423. Δακτύλιοι και Πρότυπα

Διδασκων:
Ι. Εμμανουήλ

by
AmpalosMathimatikos

Χειμερινό Εξάμηνο 2011 - 2012

Περιεχόμενα

0.1 Δακτύλιοι και Ιδεώδη

Ορισμός 0.1.1. Έστω $R \neq \emptyset$, $+ : R \times R \to R$, $\cdot : R \times R \to R$. Ο $(R, +, \cdot)$ ονομάζεται **δακτύλιος** αν:

(i) $(a + b) + c = a + (b + c)$ για κάθε $a, b, c \in R$.

(ii) Υπάρχει το $0_R \in R$ με $a + 0_R = 0_r + a = a$ για κάθε $a \in R$.

(iii) Για κάθε $a \in R$ υπάρχει το $a' \in R$ με $a + a' = a' + a = 0_R$.

(iv) $a + b = b + a$ για κάθε $a, b \in R$.

(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ για κάθε $a, b, c \in R$.

(vi) $a \cdot (b + c) = a \cdot b + a \cdot c$ για κάθε $a, b, c \in R$.

(vii) $(a + b) \cdot c = a \cdot c + b \cdot c$ για κάθε $a, b, c \in R$.

Ορισμός 0.1.2. Αν επιπλέον, $a \cdot b = b \cdot a$ για κάθε $a, b \in R$, τοτε ο R καλείται **μεταθετικός**.

Ορισμός 0.1.3. Ένας δακτύλιος R καλείται **ακέραια περιοχή** αν:

(i) $1_R \neq 0_R$.

(ii) Αν $a, b \in R \backslash \{0\}$, τότε $ab \neq 0_R$.

Ορισμός 0.1.4. Ένα $a \in R$ καλείται **αντιστρέψιμο** αν υπάρχει $b \in R$ με $ab = 1_R$.

Παρατήρηση 0.1.1. Αν το $a \in R$ είναι αντιστρέψιμο, τότε το $b \in R$ με $ab = 1_R$ είναι μοναδικό.

Πρόταση 0.1.1. *Αν $U(R) = \{a \in R : a \, \text{αντιστρέψιμο}\}$, τότε το $U(R)$ είναι μια (αβελιανή) ομάδα με πράξη τον πολλαπλασιασμό του R.*

Απόδειξη. Προφανώς, $1 \in U(R)$.

Επίσης, αν $a, b \in U(R)$, τότε $ab \in U(R)$, $(ab)^{-1} = a^{-1}b^{-1}$. Τέλος, αν $a \in U(R)$, τότε $a^{-1} \in U(R)$ και $(a^{-1})^{-1} = a$. □

Παραδείγματα 0.1.1. (i) Ισχύει ότι $U(\mathbb{Z}) = \{1, -1\} \simeq \mathbb{Z}_2$.

(ii) Έστω

$$\mathbb{Z}[i] = \{a + bi \colon a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

Τότε $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\} \simeq \mathbb{Z}_4$.

Προφανώς, $\{\pm 1, \pm i\} \subseteq U(\mathbb{Z}[i])$. Θεωρούμε την

$$N : \mathbb{Z}[i] \to \mathbb{N}, \qquad N(a + bi) = a^2 + b^2, \quad \forall a + bi \in \mathbb{Z}[i]$$

Παρατηρούμε ότι

$$N(kl) = N(k)N(\ell) \quad \forall k, \ell \in \mathbb{Z}[i]$$

Αν $a + bi \in U(\mathbb{Z}[i])$, τότε υπάρχει $p \in \mathbb{Z}[i]$ με $(a + bi)p = 1 \in \mathbb{Z}[i]$.

Συνεπώς,

$$1 = N(1) = N[(a + bi)p] = N(a + bi)N(p) \in \mathbb{N}$$

άρα $a^2 + b^2 = 1$ και $a + bi \in \{\pm 1, \pm i\}$.

(iii) Έστω

$$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \colon a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

Τότε $U(\mathbb{Z}[\sqrt{-5}]) = \{\pm 1\} \simeq \mathbb{Z}_2$.

Θεωρούμε την

$$N \colon R \to \mathbb{N}, \qquad N(a + b\sqrt{-5}) = a^2 + 5b^2$$

Και εδώ

$$N(k\ell) = N(k)N(\ell) \quad \forall k, \ell \in R$$

Συνεπώς, αν $k \in U(R)$, τότε $kk^{-1} = 1$, άρα

$$N(k)N(k^{-1}) = N(kk^{-1}) = N(1) = 1 \in \mathbb{N}$$

Οπότε $N(k) = 1$. Έτσι, αν $k = a + b\sqrt{-5}$, τότε $a^2 + 5b^2 = 0$ και $k = a + b\sqrt{-5} \in \{\pm 1\}$.

(iv) Αν $\mathbb{F}$ σώμα και $\mathbb{F}[x]$ ο δακτύλιος των πολυωνύμων στη μεταβλητή x επί του $\mathbb{F}$, τότε $U(\mathbb{F}[x]) = \mathbb{F}^*$.

(v) Άμεσα, έπεται ότι αν R είναι μια ακέραια περιοχή, τότε $U(R[x]) = U(R)$.

Πρόταση 0.1.2. *Έστω R δακτύλιος και $\emptyset \neq S \subseteq R$. Τότε το S είναι **υποδακτύλιος** του R ανν ισχύει ότι αν $a, b \in S$, τότε $a - b, ab \in S$.*

Ορισμός 0.1.5. Έστω R δακτύλιος. Ένα μη κενό υποσύνολο I του R ονομάζεται **ιδεώδες** του R αν:

(i) Αν $a, b \in I$, τότε $a - b \in I$.

(ii) Αν $a \in I, r \in R$, τότε $ar \in I$.

0.2 Ομάδες

Ορισμός 0.2.1. Έστω $\emptyset \neq G$, $\cdot : G \times G \to G$. Η $(G, \cdot)$ λέγεται **ομάδα** αν:

(i) Υπάρχει το $e \in G$ τέτοιο ώστε $x \cdot e = e \cdot x = x$ για κάθε $x \in G$.

(ii) Για κάθε $x \in G$ υπάρχει $y \in G : x \cdot y = y \cdot x = e$.

(iii) $x \circ (y \cdot z) = (x \cdot y) \cdot z$ για κάθε $x, y, z \in G$.

Ορισμός 0.2.2. Αν επιπλέον, $x \cdot y = y \cdot x$ για κάθε $x, y \in G$, η ομάδα θα λέγεται **αβελιανή**.

Ορισμός 0.2.3. Το πλήθος των στοιχείων μιας ομάδας καλείται **τάξη** της ομάδας.

Ορισμός 0.2.4. Έστω a ένα στοιχείο μιας ομάδας G. Αν υπάρχει θετικός ακέραιος m για τον οποίο $a^m = e$, τότε ο μικρότερος φυσικός n για τον οποίο ισχύει $a^n = e$ ονομάζεται **τάξη** του a. Αν δεν υπάρχει θετικός ακέραιος m ώστε $a^m = e$, τότε λέμε ότι το στοιχείο έχει άπειρη τάξη.

Πρόταση 0.2.1. *Έστω G ομάδα και $\emptyset \neq H \subseteq G$. Τότε, τα επόμενα είναι ισοδύναμα:*

*(i) H H είναι **υποομάδα** της G.*

(ii) Αν $h_1, h_2 \in H$, τότε $h_1 h_2^{-1} \in H$.

(iii) Αν $h_1, h_2 \in H$, τότε $h_1 h_2 \in H$ και $h_1^{-1} \in H$.

0.3 Διανυσματικοί Χώροι

Ορισμός 0.3.1. Ένας μεταθετικός δακτύλιος με $1_R \neq 0_R$ στο οποίο κάθε μη μηδενικό στοιχείο είναι αντιστρέψιμο καλείται **σώμα**.

Ορισμός 0.3.2. Έστω $\mathbb{F} = \mathbb{R}$ ή $\mathbb{F} = \mathbb{C}$. Ένας **διανυσματικός χώρος** επί του $\mathbb{F}$ αποτελείται από ένα μη κενό σύνολο V και δύο απεικονίσεις $+ : V \times V \to V, \cdot : \mathbb{F} \times V \to V$ έτσι ώστε να ισχύουν:

(i) $a + b = b + a$ για κάθε $a, b \in V$.

(ii) $(a + b) + c = a + (b + c)$ για κάθε $a, b, c \in V$.

(iii) Υπάρχει $0_V \in V$ με $a + 0_V = 0_V + a = a$ για κάθε $a \in V$.

(iv) Για κάθε $a \in V$ υπάρχει το $-a \in V$ με $a + (-a) = (-a) + a = 0_V$.

(v) $\lambda(a + b) = \lambda a + \lambda b$ για κάθε $\lambda \in \mathbb{F}$, $a, b \in V$.

(vi) $(\lambda + \mu)a = \lambda a + \mu a$ για κάθε $\lambda, \mu \in \mathbb{F}$, $a \in V$.

(vii) $(\lambda\mu)a = \lambda(\mu a)$ για κάθε $\lambda, \mu \in \mathbb{F}$, $a \in V$.

(viii) $1a = a$ για κάθε $a \in V$.

Ορισμός 0.3.3. Έστω V ένας διανυσματικός χώρος επί του $\mathbb{F}$. Ένα υποσύνολο A του V λέγεται **υπόχωρος** του V αν:

(i) $0_V \in A$.

(ii) Αν $a, b \in A$, τότε $a + b \in A$.

(iii) Αν $\lambda \in \mathbb{F}$, $a \in A$, τότε $\lambda a \in A$.

Ορισμός 0.3.4. Έστω V διανυσματικός χώρος επί του $\mathbb{F}$ και B ένα υποσύνολο του. Το B θα λέγεται **βάση** του V, αν:

(i) Το σύνολο B είναι γραμμικά ανεξάρτητο.

(ii) $\langle B \rangle = V$.

Ορισμός 0.3.5. Έστω V ένας διανυσματικός χώρος επί του $\mathbb{F}$, πεπερασμένα παραγόμενος. Ο αριθμός των στοιχείων μιας οποιασδήποτε βάσης του, λέγεται **διάσταση** του χώρου και συμβολίζεται με $\dim_{\mathbb{F}} V$.

Κεφάλαιο 1

Παραγοντοποίηση σε Ακέραιες Περιοχές

1.1 Βασικές Έννοιες

Πρόταση 1.1.1. *Έστω R ακέραια περιοχή και $a, b \in R$. Τότε τα εξής είναι ισοδύναμα:*

(i) Υπάρχει $r \in R$ τέτοιο ώστε $b = ra$.

(ii) $(b) \subseteq (a)$.

*Στην περίπτωση αυτή, λέμε ότι το a **διαιρεί** το b (στον R) και γράφουμε $a|b$.*

Απόδειξη. (i) $\Rightarrow$ (ii) Αν $x \in (b)$, τότε $x = lb$ για κάποιο $l \in R$. Τότε, όμως,

$$x = lra = (lr)a \in (a)$$

(ii) $\Rightarrow$ (i) Είναι $b = 1b$ και άρα $b \in (b)$. Συνεπώς, $b \in (a)$, άρα $b = ra$ για κάποιο $r \in R$. $\square$

Πρόταση 1.1.2. *Έστω R μια ακέραια περιοχή. Τότε:*

(i) $a|a$ για κάθε $a \in R$.

(ii) Αν $a|b$ και $b|c$, τότε $a|c$ ανν $(c) \subseteq (b) \subseteq (a)$.

(iii) Αν $a|b$ και $a|c$, τότε $a|rb + sc$ για κάθε $r, s \in R$.

Πρόταση 1.1.3. *Έστω R ακέραια περιοχή και $a, b \in R$. Τότε, τα εξής είναι ισοδύναμα:*

(i) $a|b$ και $b|a$.

(ii) $(a) = (b)$.

(iii) Υπάρχει $r \in U(R)$ τέτοιο ώστε $b = ra$ ανν $a = r^{-1}b$.

*Στην περίπτωση αυτή, λέμε ότι τα a και b είναι **συντροφικά** (στον δακτύλιο R) και γράφουμε $a \sim b$.*

Απόδειξη. (ii) $\Rightarrow$ (iii) Έχουμε $a|b$ και $b|a$, συνεπώς $(b) \subseteq (a)$ και $(a) \subseteq (b)$. Τελικά, $(a) = (b)$.
(ii) $\Rightarrow$ (i) Έστω $b \neq 0$. Καθώς $b \in (b) = (a)$ έχουμε $b = ra$, για κάποιο $r \in R$.

Όμοια, $a \in (a) = (b)$, άρα $a = sb$, για κάποιο $s \in R$. Τότε, $b = ra = rsb$, δηλαδή $1 = rs$, οπότε $r \in U(R)$.

Αν $b = 0$, τότε $(b) = \{0\}$ και άρα $(a) = \{0\}$, συνεπώς $a = 0$. Τελικά, $0 = b = 1 \cdot 0 = 0 = a$.
(iii) $\Rightarrow$ (i) Καθώς $b = ra$, έχουμε $a|b$. Επίσης, $a = r^{-1}b$, άρα $b|a$. □

Πρόταση 1.1.4. *Έστω R ακέραια περιοχή και $p \in R$ με $p \notin U(R) \cup \{0\}$. Τότε, τα εξής είναι ισοδύναμα:*

(i) Αν $a|p$, τότε $a \in U(R)$ ή $a \sim b$.

(ii) Αν $a, b \in R$ και $p = ab$, τότε $a \in U(R)$ ή $b \in U(R)$.

(iii) Αν $a \in R$ και $(p) \subseteq (a)$, τότε $(a) = (p)$ ή $(a) = R$.

*Στην περίπτωση που τα παραπάνω ισχύουν, λέμε ότι το $p \in R$ είναι **ανάγωγο**.*

Απόδειξη. (i) $\Rightarrow$ (ii) Έστω $a, b \in R$ με $p = ab$. Τότε, $a|p$ και άρα $a \in U(R)$ ή $a \sim p$. Αν $a \sim p$, υπάρχει $r \in U(R)$ τέτοιο ώστε $p = ra$. Όμως, $p = ab$ και άρα $ra = ab$, δηλαδή $b = r \in U(R)$.
(ii) $\Rightarrow$ (iii) Αν $a \in R$ και $(p) \subseteq (a)$, είναι $p \in (p) \subseteq (a)$, και άρα $p = ar$, για κάποιο $r \in R$. Από το (ii) ή $a \in U(R)$ ή $r \in U(R)$. Αν $a \in U(R)$, τότε $(a) = R$. Αν $r \in U(R)$, τότε $a \sim p$, και άρα $(a) = (p)$.
(iii) $\Rightarrow$ (i) Έστω $a \in R$ με $a|p$. Τότε, $(p) \subseteq (a)$, άρα $(a) = (p)$ ή $(a) = R$. Αν $(a) = (p)$, τότε $a \sim p$. Αν $(a) = R$, τότε $a \in U(R)$. □

Παραδείγματα 1.1.1. (i) Έστω $R = \mathbb{Z}$. Δύο στοιχεία $a, b \in \mathbb{Z}$ είναι συντροφικά ανν $b = \pm a$. Ένα $p \in \mathbb{Z}\backslash\{\pm 0, \pm 1\}$ είναι ανάγωγο ανν ο p είναι πρώτος.

