της πρώτης) κατάλληλα πολλαπλάσια της πρώτης γραμμής και μηδενίσουμε έτσι και όλα τα υπόλοιπα στοιχεία της πρώτης στήλης.
Ο πίνακάς μας έχει τώρα μετασχηματιστεί σε έναν πίνακα της μορφής

$$\left(\begin{array}{c|ccc} \alpha_{11} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \boldsymbol{C} & \\ 0 & & & \end{array}\right).$$

Τι γίνεται όμως αν το στοιχείο α_{11} δεν διαιρεί κάποιο στοιχείο του C; Τότε προσθέτουμε στην πρώτη γραμμή (ή στην πρώτη στήλη αντίστοιχα) τη γραμμή (ή την στήλη αντίστοιχα) στην οποία ανήκει το στοιχείο αυτό του C που δεν διαιρείται από το α_{11} και αναγόμαστε στην πρώτη περίπτωση (ή στη δεύτερη περίπτωση αντίστοιχα). Τελικώς, λόγω της επαγωγικής ως προς $\lambda(A)$ διαδικασίας, θα οδηγηθούμε στη μορφή **(1)**. ■

ΠΟΡΙΣΜΑ 4.3. Έστω A ένας $n \times m$ πίνακας με στοιχεία από το R. Τότε ο A είναι ισοδύναμος με έναν πίνακα της μορφής

$$\begin{pmatrix} \delta_1 & & & \\ & \delta_2 & & \\ & & \ddots & \\ & & & \delta_\kappa \end{pmatrix} \qquad (\star),$$

όπου $\kappa = \min\{m, n\}$ και $\delta_i \mid \delta_{i+1}$, για κάθε $i = 1, 2, \ldots, \kappa - 1$.

ΑΠΟΔΕΙΞΗ: Σύμφωνα με το προηγούμενο λήμμα, ο A είναι ισοδύναμος με έναν πίνακα της μορφής

$$\left(\begin{array}{c|ccc} \delta_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \boldsymbol{C} & \\ 0 & & & \end{array}\right), \qquad (1)$$

όπου το δ_1 διαιρεί κάθε στοιχείο του πίνακα C. Τώρα, όλα τα στοιχεία του C είναι πολλαπλάσια του τελικού στοιχείου δ_1 που βρίσκεται στην $(1,1)$-θέση. Κατά συνέπεια θα διαιρεί και κάθε στοιχείο που θα προκύψει από τον C, όταν εφαρμόσουμε σ' αυτόν κάποιον από τους προηγούμενους μετασχηματισμούς που εφαρμόσαμε στον A. Έτσι, επαγωγικά όλη η προηγούμενη δουλειά μπορεί να συνεχιστεί πλέον στον πίνακα C, πολλαπλασιάζοντας από δεξιά ή αριστερά με (αντιστρέψιμους) πίνακες της μορφής $\begin{pmatrix} 1 & \boldsymbol{O} \\ \boldsymbol{O} & Y' \end{pmatrix}$ ή $\begin{pmatrix} 1 & \boldsymbol{O} \\ \boldsymbol{O} & X' \end{pmatrix}$ κ.ο.κ. καταλήγοντας έτσι βαθμιαία σε έναν πίνακα της επιθυμητής μορφής. ■

Ο αλγόριθμος που εφαρμόσαμε ονομάζεται **αλγόριθμος του Smith**. Η μορφή $(\star)$ **ονομάζεται κανονική μορφή Smith** του πίνακα A.

Τίθεται τώρα το ερώτημα: Αν ο πίνακας A είναι ισοδύναμος με έναν πίνακα της μορφής

$$\begin{pmatrix} \delta'_1 & & & \\ & \delta'_2 & & \\ & & \ddots & \\ & & & \delta'_\kappa \end{pmatrix} \qquad (\star\star),$$

όπου $\kappa = \min\{m, n\}$ και $\delta'_i \mid \delta'_{i+1}$, για κάθε $i = 1, 2, \ldots, \kappa - 1$, τότε τι σχέση έχουν τα δ_i και δ'_i;

ΠΡΟΤΑΣΗ 4.4. Αν $(\star)$ και $(\star\star)$ είναι δύο κανονικές μορφές Smith, όπως προηγουμένως, τότε
$$\delta_i \sim \delta'_i, \text{ για κάθε } i = 1, 2, \ldots, k.$$
Επομένως, υπ' αυτήν την έννοια **η κανονική μορφή Smith είναι μοναδική**. ■

Για να αποδείξουμε την παραπάνω πρόταση ας δούμε κάποια προκαταρκτικά. Αν $A = (\alpha_{ij}) \in$ $\in R^{n\times m}$, όπου R περιοχή κυρίων ιδεωδών, τότε συμβολίζουμε με $\boldsymbol{J_t(A)}$ **το ιδεώδες της** $\boldsymbol{R}$ **που παράγεται από όλες τις ελάσσονες** $\boldsymbol{t \times t}$ **ορίζουσες του** $\boldsymbol{A}$, για κάθε $t = 1, 2, \ldots, \min\{m, n\}$. Προφανώς $J_t(A) = J_t(A^T)$, αφού η ορίζουσα ενός $t \times t$ υποπίνακα του A^T είναι η ορίζουσα του

αντίστοιχου αναστρόφου υποπίνακα του A.

Τώρα, έστω $\Sigma_j = \begin{pmatrix} \alpha_{1j} \\ \alpha_{2j} \\ \vdots \\ \alpha_{nj} \end{pmatrix}$ η j-στήλη του πίνακα $A = (\Sigma_1, \Sigma_2, \ldots, \Sigma_m)$. Αν $Y = (y_{ij}) \in R^{m\times m}$, τότε ποια είναι η j-στήλη του πίνακα AY; Η j-στήλη του πίνακα $AY = B$ είναι η $\begin{pmatrix} \beta_{1j} \\ \beta_{2j} \\ \vdots \\ \beta_{nj} \end{pmatrix}$, όπου

$$\beta_{ij} = \sum_{s=1}^{m} \alpha_{is} y_{sj}.$$

Επομένως $$\begin{pmatrix} \beta_{1j} \\ \beta_{2j} \\ \vdots \\ \beta_{nj} \end{pmatrix} = \begin{pmatrix} \sum_{s=1}^{m} \alpha_{1s} y_{sj} \\ \sum_{s=1}^{m} \alpha_{2s} y_{sj} \\ \vdots \\ \sum_{s=1}^{m} \alpha_{ns} y_{sj} \end{pmatrix} = \sum_{s=1}^{m} y_{sj} \begin{pmatrix} \alpha_{1s} \\ \alpha_{2s} \\ \vdots \\ \alpha_{ns} \end{pmatrix} = \sum_{s=1}^{m} y_{sj} \Sigma_s.$$

Έτσι, αν θέλουμε να διαγράψουμε από την j-στήλη του πίνακα $B = AY$ το στοιχείο β_{ij}, αυτό επιτυγχάνεται με το να διαγράψουμε το στοιχείο α_{is} από κάθε στήλη Σ_s του πίνακα A, για κάθε $s = 1, 2, \ldots, m$, δηλαδή να διαγράψουμε **όλη την i-γραμμή** από τον πίνακα A. Άρα για να διαγράψουμε όλη την i-γραμμή από τον πίνακα AY αρκεί να διαγράψουμε όλη την i-γραμμή του πίνακα A.

Για παράδειγμα, αν $A = \begin{pmatrix} -1 & 2 & 5 \\ 3 & -2 & 7 \\ 2 & 3 & -4 \end{pmatrix}$ και $Y = \begin{pmatrix} -2 & 1 \\ 3 & 5 \\ 7 & -1 \end{pmatrix}$ και διαγράψουμε τη 2η γραμμή από τον πίνακα AY, τότε έχουμε

$$AY = \begin{pmatrix} -1 & 2 & 5 \\ 3 & -2 & 7 \\ 2 & 3 & -4 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ 3 & 5 \\ 7 & -1 \end{pmatrix} = \begin{pmatrix} 43 & 4 \\ \cancel{37} & \cancel{-14} \\ -23 & 21 \end{pmatrix} \longrightarrow \begin{pmatrix} 43 & 4 \\ -23 & 21 \end{pmatrix}$$

ενώ, αν διαγράψουμε από τον πίνακα A τη 2η γραμμή, θα πάρουμε τον πίνακα $\begin{pmatrix} -1 & 2 & 5 \\ 2 & 3 & -4 \end{pmatrix}$ και

$$\begin{pmatrix} -1 & 2 & 5 \\ 2 & 3 & -4 \end{pmatrix} \begin{pmatrix} -2 & 1 \\ 3 & 5 \\ 7 & -1 \end{pmatrix} = \begin{pmatrix} 43 & 4 \\ -23 & 21 \end{pmatrix},$$

δηλαδή το ίδιο αποτέλεσμα. Συνεπώς, αν επιλέξουμε να κρατήσουμε από τον πίνακα $B = AY$ μόνον τις γραμμές $\kappa_1, \kappa_2, \ldots, \kappa_t$, όπου $1 \le \kappa_1 < \kappa_2 < \cdots < \kappa_t \le n$ και να διαγράψουμε τις υπόλοιπες, τότε η j-στήλη του $t \times m$ πίνακα που θα προκύψει είναι της μορφής $\sum_{s=1}^{m} y_{sj} \Sigma'_s$, όπου $\Sigma'_s = \begin{pmatrix} \alpha_{\kappa_1,s} \\ \alpha_{\kappa_2,s} \\ \vdots \\ \alpha_{\kappa_t,s} \end{pmatrix}$ είναι η «κολοβή» s-στήλη του πίνακα A, δηλαδή αυτή που προκύπτει αν διαγράψουμε από αυτήν όλα τα στοιχεία που **δεν ανήκουν** στις $\kappa_1, \kappa_2, \ldots, \kappa_t$ γραμμές του A. Αν τέλος θέλουμε να κρατήσουμε μόνον τις $\lambda_1, \lambda_2, \ldots, \lambda_t$-στήλες του πίνακα AY, όπου $1 \le \lambda_1 < \lambda_2 < \cdots < \lambda_t \le m$, αφού προηγουμένως έχουμε κρατήσει μόνον τις $\kappa_1, \kappa_2, \ldots, \kappa_t$-

στήλες αυτού, τότε θα πάρουμε τον $t \times t$ πίνακα

$$S = \left(\sum_{s=1}^{m} y_{s,\lambda_1} \Sigma'_s, \quad \sum_{s=1}^{m} y_{s,\lambda_2} \Sigma'_s, \quad \dots \quad , \sum_{s=1}^{m} y_{s,\lambda_t} \Sigma'_s \right).$$

Έτσι παίρνουμε όλους τους $t \times t$ υποπίνακες του AY.

Ξέρουμε ότι η ορίζουσα ενός πίνακα είναι γραμμική ως προς τις στήλες. Επομένως

$$\begin{aligned} \det(S) &= \det \left(\sum_{s=1}^{m} y_{s,\lambda_1} \Sigma'_s, \quad \sum_{s=1}^{m} y_{s,\lambda_2} \Sigma'_s, \quad \dots \quad , \sum_{s=1}^{m} y_{s,\lambda_t} \Sigma'_s \right) = \\ &= \det \left(\sum_{s_1=1}^{m} y_{s_1,\lambda_1} \Sigma'_{s_1}, \quad \sum_{s_2=1}^{m} y_{s_2,\lambda_2} \Sigma'_{s_2}, \quad \dots \quad , \sum_{s_t=1}^{m} y_{s_t,\lambda_t} \Sigma'_{s_t} \right) = \\ &= \sum_{s_1=1}^{m} \sum_{s_2=1}^{m} \cdots \sum_{s_t=1}^{m} y_{s_1,\lambda_1} y_{s_2,\lambda_2} \cdots y_{s_t,\lambda_t} \det \left(\Sigma'_{s_1}, \quad \Sigma'_{s_2}, \quad \dots \quad , \Sigma'_{s_t} \right). \end{aligned}$$

Στο τελευταίο άθροισμα οι ορίζουσες που εμφανίζονται είναι μηδέν αν $s_\mu = s_\nu$, για διαφορετικά $\mu, \nu \in \{1, 2, \dots, t\}$, αλλιώς είναι $\pm$ επί ελάσσονες ορίζουσες του A. (Το πρόσημο $\pm$ εξαρτάται από τη διάταξη των $s_1, s_2, \dots, s_t$ και είναι το πρόσημο της αντίστοιχης μετάθεσης).

Επομένως $\det \left(\Sigma'_{s_1}, \quad \Sigma'_{s_2}, \quad \dots \quad , \Sigma'_{s_t} \right) \in J_t(A)$ και κατά συνέπεια $\det(S) \in J_t(A)$. Με άλλα λόγια, όλες οι ελάσσονες $t \times t$ ορίζουσες του AY περιέχονται στο $J_t(A)$, δηλαδή $J_t(AY) \subseteq J_t(A)$. Αν τώρα ο Y είναι αντιστρέψιμος στο R, με την ίδια λογική, θέτοντας AY στη θέση του A και Y^{-1} στη θέση του Y, παίρνουμε $J_t(A) = J_t((AY)Y^{-1}) \subseteq J(AY)$. Στην περίπτωση λοιπόν που ο Y είναι αντιστρέψιμος παίρνουμε $J_t(AY) = J_t(A)$.

Αν δουλέψουμε συμμετρικά από αριστερά με τις γραμμές του A θα συμπεράνουμε ότι $J_t(XA) = = J_t(A)$, για κάθε αντιστρέψιμο $n \times n$ πίνακα X. Εναλλακτικά, $J_t(XA) = J_t((XA)^T) = = J_t(A^T X^T) = J_t(A^T) = J_t(A)$, σύμφωνα με τα προηγούμενα.

Συμπέρασμα: $J_t(XAY) = J_t(A)$, για κάθε αντιστρέψιμους $n \times n$ και $m \times m$ πίνακες X και Y αντίστοιχα.

ΑΠΟΔΕΙΞΗ ΤΗΣ ΠΡΟΤΑΣΗΣ 4.4: Έστω

$$S_1 = \begin{pmatrix} \delta_1 & & & \\ & \delta_2 & & \\ & & \ddots & \\ & & & \delta_\kappa \end{pmatrix} \text{ και } S_2 = \begin{pmatrix} \delta'_1 & & & \\ & \delta'_2 & & \\ & & \ddots & \\ & & & \delta'_\kappa \end{pmatrix}$$

δύο κανονικές μορφές Smith ενός $n \times m$ πίνακα A. Τότε $S_1 = X_1 A Y_1$ και $S_2 = X_2 A Y_2$, όπου X_1, X_2 αντιστρέψιμοι $n \times n$ και Y_1, Y_2 αντιστρέψιμοι $m \times m$ πίνακες αντίστοιχα. Τότε $J_t(S_1) = J_t(A) = J_t(S_2)$, για κάθε $t = 1, 2, \dots, \kappa = \min\{m, n\}$. Τότε για κάθε $t = 1, 2, \dots, \kappa$ έχουμε: $(\delta_1 \delta_2 \cdots \delta_t) = J_t(S_1) = J_t(A) = J_t(S_2) = (\delta'_1 \delta'_2 \cdots \delta'_t)$. Έστω ότι υπάρχει μ με $\delta_\mu = 0$ και ο μ είναι ο ελάχιστος τέτοιος ακέραιος, δηλαδή $\delta_t \neq 0$, για κάθε $t < \mu$. Τότε $(0) = (\delta_1 \delta_2 \cdots \delta_\mu) = J_\mu(A) = (\delta'_1 \delta'_2 \cdots \delta'_\mu)$. Άρα υπάρχει $\nu \leq \mu$ τέτοιο, ώστε $\delta'_\nu = 0$, οπότε $(0) = (\delta'_1 \cdots \delta'_\nu) = J_\nu(A) = (\delta_1 \cdots \delta_\nu)$. Αν $\nu < \mu$ καταλήγουμε σε άτοπο, γιατί $\delta_t \neq 0$, για κάθε $t < \mu$. Άρα $\nu = \mu$. Επίσης, επειδή $\delta_\mu \mid \delta_{\mu+1} \mid \delta_{\mu+2} \mid \cdots$, θα είχαμε $\delta_t = 0$, για κάθε t με $\mu \leq t \leq \kappa$ και ομοίως $\delta'_t = 0$, για κάθε t με $\mu \leq t \leq \kappa$. Άρα $\delta_t = 0 \sim 0 = \delta'_t$, για κάθε t με $\mu \leq t \leq \kappa$.

Τώρα έχουμε τις σχέσεις: $(\delta_1) = J_1(A) = (\delta'_1) \Leftrightarrow \delta_1 \sim \delta'_1$, $(\delta_1 \delta_2) = J_2(A) = (\delta'_1 \delta'_2) \Leftrightarrow \delta_1 \delta_2 \sim \sim \delta'_1 \delta'_2 \underset{\delta_1 \sim \delta'_1}{\Leftrightarrow} \delta_2 \sim \delta'_2$, $(\delta_1 \delta_2 \delta_3) = J_3(A) = (\delta'_1 \delta'_2 \delta'_3) \Leftrightarrow \delta_1 \delta_2 \delta_3 \sim \delta'_1 \delta'_2 \delta'_3 \underset{\delta_1 \delta_2 \sim \delta'_1 \delta'_2}{\Leftrightarrow} \delta_3 \sim \delta'_3$ και ούτω καθεξής, μέχρι να φτάσουμε στη σχέση $\delta_{\mu-1} \sim \delta'_{\mu-1}$. Είναι σαφές ότι αν δεν υπήρχε $t \leq \kappa$ με $\delta_t = 0$, τότε οι σχέσεις $\delta_t \sim \delta'_t$ θα προέκυπταν επαγωγικά με την ίδια μέθοδο μέχρι $t = \kappa$. ■

ΟΡΙΣΜΟΣ 4.5. Τα στοιχεία $\delta_1, \delta_2, \ldots, \delta_\kappa$, τα οποία προκύπτουν από τον αλγόριθμο του Smith και είναι μοναδικά ως προς την συντροφικότητα, ονομάζονται **αναλλοίωτοι παράγοντες του πίνακα A**.

4.2 Ανάλυση ενός Πεπερασμένα Παραγόμενου Προτύπου επί μιας Περιοχής Κυρίων Ιδεωδών σε Ευθύ Άθροισμα Κυκλικών Υποπροτύπων

Έστω R περιοχή κυρίων ιδεωδών. Ας υποθέσουμε ότι έχουμε έναν R-ομομορφισμό $f : F \to F'$ μεταξύ δύο ελεύθερων προτύπων F και F', με βάσεις $\hat{u} = (u_1, u_2, \ldots, u_m)$ και $\hat{v} = (v_1, v_2, \ldots, v_n)$ αντίστοιχα.
Έστω $A = (\alpha_{ij})$ ο πίνακας της f ως προς τις βάσεις $\hat{u}$ και $\hat{v}$, δηλαδή $A = (f \mid \hat{u}, \hat{v})$. Αυτό σημαίνει ότι έχουμε τις σχέσεις

$$f(u_j) = \sum_{i=1}^{n} \alpha_{ij} v_i,$$

για κάθε $j = 1, 2, \ldots, m$. Εφαρμόζοντας τον αλγόριθμο Smith στον πίνακα A θα βρούμε δύο αντιστρέψιμους πίνακες $X \in R^{n\times n}$ και $Y \in R^{m\times m}$ τέτοιους, ώστε

$$XAY = \begin{pmatrix} \delta_1 & & & \boldsymbol{O} \\ & \delta_2 & & \\ & & \ddots & \\ \boldsymbol{O} & & & \delta_\kappa \end{pmatrix},$$

όπου $\kappa = \min\{m, n\} = n$ και $\delta_1 \mid \delta_2 \mid \delta_3 \mid \cdots$ οι αναλλοίωτοι παράγοντες του A.
Σύμφωνα με το **(iii)** της πρότασης **3.54** ο πίνακας X είναι ο πίνακας αλλαγής βάσης $(\mathbf{1}_{F'} \mid \hat{v}, \hat{v}')$ του F' και ο Y ο πίνακας αλλαγής βάσης $(\mathbf{1}_F \mid \hat{u}', \hat{u})$ του F. Συμπεραίνουμε λοιπόν ότι

$$\begin{pmatrix} \delta_1 & & & \boldsymbol{O} \\ & \delta_2 & & \\ & & \ddots & \\ \boldsymbol{O} & & & \delta_\kappa \end{pmatrix} = XAY = (\mathbf{1}_{F'} \mid \hat{v}, \hat{v}')(f \mid \hat{u}, \hat{v})(\mathbf{1}_F \mid \hat{u}', \hat{u}) = (f \mid \hat{u}', \hat{v}') \qquad \textbf{(1)}$$

Με άλλα λόγια,

$$f(u'_j) = \delta_j v'_j \qquad \textbf{(2)},$$

για κάθε $j = 1, 2, \ldots, \kappa$ και $f(u'_j) = 0_{F'}$, για κάθε j με $\kappa < j \leq m$, $\big($αν $m > n = \kappa\big)$.
Με αυτόν τον τρόπο μπορούμε να διασπάσουμε το πρότυπο-πηλίκο $F'/\mathrm{Im}f$ σε ευθύ άθροισμα κυκλικών υποπροτύπων. Έχουμε λοιπόν την επόμενη βασική πρόταση:

ΠΡΟΤΑΣΗ 4.6. Αν $f : F \to F'$ είναι ένας ομομορφισμός R-προτύπων, όπου R περιοχή κυρίων ιδεωδών. Υποθέτουμε ότι $F = Ru_1 \oplus Ru_2 \oplus \cdots \oplus Ru_m$ και $F' = Rv_1 \oplus Rv_2 \oplus \cdots \oplus Rv_n$. $\big(\hat{u} = (u_1, u_2, \ldots, u_m)$ και $\hat{v} = (v_1, v_2, \ldots, v_n)$ διατεταγμένες βάσεις των F και F' αντίστοιχα$\big)$. Τότε

$$F'/\mathrm{Im}f \;\cong\; M_1 \oplus M_2 \oplus \cdots \oplus M_n,$$

όπου $M_i = (x_i)$ κυκλικό R-πρότυπο και αν $Ann(x_i) = \delta_i$, για $i = 1, 2, \ldots, n$, τότε $\delta_i \mid \delta_{i+1}$, για κάθε $i = 1, 2, \ldots, n-1$.
ΑΠΟΔΕΙΞΗ: Από τα προηγούμενα προκύπτει ότι υπάρχουν διατεταγμένες βάσεις $\hat{u}' = (u'_1, u'_2, \ldots, u'_m)$ και $\hat{v}' = (v'_1, v'_2, \ldots, v'_n)$ των F και F' αντίστοιχα έτσι, ώστε $f(u'_j) = \delta_j v'_j$, για κάθε $j = 1, 2, \ldots, \kappa$, όπου $\kappa = \min\{m, n\}$ και $f(u'_j) = 0_{F'}$, για κάθε j με $\kappa < j \leq m$, $\big($αν

$m > n = \kappa$). Επίσης $\delta_i \mid \delta_{i+1}$, για κάθε $i = 1, 2, \ldots, \kappa - 1$. Αν $n > \kappa$, θέτουμε $\delta_i = 0_R$, για κάθε i με $\kappa < i \leq n$. Επειδή το 0_R διαιρείται από οποιοδήποτε στοιχείο της R, έχουμε $\delta_i \mid \delta_{i+1}$, για κάθε $i = 1, 2, \ldots, n-1$.
Επομένως $\mathrm{Im}f = R\delta_1 v_1' \oplus R\delta_2 v_2' \oplus \cdots \oplus R\delta_n v_n' = R\delta_1 v_1' \oplus R\delta_2 v_2' \oplus \cdots \oplus R\delta_\kappa v_\kappa'$. Συνεπώς

$$F'/\mathrm{Im}f = \bigoplus_{i=1}^{n} Rv_i' \Big/ \bigoplus_{i=1}^{\kappa} R\delta_i v_i' \cong \left(\bigoplus_{i=1}^{\kappa} Rv_i' \Big/ \bigoplus_{i=1}^{\kappa} R\delta_i v_i'\right) \oplus \left(\bigoplus_{\kappa<i\leq n} Rv_i'\right) \cong$$
$$\cong \left(\bigoplus_{i=1}^{\kappa} Rv_i'/R\delta_i v_i'\right) \oplus \left(\bigoplus_{\kappa<i\leq n} Rv_i'\right) = \left(\bigoplus_{i=1}^{\kappa} R(v_i' + (\delta_i)v_i')\right) \oplus \left(\bigoplus_{\kappa<i\leq n} Rv_i'\right).$$

Θέτουμε $x_i = v_i' + (\delta_i)v_i'$, για κάθε $i = 1, 2, \ldots, \kappa$ και $x_i = v_i'$ για κάθε i με $\kappa < i \leq n$. Εξυπακούεται ότι το άθροισμα $\bigoplus_{\kappa<i\leq n} Rv_i'$ είναι μηδενικό αν $\kappa = n$.
(Το ότι $Rv_i'/R\delta_i v_i' \cong R/(\delta_i)$, για κάθε $i = 1, 2, \ldots, \kappa$ προκύπτει αν θεωρήσουμε την απεικόνιση $\varphi_i : R \to Rv_i'/R\delta_i v_i'$ με $\varphi_i(r) = rv_i' + R\delta_i v_i' = rv_i' + (\delta_i)v_i'$, για κάθε $r \in R$. Εύκολα αποδεικνύεται ότι η φ_i είναι R-γραμμική και επειδή $\varphi_i(1_R) = v_i' + (\delta_i)v_i'$, το οποίο παράγει το R-πρότυπο $Rv_i'/R\delta_i v_i'$, η φ_i είναι επιμορφισμός. Τώρα, $r \in \mathrm{Ker}\varphi_i \Leftrightarrow \varphi(r) = rv_i' + (\delta_i)v_i' = 0_{Rv_i'/(\delta_i)v_i'} = (\delta_i)v_i' = R\delta_i v_i'$. Ισοδύναμα, υπάρχει $s \in R$ τέτοιο, ώστε $rv_i' = s\delta_i v_i' \Leftrightarrow (r - s\delta_i)v_i' = 0_{F'}$. Το v_i' είναι R-γραμμικά ανεξάρτητο, ως στοιχείο της βάσης του F' και συνεπώς $r = s\delta_i \in (\delta_i)$. Άρα $\mathrm{Ker}\varphi_i = (\delta_i)$). ■

ΜΙΑ ΣΗΜΑΝΤΙΚΗ ΠΑΡΑΤΗΡΗΣΗ: Τα εμφανιζόμενα κυκλικά υποπρότυπα $M_1, M_2, \ldots, M_n$, όπου $n = \mathrm{rank}F'$ στην πραγματικότητα δεν είναι εν γένει n το πλήθος. Πράγματι, αν $\delta_1, \delta_2, \ldots, \delta_t$ είναι αντιστρέψιμα στοιχεία της R, τότε $M_i = Rv_i'/R\delta_i v_i' = Rv_i'/Rv_i' = \{0\}$, το μηδενικό υποπρότυπο, για κάθε $i = 1, 2, \ldots, t$. Επομένως τα μη μηδενικά υποπρότυπα M_i είναι $k = n - t$ το πλήθος. Διαγράφοντας λοιπόν τα t πρώτα μηδενικά υποπρότυπα M_i παίρνουμε

$$F'/\mathrm{Im}f \cong M_1' \oplus M_2' \oplus \cdots \oplus M_k',$$

όπου $M_i' = M_{t+i}$, για κάθε $i = 1, 2, \ldots, k$ και $R \supsetneq Ann(M_1') \supseteq Ann(M_2') \supseteq \cdots \supseteq Ann(M_k')$ ή ισοδύναμα $\delta_i' \mid \delta_{i+1}'$, για κάθε $i = 1, 2, \ldots, k-1$, όπου $Ann(M_i') = (\delta_i') = (\delta_{t+i})$ και δ_1' μη αντιστρέψιμο.
Ας δούμε τέσσερα άλλα παραδείγματα:

ΠΑΡΑΔΕΙΓΜΑΤΑ 4.7. (i) Θεωρούμε την απεικόνιση $f : \mathbb{Z}^4 \to \mathbb{Z}^3$ με $f(x, y, z, w) = (17x + 39y + 35z + 97w, 16x + 36y + 32z + 92w, 13x + 27y + 23z + 77w)$, για κάθε $(x, y, z, w) \in \mathbb{Z}^4$.
Αν $\hat{u} = (u_1, u_2, u_3, u_4)$ και $\hat{v} = (v_1, v_2, v_3)$ είναι οι συνήθεις βάσεις, δηλαδή $u_1 = (1, 0, 0, 0)$, $u_2 = (0, 1, 0, 0)$, $u_3 = (0, 0, 1, 0)$ και $u_4 = (0, 0, 0, 1)$ και $v_1 = (1, 0, 0)$, $v_2 = (0, 1, 0)$ και $v_3 = (0, 0, 1)$, τότε ο πίνακας της f ως προς τις βάσεις αυτές είναι ο

$$A = (f \mid \hat{u}, \hat{v}) = \begin{pmatrix} 17 & 39 & 35 & 97 \\ 16 & 36 & 32 & 92 \\ 13 & 27 & 23 & 77 \end{pmatrix}$$

Η κανονική μορφή Smith του A θα έχει τη μορφή

$$\begin{pmatrix} \delta_1 & 0 & 0 & 0 \\ 0 & \delta_2 & 0 & 0 \\ 0 & 0 & \delta_3 & 0 \end{pmatrix}$$

και συνεπώς $f(u_4') = 0_{\mathbb{Z}^3}$. Εφαρμόζουμε τον αργόριθμο του Smith και βρίσκουμε πίνακες $X \in \mathbb{Z}^{3\times 3}$ και $Y \in \mathbb{Z}^{4\times 4}$ τέτοιους ώστε ο XAY να έχει τη ζητούμενη μορφή. Είναι

$$X=\begin{pmatrix}1&-1&0\\0&1&0\\3&-4&1\end{pmatrix},\qquad Y=\begin{pmatrix}1&0&3&-5\\-4&1&-4&-3\\4&-1&3&3\\0&0&0&1\end{pmatrix}\quad\text{και}\quad XAY=\begin{pmatrix}1&0&0&0\\0&4&0&0\\0&0&0&0\end{pmatrix}.$$

Η νέα βάση $\hat{v}'=(v_1',v_2',v_3')$ του $\mathbb{Z}^3$ δίνεται από τον πίνακα $(\mathbf{1}_{\mathbb{Z}^3}\mid\hat{v}',\hat{v})=(\mathbf{1}_{\mathbb{Z}^3}\mid\hat{v},\hat{v}')^{-1}=$ $=X^{-1}=\begin{pmatrix}1&-1&0\\0&1&0\\3&-4&1\end{pmatrix}^{-1}=\begin{pmatrix}1&1&0\\0&1&0\\-3&1&1\end{pmatrix}$, δηλαδή $v_1'=(1,0,-3)=v_1-3v_3$, $v_2'=(1,1,1)=$ $=v_1+v_2+v_3$ και $v_3'=(0,0,1)=v_3$. Το πρότυπο-πηλίκο $\mathbb{Z}^3\Big/\mathrm{Im}f$ είναι ισόμορφο με

$$\mathbb{Z}v_1'\Big/\mathbb{Z}v_1'\oplus\mathbb{Z}v_2'\Big/4\mathbb{Z}v_2'\oplus\mathbb{Z}v_3'\Big/0\mathbb{Z}v_3'\;\cong\;\mathbb{Z}\Big/\mathbb{Z}\oplus\mathbb{Z}\Big/4\mathbb{Z}\oplus\mathbb{Z}\Big/(0)\;\cong\;\mathbb{Z}_4\oplus\mathbb{Z}.$$ ■

(ii) Θεωρούμε την απεικόνιση $g:\mathbb{Z}^3\to\mathbb{Z}^4$ με $g(x,y,z)=(76x+36y-12z,12x+6y,60x+$ $+30y-12z,38x+18y-6z)$, για κάθε $(x,y,z)\in\mathbb{Z}^3$.

Αν $\hat{u}=(u_1,u_2,u_3)$ και $\hat{v}=(v_1,v_2,v_3,v_4)$ είναι οι συνήθεις βάσεις, δηλαδή $u_1=(1,0,0)$, $u_2=(0,1,0)$ και $u_3=(0,0,1)$ και $v_1=(1,0,0,0)$, $v_2=(0,1,0,0)$, $v_3=(0,0,1,0)$ και $v_4=(0,0,0,1)$, τότε ο πίνακας της g ως προς τις βάσεις αυτές είναι ο

$$A=(g\mid\hat{u},\hat{v})=\begin{pmatrix}76&36&-12\\12&6&0\\60&30&-12\\38&18&-6\end{pmatrix}$$

Η κανονική μορφή Smith του A θα έχει τη μορφή

$$\begin{pmatrix}\delta_1&0&0\\0&\delta_2&0\\0&0&\delta_3\\0&0&0\end{pmatrix}.$$

Επομένως $\delta_4=0$. Συνεπώς το πρότυπο-πηλίκο $\mathbb{Z}^4\Big/\mathrm{Im}g$ θα έχει έναν τουλάχιστον ευθύ προσθετέο ισόμορφο με το $\mathbb{Z}$.

Τώρα, κατά τα γνωστά υπολογίζουμε την κανονική μορφή Smith του A

$$XAY=\begin{pmatrix}2&0&0\\0&6&0\\0&0&12\\0&0&0\end{pmatrix},\quad\text{όπου}\quad X=\begin{pmatrix}0&0&0&1\\0&1&0&0\\0&-1&-1&0\\1&0&0&-2\end{pmatrix}\quad\text{και}\quad Y=\begin{pmatrix}1&0&3\\-2&1&-6\\0&3&1\end{pmatrix}.$$

Η νέα βάση $\hat{v}'=(v_1',v_2',v_3',v_4')$ του $\mathbb{Z}^4$ δίνεται από τον πίνακα $(\mathbf{1}_{\mathbb{Z}^4}\mid\hat{v}',\hat{v})=(\mathbf{1}_{\mathbb{Z}^4}\mid\hat{v},\hat{v}')^{-1}=$ $=X^{-1}=\begin{pmatrix}0&0&0&1\\0&1&0&0\\0&-1&-1&0\\1&0&0&-2\end{pmatrix}^{-1}=\begin{pmatrix}2&0&0&1\\0&1&0&0\\0&-1&-1&0\\1&0&0&0\end{pmatrix}$, δηλαδή $v_1'=(2,0,0,1)=2v_1+v_4$, $v_2'=(0,1,-1,0)=v_2-v_3$, $v_3'=(0,0,-1,0)=-v_3$ και $v_4'=(1,0,0,0)=v_1$. Το πρότυπο-πηλίκο $\mathbb{Z}^4\Big/\mathrm{Im}g$ είναι ισόμορφο με

$$\mathbb{Z}v_1'\Big/2\mathbb{Z}v_1'\oplus\mathbb{Z}v_2'\Big/6\mathbb{Z}v_2'\oplus\mathbb{Z}v_3'\Big/12\mathbb{Z}v_3'\oplus\mathbb{Z}v_4'\Big/0\mathbb{Z}v_4'\;\cong\;\mathbb{Z}\Big/2\mathbb{Z}\oplus\mathbb{Z}\Big/6\mathbb{Z}\oplus\mathbb{Z}\Big/12\mathbb{Z}\oplus\mathbb{Z}\Big/(0)\;\cong$$
$$\cong\mathbb{Z}_2\oplus\mathbb{Z}_6\oplus\mathbb{Z}_{12}\oplus\mathbb{Z}.$$ ■

(iii) Έστω $R=\mathbb{R}[x]$. Θεωρούμε τον $\mathbb{R}[x]$-ομομορφισμό $h:\mathbb{R}[x]^3\to\mathbb{R}[x]^3$ με

$$\begin{cases} g(1,0,0) = (x^2+x-2, x^3-6x-4, x^3-3x+2) \\ g(0,1,0) = (x^2-4, x^3-x^2-8x-4, x^3-x^2-4x+4) \\ g(0,0,1) = (x^2+5x+6, x^3+5x^2+6x, x^3+4x^2+x-6) \end{cases}$$

Αν $\hat{u} = (u_1, u_2, u_3)$ είναι η συνήθης βάση, δηλαδή $u_1 = (1,0,0)$, $u_2 = (0,1,0)$ και $u_3 = (0,0,1)$ $\big(1$ το σταθερό πολυώνυμο$\big)$, τότε ο πίνακας της h ως προς τη βάση αυτή είναι ο

$$A = (h \mid \hat{u}, \hat{u}) = \begin{pmatrix} x^2+x-2 & x^2-4 & x^2+5x+6 \\ x^3-6x-4 & x^3-x^2-8x-4 & x^3+5x^2+6x \\ x^3-3x+2 & x^3-x^2-4x+4 & x^3+4x^2+x-6 \end{pmatrix}$$

Η κανονική μορφή Smith του A είναι

$$XAY = \begin{pmatrix} x+2 & 0 & 0 \\ 0 & (x+2)^2 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

όπου $X = \begin{pmatrix} -1 & 0 & 0 \\ x & -1 & 0 \\ x-1 & 0 & -1 \end{pmatrix}$ και $Y = \begin{pmatrix} -1 & 2-x & -x-3 \\ 1 & x-1 & x+3 \\ 0 & 0 & 1 \end{pmatrix}$. $\big($Οι πράξεις έγιναν με το ελεύθερο λογισμικό Maxima$\big)$.