(ii) Έστω $R = \mathbb{F}[x]$, όπου $\mathbb{F}$ σώμα. Δύο πολυώνυμα $f(x), g(x) \in \mathbb{F}[x]$ είναι συντροφικά ανν $g(x) = cf(x)$, για κάποιο $c \in \mathbb{F}^*$. Ένα μη-σταθερό πολυώνυμο $f(x) \in \mathbb{F}[x]$ είναι ανάγωγο (σύμφωνα με τον ορισμό που δώσαμε) ανν $f(x) = af_0(x)$, για κάποιο $a \in \mathbb{F}^*$ και κάποιο μονικό ανάγωγο πολυώνυμο (σύμφωνα με τον κλασσικό ορισμό) $f_0(x) \in \mathbb{F}[x]$.

(iii) Έστω $R = \mathbb{Z}[\sqrt{-5}]$. Το στοιχείο $5 \in \mathbb{Z}[\sqrt{-5}]$ δεν είναι ανάγωγο μιας και $5 = (\sqrt{-5})(-\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$. Γνωρίζουμε ότι $U(R) = \{\pm 1\}$ και άρα $\pm\sqrt{-5} \notin U(R)$.

(iv) Όμοια, η σχέση $5 = (2+i)(2-i) \in \mathbb{Z}[\sqrt{-5}]$ δείχνει ότι ο $5 \in \mathbb{Z}[\sqrt{-5}]$ δεν είναι ανάγωγο.

1.2 Περιοχές Μοναδικής Παραγοντοποίησης

Ορισμός 1.2.1. Μια ακέραια περιοχή R καλείται **περιοχή μοναδικής παραγοντοποίησης** (ΠΜΠ) αν:

(i) Κάθε στοιχείο $r \in R$ με $r \notin U(R) \cup \{0\}$ γράφεται ως γινόμενο της μορφής $p_1 p_2 \cdots p_m$, όπου $p_1, p_2, \ldots, p_m \in R$ ανάγωγα.

(ii) Αν $p_1, p_2, \ldots, p_m$ και $q_1, q_2, \ldots, q_n$ ανάγωγα στο R με $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$, τότε $m = n$ και υπάρχει $\sigma \in S_n$ τέτοια ώστε $p_i \sim q_{\sigma(i)}$ για κάθε $i = 1, 2, \ldots, n$.

Παραδείγματα 1.2.1. (i) Οι δακτύλιοι $\mathbb{Z}$ και $\mathbb{F}[x]$, όπου $\mathbb{F}$ σώμα, είναι ΠΜΠ.

(ii) Ο $R = \mathbb{Z}[\sqrt{-5}]$ δεν είναι ΠΜΠ.

Θεωρούμε την παραγοντοποίηση $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \in R$.

Καθώς $U(R) = \{\pm 1\}$, τα συντροφικά του 2 είναι το 2 και το -2. Προφανώς, $1 \pm \sqrt{-5} \notin \{\pm 2\}$, άρα $2 \not\sim 1 \pm \sqrt{-5}$. Όμοια, $3 \not\sim 1 \pm \sqrt{-5}$.

Δείχνουμε ότι τα $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ είναι ανάγωγα.

Έστω $N \colon R \to \mathbb{N}$, με $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Γνωρίζουμε ότι, $N(k\ell) = N(k)N(\ell)$ για κάθε $k, \ell \in R$ και $N(k) = 1$ ανν $k \in \{\pm 1\} = U(R)$. Συνεπώς, αν $k \in \mathbb{Z}[\sqrt{-5}]$ και $N(k) = p \in \mathbb{Z}$, όπου p πρώτος (στον $\mathbb{Z}$), τότε το $k \in \mathbb{Z}[\sqrt{-5}]$ είναι ανάγωγο. Πράγματι, αν $k = k_1 k_2$, τότε $N(k) = N(k_1)N(k_2)$, και άρα $N(k_1) = 1$ ή $N(k_2) = 1$. Τότε, $k_1 \in U(R)$ ή $k_2 \in U(R)$. Τώρα, το $2 \in \mathbb{Z}[\sqrt{-5}]$ είναι ανάγωγο. Αν $2 = k\ell \in R$, τότε $N(2) = N(k)N(\ell)$, οπότε $4 = N(k)N(\ell)$. Συνεπώς,

Π1. $N(k) = 1$ και $N(\ell) = 4$ ή

Π2. $N(k) = 2$ και $N(\ell) = 2$ ή

Π3. $N(k) = 4$ και $N(\ell) = 1$

Καθώς, $N(a + b\sqrt{-5}) = a^2 + 5b^2 \neq 2$ για καθε $a, b \in \mathbb{Z}$, έπεται ότι το ενδεχόμενο Π2 είναι αδύνατο. Όμοια, τα 3, $1 \pm \sqrt{-5}$ είναι ανάγωγα.

Πρόταση 1.2.1. *Έστω R ακέραια περιοχή και $p \notin U(R) \cup \{0\}$. Τότε, τα εξής είναι ισοδύναμα:*

(i) Αν $a, b \in R$ και $p|ab$, τότε $p|a$ ή $p|b$.

(ii) Ο δακτύλιος-πηλίκο $R/(p)$ είναι μια ακέραια περιοχή.

*Στην περίπτωση αυτή, λέμε ότι το $p \in R$ είναι **πρώτο**.*

Απόδειξη. (i) $\Rightarrow$ (ii) Καθώς $p \in U(R)$ και $(p) \neq R$ έχουμε ότι $R/(p) \neq 0$. Θα δείξουμε ότι ο $R/(p)$ είναι ακέραια περιοχή. Έστω

$$a + (p), b + (p) \in R/(p) \, : \, [a + (p)][b + (p)] = 0 + (p)$$

Τότε, $ab + (p) = 0 + (p) \in R/(p)$. Άρα $ab \in (p)$. Συνεπώς, $p|ab$, και άρα $p|a$ ή $p|b$. Τότε, $a \in (p)$ ή $b \in (p)$, δηλαδή

$$a + (p) = 0 + (p) \in R/(p)$$

ή

$$b + (p) = 0 + (p) \in R/(p)$$

Άρα ο $R/(p)$ είναι ακέραια περιοχή.
(ii) $\Rightarrow$ (i) Έστω $a, b \in R$ με $p|ab$. Τότε $ab \in (p)$ και

$$[a + (p)][b + (p)] = ab + (p) = 0 + (p) \in R/(p)$$

Όμως, ο $R/(p)$ είναι ακέραια περιοχή, άρα $a + (p) = 0 + (p)$ ή $b + (p) = 0 + (p)$, και έτσι $a \in (p)$ ή $b \in (p)$. Τελικά, $p|a$ ή $p|b$. □

Παρατηρήσεις 1.2.1. (i) Έστω R ακέραια περιοχή και $p \in R$ με $p \notin U(R) \cup \{0\}$, που είναι πρώτο. Τότε, το $p \in R$ είναι ανάγωγο.

Αν $a, b \in R$ με $p = ab$, προφανώς $p|ab$ και άρα $p|a$ ή $p|b$. Αν $p|a$, γράφουμε $a = px$, για κάποιο $x \in R$ και $p = (px)b = pxb$, δηλαδή $1 = xb$, οπότε $b \in U(R)$. Όμοια, αν $p|b$, τότε $a \in U(R)$.

(ii) Στον δακτύλιο $\mathbb{Z}[\sqrt{-5}]$, το στοιχείο 2 είναι ανάγωγο, αλλά όχι πρώτο.

Γνωρίζουμε ότι το $2 \in \mathbb{Z}[\sqrt{-5}]$ δεν είναι ανάγωγο. Για να δείξουμε ότι το $2 \in \mathbb{Z}[\sqrt{-5}]$ δεν είναι πρώτο, παρατηρούμε ότι $2|6 = (1+\sqrt{-5})(1-\sqrt{-5})$, αλλά $2 \not| 1 \pm \sqrt{-5}$.

(iii) Αν ο R είναι ΠΜΠ και το $p \in R$ ανάγωγο, τότε το $p \in R$ είναι πρώτο.

Πράγματι, αν $a, b \in R$ και $p|ab$, τότε υπάρχει $c \in R$ τέτοιο ώστε $ab = pc$. Γράφουμε

$$a = p_1 p_2 \cdots p_n,\ b = q_1 q_1 \cdots q_m,\ c = s_1 s_2 \cdots s_\ell$$

όπου n, m, $\ell \in \mathbb{N}$ και p_i, q_j, $s_t \in R$ ανάγωγα. Τότε,

$$p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m = p s_1 s_2 \cdots s_\ell$$

και άρα από την "μοναδικότητα" της παραγοντοποίησης , έχουμε $p \sim p_i$ για κάποιο $i = 1, 2, \ldots, n$ ή $p \sim q_j$ για κάποιο $j = 1, 2, \ldots, m$. Στην 1η περίπτωση $(a) \subseteq (p_i) = (p)$ άρα $p|a$, ενώ στην 2η $(b) \subseteq (q_j) = (p)$ άρα $p|b$.

(iv) Αν R μια ΠΜΠ και $r \in R$ με $r \notin U(R) \cup \{0\}$, μπορούμε να γράψουμε

$$r = u p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

όπου $u \in U(R)$, $a_i \geq 0$, $p_i \in R$ ανάγωγα και ανά δύο μη-συντροφικά. Αν

$$s = v p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

όπου $v \in U(R)$, $b_j \geq 0$, τότε

$$r|s \Leftrightarrow a_1 \leq b_1, a_2 \leq b_2, \ldots a_n \leq b_n$$

Πρόταση 1.2.2. *Έστω R ΠΜΠ και $a, b \in R$ με*

$$a = u p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k},\ b = v p_i^{m_1} p_2^{m_2} \cdots p_k^{m_k}$$

όπου u, $v \in U(R)$, n_i, $m_i \geq 0$, p_i, $p_2 \ldots, p_k \in R$ είναι ανάγωγα και ανα δυο μη-συντροφικά. Τότε,

$$a|b \Leftrightarrow n_i \leq m_i, \quad \forall i = 1, 2, \ldots, k$$

Απόδειξη. : ($\Leftarrow$) Έστω $n_i \leq m_i$ για κάθε i, $\ell_i = m_i - n_i \geq 0$ και

$$c = v u^{-1} p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{\ell_k} \in R$$

Παρατηρούμε ότι

$$\begin{aligned} ac &= u p_1^{m_1} p_2^{m_2} \cdots p_k^{n_k} v u^{-1} p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{\ell_k} \\ &= v p_1^{n_1+\ell_1} p_2^{n_2+\ell_2} \cdots p_k^{n_k+\ell_k} \\ &= v p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} = b \end{aligned}$$

Άρα, $a|b$.
($\Rightarrow$) Έστω $a|b$, αλλά $n_1 > m_1$. Καθώς, $a|b$, υπάρχει $c \in R$ με $b = ac$, άρα

$$v p_i^{m_1} p_2^{m_2} \cdots p_k^{m_k} = u p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} c$$

και

$$vp_2^{m_2}\cdots p_k^{m_k} = up_1^{n_1-m_1}p_2^{n_2}\cdots p_k^{n_k}c$$

άρα

$$p_1|vp_2^{m_2}\cdots p_k^{m_k}$$

Οπότε $p_1|v$ ή $p_1|p_i$, για κάποιο $i = 2,\ldots,k$. Αν $p_1|v$, τότε $R = (v) \subseteq (p_1)$, άρα $(p_1) = R$ και $p_1 \in U(R)$ -άτοπο.
Αν $p_1|p_i$. τότε $(p_i) \subseteq (p_1) \subset R$ άρα $(p_i) = (p_1)$, οπότε $p_i \sim p_1$ -άτοπο. □

Παρατήρηση 1.2.1. Έστω R ΠΜΠ και

$$\lambda\colon R\backslash[\{0\}\cup U(R)] \to \mathbb{N}, \quad \lambda(r) = n$$

αν μπορούμε να γράψουμε $r = p_1p_2\cdots p_n$, για κάποια ανάγωγα $p_i \in R$. Αν $a, b \in R$ και $(b) \subset (a)$, τότε $\lambda(a) < \lambda(b)$.

Πράγματι, όπως πριν, μπορούμε να γράψουμε

$$a = up_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}, \quad b = vp_i^{m_1}p_2^{m_2}\cdots p_k^{m_k}$$

Τότε, $\lambda(a) = n_1 + n_2 + \cdots + n_k$ και $\lambda(b) = m_1 + m_2 + \cdots + m_k$.

Καθώς, $(b) \subseteq (a)$ έχουμε $a|b$, άρα $n_i \leq m_i$. Συνεπώς, $\lambda(a) \leq \lambda(b)$. Καθώς $(b) \subset (a)$, τουλάχιστον μία από τις ανισότητες είναι γνήσια. Αν $n_i = m_i$ για κάθε i, τότε $m_i \leq n_1$ για κάθε i, δηλαδή $b|a$. Έτσι $(a) \subseteq (b)$, οπότε $(a) = (b)$.
Τελικά, $\lambda(a) < \lambda(b)$.

Πρόταση 1.2.3. *Έστω R ΠΜΠ και $r_1, r_2, \ldots, r_n, \ldots \in R$ με*

$$(r_1) \subseteq (r_2) \subseteq \ldots \subseteq (r_n) \subseteq \ldots$$

Τότε, η ακολουθία αυτή είναι τελικά σταθερή, δηλαδή υπάρχει $n_0 \in \mathbb{N}$ τέτοιο ώστε

$$(r_{n_0}) = (r_{n_0+1}) = \cdots$$

Μια ΠΜΠ ικανοποιεί την συνθήκη αύξουσας άλυσης στα κύρια ιδεώδη του.

Απόδειξη. Έστω ότι η ακολουθία των κυρίων ιδεωδών δεν είναι τελικά σταθερή. Τότε, υπάρχει (k_n) τέτοιο ώστε

$$1 = k_1 < k_2 < \cdots < k_m < \cdots$$

Τότε, έχουμε

$$(r_{k_1}) \subset (r_{k_2}) \subset \ldots \subset (r_{k+m}) \subset \ldots$$

Προφανώς, $(r_{k_n}) \neq R$ για κάθε $n \in \mathbb{N}$, και άρα $r_{k_n} \notin U(R)$. Όμοια, $r_{k_n} \neq 0$ για κάθε $n \geq 2$. Από την Παρατήρηση 1.2.1 έπεται ότι

$$\lambda(r_{k_2}) < \lambda(r_{k_3}) < \cdots < \lambda(r_{k_n}) < \cdots$$

-άτοπο. □

Θεώρημα 1.2.1. *Μια ακέραια περιοχή R είναι ΠΜΠ αν:*

(i) Κάθε ανάγωγο στοιχείο $p \in R$ είναι πρώτο και

(ii) Ο R ικανοποιεί τη συνθήκη αύξουσας άλυσης στα κύρια ιδεώδη του.

Απόδειξη. ($\Rightarrow$) Γνωρίζουμε ότι μια ΠΜΠ ικανοποιεί τα (i),(ii).
($\Leftarrow$) Σε μια ακέραια περιοχή R θεωρούμε ένα στοιχείο $a \in R$ με $q \notin U(R) \cup \{0\}$, το οποίο δεν μπορεί να γραφεί ως γινόμενο αναγώγων στοιχείων. Τότε, προφανώς, το a δεν είναι ανάγωγο και άρα μπορούμε να γράψουμε $a = xy$, για κάποια $x, y \in R \backslash U(R)$ που δεν μπορούν να γραφτούν ως γινόμενο αναγώγων. Παρατηρούμε ότι, $(a) \subset (x)$, $(a) \subset (y)$. Πράγματι, αν $(a) = (x)$, τότε $a \sim x$, άρα $a = xu$ για κάποιο $u \in U(R)$. Όμως, $a = xy$, άρα $xy = xu$, οπότε $y = u \in U(R)$-άτοπο.

Επιστρέφοντας στην απόδειξη, θα δείξουμε ότι η (ii) εγγυάται ότι κάθε $a \in R \backslash [U(R) \cup \{0\}]$ γράφεται ως γινόμενο αναγώγων. Έστω $a \in R \backslash [U(R) \cup \{0\}]$, που να μην γράφεται ως γινόμενο αναγώγων. Τότε, μπορούμε να βρούμε $b \in R \backslash [U(R) \cup \{0\}]$ τέτοιο ώστε $(a) \subset (b)$ και το b να μην γράφεται ως γινόμενο αναγώγων. Μπορούμε, επιπλέον, να βρούμε $c \in R \backslash [U(R) \cup \{0\}]$ με $(a) \subset (b) \subset (c)$ και το c να ικανοποιεί την ίδια απαίτηση. Συνεχίζοντας, κατασκευάζουμε μια γνησίως αύξουσα ακολουθία κυρίων ιδεωδών του R -άτοπο. Έστω ότι για το a μπορούμε να γράψουμε

$$a = up_1p_2 \cdots p_n = q_1q_2 \cdots q_m$$

για κάποια ανάγωγα $p_1, p_2, \ldots, p_n$, $q_1, q_2, \ldots, q_m$. Τότε, $p_1 | aq_1q_2 \cdots q_m$, άρα $p_1 | q_i$ για κάποιο i. Συνεπώς, $q_i = p_1\ell$, για κάποιο $\ell \in R$. Καθώς, το q_i είναι ανάγωγο, έπεται ότι $\ell \in U(R)$. Έχουμε, λοιπόν,

$$p_1p_2 \cdots p_n = (p_1\ell)q_1q_2 \cdots q_m$$

άρα

$$p_2 \cdots p_n = (\ell q_2) \cdots q_m$$

Χρησιμοποιώντας επαγωγή στο πλήθος $n + m$, έπεται ότι $n - 1 = m - 1$ και ότι υπάρχει $\sigma \in S_n$ με $p_{\sigma(i)} \sim q_i$ για κάθε $i \geq 3$ και $p_{\sigma(2)} \sim q_2$. □

Πρόταση 1.2.4. *Έστω R ΠΜΠ και $a, b \notin U(R) \cup \{0\}$. Τότε, υπάρχει μοναδικό ως προς συντροφικότητα στοιχείο $\delta \in R$, τέτοιο ώστε να ικανοποιούνται τα εξής ισοδύναμα:*

(i) $\delta | a$, $\delta | b$ και για κάθε $\delta_0 \in R$ τέτοιο ώστε $\delta_0 | a$ και $\delta_0 | b$, ισχύει $\delta_0 | \delta$.

(ii) $(a) \subseteq (\delta)$, $(b) \subseteq (\delta)$ και για κάθε κύριο ιδεώδες $I \subseteq R$, με $(a) \subseteq I$, $(b) \subseteq I$ ισχύει $(\delta) \subseteq I$.

Απόδειξη. Προφανώς, τα (i) και (ii) είναι ισοδύναμα. Γράφουμε

$$a = up_1^{n_1}p_2^{n_2} \cdots p_k^{n_k},\ b = vp_i^{m_1}p_2^{m_2} \cdots p_k^{m_k}$$

όπου $u, v \in U(R)$, $n_i, m_i \geq 0$ για κάθε i και p_i ανάγωγα, ανά δυο μη-συντροφικά. Αν

$$\ell_i = \min\{n_i, m_i\}, \quad \forall i = 1, 2, \ldots, k$$

τότε το

$$\delta = p_1^{\ell_1}p_2^{\ell_2} \cdots p_k^{\ell_k}$$

έχει τις ιδιότητες της πρότασης.
Έστω, τώρα, $\delta' \in R$ με την ιδιότητα (i). Τότε, $\delta' | a$, $\delta' | b$, άρα $\delta' | \delta$. Ταυτόχρονα, $\delta | a$, $\delta | b$. Έτσι $\delta | \delta'$. Τελικά, $(\delta) = (\delta')$. □

1.3 Περιοχές Κυρίων Ιδεωδών

Ορισμός 1.3.1. Μια ακέραια περιοχή R καλείται **περιοχή κυρίων ιδεωδών** (ΠΚΙ) αν κάθε ιδεώδες $I \subseteq R$ είναι κύριο.

Παραδείγματα 1.3.1. (i) Οι δακτύλιοι $\mathbb{Z}$ και $\mathbb{F}[x]$, όπου $\mathbb{F}$ σώμα είναι ΠΚΙ.

(ii) Ο δακτύλιος $\mathbb{Z}[x]$ δεν είναι ΠΚΙ. Γνωρίζουμε ότι το ιδεώδες

$$I = \{f(x) \in \mathbb{Z}[x] : f(0) \in 2\mathbb{Z}\} \subseteq \mathbb{Z}[x]$$

δεν είναι κύριο.

Πρόταση 1.3.1. *Κάθε ΠΚΙ είναι ΠΜΠ.*

Απόδειξη. θέλουμε να δείξουμε ότι αν R ΠΚΙ, τότε ικανοποιούνται οι ιδιότητες (i),(ii) του ορισμού των ΠΜΠ. Έστω $I_0, I_1, \ldots \subseteq R$ κύρια ιδεώδη με

$$I_0 \subseteq I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

Θεωρούμε το

$$I = \bigcup_{n=0}^{\infty} I_n = \{r \in R : \ r \in R_n \text{ για κάποιο } n \in \mathbb{N}\}$$

Το $I \subseteq R$ είναι ιδεώδες.

Προφανώς, $0 \in I$. Έστω $a, b \in I$ και $r \in R$. Τότε, υπάρχουν $n, m \in \mathbb{N}$ τέτοια ώστε $a \in I_n$, $b \in I_m$. Συνεπώς $ra \in I_n \subseteq I$. Υποθέτουμε ότι $n \geq m$ και παρατηρουμε ότι $I_m \subseteq I_n$, άρα $b \in I_n$. Έτσι, $a + b \in I_n \subseteq I$, άρα υπάρχει $\ell \in R$ με $I = (l)$.

Καθώς $\ell \in I$ έχουμε ότι υπάρχει $n_0 \in \mathbb{N}$ τέτοιο ώστε $\ell \in I_{n_0}$, άρα

$$I = (\ell) \subseteq I_{n_0} \subseteq I_{n_0+1} \subseteq \ldots \subseteq I$$

Συνεπώς,

$$I_{n_0} = I_{n_0+1} = \cdots$$

Θέλουμε, επίσης, να δείξουμε ότι κάθε ανάγωγο στοιχείο είναι πρώτο. Θεωρούμε $p \in R$ ανάγωγο και $a, b \in R$ με $p|ab$. Υποθέτουμε ότι $p \not| a$ και θεωρούμε το

$$I = \{px + ay : x, y \in R\} \subseteq R$$

Είναι φανερό ότι το I είναι ένα ιδεώδες του R.

Καθώς, ο R είναι ΠΚΙ υπάρχει $m \in R$ με $I = (m)$. Αφού $p \in I = (m)$, έχουμε $p = mr$ για κάποιο $r \in R$. Αν $r \in U(R)$, τότε $p \sim m$, οπότε $I = (m) = (p)$. Έτσι $a \in I = (p)$, και άρα $p|a$ -άτοπο.

Έτσι $r \in U(R)$, άρα $m \in U(R)$ και $I = (m) = R$, οπότε $1 \in I$. Τότε, υπάρχουν $x_0, y_0 \in R$ τέτοια ώστε $px_0 = ay_0 = 1$. Συνεπώς, $b = px_0b + ay_0b$, οπότε $p|b$.
Τελικά, το p είναι πρώτο. □

Παρατηρήσεις 1.3.1. (i) Υπάρχουν ΠΜΠ που δεν είναι ΠΚΙ.

(ii) Έστω R ΠΚΙ και $a, b \in R$. Τότε, θεωρούμε το ιδεώδες

$$I = \{ax + by : x, y \in R\} \subseteq R$$

και έχουμε ότι $I = (\delta)$, όπου $\delta = \text{μκδ}(a, b)$.

Πράγματι, με βάση τον ορισμό του μέγιστου κοινού διαιρέτη, αρκεί να δείξουμε ότι το I είναι το ελάχιστο ιδεώδες που περιέχει τα (a) και (b).

Προφανώς $a \in I$, άρα $(a) \subseteq I$ και $b \in I$, άρα $(b) \subseteq I$. Επιπλέον, αν $J \subseteq R$ ένα ιδεώδες με $(a) \subseteq J$, $(b) \subseteq J$, τότε $a, b \in J$. Άρα για κάθε $x, y \in R$ ισχύει $ax + by \in J$, δηλαδή $I \subseteq J$.

1.4 Ευκλείδειες Περιοχές

Ορισμός 1.4.1. Έστω R μια ακέραια περιοχή. Ο R καλείται **Ευκλείδεια Περιοχή** αν υπάρχει $\delta\colon R^* \to \mathbb{N}$ τέτοια ώστε:

(i) Αν $a, b \in R^*$ και $a|b$, τότε $\delta(a) \leq \delta(b)$.

(ii) Αν $a, b \in R$ και $b \neq 0$, τότε υπάρχουν $\pi, u \in R$ με $a = b\pi + u$ και $u = 0$ ή $\delta(u) < \delta(b)$.

Παραδείγματα 1.4.1. (i) Ο δακτύλιος $\mathbb{Z}$ είναι μια Ευκλείδεια περιοχή με

$$\delta\colon \mathbb{Z}^* \to \mathbb{N}, \qquad \delta(n) = |n|$$

(ii) Ο δακτύλιος $\mathbb{F}[x]$, όπου $\mathbb{F}$ σώμα είναι μια Ευκλείδεια περιοχή, με

$$\delta\colon \mathbb{F}[x]^* \to \mathbb{N}, \qquad \delta(f(x)) = \deg(f(x))$$

(iii) Ο δακτύλιος $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ είναι μια Ευκλείδεια περιοχή, με

$$\delta\colon \mathbb{Z}[i]^* \to \mathbb{N}, \qquad \delta(a + bi) = a^2 + b^2$$

Έστω $k, \ell \in \mathbb{Z}[i]^*$ τέτοια ώστε $k|\ell$. Τοτε, $\ell = kr$ για κάποιο $r \in \mathbb{Z}[i]$. Άρα

$$\delta(\ell) = |\ell|^2 = |kr|^2 = |k|^2|r|^2 \geq |k|^2 = \delta(k)$$

Έστω $k, \ell \in \mathbb{Z}[i]$ με $\ell \neq 0$. Θεωρούμε τον $\frac{k}{\ell} \in \mathbb{C}$ και έχουμε ότι υπάρχει $\pi \in \mathbb{Z}[i]$ τέτοιο ώστε

$$|\pi - k/\ell| \leq \sqrt{2}/2 < 1$$

Θεωρούμε τον $u = k - \ell\pi$. Τότε $k = \ell\pi + u$ και αν $u \neq 0$, ισχύει

$$\delta(u) = |k - \ell\pi|^2 = |k/\ell - \pi|^2|\ell|^2 < |\ell|^2 = \delta(\ell)$$

(iv) Το ίδιο επιχείρημα λειτουργεί και για τον $\mathbb{Z}[\sqrt{-2}]$.

(v) Το επιχείρημα, όμως, δεν λειτουργεί για τον $\mathbb{Z}[\sqrt{-5}]$.

Πρόταση 1.4.1. *Αν R είναι μια Ευκλείδεια Περιοχή, τότε ο R είναι ΠΚΙ.*

Απόδειξη. Έστω $I \subseteq R$ με $I \neq 0$. Επιλέγουμε $r \in I$ τέτοιο ώστε $r \neq 0$ και $\delta(r)$ ελάχιστο. Προφανώς, $(r) \subseteq I$.

Αντίστροφα, έστω $a \in I$. Επιλέγουμε $\pi, u \in R$ με $a = r\pi + u$ και $u = 0$ ή $\delta(u) < \delta(r)$. Όμως, $u = a = r\pi \in I$, άρα $u = 0$ και $a = r\pi \in (r)$. Έτσι, $I \subseteq (r)$. □

Παραδείγματα 1.4.2. (i) Ο δακτύλιος $\mathbb{Z}[\sqrt{-5}]$ δεν είναι Ευκλείδεια Περιοχή (μιας και δεν είναι ΠΜΠ).

(ii) Αν R μια Ευκλείδεια Περιοχή με συνάρτηση $\delta\colon R^* \to \mathbb{N}$, τότε

$$U(R) = \{r \in R^* : \delta(r) = \delta(1)\}$$

Αρχικά, παρατηρούμε ότι $\delta(1) \leq \delta(r)$ για κάθε $r \in R^*(1|r)$. Αν $r \in U(R)$, τότε υπάρχει $r^{-1} \in R$ τέτοιο ώστε $rr^{-1} = 1$, άρα $r|1$ και $\delta(r) \leq \delta(1)$. Τελικά, $\delta(r) = \delta(1)$.

Αντίστροφα, έστω $r \in R^*$ με $\delta(r) = \delta(1)$. Τότε, υπάρχουν $\pi, u \in R$ τέτοια ώστε $1 = \pi r + u$ και $u = 0$ ή $\delta(u) < \delta(1)$. Καθώς, όμως, $\delta(x) \geq \delta(1)$ για κάθε $x \in R^*$, έχουμε $u = 0$, δηλαδή $1 = \pi r$. Συνεπώς, $r \in U(R)$.