Η νέα βάση $\hat{u}' = (u_1', u_2', u_3')$ του $\mathbb{R}[x]^3$ δίνεται από τον πίνακα $(\mathbf{1}_{\mathbb{R}[x]^3} \mid \hat{u}', \hat{u}) = (\mathbf{1}_{\mathbb{R}[x]^3} \mid \hat{u}, \hat{u}')^{-1} =$ $= X^{-1} = \begin{pmatrix} -1 & 0 & 0 \\ x & -1 & 0 \\ x-1 & 0 & -1 \end{pmatrix}^{-1} = \begin{pmatrix} -1 & 0 & 0 \\ -x & -1 & 0 \\ 1-x & 0 & -1 \end{pmatrix}$, δηλαδή $u_1' = (-1, -x, 1-x) =$ $= -u_1 - xu_2 + (1-x)u_3$, $u_2' = (0,-1,0) = -u_2$ και $u_3' = (0,0,-1) = -u_3$. Το πρότυποπηλίκο $\mathbb{R}[x]^3 \Big/ \mathrm{Im}h$ είναι ισόμορφο με

$$\mathbb{R}[x] \Big/ (x+2) \oplus \mathbb{R}[x] \Big/ \big((x+2)^2\big) \oplus \mathbb{R}[x]. \qquad \blacksquare$$

(iv) Δίνεται ο πίνακας-στήλη $A = \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_k \end{pmatrix}$, όπου ένας μέγιστος κοινός διαιρέτης των $r_1, r_2, \ldots, r_k$ είναι το 1_R. Να αποδειχθεί ότι η στήλη αυτή είναι η πρώτη στήλη ενός αντιστρέψιμου στο R $k \times k$ πίνακα.

ΑΠΟΔΕΙΞΗ: Αν εφαρμόσουμε τον αλγόριθμο Smith στον πίνακα A, θα βρούμε αντιστρέψιμους $k \times k$ και 1×1 πίνακες X και Y αντίστοιχα τέτοιους, ώστε $XAY = \begin{pmatrix} 1_R \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. Ένας αντιστρέψιμος 1×1 πίνακας Y είναι στην ουσία ένα αντιστρέψιμο στοιχείο u του R. Επομένως θα έχουμε: $X \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_k \end{pmatrix} (u) = (uX) \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_k \end{pmatrix} = X' \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_k \end{pmatrix} = \begin{pmatrix} 1_R \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, όπου ο $X' = uX$ είναι προφανώς αντιστρέψιμος. Συνεπώς $\begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_k \end{pmatrix} = X'^{-1} \begin{pmatrix} 1_R \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, η οποία είναι η πρώτη στήλη του αντιστρέψιμου πίνακα

X'^{-1}. ■

Τώρα εξετάζουμε ένα κεντρικής σημασίας θέμα. Γνωρίζουμε ότι αν M είναι ένα πεπερασμένα R-παραγόμενο πρότυπο, όπου R περιοχή κυρίων ιδεωδών, τότε το M είναι ισόμορφο με το πηλίκο F/F' δύο ελεύθερων R-προτύπων. (Θεώρημα 3.53). Επίσης, από την πρόταση 3.51, rank$F' \leq$ rank$F$. Για να είμαστε όμως σύμφωνοι με τον συμβολισμό αυτής της παραγράφου, ας συμβολίζουμε το «μεγάλο» πρότυπο με F' και το «μικρό» με F. Έτσι, αναδιατυπώνουμε τα αποτελέσματα του θεωρήματος 3.53 και της πρότασης 3.51 εναλλάσσοντας τους συμβολισμούς F και F':
Κάθε πεπερασμένα παραγόμενο R-πρότυπο M, όπου R περιοχή κυρίων ιδεωδών, είναι ισόμορφο με το πηλίκο F'/F δύο ελεύθερων R-προτύπων F και F', όπου $F \leqslant F'$ και άρα rank$F \leq$ $\leq$ rankF'.
Αν λοιπόν στην πρόταση 4.5 αντικαταστήσουμε την f με την εμφύτευση $i : F \hookrightarrow F'$ παίρνουμε αυτομάτως τη δομή του $M \cong F'/F$ ως ευθύ άθροισμα κυκλικών υποπροτύπων. Με βάση λοιπόν και την παρατήρηση μετά την πρόταση 4.5, παίρνουμε το ακόλουθο συμπέρασμα:

ΠΡΟΤΑΣΗ 4.8. Έστω M ένα πεπερασμένα παραγόμενο R-πρότυπο, όπου R περιοχή κυρίων ιδεωδών. Τότε το M είναι ίσο με το ευθύ άθροισμα (πεπερασμένου πλήθους) κυκλικών υποπροτύπων του
$$(x_1) \oplus (x_2) \oplus \cdots \oplus (x_k),$$
όπου $R \supsetneq Ann(x_1) \supseteq Ann(x_2) \supseteq \cdots \supseteq Ann(x_k)$.

Το όλο πρόβλημα ανάγεται λοιπόν στον αλγόριθμο του Smith. **Προσοχή όμως! Ο πίνακας A της εμφύτευσης $i : F \hookrightarrow F'$ είναι γνωστός μόνον αν γνωρίζουμε μια βάση του υποπροτύπου F**. Αλλά το πρόβλημα αυτό ξεπερνιέται όπως στο παράδειγμα 4.1.(i). Εκεί είχαμε τον πίνακα $A = \begin{pmatrix} 42 & 16 & 20 \\ 10 & 10 & 6 \end{pmatrix}$. Με άλλα λόγια είχαμε ένα υποπρότυπο F του $\mathbb{Z}^2$, το οποίο παράγεται από τα στοιχεία $(42, 10)$, $(16, 10)$ και $(20, 6)$. Ξέρουμε ότι ο βαθμός αυτού του υποπροτύπου F είναι μικρότερος ή ίσος του βαθμού του $\mathbb{Z}^2$, δηλαδή του 2. Αλλά δεν έχουμε συγκεκριμένη βάση του F. Το όλο πρόβλημα ξεπερνιέται αν θεωρήσουμε ότι το F είναι η εικόνα Imf μιας απεικόνισης $f : \mathbb{Z}^3 \to \mathbb{Z}^2$ με πίνακα τον A.
Είδαμε ότι $\begin{pmatrix} 0 & -1 \\ 1 & -12 \end{pmatrix} \begin{pmatrix} 42 & 16 & 20 \\ 10 & 10 & 6 \end{pmatrix} \begin{pmatrix} 0 & -1 & -2 \\ 1 & -2 & -1 \\ -2 & 5 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 26 & 0 \end{pmatrix}$. Αυτό σημαίνει ότι το F έχει βάση τα στοιχεία $2v'_1$ και $26v'_2$, όπου (v'_1, v'_2) η νέα βάση του $\mathbb{Z}^2$, η οποία δίνεται συναρτήσει της παλιάς $(v_1 = (1, 0), v_2 = (0, 1))$ βάσει του $X^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & -12 \end{pmatrix}^{-1} = \begin{pmatrix} -12 & 1 \\ -1 & 0 \end{pmatrix}$.
Δηλαδή $v'_1 = -12v_1 - v_2$ και $v'_2 = v_1$. Επομένως το F έχει βάση τα στοιχεία $2v'_1 = -24v_1 - 2v_2 =$ $= (-24, -2)$ και $26v'_2 = 26v_1 = (26, 0)$.
Το δε πρότυπο-πηλίκο $\mathbb{Z}^2/F$ είναι ισόμορφο με το $\mathbb{Z}_2 \oplus \mathbb{Z}_{26}$. «Δηλαδή, με ένα σμπάρο δυο τρυγόνια».

Στα επόμενα παρουσιάζονται μερικά ακόμα αριθμητικά παραδείγματα.

ΠΑΡΑΔΕΙΓΜΑΤΑ 4.9. (i) Έστω G μια αβελιανή ομάδα που παράγεται από τα στοιχεία α, β, τα

οποία ικανοποιούν τις συνθήκες

$$\begin{cases} 2\alpha + 3\beta = 0 \\ \alpha - 7\beta = 0 \end{cases}$$

Να βρεθεί η τάξη και η δομή της ομάδας.

ΛΥΣΗ: Η G είναι επιμορφική εικόνα του ευθέος αθροίσματος $\mathbb{Z}\oplus\mathbb{Z} = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$, όπου $e_1 = (1,0)$ και $e_2 = (0,1)$. Αν $f : \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \to G$ ο επιμορφισμός, $f(e_1) = \alpha$ και $f(e_2) = \beta$. Από τις παραπάνω σχέσεις προκύπτει ότι πυρήνας του επιμορφισμού είναι το υποπρότυπο του $\mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ που παράγεται από τα στοιχεία $v_1 = 2e_1 + 3e_2 = (2,3)$ και $v_2 = e_1 - 7e_2 = (1,-7)$. Σχηματίζουμε τον πίνακα

$$\begin{pmatrix} 2 & 1 \\ 3 & -7 \end{pmatrix}$$

και εφαρμόζουμε σε αυτόν τον αλγόριθμο του Smith. Έχουμε $\begin{pmatrix} 2 & 1 \\ 3 & -7 \end{pmatrix} \overset{\Sigma_1 \leftrightarrow \Sigma_2}{\longrightarrow} \begin{pmatrix} 1 & 2 \\ -7 & 3 \end{pmatrix} \overset{\Gamma_2 \to \Gamma_2 + 7\Gamma_1}{\longrightarrow} \begin{pmatrix} 1 & 2 \\ 0 & 17 \end{pmatrix} \overset{\Sigma_2 \to \Sigma_2 - 2\Sigma_1}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & 17 \end{pmatrix}$. Ο πίνακας αλλαγής βάσης του πυρήνα είναι $Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$ και όλου του $\mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ είναι $X = \begin{pmatrix} 1 & 0 \\ 7 & 1 \end{pmatrix}$. Πράγματι, $\begin{pmatrix} 1 & 0 \\ 7 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 3 & -7 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$.

Κατά συνέπεια $G \cong \mathbb{Z}\Big/_{\mathbb{Z}} \oplus \mathbb{Z}\Big/_{17\mathbb{Z}} \cong 0 \oplus \mathbb{Z}_{17} = \mathbb{Z}_{17}$, κυκλική με 17 στοιχεία. Ο πίνακας $X^{-1} = \begin{pmatrix} 1 & 0 \\ 7 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -7 & 1 \end{pmatrix}$ είναι ο πίνακας $(\mathbf{1}_{\mathbb{Z}\oplus\mathbb{Z}} \mid \hat{e}', \hat{e})$, ο οποίος μας δίνει τη νέα βάση $(e_1', e_2') = (e_1 - 7e_2, e_2)$ του $\mathbb{Z} \oplus \mathbb{Z}$ συναρτήσει της παλαιάς (e_1, e_2).

Ο πίνακας $Y = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = (\mathbf{1}_{\mathrm{Ker}f} \mid \hat{v}', \hat{v})$ μας δίνει την νέα βάση (v_1', v_2') του $\mathrm{Ker}f$ συναρτήσει της παλαιάς βάσης $(v_1 = 2e_1 + 3e_2, v_2 = e_1 - 7e_2)$. Επομένως $(v_1', v_2') = (v_2, v_1 - 2v_2) = = (e_1 - 7e_2, 2e_1 + 3e_2 - 2(e_1 - 7e_2)) = (e_1 - 7e_2, 17e_2) = (e_1', 17e_2')$, όπως αναμενόταν. ■

(ii) Να βρεθεί η δομή του πηλίκου $\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\Big/_{\mathrm{Im}g}$, όπου g η απεικόνιση $g : \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z} \to \to \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}$, με $g(x,y,z) = (-114x - 36y + 231z, -12x + 21z, 27x + 9y - 54z)$, για κάθε $(x,y,z) \in \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z} \cong \mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$.

ΛΥΣΗ: Ο πίνακας της g ως προς τη συνήθη βάση $\hat{e} = (e_1, e_2, e_3)$ είναι ο

$$\begin{pmatrix} -114 & -12 & 27 \\ -36 & 0 & 9 \\ 231 & 21 & -54 \end{pmatrix}$$

Εφαρμόζουμε τον αλγόριθμο του Smith: $\begin{pmatrix} -114 & -12 & 27 \\ -36 & 0 & 9 \\ 231 & 21 & -54 \end{pmatrix} \overset{\Gamma_1 \to \Gamma_1 - 3\Gamma_2}{\longrightarrow} \begin{pmatrix} -6 & -12 & 0 \\ -36 & 0 & 9 \\ 231 & 21 & -54 \end{pmatrix}$
$\overset{\Gamma_1 \to -\Gamma_1}{\longrightarrow} \begin{pmatrix} 6 & 12 & 0 \\ -36 & 0 & 9 \\ 231 & 21 & -54 \end{pmatrix} \overset{\Gamma_2 \to \Gamma_2 + 6\Gamma_1}{\longrightarrow} \begin{pmatrix} 6 & 12 & 0 \\ 0 & 72 & 9 \\ 231 & 21 & -54 \end{pmatrix} \overset{\Sigma_1 \to \Sigma_1 + \Sigma_3}{\longrightarrow} \begin{pmatrix} 6 & 12 & 0 \\ 9 & 72 & 9 \\ 177 & 21 & -54 \end{pmatrix} \overset{\Gamma_2 \to \Gamma_2 - \Gamma_1}{\longrightarrow}$
$\begin{pmatrix} 6 & 12 & 0 \\ 3 & 60 & 9 \\ 177 & 21 & -54 \end{pmatrix} \overset{\Gamma_1 \to \Gamma_1 - \Gamma_2}{\longrightarrow} \begin{pmatrix} 3 & -48 & -9 \\ 3 & 60 & 9 \\ 177 & 21 & -54 \end{pmatrix} \overset{\Gamma_2 \to \Gamma_2 - \Gamma_1}{\longrightarrow} \begin{pmatrix} 3 & -48 & -9 \\ 0 & 108 & 18 \\ 177 & 21 & -54 \end{pmatrix} \overset{\Gamma_3 \to \Gamma_3 - 59\Gamma_1}{\longrightarrow}$
$\begin{pmatrix} 3 & -48 & -9 \\ 0 & 108 & 18 \\ 0 & 2853 & 477 \end{pmatrix} \overset{\Sigma_2 \to \Sigma_2 + 16\Sigma_1}{\longrightarrow} \begin{pmatrix} 3 & 0 & -9 \\ 0 & 108 & 18 \\ 0 & 2853 & 477 \end{pmatrix} \overset{\Sigma_3 \to \Sigma_3 + 3\Sigma_1}{\longrightarrow} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 108 & 18 \\ 0 & 2853 & 477 \end{pmatrix} \overset{\Sigma_2 \to \Sigma_2 - 6\Sigma_3}{\longrightarrow}$

$\begin{pmatrix}3&0&0\\0&0&18\\0&-9&477\end{pmatrix} \overset{\Gamma_2\leftrightarrow\Gamma_3}{\longrightarrow} \begin{pmatrix}3&0&0\\0&-9&477\\0&0&18\end{pmatrix} \overset{\Sigma_3\to\Sigma_3+53\Sigma_2}{\longrightarrow} \begin{pmatrix}3&0&0\\0&-9&0\\0&0&18\end{pmatrix} \overset{\Gamma_2\to-\Gamma_2}{\longrightarrow} \begin{pmatrix}3&0&0\\0&9&0\\0&0&18\end{pmatrix}$.

Επομένως $\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\big/_{\mathrm{Im}g} \cong \mathbb{Z}_3\oplus\mathbb{Z}_9\oplus\mathbb{Z}_{18}$. ■

(iii) Έστω $M\subseteq\mathbb{Z}^3$ το σύνολο των ακεραίων λύσεων του συστήματος

$$\begin{cases}-3x+5y+3z=0\\-6x+20y+9z=0\\-3x+25y+9z=0\end{cases}$$

Να βρεθεί η δομή της ομάδας πηλίκο $\mathbb{Z}^3\big/_M$.

ΛΥΣΗ: Παρατηρούμε ότι $M=\mathrm{Ker}f$, όπου $f:\mathbb{Z}^3\to\mathbb{Z}^3$ με $f(x,y,z)=(-3x+5y+3z,-6x+$ $+20y+9z,\ -3x+25y+9z)$, για κάθε $(x,y,z)\in\mathbb{Z}^3$. Επομένως $f(e_1)=f(1,0,0)=$ $=(-3,-6,-3)=-3e_1-6e_2-3e_3$ και αντίστοιχα $f(e_2)=5e_1+20e_2+25e_3$ και $f(e_3)=$ $=3e_1+9e_2+9e_3$, όπου $\hat{e}=(e_1,e_2,e_3)$ η συνήθης βάση του $\mathbb{Z}^3$. Ο πίνακας $(f\mid\hat{e},\hat{e})$ είναι λοιπόν

$$\begin{pmatrix}-3&5&3\\-6&20&9\\-3&25&9\end{pmatrix}$$

Εφαρμόζουμε τον αλγόριθμο Smith: $\begin{pmatrix}-3&5&3\\-6&20&9\\-3&25&9\end{pmatrix} \overset{\Sigma_2\to\Sigma_2+\Sigma_1}{\longrightarrow} \begin{pmatrix}-3&2&3\\-6&14&9\\-3&22&9\end{pmatrix} \overset{\Sigma_1\to\Sigma_1+\Sigma_2}{\longrightarrow}$

$\begin{pmatrix}-1&2&3\\8&14&9\\19&22&9\end{pmatrix} \overset{\Gamma_2\to\Gamma_2+8\Gamma_1}{\longrightarrow} \begin{pmatrix}-1&2&3\\0&30&33\\19&22&9\end{pmatrix} \overset{\Gamma_3\to\Gamma_3+19\Gamma_1}{\longrightarrow} \begin{pmatrix}-1&2&3\\0&30&33\\0&60&66\end{pmatrix} \overset{\Sigma_2\to\Sigma_2+2\Sigma_1}{\longrightarrow}$

$\begin{pmatrix}-1&0&3\\0&30&33\\0&60&66\end{pmatrix} \overset{\Sigma_3\to\Sigma_3+3\Sigma_1}{\longrightarrow} \begin{pmatrix}-1&0&0\\0&30&33\\0&60&66\end{pmatrix} \overset{\Gamma_1\to-\Gamma_1}{\longrightarrow} \begin{pmatrix}1&0&0\\0&30&33\\0&60&66\end{pmatrix} \overset{\Sigma_3\to\Sigma_3-\Sigma_2}{\longrightarrow} \begin{pmatrix}1&0&0\\0&30&3\\0&60&6\end{pmatrix} \overset{\Sigma_2\to\Sigma_2-10\Sigma_3}{\longrightarrow}$

$\begin{pmatrix}1&0&0\\0&0&3\\0&0&6\end{pmatrix} \overset{\Sigma_2\leftrightarrow\Sigma_3}{\longrightarrow} \begin{pmatrix}1&0&0\\0&3&0\\0&6&0\end{pmatrix} \overset{\Gamma_3\to\Gamma_3-2\Gamma_2}{\longrightarrow} \begin{pmatrix}1&0&0\\0&3&0\\0&0&0\end{pmatrix}$. Επομένως, ως προς κατάλληλες βάσεις $\hat{u}=(u_1,u_2,u_3)$ και $\hat{v}=(v_1,v_2,v_3)$ του $\mathbb{Z}^3$ ο πίνακας της $f:\mathbb{Z}^3\to\mathbb{Z}^3$ είναι ο πίνακας $\begin{pmatrix}1&0&0\\0&3&0\\0&0&0\end{pmatrix}$.

Από τη μορφή του πίνακα αυτού προκύπτει ότι $M=\mathrm{Ker}f=\mathbb{Z}u_3$, δηλαδή ελεύθερο πρότυπο βαθμού 1. Αυτό το περιμέναμε βάσει της πρότασης 3.51. (Υποπρότυπο ελεύθερου προτύπου είναι ελεύθερο). Τώρα $\mathbb{Z}^3\big/_M \cong \mathrm{Im}f = \mathbb{Z}v_1\oplus\mathbb{Z}(3v_2)\cong\mathbb{Z}\oplus\mathbb{Z}$.

Θα μπορούσαμε βέβαια να λύσουμε στο $\mathbb{Z}$ το παραπάνω σύστημα:

$\begin{cases}-3x&+5y&+3z&=0\\-6x&+20y&+9z&=0\\-3x&+25y&+9z&=0\end{cases} \Leftrightarrow \begin{cases}-3x&+5y&+3z&=0\\&10y&+3z&=0\\&20y&+6z&=0\end{cases} \Leftrightarrow \begin{cases}-3x&+5y&+3z&=0\\&10y&+3z&=0\end{cases} \Leftrightarrow$

$\Leftrightarrow \begin{cases}-3x&-5y&&=0\\&10y&+3z&=0\end{cases} \Leftrightarrow \begin{cases}x=-\frac{5}{3}y\\z=-\frac{10}{3}y\end{cases} \underset{y=3t,\ t\in\mathbb{Z}}{\Leftrightarrow} \begin{cases}x=-5t\\y=3t\\z=-10t\end{cases}$, όπου $t\in\mathbb{Z}$. Επομένως

$M = \mathbb{Z}(-5e_1 + 3e_2 - 10e_3)$. Προφανώς ο πίνακας της εμφύτευσης $M \hookrightarrow \mathbb{Z}^3$ είναι ο $\begin{pmatrix} -5 \\ 3 \\ -10 \end{pmatrix}$. Ο αλγόριθμος Smith μας βγάζει: $\begin{pmatrix} -5 \\ 3 \\ -10 \end{pmatrix} \overset{\Gamma_3 \to \Gamma_3 - 2\Gamma_1}{\longrightarrow} \begin{pmatrix} -5 \\ 3 \\ 0 \end{pmatrix} \overset{\Gamma_1 \to \Gamma_1 + 2\Gamma_2}{\longrightarrow} \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix} \overset{\Gamma_2 \to \Gamma_2 - 3\Gamma_1}{\longrightarrow} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. Από αριστερά έχουμε πολλαπλασιάσει με $X = \begin{pmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 0 \\ -3 & -5 & 0 \\ -2 & 0 & 1 \end{pmatrix}$. Η νέα βάση $\hat{u}' = (u_1', u_2', u_3')$ ως προς την οποία ο πίνακας της εμφύτευσης $M \hookrightarrow \mathbb{Z}^3$ έχει τη μορφή $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ δίνεται συναρτήσει της παλαιάς από τον πίνακα $X^{-1} = \begin{pmatrix} 1 & 2 & 0 \\ -3 & -5 & 0 \\ -2 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} -5 & -2 & 0 \\ 3 & 1 & 0 \\ -10 & -4 & 1 \end{pmatrix}$. Στον προηγούμενο αλγόριθμο Smith η βάση $\hat{u} = (u_1, u_2, u_3)$ του πεδίου ορισμού $\mathbb{Z}^3$ της f προέκυψε με πολλαπλασιασμό από δεξιά με τον πίνακα $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -10 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 & -5 \\ 1 & 0 & 3 \\ 0 & 1 & -10 \end{pmatrix}$ (προσέξτε την τελευταία στήλη) και από δεξιά με $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 19 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 8 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 8 & 1 & 0 \\ 3 & -2 & 1 \end{pmatrix}$. Παρατηρούμε ότι $\begin{pmatrix} -1 & 0 & 0 \\ 8 & 1 & 0 \\ 3 & -2 & 1 \end{pmatrix} \begin{pmatrix} -3 & 5 & 3 \\ -6 & 20 & 9 \\ -3 & 25 & 9 \end{pmatrix} \begin{pmatrix} 2 & 1 & -5 \\ 1 & 0 & 3 \\ 0 & 1 & -10 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, το οποίο και αναμενόταν. ■

4.3 Πρότυπα Στρέψεως και Πρότυπα Ελεύθερα Στρέψεως

ΟΡΙΣΜΟΣ 4.10. Έστω M ένα R-πρότυπο. Αν για κάθε **μη μηδενικό** στοιχείο x του M ισχύει $rx \neq 0_M$, για κάθε $r \in R \setminus \{0_R\}$, το M λέγεται **ελεύθερο στρέψεως**. (Torsion-free).
Σημειώνουμε ότι το τετριμμένο πρότυπο $\{0\}$ είναι ελεύθερο στρέψεως. (Σε αντίθετη περίπτωση θα υπήρχε $x \in \{0\}$ με $x \neq 0$ (;;;) και $r \in R \setminus \{0_R\}$, τέτοια ώστε $rx = 0$. Αλλά, αν $x \in \{0\}$, τότε $x = 0$ και κατά συνέπεια δεν υπάρχουν $x \neq 0$).
Έστω M ένα μη μηδενικό R-πρότυπο. Αν για κάθε μη μηδενικό στοιχείο x του M υπάρχει $r \in R \setminus \{0_R\}$ τέτοιο, ώστε $rx = 0_M$, τότε το M λέγεται **πρότυπο στρέψεως**. (Torsion module).
Αν M είναι ένα R-πρότυπο, το σύνολο $T(M) = \{x \in M \mid rx = 0_M, \text{ για κάποιο } r \in R \setminus \{0_R\}\}$ λέγεται **υποπρότυπο στρέψεως** του M. **Σημειώνουμε ότι το $T(M)$ δεν είναι κατ' ανάγκην πρότυπο στρέψεως**. Για να είναι πρότυπο στρέψεως θα πρέπει $T(M) \neq \{0\}$.

ΠΡΟΤΑΣΗ 4.11. Έστω M ένα R-πρότυπο, όπου R ακέραια περιοχή. Τότε το $T(M)$ είναι όντως υποπρότυπο του M. Επίσης, το M είναι ελεύθερο στρέψεως αν και μόνον αν $T(M) = \{0_M\}$. Ακόμη, $T\left(M/T(M)\right) = \{0_{M/T(M)}\}$, δηλαδή το $M/T(M)$ είναι ελεύθερο στρέψεως.

ΑΠΟΔΕΙΞΗ: Έστω $x_1, x_2 \in T(M)$. Τότε υπάρχουν $r_1, r_2 \neq 0_R$ τέτοια, ώστε $r_1x_1 = r_2x_2 = 0_M$. Οπότε $r_1r_2(x_1+x_2) = r_2(r_1x_1)+r_1(r_2x_2) = r_2\cdot 0_M + r_1\cdot 0_M = 0_M$ και $r_1r_2 \neq 0_R$, γιατί η R είναι ακέραια περιοχή. Συνεπώς $x_1+x_2 \in T(M)$. Έστω τώρα $x \in T(M)$ και $s \in R$. Τότε υπάρχει $r \in R \setminus \{0_R\}$ τέτοιο, ώστε $rx = 0_M$. Επομένως $r(sx) = s(rx) = s\cdot 0_M = 0_M$. Άρα $sx \in T(M)$ και συνεπώς το $T(M)$ είναι υποπρότυπο του M.
Έστω $x+T(M) \in T\Big(M/_{T(M)}\Big)$. Τότε υπάρχει $r_1 \neq 0_R$ τέτοιο, ώστε $r_1(x+T(M)) = 0_{M/T(M)} = = T(M)$, δηλαδή $r_1x \in T(M)$. Αλλά τότε θα υπάρχει $r_2 \neq 0_R$ με $r_2r_1x = 0_M$ και $r_2r_1 \neq 0_R$, επειδή η R είναι ακέραια περιοχή. Άρα $x \in T(M) \Leftrightarrow x+T(M) = T(M)$. ■

ΠΡΟΤΑΣΗ 4.12. (i) Κάθε πεπερασμένα παραγόμενο ελεύθερο R-πρότυπο, όπου R ακέραια περιοχή, είναι ελεύθερο στρέψεως.
(ii) Αν R είναι περιοχή κυρίων ιδεωδών, τότε κάθε πεπερασμένα παραγόμενο ελεύθερο στρέψεως πρότυπο F είναι ελεύθερο.
ΑΠΟΔΕΙΞΗ: (i) Έστω $F = Ru_1 \oplus Ru_2 \oplus \cdots \oplus Ru_k$ ελεύθερο R-πρότυπο με βάση $\{u_1, u_2, \ldots, u_k\}$ και $r_1u_1 + r_2u_2 + \cdots + r_ku_k \in T(F)$. Έστω $r \in R \setminus \{0_R\}$ τέτοιο, ώστε $r(r_1u_1 + r_2u_2 + + \cdots + r_ku_k) = rr_1u_1 + rr_2u_2 + \cdots + rr_ku_k = 0_F$. Επειδή το F είναι ελεύθερο έπεται ότι $rr_i = 0_R$, για κάθε $i = 1, 2 \ldots, k$ και επειδή η R είναι ακέραια περιοχή και $r \neq 0_R$, έπεται ότι $r_1 = r_2 = \cdots = r_k = 0_R$.
(ii) 1ος τρόπος: Σύμφωνα με την πρόταση 4.8, $F = (x_1) \oplus (x_2) \oplus \cdots \oplus (x_k)$, όπου $R \supsetneq \supsetneq Ann(x_1) \supseteq Ann(x_2) \supseteq \cdots \supseteq Ann(x_k)$. Παρατηρούμε ότι $x_i \neq 0_F$ γιατί $1_R \cdot 0_F = 0_F$ και άρα, αν $x_i = 0_F$, θα είχαμε $Ann(x_i) = (1_R) = R$, άτοπο. Επομένως $Ann(x_i) = \{0_R\}$, γιατί το F είναι ελεύθερο στρέψεως. Το αποτέλεσμα προκύπτει από το (ii) της πρότασης 3.40.
2ος τρόπος: Εφαρμόζουμε επαγωγή στο πλήθος των (μη μηδενικών) γεννητόρων $x_1, x_2, \ldots, x_n$ του F. Αν $F = Rx_1$, τότε το F είναι ελεύθερο με βάση $\{x_1\}$. Έστω $n > 1$ και υποθέτουμε ότι ο ισχυρισμός είναι σωστός αν το πλήθος των γεννητόρων είναι μικρότερο του n. Θέτουμε $H = \{x \in F \mid rx \in Rx_n$ για κάποιο $r \in R \setminus \{0_R\}\}$. Το H είναι υποπρότυπο του F. Πράγματι, αν $x, y \in H$, τότε $rx, sy \in Rx_n$, για κάποια $r, s \in R\setminus\{0_R\}$. Επομένως $rs(x+y) = s(rx)+r(sy) \in \in Rx_n$ και $rs \neq 0_R$, γιατί το R είναι ακέραια περιοχή. Άρα $x+y \in H$. Επίσης, αν $x \in H$, τότε υπάρχει $r \neq 0_R$ με $rx \in Rx_n$. Αν $s \in R$, τότε $r(sx) = s(rx) \in sRx_n \subseteq Rx_n$. Συνεπώς $sx \in H$.
Έστω $F' = F/_H$. Επειδή προφανώς το x_n ανήκει στο H, το F' παράγεται από τα $x_1+H, x_2+H,$ $\ldots, x_{n-1}+H$, δηλαδή από λιγότερους από n γεννήτορες. Επίσης το F' είναι ελεύθερο στρέψεως. Πράγματι, αν $r \neq 0_R$ και $x+H \in F/_H$, με $rx \in H$, τότε θα υπήρχε $s \neq 0_R$ τέτοιο, ώστε $(sr)x = s(rx) \in Rx_n \underset{sr\neq 0_R}{\Rightarrow} x \in H \Leftrightarrow x+H = 0_{F/H} = H$. Από την επαγωγική υπόθεση το $F/_H$ είναι ελεύθερο. Τότε, από την πρόταση 3.50 προκύπτει ότι $F = H \oplus F''$, όπου $F'' \cong F'$. Επειδή η R είναι περιοχή κυρίων ιδεωδών, από το πόρισμα 3.52 προκύπτει ότι και το H είναι πεπερασμένα παραγόμενο. Επομένως $H = Ry_1 + Ry_2 + \cdots + Ry_t$. Για κάθε y_i υπάρχει λοιπόν $r_i \neq 0_R$ τέτοιο, ώστε $r_iy_i \in Rx_n$, για κάθε $i = 1, 2, \ldots, t$. Έστω $r = r_1r_2\cdots r_t \neq 0_R$. Τότε $ry \in Rx_n$, για κάθε $y \in H$. Επομένως $ry = sx_n$, για κάποιο $s \in R$. Το $s \in R$ είναι μοναδικό, δηλαδή αν $ry = sx_n = s'x_n$, τότε $s = s'$. Πράγματι, αν $sx_n = s'x_n$, τότε $(s-s')x_n = 0_M$ και επειδή το F είναι ελεύθερο στρέψεως έπεται ότι $s = s'$.
Ορίζουμε την απεικόνιση $f : H \to R$ με $f(y) = s$, όπου $ry = sx_n$. Όπως είδαμε προηγουμένως, η f είναι καλά ορισμένη. Παρατηρούμε ότι αν $ry = sx_n$ και $ry' = s'x_n$, τότε $r(y+y') = (s+s')x_n$, δηλαδή $f(y+y') = f(y)+f(y')$. Επίσης, αν $ry = sx_n$, τότε $r(r'y) = r'ry = r'sx_n$, δηλαδή $f(r'y) = r's = r'f(y)$. Συνεπώς η $f : H \to R$ είναι R-γραμμική. Αν $y \in \mathrm{Ker}f$, τότε $ry = 0_R \cdot x_n = 0_M$ και επειδή το F είναι ελεύθερο στρέψεως, $y = 0_M$. Άρα η f είναι R-μονομορφισμός. Η εικόνα της $\mathrm{Im}f \cong H$ είναι ένα R-υποπρότυπο του R, δηλαδή ιδεώδες

αυτού. Η R είναι περιοχή κυρίων ιδεωδών, άρα $\text{Im}f = (\delta) = R\delta$, για κάποιο $\delta \in R$. Επειδή $x_n \neq 0_M$ και $x_n \in H \cong R\delta$, έχουμε $\delta \neq 0_R$. Άρα $R\delta$ ελεύθερο με βάση $\{\delta\}$. Επομένως $F \cong R\delta \oplus F''$, ελεύθερο R-πρότυπο. ■

Σχόλιο: Η εμμονή στον φαινομενικά πιο δύσκολο 2ο τρόπο οφείλεται στο γεγονός ότι δεν χρησιμοποιεί τον αλγόριθμο Smith.

ΠΟΡΙΣΜΑ 4.13. Αν R είναι περιοχή κυρίων ιδεωδών, τότε κάθε πεπερασμένα παραγόμενο R-πρότυπο M γράφεται στη μορφή

$$M = T(M) \oplus F,$$

όπου F ελεύθερο R-πρότυπο.

ΑΠΟΔΕΙΞΗ: Θεωρούμε την απεικόνιση $\big($φυσική προβολή$\big)$ $f : M \to {}^{M}\!/_{T(M)}$. Το ${}^{M}\!/_{T(M)}$ είναι ελεύθερο στρέψεως, άρα σύμφωνα με το (ii) της προηγούμενης πρότασης είναι ελεύθερο. Σύμφωνα με την πρόταση 3.50 το M γράφεται στη μορφή $M = \text{Ker}f \oplus F$, όπου F ελεύθερο υποπρότυπο του M ισόμορφο προς το ${}^{M}\!/_{T(M)}$. Προφανώς $\text{Ker}f = T(M)$. ■

4.4 Μοναδικότητα της Ανάλυσης σε Ευθύ Άθροισμα Κυκλικών Υποπροτύπων (Α΄ Μορφή) - Αναλλοίωτοι Παράγοντες

Υπενθυμίζουμε ότι με βάση την πρόταση 4.8 ένα $\big($μη μηδενικό$\big)$ πεπερασμένα παραγόμενο R-πρότυπο M γράφεται στη μορφή

$$M = (x_1) \oplus (x_2) \oplus \cdots \oplus (x_k),$$

με $\delta_i \mid \delta_{i+1}$, για κάθε $i = 1, 2, \ldots, k-1$, όπου θέσαμε $(\delta_i) = Ann(x_i)$, για κάθε $i = 1, 2, \ldots, k$. Επίσης το δ_1, άρα και κάθε δ_i είναι μη αντιστρέψιμο στοιχείο της R.

Τίθεται το ερώτημα: **Είναι η γραφή αυτή μοναδική;** Η απάντηση στο ερώτημα αυτό είναι καταφατική υπό την εξής έννοια: Αν

$$M = (y_1) \oplus (y_2) \oplus \cdots \oplus (y_\mu),$$

με $\delta'_i \mid \delta'_{i+1}$, για κάθε $i = 1, 2, \ldots, \mu-1$, όπου θέσαμε $(\delta'_i) = Ann(y_i)$, για κάθε $i = 1, 2, \ldots, \mu$ και το δ'_1, είναι μη αντιστρέψιμο στοιχείο, τότε $k = \mu$ και $\delta_i \sim \delta'_i$, για κάθε $i = 1, 2, \ldots, k$. Επομένως $(x_i) \cong (y_i)$, για κάθε $i = 1, 2, \ldots, k$.

ΛΗΜΜΑ 4.14. Έστω $M = (x_1) \oplus (x_2) \oplus \cdots \oplus (x_k)$ και $(\delta_i) = Ann(x_i)$, όπως παραπάνω. Τότε το υποπρότυπο στρέψης $T(M)$ του M ισούται με το ευθύ άθροισμα όλων εκείνων των (x_i) για τα οποία $\delta_i \neq 0_R$.

ΑΠΟΔΕΙΞΗ: Αν $\delta_i = 0_R$, για κάθε $i = 1, 2, \ldots, k$, τότε με βάση το (ii) της πρότασης 3.40 το M είναι ελεύθερο και συνεπώς βάσει του (i) της πρότασης 4.11, είναι ελεύθερο στρέψεως. Έστω ν ο μεγαλύτερος δείκτης για τον οποίο $\delta_i \neq 0_R$, για κάθε $i = 1, \ldots, \nu$, όπου $1 \leq \nu \leq k$. Έστω $x = r_1x_1 + r_2x_2 + \cdots + r_\nu x_\nu + \sum_{\nu<i\leq k} r_i x_i$ τυχόν στοιχείο του $T(M)$. $\big($Εννοείται ότι αν $\nu = k$, τότε το άθροισμα $\sum_{\nu<i\leq k} r_i x_i$ θεωρείται μηδενικό$\big)$. Τότε υπάρχει $\delta \neq 0_R$ τέτοιο, ώστε $\delta r_1x_1 + \delta r_2x_2 + \cdots + \delta r_\nu x_\nu + \sum_{\nu<i\leq k} \delta r_i x_i = 0_M$. Επειδή το άθροισμα $(x_1)+(x_2)+\cdots+(x_k)$ είναι ευθύ, παίρνουμε $\delta r_i x_i = 0_M$, για κάθε $i = 1, 2, \ldots, k$. Ειδικότερα, επειδή $Ann(x_i) = \{0_R\}$, για κάθε i με $\nu < i \leq k$ $\big($αν υπάρχουν τέτοια $i\big)$, $\delta r_i = 0 \underset{\delta\neq 0_R}{\Leftrightarrow} r_i = 0_R$, για κάθε i με $\nu < i \leq k$. Επομένως το τυχόν στοιχείο x του $T(M)$ είναι της μορφής $x = r_1x_1 + r_2x_2 + \cdots + r_\nu x_\nu \in (x_1) \oplus (x_2) \oplus \cdots \oplus (x_\nu)$.