1.4.1 Παραγοντοποίηση στον $\mathbb{Z}[i]$

Από τα προηγούμενα έχουμε εντοπίσει αρκετές σημαντικές ιδιότητες του $\mathbb{Z}[i]$.
Ο $\mathbb{Z}[i]$ είναι Ευκλείδεια περιοχή, με

$$\delta\colon \mathbb{Z}[i] \to \mathbb{N}, \delta(k) = |k|^2$$

Ξέρουμε, επίσης ότι

$$U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$$

και ότι

$$\delta(k\ell) = \delta(k)\delta(\ell), \quad \forall k, \ell \in \mathbb{Z}[i]$$

Τέλος, είδαμε ότι αν $k \in \mathbb{Z}[i]^*$ και $\delta(k) = p$, όπου $p \in \mathbb{N}$ πρώτος, τότε το $k \in \mathbb{Z}[i]^*$ είναι ανάγωγο.

Παράδειγμα 1.4.1. Παραγοντοποίηση του $6 \in \mathbb{Z}[i]$

(α) $6 = 2 \cdot 3 \in \mathbb{Z}[i]$.

(β) Έχουμε $\delta(2) = 4$, άρα αν $2 = k\ell$, τότε $\delta(k)\delta(\ell) = 4$. Αν $a, b \in \mathbb{Z}$ και $\delta(a + bi) = 2$, τότε το $a + bi \in \mathbb{Z}[i]$ είναι ανάγωγο και $a^2 + b^2 = 2$.

Υπάρχουν, λοιπόν, τέσσερα στοιχεία $a + bi \in \mathbb{Z}[i]$ με $\delta(a + bi) = 2$, τα $1 + i, 1 - i, -1 + i, -1 - i$.

(γ) $2 = (1 + i)(1 - i)$.

(δ) Εργάζομαστε ανάλογα για να ελέγξουμε αν το $3 \in \mathbb{Z}[i]$ είναι ανάγωγο.

Μια μη-τετριμμένη παραγοντοποίηση του $3 = k\ell$, θα ήταν τέτοια ώστε $\delta(k) = \delta(\ell) = 3$. Όμως, η εξίσωση $a^2 + b^2 = 3$ δεν λύνεται (με $a, b \in \mathbb{Z}$), και άρα δεν υπάρχουν τέτοια k, ℓ.

Συνεπώς,το $3 \in \mathbb{Z}[i]$ είναι ανάγωγο.

Τελικά, $6 = 3 \cdot 2 = 3 \cdot (1 + i)(1 - i) \in \mathbb{Z}[i]$.

Πρόταση 1.4.2 (Ευκλείδειος Αλγόριθμος). *Αν R μια ΠΜΠ και $a, b, \pi, u \in R$ με $a = b + \pi u$, τότε οι κοινοί διαιρέτες των a, b είναι ακριβώς οι κοινοί διαιρέτες των b, u.*

Παράδειγμα 1.4.2. Υπολογισμός του δ=μκδ$(14 - 14i, 6 + 20i)$

(α) Έχουμε $14 - 14i = 2 \cdot (7 - 7i)$ και $6 + 20i = 2(3 + 10i)$, άρα $\delta = 2$ μκδ$(7 - 7i, 3 + 10i)$.
Καθώς, τώρα, $\delta(3 + 10i) = 109$ πρώτος, το $3 + 10i$ είναι ανάγωγο στο $\mathbb{Z}[i]$.
Επίσης, $3 + 10i \not| 7 - 71$, άρα $\delta = 2 \cdot 1 = 2$.

(β) δ=μκδ$(7 - 71, 3 + 10i)$ και $\delta(a) = 98$, $\delta(b) = 109$.
Έχουμε $a/b = -49/98 + 91/98i$ άρα $\pi = i$ και $u = b - ia = -4 + 3i$.

(γ) δ'=μκδ$(7 - 7i, -4 + 3i)$ και $\delta(a) = 98, \delta(u) = 25$.
Έχουμε $a/u = -49/25 + 7/25i$ άρα $\pi' = -2$ και $u' = -1 - i$.

(δ) δ"=μκδ$(-4 + 3i, -1 - i)$ και $\delta(u) = 25, \delta(u') = 2$.
Έχουμε $u/u' = 1/2 + -7/2i$ άρα $\pi'' = -3i$ και $u'' = -1 \in U(\mathbb{Z}[i])$.

(ε) Τώρα,

$$\begin{aligned} -1 &= u + 3iu' \\ &= u + 3i(a + 2u) \\ &= u + 3i(a + 2(b - ia)) \\ &= (1 + 6i)(b - ia) + 3ia \\ &= (3i - i + 6)a + (1 + 6i)b \\ &= (2i + 6)a + (1 + 6i)b \end{aligned}$$

Έτσι, $1 = (-6 - 2i)a + (-1 - 6i)b$.

Τελικά, μκδ$(14 - 14i, 6 + 20i) = 2 = (14 - 14i)(-6 - 2i) + (6 + 20i)(-1 - 6i)$.

1.5 Ασκήσεις

1.

Κεφάλαιο 2

Πρότυπα

2.1 Βασικές Έννοιες

Ορισμός 2.1.1. Έστω R δακτύλιος με μονάδα και $(M,+)$ μια αβελιανή ομάδα. Θα λέμε, ότι το M είναι ένα **R-πρότυπο** αν υπάρχει απεικόνιση (εξωτερικός πολλαπλασιασμός) $R \times M \to M$, για την οποία ισχύουν τα εξής:

(i) $r(m+m') = rm + rm'$ για κάθε $r \in R$, $m, m' \in M$.

(ii) $(r+r')m = rm + r'm$ για κάθε $r, r' \in R$, $m \in M$.

(iii) $(rr')m = r(r'm)$ για κάθε $r, r' \in R$, $m \in M$.

(iv) $1_R m = m$ για κάθε $m \in M$.

Πρόταση 2.1.1 (Βασικές ιδιότητες R-προτύπων M). *(i)* $0_R m = 0_m$ *για κάθε* $m \in M$.

(ii) $r0_M = 0_M$ *για κάθε* $r \in R$.

(iii) $(-r)m = -rm$ *για κάθε* $r \in R$, $m \in M$.

(iv) $r(-m) = -rm$ *για κάθε* $r \in R$, $m \in M$.

Παραδείγματα 2.1.1. (i) Αν $\mathbb{F}$ σώμα, τότε ένα $\mathbb{F}$-πρότυπο είναι ακριβώς ένας $\mathbb{F}$-διανυσματικός χώρος.

(ii) Ένα $\mathbb{Z}$-πρότυπο είναι ακριβώς μια αβελιανή ομάδα.

Προφανώς, ένα $\mathbb{Z}$-πρότυπο είναι μιά αβελιανή ομάδα. Αντίστροφα, έστω $(M,+)$ μια αβελιανή ομάδα. Μπορούμε να ορίσουμε με μοναδικό τρόπο τη δομή ενός $\mathbb{Z}$-πρότυπου στην M με εξωτερικό πολλαπλασιασμό: $\mathbb{Z} \times M \to M$, με

$$(n,x) \mapsto \begin{cases} x + x + \cdots + x, & n > 0 \\ 0, & x = 0 \\ -[(-n)x], & n < 0 \end{cases}$$

Είναι εύκολο να δειχθεί ότι ισχύουν οι απαιτήσεις του ορισμού ενός $\mathbb{Z}$-πρότυπου.

(iii) Έστω $\mathbb{F}$ σώμα και V ένας $\mathbb{F}$-διανυσματικός χώρος. Θεωρούμε, επίσης, μια $\mathbb{F}$-γραμμική απεικόνιση $\phi\colon V \to V$. Μπορούμε να θεωρήσουμε τον δακτύλιο $R = \mathbb{F}[x]$ και να ορίσουμε στην αβελιανή ομάδα $(V, +)$ την δομή ενός $\mathbb{F}[x]$ προτύπου με εξωτερικό πολλαπλασιασμό

$$\mathbb{F}[x] \times V \to V, \quad (f(x), u) \mapsto f(x)u$$

που ορίζεται ως εξής:

Αν

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$$

και $u \in V$, τότε

$$f(x)u = a_0 u + a_1 \phi(u) + \cdots + a_n \phi^n(u)$$

Είναι εύκολο να δειχθεί ότι το V με τον πολλαπλασιασμό αυτό ορίζει ένα $\mathbb{F}[x]$-πρότυπο. Το παραπάνω $\mathbb{F}[x]$-πρότυπο συμβολίζεται με V_ϕ).

Έστω

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{j=0}^{m} g_j x^j$$

και $u \in V$. Τότε

$$\begin{aligned}
[f(x)g(x)]u &= \left[\sum_{k=0}^{n+m} \left(\sum_{i=+j=k} a_i b_i\right) x^k\right] u \\
&= \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j\right) \phi^k(u) \\
&= \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j \phi^i(u)[\phi^j(u)] \\
&= \sum_{i=0}^{n} a_i \phi^i \left[\sum_{j=0}^{m} b_j \phi^j(u)\right] \\
&= \sum_{i=0}^{n} a_i \phi^i(u)[g(x)u] = f(x)[g(x)u]
\end{aligned}$$

(iv) Έστω R δακτύλιος και $M_1, M_2, \ldots, M_n$ R-πρότυπα. Θεωρούμε το καρτεσιανό γινόμενο

$$M = M_1 \times M_2 \times \cdots \times M_n$$

και ορίζουμε σε αυτό τη δομή ενός R-προτύπου με

$$(m_1, m_2, \ldots, m_n) + (m_1', m_2', \ldots, m_n') = (m_1 + m_1', m_2 + m_2', \ldots, m_n + m_n')$$

και

$$r(m_1, m_2, \ldots, m_n) = (rm_1, rm_2, \ldots, rm_n)$$

Είναι εύκολο να δειχθεί ότι το M είναι ένα R-πρότυπο. Το M καλείται **ευθύ άθροισμα** των $M_1, M_2, \ldots, M_n$ και συμβολίζεται

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

(v) Έστω R μεταθετικός δακτύλιος και $I \subseteq R$ ένα ιδεώδες του. Μπορούμε να ορίσουμε στην αβελιανή ομάδα $(I, +)$ την δομή ενός R-προτύπου με εξωτερικό πολλαπλασιασμό

$$R \times I \to I, \qquad (r, x) \mapsto rx$$

το γινόμενο στον R.

Οι ιδιότητες (i)-(iv) στον ορισμό του R-προτύπου είναι άμεσες συνέπειες των ιδιοτήτων του πολλαπλασιασμού στον R.

(vi) Έστω $\phi\colon S \to R$ ένας ομομορφισμός δακτυλίων και M ένα R-πρότυπο. Μπορούμε να ορίσουμε στην αβελιανή ομάδα $(M, +)$ τη δομή ενός S-προτύπου θέτοντας:

$$s \cdot x = \phi(s)x, \quad \forall s \in S, x \in M$$

Έστω $s, s' \in S$, $x, x' \in M$. Υπολογίζουμε:

$$\begin{aligned} s \cdot (x + x') &= \phi(s)(x + x') \\ &= \phi(s)x + \phi(s)x' \\ &= s \cdot x + s \cdot x' \end{aligned}$$

$$\begin{aligned} (s + s') \cdot x &= \phi(s + s')x \\ &= [\phi(s) + \phi(s')]x \\ &= \phi(s)x + \phi(s')x \\ &= s \cdot x + s' \cdot x \end{aligned}$$

$$\begin{aligned} (ss') \cdot x &= \phi(ss')x \\ &= [\phi(s)\phi(s')]x \\ &= \phi(s)[\phi(s')x] \\ &= s \cdot [s' \cdot x] \end{aligned}$$

Τέλος,

$$1_S \cdot x = \phi(1)x = 1_R x = x$$

2.1.1 Ο Δακτύλιος Ενδομορφισμών $\mathrm{End}(M, +)$

Έστω M μια αβελιανή ομάδα και

$$\mathrm{End}(M, +) = \{f\colon M \to M \mid f \text{ προσθετική}\}$$

Μπορούμε να ορίσουμε στο σύνολο $\mathrm{End}(M, +)$ τη δομή ενός δακτυλίου, ως εξής:
Αν $f, g \in \mathrm{End}(M, +)$ ορίζουμε

$$f + g\colon M \to M \qquad (f + g)(x) = f(x) + g(x), \quad \forall x \in M$$

$$f \cdot g\colon M \to M \qquad (f \cdot g) = f[g(x)], \quad \forall x \in M$$

και

$$1\colon M \to M \qquad 1(x) = x, \quad \forall x \in M$$

Η πρόσθεση και ο πολλαπλασιασμός είναι καλά ορισμένες πράξεις. Γνωρίζουμε ότι η σύνθεση προσθετικών συναρτήσεων είναι μια προσθετική συνάρτηση. Για το άθροισμα, θεωρούμε, $f, g \in \mathrm{End}(M,+)$ και έχουμε ότι για κάθε $x, y \in M$

$$\begin{aligned}(f+g)(x+y) &= f(x+y)+g(x+y)\\ &= f(x)+f(y)+g(x)+g(y)\\ &= (f+g)(x)+(f+g)(y)\end{aligned}$$

Άρα $f+g \in \mathrm{End}(M,+)$.

Οι ιδιότητες του δακτυλίου επαληθεύονται άμεσα. Ο δακτύλιος $\mathrm{End}(M,+)$ καλείται ο **δακτύλιος των ενδομορφισμών** της αβελιανής ομάδας $(M,+)$.

Η αβελιανή ομάδα $(M,+)$ είναι ένα $\mathrm{End}(M,+)$-πρότυπο με

$$\mathrm{End} \times M \to M, \qquad (f,x) \mapsto f(x)$$

Έστω $f, g \in \mathrm{End}(M,+)$, $x, y \in M$. Τότε

$$(f+g)\cdot x = f\cdot x + g\cdot x = f(x)+g(x)$$

$$f\cdot(x+y) = f\cdot x + f\cdot y = f(x)+f(y)$$

και

$$1\cdot x = x$$

Παρατηρήσεις 2.1.1. (i) Έστω αβελιανή ομάδα $(M,+)$ και $E = \mathrm{End}(M,+)$, ο δακτύλιος των ενδομορφισμών της. Έστω δακτύλιος R και ένας ομομορφισμός δακτυλίων $\ell\colon R \to E$. Τότε ο ομομορφισμός ℓ μπορεί να ορίσει, ξεκινώντας από το E-πρότυπο που ορίσαμε, τη δομή ενός R-προτύπου στο M θέτοντας $rx = \ell(r)(x)$ για κάθε $r \in R$, $x \in M$.

(ii) Έστω R δακτύλιος και M ένα R-πρότυπο. Τότε, ορίζουμε την απεικόνιση $\ell\colon R \to \mathrm{End}(M,+)$, με $\ell(r)\colon M \to M$ να είναι η απεικόνιση με $\ell(r)(x) = rx$ για κάθε $r \in R$, $x \in M$.

- Η ℓ είναι καλά ορισμένη.
  Αν $r \in R$, $x, y \in M$, τότε

$$\begin{aligned}\ell(r)(x+y) &= r(x+y)\\ &= rx+ry\\ &= \ell(r)(x)+\ell(r)(y)\end{aligned}$$

- Η ℓ είναι προσθετική.
  Έστω $r, r' \in R$.Θεωρούμε $x \in M$, οπότε

$$\begin{aligned}\ell(r+r')(x) &= (r+r')x\\ &= rx+r'x\\ &= \ell(r)(x)+\ell(r')(x)\end{aligned}$$

– Η l είναι πολλαπλασιαστική.
Αν $r, r' \in R$, τότε

$$\begin{aligned}\ell(rr')(x) &= (rr')x \\ &= r(r'x) - \ell(r)[\ell(r')(x)] \\ &= \ell(r)\ell(r')(x) = [\ell(r)\ell(r')]x, \quad \forall x \in M\end{aligned}$$

– Έστω $x \in M$. Τότε $\ell(1_R)(x) = 1_R x = x = 1_{\mathrm{End}}(x)$

2.2 Υποπρότυπα

Ορισμός 2.2.1. Έστω M ένα R-πρότυπο. Ένα $N \subseteq M$ καλείται **R-υποπρότυπο** αν:

(i) $0 \in N$.

(ii) Αν $x, y \in N$, τότε $x \pm y \in N$.

(iii) Αν $r \in R, x \in N$, τότε $rx \in N$.

Παρατήρηση 2.2.1. Έστω υποπρότυπο N ενός R-προτύπου M. Τότε το N είναι ένα R-πρότυπο με τους περιορισμούς των πράξεων.

Παραδείγματα 2.2.1. (i) Έστω $\mathbb{F}$ σώμα και V ένα $\mathbb{F}$-πρότυπο, δηλαδή ένας $\mathbb{F}$-διανυσματικός χώρος. Τότε, τα $\mathbb{F}$-υποπρότυπα του V είναι ακριβώς οι διανυσματικοί του υπόχωροι.

(ii) Έστω M ένα $\mathbb{Z}$-πρότυπο, δηλαδή μια αβελιανή ομάδα. Τότε, τα $\mathbb{Z}$-υποπρότυπα $N \subseteq M$ είναι ακριβώς οι υποομάδες του M.

Προφανώς, ένα $\mathbb{Z}$-υποπρότυπο είναι υποομάδα της M.
Αν $N \subseteq M$ υποομάδα, τότε το N είναι ένα $\mathbb{Z}$-υποπρότυπο, μιας και για κάθε $n \in \mathbb{Z}$, $x \in N$ ισχύει $nx \in N$.

(iii) Έστω $\mathbb{F}$ σώμα, V ένας $\mathbb{F}$-διανυσματικός χώρος και $\phi\colon V \to V$ μια $\mathbb{F}$-γραμμική απεικόνιση. Θεωρούμε το επαγόμενο $\mathbb{F}[x]$-πρότυπο $V = V_\phi$. Τότε, ένα $\mathbb{F}[x]$-υποπρότυπο $U \subseteq V$ είναι ακριβώς ένας $\mathbb{F}$-διανυσματικός υπόχωρος τέτοιος ώστε $\phi(U) \subseteq U$, δηλαδή ϕ-αναλλοίωτος.

Προφανώς, ένα $\mathbb{F}[x]$-υποπρότυπο $U \subseteq V$ είναι ένας διανυσματικός υπόχωρος. Επιπλέον, αν $u \in U$, τότε $\phi(u) = xu$.
Έστω $U \subseteq V$ ένας ϕ-αναλλοίωτος υπόχωρος. Τότε, για κάθε $u \in U$ ισχύει $\phi(u) \in U$, άρα $\phi(\phi(u)) = \phi^2(u) \in U$ κτλπ. Έστω $f(x) \in \mathbb{F}$, $u \in U$. Γράφουμε

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

και έχουμε

$$f(x)u = a_0 u + a_1 \phi(u) + \cdots a_n \phi^n(u) \in U$$

άρα το U είναι ένα $\mathbb{F}[x]$-υποπρότυπο.

(iv) Έστω R μεταθετικός δακτύλιος. Θεωρώντας το R ως ένα R-πρότυπο, παρατηρούμε ότι τα R-υποπρότυπα του R είναι ακριβώς τα ιδεώδη $I \subseteq R$.

(v) Έστω R ακέραια περιοχή και M ένα R-πρότυπο. Θεωρούμε το $N \subseteq M$ που ορίζεται ως εξής

$$N := \{m \in M \mid \exists r \in R^* : rm = 0 \in M\}$$

Τότε, το N είναι ένα R-υποπρότυπο του M, που ονομάζεται **υποπρότυπο στρέψεως** του M και συμβολίζεται με $N = M_t$.

- $0 \in N$
- Αν $x, y \in N$, τότε υπάρχουν $r, r' \in R^*$ με $rx = 0, r'y = 0$. θεωρούμε το $rr' \in R^*$ και παρατηρούμε ότι

$$\begin{aligned}(rr')(x \pm y) &= rr'x \pm rr'y \\ &= r'(rx) \pm r(r'y) \\ &= r'0 + r0 = 0\end{aligned}$$

  Συνεπώς, $x \pm y \in N$.
- Αν $x \in N, r \in R$, τότε υπάρχει $r_x \in R^*$ τέτοιο ώστε $r_x r = 0$. Τότε,

$$\begin{aligned}r_x(rx) = (r_x r)x &= (rr_x)x \\ &= r(r_x x) = r0 = 0\end{aligned}$$

  Έτσι, $rx \in N$.

2.3 Πρότυπα Στρέψεως

Ορισμός 2.3.1. Έστω R ακέραια περιοχή και M ένα R-πρότυπο.

(i) Το M καλείται **ελεύθερο στρέψεως** αν $M_t = 0$.

(ii) Το M καλείται **πρότυπο στρέψεως** αν $M_t = M$.

Παραδείγματα 2.3.1. (i) Αν $\mathbb{F}$ σώμα, τότε κάθε $\mathbb{F}$-πρότυπο ($\mathbb{F}$-δ.χ.) είναι ελεύθερο στρέψεως.

(ii) Αν M ένα $\mathbb{Z}$-πρότυπο, τότε το υποπρότυπο στρέψεως M_t περιέχει ακριβώς τα $x \in M$ για τα οποία $o(x) < \infty$.

(iii) Έστω $\mathbb{F}$ σώμα, V ένας $\mathbb{F}$-διανυσματικός χώρος με $\dim_{\mathbb{F}} V < \infty$ και $\phi \colon V \to V$ μια $\mathbb{F}$-γραμμική απεικόνιση.

Τότε το $\mathbb{F}[x]$-πρότυπο $V = V_\phi$ είναι ένα πρότυπο στρέψεως, και μάλιστα υπάρχει $f(x) \in \mathbb{F}[x]$ με $f(x) \neq 0$ τέτοιο ώστε $f(x)u = f(\phi)(u) = 0 \in V$ για κάθε $u \in V$.

Πράγματι, αν $f(x) \in \mathbb{F}[x]$ το χαρακτηριστικό πολυώνυμο της ϕ, τότε

$$f(\phi) = 0 : V \to V$$

από το Θεώρημα Cayley-Hamilton, και άρα

$$f(x)u = f(\phi)(u) = 0 \in V, \quad \forall u \in V$$

(iv) Το $\mathbb{Z}$-πρότυπο $\mathbb{Q}$ είναι ελεύθερο στρέψεως.

Αν $q \in \mathbb{Q}$, $n \in \mathbb{Z}^*$, τότε $nq = 0$, άρα $q = 0$.

(v) Θεωρούμε την ομάδα $(\mathbb{Q}, +)$, την υποομάδα $(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +)$ και ορίζουμε μια σχέση ισοδυναμίας στο $\mathbb{Q}$ ως εξής:
Αν $q_1, q_2 \in \mathbb{Q}$ λέμε ότι

$$q_1 \equiv q_2 \pmod{\mathbb{Z}} \Leftrightarrow q_2 - q_1 \in \mathbb{Z}$$

Η σχέση αυτή είναι μιά σχέση ισοδυναμίας.

Η κλάση ισοδυναμίας $[q]$ του $q \in \mathbb{Q}$ είναι το

$$q + \mathbb{Z} = \{q + n : n \in \mathbb{Z}\}$$

Στο σύνολο-πηλίκο

$$\mathbb{Q}/\mathbb{Z} = \{q + \mathbb{Z} : q \in \mathbb{Q}\}$$

ορίζουμε τη δομή μιας αβελιανής ομάδας θέτοντας

$$(q + \mathbb{Z}) + (q' + \mathbb{Z}) = (q + q') + \mathbb{Z}$$

Η ομάδα-πηλίκο $\mathbb{Q}/\mathbb{Z}$ είναι ομάδα στρέψεως.

Πράγματι, αν $k \in \mathbb{Q}/\mathbb{Z}$, τότε $k = q + \mathbb{Z}$, για κάποιο $q \in \mathbb{Q}$. Υπάρχει ένα $n \in \mathbb{Z}^*$ τέτοιο ώστε $nq \in \mathbb{Z}$. Τότε, είναι

$$nk = n(q + \mathbb{Z}) = nq + \mathbb{Z} = 0 + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$$

Παρατηρούμε ότι για κάθε $n \in \mathbb{Z}^*$, $\ell \in \mathbb{Q}/\mathbb{Z}$ ισχύει $n\ell \neq 0 + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$.

(vi) Έστω R ακέραια περιοχή και R-πρότυπα M_1, $M_2, \ldots, M_n$. Αν

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

τότε

$$M_t = M_{1,t} \oplus M_{2,t} \oplus \cdots \oplus M_{n,t}$$

Ειδικότερα για το $\mathbb{Z}$-πρότυπο

$$A = \mathbb{Q} \oplus \mathbb{Q}/\mathbb{Z}$$

είναι

$$A_t = \mathbb{Q}_t \oplus (\mathbb{Q}/\mathbb{Z})_t = 0 \oplus \mathbb{Q}/\mathbb{Z}$$

Έστω $(m_1, m_2, \ldots, m_n) \in M$. Τότε,

$$\begin{aligned}
(m_1, m_2, \ldots, m_n) \in M_t &\Leftrightarrow \exists r \in R^* : (rm_1, rm_2, \ldots, rm_n) = 0 \\
&\Leftrightarrow \exists r \in R^* : r(m_1, m_2, \ldots, m_n) = 0 \\
&\Leftrightarrow \exists r \in R^* : rm_1 = 0 \in M_1, \ldots, rm_n = 0 \in M_n \\
&\Leftrightarrow m_1 \in M_{1,t}, \ldots, m_n \in M_{n,t} \\
&\Leftrightarrow (m_1, m_2, \ldots, m_n) \in M_{1,t} \oplus M_{2,t} \oplus \cdots \oplus M_{n,t}
\end{aligned}$$

(vii) Έστω R ακέραια περιοχή και $I \subseteq R$ ένα ιδεώδες. Θεωρούμε τον δακτύλιο-πηλίκο R/I ως R/I-πρότυπο. Με περιορισμό των βαθμωτών μέσω του ομομορφισμού-πηλίκο $R \to R/I$ μπορούμε να θεωρήσουμε το R/I ως R-πρότυπο. Αν το R-πρότυπο R/I είναι ελεύθερο στρέψεως, τότε $I = 0$ ή $I = R$.

Έστω ότι $I \neq 0$. Επιλέγουμε $r \in I^*$. Τότε,

$$\begin{aligned} r(1+I) &= (r+I)(1+I) \\ &= r1 + I \\ &= r + I = 0 + I \end{aligned}$$

άρα το $1 + I \in R/I$ είναι σημείο στρέψεως.

Όμως, το R/I είναι ελεύθερο στρέψεως και άρα $1 + I = 0 + I \in R/I$, οπότε $1 \in I$ και $I = R$.

Πρόταση 2.3.1. *Έστω R δακτύλιος, M ένα R-πρότυπο και $x_1, x_2, \ldots, x_n \in M$. Τότε, το $N \subseteq M$, με*

$$N = \{x \in M \mid \exists r_1, r_2, \ldots, r_n \in R : x = r_1x_1 + r_2x_2 + \cdots + r_nx_n\}$$

είναι το ελάχιστο υποπρότυπο M που περιέχει τα $x_1, x_2, \ldots, x_n$.

Το N συμβολίζεται με

$$\langle x_1, x_2, \ldots, x_n \rangle$$

και καλείται το υποπρότυπο του M που παράγεται από τα $x_1, x_2, \ldots, x_n$.

Απόδειξη. Το N είναι υποπρότυπο του M και μάλιστα $x_1, x_2, \ldots, x_n \in N$.

Έστω $L \subseteq M$ και $x_1, x_2, \ldots, x_n \in L$. Για να δείξουμε ότι $N \subseteq L$ θεωρούμε $x \in N$. Τότε,

$$\exists\, r_1, r_2, \ldots, r_n \in R\colon x = r_1x_1 + r_2x_2 + \cdots + r_nx_n$$

Καθώς $x_1, x_2, \ldots, x_n \in L$ και το L είναι R-υποπρότυπο του M, προκύπτει ότι $x \in L$. □

Ορισμός 2.3.2. Έστω M ένα R-πρότυπο.

(i) Λέμε ότι το M είναι **πεπερασμένα παραγόμενο** αν υπάρχουν $n \in \mathbb{N}$ και $x_1, x_2, \ldots, x_n \in M$, με

$$M = \langle x_1, x_2, \ldots, x_n \rangle$$

(ii) Λέμε ότι το M είναι **κυκλικό** αν υπάρχει $x \in M$ τέτοιο ώστε $M = \langle x \rangle$.

Παραδείγματα 2.3.2. (i) Έστω $\mathbb{F}$ ένα σώμα και V ένα $\mathbb{F}$-πρότυπο. Τότε, το V είναι πεπερασμένα παραγόμενο $\mathbb{F}$-πρότυπο ανν $\dim_{\mathbb{F}} V < \infty$. Επίσης, το V είναι κυκλικό πρότυπο ανν $\dim_{\mathbb{F}} V = 0$ ή 1.

(ii) Ένα $\mathbb{Z}$-πρότυπο M είναι κυκλικό ανν η αβελιανή ομάδα M είναι κυκλική.

(iii) Το $\mathbb{Z}$-πρότυπο $\mathbb{Q}$ δεν είναι πεπερασμένα παραγόμενο.