Αντιστρόφως, έστω $x = r_1x_1 + r_2x_2 + \cdots + r_\nu x_\nu \in (x_1) \oplus (x_2) \oplus \cdots \oplus (x_\nu)$. Επειδή $(\delta_i) = Ann(x_i)$

και $\delta_i \mid \delta_\nu$, για κάθε $i = 1, 2, \ldots, \nu$, έχουμε $\delta_\nu x_i = 0_M$, για κάθε $i = 1, 2 \ldots, \nu$. Συνεπώς $\delta_\nu x = r_1\delta_\nu x_1 + r_2\delta_\nu x_2 + \cdots + r_\nu\delta_\nu x_\nu = 0_M$. Επειδή $\delta_\nu \neq 0_R$, το x ανήκει στο $T(M)$. ■

ΠΟΡΙΣΜΑ 4.15. Έστω $M = (x_1) \oplus (x_2) \oplus \cdots \oplus (x_k)$ και $(\delta_i) = Ann(x_i)$, όπως παραπάνω. Τότε το ελεύθερο R-πρότυπο $M/T(M)$ (βλέπε πρόταση 4.10 και το (ii) της πρότασης 4.11 ή το πόρισμα 4.12) είναι ισόμορφο με το ευθύ άθροισμα όλων εκείνων των (x_i) για τα οποία $\delta_i = 0_R$. ■

Γνωρίζουμε (πρόταση 3.35.(i)) ότι αν I είναι ένα μέγιστο ιδεώδες ενός δακτυλίου R και M είναι ένα R-πρότυπο, τότε το M/IM καθίσταται R/I -διανυσματικός χώρος.

ΛΗΜΜΑ 4.16. (i) Έστω R περιοχή κυρίων ιδεωδών και p ένα ανάγωγο στοιχείο αυτής. Τότε το (p) είναι μέγιστο ιδεώδες της R και κατά συνέπεια ο δακτύλιος-πηλίκο $R/(p)$ είναι σώμα.
(ii) Έστω R περιοχή κυρίων ιδεωδών και p ένα ανάγωγο στοιχείο αυτής. Αν (x) είναι ένα κυκλικό R-πρότυπο και $(\delta) = Ann(x)$, τότε

$$\dim_{R/(p)} (x)/p\cdot(x) = \dim_{R/(p)} Rx/pRx = \dim_{R/(p)} Rx/(p)x = \begin{cases} 1, & \text{αν } p \mid \delta, \\ 0, & \text{αν } p \nmid \delta \end{cases}$$

ΑΠΟΔΕΙΞΗ: (i) Έστω $r + (p) \in R/(p) \setminus \{0_{R/(p)}\} \Leftrightarrow r \notin (p)$. Θεωρούμε το ιδεώδες $(\alpha) = (r, p)$. Τότε $\alpha \mid p$ και επειδή το p είναι ανάγωγο, το α θα είναι είτε αντιστρέψιμο είτε συντροφικό του p. Αν $\alpha \sim p$, τότε επειδή $\alpha \mid r$, θα είχαμε και $p \mid r \Leftrightarrow r \in (p)$, άτοπο. Άρα το α δεν είναι συντροφικό του p και συνεπώς είναι αντιστρέψιμο. Άρα $(r, p) = (\alpha) = (1_R) = R$. Συνεπώς υπάρχουν $s, t \in R$, τέτοια ώστε $sr + tp = 1_R$ και κατά συνέπεια $sr + (p) = sr + tp + (p) = 1_R + (p) = 1_{R/(p)}$. Δηλαδή $(s + (p))(r + (p)) = 1_{R/(p)}$ και επομένως το $r + (p)$ είναι αντιστρέψιμο στον δακτύλιο $R/(p)$.
(ii) Το $Rx/(Rp)x = Rx/(p)x$ έχει έναν R-γεννήτορα και άρα $R/(p)$-γεννήτορα το $x + (p)x$. Έστω $Rx/(p)x = \{0_{Rx/(p)x}\} = \{(p)x\}$. Τότε $x + (p)x = (p)x \Leftrightarrow x \in (p)x \Leftrightarrow x = rpx$, για κάποιο $r \in R$. Επομένως $(1_R - rp)x = 0_M \Leftrightarrow 1_R - rp \in Ann(x) = (\delta)$. Συνεπώς $1_R - rp = s\delta \Leftrightarrow s\delta + rp = 1_R$, για κάποιο $s \in R$. Αν $p \mid \delta$, τότε $p \mid rp + s\delta = 1_R$, άτοπο. Άρα $p \nmid \delta$.
Αντιστρόφως, έστω ότι $p \nmid \delta$. Αν r είναι ένας μέγιστος κοινός διαιρέτης των p και δ, δηλαδή $(r) = (p, \delta)$, τότε επειδή $r \mid p$ και το p ανάγωγο, το r είναι είτε αντιστρέψιμο είτε συντροφικό του p. Η τελευταία περίπτωση αποκλείεται γιατί αν $p \sim r$, τότε επειδή $r \mid \delta$, θα είχαμε και $p \mid \delta$, άτοπο. Άρα το r είναι αντιστρέψιμο, δηλαδή $(p, \delta) = R$. Επομένως υπάρχουν $y, z \in R$ τέτοια, ώστε $1_R = py + \delta z$. Επομένως $x = 1_R \cdot x = (py + \delta z)x = (yp)x \in (p)x$. Κατά συνέπεια ο $R/(p)$-γεννήτορας $x + (p)x$ του $(x)/(p)x$ είναι μηδέν.
Αυτό που αποδείξαμε είναι $\dim_{R/(p)} (x)/p(x) = 0 \Leftrightarrow p \nmid \delta$.
Επειδή ο $R/(p)$-διανυσματικός χώρος παράγεται από έναν μόνον γεννήτορα, τον $x + (p)x$, θα έχουμε επίσης $\dim_{R/(p)} (x)/p(x) = 1 \Leftrightarrow p \mid \delta$. ■

ΘΕΩΡΗΜΑ 4.17. Κάθε (μη μηδενικό) πεπερασμένα παραγόμενο R-πρότυπο M, όπου R περιοχή κυρίων ιδεωδών αναλύεται σε ευθύ άθροισμα

$$M = (x_1) \oplus (x_2) \oplus \cdots \oplus (x_k)$$

κυκλικών υποπροτύπων, με δ_1 μη αντιστρέψιμο και $\delta_i \mid \delta_{i+1}$, για κάθε $i = 1, 2, \ldots, k-1$, όπου θέσαμε $(\delta_i) = Ann(x_i)$, για κάθε $i = 1, 2, \ldots, k$.
Αν

$$M = (y_1) \oplus (y_2) \oplus \cdots \oplus (y_\mu),$$

με $(\delta'_i) = Ann(y_i)$, για κάθε $i = 1, 2, \ldots, \mu$, έτσι ώστε δ'_1 μη αντιστρέψιμο και $\delta'_i \mid \delta'_{i+1}$, για κάθε $i = 1, 2, \ldots, \mu - 1$, τότε $k = \mu$ και $\delta_i \sim \delta'_i$, για κάθε $i = 1, 2, \ldots, k$.
Επομένως $(x_i) \cong (y_i)$, για κάθε $i = 1, 2, \ldots, k$. Επιπλέον, αν ν είναι ο μεγαλύτερος δείκτης με την ιδιότητα $\delta_\nu \neq 0_R$, τότε $Ann(T(M)) = (\delta_\nu)$.

ΑΠΟΔΕΙΞΗ: Σύμφωνα με το πόρισμα 4.15, το ελεύθερο R-πρότυπο $M/T(M)$ είναι ισόμορφο με το ευθύ άθροισμα F όλων εκείνων των (x_i) για τα οποία $\delta_i = 0_R$. Το ίδιο πρότυπο $M/T(M)$ είναι ισόμορφο με το ευθύ άθροισμα F' όλων εκείνων των (y_j) για τα οποία $\delta'_j = 0_R$. Εφόσον ο βαθμός (rank) ενός ελεύθερου προτύπου είναι ανεξάρτητο της βάσης του, το πλήθος των (x_i), για τα οποία $\delta_i = 0_R$ συμπίπτει με το πλήθος των (y_j), για τα οποία $\delta'_j = 0_R$.
Τώρα, με βάση το πόρισμα 4.12, θα έχουμε $M = T(M) \oplus F = T(M) \oplus F'$. Για να αποδείξουμε ότι $k = \mu$ αρκεί με βάση το λήμμα 4.13 να αποδείξουμε ότι το πλήθος των (x_i) για τα οποία $\delta_i \neq 0_R$ συμπίπτει με το πλήθος των (y_j) για τα οποία $\delta'_j \neq 0_R$.
Έστω λοιπόν $T(M) = (x_1) \oplus \cdots \oplus (x_\nu) = (y_1) \oplus \cdots \oplus (y_\lambda)$. Υποθέτουμε ότι $\nu > \lambda$. Εφόσον δ_1 μη αντιστρέψιμο, θα έχει έναν ανάγωγο παράγοντα p. Τότε $\dim_{R/(p)} \left(T(M) \Big/ pT(M) \right) =$

$$= \dim_{R/(p)} Rx_1 \Big/ (p)x_1 + \cdots + \dim_{R/(p)} Rx_\nu \Big/ (p)x_\nu = \underbrace{1 + 1 + \cdots + 1}_{\nu \text{ φορές}} = \nu,$$

γιατί $p \mid \delta_1 \mid \delta_2 \mid \cdots \mid \delta_\nu$. Κατά συνέπεια

$$\dim_{R/(p)} \left(T(M) \Big/ pT(M) \right) = \nu \Leftrightarrow \dim_{R/(p)} Ry_1 \Big/ (p)y_1 + \cdots + \dim_{R/(p)} Ry_\lambda \Big/ (p)y_\lambda = \nu.$$

Αλλά το τελευταίο άθροισμα στην καλύτερη περίπτωση θα μας δώσει $\lambda < \nu$, αν $p \mid \delta'_1$. Στη χειρότερη, αν $p \nmid \delta'_1$ θα μηδενιστεί ο πρώτος τουλάχιστον όρος και θα μας δώσει τιμή μικρότερη του λ, δηλαδή ακόμη μικρότερη του ν. Επομένως η υπόθεση $\nu > \lambda$ οδηγεί σε άτοπο. Συμμετρικά σκεπτόμενοι και η υπόθεση $\lambda > \nu$ θα μας οδηγήσει σε άτοπο. Επομένως $\nu = \lambda$ και κατά συνέπεια $k = \mu$.
Καταλήξαμε λοιπόν στο αποτέλεσμα ότι $T(M) = (x_1) \oplus (x_2) \oplus \cdots \oplus (x_\nu) = (y_1) \oplus (y_2) \oplus \cdots \oplus (y_\nu)$, όπου $(\delta_i) = Ann(x_i)$, $(\delta'_i) = Ann(y_i)$ με $\delta_i, \delta'_i \neq 0_R$, για κάθε $i = 1, 2, \ldots, \nu$.
Επίσης $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_\nu$ και $\delta'_1 \mid \delta'_2 \mid \cdots \mid \delta'_\nu$, ισοδύναμα $Ann(x_1) \supseteq Ann(x_2) \supseteq \cdots \supseteq Ann(x_\nu)$ και $Ann(y_1) \supseteq Ann(y_2) \supseteq \cdots \supseteq Ann(y_\nu)$.

Παρατήρηση 1η: Αυτό που αποδείξαμε προηγουμένως είναι ότι αν έχουμε ένα πρότυπο στρέψης, το οποίο αναλύεται κατά δύο διαφορετικούς τρόπους σε ευθύ άθροισμα μη μηδενικών κυκλικών υποπροτύπων

$$(x_1) \oplus (x_2) \oplus \cdots \oplus (x_\nu) = (y_1) \oplus (y_2) \oplus \cdots \oplus (y_\lambda)$$

με $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_\nu$ και $\delta'_1 \mid \delta'_2 \mid \cdots \mid \delta'_\lambda$, όπου $(\delta_i) = Ann(x_i)$ και $(\delta'_j) = Ann(y_j)$, για κάθε $i = 1, 2, \ldots, \nu$ και $j = 1, 2, \ldots, \lambda$, ισοδύναμα $Ann(x_1) \supseteq Ann(x_2) \supseteq \cdots \supseteq Ann(x_\nu)$ και $Ann(y_1) \supseteq Ann(y_2) \supseteq \cdots \supseteq Ann(y_\lambda)$, τότε $\nu = \lambda$.

Παρατήρηση 2η: Αν $Ann(z_1) \supseteq Ann(z_2) \supseteq \cdots \supseteq Ann(z_\rho)$ και $r \in R$, τότε $Ann(rz_1) \supseteq$

$\supseteq Ann(rz_2) \supseteq \cdots \supseteq Ann(rz_\rho)$, ακόμα και αν κάποια από τα κυκλικά πρότυπα (rz_i) είναι μηδενικά. Πράγματι, αν $s \in Ann(rz_i)$, όπου $i > 1$, τότε $srz_i = 0 \Leftrightarrow sr \in Ann(z_i) \subseteq Ann(z_{i-1}) \Rightarrow$ $\Rightarrow sr \in Ann(z_{i-1}) \Leftrightarrow srz_{i-1} = 0 \Leftrightarrow s \in Ann(rz_{i-1})$.
Τώρα, επιλέγουμε ένα $i \in \{1, 2, \ldots, \nu\}$ και θεωρούμε το πρότυπο

$$\delta_i T(M) = (\delta_i x_1) \oplus (\delta_i x_2) \oplus \cdots \oplus (\delta_i x_\nu) = (\delta_i y_1) \oplus (\delta_i y_2) \oplus \cdots \oplus (\delta_i y_\nu). \qquad (1)$$

Το δ_i θα μηδενίσει τουλάχιστον τα $x_1, \ldots, x_i$. Και λέμε «τουλάχιστον», γιατί μπορεί να μηδενίσει και κάποια από τα x_{i+1}, x_{i+2} κτλ αν το δ_i είναι συντροφικό με τα $\delta_{i+1}, \delta_{i+2}$ κτλ, Πάντως θα μηδενίσει $t \geq i$ όρους από το ευθύ άθροισμα στα αριστερά της (1). (Υπάρχει πιθανότητα να τους μηδενίσει όλους). Επομένως η (1) ξαναγράφεται ως εξής:

$$\bigoplus_{t<j\leq\nu} (\delta_i x_j) = (\delta_i y_1) \oplus (\delta_i y_2) \oplus \cdots \oplus (\delta_i y_\nu). \qquad (1')$$

Σύμφωνα με τη 2^{η} παρατήρηση $Ann(\delta_i x_{t+1}) \supseteq Ann(\delta_i x_{t+2}) \supseteq \cdots \supseteq Ann(\delta_i x_\nu)$, αν φυσικά υπάρχουν τέτοιοι όροι, και $Ann(\delta_i y_1) \supseteq Ann(\delta_i y_2) \supseteq \cdots \supseteq Ann(\delta_i y_\nu)$. Σύμφωνα με την 1^{η} παρατήρηση, όσοι όροι υπάρχουν στα αριστερά της $(1')$, υπάρχουν και στα δεξιά. Κατά συνέπεια το δ_i θα μηδενίσει t ακριβώς όρους στο άθροισμα $(\delta_i y_1) \oplus (\delta_i y_2) \oplus \cdots \oplus (\delta_i y_\nu)$. Ποιους όρους θα μηδενίσει; Λόγω της σχέσης $Ann(y_t) \supseteq Ann(y_{t+1}) \supseteq \cdots \supseteq Ann(y_\nu)$, αν δεν μηδενίσει το y_t, δηλαδή $\delta_i \notin Ann(y_t)$, τότε $\delta_i \notin Ann(y_j)$, για κάθε j με $t \leq j \leq \nu$. Επομένως στο δεξιό μέλος της $(1')$ θα υπάρχουν τουλάχιστον $\nu - t + 1 > \nu - t$ μη μηδενικοί όροι, οι $(\delta_i y_t), (\delta_i y_{t+1}), \ldots, (\delta_i y_\nu)$, ενώ στο αριστερό ακριβώς $\nu - t$. Αυτό είναι άτοπο λόγω της $1^{\eta\varsigma}$ παρατήρησης. Επομένως $\delta_i \in Ann(y_t) \subseteq Ann(y_{t-1}) \subseteq \cdots \subseteq Ann(y_1)$. Ιδιαιτέρως $\delta_i \in Ann(y_i) = (\delta_i')$, δηλαδή $\delta_i' \mid \delta_i$. Με παρόμοιο συλλογισμό, θεωρώντας συμμετρικά το $\delta_i' T(M)$ αποδεικνύουμε ότι $\delta_i \mid \delta_i'$. Άρα $\delta_i \sim \delta_i'$, για κάθε $i = 1, 2, \ldots, \nu$. ■

ΟΡΙΣΜΟΣ 4.18. Τα στοιχεία $\delta_1, \delta_2, \ldots, \delta_k$ με $\delta_i \mid \delta_{i+1}$, για κάθε $i = 1, 2, \ldots, k-1$ και $(\delta_i) = = Ann(x_i)$, για κάθε $i = 1, 2, \ldots, k$, όπου $M = (x_1) \oplus (x_2) \oplus \cdots \oplus (x_k)$ και τα οποία είναι μοναδικά ως προς τη σχέση της συντροφικότητας, ονομάζονται **αναλλοίωτοι παράγοντες του M**.

ΠΑΡΑΤΗΡΗΣΗ: Επειδή $(x_i) \cong {}^{R}\!/_{(\delta_i)}$, (βλέπε σχόλιο μετά την απόδειξη της πρότασης 3.37) οι αναλλοίωτοι παράγοντες του M καθορίζουν πλήρως τη δομή του προτύπου M. Πιο συγκεκριμένα,

$$M \cong {}^{R}\!/_{(\delta_1)} \oplus {}^{R}\!/_{(\delta_2)} \oplus \cdots \oplus {}^{R}\!/_{(\delta_k)}.$$

ΠΟΡΙΣΜΑ 4.19. Έστω G μια πεπερασμένα παραγόμενη αβελιανή ομάδα (ℤ-πρότυπο). Έστω $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_k$ οι αναλλοίωτοι παράγοντες της G. Οι $\delta_1, \delta_2, \ldots, \delta_k$ είναι ακέραιοι και επειδή δεν λαμβάνουμε υπ' όψιν τη συντροφικότητα, αυτοί μπορεί να θεωρηθούν θετικοί ακέραιοι μεγαλύτεροι της μονάδος ή μηδέν. Τότε η G αναλύεται κατά μοναδικό τρόπο ως

$$G \cong \mathbb{Z}_{\delta_1} \oplus \mathbb{Z}_{\delta_2} \oplus \cdots \oplus \mathbb{Z}_{\delta_\nu} \oplus \underbrace{\mathbb{Z} \oplus \mathbb{Z} \cdots \oplus \mathbb{Z}}_{k-\nu \text{ το πλήθος}}.$$

Ιδιαιτέρως, αν η G είναι πεπερασμένη, τότε

$$G \cong \mathbb{Z}_{\delta_1} \oplus \mathbb{Z}_{\delta_2} \oplus \cdots \oplus \mathbb{Z}_{\delta_\nu}$$

και $|G| = \delta_1 \delta_2 \cdots \delta_\nu$. ■

ΠΑΡΑΔΕΙΓΜΑΤΑ 4.20. (i) Να ταξινομηθούν όλες οι ανά δύο μη ισόμορφες αβελιανές ομάδες τάξεως 432.
ΛΥΣΗ: $432 = 2^4 \cdot 3^3$. Για το 2 έχουμε τις ακόλουθες περιπτώσεις: 2^4, $2 \mid 2^3$, $2^2 \mid 2^2$, $2 \mid 2 \mid 2^2$ και $2 \mid 2 \mid 2 \mid 2$. Για το 3 έχουμε τις ακόλουθες περιπτώσεις: 3^3, $3 \mid 3^2$ και $3 \mid 3 \mid 3$. Συνδυάζοντας τα ανωτέρω παίρνουμε τις ακόλουθες περιπτώσεις για τους αναλλοίωτους παράγοντες:

1) $2^4 \cdot 3^3 = 432$, **2)** $3 \mid 2^4 \cdot 3^2$, **3)** $3 \mid 3 \mid 2^4 \cdot 3$, **4)** $2 \mid 2^3 \cdot 3^3$,
5) $2 \cdot 3 \mid 2^3 \cdot 3^2$, **6)** $3 \mid 2 \cdot 3 \mid 2^3 \cdot 3$, **7)** $2^2 \mid 2^2 \cdot 3^3$, **8)** $2^2 \cdot 3 \mid 2^2 \cdot 3^2$,
9) $3 \mid 2^2 \cdot 3 \mid 2^2 \cdot 3$, **10)** $2 \mid 2 \mid 2^2 \cdot 3^3$, **11)** $2 \mid 2 \cdot 3 \mid 2^2 \cdot 3^2$, **12)** $2 \cdot 3 \mid 2 \cdot 3 \mid 2^2 \cdot 3$,
13) $2 \mid 2 \mid 2 \mid 2 \cdot 3^3$, **14)** $2 \mid 2 \mid 2 \cdot 3 \mid 2 \cdot 3^2$, **15)** $2 \mid 2 \cdot 3 \mid 2 \cdot 3 \mid 2 \cdot 3$.

Μια αβελιανή ομάδα τάξεως 432 είναι λοιπόν ισόμορφη με μια από τις παρακάτω ομάδες:

1) $\mathbb{Z}_{432}$, **2)** $\mathbb{Z}_3 \oplus \mathbb{Z}_{144}$, **3)** $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{48}$,
4) $\mathbb{Z}_2 \oplus \mathbb{Z}_{216}$, **5)** $\mathbb{Z}_6 \oplus \mathbb{Z}_{72}$, **6)** $\mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{24}$,
7) $\mathbb{Z}_4 \oplus \mathbb{Z}_{108}$, **8)** $\mathbb{Z}_{12} \oplus \mathbb{Z}_{36}$, **9)** $\mathbb{Z}_3 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{12}$,
10) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{108}$, **11)** $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{36}$, **12)** $\mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{12}$,
13) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{54}$, **14)** $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{18}$, **15)** $\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_6$. ■

(ii) Να βρεθεί η αβελιανή ομάδα τάξης $2^3 \cdot 5^3 \cdot 7^4$ με αναλλοίωτους παράγοντες $\delta_1 = 7$ και $\delta_\nu = 2^2 \cdot 5 \cdot 7$.

ΛΥΣΗ: Εφόσον η τάξη της ομάδας έχει το 7^4 ως μέγιστη δύναμη του 7 και υπάρχουν ήδη δύο αναλλοίωτοι παράγοντες που διαιρούνται με το 7 $\big($ο πρώτος και ο τελευταίος$\big)$, οι ενδιάμεσοι αναλλοίωτοι παράγοντες θα διαιρούνται επίσης με το 7. Επομένως αυτοί είναι το πολύ δύο. Αν ήταν ένας, αυτός θα διαιρείτο με το 7^2, το οποίο όμως δεν διαιρεί το $\delta_\nu = 2^2 \cdot 5 \cdot 7$. Επομένως έχουμε 4 αναλλοίωτους παράγοντες $\delta_1 = 7 \mid \delta_2 \mid \delta_3 \mid \delta_4 = \delta_\nu = 2^2 \cdot 5 \cdot 7$ και το 7 διαιρεί και το δ_2 και το δ_3. Ομοίως το 5^2 δεν μπορεί να διαιρεί τον δ_2 ή τον δ_3, γιατί τότε θα διαιρούσε και τον $\delta_4 = 2^2 \cdot 5 \cdot 7$, πράγμα αδύνατον. Άρα το 5 διαιρεί και το δ_2 και το δ_3. Απομένει ένα 2, το οποίο αναγκαστικά θα διαιρεί το δ_3. Επομένως οι αναλλοίωτοι παράγοτες της ομάδας είναι $\delta_1 = 7$, $\delta_2 = 5 \cdot 7 = 35$, $\delta_3 = 2 \cdot 5 \cdot 7 = 70$ και $\delta_4 = 2^2 \cdot 5 \cdot 7 = 140$.
Η ζητούμενη ομάδα είναι η $\mathbb{Z}_7 \oplus \mathbb{Z}_{35} \oplus \mathbb{Z}_{70} \oplus \mathbb{Z}_{140}$. ■

Ένα άλλο ενδιαφέρον αποτέλεσμα αφορά την πολλαπλασιαστική ομάδα των μη μηδενικών στοιχείων ενός πεπερασμένου σώματος $\mathbb{F}$. $\big($Όσοι είναι εξοικειωμένοι με πεπερασμένα σώματα γνωρίζουν ότι κάθε πεπερασμένο σώμα έχει τάξη δύναμη p^r, όπου p πρώτος και r θετικός ακέραιος και είναι μια αλγεβρική επέκταση του $\mathbb{Z}_p$. Συγκεκριμένα είναι το σώμα ριζών του πολυωνύμου $x^{p^r} - 1$ επί του πρώτου υποσώματος $\mathbb{Z}_p\big)$.

ΕΦΑΡΜΟΓΗ 4.21. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα και $\mathbb{F}^* = \mathbb{F} \backslash \{0\}$ το σύνολο των μη μηδενικών στοιχείων αυτού. Προφανώς το $\mathbb{F}^*$ με πράξη τον πολλαπλασιασμό του σώματος είναι αβελιανή ομάδα. Η ομάδα αυτή $(\mathbb{F}^*, \cdot)$ είναι κυκλική.
ΑΠΟΔΕΙΞΗ: Εδώ θα χρησιμοποιήσουμε τον πολλαπλασιαστικό συμβολισμό. Έστω $0 < \delta_1 \mid \delta_2 \mid \cdots \mid \delta_\nu$ οι αναλλοίωτοι παράγοντες της $\mathbb{F}^*$. Τότε $\mathbb{F}^* = (g_1) \cdot (g_2) \cdots (g_\nu)$, όπου $(g_i) \cong C_{\delta_i}$, η κυκλική ομάδα τάξεως δ_i, για κάθε $i = 1, 2, \ldots, \nu$. Επειδή $\delta_i \mid \delta_\nu$, έχουμε $g_i^{\delta_\nu} = 1$, για κάθε $i = 1, 2, \ldots, \nu$. Επομένως τα στοιχεία του $\mathbb{F}^*$ είναι ρίζες του πολυωνύμου $x^{\delta_\nu} - 1$, το οποίο έχει το πολύ δ_ν διαφορετικές ρίζες. Επομένως $|\mathbb{F}^*| \leq \delta_\nu$. Αν $\nu > 1$, τότε από το πόρισμα 4.18 παίρνουμε $|\mathbb{F}^*| = \delta_1 \delta_2 \cdots \delta_\nu > \delta_\nu \geq |\mathbb{F}^*|$, άτοπο. Άρα $\nu = 1$ και $\mathbb{F}^* = (g_1) \cong C_{\delta_1}$. ■

*4.5 Διαφορετική Απόδειξη του Θεωρήματος 4.17

Αν θέλουμε να αποφύγουμε την απόδειξη μέσω διαστάσεων, υπάρχει και μια άλλη μέθοδος:

ΛΗΜΜΑ 4.22. Έστω R περιοχή κυρίων ιδεωδών.
(i) Έστω M πεπερασμένα παραγόμενο R-πρότυπο και $x \in M \setminus \{0_M\}$ με $Ann(x) = (\delta)$, όπου $\delta \neq 0_R$. Αν $Rx \subseteq Ry$ και $\delta y = 0_M$, τότε $Rx = Ry$.
(ii) Έστω M πεπερασμένα παραγόμενο R-πρότυπο και $x \in M \backslash \{0_M\}$ τέτοιο, ώστε $Ann(x) = (\delta)$,

όπου $\delta \neq 0_R$ και $(\delta) \subseteq Ann(z)$, για κάθε $z \in M$. Έστω $f : F \to M$ R-επιμορφισμός, όπου F ελεύθερο με rank$F = m$. Τότε υπάρχει βάση $(u_1, u_2, \ldots, u_m)$ του F και $x' \in M$ τέτοια, ώστε $Rx = Rx'$ και $f(u_1) = x'$.

ΑΠΟΔΕΙΞΗ: (i) Επειδή $x \in Rx \subseteq Ry$, έχουμε $x = ry$, για κάποιο $r \in R$. Έστω $u \in R$ με $(u) = (r, \delta)$. (Το u είναι ένας μέγιστος κοινός διαιρέτης των r και δ). Τότε $\delta = \delta' u \neq 0_R \Rightarrow \delta' \neq 0_R$ και $r = su$, για κάποια $\delta', s \in R$. Επομένως $\delta' x = \delta' ry = \delta' usy = s\delta y = 0_M$. Άρα $\delta' \in Ann(x) = (\delta) \Leftrightarrow \delta \mid \delta'$, δηλαδή $\delta' = t\delta = tu\delta'$, για κάποιο $t \in R$. Εφόσον $\delta' \neq 0_R$ και R ακέραια περιοχή, $tu = 1_R$, δηλαδή το u είναι αντιστρέψιμο και άρα $(r, \delta) = (1_R)$. Επομένως υπάρχουν $\alpha, \beta \in R$ τέτοια, ώστε $\alpha r + \beta\delta = 1_R$. Κατά συνέπεια $y = 1_R \cdot y = \alpha ry + \beta\delta y \underset{\delta y = 0_M}{=} \alpha x \in Rx$. Άρα $Ry \subseteq Rx$ και επειδή $Rx \subseteq Ry$, έπεται ότι $Rx = Ry$.

(ii) Εφόσον f επιμορφισμός, υπάρχει $y \in F$ τέτοιο, ώστε $f(y) = x$. Επειδή $x \neq 0_M$, έχουμε και $y \neq 0_F$. Θεωρούμε το υποπρότυπο $F_1 = Ry$ του F. Εφόσον το F είναι ελεύθερο, θα είνει και ελεύθερο στρέψεως. Άρα και $F_1 = Ry$ είναι ελεύθερο στρέψεως και άρα ελεύθερο με βάση το y. Αν $A \in R^{m\times 1}$ είναι ο πίνακας της εμφύτευσης $F_1 = Ry \hookrightarrow F$, ως προς τη βάση (y) του $F_1 = Ry$ και κάποια βάση $(v_1, v_2, \ldots, v_m)$ του F, από τον αλγόριθμο του Smith προκύπτει ότι υπάρχουν αντιστρέψιμοι πίνακες $X \in R^{m\times m}$ και $Y \in R^{1\times 1} \cong R$ τέτοιοι, ώστε $XAY = \begin{pmatrix} r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, για κάποιο $r \in R$. Ο πίνακας X είναι πίνακας αλλαγής βάσης του F και ο Y πίνακας αλλαγής βάσης του $F_1 = Ry$. Ο πίνακας $XAY = \begin{pmatrix} r \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ είναι ο πίνακας της εμφύτευσης $F_1 = Ry \hookrightarrow F$ ως προς τις νέες βάσεις (y') του $F_1 = Ry$ και $(u_1, u_2, \ldots, u_m)$ του F. Εφόσον $Ry' = Ry$, $y' = uy$, για κάποιο αντιστρέψιμο $u \in R$ και $y' = ru_1$. Θέτουμε $x' = f(u_1)$. Τότε $uy = ru_1 \Rightarrow ux = uf(y) = rf(u_1) = rx' \Rightarrow x = u^{-1}rx' \in Rx' \Rightarrow Rx \subseteq Rx'$. Αλλά $\delta x' = 0_M$, γιατί $(\delta) \subseteq Ann(z)$, για κάθε $z \in M$. Από το (i) προκύπτει ότι $Rx = Rx'$. ■

ΛΗΜΜΑ 4.23. Έστω $M = (x_1) \oplus (x_2) \oplus \cdots \oplus (x_\nu)$ ένα πρότυπο στρέψεως με $x_i \neq 0_M$, για κάθε $i = 1, 2, \ldots, \nu$. Υποθέτουμε επίσης ότι $Ann(x_i) = (\delta_i)$, για κάθε $i = 1, 2, \ldots, \nu$ με $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_\nu$. Έστω επίσης $f : F \to M$ ένας R-επιμορφισμός, όπου F ελεύθερο R-πρότυπο. Τότε υπάρχει βάση $(u_1, u_2, \ldots, u_m)$ του F και στοιχεία $x'_1, x'_2, \ldots, x'_\nu$ τέτοια, ώστε $f(u_i) = x'_i \in (x_i)$ και $(x'_i) = (x_i)$, για κάθε $i = 1, 2, \ldots, \nu$ και $f(u_j) = 0_M$, για κάθε j με $\nu < j \leq m$.

ΑΠΟΔΕΙΞΗ: Εφαρμόζουμε επαγωγή επί του ν για να αποδείξουμε αρχικά ότι υπάρχει βάση $(u'_1, u'_2, \ldots, u'_\nu, \ldots, u'_m)$ τέτοια, ώστε $f(u'_i) = x'_i \in (x_i)$ και $(x'_i) = (x_i)$, για κάθε $i = 1, 2, \ldots, \nu$. Για $\nu = 1$ είναι το προηγούμενο λήμμα. Έστω λοιπόν $\nu > 1$. Σύμφωνα πάλι με το προηγούμενο λήμμα υπάρχει βάση $(u'_1, u'_2, \ldots, u'_\nu, \ldots, u'_m)$ τέτοια, ώστε $x'_\nu = f(u'_\nu) \in (x_\nu)$ και $(x'_\nu) = (x_\nu)$, όπου αλλάζοντας την αρίθμηση στη βάση, θεωρούμε ότι το x'_ν να είναι η εικόνα του ν-στού στοιχείου u'_ν της βάσης, αντί του πρώτου. Θέτουμε $u_\nu = u'_\nu$.