Πράγματι, έστω $n \in \mathbb{N}$, $q_1, q_2, \ldots, q_n \in \mathbb{Q}$. Μπορούμε να γράψουμε $q_i = \frac{a_i}{b}$, για κάποια $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, $b \in \mathbb{Z}^*$. Εαν $p \in \mathbb{Z}$ πρώτος και $p \nmid b$, τότε

$$\frac{1}{p} \notin \langle q_1, q_2, \ldots, q_n \rangle$$

Πράγματι, αν $k_1, k_2, \ldots, k_n \in \mathbb{Z}$, με

$$\frac{1}{p} = k_1q_1 + k_2q_2 + \cdots + k_nq_n$$

τότε

$$\frac{1}{p} = \frac{k_1a_1 + k_2a_2 + \cdots + k_na_n}{b} \in \mathbb{Q}$$

άρα

$$b = p(k_1a_1 + k_2a_2 + \cdots + k_na_n) \in \mathbb{Z}$$

και τελικά $p|b$ -άτοπο.

2.4 Πρότυπα-Πηλίκο

Θεωρούμε ένα R-πρότυπο M και ένα R-υποπρότυπο $N \subseteq M$. Θεωρούμε, επίσης, την αβελιανή ομάδα-πηλίκο $(M/N, +)$.

Τα στοιχεία της είναι σύμπλοκα της μορφής $m + N$, $m \in M$ και ισχύει

$$m + N = m' + N \in M/N \Leftrightarrow m' - m \in N$$

Η πράξη της πρόσθεσης είναι $(m_1 + N) + (m_2 + N) = (m_1 + m_2 + N) \in M/N$.

Το ουδέτερο στοιχείο της αβελιανής ομάδας M/N είναι το $0 + N$ και

$$-(m + N) = (-m) + N, \quad \forall m + N \in M/N$$

Μπορούμε να ορίσουμε στην αβελιανή ομάδα $(M/N, +)$ τη δομή ενός R-προτύπου με εξωτερικό πολλαπλασιασμό

$$R \times M/N \to M/N$$

$$(r, m + N) \mapsto r \cdot (m + N) := rm + N$$

Αυτός ο εξωτερικός πολλαπλασιασμός είναι καλά ορισμένος.

Έστω $r \in R, m, m' \in M$, με $m+N = m'+N \in M/N$. Τότε, $m'-m \in N$, άρα $r(m'-m) \in N$, $rm' - rm \in N$ οπότε $rm + N = rm' + N \in M/N$.

Επιπλέον, ισχύουν οι τέσσερις ιδιότητες του ορισμού των R-προτύπων.

Παραδείγματα 2.4.1. (i) Έστω M ένα πεπερασμένα παραγόμενο R-πρότυπο και $N \subseteq M$ ένα υποπρότυπο. Τότε, το R-πρότυπο M/N είναι πεπερασμένα παραγόμενο.

Πράγματι, έστω ότι $M = \langle m_1, m_2, \ldots, m_n\rangle$, για κάποια $m_1, m_2, \ldots, m_n \in M$, $n \in \mathbb{N}$. Θα δείξουμε ότι

$$M/N = \langle m_1 + N, m_2 + N, \ldots, m_n + N\rangle$$

Αν $k \in M/N$, τότε $k = m+N$, για κάποιο $m \in M$. Καθώς, τώρα, $M = \langle m_1, m_2, \ldots, m_n\rangle$, υπάρχουν $r_1, r_2, \ldots, r_n$ τέτοια ώστε $m = r_1m_1 + r_2m_2 + \cdots + r_nm_n$.

Συνεπώς,

$$\begin{aligned} k &= m + N \\ &= (r_1m_1 + r_2m_2 + \cdots + r_nm_n) + N \\ &= (r_1m_1 + N) + (r_2m_2 + N) + \cdots + (r_nm_n + N) \\ &= r_1(m_1 + N) + r_2(m_2 + N) + \cdots + r_n(m_n + N) \in \langle m_1, m_2, \ldots, m_n\rangle \end{aligned}$$

(ii) Αν το M είναι κυκλικό, τότε το M/N είναι επίσης κυκλικό.

(iii) Έστω R μια ακέραια περιοχή, M ένα R-πρότυπο και $N = M_t$ το υποπρότυπο στρέψεως. Τότε, το R-πρότυπο M/N είναι ελεύθερο στρέψεως, δηλαδή $(M/M_t)_t = 0$.

Έστω $k \in M/N$ για το οποίο υπάρχει $r \in R^*$ με $rk = 0 + N \in M/N$. Μπορούμε να γράψουμε $k = m + N$, για κάποιο $m \in M$.

Τότε,

$$rm + N = r(m + N) = rk = 0 + N \in M/N$$

άρα $rm \in N$.

Αφού $N = M_t$, υπάρχει $r' \in R^*$ με $r'(rm) \in M$. Τότε, όμως, καθώς $rr' \neq 0$, έχουμε ότι $m \in M$, άρα $m + N = 0 + N \in M/N$.

Τελικά, $k = 0 + N \in M/N$.

2.5 Ομομορφισμοί Προτύπων

Ορισμός 2.5.1. Έστω R δακτύλιος και M, N δύο R-πρότυπα. Μιά απεικόνιση $f\colon M \to N$ καλείται **ομομορφισμός** R-προτύπων (ή R-γραμμική απεικόνιση) αν:

(i) $f(m + m') = f(m) + f(m')$ για κάθε $m, m' \in N$.

(ii) $f(rm) = rf(m)$ για κάθε $r \in R$, $m \in M$.

Παραδείγματα 2.5.1. (i) Έστω $\mathbb{F}$ σώμα και U, V δύο $\mathbb{F}$-πρότυπα. Τότε οι ομομορφισμοί $\mathbb{F}$-προτύπων $f\colon U \to V$ είναι ακριβώς οι $\mathbb{F}$-γραμμικές απεικονίσεις.

(ii) Έστω M, N δύο $\mathbb{Z}$-πρότυπα, δηλαδή δύο αβελιανές ομάδες. Τότε, οι ομομορφισμοί $\mathbb{Z}$-προτύπων $f\colon M \to N$ είναι ακριβώς οι προσθετικές απεικονίσεις $f\colon M \to N$.

Προφανώς, ένας ομομορφισμός $\mathbb{Z}$-προτύπων είναι μιά προσθετική συνάρτηση.

Αντίστροφα, έστω $f\colon M \to N$. Τότε, για κάθε $n \in \mathbb{Z}$, $x \in M$ έχουμε $f(nx) = nf(x)$.

- Αν $n > 0$, τότε $f(nx) = f(x + x + \cdots + x) = f(x) + \cdots + f(x) = nf(x)$.
- Αν $n = 0$, τότε $f(0x) = f(0) = 0 = 0f(x)$.
- Αν $n < 0$, τότε $-n > 0$ και $f[(-n)x] = (-n)f(x)$, άρα $f(nx) = nf(x)$.

Άρα η f είναι $\mathbb{Z}$-γραμμική απεικόνιση.

(iii) Έστω $\mathbb{F}$ σώμα, U, V δύο $\mathbb{F}$-διανυσματικοί χώροι και $\phi\colon U \to U$, $\psi\colon V \to V$ δύο $\mathbb{F}$-γραμμικές απεικονίσεις. Μπορούμε να θεωρήσουμε τα $\mathbb{F}[x]$-πρότυπα $U = U_\phi, V = V_\psi$. Τότε, μια απεικόνιση $\lambda\colon U \to V$ είναι $\mathbb{F}[x]$-γραμμική ανν

(α) Η λ είναι $\mathbb{F}$-γραμμική.

(β) $\lambda \circ \phi = \psi \circ \lambda$.

$$\begin{array}{ccc} U & \xrightarrow{\phi} & U \\ \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \lambda} \\ V & \xrightarrow{\psi} & V \end{array}$$

($\Rightarrow$) Έστω ότι λ είναι $\mathbb{F}[x]$-γραμμική. Τότε η λ είναι προσθετική και

$$\lambda[f(x)u] = f(x)\lambda(u), \quad \forall f(x) \in \mathbb{F}[x], u \in U$$

Ειδικότερα,

$$\lambda(au) = a\lambda(u), \quad \forall a \in \mathbb{F}, u \in U$$

συνεπώς η λ είναι $\mathbb{F}$-γραμμική.

Για να δείξουμε ότι $\lambda \circ \phi = \psi \circ \lambda$ θεωρούμε $u \in U$ και έχουμε

$$\begin{aligned}(\lambda \circ \phi)(u) &= \lambda[(\phi(u)] = \lambda(xu) \\ &= x\lambda(u) = \psi[\lambda(u)] \\ &= (\psi \circ \lambda)(u)\end{aligned}$$

($\Leftarrow$) Έστω μια $\mathbb{F}$-γραμμική απεικόνιση $\lambda \colon U \to V$ με $\lambda \circ \phi = \psi \circ \lambda$.

Παρατηρούμε ότι $\lambda \circ \phi^n = \psi^n \circ \lambda$ για κάθε $n \in \mathbb{N}$.

$$\begin{array}{ccccccccc} U & \xrightarrow{\phi} & U & \xrightarrow{\phi} & \ldots & \xrightarrow{\phi} & U & \xrightarrow{\phi} & U \\ \downarrow{\scriptstyle\lambda} & & \downarrow{\scriptstyle\lambda} & & & & \downarrow{\scriptstyle\lambda} & & \downarrow{\scriptstyle\lambda} \\ V & \xrightarrow{\psi} & V & \xrightarrow{\psi} & \ldots & \xrightarrow{\psi} & V & \xrightarrow{\psi} & V \end{array}$$

Αν $\lambda \circ \phi^n = \psi^n \circ \lambda$, τότε

$$\begin{aligned}\lambda \circ \phi^{n+1} &= \lambda \circ (\phi^n \circ \phi) = (\lambda \circ \phi^n) \circ \phi \\ &= (\psi^n \circ \lambda) \circ \phi = \psi^n \circ (\lambda \circ \phi) \\ &= \psi^n \circ (\psi \circ \lambda) = (\psi^n \circ \psi) \circ \lambda \\ &= \psi^{n+1} \circ \lambda\end{aligned}$$

Έστω $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x], u \in U$. Τότε

$$\begin{aligned}\lambda[f(x)u] &= \lambda[a_0 u + a_1\phi(u) + \cdots + a_n\phi^n(u)] \\ &= a_0\lambda(u) + a_1\lambda[\phi(u)] + \cdots + a_n\lambda[\phi^n(u)] \\ &= a_0\lambda(u) + a_1(\lambda \circ \phi)(u) + \cdots + a_n(\lambda \circ \phi^n)(u) \\ &= a_0\lambda(u) + a_1(\psi \circ \lambda)(u) + \cdots + a_n(\psi^n \circ \lambda)(u) \\ &= a_0\lambda(u) + a_1\psi[\lambda(u)] + \cdots + a_n\psi^n[\lambda(u)] = f(x)\lambda(u)\end{aligned}$$

(iv) Έστω M ένα R-πρότυπο και $N \subseteq M$ ένα R-υποπρότυπο. Τότε, οι απεικονίσεις

$$i \colon N \to M, \qquad i(n) = n, \quad \forall n \in N$$

και

$$p \colon M \to M/N, \qquad p(m) = m + N, \quad \forall m \in M$$

είναι ομομορφισμοί R-προτύπων.

Παρατηρήσεις 2.5.1. (i) Για κάθε R-πρότυπο M η ταυτοτική απεικόνιση $I_M \colon M \to M$ είναι ομομορφισμός R-προτύπων.

Πράγματι, αν $x, y \in M$, $r \in R$, τότε

$$I_M(x + y) = x + y = I_M(x) + I_M(y)$$

και

$$I_M(rx) = rx = rI_M(x)$$

(ii) Αν $f\colon M \to N$, $g\colon N \to L$ ομομορφισμοί R-προτύπων, τότε και η σύνθεση $g \circ f\colon M \to L$ είναι ομομορφισμός R-προτύπων.

Αν $x, y \in M$, $r \in R$, τότε

$$\begin{aligned}(g \circ f)(x+y) &= g[f(x+y)] \\ &= g[f(x)+f(y)] \\ &= g[f(x)] + g[f(y)] \\ &= (g \circ f)(x) + (g \circ f)(y)\end{aligned}$$

και

$$\begin{aligned}(g \circ f)(rx) &= g[f(rx)] \\ &= g[rf(x)] \\ &= rg[f(x)] \\ &= r(g \circ f)(x)\end{aligned}$$

Πρόταση 2.5.1. *Έστω $f\colon M \to N$ ένας ομομορφισμός R-προτύπων. Τότε:*

(i) Για κάθε R-υποπρότυπο $M_0 \subseteq M$ η εικόνα $f(M_0)$ είναι ένα R-υποπρότυπο του N.

(ii) Ειδικότερα, η ***εικόνα*** $\operatorname{im} f = f(M) \subseteq N$ *είναι ένα R-υποπρότυπο και μάλιστα $\operatorname{im} f = N$ ανν η f είναι επί.*

(iii) Για κάθε $N_0 \subseteq N$ υποπρότυπο η αντίστροφη εικόνα $f^{-1}(N_0)$ είναι ένα R-υποπρότυπο του .

(iv) Ειδικότερα, ο ***πυρήνας*** $\ker f = f^{-1}(0) \subseteq M$ *είναι ένα R-υποπρότυπο και μάλιστα $\ker f = 0$ ανν η f είναι 1-1.*

Απόδειξη. (i) Καθώς $0 \in M_0$ έχουμε $0 = f(0) \in f(M_0)$, άρα $f(M_0) \neq \emptyset$.
Θεωρούμε $n, n' \in f(M_0)$, $r \in R$. Τότε, υπάρχουν $m, m' \in M_0$ με $n = f(m)$, $n' = f(m')$.
Συνεπώς,

$$n + n' = f(m) + f(m') = f(m+m') \in f(M_0)$$

και

$$rn = rf(m) = f(rm) \in f(M_0)$$

(ii) Καθώς $f(0) = 0 \in N_0$ έχουμε $0 \in f^{-1}(N_0)$.
Έστω $m, m' \in f^{-1}(N_0), r \in R$. Τότε, $f(m+m') = f(m)+f(m') \in N_0$ άρα $m+m' \in f^{-1}(N_0)$, και $f(rm) = rf(m) \in N_0$ άρα $rm \in f^{-1}(N_0)$.
Τα (iii),(iv) είναι άμεσες συνέπειες των (i),(ii) αντίστοιχα. □

Πρόταση 2.5.2. *Οι επόμενες συνθήκες είναι ισοδύναμες για έναν ομομορφισμό R-προτύπων $f\colon M \to N$.*

(i) Ο f είναι 1-1 και επί.

(ii) Υπάρχει ομομορφισμός R-προτύπων $g\colon N \to M$ τέτοιος ώστε $f \circ g = I_N$ και $g \circ f = I_M$.

Αν ικανοποιούνται αυτές οι συνθήκες ο f ονομάζεται ***ισομορφισμός*** *R-προτύπων.*

Απόδειξη. (i)⇒ (ii) Θεωρούμε την συνάρτηση $f^{-1}\colon N \to M$.

Είναι φανερό ότι $f \circ f^{-1} = I_N$ και $f^{-1} \circ f = I_M$. Θα δείξουμε ότι η f^{-1} είναι ομομορφισμός.

Έστω $n, n' \in N, r \in R$. Τότε, επειδή η f είναι επί υπάρχουν $m, m' \in M$ με $f(m) = n$, $f(m') = n'$. Συνεπώς,

$$n + n' = f(m) + f(m') = f(m + m')$$

άρα

$$f^{-1}(n + n') = m + m' = f^{-1}(n) + f^{-1}(n')$$

και $rn = rf(m) = f(rm)$. Τελικά, $f^{-1}(rn) = rm = rf^{-1}(n)$.
(ii)⇒ (i) Αν $m, m' \in M : f(m) = f(m')$, τότε

$$m = g \circ f(m) = g[f(m)] = g[f(m')] = m'$$

Άρα η f είναι 1-1.

Έστω $n \in N$. Θεωρούμε το $g(n) \in M$ και υπολογίζουμε $n = f \circ g(n) = f[g(n)]$. □

Ορισμός 2.5.2. Δύο R-πρότυπα M, N καλούνται **ισόμορφα** αν υπάρχει ισομορφισμός

$$f\colon M \to N$$

Παρατηρήσεις 2.5.2. (i) Κάθε R-πρότυπο M είναι ισόμορφο με το M μέσω της ταυτοτικής $I_M : M \to M$.

(ii) Έστω M, N δύο R-πρότυπα ώστε το M να είναι ισόμορφο με το N. Τότε, το N είναι ισόμορφο με το M.

Πράγματι, αν $f\colon M \to N$ ισομορφισμός R-προτύπων, τότε ο $f^{-1}\colon N \to M$ είναι ομομορφισμός, 1-1, και επί, άρα είναι και ισομορφισμός.

(iii) Έστω M, N, L τρία R-πρότυπα. Αν το M είναι ισόμορφο με το N, και το N είναι ισόμορφο με το L, τότε το M είναι ισόμορφο με το L.

Αν $f\colon M \to N$, $g\colon N \to L$ ισομορφισμοί, τότε η σύνθεση $g \circ f\colon M \to L$ είναι ομομορφισμός, 1-1, και επί.

Θεώρημα 2.5.1 (1ο Θεώρημα Ισομορφισμών R-προτύπων). *Έστω $f\colon M \to N$ ένας ομομορφισμός προτύπων. Τότε, υπάρχει ισομορφισμός R-προτύπων $\bar{f}\colon M/\ker f \to \operatorname{im} f$ τέτοιος ώστε η f να είναι*

$$M \xrightarrow{p} M/\ker f \xrightarrow{\bar{f}} \operatorname{im} f \xrightarrow{i} N$$

όπου p η απεικόνιση πηλίκο, $p(m) = m + \ker f$ για κάθε $m \in M$ και i η ενθετική απεικόνιση, $i(n) = n$ για κάθε $n \in \operatorname{im} f$.

Απόδειξη. Γνωρίζουμε ότι η απεικόνιση

$$\bar{f}\colon M/\ker f \to \operatorname{im} f, \quad \bar{f}(m + \ker f) = f(m), \quad \forall m + \ker f \in M/\ker f$$

είναι καλά ορισμένη, 1-1, επί, και προσθετική.

Η $\bar{f}$ είναι ομομορφισμός R-προτύπων, άρα και ισομορφισμός. Πράγματι, αν $m + \ker f \in M/\ker f$, $r \in R$, τότε

$$\begin{aligned} \bar{f}[r(m + \ker f)] &= \bar{f}(rm + \ker f) \\ &= f(rm) = rf(m) \\ &= r\bar{f}(m + \ker f) \end{aligned}$$

Για να δείξουμε ότι $i \circ \bar{f} \circ p = f \colon M \to N$, θεωρούμε $m \in M$ και υπολογίζουμε

$$\begin{aligned}(i \circ \bar{f} \circ p)(m) &= i[\bar{f}[p(m)]] \\ &= i[\bar{f}(m + \ker f)] \\ &= i[f(m)] = f(m)\end{aligned}$$

□

Πόρισμα 2.5.1. *Τα πεπερασμένα παραγόμενα R-πρότυπα είναι (ως προς ισομορφισμό) ακριβώς τα R-πρότυπα της μορφής R^n/U, όπου $n \in \mathbb{N}$ και $U \subseteq R^n$ ένα υποπρότυπο.*

Απόδειξη. Έστω M ένα πεπερασμένα παραγόμενο R-πρότυπο. Τότε, υπάρχουν $n \in \mathbb{N}$, $m_1, m_2, \ldots, m_n \in M$ ώστε

$$M = \langle m_1, m_2, \ldots, m_n \rangle$$

Θεωρούμε την απεικόνιση

$$f \colon R^n \to M, \quad f(r_1, r_2, \ldots, r_n) = r_1 m_1 + r_2 m_2 + \cdots + r_n m_n$$

Η f είναι R-γραμμική. Έστω $(r_1, r_2, \ldots, r_n), (r_1' r_2', \ldots, r_n') \in R^n$, $r \in R$. Τότε,

$$\begin{aligned}f((r_1, r_2, \ldots, r_n) + (r_1', r_2', \ldots, r_n')) &= f(r_1 + r_1', r_2 + r_2', \ldots, r_n + r_n') \\ &= (r_1 + r_1')m_1 + (r_2 + r_2')m_2 + \cdots + (r_n + r_n')m_n \\ &= (r_1 m_1 + r_2 m_2 + \cdots + r_n m_n) + (r_1' m_1 + r_2' m_2 + \cdots + r_n' m_n) \\ &= f(r_1, r_2, \ldots, r_n) + f(r_1', r_2', \ldots, r_n')\end{aligned}$$

και

$$\begin{aligned}f(r(r_1, r_2, \ldots, r_n)) &= f(rr_1, rr_2, \ldots, rr_n) \\ &= rr_1 m_1 + rr_2 m_2 + \cdots + rr_n m_n \\ &= r(r_1 m_1 + r_2 m_2 + \cdots + r_n m_n) \\ &= r f(r_1, r_2, \ldots, r_n)\end{aligned}$$

Η f είναι επί. Για κάθε $m \in M$ υπάρχουν $r_1, r_2, \ldots, r_n$ με

$$m = r_1 m_1 + r_2 m_2 + \cdots + r_n m_n$$

άρα $m = f(r_1, r_2, \ldots, r_n)$.

Άρα υπάρχει ισομορφισμός $R^n/\ker f \simeq \operatorname{im} f = M$.

Αντίστροφα, καθώς το R-πρότυπο R^n είναι πεπερασμένα παραγόμενο, γνωρίζουμε ότι για κάθε R-υποπρότυπο $U \subseteq R^n$ το πηλίκο R^n/U είναι πεπερασμένα παραγόμενο. □

Πόρισμα 2.5.2. *Έστω R ένας μεταθετικός δακτύλιος. Τότε τα κυκλικά R-πρότυπα είναι (ως προς ισομορφισμό) ακριβώς τα R-πρότυπα της μορφής R/I για κάποιο ιδεώδες I/R.*

Απόδειξη. Άμεση συνέπεια της απόδειξης του Πορίσματος 2.5.1 για $n = 1$. □

Παράδειγμα 2.5.1. Έστω $M_1, M_2, \ldots M_k$ R-πρότυπα και $N_1 \subseteq M_1, N_2 \subseteq M_2, \ldots N_k \subseteq M_k$ R-υποπρότυπα. Τότε το R-πρότυπο

$$N = N_1 \oplus N_2 \oplus \cdots \oplus N_k$$

είναι ένα R-υποπρότυπο του R-προτύπου

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

και υπάρχει ισομορφισμός R-προτύπων

$$M/N \simeq M_1/N_1 \oplus M_2/N_2 \oplus \cdots \oplus M_k/N_k$$

Θεωρούμε την απεικόνιση

$$\pi \colon M \to M_1/N_1 \oplus M_2/N_2 \oplus \cdots \oplus M_k/N_k$$

$$\pi(m_1, m_2, \ldots, m_k) = (m_1+N_1, m_2+N_2, \ldots, m_k+N_k), \quad \forall (m_1, m_2, \ldots, m_k) \in M_1 \oplus M_2 \oplus \cdots \oplus M_k = M$$

Η π είναι ομομορφισμός.

$$\begin{aligned}
\pi(r(m_1, m_2, \ldots, m_k) &= \pi(rm_1, rm_2, \ldots, rm_k) \\
&= (rm_1 + N_1, rm_2 + N_2, \ldots, rm_k + N_k) \\
&= [r(m_1 + N_1), r(m_2 + N_2), \ldots, r(m_k + N_k)] \\
&= r(m_1 + N_1, m_2 + N_2, \ldots, m_k + N_k) \\
&= r\pi(m_1, m_2, \ldots, m_k)
\end{aligned}$$

Η π είναι επί. Κάθε στοιχείο του $M_1/N_1 \oplus M_2/N_2 \oplus \cdots \oplus M_k/N_k$ είναι της μορφής

$$(m_1 + N_1, m_2 + N_2, \ldots, m_k + N_k) = \pi(m_1, m_2, \ldots, m_k)$$

Τέλος,

$$\begin{aligned}
\ker \pi &= \{(m_1, m_2, \ldots, m_k) \in M | \pi(m_1, m_2, \ldots, m_k) = (0 + N_1, 0 + N_2, \ldots, 0 + N_k)\} \\
&= \{(m_1, m_2, \ldots, m_k) \in M | (m_1 + N_1, m_2 + N_2, \ldots, m_k + N_k) = (0 + N_1, 0 + N_2, \ldots, 0 + N_k)\} \\
&= \{(m_1, m_2, \ldots, m_k) \in M | m_1 + N_1 = 0 + N_1, m_2 + N_2 = 0 + N_2, \ldots, m_k + N_k = 0 + N_k\} \\
&= \{(m_1, m_2, \ldots, m_k) \in M | m_1 \in N_1, m_2 \in N_2, \ldots, m_k \in N_k\} \\
&= \{(m_1, m_2, \ldots, m_k) \in M | (m_1, m_2, \ldots, m_k) \in N_1 \oplus N_2 \oplus \cdots \oplus N_k = N\} \\
&= N
\end{aligned}$$

Συνεπώς, υπάρχει ισομορφισμός R-προτύπων

$$\bar{\pi} \colon M/N = M/\ker f \to \operatorname{im} \pi = M_1/N_1 \oplus M_2/N_2 \oplus \cdots \oplus M_k/N_k$$

Θεώρημα 2.5.2 (2ο Θεώρημα Ισομορφισμών R-προτύπων). *Έστω M ένα R-πρότυπο και $N, L \subseteq M$ δύο R-υποπρότυπα. Τότε:*

(i) Το σύνολο $N + L \subseteq M$, με

$$N + L = \{m \in M \mid \exists x \in N, y \in L : m = x + y\}$$

είναι ένα υποπρότυπο του M.

(ii) Υπάρχει ισομορφισμός R-προτύπων

$$(N + L)/N \simeq L/N \cap L$$

Απόδειξη. (i): Προφανώς $0 = 0+0 \in N+L$. Θεωρούμε $m, m' \in N+L$, $r \in R$. Τότε, υπάρχουν $x, x' \in N$, $y, y' \in L$ τέτοια ώστε $m = x + y$, $m' = x' + y'$.

Συνεπώς,

$$\begin{aligned} m + m' &= (x + y) + (x' + y') \\ &= (x + x') + (y + y') \in N + L \end{aligned}$$

και $rm = r(x + y) = rx + ry \in N + L$.

Προφανώς, $N \subseteq N + L$ και $L \subseteq N + L$.
(ii): Καθώς, $N \subseteq N + L$, έχει νόημα να θεωρήσουμε το αντίστοιχο πηλίκο. Θεωρούμε την απεικόνιση

$$f \colon L \to N + L/N, \quad f(y) = y + N \forall y \in L$$

και παρατηρούμε ότι η f είναι R-ομομορφισμός ως σύνθεση ομομορφισμών

$$L \overset{i}{\hookrightarrow} N + L \overset{p}{\to} N + L/N$$

Η f είναι επί. Αν $k \in N + L/N$, τότε υπάρχει $m \in N + L$ με $k = m + N$. Επίσης, υπάρχουν $x \in N, y \in L$ τέτοια ώστε $m = x + y$.

Καθώς $m - y = x \in M$ έχουμε $m + N = y + N \in N + L/N$. Συνεπώς,

$$k = m + N = y + N = f(y) \in \mathrm{im} f$$

Τέλος,

$$\begin{aligned} \ker f &= \{y \in L \colon f(y) = 0 + N \in N + L/N\} \\ &= \{y \in L \colon y + N = 0 + N \in N + L/N\} \\ &= L \cap N \end{aligned}$$

Συνεπώς, από το 1ο Θεώρημα Ισομορφισμών υπάρχει ισομορφισμός R-προτύπων

$$L/N \cap L = L/\ker f \overset{\bar{f}}{\to} \mathrm{im} f = N + L/N$$

□

Θεώρημα 2.5.3 (3ο Θεώρημα Ισομορφισμών R-προτύπων). *Έστω M ένα R-πρότυπο και $N \subseteq M$ ένα R-υποπρότυπο.*

(i) Αν $L \subseteq M$ είναι ένα υποπρότυπο με $L \supseteq N$, τότε το $L/N \subseteq M/N$ είναι ένα υποπρότυπο και υπάρχει ισομορφισμός R-προτύπων

$$(M/N)/(L/N) \simeq M/L$$

(ii) Κάθε υποπρότυπο $\bar{L} \subseteq M/N$ είναι επίσης της μορφής $\bar{L} = L/N$ για ένα μοναδικό R-υποπρότυπο $L \subseteq M$ με $L \supseteq N$.

Απόδειξη. (i) Θεωρούμε την απεικόνιση

$$\pi \colon M/N \to M/L, \qquad \pi(m + N) = m + L, \quad \forall m + N \in M/N$$

Η π είναι καλά ορισμένη. Έστω $m, m' \in M$ με $m + N = m' + N \in M/N$. Τότε, $m' - m \in N$, άρα $m' - m \in L$ και έτσι $m + L = m' + L \in M/L$.

Η π είναι R-γραμμική. Θεωρούμε $m+N, m'+n \in M/N$ και έχουμε

$$\begin{aligned}\pi[(m+N)+(m'+N)] &= \pi[(m+m')+N] = (m+m')+L \\ &= (m+L)+(m'+L) = \pi(m+N)+\pi(m'+N)\end{aligned}$$

και για κάθε $r \in R$ ισχύει

$$\begin{aligned}\pi[r(m+N)] &= \pi(rm+N) \\ &= rm+L = r(m+N)\end{aligned}$$

Η π είναι επί. Κάθε στοιχείο $k \in M/L$ είναι της μορφής $k = m+L = \pi(m+N)$, για κάποιο $m \in M$.