Έστω τώρα $M_1 = (x_1) \oplus \cdots \oplus (x_{\nu-1})$. Τότε $M = M_1 \oplus (x'_\nu)$. Αν $\pi : M \to M_1$ είναι η προβολή $\pi(y + rx'_\nu) = y \in M_1$, για κάθε $y \in M_1$ και $r \in R$, τότε η π είναι προφανώς επιμορφισμός και επειδή και η $f : F \to M$ είναι επιμορφισμός, η σύνθεση $\pi \circ f : F \to M_1$ είναι επιμορφισμός. Έστω F_1 το υποπρότυπο του F με βάση $(u'_1, u'_2, \ldots, u'_{\nu-1}, u'_{\nu+1}, \ldots, u'_m)$. (Αν rank$F = 1$, τότε $F = Ru_\nu$, το οποίο απεικονίζεται επιμορφικά στο (x_ν). Τότε αναγκαστικά $M = (x_\nu)$ και έχουμε

τελειώσει). Σαφώς $F = F_1 \oplus (u_\nu)$ και επειδή $(\pi \circ f)(u_\nu) = 0_M$, ο περιορισμός $f_1 = (\pi \circ f)|_{F_1} : F_1 \to M_1$ της $\pi \circ f$ στο F_1 είναι επίσης επιμορφισμός. Με επαγωγή επί του ν συμπεραίνουμε ότι υπάρχει βάση $(u_1^\star, u_2^\star, \ldots, u_{\nu-1}^\star, u_{\nu+1}^\star, \ldots, u_m^\star)$ του F_1 τέτοια, ώστε $f_1(u_i^\star) = (\pi \circ f)(u_i^\star) = x_i'$ και $(x_i') = (x_i)$, για κάθε $i = 1, 2, \ldots, \nu-1$. Αυτό σημαίνει ότι $f(u_i^\star) = x_i' + r_i x_\nu'$, για κάθε $i = 1, 2, \ldots, \nu-1$. Επίσης $f(u_j^\star) = \sum_{i=1}^{\nu} \alpha_{ij} x_i'$, για κάθε j με $\nu < j \le m$. Είναι σαφές ότι τα στοιχεία $u_1^\star, u_2^\star, \ldots, u_{\nu-1}^\star, u_\nu, u_{\nu+1}^\star, \ldots, u_m^\star$ αποτελούν βάση του $F = F_1 \oplus (u_\nu)$.
Θέτουμε $u_i = u_i^\star - r_i u_\nu \Leftrightarrow u_i^\star = u_i + r_i u_\nu$, για κάθε $i = 1, 2, \ldots, \nu-1$.
Επομένως $f(u_i) = f(u_i^\star) - r_i f(u_\nu) = x_i' + r_i x_\nu' - r_i x_\nu' = x_i'$, για κάθε $i = 1, 2, \ldots, \nu-1$ και φυσικά $f(u_\nu) = x_\nu'$.
Τέλος, θέτουμε $u_j = u_j^\star - \sum_{i=1}^{\nu} \alpha_{ij} u_i = u_j^\star - \sum_{i=1}^{\nu-1} \alpha_{ij} u_i^\star + \Big(\sum_{i=1}^{\nu-1} \alpha_{ij} r_i - \alpha_{\nu j} \Big) u_\nu$, για κάθε j με $\nu < j \le m$. Τότε $f(u_j) = f(u_j^\star) - \sum\limits_{i=1}^{\nu} \alpha_{ij} f(u_i) = \sum\limits_{i=1}^{\nu} \alpha_{ij} x_i' - \sum\limits_{i=1}^{\nu} \alpha_{ij} x_i' = 0_M$, για κάθε j με $\nu < j \le m$.
Απομένει το ανιαρό μέρος να δείξουμε ότι τα $u_1, u_2, \ldots, u_m$ αποτελούν βάση του F.
α) Γραμμικώς ανεξάρτητα: Έστω $\sum_{i=1}^{m} s_i u_i = 0_F$. Τότε $0_F = \sum_{i=1}^{\nu-1} s_i u_i^\star + \Big(s_\nu - \sum_{i=1}^{\nu-1} s_i r_i \Big) u_\nu + + \sum_{j=\nu+1}^{m} s_j u_j^\star +$ γραμμικός συνδυασμός των $\{u_1^\star, u_2^\star, \ldots, u_{\nu-1}^\star, u_\nu\}$, λόγω της μορφής των $u_{\nu+1}, u_{\nu+2}, \ldots, u_m$. Επειδή τα $u_1^\star, u_2^\star, \ldots, u_{\nu-1}^\star, u_\nu, u_{\nu+1}^\star, \ldots, u_m^\star$ αποτελούν βάση του F, έχουμε $s_{\nu+1} = = s_{\nu+2} = \cdots = s_m = 0_R$. Επομένως έχουμε $0_F = \sum_{i=1}^{\nu} s_i u_i = \sum_{i=1}^{\nu-1} s_i u_i^\star + \Big(s_\nu - \sum_{i=1}^{\nu-1} s_i r_i \Big) u_\nu$. Λόγω της γραμμικής ανεξαρτησίας των $u_1^\star, u_2^\star, \ldots, u_{\nu-1}^\star$ και u_ν παίρνουμε $s_1 = s_2 = \cdots = s_{\nu-1} = = 0_R$ και $s_\nu = \sum_{i=1}^{\nu-1} s_i r_i = 0_R$.
β) Παράγουν το F: Έστω $u \in F$. Επειδή τα $u_1^\star, u_2^\star, \ldots, u_{\nu-1}^\star, u_\nu, u_{\nu+1}^\star, \ldots, u_m^\star$ αποτελούν βάση του F, θα έχουμε $u = \sum_{i=1}^{\nu-1} s_i u_i^\star + s_\nu u_\nu + \sum_{j=\nu+1}^{m} s_j u_j^\star$, για κάποια $s_1, s_2, \ldots, s_m \in R$. Αλλά $\sum_{i=1}^{\nu-1} s_i u_i^\star + s_\nu u_\nu = \sum_{i=1}^{\nu-1} s_i u_i + \Big(s_\nu + \sum_{i=1}^{\nu-1} s_i r_i \Big) u_\nu$, δηλαδή γραμμικός συνδυασμός των $u_1, u_2, \ldots, u_{\nu-1}, u_\nu$. Επειδή δε $u_j^\star = u_j + \sum_{i=1}^{\nu} \alpha_{ij} u_i$, για κάθε $j = \nu+1, \nu+2, \ldots, m$, το άθροισμα $\sum_{j=\nu+1}^{m} s_j u_j^\star$ θα ισούται με $\sum_{j=\nu+1}^{m} s_j u_j +$ έναν γραμμικό συνδυασμό των $\{u_1, u_2, \ldots, u_{\nu-1}, u_\nu\}$. Τελικώς το $u = \sum_{i=1}^{\nu-1} s_i u_i^\star + s_\nu u_\nu + \sum_{j=\nu+1}^{m} s_j u_j^\star$ ισούται με έναν γραμμικό συνδυασμό των $u_1, u_2, \ldots, u_m$. ■

ΛΗΜΜΑ 4.24. Έστω M ένα μη μηδενικό πεπερασμένα παραγόμενο R-πρότυπο στρέψεως. Έστω $f : F \to M$ ένας R-επιμορφισμός, όπου F ελεύθερο R-πρότυπο. Έστω επίσης

$$M = (x_1) \oplus (x_2) \oplus \cdots \oplus (x_\nu)$$

με $Ann(x_i) = (\delta_i)$, για κάθε $i = 1, 2, \ldots, \nu$, $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_\nu$ και δ_1 μη αντιστρέψιμο, (ισοδύναμα $x_1 \neq 0_M$) και άρα όλα τα δ_i μη αντιστρέψιμα.
Αν $i : \mathrm{Ker} f \hookrightarrow F$ η εμφύτευση του πυρήνα της f, τότε υπάρχουν βάσεις των F και $\mathrm{Ker} f$ τέτοιες, ώστε ο πίνακας της εμφύτευσης i να έχει τη μορφή

$$\begin{pmatrix} \overbrace{1 \quad \cdots \quad 1}^{m-\nu \text{ μονάδες}} & & & & \\ & \delta_1 & & & \\ & & \delta_2 & & \\ & & & \ddots & \\ & & & & \delta_\nu \end{pmatrix} \qquad (\star)$$

ΑΠΟΔΕΙΞΗ: Από το προηγούμενο λήμμα υπάρχει βάση του $(u_1, u_2, \ldots, u_\nu, u_{\nu+1}, \ldots, u_m)$ του F και στοιχεία $x_1', x_2', \ldots, x_\nu'$ τέτοια, ώστε $f(u_i) = x_i' \in (x_i)$ και $(x_i') = (x_i)$, για κάθε $i = 1, 2, \ldots, \nu$

και $f(u_j) = 0_M$, για κάθε j με $\nu < j \leq m$. Αλλάζουμε την αρίθμηση των στοιχείων της βάσης και θεωρούμε, αντί της αρχικής, τη βάση $(u_{\nu+1}, \ldots, u_m, u_1, u_2, \ldots, u_\nu)$. Είναι σαφές ότι $u_{\nu+1}, \ldots, u_m, \delta_1 u_1, \delta_2 u_2, \ldots, \delta_\nu u_\nu \in \mathrm{Ker} f$ γιατί $f(u_i) = 0_M$, για κάθε i με $\nu < i \leq m$ και επίσης $f(\delta_i u_i) = \delta_i x_i' = 0_M$, γιατί $(\delta_i) = Ann(x_i) = Ann(x_i')$, για κάθε $i = 1, 2, \ldots, \nu$. Αντιστρόφως, έστω $u = \sum_{j=\nu+1}^{m} s_j u_j + \sum_{i=1}^{\nu} s_i u_i \in \mathrm{Ker} f$. Τότε $0_M = \sum_{j=\nu+1}^{m} s_j \underbrace{f(u_j)}_{0_M} + \sum_{i=1}^{\nu} s_i f(u_i) = \sum_{i=1}^{\nu} s_i x_i'$. Επειδή το M είναι το ευθύ άθροισμα των $(x_i') = (x_i)$, για $i = 1, 2, \ldots, \nu$, θα έχουμε $s_i x_i' = 0_M \Leftrightarrow s_i \in \in Ann(x_i') = (\delta_i)$, δηλαδή $s_i = \zeta_i \delta_i$, για κάθε $i = 1, 2 \ldots, \nu$. Άρα το u γράφεται σαν γραμμικός συνδυασμός των $u_{\nu+1}, \ldots, u_m, \delta_1 u_1, \delta_2 u_2, \ldots, \delta_\nu u_\nu$. Τελικώς τα στοιχεία αυτά αποτελούν βάση του $\mathrm{Ker} f$. $\big($Είναι μη μηδενικά πολλαπλάσια στοιχείων της βάσης του $F\big)$.
Είναι λοιπόν προφανές ότι ο πίνακας της εμφύτευσης $i : \mathrm{Ker} f \hookrightarrow F$ έχει, ως προς τις δεδομένες βάσεις, τη μορφή $(\star)$. ■

2η ΑΠΟΔΕΙΞΗ του ΘΕΩΡΗΜΑΤΟΣ 4.16: Σύμφωνα με τα προλεγόμενα της 1ης απόδειξης, το πρόβλημα ανάγεται στο να αποδείξουμε ότι η ανάλυση του $T(M)$ σε ευθύ άθροισμα κυκλικών υποπροτύπων είναι μοναδική υπό την εξής έννοια: Αν $T(M) = (x_1) \oplus \cdots \oplus (x_\nu) = (y_1) \oplus \cdots \oplus (y_\lambda)$, όπου $(\delta_i) = Ann(x_i) \neq R$, $(\delta_j') = Ann(y_j) \neq R$, για κάθε $i = 1, 2, \ldots, \nu$ και $j = 1, 2, \ldots, \lambda$, με $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_\nu$ και $\delta_1' \mid \delta_2' \mid \cdots \mid \delta_\lambda'$ και δ_1, δ_1' μη αντιστρέψιμα, τότε $\nu = \lambda$ και $\delta_i \sim \delta_i'$, για κάθε $i = 1, 2, \ldots, \nu$. Έστω $f : F \to T(M)$ ένας R-επιμορφισμός, όπου F ελεύθερο R-πρότυπο. Σύμφωνα με τα παραπάνω, ο πίνακας της εμφύτευσης $i : \mathrm{Ker} f \hookrightarrow F$ ως προς διαφορετικές ενδεχομένως βάσεις του F έχει την μορφή $(\star)$, αλλά και τη μορφή

$$\begin{pmatrix} \overbrace{1 \quad \cdots \quad 1}^{m-\nu \text{ μονάδες}} & & & & \\ & \delta_1' & & & \\ & & \delta_2' & & \\ & & & \ddots & \\ & & & & \delta_\lambda' \end{pmatrix} \qquad (\star\star)$$

Οι πίνακες $(\star)$ και $(\star\star)$ είναι προφανώς ισοδύναμοι. Επομένως $m - \nu = m - \lambda \Leftrightarrow \nu = \lambda$ και $\delta_i \sim \delta_i'$, για κάθε $i = 1, 2, \ldots, \nu$. ■

4.6 p-Πρωταρχικές Συνιστώσες

ΟΡΙΣΜΟΣ 4.25. Έστω M ένα πεπερασμένα παραγόμενο R-πρότυπο, όπου R περιοχή κυρίων ιδεωδών. Αν p είναι ένα ανάγωγο στοιχείο της R, θέτουμε

$$M_p = \{x \in M \mid p^\alpha x = 0_M, \text{ για κάποιον θετικό ακέραιο } \alpha\}.$$

Αν $M_p \neq \{0_M\}$, τότε το M_p λέγεται ***p*-πρωταρχική συνιστώσα του M** η $\big($αν το p είναι γνωστό$\big)$ απλά πρωταρχική συνιστώσα του M.

ΠΡΟΤΑΣΗ 4.26. Το M_p είναι υποπρότυπο του M. Επίσης, $M_p \neq \{0_M\}$ αν και μόνον αν $Ann(T(M)) \subseteq (p)$, δηλαδή $p \mid \delta_\nu$, όπου $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_\nu$ η ακολουθία των μη μηδενικών αναλλοίωτων παραγόντων του M.

ΑΠΟΔΕΙΞΗ: Έστω $x, y \in M_p$ και $r \in R$. Τότε υπάρχουν θετικοί ακέραιοι α, β τέτοιοι, ώστε $p^\alpha x = p^\beta y = 0_M$. Επομένως $p^{\alpha+\beta}(x + y) = p^\beta p^\alpha x + p^\alpha p^\beta y = p^\beta \cdot 0_M + p^\alpha \cdot 0_M = 0_M$. Άρα $x + y \in M_p$. Ακόμη, $p^\alpha (rx) = r(p^\alpha x) = r \cdot 0_M = 0_M$ και συνεπώς $rx \in M_p$. Συμπεραίνουμε λοιπόν ότι το M_p είναι υποπρότυπο του M.

Έστω τώρα ότι $M_p \neq \{0_M\}$. Προφανώς $M_p \subseteq T(M)$ και κατά συνέπεια $(\delta_\nu) = Ann(T(M)) \subseteq$ $\subseteq Ann(M_p)$. Έστω $x \in M_p \setminus \{0_M\}$ και α ο ελάχιστος θετικός ακέραιος για τον οποίο $p^\alpha x = 0_M$. Τότε $p^{\alpha-1}x \neq 0_M$, όπου θέτουμε $p^0 = 1_R$, αν $\alpha = 1$. Προφανώς $p^{\alpha-1}x \in M_p$ και $p(p^{\alpha-1}x) = 0_M$. Άρα $p \in Ann(Rp^{\alpha-1}x) = (p')$, όπου $p' \in R \setminus \{0_M\}$, δηλαδή $p' \mid p$. Επειδή p ανάγωγο, το p' είναι είτε αντιστρέψιμο είτε συντροφικό του p. Αν ήταν αντιστρέψιμο, τότε $Ann(Rp^{\alpha-1}x) = R = (1_R)$ και συνεπώς $p^{\alpha-1}x = 1_R \cdot p^{\alpha-1}x = 0_M$, άτοπο. Συνεπώς $p' \sim p$ και άρα $Ann(Rp^{\alpha-1}x) = (p)$. Επειδή το $Rp^{\alpha-1}x$ είναι υποπρότυπο του M_p, έχουμε $Ann(M_p) \subseteq Ann(Rp^{\alpha-1}x) = (p)$. Τελικώς $(\delta_\nu) = Ann(T(M)) \subseteq Ann(M_p) \subseteq (p) \Rightarrow p \mid \delta_\nu$.
Αντιστρόφως, έστω $p \mid \delta_\nu$. Τότε $\delta_\nu = p\zeta$ και $\zeta x_\nu \neq 0_M$, όπου x_ν, όπως στο θεώρημα 4.16 (και τα επόμενα λήμματα και προτάσεις). Επομένως $p(\zeta x_\nu) = (p\zeta)x_\nu = \delta_\nu x_\nu = 0_M$ και κατά συνέπεια $\zeta x_\nu \in M_p$. ■

ΠΡΟΤΑΣΗ 4.27. Έστω $Ann(T(M)) = (\delta_\nu)$, όπως παραπάνω. Αν $\delta_\nu = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$ είναι η ανάλυση του δ_ν σε γινόμενο πρώτων ανά δύο ανάγωγων παραγόντων ($\alpha_i > 0$, για κάθε $i = 1, 2, \ldots, t$), τότε $T(M) = M_{p_1} \oplus M_{p_2} \oplus \cdots \oplus M_{p_t}$.
Σημείωση: Έχουμε γράψει $\delta_\nu = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$ και όχι $\delta_\nu = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$, όπου u αντιστρέψιμο στοιχείο γιατί $(\delta_\nu) = (u^{-1}\delta_\nu)$.
ΑΠΟΔΕΙΞΗ: (i) Το άθροισμα $M_{p_1} + M_{p_2} + \cdots + M_{p_t}$ είναι ευθύ. Πράγματι, έστω $x \in M_{p_i} \bigcap$ $\bigcap \sum_{\substack{1\leq j\leq t \\ j\neq i}} M_{p_j}$. Τότε $x = y_1 + y_2 + \cdots + y_{i-1} + y_{i+1} + \cdots + y_t$, όπου $y_j \in M_{p_j}$, για κάθε $j \neq i$. Επίσης $p_j^{r_j}y_j = 0_M$, για κάποιους θετικούς ακέραιους r_j, όπου $j \neq i$. Έστω $\gamma = p_1^{r_1}\cdots p_{i-1}^{r_{i-1}}p_{i+1}^{r_{i+1}}\cdots p_t^{r_t}$. Επίσης, εφόσον $x \in M_{p_i}$, θα έχουμε $p_i^r x = 0_M$, για κάποιον θετικό ακέραιο r. Τώρα, τα στοιχεία p_i^r και γ είναι πρώτα μεταξύ τους. Άρα υπάρχουν $z, w \in R$ τέτοια, ώστε $zp_i^r + w\gamma = 1_R$. Επομένως $x = 1_R \cdot x = (zp_i^r + w\gamma)x = zp_i^r x + w\gamma x = w\gamma x$, γιατί $p_i^r x = 0_M$. Αλλά, επειδή $p_j^{r_j} \mid \gamma$, θα έχουμε $\gamma y_j = 0_M$, για κάθε $j \neq i$. Συνεπώς $x = w\gamma x = 0_M$.
Γενικά θέτουμε $\gamma_1 = p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_t^{\alpha_t}, \gamma_2 = p_1^{\alpha_1}p_3^{\alpha_3}\cdots p_t^{\alpha_t}, \ldots, \gamma_t = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{t-1}^{\alpha_{t-1}}$, δηλαδή $\gamma_i = \prod_{\substack{1\leq j\leq t \\ j\neq i}} p_j^{\alpha_j}$, για κάθε $i = 1, 2, \ldots, t$. Τότε ένας μέγιστος κοινός διαιρέτης των $\gamma_1, \gamma_2, \ldots, \gamma_t$ είναι το 1_R. Πράγματι, αν p ήταν ένας ανάγωγος διαιρέτης όλων των $\gamma_1, \gamma_2, \ldots, \gamma_t$, τότε $p \mid \gamma_1 = p_2^{\alpha_2}p_3^{\alpha_3}\cdots p_t^{\alpha_t}$ και κατά συνέπεια ο p θα ήταν συντροφικό στοιχείο με κάποιο από τα $p_2, \ldots, p_t$. Έστω $p \sim p_i$, για κάποιο i, με $2 \leq i \leq t$. Επειδή $p \mid \gamma_i = \prod_{\substack{1\leq j\leq t \\ j\neq i}} p_j^{\alpha_j}$, ο p θα ήταν συντροφικό στοιχείο με κάποιο από τα p_j, όπου $j \neq i$. Επομένως $p_i \sim p \sim p_j$, άτοπο γιατί $p_i \not\sim p_j$ για $i \neq j$. Συμπεραίνουμε λοιπόν ότι $(\gamma_1, \gamma_2, \ldots, \gamma_t) = (1_R) = R$. Επομένως υπάρχουν $\zeta_1, \zeta_2, \ldots, \zeta_t \in R$ τέτοια, ώστε $\zeta_1\gamma_1 + \zeta_2\gamma_2 + \cdots + \zeta_t\gamma_t = 1_R$.
Έστω τώρα $x \in T(M)$. Τότε $x = 1_R \cdot x = (\zeta_1\gamma_1 + \zeta_2\gamma_2 + \cdots + \zeta_t\gamma_t)x = \zeta_1\gamma_1 x + \zeta_2\gamma_2 x + \cdots + \zeta_t\gamma_t x$. Αλλά $p_i^{\alpha_i}\zeta_i\gamma_i x = \zeta_i\delta_\nu x = 0_M$, δηλαδή $\zeta_i\gamma_i x \in M_{p_i}$, για κάθε $i = 1, 2, \ldots, t$. Επομένως $T(M) = M_{p_1} \oplus M_{p_2} \oplus \cdots \oplus M_{p_t}$. ■

4.7 Πρωταρχική Ανάλυση Πεπερασμένα Παραγόμενου Προτύπου επί Περιοχής Κυρίων Ιδεωδών (Β΄ Μορφή)-Στοιχειώδεις Διαιρέτες

Σύμφωνα με τις προτάσεις 4.25 και 4.26 το υποπρότυπο στρέψης $T(M)$ ενός πεπερασμένα παραγόμενου προτύπου επί μιας περιοχής κυρίων ιδεωδών R αναλύεται μονοσήμαντα σε ευθύ άθροισμα πρωταρχικών συνιστωσών. Οι πρωταρχικές συνιστώσες M_p είναι ακριβώς αυτές για

τις οποίες το p είναι διαιρέτης του δ_ν, δηλαδή του αναλλοίωτου παράγοντα με το μέγιστο μήκος $\lambda(\delta_\nu)$.
Τώρα, κάθε πρωταρχική συνιστώσα M_p είναι ένα πεπερασμένα παραγόμενο R-πρότυπο. Προφανώς είναι ένα πρότυπο στρέψεως, δηλαδή $T(M_p) = M_p$. Επομένως κάθε M_p αναλύεται μονοσήμαντα σε ευθύ άθροισμα μη μηδενικών κυκλικών υποπροτύπων $(x_{p,1}) \oplus (x_{p,2}) \oplus \cdots \oplus (x_{p,k_p})$ με $Ann(x_{p,i}) \supseteq Ann(x_{p,i+1})$, για κάθε $i = 1, 2, \ldots, k_p - 1$, σύμφωνα με το θεώρημα 4.16.
Τώρα, $Ann(x_{p,i}) = (p^{\lambda_{p,i}})$, όπου $\lambda_{p,i}$ θετικός ακέραιος, για κάθε $i = 1, 2, \ldots, k_p$. Πράγματι, αφού $x_{p,i} \in M_p$, θα πρέπει $p^{\lambda_{p,i}} x_{p,i} = 0_M$, για κάποιον ελάχιστο θετικό ακέραιο $\lambda_{p,i}$. Επομένως, $p^{\lambda_{p,i}} \in Ann(x_{p,i}) \Leftrightarrow (p^{\lambda_{p,i}}) \subseteq Ann(x_{p,i})$. Αν $(\gamma_{p,i}) = Ann(x_{p,i})$, τότε $\gamma_{p,i} \mid p^{\lambda_{p,i}}$ και επειδή το p είναι ανάγωγο στοιχείο, το $\gamma_{p,i}$ είναι συντροφικό με κάποια δύναμη p^α, όπου α θετικός ακέραιος. Εφόσον η συντροφικότητα δεν αλλάζει τα κύρια ιδεώδη, μπορούμε να υποθέσουμε ότι $\gamma_{p,i} = p^\alpha$, όπου $\alpha \leq \lambda_{p,i}$. Αν $\alpha < \lambda_{p,i}$ καταλήγουμε σε άτοπο, γιατί το $p^{\lambda_{p,i}}$ είναι η ελάχιστη δύναμη του p που μηδενίζει το $x_{p,i}$. Συμπεραίνουμε λοιπόν ότι $Ann(x_{p,i}) = (p^{\lambda_{p,i}})$. Η σχέση $Ann(x_{p,i}) \supseteq Ann(x_{p,i+1})$ γράφεται ισοδύναμα $p^{\lambda_{p,i}} \mid p^{\lambda_{p,i+1}} \Leftrightarrow \lambda_{p,i} \leq \lambda_{p,i+1}$, για κάθε $i = 1, 2, \ldots, k_p - 1$.
ΣΥΜΠΕΡΑΣΜΑ: Αν $M_{p_1}, M_{p_2}, \ldots, M_{p_t}$ είναι οι πρωταρχικές συνιστώσες του M, τότε το $T(M)$ γράφεται ως ευθύ άθροισμα μη μηδενικών κυκλικών υποπροτύπων ως εξής:
$T(M) = \big((x_{p_1,1}) \oplus (x_{p_1,2}) \oplus \cdots \oplus (x_{p_1,k_{p_1}})\big) \oplus \big((x_{p_2,1}) \oplus (x_{p_2,2}) \oplus \cdots \oplus (x_{p_2,k_{p_2}})\big) \oplus \cdots \oplus \big((x_{p_t,1}) \oplus \oplus (x_{p_t,2}) \oplus \cdots \oplus (x_{p_t,k_{p_t}})\big)$, όπου $Ann(x_{p_i,j}) = (p_i^{\lambda_{p_i,j}})$, για κάθε $j = 1, 2, \ldots, k_{p_i}$ και $i = 1, 2, \ldots, t$. Επίσης $\lambda_{p_i,j} \leq \lambda_{p_i,j+1}$, για κάθε $j = 1, 2, \ldots, k_{p_i} - 1$ και $j = 1, 2, \ldots, t$.
Αντιστρόφως, έστω $q_1, q_2, \ldots, q_s$ ανάγωγα στοιχεία της R, πρώτα ανά δύο και $T(M) = \big((x_{q_1,1}) \oplus \oplus (x_{q_1,2}) \oplus \cdots \oplus (x_{q_1,n_{q_1}})\big) \oplus \big((x_{q_2,1}) \oplus (x_{q_2,2}) \oplus \cdots \oplus (x_{q_2,n_{p_2}})\big) \oplus \cdots \oplus \big((x_{q_s,1}) \oplus (x_{q_s,2}) \oplus \cdots \oplus (x_{q_s,n_{q_s}})\big)$, όπου $Ann(x_{q_i,j}) = (q_i^{\mu_{q_i,j}})$, για κάθε $j = 1, 2, \ldots, n_{q_i}$ και $i = 1, 2, \ldots, s$. Επίσης $\mu_{q_i,j} \leq \mu_{q_i,j+1}$, για κάθε $j = 1, 2, \ldots, n_{q_i} - 1$ και $j = 1, 2, \ldots, s$.
Τότε τα υποπρότυπα $M_{q_1}, M_{q_2}, \ldots, M_{q_s}$ είναι οι πρωταρχικές συνιστώσες του $T(M)$. Με βάση την πρόταση 4.25 οι πρωταρχικές συνιστώσες του $T(M)$ ορίζονται μονοσήμαντα. Άρα τα υποπρότυπα $M_{q_1}, M_{q_2}, \ldots, M_{q_s}$ είναι μια μετάθεση των $M_{p_1}, M_{p_2}, \ldots, M_{p_t}$. Επομένως $s = t$ και κάθε M_{q_i} ισούται με μία μοναδική πρωταρχική συνιστώσα $M_{p_{i'}}$ και το αντίστροφο. Τα στοιχεία q_i και $p_{i'}$, βάσει των προτάσεων 4.25 και 4.26, είναι συντροφικά. Επομένως οι αναλύσεις των M_{q_i} και $M_{p_{i'}}$ σε ευθέα αθροίσματα κυκλικών υποπροτύπων είναι ισόμορφες, δηλαδή $n_{q_i} = k_{p_{i'}}$ και ο μηδενιστής $(q_i^{\mu_{q_i,j}})$ του $x_{q_i,j}$ ισούται με τον μηδενιστή $(p_{i'}^{\lambda_{p_{i'},j}})$ του $x_{p_{i'},j}$, άρα $\mu_{q_i,j} = \lambda_{p_{i'},j}$, για κάθε $j = 1, 2, \ldots, n_{q_i} = k_{p_{i'}}$.

Μπορούμε τώρα να διατυπώσουμε το θεώρημα δομής 4.16 των πεπερασμένα παραγόμενων προτύπων επί μιας περιοχής κυρίων ιδεωδών R, ως ακολούθως. Κατ' αρχάς θέτουμε $p_i^{\lambda_{ij}}$ αντί $p_i^{\lambda_{p_i,j}}$.

ΘΕΩΡΗΜΑ 4.28. Κάθε (μη μηδενικό) πεπερασμένα παραγόμενο R-πρότυπο, όπου R περιοχή κυρίων ιδεωδών αναλύεται μονοσήμαντα, σύμφωνα με τα προηγούμενα, σε ευθύ άθροισμα κυκλικών υποπροτύπων ως εξής:
$M = \big((x_{p_1,1}) \oplus (x_{p_1,2}) \oplus \cdots \oplus (x_{p_1,k_{p_1}})\big) \oplus \big((x_{p_2,1}) \oplus (x_{p_2,2}) \oplus \cdots \oplus (x_{p_2,k_{p_2}})\big) \oplus \cdots \oplus \big((x_{p_t,1}) \oplus \oplus (x_{p_t,2}) \oplus \cdots \oplus (x_{p_t,k_{p_t}})\big) \oplus F$,
όπου F ελεύθερο R-πρότυπο, ισόμορφο με το $M\Big/T(M)$ και $Ann(x_{p_i,j}) = (p_i^{\lambda_{ij}})$, για κάθε $j = 1, 2, \ldots, k_{p_i}$ και $i = 1, 2, \ldots, t$. Επίσης $\lambda_{ij} \leq \lambda_{i,j+1}$, για κάθε $j = 1, 2, \ldots, k_{p_i} - 1$ και $j = 1, 2, \ldots, t$. ■

ΟΡΙΣΜΟΣ 4.29. Τα στοιχεία $p_i^{\lambda_{ij}}$ καθορίζουν προφανώς τη δομή του υποπροτύπου στρέψεως $T(M)$, άρα και του M, γιατί $T(M) \cong \bigoplus_{i,j} R\Big/\big(p_i^{\lambda_{ij}}\big)$ και ονομάζονται **στοιχειώδεις διαιρέτες του M**.

Η επόμενη πρόταση μας δείχνει πώς ένα κυκλικό πρότυπο διασπάται σε ευθύ άθροισμα πρωταρχικών κυκλικών υποπροτύπων.

ΠΡΟΤΑΣΗ 4.30. Έστω (x) κυκλικό υποπρότυπο ενός πεπερασμένα παραγομένου προτύπου M. Αν $Ann(x) = (\delta)$, όπου $\delta = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ με $p_1, p_2, \ldots, p_k$ ανάγωγα στοιχεία, ανά δύο πρώτα και $\alpha_1, \alpha_2, \ldots, \alpha_k$ θετικοί ακέραιοι. Θέτουμε $\gamma_i = \prod_{\substack{1 \leq j \leq k \\ j \neq i}} p_j^{\alpha_j}$, για κάθε $i = 1, 2, \ldots, k$, δηλαδή $\gamma_1 = p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}, \gamma_2 = p_1^{\alpha_1} p_3^{\alpha_3} \cdots p_k^{\alpha_k}, \ldots, \gamma_k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{k-1}^{\alpha_{k-1}}$. Επίσης θέτουμε $x_i = \gamma_i x$, για κάθε $i = 1, 2, \ldots, k$. Τότε

$$(x) = (x_1) \oplus (x_2) \oplus \cdots \oplus (x_k),$$

με $Ann(x_i) = (p_i^{\alpha_i})$, για κάθε $i = 1, 2, \ldots, k$.
ΑΠΟΔΕΙΞΗ: Προφανώς $x_i \in (x)$, για κάθε $i = 1, 2, \ldots, k$. Παρατηρούμε ότι $r \in Ann(x_i) \Leftrightarrow$ $\Leftrightarrow rx_i = r\gamma_i x = 0_M \Leftrightarrow r\gamma_i \in Ann(x) = (\delta) \Leftrightarrow \delta = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \mid r p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k} \Leftrightarrow$ $\Leftrightarrow p_i^{\alpha_i} \mid r \Leftrightarrow r \in (p_i^{\alpha_i})$.
Επίσης, $(\gamma_1, \gamma_2, \ldots, \gamma_k) = (1_R) = R$. Πράγματι, έστω ότι υπάρχει κοινός ανάγωγος διαιρέτης p των $\gamma_1, \gamma_2, \ldots, \gamma_k$. Επειδή $p \mid \gamma_1 = p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$, το p θα ήταν συντροφικό με κάποιο p_i, όπου $i \geq 2$. Αλλά $p \mid \gamma_i = p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k}$ και επομένως το p θα ήταν συντροφικό με κάποιο p_j, όπου $j \neq i$. Άρα $p_j \sim p \sim p_i$, άτοπο. Εφόσον λοιπόν $(\gamma_1, \gamma_2, \ldots, \gamma_k) = (1_R)$, θα υπάρχουν $r_1, r_2, \ldots, r_k \in R$ τέτοια, ώστε $1_R = r_1\gamma_1 + r_2\gamma_2 + \cdots + r_k\gamma_k \Rightarrow x = r_1\gamma_1 x + r_2\gamma_2 x + \cdots + r_k\gamma_k x =$ $= r_1 x_1 + r_2 x_2 + \cdots + r_k x_k \in (x_1) + (x_2) + \cdots + (x_k)$. Απομένει να δείξουμε ότι το άθροισμα $(x_1) + (x_2) + \cdots + (x_k)$ είναι ευθύ.
Έστω λοιπόν $r_1x_1 + r_2x_2 + \cdots + r_kx_k = 0_M$. Πολλαπλασιάζουμε τη σχέση αυτή με γ_1 και παίρνουμε $r_1\gamma_1x_1 + r_2\gamma_1x_2 + \cdots + r_k\gamma_1x_k = 0_M$. Επειδή $p_i^{\alpha_i} \mid \gamma_1$ και $(p_i^{\alpha_i}) = Ann(x_i)$, για κάθε $i = 2, 3, \ldots, k$, θα πάρουμε $\gamma_1x_2 = \cdots = \gamma_1x_k = 0_M$ και επομένως $r_1\gamma_1x_1 = r_1\gamma_1^2 x = 0_M$. Αυτό σημαίνει ότι $r_1\gamma_1^2 \in Ann(x) = (\delta) = (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) \Leftrightarrow p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \mid r_1\gamma_1^2 = r_1 p_2^{2\alpha_2} \cdots p_k^{2\alpha_k} \Leftrightarrow$ $\Leftrightarrow p_1^{\alpha_1} \mid r_1 p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ και επειδή τα $p_1^{\alpha_1}$ και $p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ είναι πρώτα μεταξύ τους, $p_1^{\alpha_1} \mid r_1$. (Βλέπε λήμμα 2.24). Επομένως $r_1x_1 = 0_M$. Η ίδια απόδειξη θα μπορούσε να γίνει για κάθε $i = 1, 2, \ldots, k$ ή, αφού δείξαμε ότι $r_1x_1 = 0_M$, να προχωρούσαμε με επαγωγή επί του k. ■

Ξαναδιατυπώνουμε τώρα το πόρισμα 4.18 με βάση τους στοιχειώδεις διαιρέτες μιας πεπερασμένα παραγόμενης αβελιανής ομάδος (ℤ-προτύπου) και στη συνέχεια ξαναλύνουμε τα παραδείγματα 4.19.

ΠΟΡΙΣΜΑ 4.31. Έστω G μια πεπερασμένα παραγόμενη αβελιανή ομάδα. Έστω $p_1^{\lambda_{11}} \leq p_1^{\lambda_{12}} \leq \cdots \leq p_1^{\lambda_{1,k_{p_1}}}, p_2^{\lambda_{21}} \leq p_2^{\lambda_{22}} \leq \cdots \leq p_2^{\lambda_{2,k_{p_2}}}, \ldots, p_t^{\lambda_{t1}} \leq p_t^{\lambda_{t2}} \leq \cdots \leq p_t^{\lambda_{t,k_{p_t}}}$ οι στοιχειώδεις διαιρέτες της G. (Δυνάμεις πρώτων ακεραίων). Τότε η G αναλύεται κατά μοναδικό τρόπο ως

$$G \cong \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{k_{p_i}} \mathbb{Z}_{p_i^{\lambda_{ij}}} \oplus \underbrace{\mathbb{Z} \oplus \mathbb{Z} \cdots \oplus \mathbb{Z}}_{r \text{ το πλήθος}}.$$

Ιδιαιτέρως, αν η G είναι πεπερασμένη, τότε

$$G \cong \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{k_{p_i}} \mathbb{Z}_{p_i^{\lambda_{ij}}}$$

και $|G| = \prod_{i=1}^{t} \prod_{j=1}^{k_{p_i}} p_i^{\lambda_{ij}} = \prod_{i=1}^{t} p_i^{\sum_{j=1}^{k_{p_i}} \lambda_{ij}}$. ■

ΠΑΡΑΔΕΙΓΜΑ 4.32. (i) Να ταξινομηθούν όλες οι ανά δύο μη ισόμορφες αβελιανές ομάδες τάξεως 432.

ΛΥΣΗ: $432 = 2^4 \cdot 3^3$. Για το 2 έχουμε τις ακόλουθες περιπτώσεις: 2^4, $2 \mid 2^3$, $2^2 \mid 2^2$, $2 \mid 2 \mid 2^2$ και $2 \mid 2 \mid 2 \mid 2$. Για το 3 έχουμε τις ακόλουθες περιπτώσεις: 3^3, $3 \mid 3^2$ και $3 \mid 3 \mid 3$. Συνδυάζοντας τα ανωτέρω παίρνουμε τις ακόλουθες περιπτώσεις για τους στοιχειώδεις διαιρέτες:

1) $2^4,\ 3^3$, **2)** $2^4,\ 3 \mid 3^2$, **3)** $2^4,\ 3 \mid 3 \mid 3$, **4)** $2 \mid 2^3,\ 3^3$,
5) $2 \mid 2^3,\ 3 \mid 3^2$, **6)** $2 \mid 2^3,\ 3 \mid 3 \mid 3$, **7)** $2^2 \mid 2^2,\ 3^3$, **8)** $2^2 \mid 2^2,\ 3 \mid 3^2$,
9) $2^2 \mid 2^2,\ 3 \mid 3 \mid 3$, **10)** $2 \mid 2 \mid 2^2,\ 3^3$, **11)** $2 \mid 2 \mid 2^2,\ 3 \mid 3^2$, **12)** $2 \mid 2 \mid 2^2,\ 3 \mid 3 \mid 3$,
13) $2 \mid 2 \mid 2 \mid 2,\ 3^3$, **14)** $2 \mid 2 \mid 2 \mid 2,\ 3 \mid 3^2$, **15)** $2 \mid 2 \mid 2,\ 3 \mid 3 \mid 3$.

Μια αβελιανή ομάδα τάξεως 432 είναι λοιπόν ισόμορφη με μια από τις παρακάτω ομάδες:

1) $\mathbb{Z}_{16} \oplus \mathbb{Z}_{27}$, **2)** $\mathbb{Z}_{16} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$,
3) $\mathbb{Z}_{16} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, **4)** $\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{27}$,
5) $\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$, **6)** $\mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$,
7) $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{27}$, **8)** $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$,
9) $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, **10)** $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{27}$,
11) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$, **12)** $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$,
13) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27}$, **14)** $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$,
15) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. ■

(ii) Να βρεθούν οι στοιχειώδεις διαιρέτες και η πρωταρχικ ή ανάλυση της αβελιανής ομάδας τάξεως $2^3 \cdot 5^3 \cdot 7^4$, η οποία έχει πρώτο αναλλοίωτο παράγοντα $\delta_1 = 7$ και τελευταίο τον $\delta_\nu = 2^2 \cdot 5 \cdot 7$.

ΛΥΣΗ: Στο παράδειγμα 4.19.(ii) έχουμε βρει ότι οι αναλλοίωτοι παράγοντες της ομάδας είναι οι $\delta_1 = 7$, $\delta_2 = 5 \cdot 7$, $\delta_3 = 2 \cdot 5 \cdot 7$ και $\delta_4 = 2^2 \cdot 5 \cdot 7$. Με βάση και την πρόταση 4.29 παίρνουμε τους στοιχειώδεις διαιρέτες αυτής: 2, 2^2, 5, 5, 5, 7, 7, 7 και 7. Η πρωταρχική ανάλυση της ομάδας είναι λοιπόν $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$. ■

Το πόρισμα 4.30 μας παρέχει ένα ενδιαφέρον αποτέλεσμα, το οποίο είναι το αντίστροφο του θεωρήματος Lagrange για τις αβελιανές ομάδες.

ΠΟΡΙΣΜΑ 4.33. Έστω G μια πεπερασμένη αβελιανή ομάδα τάξεως m. Τότε, για κάθε διαιρέτη n του $m = |G|$, η G έχει μια (τουλάχιστον) υποομάδα τάξεως n.

ΑΠΟΔΕΙΞΗ: Έστω $G = \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{k_{p_i}} (x_{p_i,j})$ η πρωταρχική ανάλυση της G σε άθροισμα κυκλικών υποπροτύπων, όπου $|(x_{p_i,j})| = p_i^{\lambda_{ij}}$ με $\lambda_{ij} \leq \lambda_{i,j+1}$. Τότε $m = |G| = \prod_{i=1}^{t} p_i^{\sum_{i=1}^{k_{p_i}} \lambda_{ij}}$. Έστω $n = \prod_{i=1}^{t} p_i^{\alpha_i}$ με $\alpha_i \leq \sum_{j=1}^{k_{p_i}} \lambda_{ij}$, για κάθε $i = 1, 2, \ldots, t$. Τότε για κάθε i και j υπάρχει μη αρνητικός ακέραιος μ_{ij} έτσι, ώστε $\alpha_i = \sum_{j=1}^{k_{p_i}} \mu_{ij}$. Θεωρούμε την υποομάδα $H \leqslant G$, όπου $H = \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{k_{p_i}} (p_i^{\lambda_{ij}-\mu_{ij}} x_{p_i,j})$. Τότε $|(p_i^{\lambda_{ij}-\mu_{ij}} x_{p_i,j})| = p_i^{\mu_{ij}}$, για κάθε $j = 1, 2, \ldots, k_i$ και $i = 1, 2, \ldots, t$. Επομένως $|H| = \prod_{i=1}^{t} p_i^{\sum_{i=1}^{k_{p_i}} \mu_{ij}} = \prod_{i=1}^{t} p_i^{\alpha_i} = n$. ■

Κεφάλαιο 5

Ρητή Κανονική Μορφή Τετραγωνικού Πίνακα-Μορφή Jordan

5.1 Ένας $\mathbb{K}$-Διανυσματικός Χώρος ως ένα $\mathbb{K}[x]$-Πρότυπο

Σ' αυτό το κεφάλαιο θα μελετήσουμε μια γραμμική συνάρτηση $f : V \to V$, όπου V ένας διανυσματικός χώρος πεπερασμένης διάστασης υπεράνω ενός σώματος $\mathbb{K}$, δηλαδή θα μελετήσουμε έναν $\mathbb{K}$-ενδομορφισμό $f \in \mathrm{End}_{\mathbb{K}}(V)$. Για το σκοπό αυτό θα χρησιμοποιήσουμε πολλές φορές τη γλώσσα των προτύπων επί του πολυωνυμικού δακτυλίου $\mathbb{K}[x]$, ο οποίος ξέρουμε ότι είναι ευκλείδειος περιοχή, άρα περιοχή κυρίων ιδεωδών.
Γνωρίζουμε, από το παράδειγμα 3.2.(ii) ότι μέσω της $f : V \to V$, ο διανυσματικός χώρος V καθίσταται ένα $\mathbb{K}[x]$-πρότυπο, όπου $h(x)v = h(f)(v)$. Πιο συγκεκριμένα, υπενθυμίζουμε ότι με f^n συμβολίσουμε τη σύνθεση $\underbrace{f \circ f \circ \cdots \circ f}_{n \text{ φορές}}$, αν n θετικός ακέραιος και $f^0 = \mathbf{1}_V$, αν $n = 0$.
Αν $h(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in \mathbb{K}[x]$, τότε $h(f) = b_n f^n + b_{n-1}f^{n-1} + \cdots + b_1 f + b_0 \mathbf{1}_V \in$ $\in \mathrm{End}_{\mathbb{K}}(V)$, με $h(f)(v) = b_n f^n(v) + b_{n-1}f^{n-1}(v) + \cdots + b_1 f(v) + b_0 v$, για κάθε $v \in V$.

5.2 Χαρακτηριστικό Πολυώνυμο Πίνακα ή Απεικόνισης-Θεώρημα Cayley-Hamilton-Ελάχιστο Πολυώνυμο

Ας θυμηθούμε κάποια βασικά αποτελέσματα από τη Γραμμική Άλγεβρα.
1) Αν $\hat{v} = (v_1, v_2, \ldots, v_m)$ είναι μια βάση του V επί του $\mathbb{K}$ και $f \in \mathrm{End}_{\mathbb{K}}(V)$, τότε η f καθορίζεται $\big($και καθορίζει$\big)$ μονοσήμαντα από τον πίνακα $A = (\alpha_{ij}) \in \mathbb{K}^{m\times m}$, βάσει των σχέσεων

$$f(v_j) = \sum_{i=1}^{m} \alpha_{ij} v_i, \qquad (1)$$

για κάθε $j = 1, 2, \ldots, m$. Ο πίνακας A ονομάζεται πίνακας της f ως προς τη βάση $\hat{v}$ και συμβολίζεται με $(f \mid \hat{v}, \hat{v})$ ή πιο απλά με $(f \mid \hat{v})$. Αν $\hat{u} = (u_1, u_2, \ldots, u_m)$ είναι μια άλλη βάση του V, τότε ο πίνακας $B = (\beta_{ij}) = (\mathbf{1}_V \mid \hat{u}, \hat{v})$, ο οποίος καθορίζεται από τις σχέσεις

$$u_j = \sum_{i=1}^{m} \beta_{ij} v_i, \qquad (2)$$

είναι αντιστρέψιμος με αντίστροφο τον πίνακα $B^{-1} = (\mathbf{1}_V \mid \hat{v}, \hat{u})$. Αν τώρα $A' = (f \mid \hat{u})$, τότε ισχύει η σχέση

$$A' = B^{-1}AB.$$

2) Το χαρακτηριστικό πολυώνυμο $ch_f(x)$ μιας απεικόνισης $f \in \mathrm{End}_{\mathbb{K}}(V)$ ορίζεται ως το

πολυώνυμο

$$ch_f(x) = \det(xI_m - A), \qquad \textbf{(3)}$$

όπου A ο πίνακας της f ως προς κάποια βάση $\hat{v} = (v_1, v_2, \ldots, v_m)$ του V. Το χαρακτηριστικό πολυώνυμο της f είναι ανεξάρτητο της χρησιμοποιούμενης βάσης. Γιατί, αν $A' = (f \mid \hat{u})$, όπου $u = (u_1, u_2, \ldots, u_m)$ είναι μια άλλη βάση του V και $B = (\mathbf{1}_V \mid \hat{u}, \hat{v})$ ο πίνακας αλλαγής βάσης, τότε $A' = B^{-1}AB$ και συνεπώς $\det(xI_m - A') = \det(xB^{-1}B - B^{-1}AB) = = \det\left(B^{-1}(xI_m - A)B\right) = \det(xI_m - A)$. Ως χαρακτηριστικό πολυώνυμο $ch_A(x)$ ενός $m \times m$ πίνακα ορίζεται επίσης το $\det(xI_m - A)$.

Τώρα, ένας τετραγωνικός πίνακας λέγεται πολυωνυμικός αν τα στοιχεία του είναι πολυώνυμα του x. Για παράδειγμα, ο πίνακας $\begin{pmatrix} -2x^3 + x^2 + 5x - 4 & 3x^2 + 4x - 1 \\ x^3 - 2x + 5 & x + 3 \end{pmatrix}$ είναι ένας 2×2 πολυωνυμικός πίνακας. Ο παραπάνω πίνακας μπορεί να γραφεί στη μορφή

$$x^3 \begin{pmatrix} -2 & 0 \\ 1 & 0 \end{pmatrix} + x^2 \begin{pmatrix} 1 & 3 \\ 0 & 0 \end{pmatrix} + x \begin{pmatrix} 5 & 4 \\ -2 & 1 \end{pmatrix} + \begin{pmatrix} -4 & -1 \\ 5 & 3 \end{pmatrix}.$$

Γενικά κάθε $m \times m$ πολυωνυμικός πίνακας μπορεί να γραφεί στη μορφή

$$x^k A_k + x^{k-1} A_{k-1} + \cdots + xA_1 + A_0,$$

όπου A_i σταθεροί $m \times m$ πίνακες και x^k η μέγιστη δύναμη στην οποία εμφανίζεται το x στα στοιχεία του πίνακα.

Ο προσαρτημένος $\left(\text{adjoint}\right)$ πίνακας ενός $m \times m$ πίνακα A είναι ο ανάστροφος του πίνακα $\left((-1)^{i+j} M_{ij}\right)$, όπου M_{ij} η ορίζουσα του πίνακα που προκύπτει από τον A αν διαγράψουμε την i-γραμμή και την j-στήλη. Είναι δηλαδή $\text{adj}A = \left((-1)^{i+j} M_{ij}\right)^T = \left((-1)^{i+j} M_{ji}\right)$. Γνωρίζουμε από τη Γραμμική Άλγεβρα ότι ισχύει η σχέση

$$A \cdot \text{adj}A = |A| \cdot I_m, \qquad \textbf{(4)}$$

όπου $|A| = \det(A)$, κατά τα γνωστά.

Αν εφαρμόσουμε τη σχέση **(4)** στον πίνακα $xI_m - A$, θα πάρουμε τη σχέση

$$(xI_m - A) \cdot \text{adj}(xI_m - A) = |xI_m - A| \cdot I_m = ch_A(x) I_m. \qquad \textbf{(5)}$$

Παρατηρούμε ότι ο πίνακας $\text{adj}(xI_m - A)$ είναι ένας πολυωνυμικός πίνακας. Πράγματι, τα στοιχεία του είναι $(m-1) \times (m-1)$ ορίζουσες και η μεγαλύτερη δύναμη του x που μπορεί να προκύψει στον πίνακα αυτό είναι $m - 1$. Αυτό θα συμβεί όταν διαγράψουμε την i-γραμμή και την i-στήλη, δηλαδή όταν «αποκόψουμε» μόνον το στοιχείο $x - \alpha_{ii}$. Επομένως ο $\text{adj}(xI_m - A)$ γράφεται στη μορφή

$$\text{adj}(xI_m - A) = x^{m-1} B_{m-1} + x^{m-2} B_{m-2} + \cdots + xB_1 + B_0, \qquad \textbf{(6)}$$

όπου $B_0, B_1, \ldots, B_{m-1}$ σταθεροί πίνακες. Αλ' την άλλη μεριά, το χαρακτηριστικό πολυώνυμο $ch_A(x) = |xI_m - A|$ ενός $m \times m$ πίνακα A είναι βαθμού ακριβώς m γιατί στη διαγώνιο υπάρχουν τα στοιχεία $x - \alpha_{11}, x - \alpha_{22}, \ldots, x - \alpha_{mm}$. Για τον ίδιο λόγο είναι μάλιστα μονικό, καθώς ο συντελεστής του x^m είναι 1. Έστω $ch_A(x) = x^m + b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots b_1 x + b_0$. Αν πολλαπλασιάσουμε τη σχέση **(6)** από δεξιά με xI_m, θα πάρουμε

$$xI_m \cdot \text{adj}(xI_m - A) = x^m B_{m-1} + x^{m-1} B_{m-2} + \cdots + x^2 B_1 + xB_0 \qquad \textbf{(7)}$$

και με $-A$

$$-x^{m-1} AB_{m-1} - x^{m-2} AB_{m-2} - \cdots - xAB_1 - AB_0. \qquad \textbf{(8)}$$

Προσθέτοντας κατά μέλη τις σχέσεις **(7)** και **(8)** παίρνουμε

$$\begin{aligned}(xI_m - A) \cdot \text{adj}(xI_m - A) = x^m B_{m-1} + x^{m-1}(B_{m-2} - AB_{m-1}) + x^{m-2}(B_{m-3} - AB_{m-2}) + \cdots + \\ + x^2(B_1 - AB_2) + x(B_0 - AB_1) - AB_0 = ch_A(x) I_m = \\ = x^m I_m + b_{m-1} x^{m-1} I_m + b_{m-2} x^{m-2} I_m + \cdots b_1 x I_m + b_0 I_m.\end{aligned}$$

Εξισώνοντας τους συντελεστές του x παίρνουμε τις σχέσεις:

$$\begin{cases} B_{m-1} & = & I_m \\ B_{m-2} - AB_{m-1} & = & b_{m-1}I_m \\ B_{m-3} - AB_{m-2} & = & b_{m-2}I_m \\ & \vdots & \\ B_1 - AB_2 & = & b_2 I_m \\ B_0 - AB_1 & = & b_1 I_m \\ -AB_0 & = & b_0 I_m \end{cases} \qquad (9)$$

Αν πολλαπλασιάσουμε την πρώτη σχέση από αριστερά με A^m, τη 2η με A^{m-1}, την 3η με A^{m-2} κτλ, έως την προτελευταία, την οποία θα πολλαπλασιάσουμε με A, θα πάρουμε:

$$\begin{cases} \cancel{A^m B_{m-1}} & = & A^m \\ \cancel{A^{m-1}B_{m-2}} - \cancel{A^m B_{m-1}} & = & b_{m-1}A^{m-1} \\ \cancel{A^{m-2}B_{m-3}} - \cancel{A^{m-1}B_{m-2}} & = & b_{m-2}A^{m-2} \\ & \vdots & \\ \cancel{A^2 B_1} - \cancel{A^3 B_2} & = & b_2 A^2 \\ \cancel{AB_0} - \cancel{A^2 B_1} & = & b_1 A \\ \cancel{-AB_0} & = & b_0 I_m \end{cases} \qquad (10)$$

και με πρόσθεση κατά μέλη $\mathbf{O}_m = ch_A(A)$, δηλαδή ο A μηδενίζει το χαρακτηριστικό του πολυώνυμο. Τώρα, αν A είναι ο πίνακας ενός $\mathbb{K}$-ενδομορφισμού f του V ως προς κάποια βάση $\hat{v} = (v_1, v_2, \ldots, v_m)$ του V και $h(x) \in \mathbb{K}[x]$, τότε ο πίνακας $h(A)$ είναι ο πίνακας του ενδομορφισμού $h(f)$ του V. Επομένως και $ch_f(f) = \mathbf{O}_V : V \to V$ η μηδενική απεικόνιση. Έχουμε λοιπόν το γνωστό Θεώρημα Cayley-Hamilton.

ΘΕΩΡΗΜΑ 5.1. $\big($**ΘΕΩΡΗΜΑ CAYLEY-HAMILTON**$\big)$**:** Κάθε $\mathbb{K}$-ενδομορφισμός ενός διανυσματικού χώρου V, ισοδύναμα κάθε τετραγωνικός πίνακας μηδενίζει το χαρακτηριστικό του πολυώνυμο. ■

Τώρα, από όλα τα μη μηδενικά πολυώνυμα που μηδενίζονται από την f $\big($ή τον πίνακα $A\big)$ θεωρούμε ένα ελαχίστου βαθμού. Μπορούμε να υποθέσουμε ότι ο συντελεστής του μεγιστοβάθμιου όρου του πολυωνύμου αυτού είναι 1, δηλαδή το πολυώνυμο αυτό είναι μονικό. $\big($Αλλιώς διαιρούμε με τον συντελεστή αυτό$\big)$. Έστω $min_f(x)$ ένα τέτοιο πολυώνυμο.

ΘΕΩΡΗΜΑ 5.2. Το μη μηδενικό μονικό πολυώνυμο ελαχίστου βαθμού που μηδενίζεται από την f $\big($ή τον πίνακα $A\big)$ διαιρεί κάθε άλλο πολυώνυμο που μηδενίζεται από την f $\big($ή τον πίνακα $A\big)$. Ιδιαιτέρως, διαιρεί το χαρακτηριστικό πολυώνυμο της f. Επίσης είναι μοναδικό με αυτές τις ιδιότητες.

ΑΠΟΔΕΙΞΗ: Έστω $h(f) = \mathbf{O}_V$, όπου $h(x)$ μη μηδενικό πολυώνυμο. Έστω $h(x) = min_f(x)\pi(x) + \\ +\upsilon(x)$ η ταυτότητα της διαιρέσεως $h(x) : \min_f(x)$. Τότε $\upsilon(x) = 0$ ή $\deg \upsilon(x) < \deg min_f(x)$. Στη δεύτερη περίπτωση θα είχαμε $\upsilon(f) = h(f) - \min_f(f)\pi(f) = \mathbf{O}_V - \mathbf{O}_V\pi(f) = \mathbf{O}_V$, πράγμα αδύνατον, γιατί το $min_f(x)$ είναι πολυώνυμο ελαχίστου βαθμού που μηδενίζεται από την f και $\deg \upsilon(x) < \deg min_f(x)$. Άρα $min_f(x) \mid h(x)$. Επειδή αν ένα μονικό πολυώνυμο διαιρεί ένα άλλο μονικό του ιδίου βαθμού τότε συμπίπτει με αυτό, το $min_f(x)$ είναι μοναδικό. ■

ΟΡΙΣΜΟΣ 5.3. Το πολυώνυμο $min_f(x)$ που ορίσαμε προηγουμένως ονομάζεται **ελάχιστο πολυώνυμο της f** $\big($ή του πίνακα $A\big)$.

Μπορούμε εύκολα να αποδείξουμε το ακόλουθο:

ΠΡΟΤΑΣΗ 5.4. Κάθε ανάγωγος παράγοντας του χαρακτηριστικού πολυωνύμου $ch_A(x)$ του πίνακα A είναι και ανάγωγος παράγοντας κάθε μη μηδενικού πολυωνύμου που μηδενίζεται από τον πίνακα A.
ΑΠΟΔΕΙΞΗ: Έστω $h(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0$ ένα μη μηδενικό πολυώνυμο που μηδενίζεται από τον A. Τότε $h(A) = c_k A^k + c_{k-1}A^{k-1} + \cdots + c_1 A + c_0 I_m = \mathbf{O}_m$. Επομένως $h(x)I_m = h(xI_m) = h(xI_m) - h(A) = c_k((xI_m)^k - A^k) + c_{k-1}((xI_m)^{k-1} - A^{k-1}) + \cdots + c_1(xI_m - A)$. Αλλά $(xI_m)^i - A^i = (xI_m - A)(x^{i-1}I_m + x^{i-2}A + x^{i-3}A^2 + \cdots + xA^{i-2} + A^{i-1}) = (xI_m - A)L_i(x)$, όπου $L_i(x) = x^{i-1}I_m + x^{i-2}A + x^{i-3}A^2 + \cdots + xA^{i-2} + A^{i-1}$ ένας πολυωνυμικός πίνακας, για κάθε $i = 1, 2, \ldots, k$. Επομένως $h(x)I_m = (xI_m - A)\sum_{i=1}^{k} c_i L_i(x) = (xI_m - A)C(x)$, όπου $C(x) = \sum_{i=1}^{k} c_i L_i(x)$. Συνεπώς $h(x)^m = \det(h(x)I_m) = \det(xI_m - A)\det(C(x)) = ch_A(x)\det(C(x))$.
Από την τελευταία σχέση προκύπτει ότι κάθε ανάγωγος παράγοντας του $ch_A(x)$ διαιρεί το $h(x)^m$, άρα και το $h(x)$. ■

ΠΟΡΙΣΜΑ 5.5. Τα $ch_A(x)$ και $min_A(x)$ έχουν τους ίδιους ανάγωγους παράγοντες.
ΑΠΟΔΕΙΞΗ: Προκύπτει από την προηγούμενη πρόταση και το γεγονός ότι $min_A(x) \mid ch_A(x)$. ■

5.3 f-Αναλλοίωτοι Υπόχωροι-Κυκλικοί Υπόχωροι

ΟΡΙΣΜΟΣ 5.6. Έστω $W \leqslant V$ (υπόχωρος του V). Ο W λέγεται ***f*-αναλλοίωτος ή αναλλοίωτος ως προς *f*** αν και μόνον αν $f(W) \subseteq W$. Για παράδειγμα, ο μηδενικός υπόχωρος $\{0_V\}$ και ολόκληρος ο χώρος V είναι f-αναλλοίωτοι.

ΠΑΡΑΤΗΡΗΣΗ: Είναι σαφές ότι αν ο υπόχωρος W είναι f-αναλλοίωτος (ή απλά αναλλοίωτος), τότε $h(x)W \subseteq W \Leftrightarrow h(f)(W) \subseteq W$, για κάθε πολυώνυμο $h(x) \in \mathbb{K}[x]$. Επομένως ο W είναι ένα $\mathbb{K}[x]$-υποπρότυπο του $\mathbb{K}[x]$-προτύπου V. **Επομένως οι έννοιες του *f*-αναλλοίωτου υπόχωρου και του $\mathbb{K}[x]$-υποπροτύπου ταυτίζονται**.

ΟΡΙΣΜΟΣ 5.7. Έστω $v \in V$. **Ο κυκλικός υπόχωρος $Z_v = (v)$ που παράγεται από το v** είναι ο υπόχωρος που αποτελείται από τα διανύσματα $h(f)(v)$, ή στη γλώσσα των προτύπων, από τα στοιχεία $h(x)v$, για κάθε $h(x) \in \mathbb{K}[x]$. Προφανώς ο κυκλικός υπόχωρος
$$Z_v = \mathbb{K}[x]v = \{h(x)v \mid h(x) \in \mathbb{K}[x]\} = \{h(f)(v) \mid h(x) \in \mathbb{K}[x]\}$$
είναι f-αναλλοίωτος.

Έστω v μη μηδενικό διάνυσμα. Θεωρούμε την ακολουθία διανυσμάτων $v = f^0(v), f(v), f^2(v), \ldots$ Επειδή $\dim_{\mathbb{K}} V = m < \infty$, οι όροι της ακολουθίας αυτής δεν μπορούν να είναι γραμμικώς ανεξάρτητα. Θεωρούμε τον ελάχιστο θετικό ακέραιο μ με την ιδιότητα τα διανύσματα $v, f(v), f^2(v), \ldots, f^{\mu-1}(v), f^\mu(v)$ να είναι γραμμικώς εξαρτημένα. Τότε τα διανύσματα $v, f(v), f^2(v), \ldots, f^{\mu-1}(v)$ είναι γραμμικώς ανεξάρτητα και το $f^\mu(v)$ είναι γραμμικός συνδυασμός των προηγουμένων. Κατά συνέπεια ο κυκλικός υπόχωρος που παράγεται από το v έχει σαν βάση τα διανύσματα $v_1 = v, v_2 = f(v), v_3 = f^2(v), \ldots, v_\mu = f^{\mu-1}(v)$. Επίσης $f(v_\mu) = f^\mu(v) = -\alpha_0 v - \alpha_1 f(v) - \alpha_2 f^2(v) - \cdots - \alpha_{\mu-1}f^{\mu-1}(v) \Leftrightarrow h(f)(v) = 0_V$, όπου $h(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{\mu-1}x^{\mu-1} + x^\mu$. Ισοδύναμα $f(v_i) = v_{i+1}$, για κάθε $i = 1, 2, \ldots, \mu - 1$ και $f(v_\mu) = \alpha_0 v_1 - \alpha_1 v_2 - \alpha_2 v_3 - \cdots - \alpha_{\mu-1}v_\mu$. Ο πίνακας του περιορισμού $f|_{(v)}$ της f στον κυκλικό

υπόχωρο που παράγεται από το v $\big($ως προς τη βάση $(v_1, v_2, \dots, v_\mu)\big)$ είναι ο

$$\Sigma(h(x)) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -\alpha_0 \\ 1 & 0 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & 0 & \cdots & 0 & -\alpha_2 \\ 0 & 0 & 1 & \cdots & 0 & -\alpha_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -\alpha_{\mu-1} \end{pmatrix}$$

ΟΡΙΣΜΟΣ 5.8. Ο πίνακας $\Sigma(h(x))$ λέγεται **συνοδός πίνακας** $\big($companion matrix$\big)$ **του πολυωνύμου** $\boldsymbol{h(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{\mu-1} x^{\mu-1} + x^\mu}$.

ΠΡΟΤΑΣΗ 5.9. Το χαρακτηριστικό και το ελάχιστο πολυώνυμο του συνοδού πίνακα $\Sigma(h(x))$ ενός μονικού πολυωνύμου $h(x)$ συμπίπτουν με το $h(x)$.

ΑΠΟΔΕΙΞΗ: Ο πίνακας $\Sigma(h(x))$ είναι ο πίνακας ενός $\mathbb{K}$-ενδομορφισμού f ενός διανυσματικού χώρου $W = (v_1)$ με βάση $(v_1, v_2, \dots, v_\mu)$. Η f δρα επί των στοιχείων της βάσης ως εξής: $f(v_i) = v_{i+1}$, για κάθε $i = 1, 2, \dots, \mu-1$ και $f(v_\mu) = -\alpha_0 v_1 - \alpha_1 v_2 - \alpha_2 v_3 - \cdots - \alpha_{\mu-1} v_\mu$, δηλαδή $h(f)(v_1) = \big(f^\mu + \alpha_{\mu-1} f^{\mu-1} + \alpha_{\mu-2} f^{\mu-2} + \cdots + \alpha_1 f + \alpha_0 \mathbf{1}_V\big)(v_1) = 0_V$. Επειδή $v_i = f^{i-1}(v_1)$, για κάθε $i = 2, 3, \dots, \mu$, θα έχουμε και $h(f)(v_i) = h(f) f^{i-1}(v_1) = f^{i-1} h(f)(v_1) = f^{i-1}\big(h(f)(v_1)\big) = = f^{i-1}(0_V) = 0_V$. Το $h(x)$ μηδενίζει λοιπόν την f, άρα και τον αντίστοιχο πίνακα $\Sigma(h(x))$. Επειδή είναι μονικό και $\deg h(x) = \dim W$, το $h(x)$ είναι το χαρακτηριστικό πολυώνυμο του $\Sigma(h(x))$.

Έστω $\sigma(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \cdots + \beta_{k-1} x^{k-1} + x^k$ το ελάχιστο πολυώνυμο του $\Sigma(h(x))$. Υποθέτουμε ότι $k < \mu$. Τότε $\beta_0 v_1 + \beta_1 f(v_1) + \beta_2 f^2(v_1) + \cdots + \beta_{k-1} f^{k-1}(v_1) + f^k(v_1) = 0_V$, ισοδύναμα $v_{k+1} = -\beta_{k-1} v_k - \cdots - \beta_2 v_3 - \beta_1 v_2 - \beta_0 v_1$, άτοπο, γιατί τα διανύσματα $v_1, v_2, \dots, v_k, v_{k+1}$ είναι γραμμικώς ανεξάρτητα. Άρα $k = \mu$ και επειδή $\sigma(x) \mid h(x)$, έπεται ότι $\sigma(x) = h(x)$. ■

ΣΗΜΕΙΩΣΗ: Ότι το χαρακτηριστικό πολυώνυμο του πίνακα $\Sigma(h(x))$ είναι το $h(x)$ αποδεικνύεται και στοιχειωδώς $\big($μόνο με πίνακες$\big)$ ως εξής: Έχουμε

$$ch_{\Sigma(h(x))}(x) = \begin{vmatrix} x & 0 & 0 & \cdots & 0 & \alpha_0 \\ -1 & x & 0 & \cdots & 0 & \alpha_1 \\ 0 & -1 & x & \cdots & 0 & \alpha_2 \\ 0 & 0 & -1 & \cdots & 0 & \alpha_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x & \alpha_{\mu-2} \\ 0 & 0 & 0 & \cdots & -1 & x + \alpha_{\mu-1} \end{vmatrix}$$

Αν προσθέσουμε την τελευταία γραμμή, πολλαπλασιασμένη επί x στην προτελευταία θα πάρουμε

$$ch_{\Sigma(h(x))}(x) = \begin{vmatrix} x & 0 & 0 & \cdots & 0 & \alpha_0 \\ -1 & x & 0 & \cdots & 0 & \alpha_1 \\ 0 & -1 & x & \cdots & 0 & \alpha_2 \\ 0 & 0 & -1 & \cdots & 0 & \alpha_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & x^2 + \alpha_{\mu-1} x + \alpha_{\mu-2} \\ 0 & 0 & 0 & \cdots & -1 & x + \alpha_{\mu-1} \end{vmatrix}$$

Πάλι, προσθέτουμε την προτελευταία, πολλαπλασιασμένη επί x στην αμέσως προηγούμενη κ.ο.κ. Τελικώς θα καταλήξουμε στην ορίζουσα

$$ch_{\Sigma(h(x))}(x) = \begin{vmatrix} 0 & 0 & 0 & \cdots & 0 & h(x) \\ -1 & 0 & 0 & \cdots & 0 & \star \\ 0 & -1 & 0 & \cdots & 0 & \star \\ 0 & 0 & -1 & \cdots & 0 & \star \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \star \\ 0 & 0 & 0 & \cdots & -1 & \star \end{vmatrix}$$

Αναπτύσσουμε τώρα την ορίζουσα ως προς την πρώτη γραμμή και παίρνουμε

$$(-1)^{\mu-1}h(x)\det(-I_{\mu-1}) = (-1)^{\mu-1}(-1)^{\mu-1}h(x)\det(I_{\mu-1}) = h(x).$$

5.4 Ο Διανυσματικός χώρος V ως Πηλίκο Ελεύθερων $\mathbb{K}[x]$-Προτύπων

Επανερχόμαστε τώρα στη θεώρηση του διανυσματικού χώρου V με βάση $(v_1, v_2, \ldots, v_m)$ ως ένα πεπερασμένα παραγόμενο $\mathbb{K}[x]$-πρότυπο. Όπως αναφέραμε στην αρχή του κεφαλαίου αυτού, αν $f \in \mathrm{End}_{\mathbb{K}}(V)$, δηλαδή μια $\mathbb{K}$-γραμμική απεικόνιση $f : V \to V$, τότε μπορούμε να θεωρήσουμε τον V ως ένα $\mathbb{K}[x]$-πρότυπο με δράση $h(x)v = h(f)(v)$, για κάθε $h(x) \in \mathbb{K}[x]$ και $v \in V$.

Ο V ως ένα $\mathbb{K}[x]$-πρότυπο, είναι πεπερασμένα παραγόμενο, αφού τα στοιχεία της βάσης του είναι προφανώς $\mathbb{K}[x]$-γεννήτορες αυτού.

Έστω $F = \mathbb{K}[x]e_1 \oplus \mathbb{K}[x]e_2 \oplus \cdots \oplus \mathbb{K}[x]e_m$ ένα ελεύθερο $\mathbb{K}[x]$-πρότυπο με βάση $(e_1, e_2, \ldots, e_m)$. Ορίζουμε την απεικόνιση $T : F \to V$ με

$$T\big(h_1(x)e_1 + h_2(x)e_2 + \cdots + h_m(x)e_m\big) = h_1(f)(v_1) + h_2(f)(v_2) + \cdots + h_m(f)(v_m),$$

για κάθε $h_1(x), h_2(x), \ldots, h_m(x) \in \mathbb{K}[x]$. Η T είναι $\mathbb{K}[x]$-ομομορφισμός, αφού αν $h'_1(x)e_1 + h'_2(x)e_2 + \cdots + h'_m(x)e_m \in F$, τότε

$$\begin{aligned} &T\big((h_1(x)e_1 + h_2(x)e_2 + \cdots + h_m(x)e_m) + (h'_1(x)e_1 + h'_2(x)e_2 + \cdots + h'_m(x)e_m)\big) = \\ &= T\big((h_1(x) + h'_1(x))e_1 + (h_2(x) + h'_2(x))e_2 + \cdots + (h_m(x) + h'_m(x))e_m\big) = \\ &= (h_1(f) + h'_1(f))(v_1) + (h_2(f) + h'_2(f))(v_2) + \cdots + (h_m(f) + h'_m(f))(v_m) = \\ &= h_1(f)(v_1) + h'_1(f)(v_1) + h_2(f)(v_2) + h'_2(f)(v_2) + \cdots + h_m(f)(v_m) + h'_m(f)(v_m) = \\ &= \big(h_1(f)(v_1) + h_2(f)(v_2) + \cdots + h_m(f)(v_m)\big) + \big(h'_1(f)(v_1) + h'_2(f)(v_2) + \cdots + h'_m(f)(v_m)\big) = \\ &= T\big(h_1(x)e_1 + h_2(x)e_2 + \cdots + h_m(x)e_m\big) + T\big(h'_1(x)e_1 + h'_2(x)e_2 + \cdots + h'_m(x)e_m\big) \end{aligned}$$

και

$$\begin{aligned} &T\big(r(x)(h_1(x)e_1 + h_2(x)e_2 + \cdots + h_m(x)e_m)\big) = \\ &= T\big(r(x)h_1(x)e_1 + r(x)h_2(x)e_2 + \cdots + r(x)h_m(x)e_m\big) = \\ &= r(f)h_1(f)(v_1) + r(f)h_2(f)(v_2) + \cdots + r(f)h_m(f)(v_m) = \\ &= r(f)\big(h_1(f)(v_1) + h_2(f)(v_2) + \cdots + h_m(f)(v_m)\big) = \\ &= r(f)\big(T\big(h_1(x)e_1 + h_2(x)e_2 + \cdots + h_m(x)e_m\big)\big) = \\ &= r(x)T\big(h_1(x)e_1 + h_2(x)e_2 + \cdots + h_m(x)e_m\big). \end{aligned}$$

Η απεικόνιση $T : F \to V$ είναι $\mathbb{K}[x]$-επιμορφισμός. Πράγματι, αν $v = s_1v_1 + s_2v_2 + \cdots + s_mv_m \in V$, με $s_i \in \mathbb{K}$, για κάθε $i = 1, 2, \ldots, m$, τότε θεωρούμε τα σταθερά πολυώνυμα $h_i(x) = s_i$, για κάθε $i = 1, 2, \ldots, m$. Έχουμε: $T(s_1e_1 + s_2e_2 + \cdots + s_me_m) = s_1\mathbf{1}_V(v_1) + s_2\mathbf{1}_V(v_2) + \cdots + s_m\mathbf{1}_V(v_m) = s_1v_1 + s_2v_2 + \cdots + s_mv_m = v$.

Τίθεται τώρα το ερώτημα: Ποιος είναι ο πυρήνας του T; Εφόσον ο $\mathrm{Ker}T$ είναι υποπρότυπο του ελεύθερου προτύπου F, ο $\mathrm{Ker}T$ είναι ένα ελεύθερο υποπρότυπο αυτού. (Πρόταση 3.51). Αν προσδιορίσουμε μια βάση του $\mathrm{Ker}T$, τότε από την πρόταση 4.7 και εφαρμόζοντας τον αλ-

γόριθμο Smith μπορούμε να προσδιορίσουμε τη δομή του $V \cong {}^{F}\Big/_{\mathrm{Ker}T}$ ως ευθύ άθροισμα κυκλικών υποπροτύπων. Το μόνο που ξέρουμε είναι ότι οι σταθερές δρουν ως σταθερές επί του V, αλλά το x δρα όπως ο $\mathbb{K}$-ενδομορφισμός f του V. Συγκεκριμένα, έχουμε τις σχέσεις:

$$T(xe_j) = f(v_j) = \sum_{i=1}^{m} \alpha_{ij} v_i = T\Big(\sum_{i=1}^{m} \alpha_{ij} e_i \Big), \text{ για κάθε } j = 1, 2, \ldots, m,$$

δηλαδή $$T\Big(xe_j - \sum_{i=1}^{m} \alpha_{ij} e_i \Big) = 0_V, \text{ για κάθε } j = 1, 2, \ldots, m.$$

ΘΕΩΡΗΜΑ 5.10. Τα στοιχεία $w_j = xe_j - \sum_{i=1}^{m} \alpha_{ij} e_i$, όπου $j = 1, 2, \ldots, m$, αποτελούν βάση του $\mathbb{K}[x]$-προτύπου $\mathrm{Ker}T$.

ΑΠΟΔΕΙΞΗ: Αρχικώς θα αποδείξουμε ότι τα $w_1, w_2, \ldots, w_m$ είναι $\mathbb{K}[x]$-γραμμικώς ανεξάρτητα. Έστω λοιπόν $h_1(x)w_1 + h_2(x)w_2 + \cdots + h_m(x)w_m = 0_F$, για κάποια πολυώνυμα $h_1(x), h_2(x), \ldots, h_m(x) \in \mathbb{K}[x]$, όχι όλα μηδέν. Από τα μη μηδενικά $h_1(x), h_2(x), \ldots, h_m(x)$ επιλέγουμε ένα με το μεγαλύτερο δυνατό βαθμό. $\big($Πιθανότατα μηδέν$\big)$. Χωρίς βλάβη της γενικότητας, ας είναι αυτό το $h_1(x)$. Παρατηρούμε ότι στο άθροισμα $h_1(x)w_1 + h_2(x)w_2 + \cdots + h_m(x)w_m = $
$= h_1(x)xe_1 - \sum_{i=1}^{m} h_1(x)\alpha_{i1}e_i + h_2(x)xe_2 - \sum_{i=1}^{m} h_2(x)\alpha_{i2}e_i + \cdots + h_m(x)xe_m - \sum_{i=1}^{m} h_m(x)\alpha_{im}e_i$ το e_1 εμφανίζεται με συντελεστή $h_1'(x) = h_1(x)x - h_1(x)\alpha_{11} - h_2(x)\alpha_{12} - \cdots - h_m(x)\alpha_{1m}$. Επειδή από τα $h_2(x), \ldots, h_m(x)$ άλλα είτε είναι μηδενικά είτε έχουν βαθμό μικρότερο ή ίσο του $h_1(x)$, έχουμε $\deg h_1'(x) = \deg(h_1(x)x) = \deg h_1(x) + 1 > \deg h_1(x)$ και άρα το πολυώνυμο $h_1'(x)$, το οποίο είναι ο συντελεστής του e_1 στο ανάπτυγμα του $h_1(x)w_1 + h_2(x)w_2 + \cdots + h_m(x)w_m = 0_F$ ως $\mathbb{K}[x]$-γραμμικού συνδυασμού των στοιχείων της βάσης $(e_1, e_2, \ldots, e_m)$ είναι διάφορο του μηδενικού. Αυτό είναι άτοπο, γιατί το F είναι ελεύθερο $\mathbb{K}[x]$-πρότυπο επί του $e_1, e_2, \ldots, e_m$. Συνεπώς τα $w_1, w_2, \ldots, w_m$ είναι $\mathbb{K}[x]$-γραμμικώς ανεξάρτητα.

Τώρα θα αποδείξουμε ότι τα $w_1, w_2, \ldots, w_m$ παράγουν τον $\mathrm{Ker}T$. Έστω $h_1(x)e_1 + h_2(x)e_2 + \cdots + h_m(x)e_m \in \mathrm{Ker}T$. Αν όλα τα $h_j(x) = \lambda_j \in \mathbb{K}$ ήταν σταθερά, τότε θα είχαμε $T(h_1(x)e_1 + h_2(x)e_2 + \cdots + h_m(x)e_m) = T(\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_m e_m) = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_m v_m = 0_V$, οπότε $\lambda_1 = \lambda_2 = \cdots = \lambda_m = 0$. Άρα $\lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_m e_m = 0_F = \lambda_1 w_1 + \lambda_2 w_2 + \cdots + \lambda_m w_m$. Υποθέτουμε ότι κάποια από τα $h_1(x), h_2(x), \ldots, h_m(x)$ είναι μη σταθερά.

Έστω $h_j(x) = \sigma_j(x)x + \lambda_j$, όπου $\lambda_j = h_j(0) \in \mathbb{K}$, για κάθε $j = 1, 2, \ldots, m$, όπου κάποια από τα $\sigma_j(x) \in \mathbb{K}[x]$ δεν είναι μηδέν.

Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $\sigma_1(x) \neq 0$ και ότι το $\sigma_1(x)$ είναι μεγίστου βαθμού από όλα τα $\sigma_j(x) \neq 0$. Άρα και το $h_1(x)$ έχει τον μέγιστο δυνατό βαθμό μεταξύ των $h_j(x)$, όπου $h_j(x) \neq 0$.

Τότε $h_j(x)e_j = \sigma_j(x)xe_j + \lambda_j e_j = \sigma_j(x)\Big(xe_j - \sum_{i=1}^{m} \alpha_{ij}e_i \Big) + \sum_{i=1}^{m} \sigma_j(x)\alpha_{ij}e_i + \lambda_j e_j = \sigma_j(x)w_j +$
$+ \sum_{i=1}^{m} \sigma_j(x)\alpha_{ij}e_i + \lambda_j e_j$. Επομένως $\sum_{j=1}^{m} h_j(x)e_j = \sum_{j=1}^{m} \sigma_j(x)w_j + \sum_{j=1}^{m} \lambda_j e_j + \sum_{j=1}^{m}\sum_{i=1}^{m} \sigma_j(x)\alpha_{ij}e_i =$
$= \sum_{j=1}^{m} \sigma_j(x)w_j + \sum_{j=1}^{m} \lambda_j e_j + \sum_{i=1}^{m}\sum_{j=1}^{m} \sigma_j(x)\alpha_{ij}e_i$. Στο άθροισμα $\sum_{i=1}^{m}\sum_{j=1}^{m} \sigma_j(x)\alpha_{ij}e_i$ μπορούμε να εναλλάξουμε τους ρόλους των δεικτών i και j, χωρίς να μεταβληθεί το άθροισμα αυτό.

Καταλήγουμε δηλαδή στη σχέση $h_j(x)e_j = \sum_{j=1}^{m}\sigma_j(x)w_j + \sum_{j=1}^{m}\lambda_j e_j + \sum_{j=1}^{m}\left(\sum_{i=1}^{m}\sigma_i(x)\alpha_{ji}\right)e_j =$ $= \sum_{j=1}^{m}\sigma_j(x)w_j + \sum_{j=1}^{m}\left(\lambda_j + \sum_{i=1}^{m}\sigma_i(x)\alpha_{ji}\right)e_j = \sum_{j=1}^{m}\sigma_j(x)w_j + \sum_{j=1}^{m}\sigma'_j(x)e_j$, όπου $\sigma'_j(x) = \lambda_j + \sum_{i=1}^{m}\sigma_i(x)\alpha_{ji}$. Επειδή $\sum_{j=1}^{m}\sigma_j(x)w_j \in \mathrm{Ker}T$, έπεται ότι $\sum_{j=1}^{m}\sigma'_j(x)e_j \in \mathrm{Ker}T$. Τώρα κάθε πολυώνυμο $\sigma'_j(x) = \lambda_j + \sum_{i=1}^{m}\sigma_i(x)\alpha_{ji}$ είναι γραμμικός συνδυασμός των $\sigma_1(x), \sigma_2(x), \ldots, \sigma_m(x)$ συν μία σταθερά, όπου τα $\sigma_i(x)$ είναι είτε μηδέν είτε ο βαθμός τους είναι μικρότερος ή ίσος του $\deg\sigma_1(x) = \deg h_1(x) - 1 < \deg h_1(x)$. Επομένως είτε είναι όλα μηδέν είτε όσα έχουν απομείνει έχουν βαθμό μικρότερο του βαθμού του $h_1(x)$. Αν είναι όλα μηδέν ή σταθερά έχουμε τελειώσει. Αν όχι, τότε εφαρμόζουμε επαγωγή επί του μεγίστου βαθμού των πολυωνύμων-συντελεστών των $e_1, e_2, \ldots, e_m$, για να καταλήξουμε στο συμπέρασμα ότι $\sum_{j=1}^{m}\sigma'_j(x)e_j \in \mathbb{K}[x]w_1 + \mathbb{K}[x]w_2 + \cdots + \mathbb{K}[x]w_m$. ■

ΠΟΡΙΣΜΑ 5.11. Ο πίνακας της εμφύτευσης $i : \mathrm{Ker}T = \mathbb{K}[x]w_1 \oplus \mathbb{K}[x]w_2 \oplus \cdots \oplus \mathbb{K}[x]w_m \hookrightarrow F$ είναι ο

$$\begin{pmatrix} x-\alpha_{11} & -\alpha_{12} & -\alpha_{13} & \cdots & -\alpha_{1m} \\ -\alpha_{21} & x-\alpha_{22} & -\alpha_{23} & \cdots & -\alpha_{2m} \\ -\alpha_{31} & -\alpha_{32} & x-\alpha_{33} & \cdots & -\alpha_{3m} \\ \vdots & \vdots & \vdots & & \vdots \\ -\alpha_{m1} & -\alpha_{m2} & -\alpha_{m3} & \cdots & x-\alpha_{mm} \end{pmatrix} = xI_m - A,$$

όπου A ο πίνακας του ενδομορφισμού f ως προς τη βάση $(v_1, v_2, \ldots, v_m)$ του V. ■

ΠΟΡΙΣΜΑ 5.12. Ο διανυσματικός χώρος V ως $\mathbb{K}[x]$-πρότυπο είναι πρότυπο στρέψεως.
ΑΠΟΔΕΙΞΗ: Έστω $T : F \to V$ ο $\mathbb{K}[x]$-επιμορφισμός, όπως προηγουμένως. Αν το υποπρότυπο στρέψεως $T(V)$ δεν ήταν όλος ο V, τότε το $\mathbb{K}[x]$-πρότυπο $V\Big/_{T(V)}$ δεν θα ήταν μηδενικό, άρα ελεύθερο, εφόσον είναι πεπερασμένα παραγόμενο. Η απεικόνιση $p \circ T : F \to V\Big/_{T(V)}$, όπου $p : V \to V\Big/_{T(V)}$ η φυσική προβολή είναι $\mathbb{K}[x]$-επιμορφισμός. Με βάση την πρόταση 3.50, θα είχαμε $F = \mathrm{Ker}(p \circ T) \oplus F'$, όπου F' ελεύθερο και ισόμορφο με το $V\Big/_{T(V)}$, το οποίο δεν είναι μηδενικό. Άρα $\mathrm{rank}_{\mathbb{K}[x]}F' \geq 1$. Προφανώς $\mathrm{Ker}T \subseteq \mathrm{Ker}(p \circ T)$ και επομένως $m = \mathrm{rank}_{\mathbb{K}[x]}\mathrm{Ker}T \leq \mathrm{rank}_{\mathbb{K}[x]}\mathrm{Ker}(p \circ T)$.
Συνεπώς $m = \mathrm{rank}_{\mathbb{K}[x]}F = \mathrm{rank}_{\mathbb{K}[x]}\mathrm{Ker}(p \circ T) + \mathrm{rank}_{\mathbb{K}[x]}F' \geq \mathrm{rank}_{\mathbb{K}[x]}\mathrm{Ker}T + 1 = m + 1$, άτοπο. ■

ΠΑΡΑΤΗΡΗΣΕΙΣ : 1) Με βάση τη θεώρηση του διανυσματικού χώρου V ως πεπερασμένα παραγομένου $\mathbb{K}[x]$-προτύπου **οι κυκλικοί υπόχωροι Z_v του V ταυτίζονται με τα μη μηδενικά κυκλικά $\mathbb{K}[x]$-υποπρότυπα του V**.
2) Μπορούμε να εφαρμόσουμε τον αλγόριθμο Smith στον πίνακα $xI_m - A$ για να βρούμε τους αναλλοίωτους παράγοντες του V.
3) Οι αναλλοίωτοι παράγοντες είναι πολυώνυμα του x. Εφόσον στο $\mathbb{K}[x]$ κάθε μη μηδενικό

πολυώνυμο είναι συντροφικό με ένα μονικό πολυώνυμο, όλοι οι αναλλοίωτοι παράγοντες θα είναι μονικά πολυώνυμα. Σύμφωνα με το πόρισμα 5.12 **δεν υπάρχει μηδενικός αναλλοίωτος παράγων**.
4) Με βάση την παρατήρηση μετά την πρόταση 4.5 (σελίδα 66) **οι αντιστρέψιμοι αναλλοίωτοι παράγοντες του πίνακα $xI_m - A$ δεν θεωρούνται αναλλοίωτοι παράγοντες του V.**

ΠΡΟΤΑΣΗ 5.13. (i) Αν οι πίνακες $xI_m - A$ και $xI_m - B$ είναι ισοδύναμοι στο $\mathbb{K}[x]^{m\times m}$, τότε έχουν τους ίδιους αναλλοίωτους παράγοντες.
(ii) Αν οι πίνακες A και B είναι όμοιοι, τότε οι πίνακες $xI_m - A$ και $xI_m - B$ έχουν τους ίδιους αναλλοίωτους παράγοντες.
(iii) Οι αναλλοίωτοι παράγοντες του $\mathbb{K}[x]$-προτύπου V δεν εξαρτώνται από τη χρησιμοποιούμενη βάση $\hat{v} = (v_1, v_2, \ldots, v_n)$.
ΑΠΟΔΕΙΞΗ: (i) Έστω ότι οι πίνακες οι πίνακες $xI_m - A$ και $xI_m - B$ είναι ισοδύναμοι στο $\mathbb{K}[x]^{m\times m}$. Τότε υπάρχουν αντιστρέψιμοι πίνακες $X, Y \in \mathbb{K}[x]^{m\times m}$ τέτοιοι, ώστε $xI_m - B = X(xI_m - A)Y$. Κατά συνέπεια τα γινόμενα όλων των t πρώτων αναλλοιώτων παραγόντων (αντιστρεψίμων και μη αντιστρεψίμων) $\mathrm{J}_t(xI_m - B)$ και $\mathrm{J}_t(xI_m - B)$ των $xI_m - B$ και $xI_m - A$ ταυτίζονται, για κάθε $t = 1, 2, \ldots, m$, σύμφωνα με την απόδειξη της πρότασης 4.2. Επομένως οι πίνακες $xI_m - A$ και $xI_m - B$ έχουν τους ίδιους αναλλοίωτους παράγοντες, δηλαδή την ίδια κανονική μορφή Smith.
(ii) Προκύπτει από το (i), αφού αν $B = Q^{-1}AQ$, τότε οι $xI_m - B = xI_m - Q^{-1}AQ = Q^{-1}(xI_m - A)Q$ και οι πίνακες $xI_m - A$ και $xI_m - B$ είναι ισοδύναμοι.
(iii) Προκύπτει από το θεώρημα 4.16, αφού κάθε $\mathbb{K}[x]$-πρότυπο έχει την ίδια ακολουθία αναλλοιώτων παραγόντων. Εναλλακτικά, αν B είναι ο πίνακας της f ως προς κάποια άλλη βάση $\hat{v}' = (v_1', v_2', \ldots, v_m')$, τότε $B = Q^{-1}AQ$, όπου $Q = (\mathbf{1}_V \mid \hat{v}', \hat{v})$ ο πίνακας αλλαγής βάσης. Από το (ii) προκύπτει ότι οι πίνακες $xI_m - A$ και $xI_m - B$ έχουν τους ίδιους αναλλοίωτους παράγοντες. Διαγράφοντας τους μοναδιαίους αναλλοίωτους παράγοντες, παίρνουμε τους ίδιους μη αντιστρέψιμους αναλλοίωτους παράγοντες. ■

Ας δούμε τα επόμενα παραδείγματα:

ΠΑΡΑΔΕΙΓΜΑΤΑ 5.14. (i) Έστω V διανυσματικός χώρος επί του $\mathbb{R}$ με $\dim_{\mathbb{R}} V = 2$ και $\hat{v} = (v_1, v_2)$ μια βάση αυτού. Έστω $f : V \to V$ με $f(xv_1 + yv_2) = (8x - 9y)v_1 + (4x - 4y)v_2$, για κάθε $x, y \in \mathbb{R}$. Να βρεθούν οι f-αναλλοίωτοι παράγοντες του V.
ΛΥΣΗ: Ο πίνακας της f ως προς τη βάση $\hat{v}$ είναι ο $A = \begin{pmatrix} 8 & -9 \\ 4 & -4 \end{pmatrix}$. Επομένως $xI_2 - A =$
$= \begin{pmatrix} x-8 & 9 \\ -4 & x+4 \end{pmatrix} \overset{\Gamma_2\to\Gamma_2-\Gamma_1}{\longrightarrow} \begin{pmatrix} x-8 & 9 \\ -x+4 & x-5 \end{pmatrix} \overset{\Sigma_2\to\Sigma_2+\Sigma_1}{\longrightarrow} \begin{pmatrix} x-8 & x+1 \\ -x+4 & -1 \end{pmatrix} \overset{\Sigma_1\leftrightarrow\Sigma_2}{\longrightarrow}$
$\begin{pmatrix} x+1 & x-8 \\ -1 & -x+4 \end{pmatrix} \overset{\Gamma_1\leftrightarrow\Gamma_2}{\longrightarrow} \begin{pmatrix} -1 & -x+4 \\ x+1 & x-8 \end{pmatrix} \overset{\Gamma_1\to-\Gamma_1}{\longrightarrow} \begin{pmatrix} 1 & x-4 \\ x+1 & x-8 \end{pmatrix} \overset{\Sigma_2\to\Sigma_2-(x-4)\Sigma_1}{\longrightarrow}$
$\begin{pmatrix} 1 & 0 \\ x+1 & -x^2+4x-4 \end{pmatrix} \overset{\Gamma_2\to\Gamma_2-(x+1)\Gamma_1}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & -x^2+4x-4 \end{pmatrix} \overset{\Gamma_2\to-\Gamma_2}{\longrightarrow} \begin{pmatrix} 1 & 0 \\ 0 & x^2-4x+4 \end{pmatrix} =$
$= \begin{pmatrix} 1 & 0 \\ 0 & (x-2)^2 \end{pmatrix}$. Ο μοναδικός f-αναλλοίωτος παράγων του $\mathbb{R}^2$ είναι λοιπόν το $(x-2)^2$. ■
(ii) Έστω $f : \mathbb{R}^2 \to \mathbb{R}^2$, της οποίας ο πίνακας ως προς τη συνήθη βάση $(v_1 = (1, 0), v_2 = (0, 1))$ (χρησιμοποιούμε τα σύμβολα v_1, v_2 γιατί με τα e_i συμβολίζουμε τα στοιχεία της βάσης του ελεύθερου προτύπου F) είναι ο

$$A=\begin{pmatrix}-6 & 2\\ -20 & 7\end{pmatrix}$$

Να βρεθούν οι f-αναλλοίωτοι παράγοντες του $\mathbb{R}^2$.

ΛΥΣΗ: $xI_2-A=\begin{pmatrix}x+6 & -2\\ 20 & x-7\end{pmatrix}\overset{\Sigma_1\leftrightarrow\Sigma_2}{\longrightarrow}\begin{pmatrix}-2 & x+6\\ x-7 & 20\end{pmatrix}\overset{\Gamma_1\to-\frac{1}{2}\Gamma_1}{\longrightarrow}\begin{pmatrix}1 & -\frac{1}{2}x-3\\ x-7 & 20\end{pmatrix}\overset{\Gamma_2\to\Gamma_2-(x-7)\Gamma_1}{\longrightarrow}$
$\begin{pmatrix}1 & -\frac{1}{2}x-3\\ 0 & \frac{1}{2}x^2-\frac{1}{2}x-1\end{pmatrix}\overset{\Gamma_2\to2\Gamma_2}{\longrightarrow}\begin{pmatrix}1 & -\frac{1}{2}x-3\\ 0 & x^2-x-2\end{pmatrix}\overset{\Sigma_2\to\Sigma_2+(\frac{1}{2}x+3)\Sigma_1}{\longrightarrow}\begin{pmatrix}1 & 0\\ 0 & x^2-x-2\end{pmatrix}=$
$=\begin{pmatrix}1 & 0\\ 0 & (x+1)(x-2)\end{pmatrix}$. Ο μοναδικός f-αναλλοίωτος παράγων του $\mathbb{R}^2$ είναι λοιπόν το πολυώνυμο $(x+1)(x-2)$. ■

(iii) Έστω $f:\mathbb{R}^3\to\mathbb{R}^3$ με πίνακα ως προς τη συνηθισμένη βάση ($v_1=(1,0,0)$, $v_2=(0,1,0)$, $v_3=(0,0,1)$)

$$A=\begin{pmatrix}6 & 9 & -4\\ -2 & -2 & 1\\ 8 & 13 & -6\end{pmatrix}.$$

Να βρεθούν οι f-αναλλοίωτοι παράγοντες του $\mathbb{R}^3$.

ΛΥΣΗ: Έχουμε: $xI_3-A=\begin{pmatrix}x-6 & -9 & 4\\ 2 & x+2 & -1\\ -8 & -13 & x+6\end{pmatrix}\overset{\Sigma_1\leftrightarrow\Sigma_3}{\longrightarrow}\begin{pmatrix}4 & -9 & x-6\\ -1 & x+2 & 2\\ x+6 & -13 & -8\end{pmatrix}\overset{\Gamma_1\leftrightarrow\Gamma_2}{\longrightarrow}$
$\begin{pmatrix}-1 & x+2 & 2\\ 4 & -9 & x-6\\ x+6 & -13 & -8\end{pmatrix}\overset{\Gamma_1\to-\Gamma_1}{\longrightarrow}\begin{pmatrix}1 & -x-2 & -2\\ 4 & -9 & x-6\\ x+6 & -13 & -8\end{pmatrix}\overset{\Gamma_2\to\Gamma_2-4\Gamma_1}{\longrightarrow}\begin{pmatrix}1 & -x-2 & -2\\ 0 & 4x-1 & x+2\\ x+6 & -13 & -8\end{pmatrix}$
$\overset{\Gamma_3\to\Gamma_3-(x+6)\Gamma_1}{\longrightarrow}\begin{pmatrix}1 & -x-2 & -2\\ 0 & 4x-1 & x+2\\ 0 & x^2+8x-1 & 2x+4\end{pmatrix}\overset{\Sigma_2\to\Sigma_2+(x+2)\Sigma_1}{\longrightarrow}\begin{pmatrix}1 & 0 & -2\\ 0 & 4x-1 & x+2\\ 0 & x^2+8x-1 & 2x+4\end{pmatrix}\overset{\Sigma_3\to\Sigma_3+2\Sigma_1}{\longrightarrow}$
$\begin{pmatrix}1 & 0 & 0\\ 0 & 4x-1 & x+2\\ 0 & x^2+8x-1 & 2x+4\end{pmatrix}\overset{\Sigma_2\to\Sigma_2-4\Sigma_3}{\longrightarrow}\begin{pmatrix}1 & 0 & 0\\ 0 & -9 & x+2\\ 0 & x^2-17 & 2x+4\end{pmatrix}\overset{\Gamma_2\to-\frac{1}{9}\Gamma_2}{\longrightarrow}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & -\frac{x+2}{9}\\ 0 & x^2-17 & 2x+4\end{pmatrix}$
$\overset{\Sigma_3\to\Sigma_3+\frac{x+2}{9}\Sigma_2}{\longrightarrow}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & x^2-17 & \frac{x^3+2x^2+x+2}{9}\end{pmatrix}\overset{\Gamma_3\to\Gamma_3-(x^2-17)\Gamma_2}{\longrightarrow}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & \frac{x^3+2x^2+x+2}{9}\end{pmatrix}\overset{\Gamma_3\to9\Gamma_3}{\longrightarrow}$
$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & x^3+2x^2+x+2\end{pmatrix}=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & (x+2)(x^2+1)\end{pmatrix}$. Ο μοναδικός f-αναλλοίωτος παράγων του $\mathbb{R}^3$ είναι λοιπόν το πολυώνυμο $(x+2)(x^2+1)$. ■

(iv) Έστω V διανυσματικός χώρος με βάση $\hat{v}=(v_1,v_2,v_3)$. Θεωρούμε τη γραμμική απεικόνιση $f:V\to V$ με $f(v_1)=-11v_1-4v_2-12v_3$, $f(v_2)=130v_1+62v_2+195v_3$ και $f(v_3)=-38v_1-19v_2-60v_3$. Να βρεθούν οι f-αναλλοίωτοι παράγοντες του V.

ΛΥΣΗ: Ο πίνακας της f ως προς τη βάση $\hat{v}$ είναι ο

$$A=\begin{pmatrix}-11 & 130 & -38\\ -4 & 62 & -19\\ -12 & 195 & -60\end{pmatrix}$$

και $xI_3 - A = \begin{pmatrix} x+11 & -130 & 38 \\ 4 & x-62 & 19 \\ 12 & -195 & x+60 \end{pmatrix} \xrightarrow{\Sigma_3 \to \Sigma_3 - 5\Sigma_1} \begin{pmatrix} x+11 & -130 & -5x-17 \\ 4 & x-62 & -1 \\ 12 & -195 & x \end{pmatrix} \xrightarrow{\Sigma_1 \leftrightarrow \Sigma_3}$

$\begin{pmatrix} -5x-17 & -130 & x+11 \\ -1 & x-62 & 4 \\ x & -195 & 12 \end{pmatrix} \xrightarrow{\Gamma_1 \leftrightarrow \Gamma_2} \begin{pmatrix} -1 & x-62 & 4 \\ -5x-17 & -130 & x+11 \\ x & -195 & 12 \end{pmatrix} \xrightarrow{\Gamma_1 \to -\Gamma_1}$

$\begin{pmatrix} 1 & -x+62 & -4 \\ -5x-17 & -130 & x+11 \\ x & -195 & 12 \end{pmatrix} \xrightarrow{\Gamma_2 \to \Gamma_2 + (5x+17)\Gamma_1} \begin{pmatrix} 1 & -x+62 & -4 \\ 0 & -5x^2+293x+924 & -19x-57 \\ x & -195 & 12 \end{pmatrix} \xrightarrow{\Gamma_3 \to \Gamma_3 - x\Gamma_1}$

$\begin{pmatrix} 1 & -x+62 & -4 \\ 0 & -5x^2+293x+924 & -19x-57 \\ 0 & x^2-62x-195 & 4x+12 \end{pmatrix} \xrightarrow{\Sigma_2 \to \Sigma_2 + (x-62)\Sigma_1} \begin{pmatrix} 1 & 0 & -4 \\ 0 & -5x^2+293x+924 & -19x-57 \\ 0 & x^2-62x-195 & 4x+12 \end{pmatrix}$

$\xrightarrow{\Sigma_3 \to \Sigma_3 + 4\Sigma_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -5x^2+293x+924 & -19x-57 \\ 0 & x^2-62x-195 & 4x+12 \end{pmatrix} \xrightarrow{\Gamma_2 \to \Gamma_2 + 5\Gamma_3} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -17x-51 & x+3 \\ 0 & x^2-62x-195 & 4x+12 \end{pmatrix} \xrightarrow{\Sigma_2 \leftrightarrow \Sigma_3}$

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & x+3 & -17x-51 \\ 0 & 4x+12 & x^2-62x-195 \end{pmatrix} \xrightarrow{\Gamma_3 \to \Gamma_3 - 4\Gamma_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+3 & -17x-51 \\ 0 & 0 & x^2+6x+9 \end{pmatrix} \xrightarrow{\Sigma_3 \to \Sigma_3 + 17\Sigma_2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & x+3 & 0 \\ 0 & 0 & (x+3)^2 \end{pmatrix}$

Οι f-αναλλοίωτοι παράγοντες του V είναι λοιπόν οι $x+3$, $(x+3)^2$. ■

(v) Έστω V διανυσματικός χώρος επί του $\mathbb{R}$ διάστασης 4. Αν $\hat{v} = (v_1, v_2, v_3, v_4)$ είναι μια διατεταγμένη βάση του V και $f : V \to V$ με

$$A = (f \mid \hat{v}) = \begin{pmatrix} 18 & 5 & 5 & -1 \\ -92 & -26 & -26 & 5 \\ 39 & 11 & 11 & -2 \\ 59 & 15 & 16 & -3 \end{pmatrix}$$

να βρεθούν οι f-αναλλοίωτοι παράγοντες του V. Να απαντήσετε στο ίδιο ερώτημα αν ο V θεωρηθεί διανυσματικός χώρος επί του $\mathbb{C}$.

ΛΥΣΗ: $xI_4 - A = \begin{pmatrix} x-18 & -5 & -5 & 1 \\ 92 & x+26 & 26 & -5 \\ -39 & -11 & x-11 & 2 \\ -59 & -15 & -16 & x+3 \end{pmatrix} \xrightarrow{\Sigma_1 \leftrightarrow \Sigma_4} \begin{pmatrix} 1 & -5 & -5 & x-18 \\ -5 & x+26 & 26 & 92 \\ 2 & -11 & x-11 & -39 \\ x+3 & -15 & -16 & -59 \end{pmatrix}$

$\xrightarrow{\Sigma_2 \to \Sigma_2 + 5\Sigma_1} \begin{pmatrix} 1 & 0 & -5 & x-18 \\ -5 & x+1 & 26 & 92 \\ 2 & -1 & x-11 & -39 \\ x+3 & 5x & -16 & -59 \end{pmatrix} \xrightarrow{\Sigma_3 \to \Sigma_3 + 5\Sigma_1} \begin{pmatrix} 1 & 0 & 0 & x-18 \\ -5 & x+1 & 1 & 92 \\ 2 & -1 & x-1 & -39 \\ x+3 & 5x & 5x-1 & -59 \end{pmatrix} \xrightarrow{\Sigma_4 \to \Sigma_4 - (x-18)\Sigma_1}$

$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -5 & x+1 & 1 & 5x+2 \\ 2 & -1 & x-1 & -2x-3 \\ x+3 & 5x & 5x-1 & -x^2+15x-5 \end{pmatrix} \xrightarrow{\Gamma_2 \to \Gamma_2 + 5\Gamma_1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x+1 & 1 & 5x+2 \\ 2 & -1 & x-1 & -2x-3 \\ x+3 & 5x & 5x-1 & -x^2+15x-5 \end{pmatrix} \xrightarrow{\Gamma_3 \to \Gamma_3 - 2\Gamma_1}$

$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x+1 & 1 & 5x+2 \\ 0 & -1 & x-1 & -2x-3 \\ x+3 & 5x & 5x-1 & -x^2+15x-5 \end{pmatrix} \xrightarrow{\Gamma_4 \to \Gamma_4 - (x+3)\Gamma_1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & x+1 & 1 & 5x+2 \\ 0 & -1 & x-1 & -2x-3 \\ 0 & 5x & 5x-1 & -x^2+15x-5 \end{pmatrix} \xrightarrow{\Sigma_2 \leftrightarrow \Sigma_3}$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x+1 & 5x+2 \\ 0 & x-1 & -1 & -2x-3 \\ 0 & 5x-1 & 5x & -x^2+15x-5 \end{pmatrix} \xrightarrow{\Sigma_3 \to \Sigma_3-(x+1)\Sigma_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 5x+2 \\ 0 & x-1 & -x^2 & -2x-3 \\ 0 & 5x-1 & -5x^2+x+1 & -x^2+15x-5 \end{pmatrix}$$

$$\xrightarrow{\Sigma_4 \to \Sigma_4-(5x+2)\Sigma_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & x-1 & -x^2 & -5x^2+x-1 \\ 0 & 5x-1 & -5x^2+x+1 & -26x^2+10x-3 \end{pmatrix} \xrightarrow{\Gamma_3 \to \Gamma_3-(x-1)\Gamma_2}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -x^2 & -5x^2+x-1 \\ 0 & 5x-1 & -5x^2+x+1 & -26x^2+10x-3 \end{pmatrix} \xrightarrow{\Gamma_4 \to \Gamma_4-(5x-1)\Gamma_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -x^2 & -5x^2+x-1 \\ 0 & 0 & -5x^2+x+1 & -26x^2+10x-3 \end{pmatrix}$$

$$\xrightarrow{\Gamma_4 \to \Gamma_4-5\Gamma_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -x^2 & -5x^2+x-1 \\ 0 & 0 & x+1 & -x^2+5x+2 \end{pmatrix} \xrightarrow{\Sigma_4 \to \Sigma_4-5\Sigma_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -x^2 & x-1 \\ 0 & 0 & x+1 & -x^2-3 \end{pmatrix} \xrightarrow{\Gamma_4 \leftrightarrow \Gamma_3}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x+1 & -x^2-3 \\ 0 & 0 & -x^2 & x-1 \end{pmatrix} \xrightarrow{\Gamma_4 \to \Gamma_4+x\Gamma_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x+1 & -x^2-3 \\ 0 & 0 & x & -x^3-2x-1 \end{pmatrix} \xrightarrow{\Gamma_3 \to \Gamma_3-\Gamma_4}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & x^3-x^2+2x-2 \\ 0 & 0 & x & -x^3-2x-1 \end{pmatrix} \xrightarrow{\Gamma_4 \to \Gamma_4-x\Gamma_3} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & x^3-x^2+2x-2 \\ 0 & 0 & 0 & -x^4-2x^2-1 \end{pmatrix} \xrightarrow{\Sigma_4 \to \Sigma_4-(x^3-x^2+2x-2)\Sigma_3}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -x^4-2x^2-1 \end{pmatrix} \xrightarrow{\Gamma_4 \to -\Gamma_4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & x^4+2x^2+1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & (x^2+1)^2 \end{pmatrix}.$$

Ο μοναδικός αναλλοίωτος παράγων είναι το πολυώνυμο $(x^2+1)^2 = x^4+2x^2+1$.
Αν ο V θεωρηθεί μιγαδικός διανυσματικός χώρος, η απάντηση παραμένει η ίδια. Ο μοναδικός αναλλοίωτος παράγων είναι το πολυώνυμο $(x^2+1)^2$, μόνο που εδώ μπορεί να γραφεί ως $(x^2+1)^2 = (x-\mathbf{i})^2(x+\mathbf{i})^2$. ■

(vi) Έστω V διανυσματικός χώρος επί του $\mathbb{R}$ διάστασης 4. Αν $\hat{v} = (v_1, v_2, v_3, v_4)$ είναι μια διατεταγμένη βάση του V και $f : V \to V$ με

$$A = (f \mid \hat{v}) = \begin{pmatrix} -14 & 4 & 7 & -28 \\ 3 & 0 & 0 & 7 \\ -6 & 0 & 2 & -12 \\ 6 & -2 & -3 & 12 \end{pmatrix}$$

να βρεθούν οι f-αναλλοίωτοι παράγοντες του V. Να απαντήσετε στο ίδιο ερώτημα αν ο V θεωρηθεί διανυσματικός χώρος επί του $\mathbb{C}$.

ΛΥΣΗ: $xI_4 - A = \begin{pmatrix} x+14 & -4 & -7 & 28 \\ -3 & x & 0 & -7 \\ 6 & 0 & x-2 & 12 \\ -6 & 2 & 3 & x-12 \end{pmatrix} \xrightarrow{\Sigma_4 \to \Sigma_4-3\Sigma_1} \begin{pmatrix} x+14 & -4 & -7 & -2x \\ -3 & x & 0 & -1 \\ 6 & 0 & x-2 & 0 \\ -6 & 2 & 3 & x \end{pmatrix} \xrightarrow{\Sigma_1 \leftrightarrow \Sigma_4}$

$$\begin{pmatrix} -2x & -4 & -7 & x+14 \\ -1 & x & 0 & -3 \\ 0 & 0 & x-2 & 6 \\ x & 2 & 3 & -6 \end{pmatrix} \xrightarrow{\Gamma_1 \leftrightarrow \Gamma_2} \begin{pmatrix} -1 & x & 0 & -3 \\ -2x & -4 & -7 & x+14 \\ 0 & 0 & x-2 & 6 \\ x & 2 & 3 & -6 \end{pmatrix} \xrightarrow{\Gamma_1 \to -\Gamma_1}$$

$$\begin{pmatrix} 1 & -x & 0 & 3 \\ -2x & -4 & -7 & x+14 \\ 0 & 0 & x-2 & 6 \\ x & 2 & 3 & -6 \end{pmatrix} \xrightarrow{\Gamma_2 \to \Gamma_2 + 2x\Gamma_1} \begin{pmatrix} 1 & -x & 0 & 3 \\ 0 & -2x^2-4 & -7 & 7x+14 \\ 0 & 0 & x-2 & 6 \\ x & 2 & 3 & -6 \end{pmatrix} \xrightarrow{\Gamma_4 \to \Gamma_4 - x\Gamma_1}$$

$$\begin{pmatrix} 1 & -x & 0 & 3 \\ 0 & -2x^2-4 & -7 & 7x+14 \\ 0 & 0 & x-2 & 6 \\ 0 & x^2+2 & 3 & -3x-6 \end{pmatrix} \xrightarrow{\Sigma_2 \to \Sigma_2 + x\Sigma_1} \begin{pmatrix} 1 & 0 & 0 & 3 \\ 0 & -2x^2-4 & -7 & 7x+14 \\ 0 & 0 & x-2 & 6 \\ 0 & x^2+2 & 3 & -3x-6 \end{pmatrix} \xrightarrow{\Sigma_4 \to \Sigma_4 - 3\Sigma_1}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -2x^2-4 & -7 & 7x+14 \\ 0 & 0 & x-2 & 6 \\ 0 & x^2+2 & 3 & -3x-6 \end{pmatrix} \xrightarrow{\Gamma_2 \to \Gamma_2 + 2\Gamma_4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & x+2 \\ 0 & 0 & x-2 & 6 \\ 0 & x^2+2 & 3 & -3x-6 \end{pmatrix} \xrightarrow{\Sigma_2 \leftrightarrow \Sigma_3}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & x+2 \\ 0 & x-2 & 0 & 6 \\ 0 & 3 & x^2+2 & -3x-6 \end{pmatrix} \xrightarrow{\Gamma_2 \to -\Gamma_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -x-2 \\ 0 & x-2 & 0 & 6 \\ 0 & 3 & x^2+2 & -3x-6 \end{pmatrix} \xrightarrow{\Sigma_4 \to \Sigma_4 + (x+2)\Sigma_2}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & x-2 & 0 & x^2+2 \\ 0 & 3 & x^2+2 & 0 \end{pmatrix} \xrightarrow{\Gamma_3 \to \Gamma_3 - (x-2)\Gamma_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & x^2+2 \\ 0 & 3 & x^2+2 & 0 \end{pmatrix} \xrightarrow{\Gamma_4 \to \Gamma_4 - 3\Gamma_2}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & x^2+2 \\ 0 & 0 & x^2+2 & 0 \end{pmatrix} \xrightarrow{\Sigma_3 \leftrightarrow \Sigma_4} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x^2+2 & 0 \\ 0 & 0 & 0 & x^2+2 \end{pmatrix}$$

Οι f-αναλλοίωτοι παράγοντες είναι οι x^2+2, x^2+2.
Αν ο V θεωρηθεί μιγαδικός διανυσματικός χώρος, η απάντηση παραμένει η ίδια. Οι f-αναλλοίωτοι παράγοντες είναι οι x^2+2, x^2+2, οι οποίοι όμως γράφονται $(x+\mathrm{i}\sqrt{2})(x-\mathrm{i}\sqrt{2})$, $(x+\mathrm{i}\sqrt{2})(x-\mathrm{i}\sqrt{2})$. ■

5.5 Ρητή Κανονική Μορφή Πίνακα (Α΄ Μορφή)

ΘΕΩΡΗΜΑ 5.15. Έστω f ένας ενδομορφισμός του διανυσματικού χώρου V επί του σώματος $\mathbb{K}$. Έστω επίσης $\delta_1(x), \delta_2(x), \ldots, \delta_m(x)$ με $\delta_1(x) \mid \delta_2(x) \mid \cdots \mid \delta_m(x)$ οι αναλλοίωτοι μονικοί παράγοντες του ενδομορφισμού f. Τότε:
(i) Ο V ως διανυσματικός χώρος, γράφεται ως ευθύ άθροισμα κυκλικών διανυσματικών υποχώρων.

$$V = Z_{u_1} \oplus Z_{u_2} \oplus \ldots \oplus Z_{u_\nu} = (u_1) \oplus (u_2) \oplus \cdots \oplus (u_\nu) \qquad (\star)$$

με $Ann(Z_{u_i}) = (\delta_i(x))$, για κάθε $i = 1, 2, \ldots, \nu$. Κάθε διανυσματικός υπόχωρος Z_{u_i} συμπίπτει με το $\mathbb{K}[x]$-κυκλικό υποπρότυπο (u_i), το οποίο παράγεται από το διάνυσμα u_i, για κάθε $i = 1, 2, \ldots, \nu$. Το ν και τα $\delta_i(x)$ εξαρτώνται μόνον από τον διανυσματικό χώρο V και τον $\mathbb{K}$-ενδομορφισμό f.
(ii) Το χαρακτηριστικό και το ελάχιστο πολυώνυμο του περιορισμού $f|_{Z_{u_i}}$ της f στον Z_{u_i} συ-

μπίπτουν με το $\delta_i(x)$, για κάθε $i = 1, 2, \ldots, \nu$.
(iii) $\dim_{\mathbb{K}} Z_{u_i} = \deg \delta_i(x)$, για κάθε $i = 1, 2, \ldots, \nu$.
(iv) Το χαρακτηριστικό πολυώνυμο της f είναι το γινόμενο $\delta_1(x)\delta_2(x)\cdots\delta_\nu(x)$ και το ελάχιστο το $\delta_\nu(x)$. Επειδή δε $\delta_1(x) \mid \delta_2(x) \mid \cdots \mid \delta_\nu(x)$, το ελάχιστο και το χαρακτηριστικό πολυώνυμο της f έχουν τους ίδιους ανάγωγους παράγοντες. (Ήδη έχουμε δώσει μια στοιχειώδη απόδειξη αυτού-βλέπε πρόταση 5.4 και πόρισμα 5.5).
(v) Υπάρχει βάση $\hat{v} = (v_1, v_2, \ldots, v_m)$ του V επί του $\mathbb{K}$ $(m = \dim_{\mathbb{K}} V)$ ως προς την οποία ο πίνακας της f έχει τη μορφή

$$M = \begin{pmatrix} \Sigma(\delta_1(x)) & & & \\ & \Sigma(\delta_2(x)) & & \mathbf{O} \\ & & \ddots & \\ \mathbf{O} & & & \Sigma(\delta_\nu(x)) \end{pmatrix},$$

όπου $\Sigma(h(x))$ ο συνοδός πίνακας του πολυωνύμου $h(x)$. (Βλέπε ορισμό 5.8).
ΑΠΟΔΕΙΞΗ: (i) Το $\mathbb{K}[x]$-πρότυπο V αναλύεται σε ευθύ άθροισμα κυκλικών $\mathbb{K}[x]$-υποπροτύπων, σύμφωνα με το θεώρημα 4.16 $(u_1) \oplus (u_2) \oplus \cdots \oplus (u_\nu)$. Όμως κάθε κυκλικό υποπρότυπο (u_i) είναι εξ ορισμού ο κυκλικός υπόχωρος $Z_{u_i} = \{h(x)u_i = h(f)(u_i) \mid h(x) \in \mathbb{K}[x]\}$ που παράγεται από το διάνυσμα u_i. (Ορισμός 5.7). Το άθροισμα στη σχέση $(\star)$ είναι ευθύ είτε το θεωρήσουμε ως άθροισμα $\mathbb{K}[x]$-υποπροτύπων του V είτε ως άθροισμα $\mathbb{K}$-διανυσματικών υποχώρων του V.
(ii) Ο μηδενιστής του u_i, άρα και του Z_{u_i} είναι το ιδεώδες $(\delta_i(x))$. Συνεπώς το $\delta_i(x)$ είναι το μονικό πολυώνυμο ελαχίστου βαθμού που μηδενίζει τον Z_{u_i}, δηλαδή το ελάχιστο πολυώνυμο του περιορισμού $f|_{Z_{u_i}}$ στον Z_{u_i}. Αυτό, όπως ξέρουμε (πρόταση 5.9) συμπίπτει με το χαρακτηριστικό πολυώνυμο της $f|_{Z_{u_i}}$.
(iii) Εφόσον το χαρακτηριστικό πολυώνυμο της $f|_{Z_{u_i}}$ συμπίπτει με το $\delta_i(x)$, έπεται ότι $\deg \delta_i(x) = \dim_{\mathbb{K}} Z_{u_i}$.
(iv) Το χαρακτηριστικό πολυώνυμο της f ισούται με $\det(xI_m - A)$, όπου A ο πίνακας της f ως προς κάποια βάση του V. Γνωρίζουμε ότι η ορίζουσα $\det(xI_m - A)$ ισούται με το γινόμενο των αναλλοίωτων παραγόντων του πίνακα $xI_m - A$, αν αυτός θεωρηθεί στοιχείο του $\mathbb{K}[x]^{m\times m}$. (Βλέπε απόδειξη της πρότασης 4.2). Αν από τους αναλλοίωτους παράγοντες του πίνακα $xI_m - A$ παραλείψουμε τα αντιστρέψιμα πολυώνυμα, δηλαδή αυτά που είναι 1 (μπορούμε να αντικαταστήσουμε αναλλοίωτους παράγοντες με συντροφικά τους στοιχεία στο $\mathbb{K}[x]$), τότε το γινόμενο δεν αλλάζει και ισούται με το γινόμενο $\delta_1(x)\delta_2(x)\cdots\delta_\nu(x)$ των αναλλοίωτων παραγόντων της f. Τώρα, εφόσον $\delta_1(x) \mid \delta_2(x) \mid \cdots \mid \delta_\nu(x)$, το $\delta_\nu(x)$ μηδενίζει κάθε κυκλικό υπόχωρο Z_{u_i}, $i = 1, 2, \ldots, \nu$. Επομένως μηδενίζει όλον τον χώρο V, δηλαδή $\delta_\nu(x)V = \delta_\nu(f)(V) = \{0_V\}$. Αν υπήρχε μη μηδενικό πολυώνυμο $\sigma(x)$ με $\deg \sigma(x) < \deg \delta_\nu(x)$ τέτοιο, ώστε $\sigma(f)(V) = \{0_V\}$, τότε το $\sigma(x)$ θα μηδένιζε τον υπόχωρο Z_{u_ν} και άρα θα ήταν πολλαπλάσιο του ελαχίστου πολυωνύμου του περιορισμού $f|_{Z_{u_\nu}}$ της f στον Z_{u_ν}, το οποίο είναι το $\delta_\nu(x)$. Άτοπο γιατί $\deg \sigma(x) < \deg \delta_\nu(x)$.
(v) Για κάθε $i = 1, 2, \ldots, \nu$ υπάρχει διατεταγμένη βάση $\hat{g}_i$ του Z_{u_i}, ως προς την οποία ο πίνακας του περιορισμού της f στον Z_{u_i} να είναι ο $\Sigma(\delta_i(x))$. Αν θεωρήσουμε τη βάση $\hat{v}$, η οποία προκύπτει από την ένωση όλων αυτών των επιμέρους βάσεων, τότε είναι προφανές ότι ο πίνακας της f ως προς της $\hat{v}$ θα έχει τη ζητούμενη μορφή. ■

ΠΟΡΙΣΜΑ 5.16. (i) Δύο πίνακες $A, B \in \mathbb{K}^{m\times m}$ είναι όμοιοι αν και μόνον αν οι πίνακες $xI_m - A$ και $xI_m - B$ έχουν τους ίδιους αναλλοίωτους παράγοντες.
(ii) Κάθε τετραγωνικός πίνακας $A \in \mathbb{K}^{m\times m}$ είναι όμοιος με τον ανάστροφό του.
ΑΠΟΔΕΙΞΗ: (i) Αν οι πίνακες $xI_m - A$ και $xI_m - B$ έχουν τους ίδιους αναλλοίωτους παράγοντες, θα έχουν και τους ίδιους μη μοναδιαίους αναλλοίωτους παράγοντες

$$\delta_1(x) \mid \delta_2(x) \mid \cdots \mid \delta_\nu(x).$$

Αν ο A είναι ο πίνακας ενός $\mathbb{K}$-ενδομορφισμού $f : V \to V$ ως προς κάποια βάση $\hat{v} = (v_1, v_2, \ldots, v_m)$ του V, τότε υπάρχει βάση $\hat{v}' = (v'_1, v'_2, \ldots, v'_m)$ του V, ως προς την οποία ο πίνακας της f να έχει τη μορφή

$$M = \begin{pmatrix} \Sigma(\delta_1(x)) & & & \\ & \Sigma(\delta_2(x)) & & \mathbf{O} \\ & & \ddots & \\ \mathbf{O} & & & \Sigma(\delta_\nu(x)) \end{pmatrix},$$

όπου $\Sigma_i(\delta_i(x))$ ο συνοδός πίνακας του πολυωνύμου $\delta_i(x)$, για κάθε $i = 1, 2, \ldots, \nu$, σύμφωνα με το (v) του προηγούμενου θεωρήματος. Δηλαδή ο A είναι όμοιος με τον M. Ομοίως, αν ο B είναι ο πίνακας ενός $\mathbb{K}$-ενδομορφισμού $g : V \to V$ ως προς κάποια βάση $\hat{u} = (u_1, u_2, \ldots, u_m)$ του V, τότε υπάρχει βάση $\hat{u}' = (u'_1, u'_2, \ldots, u'_m)$ του V, ως προς την οποία ο πίνακας της g να έχει επίσης τη μορφή M. Επομένως και ο B είναι όμοιος προς τον M. Εφόσον οι A και B είναι όμοιοι προς τον M, τότε είναι και μεταξύ τους όμοιοι. Το αντίστροφο είναι το (ii) της πρότασης 5.13.

(ii) Παρατηρούμε ότι $xI_m - A^T = (xI_m - A)^T$. Σύμφωνα με την απόδειξη της πρότασης 4.2 έχουμε $\mathrm{J}_t(xI_m - A^T) = \mathrm{J}_t((xI_m - A)^T) = \mathrm{J}_t(xI_m - A)$, δηλαδή τα γινόμενα των t πρώτων αναλλοιώτων παραγόντων των $xI_m - A$ και $\mathrm{J}_t(xI_m - A^T)$ συμπίπτουν, για κάθε $t = 1, 2, \ldots, m$. Όπως στην απόδειξη της πρότασης 4.2, προκύπτει ότι οι πίνακες $xI_m - A$ και $xI_m - A^T$ έχουν τους ίδιους αναλλοίωτους παράγοντες. Το αποτέλεσμα προκύπτει από το (i). ■

ΣΧΟΛΙΟ : Το ότι ένας τετραγωνικός πίνακας με στοιχεία από ένα σώμα $\mathbb{K}$ είναι όμοιος με τον ανάστροφό του αποδεικνύεται στοιχειωδώς ως εξής:

Πρώτα αποδεικνύουμε ότι ο συνοδός πίνακας ενός πολυωνύμου $h(x) = x^m + \alpha_{m-1}x^{m-1} + \cdots + +\alpha_1 x + \alpha_0$ είναι όμοιος με τον ανάστροφό του. Έστω λοιπόν

$$\Sigma(h(x)) = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -\alpha_0 \\ 1 & 0 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & 0 & \cdots & 0 & -\alpha_2 \\ 0 & 0 & 1 & \cdots & 0 & -\alpha_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -\alpha_{m-1} \end{pmatrix}$$

ο συνοδός πίνακας του πολυωνύμου $h(x)$. Θεωρούμε τον πίνακα

$$Q = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{m-2} & \alpha_{m-1} & 1 \\ \alpha_2 & \alpha_3 & \alpha_4 & \cdots & \alpha_{m-1} & 1 & 0 \\ \alpha_3 & \alpha_4 & \alpha_5 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots \\ \alpha_{m-2} & \alpha_{m-1} & 1 & \cdots & 0 & 0 & 0 \\ \alpha_{m-1} & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}$$

Ο πίνακας Q είναι προφανώς αντιστρέψιμος. Με στοιχειώδεις πράξεις επαληθεύουμε ότι

$$Q\cdot\Sigma(h(x))^T=\Sigma(h(x))\cdot Q=\begin{pmatrix}-\alpha_0 & 0 & 0 & 0 & \cdots & 0 & 0\\ 0 & \alpha_2 & \alpha_3 & \alpha_4 & \cdots & \alpha_{m-1} & 1\\ 0 & \alpha_3 & \alpha_4 & \alpha_5 & \cdots & 1 & 0\\ \vdots & \vdots & \vdots & \vdots & \iddots & \vdots & \vdots\\ 0 & \alpha_{m-2} & \alpha_{m-1} & 1 & \cdots & 0 & 0\\ 0 & \alpha_{m-1} & 1 & 0 & \cdots & 0 & 0\\ 0 & 1 & 0 & 0 & \cdots & 0 & 0\end{pmatrix}$$

και κατά συνέπεια $\Sigma(h(x))^T=Q^{-1}\Sigma(h(x))Q$.
Γνωρίζουμε ότι αν A είναι ένας τετραγωνικός πίνακας με στοιχεία από το σώμα $\mathbb{K}$, τότε υπάρχει αντιστρέψιμος πίνακας $P\in\mathbb{K}^{m\times m}$ τέτοιος, ώστε

$$P^{-1}AP=\begin{pmatrix}\Sigma(\delta_1(x)) & & & \\ & \Sigma(\delta_2(x)) & & \mathbf{O}\\ & & \ddots & \\ \mathbf{O} & & & \Sigma(\delta_\nu(x))\end{pmatrix}=M,$$

όπου $\delta_1(x)\mid\delta_2(x)\mid\cdots\mid\delta_\nu(x)$ οι μη αντιστρέψιμοι αναλλοίωτοι παράγοντες του xI_m-A. Σύμφωνα με τα προηγούμενα, για κάθε $i=1,2,\ldots,\nu$ υπάρχει αντιστρέψιμος πίνακας $Q_i\in\mathbb{K}^{m_i\times m_i}$, όπου $m_i=\deg\delta_i(x)$ τέτοιος, ώστε $Q_i^{-1}\Sigma(\delta_i(x))Q=\Sigma(\delta_i(x))^T$. Αν Q είναι ο πίνακας

$$\begin{pmatrix}Q_1 & & & \\ & Q_2 & & \mathbf{O}\\ & & \ddots & \\ \mathbf{O} & & & Q_\nu\end{pmatrix},$$

τότε $Q^{-1}P^{-1}APQ=\begin{pmatrix}Q_1^{-1}\Sigma(\delta_1(x))Q_1 & & & \\ & Q_2^{-1}\Sigma(\delta_2(x))Q_2 & & \mathbf{O}\\ & & \ddots & \\ \mathbf{O} & & & Q_\nu^{-1}\Sigma(\delta_\nu(x))Q_\nu\end{pmatrix}=$

$=\begin{pmatrix}\Sigma(\delta_1(x))^T & & & \\ & \Sigma(\delta_2(x))^T & & \mathbf{O}\\ & & \ddots & \\ \mathbf{O} & & & \Sigma(\delta_\nu(x))^T\end{pmatrix}=M^T=(P^{-1}AP)^T=P^TA^T(P^T)^{-1}$. Επομένως $(P^T)^{-1}Q^{-1}P^{-1}APQP^T=A^T\Leftrightarrow(PQP^T)^{-1}A(PQP^T)=A^T$.

Τώρα επανερχόμαστε στο πρόβλημα καθορισμού βάσης του V ως προς την οποία ο πίνακας A του ενδομορφισμού $f:V\to V$ έχει την επιθυμητή μορφή M. Συγκεκριμένα, στα παραδείγματα 5.14 εφαρμόζουμε τη μέθοδο που εφαρμόσαμε και στα παραδείγματα 4.6 (i)-(iii).

Στο παράδειγμα 4.6.(i) πολλαπλασιάσαμε από δεξιά τον πίνακα xI_2-A με τον πίνακα $X=$ $=\begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}1&0\\-x-1&1\end{pmatrix}\begin{pmatrix}-1&0\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\-1&1\end{pmatrix}=\begin{pmatrix}1&-1\\x&-x-1\end{pmatrix}$. Ο πίνακας αυτός είναι ο πίνακας αλλαγής βάσης του $\mathbb{R}[x]$-προτύπου $F=\mathbb{R}e_1\oplus\mathbb{R}[x]e_2$ από τη βάση $\hat{e}$ στη νέα βάση $\hat{e}'$. Ο πίνακας που μας δίνει τη βάση $\hat{e}'$ ως προς τη βάση $\hat{e}$ είναι ο αντίστροφος $\begin{pmatrix}1&-1\\x&-x-1\end{pmatrix}^{-1}=\begin{pmatrix}x+1&-1\\x&-1\end{pmatrix}$. Παρατηρούμε ότι $e_2'=-e_1-e_2$. Η εικόνα του μέσω του T είναι η $T(e_2')=-v_1-v_2$. Από την κανονική μορφή Smith του πίνακα xI_2-A ο V ως $\mathbb{R}[x]$-πρότυπο είναι κυκλικό. Άρα παράγεται από το $-v_1-v_2$. Έστω $v_1'=-v_1-v_2$. Τότε

$v_2' = f(-v_1 - v_2) = = -8v_1 - 4v_2 + 9v_1 + 4v_2 = v_1$ και $f(v_2') = f(v_1) = 8v_1 + 4v_2 = -4(-v_1 - v_2) + 4v_1 = -4v_1' + 4v_2'$. Επομένως ο πίνακας της f ως προς τη βάση $\hat{v}' = (v_1', v_2')$ είναι ο $\begin{pmatrix} 0 & -4 \\ 1 & 4 \end{pmatrix}$, δηλαδή ο συνοδός πίνακας του πολυωνύμου $(x-2)^2 = x^2 - 4x + 4$, όπως αναμενόταν.

Θα μπορούσε βέβαια κάποιος να υπολογίσει εύκολα το χαρακτηριστικό πολυώνυμο του πίνακα $A = \begin{pmatrix} 8 & -9 \\ 4 & -4 \end{pmatrix}$, δηλαδή $ch_A(x) = \begin{vmatrix} x-8 & 9 \\ -4 & x+4 \end{vmatrix} = (x-8)(x+4) + 36 = x^2 - 4x - 32 + 36 = = x^2 - 4x + 4 = (x-2)^2$ και στη συνέχεια να βρει ένα διάνυσμα, το οποίο δεν είναι ιδιοδιάνυσμα της f. Επειδή $f(v_1) = 8v_1 + 4v_2 \neq 2v_1$, ένα τέτοιο είναι το v_1. Η νέα βάση του V είναι η $v_1' = v_1$ και $v_2' = f(v_1) = 8v_1 + 4v_2$. Ο πίνακας αλλαγής βάσης $(f \mid \hat{v}', \hat{v})$ είναι προφανώς ο $\begin{pmatrix} 1 & 8 \\ 0 & 4 \end{pmatrix}$ με αντίστροφο τον $\begin{pmatrix} 1 & 8 \\ 0 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1/4 \end{pmatrix}$. Προφανώς $\begin{pmatrix} 1 & -2 \\ 0 & 1/4 \end{pmatrix} \begin{pmatrix} 8 & -9 \\ 4 & -4 \end{pmatrix} \begin{pmatrix} 1 & 8 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & -4 \\ 1 & 4 \end{pmatrix}$, ο συνοδός πίνακας του πολυωνύμου $x^2 - 4x + 4 = (x-2)^2$.

Στο παράδειγμα 4.6.(ii) ο πίνακας $\begin{pmatrix} -6 & 2 \\ -20 & 7 \end{pmatrix}$ έχει χαρακτηριστικό πολυώνυμο $\begin{vmatrix} x+6 & -2 \\ 20 & x-7 \end{vmatrix} = = x^2 - x - 42 + 40 = x^2 - x - 2 = (x+1)(x-2)$. Αμέσως προκύπτει το συμπέρασμα ότι ο πίνακας αυτός διαγωνοποιείται. Για την ιδιοτιμή -1 παίρνουμε το αντίστοιχο ιδιοδιάνυσμα από τη λύση του «συστήματος» $\begin{cases} -6x + 2y = -x \\ -20x + 7y = -y \end{cases} \Leftrightarrow y = \frac{5}{2}x$. Ένα ιδιοδιάνυσμα είναι το $v_1' = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$. Για την ιδιοτιμή 2 έχουμε $\begin{cases} -6x + 2y = 2x \\ -20x + 7y = 2y \end{cases} \Leftrightarrow y = 4x$. Ένα ιδιοδιάνυσμα είναι το $v_2' = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$. Είναι σαφές ότι $\begin{pmatrix} 2 & 1 \\ 5 & 4 \end{pmatrix}^{-1} \begin{pmatrix} -6 & 2 \\ -20 & 7 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 5 & 4 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix}$, σαφώς καλύτερη μορφή απ' αυτήν του συνοδού πίνακα $\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}$ του πολυωνύμου $x^2 - x - 2 = (x+1)(x-2)$.

Στο παράδειγμα 4.6.(iii) ο ίδιος ο αλγόριθμος Smith αρχίζει να έχει πρόβλημα. (Πολλές πράξεις). Από δεξιά, αν δεν έχουμε κάνει λάθος (!) έχουμε πολλαπλασιάσει τον $xI_3 - A$ με τον πίνακα $X = \begin{pmatrix} 0 & -1 & 0 \\ -\frac{1}{9} & -\frac{4}{9} & 0 \\ x^2 - 17 & 4x^2 + 9x - 14 & 9 \end{pmatrix}$. Ο πίνακας $X^{-1} = \begin{pmatrix} 4 & -9 & 0 \\ -1 & 0 & 0 \\ x+6 & x^2 - 17 & \frac{1}{9} \end{pmatrix}$, αν φυσικά αντέχουμε να κάνουμε όλες τις επί μέρους πράξεις, μας παρέχει το διάνυσμα $T(\frac{1}{9}e_3) = \frac{1}{9}v_3$, ως τον γεννήτορα του κυκλικού $\mathbb{R}[x]$-προτύπου $\mathbb{R}^3$, όπου $\hat{e} = (e_1, e_2, e_3)$ η βάση του αντίστοιχου ελεύθερου $\mathbb{R}[x]$-προτύπου, βαθμού 3. Για ευκολία μπορούμε να πάρουμε ως γεννήτορα το $v_3 = (0, 0, 1)$. Έστω λοιπόν $u_1 = v_3 = (0, 0, 1)$. Τότε $u_2 = f(u_1) = (-4, 1, -6)$ και $u_3 = f(u_2)$, όπου $u_3^T = \begin{pmatrix} 6 & 9 & -4 \\ -2 & -2 & 1 \\ 8 & 13 & -6 \end{pmatrix} \begin{pmatrix} -4 \\ 1 \\ -6 \end{pmatrix} = \begin{pmatrix} 9 \\ 0 \\ 17 \end{pmatrix}$. Έστω $U = \begin{pmatrix} 0 & -4 & 9 \\ 0 & 1 & 0 \\ 1 & -6 & 17 \end{pmatrix}$ ο πίνακας που σχηματίζεται από τα u_1, u_2, u_3. Τότε $U^{-1} = \begin{pmatrix} -\frac{17}{9} & -\frac{14}{9} & 1 \\ 0 & 1 & 0 \\ \frac{1}{9} & \frac{4}{9} & 0 \end{pmatrix}$ και

$$U^{-1}AU = \begin{pmatrix} -\frac{17}{9} & -\frac{14}{9} & 1 \\ 0 & 1 & 0 \\ \frac{1}{9} & \frac{4}{9} & 0 \end{pmatrix} \begin{pmatrix} 6 & 9 & -4 \\ -2 & -2 & 1 \\ 8 & 13 & -6 \end{pmatrix} \begin{pmatrix} 0 & -4 & 9 \\ 0 & 1 & 0 \\ 1 & -6 & 17 \end{pmatrix} = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & -1 \\ 0 & 1 & -2 \end{pmatrix},$$

ο συνοδός πίνακας του πολυωνύμου $x^3+2x^2+x+2=(x+2)(x^2+1)$. Θα μπορούσαμε να κάνουμε κάτι άλλο; Ίσως ναι. Το χαρακτηριστικό πολυώνυμο $\begin{vmatrix} x-6 & -9 & 4 \\ 2 & x+2 & -1 \\ -8 & -13 & x+6 \end{vmatrix}$ του πίνακα A υπολογίζεται με σχετική προσοχή εύκολα. (Π.χ. με τον κανόνα του Sarrus). Έχουμε: $ch_A(x)=\begin{vmatrix} x-6 & -9 & 4 \\ 2 & x+2 & -1 \\ -8 & -13 & x+6 \end{vmatrix}=(x^2-36)(x+2)-72-104+32(x+2)+18(x+6)-13(x-6)=$ $=x^3+2x^2+x+2=(x+2)(x^2+1)$. Μπορούμε αρχικά να βρούμε ένα ιδιοδιάνυσμα που αντιστοιχεί στην ιδιοτιμή -2. Έχουμε:

$$\begin{pmatrix} 6 & 9 & -4 \\ -2 & -2 & 1 \\ 8 & 13 & -6 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix}=\begin{pmatrix} 6x+9y-4z \\ -2x-2y+z \\ 8x+13y-6z \end{pmatrix}=\begin{pmatrix} -2x \\ -2y \\ -2z \end{pmatrix}\Leftrightarrow\begin{cases} 8x+9y-4z=0 \\ -2x+z=0 \\ 8x+13y-4z=0 \end{cases}\Leftrightarrow$$

$\Leftrightarrow\begin{cases} y=0 \\ z=2x \end{cases}$ Ένα τέτοιο ιδιοδιάνυσμα είναι το $u_1=\begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$. Στη συνέχεια υπολογίζουμε τον πίνακα $A^2+I_3=\begin{pmatrix} 6 & 9 & -4 \\ -2 & -2 & 1 \\ 8 & 13 & -6 \end{pmatrix}^2+I_3=\begin{pmatrix} -13 & -16 & 9 \\ 0 & 0 & 0 \\ -26 & -32 & 18 \end{pmatrix}$, ο οποίος αντιστοιχεί στη γραμμική απεικόνιση $f^2+\mathbf{1}_{\mathbb{R}^3}$ με πυρήνα που ορίζεται από την εξίσωση $-13x-16y+9z=0\Leftrightarrow z=\frac{13}{9}x+\frac{16}{9}y$. Αν θέσουμε $x=-9$ και $y=9$, παίρνουμε $z=3$. Θεωρούμε τα διανύσματα $u_2=\begin{pmatrix} -9 \\ 9 \\ 3 \end{pmatrix}$ και $u_3=\begin{pmatrix} 6 & 9 & -4 \\ -2 & -2 & 1 \\ 8 & 13 & -6 \end{pmatrix}\begin{pmatrix} -9 \\ 9 \\ 3 \end{pmatrix}=\begin{pmatrix} 15 \\ 3 \\ 27 \end{pmatrix}$. Ο πίνακας $Q=\begin{pmatrix} 1 & -9 & 15 \\ 0 & 9 & 3 \\ 2 & 3 & 27 \end{pmatrix}$ που σχηματίζεται από τα διανύσματα u_1,u_2,u_3 έχει αντίστροφο $Q^{-1}=\begin{pmatrix} -13/5 & -16/5 & 9/5 \\ -1/15 & 1/30 & 1/30 \\ 1/5 & 7/30 & -1/10 \end{pmatrix}$.

Τότε έχουμε: $Q^{-1}AQ=\left(\begin{array}{c|cc} -2 & 0 & 0 \\ \hline 0 & 0 & -1 \\ 0 & 1 & 0 \end{array}\right)$, μια σαφώς καλύτερη μορφή απ' την $\begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & -1 \\ 0 & 1 & -2 \end{pmatrix}$, του συνοδού δηλαδή πίνακα του $(x+2)(x^2+1)$. Σε τέτοιου είδους μορφές θα αναφερθούμε στην επόμενη παράγραφο.

Στο παράδειγμα 4.6.(iv) ο αλγόριθμος Smith μας δίνει $X(xI_3-A)Y=\begin{pmatrix} 1 & 0 & 0 \\ 0 & x+3 & 0 \\ 0 & 0 & (x+3)^2 \end{pmatrix}$. Εξετάζοντας τις γραμμοπράξεις βρίσκουμε $X=\begin{pmatrix} 0 & -1 & 0 \\ 1 & -17 & 5 \\ -4 & x+68 & -19 \end{pmatrix}$ με αντίστροφο $X^{-1}=$ $=\begin{pmatrix} -5x-17 & -19 & -5 \\ -1 & 0 & 0 \\ x & 4 & 1 \end{pmatrix}$.

Έστω $u_1=\begin{pmatrix} -19 \\ 0 \\ 4 \end{pmatrix}$, $u_2=\begin{pmatrix} -5 \\ 0 \\ 1 \end{pmatrix}$ και $u_3=\begin{pmatrix} -11 & 130 & -38 \\ -4 & 62 & -19 \\ -12 & 195 & -60 \end{pmatrix}\begin{pmatrix} -5 \\ 0 \\ 1 \end{pmatrix}=\begin{pmatrix} 17 \\ 1 \\ 0 \end{pmatrix}$. Θεωρούμε

τον πίνακα $Q=\begin{pmatrix}-19 & -5 & 17\\ 0 & 0 & 1\\ 4 & 1 & 0\end{pmatrix}$ με αντίστροφο $Q^{-1}=\begin{pmatrix}1 & -17 & 5\\ -4 & 68 & -19\\ 0 & 1 & 0\end{pmatrix}$.

Τότε $Q^{-1}AQ=\left(\begin{array}{c|cc}-3 & 0 & 0\\ \hline 0 & 0 & -9\\ 0 & 1 & -6\end{array}\right)$.

Στο παράδειγμα 4.6.(v) ο αλγόριθμος Smith μας δίνει $X(xI_3-A)Y=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & (x^2+1)^2\end{pmatrix}$.

$$X=\begin{pmatrix}1 & 0 & 0 & 0\\ 5 & 1 & 0 & 0\\ x^2+17x-16 & 5x-5 & 5x-6 & 1-x\\ x^3+18x^2+2x-3 & 5x^2-1 & 5x^2-x-1 & -x^2\end{pmatrix}\text{ και}$$

$$X^{-1}=\begin{pmatrix}1 & 0 & 0 & 0\\ -5 & 1 & 0 & 0\\ 2 & x-1 & -x^2 & x-1\\ x+3 & 5x-1 & -5x^2+x+1 & 5x-6\end{pmatrix}$$

Επίσης, $A-I_4=\begin{pmatrix}17 & 5 & 5 & -1\\ -92 & -27 & -26 & 5\\ 39 & 11 & 10 & -2\\ 59 & 15 & 16 & -4\end{pmatrix}$ και $5A-6I_4=\begin{pmatrix}84 & 25 & 25 & -5\\ -460 & -136 & -130 & 25\\ 195 & 55 & 49 & -10\\ 295 & 75 & 80 & -21\end{pmatrix}$.

Επομένως $(A-I_4)\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=\begin{pmatrix}17 & 5 & 5 & -1\\ -92 & -27 & -26 & 5\\ 39 & 11 & 10 & -2\\ 59 & 15 & 16 & -4\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=\begin{pmatrix}5\\-26\\10\\16\end{pmatrix}$ και

$(5A-6I_4)\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}84 & 25 & 25 & -5\\ -460 & -136 & -130 & 25\\ 195 & 55 & 49 & -10\\ 295 & 75 & 80 & -21\end{pmatrix}\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}-5\\25\\-10\\-21\end{pmatrix}$.

Άρα $(A-I_4)\begin{pmatrix}0\\0\\1\\0\end{pmatrix}+(5A-6I_4)\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}5\\-26\\10\\16\end{pmatrix}+\begin{pmatrix}-5\\25\\-10\\-21\end{pmatrix}=\begin{pmatrix}0\\-1\\0\\-5\end{pmatrix}$.

Τώρα, $\begin{pmatrix}18 & 5 & 5 & -1\\ -92 & -26 & -26 & 5\\ 39 & 11 & 11 & -2\\ 59 & 15 & 16 & -3\end{pmatrix}\begin{pmatrix}0\\-1\\0\\-5\end{pmatrix}=\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$, $\begin{pmatrix}18 & 5 & 5 & -1\\ -92 & -26 & -26 & 5\\ 39 & 11 & 11 & -2\\ 59 & 15 & 16 & -3\end{pmatrix}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\-1\end{pmatrix}$

και $\begin{pmatrix}18 & 5 & 5 & -1\\ -92 & -26 & -26 & 5\\ 39 & 11 & 11 & -2\\ 59 & 15 & 16 & -3\end{pmatrix}\begin{pmatrix}0\\0\\0\\-1\end{pmatrix}=\begin{pmatrix}1\\-5\\2\\3\end{pmatrix}$. Ο πίνακας αλλαγής βάσης $(\mathbf{1}_V\mid \hat{v}',\hat{v})$ είναι λοιπόν ο $\begin{pmatrix}0 & 0 & 0 & 1\\ -1 & 1 & 0 & -5\\ 0 & -1 & 0 & 2\\ -5 & 0 & -1 & 3\end{pmatrix}$ με αντίστροφο τον $(\mathbf{1}_V\mid \hat{v},\hat{v}')=\begin{pmatrix}-3 & -1 & -1 & 0\\ 2 & 0 & -1 & 0\\ 18 & 5 & 5 & -1\\ 1 & 0 & 0 & 0\end{pmatrix}$. Πραγ-

ματικά,

$$\begin{pmatrix} -3 & -1 & -1 & 0 \\ 2 & 0 & -1 & 0 \\ 18 & 5 & 5 & -1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 18 & 5 & 5 & -1 \\ -92 & -26 & -26 & 5 \\ 39 & 11 & 11 & -2 \\ 59 & 15 & 16 & -3 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ -1 & 1 & 0 & -5 \\ 0 & -1 & 0 & 2 \\ -5 & 0 & -1 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

ο συνοδός πίνακας του πολυωνύμου $(x^2+1)^2 = x^4 + 2x^2 + 1$.

5.6 Ρητή Κανονική Μορφή Πίνακα (Β΄ Μορφή)-Στοιχειώδεις Διαιρέτες-Μορφή Jordan

Έστω $f \in \mathrm{End}_{\mathbb{K}} V$. Όπως στον ορισμό 4.24 θέτουμε

$$V_{p(x)} = \{v \in V \mid p(x)^\alpha \cdot v = p(f)^\alpha(v) = 0_V, \text{ για κάποιον θετικό ακέραιο } \alpha\},$$

για κάθε ανάγωγο (μονικό) πολυώνυμο $p(x) \in \mathbb{K}[x]$. Το $V_{p(x)}$ είναι ένα $\mathbb{K}[x]$-υποπρότυπο του V. Σύμφωνα με την πρόταση 4.25 και το (iv) του θεωρήματος 5.15, $V_{p(x)} \neq \{0_V\}$ αν και μόνον αν $p(x) \mid min_f(x) = \delta_\nu(x) \Leftrightarrow p(x) \mid ch_f(x)$. Τότε το $\mathbb{K}[x]$-υποπρότυπο $V_{p(x)}$ του V, το οποίο είναι και διανυσματικός υπόχωρος του V, λέγεται $p(x)$-πρωταρχική συνιστώσα.
Σύμφωνα και με την πρόταση 4.26 ο V γράφεται ως ευθύ άθροισμα υποχώρων (και $\mathbb{K}[x]$-υποπροτύπων ταυτόχρονα)

$$V = V_{p_1(x)} \oplus V_{p_2(x)} \oplus \cdots \oplus V_{p_t(x)},$$

όπου $ch_f(x) = p_1(x)^{\alpha_1} p_2(x)^{\alpha_2} \cdots p_t(x)^{\alpha_t}$ είναι η ανάλυση του χαρακτηριστικού πολυωνύμου της f σε γινόμενο αναγώγων (επί του $\mathbb{K}$) πολυωνύμων. Στην περίπτωσή μας το θεώρημα 4.27 διατυπώνεται ως εξής:

ΘΕΩΡΗΜΑ 5.17. Αν $f : V \to V$ είναι ένας $\mathbb{K}$-ενδομορφισμός του διανυσματικού χώρου V, τότε ο V αναλύεται μονοσήμαντα, σύμφωνα με τα προηγούμενα, σε ευθύ άθροισμα κυκλικών υποχώρων ως εξής:
$V = \left(Z_{u_{11}} \oplus Z_{u_{12}} \oplus \cdots \oplus Z_{u_{1,k_1}}\right) \oplus \left(Z_{u_{21}} \oplus Z_{u_{22}} \oplus \cdots \oplus Z_{u_{2,k_2}}\right) \oplus \cdots \oplus \left(Z_{u_{t1}} \oplus Z_{u_{t2}} \oplus \cdots \oplus Z_{u_{t,k_t}}\right)$,
όπου το χαρακτηριστικό και το ελάχιστο πολυώνυμο του περιορισμού $f|_{Z_{u_{ij}}}$ της f στον κυκλικό υπόχωρο $Z_{u_{ij}}$ ισούται με $p_i(x)^{\lambda_{ij}}$, για κάθε $j = 1, 2, \ldots, k_i$ και $i = 1, 2, \ldots, t$. Επίσης $\lambda_{ij} \leq \lambda_{i,j+1}$, για κάθε $j = 1, 2, \ldots, k_i - 1$ και $j = 1, 2, \ldots, t$. ■

ΟΡΙΣΜΟΣ 5.18. Τα στοιχεία $p_i(x)^{\lambda_{ij}}$ καθορίζουν προφανώς τη δομή του διανυσματικού χώρου V ως $\mathbb{K}[x]$-προτύπου και ονομάζονται **στοιχειώδεις διαιρέτες της f ή του αντίστοιχου πίνακά της A**.

Η επόμενη πρόταση μας δείχνει πώς ένας κυκλικός υπόχωρος διασπάται σε ευθύ άθροισμα πρωταρχικών κυκλικών υποχώρων και αποτελεί αναδιατύπωση στην περίπτωσή μας της πρότασης 4.29.

ΠΡΟΤΑΣΗ 5.19. Έστω Z_u ένας κυκλικός υπόχωρος του V που παράγεται από το διάνυσμα u. Αν το χαρακτηριστικό πολυώνυμο του περιορισμού $f|_{Z_u}$ ισούται με $h(x) = p_1(x)^{\alpha_1} p_2(x)^{\alpha_2} \cdots p_k(x)^{\alpha_k}$ με $p_1(x), p_2(x), \ldots, p_k(x)$ ανά δύο πρώτα ανάγωγα μονικά πολυώνυμα και $\alpha_1, \alpha_2, \ldots, \alpha_k$ θετικοί ακέραιοι. Θέτουμε

$$h_i(x) = \prod_{\substack{1\le j\le k\\ j\neq i}} p_j(x)^{\alpha_j},$$

για κάθε $i = 1, 2, \ldots, k$. Επίσης θέτουμε $u_i = h_i(x)\cdot u = h_i(f)(u)$, για κάθε $i = 1, 2, \ldots, k$. Τότε $Z_u = Z_{u_1} \oplus Z_{u_2} \oplus \cdots \oplus Z_{u_k}$, όπου το χαρακτηριστικό πολυώνυμο του $f|_{Z_{u_i}}$ είναι το $p_i(x)^{\alpha_i}$, για κάθε $i = 1, 2, \ldots, k$. ■

Με βάση τα παραπάνω και το γεγονός ότι $\dim Z_{u_{ij}} = \deg p_i(x)^{\lambda_{ij}} = \lambda_{ij}\cdot \deg p_i(x)$ παίρνουμε το ακόλουθο πόρισμα:

ΠΟΡΙΣΜΑ 5.20. Έστω $f : V \to V$ είναι ένας $\mathbb{K}$-ενδομορφισμός του διανυσματικού χώρου V και $p_1(x)^{\lambda_{11}} \mid p_1(x)^{\lambda_{12}} \mid \cdots \mid p_1(x)^{\lambda_{1,k_1}}, p_2(x)^{\lambda_{21}} \mid p_2(x)^{\lambda_{22}} \mid \cdots \mid p_2(x)^{\lambda_{2,k_2}}, \ldots, p_t(x)^{\lambda_{t1}} \mid p_t(x)^{\lambda_{t2}} \mid \cdots \mid p_t(x)^{\lambda_{t,k_t}}$ οι στοιχειώδεις διαιρέτες της f. (Δυνάμεις αναγώγων πολυωνύμων). Τότε

$$\dim V = \sum_{i=1}^{t}\sum_{j=1}^{k_i} \lambda_{ij}\deg p_i(x).$$ ■

ΠΑΡΑΔΕΙΓΜΑ 5.21. Στο παράδειγμα 5.14. (iv) ο πίνακας της f είναι ο

$$A = \begin{pmatrix} -11 & 130 & -38\\ -4 & 62 & -19\\ -12 & 195 & -60\end{pmatrix}$$

με χαρακτηριστικό πολυώνυμο $ch_f(x) = \begin{vmatrix} x+11 & -130 & 38\\ 4 & x-62 & 19\\ 12 & -195 & x+60\end{vmatrix} = x^3+9x^2+27x+27 =$
$= x^3+27+9x(x+3) = (x+3)(x^2-3x+9)+9x(x+3) = (x+3)(x^2+6x+9) = (x+3)^3$.
Ποιοι είναι οι στοιχειώδεις διαιρέτες; Υπολογίζουμε ιδιοδιανύσματα με ιδιοτιμή το -3:

$$\begin{pmatrix} -11 & 130 & -38\\ -4 & 62 & -19\\ -12 & 195 & -60\end{pmatrix}\begin{pmatrix} x\\ y\\ z\end{pmatrix} = \begin{pmatrix} -3x\\ -3y\\ -3z\end{pmatrix} \Leftrightarrow \begin{cases} -8x+130y-38z=0\\ -4x+65y-19z=0\\ -12x+195y-57z=0\end{cases} \Leftrightarrow \begin{cases} -4x+65y-19z=0\\ -12x+195y-57z=0\end{cases}$$

$\Leftrightarrow \begin{cases} -4x+65y-19z=0\\ -12x+195y-57z=0\end{cases} \Leftrightarrow -4x+65y-19z = 0 \Leftrightarrow x = \frac{65}{4}y - \frac{19}{4}z$. Επομένως $\begin{pmatrix} x\\ y\\ z\end{pmatrix} = \begin{pmatrix} (65/4)y-(19/4)z\\ y\\ z\end{pmatrix} = y\begin{pmatrix} \frac{65}{4}\\ 1\\ 0\end{pmatrix} + z\begin{pmatrix} -\frac{19}{4}\\ 0\\ 1\end{pmatrix}$. Τα ιδιοδιανύσματα $\begin{pmatrix} \frac{65}{4}\\ 1\\ 0\end{pmatrix}$ και $\begin{pmatrix} -\frac{19}{4}\\ 0\\ 1\end{pmatrix}$ ή καλύτερα τα ιδιοδιανύσματα $\begin{pmatrix} 65\\ 4\\ 0\end{pmatrix}$ και $\begin{pmatrix} -19\\ 0\\ 4\end{pmatrix}$ αποτελούν βάση του ιδιόχωρου $V(-3)$. Εφόσον $\dim V(-3) = 2 < 3 = \dim V$, οι στοιχειώδεις διαιρέτες θα είναι οι $x+3$ και $(x+3)^2$.
Για να βρούμε τον κυκλικό υπόχωρο που αντιστοιχεί στον $(x+3)^2$ παίρνουμε ένα διάνυσμα που δεν ανήκει στον $V(-3)$. Για παράδειγμα, το $\begin{pmatrix} 1\\ 0\\ 0\end{pmatrix}$. Πολλαπλασιάζουμε με τον πίνακα

$A+3I_3 = \begin{pmatrix} -8 & 130 & -38\\ -4 & 65 & -19\\ -12 & 195 & -57\end{pmatrix}$ και παίρνουμε το διάνυσμα $\begin{pmatrix} -8\\ -4\\ -12\end{pmatrix} = -3\cdot\begin{pmatrix} -19\\ 0\\ 4\end{pmatrix} - \begin{pmatrix} 65\\ 4\\ 0\end{pmatrix}$.

Επομένως $(A+3I_3)^2\begin{pmatrix}1\\0\\0\end{pmatrix}=\mathrm{O}_{3\times 1}$, γιατί τα $\begin{pmatrix}65\\4\\0\end{pmatrix}$ και $\begin{pmatrix}-19\\0\\4\end{pmatrix}$ είναι ιδιοδιανύσματα ως προς την ιδιοτιμή -3. Άρα ο περιορισμός της f στον υπόχωρο που παράγεται από τα διανύσματα $\begin{pmatrix}1\\0\\0\end{pmatrix}$ και $\begin{pmatrix}-8\\-4\\-12\end{pmatrix}$ έχει χαρακτηριστικό πολυώνυμο $(x+3)^2$. Συμπληρώνουμε με ένα από τα διανύσματα $\begin{pmatrix}65\\4\\0\end{pmatrix}$ ή $\begin{pmatrix}-19\\0\\4\end{pmatrix}$, έστω το $\begin{pmatrix}-19\\0\\4\end{pmatrix}$. Θέτουμε $u_1=\begin{pmatrix}1\\0\\0\end{pmatrix}$, $u_2=\begin{pmatrix}-8\\-4\\-12\end{pmatrix}$ και $u_3=\begin{pmatrix}-19\\0\\4\end{pmatrix}$. Έστω $U=\begin{pmatrix}1&-8&-19\\0&-4&0\\0&-12&4\end{pmatrix}$. Τότε $U^{-1}=\begin{pmatrix}1&-\frac{65}{4}&\frac{19}{4}\\0&-\frac{1}{4}&0\\0&-\frac{3}{4}&\frac{1}{4}\end{pmatrix}$.

Ακόμη, $U^{-1}AU=\begin{pmatrix}1&-\frac{65}{4}&\frac{19}{4}\\0&-\frac{1}{4}&0\\0&-\frac{3}{4}&\frac{1}{4}\end{pmatrix}\begin{pmatrix}-11&130&-38\\-4&62&-19\\-12&195&-60\end{pmatrix}\begin{pmatrix}1&-8&-19\\0&-4&0\\0&-12&4\end{pmatrix}=\left(\begin{array}{cc|c}-3&0&0\\1&-3&0\\\hline 0&0&-3\end{array}\right)$.

Αν αντί του $u_2=\begin{pmatrix}-8\\-4\\-12\end{pmatrix}$ παίρναμε το $u_2'=Au_1=\begin{pmatrix}-11\\-4\\-12\end{pmatrix}$, τότε επειδή $(A+3I_3)^2=\mathrm{O}_{3\times 1}\Leftrightarrow$ $\Leftrightarrow A^2+6A+9I_3=\mathrm{O}_{3\times 1}\Leftrightarrow A^2=-9I_3-6A$, θα είχαμε $A^2u_1=-9u_1-6Au_1=-9u_1-6u_2'$. Αν θέσουμε λοιπόν $u_1'=u_1=\begin{pmatrix}1\\0\\0\end{pmatrix}$, $u_2'=Au_1=\begin{pmatrix}-11\\-4\\-12\end{pmatrix}$ και $u_3'=u_3=\begin{pmatrix}-19\\0\\4\end{pmatrix}$ και σχηματίσουμε τον πίνακα $W=\begin{pmatrix}1&-11&-19\\0&-4&0\\0&-12&4\end{pmatrix}$, θα έχουμε $W^{-1}=\begin{pmatrix}1&-17&\frac{19}{4}\\0&-\frac{1}{4}&0\\0&-\frac{3}{4}&\frac{1}{4}\end{pmatrix}$ και κατά συνέπεια $W^{-1}AW=\begin{pmatrix}1&-17&\frac{19}{4}\\0&-\frac{1}{4}&0\\0&-\frac{3}{4}&\frac{1}{4}\end{pmatrix}\begin{pmatrix}-11&130&-38\\-4&62&-19\\-12&195&-60\end{pmatrix}\begin{pmatrix}1&-11&-19\\0&-4&0\\0&-12&4\end{pmatrix}=\left(\begin{array}{cc|c}0&-9&0\\1&-6&0\\\hline 0&0&-3\end{array}\right)$. Παρατηρούμε ότι τόσο ο πίνακας $\begin{pmatrix}-3&0\\1&-3\end{pmatrix}$ όσο και ο $\begin{pmatrix}0&-9\\1&-6\end{pmatrix}$, με τον τελευταίο να είναι ο συνοδός πίνακας του πολυωνύμου $(x+3)^2$, εκφράζουν την f όταν αυτή δρα στον κυκλικό υπόχωρο Z_{u_1}, αλλά ως προς διαφορετικές βάσεις. Λέμε ότι ο πίνακας $\begin{pmatrix}-3&0\\1&-3\end{pmatrix}$ είναι ένα **block του Jordan**.

ΠΡΟΤΑΣΗ 5.22. Έστω $f\in\mathrm{End}_K V$, όπου V ένας f-κυκλικός χώρος που παράγεται από το διάνυσμα $u=u_1$. Υποθέτουμε ότι το χαρακτηριστικό πολυώνυμο της f είναι της μορφής $(x-\lambda)^n$, όπου $n=\dim V$. Τότε υπάρχει βάση $\hat{w}=(w_1,w_2,\ldots,w_n)$ του V ως προς την οποία ο πίνακας της f έχει τη μορφή

$$\mathrm{J}(\lambda,n)=\begin{pmatrix}\boldsymbol{\lambda}&0&0&0&\cdots&0&0\\\mathbf{1}&\boldsymbol{\lambda}&0&0&\cdots&0&0\\0&\mathbf{1}&\boldsymbol{\lambda}&0&\cdots&0&0\\0&0&\mathbf{1}&\boldsymbol{\lambda}&\cdots&0&0\\\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&0&0&\cdots&\boldsymbol{\lambda}&0\\0&0&0&0&\cdots&\mathbf{1}&\boldsymbol{\lambda}\end{pmatrix}$$

Η παραπάνω μορφή λέγεται **μορφή Jordan**.

ΑΠΟΔΕΙΞΗ: Έστω $u_2 = f(u_1) = f(u)$, $u_3 = f(u_2) = f^2(u), \dots, u_n = f^{n-1}(u)$ η συνήθης βάση του κυκλικού χώρου V. Αντ' αυτής θεωρούμε τη βάση $w_1 = u_1 = u$, $w_2 = (f - \lambda\mathbf{1}_V)(u_1), w_3 = = (f - \lambda\mathbf{1}_V)^2(u), \dots, w_n = (f - \lambda\mathbf{1}_V)^{n-1}(u)$. Προφανώς έχουμε $(f - \lambda\mathbf{1}_V)(w_i) = w_{i+1}$, για κάθε $i = 1, 2, \dots, n-1$ και $(f - \lambda\mathbf{1}_V)(w_n) = (f - \lambda\mathbf{1}_v)^n(u) = 0_V$. Επομένως $f(w_i) - \lambda w_i = w_{i+1} \Leftrightarrow$ $\Leftrightarrow f(w_i) = \lambda w_i + w_{i+1}$, για κάθε $i = 1, 2, \dots, n-1$ και $f(w_n) = \lambda w_n$. Το μόνο που μένει είναι να αποδείξουμε ότι τα στοιχεία αυτά αποτελούν βάση του V. Επειδή είναι $n = \dim V$ το πλήθος, αρκεί να δείξουμε ότι είναι γραμμικά ανεξάρτητα.

Έστω $\sum_{i=1}^{n} s_i w_i = 0_V$, για κάποια $s_1, s_2, \dots, s_n \in \mathbb{K}$. Επομένως $\sum_{i=1}^{n} s_i (f - \lambda\mathbf{1}_V)^{i-1}(u) = 0_V$, δηλαδή η $\sum_{i=1}^{n} s_i (f - \lambda\mathbf{1}_V)^{i-1}$ μηδενίζει τον f-γεννήτορα u και επομένως μηδενίζει όλον τον V.

Άρα η f μηδενίζει το πολυώνυμο $h(x) = \sum_{i=1}^{n} s_i (x - \lambda)^{i-1}$. Υποθέτουμε ότι κάποια s_i δεν είναι μηδέν και έστω $k \leq n$ ο μεγαλύτερος δείκτης, για τον οποίο $s_k \neq 0$. Τότε το $h(x)$ είναι βαθμού $k - 1 \leq n - 1 < n$, πράγμα αδύνατον, γιατί το ελάχιστο πολυώνυμο της f συμπίπτει με το χαρακτηριστικό και είναι ακριβώς n βαθμού. ■

ΠΟΡΙΣΜΑ 5.23. Αν $f : V \to V$ είναι ένας $\mathbb{K}$-ενδομορφισμός του διανυσματικού χώρου V, και $V = \big(Z_{u_{11}} \oplus Z_{u_{12}} \oplus \cdots \oplus Z_{u_{1,k_1}}\big) \oplus \big(Z_{u_{21}} \oplus Z_{u_{22}} \oplus \cdots \oplus Z_{u_{2,k_2}}\big) \oplus \cdots \oplus \big(Z_{u_{t1}} \oplus Z_{u_{t2}} \oplus \cdots \oplus Z_{u_{t,k_t}}\big)$, είναι η πρωταρχική ανάλυση του V σε ευθύ άθροισμα κυκλικών υποχώρων με αντίστοιχους στοιχειώδεις διαιρέτες
$(x-\lambda_1)^{n_{11}}, (x-\lambda)^{n_{12}}, \dots, (x-\lambda_1)^{n_{1,k_1}}, (x-\lambda_2)^{n_{21}}, \dots, (x-\lambda_2)^{n_{22}}, \dots, (x-\lambda_2)^{n_{2,k_2}}, \dots, (x-\lambda_t)^{n_{t1}}$, $(x-\lambda_t)^{n_{t2}}, \dots, (x-\lambda_t)^{n_{t,k_t}}$, όπου $\lambda_i \neq \lambda_j$, για $i \neq j$ και $n_{ij} \leq n_{i,j+1}$, για κάθε $j = 1, 2, \dots, k_i - 1$ και $i = 1, 2, \dots, t$, τότε υπάρχει βάση του V ως προς την οποία η f έχει πίνακα της μορφής

$$\begin{pmatrix} \mathrm{J}(\lambda_1, n_{11}) & & & & & & \\ & \mathrm{J}(\lambda_1, n_{12}) & & & & \mathbf{O} & \\ & & \ddots & & & & \\ & & & \mathrm{J}(\lambda_1, n_{1,k_1}) & & & \\ & & & & \ddots & & \\ & & & & & \mathrm{J}(\lambda_t, n_{t1}) & \\ & & & & & & \mathrm{J}(\lambda_t, n_{t2}) \\ & & & & & & & \ddots \\ \mathbf{O} & & & & & & & & \mathrm{J}(\lambda_t, n_{t,k_t}) \end{pmatrix}$$

Η μορφή αυτή λέγεται μορφή Jordan του πίνακα. ■

ΠΟΡΙΣΜΑ 5.24. Έστω Z_u ένας f-κυκλικός υπόχωρος με χαρακτηριστικό (και ελάχιστο) πολυώνυμο $(x-\lambda)^k$, όπου $\lambda \in \mathbb{K}$ και k θετικός ακέραιος. Τότε η διάσταση του ιδιόχωρου $V(\lambda) \cap Z_u$, δηλαδή του ιδιόχωρου του περιορισμού $f|_{Z_u}$ της f στον Z_u είναι 1.

ΑΠΟΔΕΙΞΗ: Υπενθυμίζουμε ότι ένας κυκλικός υπόχωρος είναι ένα $\mathbb{K}[x]$-υποπρότυπο του V, το οποίο παράγεται από το u. Επίσης, αν $v \neq 0_V$ είναι ένα ιδιοδιάνυσμα της f που αντιστοιχεί στην ιδιοτιμή λ, τότε και ο μονοδιάστατος υπόχωρος $\mathbb{K}v = \{sv \mid s \in \mathbb{K}\}$ είναι επίσης ένα $\mathbb{K}[x]$-υποπρότυπο, αφού είναι f-αναλλοίωτος. (Βλέπε παρατήρηση μετά τον ορισμό 5.6).

Θέτουμε $g = f|_{Z_u}$. Σύμφωνα με την πρόταση 5.22 ο κυκλικός υπόχωρος Z_u έχει μια βάση $\hat{w} = (w_1, w_2, \dots, w_k)$, όπου $w_1 = u$ και $w_i = (f - \lambda\mathbf{1}_V)^{i-1}(u)$, για κάθε $i = 2, 3, \dots, k$, ως προς

την οποία ο πίνακας της g έχει τη μορφή

$$\mathrm{J}(\lambda,k)=\begin{pmatrix}\lambda&0&0&0&\cdots&0&0\\1&\lambda&0&0&\cdots&0&0\\0&1&\lambda&0&\cdots&0&0\\0&0&1&\lambda&\cdots&0&0\\\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&0&0&\cdots&\lambda&0\\0&0&0&0&\cdots&1&\lambda\end{pmatrix}$$

και άρα ο πίνακας της $g=f|_{Z_u}-\lambda\mathbf{1}_{Z_u}$ είναι ο

$$\mathrm{J}(\lambda,k)-\lambda I_k=\begin{pmatrix}0&0&0&0&\cdots&0&0\\1&0&0&0&\cdots&0&0\\0&1&0&0&\cdots&0&0\\0&0&1&0&\cdots&0&0\\\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&0&0&\cdots&0&0\\0&0&0&0&\cdots&1&0\end{pmatrix}$$

Ο πίνακας αυτός έχει $k-1$ γραμμικά ανεξάρτητες γραμμές (ή στήλες). Άρα $\dim_{\mathbb{K}}\mathrm{Im}g=k-1=\dim_{\mathbb{K}}Z_u-1$, αλλά από τη Γραμμική Άλγεβρα ξέρουμε ότι $\dim_{\mathbb{K}}\mathrm{Im}g=\dim_{\mathbb{K}}Z_u-\dim_{\mathbb{K}}\mathrm{Ker}g$. Επομένως $\dim_{\mathbb{K}}\mathrm{Ker}g=1$ και ο $\mathrm{Ker}g$ ισούται προφανώς με τον $V(\lambda)\cap Z_u$.
Εναλλακτικά, θα μπορούσε να παρατηρήσει κανείς από τον πίνακα $\mathrm{J}(\lambda,k)$ ότι $f(w_1)=\lambda w_1+w_2$, $f(w_2)=\lambda w_2+w_3,\ldots,f(w_{k-1})=\lambda w_{k-1}+w_k$ και $f(w_k)=\lambda w_k$. Έστω $f\big(\sum_{i=1}^k s_iw_i\big)=$ $=\sum_{i=1}^k\lambda s_iw_i\Leftrightarrow\sum_{i=1}^{k-1}s_i(\lambda w_i+w_{i+1})+\lambda s_kw_k=\sum_{i=1}^{k-1}\lambda s_iw_i+\lambda s_kw_k\Leftrightarrow\sum_{i=1}^{k-1}s_iw_{i+1}=0_{Z_u}\Leftrightarrow$ $\Leftrightarrow\sum_{i=2}^k s_{i-1}w_i=0_{Z_u}$, και επειδή τα $w_2,\ldots,w_k$ είναι γραμμικά ανεξάρτητα, έπεται ότι $s_1=$ $=s_2=\cdots=s_{k-1}=0$. Επομένως $\sum_{i=1}^k s_iw_i=s_kw_k\in\mathbb{K}w_k$. ■

ΣΥΜΠΕΡΑΣΜΑΤΑ 1ο: Αν οι στοιχειώδεις διαιρέτες του πίνακα A της μορφής $(x-\lambda)^\rho$ είναι οι $(x-\lambda)^{k_1}\mid(x-\lambda)^{k_2}\mid\cdots\mid(x-\lambda)^{k_t}$, τότε ο ιδιόχωρος $V(\lambda)$ έχει διάσταση t.
2ο: Αν οι δυνάμεις του $x-\lambda$ εμφανίζονται στους τελευταίους t αναλλοίωτους παράγοντες του A, ισοδύναμα στους τελευταίους t μη μοναδιαίους αναλλοίωτους παράγοντες του xI_m-A, τότε η διάσταση του ιδιόχωρου $V(\lambda)$ είναι t.

Έτσι, στο παράδειγμα 5.21 (βλέπε επίσης παράδειγμα 5.14.(iv)) ο πίνακας

$$A=\begin{pmatrix}-11&130&-38\\-4&62&-19\\-12&195&-60\end{pmatrix}$$

έχει χαρακτηριστικό πολυώνυμο $(x+3)^3$. Οι αναλλοίωτοι παράγοντες θα μπορούσαν να είναι $x+3,x+3,x+3$ ή $x+3,(x+3)^2$ ή $(x+3)^3$. Στην πρώτη περίπτωση ο ιδιόχωρος $V(-3)$ θα είχε διάσταση $3=\dim_{\mathbb{R}}V$ και άρα ο A θα ήταν διαγωνίσιμος με μοναδική ιδιοτιμή το -3, δηλαδή $A=-3I_3$, πράγμα που δεν συμβαίνει. Στην τελευταία θα είχαμε $\dim_{\mathbb{R}}V(-3)=1$, που επίσης δεν συμβαίνει. Απομένει η περίπτωση $x+3,(x+3)^2$, η οποία μας δίνει $\dim_{\mathbb{R}}V(-3)=2$, όπως και συμβαίνει. Εδώ λοιπόν οι αναλλοίωτοι παράγοντες (στην περίπτωση αυτή είναι και οι στοιχειώδεις διαιρέτες) υπολογίζονται πιο γρήγορα απ' ότι υπολογίζονται με τον αλγόριθμο Smith.

Ας δούμε πάλι το **παράδειγμα 5.14. (v)**. Ο πίνακας της απεικόνισης $f:V\to V$ είναι ο

$A=\begin{pmatrix}18 & 5 & 5 & -1\\ -92 & -26 & -26 & 5\\ 39 & 11 & 11 & -2\\ 59 & 15 & 16 & -3\end{pmatrix}$, με χαρακτηριστικό πολυώνυμο

$$ch_A(x)=\begin{vmatrix}x-18 & -5 & -5 & 1\\ 92 & x+26 & 26 & -5\\ -39 & -11 & x-11 & 2\\ -59 & -15 & -16 & x+3\end{vmatrix}=-\begin{vmatrix}1 & -5 & -5 & x-18\\ -5 & x+26 & 26 & 92\\ 2 & -11 & x-11 & -39\\ x+3 & -15 & -16 & -59\end{vmatrix}=$$

$$=-\begin{vmatrix}1 & -5 & -5 & x-18\\ -5 & x+26 & 26 & 92\\ 2 & -11 & x-11 & -39\\ x+3 & -15 & -16 & -59\end{vmatrix}=-\begin{vmatrix}1 & 0 & -5 & x-18\\ -5 & x & 26 & 92\\ 2 & -x & x-11 & -39\\ x+3 & 1 & -16 & -59\end{vmatrix}=$$

$$=-\begin{vmatrix}1 & 0 & -5 & x-18\\ 0 & x & 1 & 5x+2\\ 2 & -x & x-11 & -39\\ x+3 & 1 & -16 & -59\end{vmatrix}=-\begin{vmatrix}1 & 0 & -5 & x-18\\ 0 & x & 1 & 5x+2\\ 0 & -x & x-1 & -2x-3\\ x+3 & 1 & -16 & -59\end{vmatrix}=$$

$$=-\begin{vmatrix}1 & 0 & -5 & x-18\\ 0 & x & 1 & 5x+2\\ 0 & -x & x-1 & -2x-3\\ 0 & 1 & 5x-1 & -x^2+15x-5\end{vmatrix}=\begin{vmatrix}1 & -5 & 0 & x-18\\ 0 & 1 & x & 5x+2\\ 0 & x-1 & -x & -2x-3\\ 0 & 5x-1 & 1 & -x^2+15x-5\end{vmatrix}=$$

$$=\begin{vmatrix}1 & x & 5x+2\\ x-1 & -x & -2x-3\\ 5x-1 & 1 & -x^2+15x-5\end{vmatrix}=\begin{vmatrix}1 & x & 5x+2\\ x & 0 & 3x-1\\ 5x & x+1 & -x^2+20x-3\end{vmatrix}=\begin{vmatrix}1 & x & 5x+2\\ 0 & -x^2 & -5x^2+x-1\\ 5x & x+1 & -x^2+20x-3\end{vmatrix}=$$

$$=\begin{vmatrix}1 & x & 5x+2\\ 0 & -x^2 & -5x^2+x-1\\ 0 & -5x^2+x+1 & -26x^2+10x-3\end{vmatrix}=\begin{vmatrix}-x^2 & -5x^2+x-1\\ -5x^2+x+1 & -26x^2+10x-3\end{vmatrix}=26x^4-10x^3+$$

$+3x^2-25x^4+5x^3+5x^2+5x^3-x^2-x-5x^2+x+1=x^4+2x^2+1=(x^2+1)^2$.

Παρατηρούμε ότι $A^2=\begin{pmatrix}18 & 5 & 5 & -1\\ -92 & -26 & -26 & 5\\ 39 & 11 & 11 & -2\\ 59 & 15 & 16 & -3\end{pmatrix}^2=\begin{pmatrix}0 & 0 & -1 & 0\\ 17 & 5 & 10 & -1\\ 1 & 0 & -2 & 0\\ 129 & 36 & 33 & -7\end{pmatrix}\neq -I_4$. Επομένως το ελάχιστο πολυώνυμο συμπίπτει με το χαρακτηριστικό. Αν θεωρήσουμε τον A ως μιγαδικό πίνακα, τότε χαρακτηριστικό και ελάχιστο είναι το ίδιο $(x^2+1)^2=(x-\mathbf{i})^2(x+\mathbf{i})^2$. Τα $(x-\mathbf{i})^2$ και $(x+\mathbf{i})^2$ είναι οι στοιχειώδεις διαιρέτες στο $\mathbb{C}[x]$ και ο A είναι όμοιος με τον πίνακα

$$\left(\begin{array}{cc|cc}\mathbf{i} & 0 & 0 & 0\\ 1 & \mathbf{i} & 0 & 0\\ \hline 0 & 0 & -\mathbf{i} & 0\\ 0 & 0 & 1 & -\mathbf{i}\end{array}\right)$$

σε μορφή Jordan. Εδώ σημειώνουμε το εξής: Για να αποδείξει κάποιος ότι $A^2\neq -I_4$, αρκεί να βρει ένα στοιχείο του A^2 που να μην είναι ίσο με το αντίστοιχο του $-I_4$. Διαλέγουμε τα μικρότερα νούμερα: Το $(1,4)$-στοιχείο του A^2 είναι το $18\cdot(-1)+5\cdot 5+5\cdot(-2)+(-1)(-3)=$ $=-18+25-10+3=0$, δεν μας κάνει γιατί ισούται με το αντίστοιχο στοιχείο του $-I_4$. Δοκιμάζουμε το $(1,3)$. Αυτό ισούται με $18\cdot 5+5(-26)+5\cdot 11-16=90-130+55-16=-1$, το οποίο **δεν ισούται** με το αντίστοιχο στοιχείο του $-I_4$. Άρα $A^2\neq -I_4$. Ένας άλλος τρόπος είναι να βρει κανείς ιδιοδιανύσματα που αντιστοιχούν σε μια ιδιοτιμή, π.χ. το $\mathbf{i}$. Αν δείξει ότι ο αντίστοιχος ιδιόχωρος έχει διάσταση 1, τότε το $(x-\mathbf{i})^2$ είναι στοιχειώδης διαιρέτης και λόγω

συμμετρίας και το $(x+\mathbf{i})^2$ είναι επίσης στοιχειώδης διαιρέτης. Άρα ο πίνακας έχει (είναι όμοιος με) την παραπάνω μορφή Jordan. Η επίλυση του αντίστοιχου συστήματος μπορεί να είναι επίπονη και να οδηγήσει σε λάθη. Πάντοτε επιλέγουμε την πιο σύντομη και εύκολη μέθοδο. Τέλος, αν θεωρήσουμε τον πίνακα ως πραγματικό και όχι μιγαδικό, τότε αυτός είναι όμοιος με τον συνοδό πίνακα του πολυωνύμου $(x^2+1)^2 = x^4+0x^3+2x^2+0x+1$, δηλαδή με τον πίνακα

$$\begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Τέλος, στο **παράδειγμα 5.14. (vi)** το χαρακτηριστικό πολυώνυμο του πίνακα

$$A = \begin{pmatrix} -14 & 4 & 7 & -28 \\ 3 & 0 & 0 & 7 \\ -6 & 0 & 2 & -12 \\ 6 & -2 & -3 & 12 \end{pmatrix}$$

είναι $ch_A(x) = \begin{vmatrix} x+14 & -4 & -7 & 28 \\ -3 & x & 0 & -7 \\ 6 & 0 & x-2 & 12 \\ -6 & 2 & 3 & x-12 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x^2+2 & 0 \\ 0 & 0 & 0 & x^2+2 \end{vmatrix} = (x^2+2)^2.$

Εδώ ο αλγόριθμος Smith δουλεύει καλύτερα.
Επομένως το ελάχιστο πολυώνυμο του A είναι x^2+2. Ως μιγαδικός ο πίνακας A είναι όμοιος με τον

$$\begin{pmatrix} \mathbf{i}\sqrt{2} & 0 & 0 & 0 \\ 0 & \mathbf{i}\sqrt{2} & 0 & 0 \\ 0 & 0 & -\mathbf{i}\sqrt{2} & 0 \\ 0 & 0 & 0 & -\mathbf{i}\sqrt{2} \end{pmatrix},$$

δηλαδή διαγωνίσιμος, ενώ ως πραγματικός με τον

$$\begin{pmatrix} \boxed{\begin{matrix} 0 & -2 \\ 1 & 0 \end{matrix}} & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \boxed{\begin{matrix} 0 & -2 \\ 1 & 0 \end{matrix}} \end{pmatrix}.$$

Σημειωτέον ότι ο 2×2 πίνακας $\begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}$ είναι ο συνοδός πίνακας του πολυωνύμου x^2+2.

ΕΦΑΡΜΟΓΗ 5.25. α) Έστω V ένας πραγματικός διανυσματικός χώρος με $\dim_{\mathbb{R}} V = 7$ και $f \in \mathrm{End}_{\mathbb{R}} V$. Αν το ελάχιστο πολυώνυμο του f είναι το $(x+2)^2(x-1)^2$, να βρεθούν οι πιθανοί αναλλοίωτοι παράγοντες και οι πιθανές μορφές Jordan του πίνακά του (ως προς κατάλληλη βάση του V).
β) Δείξτε ότι δεν υπάρχει $A \in \mathbb{Q}^{3\times 3}$ τέτοιος, ώστε $A^8 = I$ και $A^4 \neq I$.
ΛΥΣΗ: α) Πιθανοί αναλλοίωτοι παράγοντες:

1) $x+2, x+2, x+2, (x+2)^2(x-1)^2$ **2)** $x+2, (x+2)^2, (x+2)^2(x-1)^2$
3) $x-1, x-1, x-1, (x+2)^2(x-1)^2$ **4)** $x-1, (x-1)^2, (x+2)^2(x-1)^2$
5) $x+2, (x+2)(x-1), (x+2)^2(x-1)^2$ **6)** $x-1, (x+2)(x-1), (x+2)^2(x-1)^2$
7) $(x+2)^2(x-1), (x+2)^2(x-1)^2$ **8)** $(x+2)(x-1)^2, (x+2)^2(x-1)^2$.

Πιθανές μορφές Jordan:

1) $\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$ **2)** $\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$

3) $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}$ **4)** $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}$

5) $\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$ **6)** $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}$

7) $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}$ **8)** $\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$

β) Ο A μηδενίζει το πολυώνυμο $x^8-1=(x^4-1)(x^4+1)=(x+1)(x-1)(x^2+1)(x^4+1)$, άρα το ελάχιστο πολυώνυμό του διαιρεί το x^8-1 και έχει τους ίδιους ανάγωγους παράγοντες με το χαρακτηριστικό, το οποίο είναι $3^{ου}$ βαθμού. Τώρα, τα πολυώνυμα $x+1$, $x-1$, x^2+1 είναι ανάγωγα επί του $\mathbb{R}$, άρα και επί του $\mathbb{Q}$. Το $x^4+1=(x^2+1)-\left(\sqrt{2}\,x\right)^2=\left(x^2+\sqrt{2}\,x+1\right)\left(x^2-\sqrt{2}\,x+1\right)$ δεν είναι ανάγωγο επί του $\mathbb{R}$. Θα αποδείξουμε ότι είναι ανάγωγο επί του $\mathbb{Q}$. Προφανώς δεν έχει πρωτοβάθμιο παράγοντα στο $\mathbb{Q}[x]$ γιατί δεν έχει ρητή, αλλά ούτε και πραγματική ρίζα. Υποθέτουμε ότι το x^4+1 είναι γινόμενο δύο δευτεροβαθμίων πολυωνύμων από το $\mathbb{Q}[x]$, τα οποία, επειδή το x^4+1 είναι μονικό, μπορούμε να υποθέσουμε ότι είναι μονικά. Έστω $x^2+\alpha x+\beta\in\mathbb{Q}[x]$ ο ένας από τους δύο παράγοντες. Όπως προαναφέραμε, το $x^2+\alpha x+\beta$ δεν έχει πρωτοβάθμιο παράγοντα στο $\mathbb{Q}[x]$, ούτε και στο $\mathbb{R}[x]$. Επομένως το $x^2+\alpha x+\beta$ θα είναι ανάγωγο στο $\mathbb{R}[x]$. Επειδή $x^2+\alpha x+\beta \mid \left(x^2+\sqrt{2}\,x+1\right)\left(x^2-\sqrt{2}\,x+1\right)$, θα έχουμε $x^2+\alpha x+\beta=x^2+\sqrt{2}\,x+1$ ή $x^2+\alpha x+\beta=x^2-\sqrt{2}\,x+1$. Και στις δύο περιπτώσεις καταλήγουμε σε άτοπο, γιατί $x^2\pm\sqrt{2}\,x+1\notin\mathbb{Q}[x]$.

Εφόσον και οι τέσσερις παράγοντες $x+1$, $x-1$, x^2+1 και x^4+1 είναι ανάγωγοι επί του $\mathbb{Q}$ και το

χαρακτηριστικό πολυώνυμο είναι $3^{ου}$ βαθμού, το ελάχιστο θα είναι βαθμού μικρότερου ή ίσου του 3 και θα έχει ανάγωγους παράγοντες κάποιους από τους $x+1$, $x-1$, x^2+1 και μάλιστα στην $1^η$ δύναμη, γιατί σ' αυτήν εμφανίζεται στο πολλαπλάσιό του x^8-1. $\big($Το x^4+1 αποκλείεται γιατί είναι βαθμού μεγαλύτερου του $3\big)$. Επομένως το ελάχιστο πολυώνυμο θα διαιρεί το γινόμενο $(x+1)(x-1)(x^2+1)=x^4-1$ και συνεπώς $A^4=I_3$, άτοπο. ■