Τέλος,

$$\begin{aligned}\ker\pi &= \{m+N \in M/N \colon \pi(m+N) = 0+L \in M/L\} \\ &= \{m+N \in M/N \colon m+L = 0+L \in M/L\} \\ &= \{m+N \in M/N \colon m \in L\} \\ &= L/N\end{aligned}$$

Συνεπώς, από 1ο Θεώρημα Ισομορφισμών

$$(M/N)/(L/N) = (M/N)/\ker \xrightarrow{\bar{\pi}} \mathrm{im}\pi = M/L$$

(ii) Αν $\bar{L} \subseteq M/N$ είναι ένα υποπρότυπο, τότε θεωρούμε τον ομομορφισμό πηλίκο

$$p \colon M \to M/N$$

και το υποπρότυπο

$$L = p^{-1}(\bar{L}) \subseteq M$$

Παρατηρούμε ότι

$$L = p^{-1}(\bar{L}) \supseteq p^{-1}(0) = \ker p = N$$

και

$$\bar{L} = p[p^{-1}(\bar{L})] = p(L) = L/N$$

γιατί η p είναι επί.

Επιπλέον, το L είναι μοναδικό. Αν $L' \subseteq M$ είναι ένα υποπρότυπο με $L' \supseteq N$ και $L'/N = \bar{L}$, τότε $L' \subseteq \{m \in M \colon m+N \in \bar{L}\} = L$ άρα $L' \subseteq L$.

Αν $x \in L$, τότε $x+N \in L/N = \bar{L} = L'/N$, άρα υπάρχει $x' \in L$ ώστε $x+N = x'+N \in \bar{L}$.

Συνεπώς, $x'-x \in N$, άρα $x'-x \in L'$. Τότε, $x = x'-(x'-x) \in L'$. Έτσι, $L \subseteq L'$.

Τελικά, $L' = L$. □

2.6 Ασκήσεις

1.

Κεφάλαιο 3

Ελεύθερα Πρότυπα και Κανονική Μορφή Smith

3.1 Ελεύθερα Πρότυπα

Ορισμός 3.1.1. Έστω M ένα R-πρότυπο.

(i) Ένα $B \subseteq M$ καλείται **γραμμικά ανεξάρτητο** αν για κάθε πεπερασμένο $B_0 \subseteq B$ με $|B_0| = n$ και

$$B_0 = \{m_1, m_2, \ldots, m_n\}$$

και κάθε $r_1, r_2, \ldots, r_n \in R$ με $(r_1, r_2, \ldots, r_n) \neq (0, 0, \ldots, 0)$ ισχύει

$$r_1 m_1 + r_2 m_2 + \cdots + r_n m_n \neq 0 \in M$$

(ii) Ένα $B \subseteq M$ **παράγει** το R-πρότυπο M αν για κάθε $m \in M$ υπάρχει πεπερασμένο $B_0 \subseteq B$ με

$$B_0 = \{m_1, m_2, \ldots, m_n\}$$

τέτοιο ώστε

$$m \in \langle m_1, m_2, \ldots, m_n \rangle$$

(iii) Ένα $B \subseteq M$ καλείται **βάση** του M αν αυτό είναι γραμμικά ανεξάρτητο και παράγει το M.

(iv) Το R-πρότυπο M καλείται **ελεύθερο** αν έχει βάση.

Παραδείγματα 3.1.1. (i) Έστω $\mathbb{F}$ σώμα. Τότε, κάθε πεπερασμένο $\mathbb{F}$-πρότυπο ($\mathbb{F}$-διανυσματικός χώρος) έχει μια πεπερασμένη βάση B. Συνεπώς, κάθε πεπερασμένα παραγόμενο $\mathbb{F}$-πρότυπο είναι ελεύθερο.

Επιπλέον, το πλήθος των στοιχείων μιας βάσης B εξαρτάται μόνο από τον $\mathbb{F}$-διανυσματικό χώρο και ονομάζεται διάσταση του.

(ii) Το $\mathbb{Z}$-πρότυπο $\mathbb{Q}$ δεν είναι ελεύθερο (ούτε πεπερασμένα παραγόμενο).

Πράγματι, έστω ότι υπάρχει βάση B του $\mathbb{Z}$-πρότυπου $\mathbb{Q}$.

Ισχυρισμός: $|B| \leq 1$.

Αν $|B| \geq 2$, τότε υπάρχουν $q_1, q_2 \in B$ με $q_1 \neq q_2$. Γράφουμε $q_1 = \frac{a_1}{b_1}, q_2 = \frac{a_2}{b_2}$, όπου $a_1, a_2, b_1, b_2 \neq 0$ και έχουμε

$$(a_2 b_1)q_1 + (-a_1 b_2)q_2 = 0 \in \mathbb{Q}$$

-άτοπο.

Καθώς, $B \neq \emptyset$, έπεται ότι $B = \{q\}$. Γράφουμε $q = \frac{a}{b}$, με $a, b \in \mathbb{Z}$, $b \neq 0$ και μκδ$(a, b) = 1$ και παρατηρούμε ότι αν $p \in \mathbb{Z}$ πρώτος με $p \nmid b$, τότε $\frac{1}{p} \notin < q >$.

Πράγματι, αν $\frac{1}{p} = nq$, για κάποιο $n \in \mathbb{Z}$, τότε $\frac{1}{p} = \frac{na}{b}$, άρα $b = pna$ και $p|b$ -άτοπο.

(iii) Έστω R ακέραια περιοχή και $I \subseteq R$ ένα κύριο ιδεώδες. Τότε, το R-πρότυπο I είναι ελεύθερο.

Αν $I = 0$, τότε μια βάση του είναι το $B = 0$ Αν $I \neq 0$, τότε υπάρχει $a \in I$ με $a \neq 0$ ώστε $I = (a)$. Καθώς, $I = (a)$, το $B = \{a\}$ παράγει το R-πρότυπο I.

Για να δείξουμε ότι το B είναι γραμμικά ανεξάρτητο, παρατηρούμε ότι για κάθε $r \in R$ με $r \neq 0$ είναι $ra \neq 0$, αφού το R είναι ακέραια περιοχή.

(iv) Έστω R μεταθετικός δακτύλιος και $I \subseteq R$ ένα ιδεώδες. Αν το I είναι ελεύθερο ως R-πρότυπο, τότε το I είναι κύριο.

Αν $I = 0$, τότε $I = (0)$ κύριο. Αν $I \neq 0$, τότε υπάρχει μια βάση B του R-προτύπου I με $B \neq \emptyset$.

Ισχυρισμός: $B = \{a\}$,και άρα $I = (a)$ κύριο. Αν $|B| \geq 2$, μπορούμε να βρούμε $B_0 \subseteq B$ με $|B_0| = 2$. Αν $B_0 = \{a, b\}$, τότε αυτά δεν μπορεί να είναι γραμμικά ανεξάρτητα μιας και $ba + (-a)b = 0 \in I$.

(v) Το ιδεώδες

$$(2, x) \subseteq \mathbb{Z}[x]$$

δεν είναι κύριο, και άρα δεν είναι ελεύθερο ως $\mathbb{Z}[x]$-πρότυπο.

Πρόταση 3.1.1. *Οι επόμενες συνθήκες ειναι ισοδύναμες για το R-πρότυπο M:*

(i) Το M είναι πεπερασμένα παραγόμενο και ελεύθερο.

(ii) Το M έχει μια βάση με n στοιχεία, για κάποιο $n \in \mathbb{N}$.

(iii) Υπάρχει ισομορφισμός R-προτύπων $M \simeq R^n$, για κάποιο $n \in \mathbb{N}$.

Απόδειξη. (i) $\Rightarrow$ (ii)Έστω B μια βάση του M. Καθώς το M είναι πεπερασμένα παραγόμενο, υπάρχουν $n \in \mathbb{N}$, $m_1, m_2, \ldots, m_n \in M$ ώστε

$$M = \langle m_1, m_2, \ldots, m_n \rangle$$

Τότε, υπάρχει πεπερασμένο υποσύνολο $B_0 \subseteq B$ με $B_0 = \{x_1, x_2, \ldots, x_k\}$ και

$$m_1, m_2, \ldots, m_n \in \langle x_1, x_2, \ldots, x_k \rangle$$

Τώρα, θα δείξουμε ότι $B = B_0$.

Αν $B_0 \subset B$ μπορούμε να βρούμε $x \in B \backslash B_0$. Τότε, $x \in M =< m_1, m_2, \ldots, m_n >$ και άρα $x \in < x_1, x_2, \ldots, x_k >$, δηλαδή υπάρχουν $r_1, r_2, \ldots, r_k$ με $x = r_1 x_1 + r_2 x_2 + \cdots + r_k x_k$. Συνεπώς,

$$r_1 x_1 + r_2 x_2 + \cdots + r_k x_k + (-1)x = 0 \in M$$

άρα το

$$B_0 \cup \{x\} = \{x_1, x_2, \ldots, x_k, x\} \subseteq B$$

είναι γραμμικά εξαρτημένο -άτοπο.
(ii) $\Rightarrow$ (iii) Έστω $m_1, m_2, \ldots, m_n$ στοιχεία μιας βάσης B του M. Θεωρούμε την απεικόνιση

$$f : R^n \to M, \quad f(r_1, r_2, \ldots, r_n) = r_1 m_1 + r_2 m_2 + \cdots + r_n m_n, \quad \forall (r_1, r_2, \ldots, r_n) \in R^n$$

Εύκολα δείχνεται ότι η f είναι ομομορφισμός R-προτύπων. Επιπλέον, λόγω της ανεξαρτησίας των $m_1, m_2, \ldots, m_n$, η f είναι 1-1. Τέλος, είναι

$$m_i = f(0, 0, \ldots, 1, 0, \ldots, 0) \in \text{im}\, f, \quad i = 1, 2, \ldots, n$$

και άρα

$$M = \langle m_1, m_2, \ldots, m_n \rangle \subseteq \text{im}\, f \subseteq M$$

οπότε $\text{im}\, f = M$ και η f είναι επί. Άρα, η f είναι ισομορφισμός.
(iii) $\Rightarrow$ (i) Έστω $f : R^n \to M$ ένας ισομορφισμός. Θεωρούμε τα $m_1, m_2, \ldots, m_n \in M$, με

$$m_1 = f(1, 0, \ldots, 0),\ m_2 = f(0, 1, 0, \ldots, 0), \ldots,\ m_n = f(0, 0, \ldots, 0, 1)$$

Θα δείξουμε ότι το $\{m_1, m_2, \ldots, m_n\}$ είναι μια βάση του M.

Αν $m \in M$ υπάρχει μοναδικό $(r_1, r_2, \ldots, r_n) \in R^n$ με $m = f(r_1, r_2, \ldots, r_n)$. Τότε, όμως

$$\begin{aligned} &f[r_1(1, 0, \ldots, 0) + r_2(0, 1, \ldots, 0) + \cdots + r_n(0, 0, \ldots, 1)] \\ &= r_1 f(1, 0, \ldots, 0) + r_2 f(0, 1, \ldots, 0) + \cdots + r_n f(0, 0, \ldots, 1) \\ &= r_1 m_1 + r_2 m_2 + \cdots + r_n m_n \end{aligned}$$

Συνεπώς,

$$M = \langle m_1, m_2, \ldots, m_n \rangle$$

Για να δείξουμε ότι τα $m_1, m_2, \ldots, m_n$ είναι γραμμικά ανεξάρτητα, υποθέτουμε ότι

$$\exists s_1, s_2, \ldots, s_n \in R : s_1 m_1 + s_2 m_2 + \cdots + s_n m_n = 0 \in M$$

Τότε,

$$f(s_1, s_2, \ldots, s_n) = \cdots = s_1 m_1 + s_2 m_2 + \cdots + s_n m_n = 0$$

και άρα έχουμε ότι

$$(s_1, s_2, \ldots, s_n) = (0, 0, \ldots, 0)$$

άρα $s_i = 0$, $i = 1, 2, \ldots, n$. □

Έστω M, N δύο πεπερασμένα παραγόμενα ελεύθερα R-πρότυπα. Επιλέγουμε διατεταγμένες βάσεις $\widehat{m} = (m_1, m_2, \ldots, m_\mu)$ του M και $\widehat{n} = (n_1, n_2, \ldots, n_\nu)$. Αν $f : M \to N$ είναι μια γραμμική απεικόνιση, θεωρούμε τα $f(m_1), f(m_2), \ldots, f(m_\mu) \in N$ και κατασκευάζουμε τον πίνακα

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1\mu} \\ a_{21} & a_{22} & \ldots & a_{2\mu} \\ \vdots & \vdots & \ddots & \vdots \\ a_{\nu 1} & a_{\nu 2} & \ldots & a_{\nu\mu} \end{pmatrix} \in R^{\nu \times \mu}$$

με

$$f(m_1) = a_{11}n_1 + a_{12}n_2 + \cdots + a_{1\mu}n_\nu$$

$$f(m_2) = a_{21}n_1 + a_{22}n_2 + \cdots + a_{1\mu}n_{2\nu}$$

$$\vdots$$

$$f(m_\mu) = a_{\nu 1}n_1 + a_{\nu 2}n_2 + \cdots + a_{\nu\mu}n_\nu$$

Αν γράψουμε $A = (f : \widehat{m}, \widehat{n})$ ορίζουμε με τον τρόπο αυτό μια απεικόνιση

$$\{M \to N \mid f \in \mathrm{Hom}_R(M,N)\} \xrightarrow{\lambda} R^{\nu\times\mu}, \quad f \mapsto (f : \widehat{m}, \widehat{n})$$

Ιδιότητες της απεικόνισης λ:

(i) Η λ είναι 1-1 και επί.

(ii) Έστω V ένα πεπερασμένα παραγόμενο και ελεύθερο R-πρότυπο με μια διατεταγμένη βάση $\widehat{\ell} = (\ell_1, \ell_2, \ldots, \ell_\lambda)$.

Θεωρούμε ομομορφισμούς $f : M \to N$, $g : N \to L$ και τη σύνθεση τους $g \circ f : M \to L$. Τότε,

$$(g \circ f : \widehat{m}, \widehat{\ell}) = (g : \widehat{m}, \widehat{\ell}) \cdot (f : \widehat{m}, \widehat{n})$$

Παραδείγματα 3.1.2. (i) (**Πίνακας αλλαγής βάσης**) Έστω M ένα πεπερασμένα παραγόμενο ελεύθερο R-πρότυπο και $\widehat{m} = (m_1, m_2, \ldots, m_\mu)$, $\widehat{m}' = (m'_1, m'_2, \ldots, m'_\mu)$ δύο διατεταγμένες βάσεις του.

Ο πίνακας $P = (I_M : \widehat{m}, \widehat{m}')$ είναι αντιστρέψιμος και καλείται πίνακας αλλαγής βάσης από την $\widehat{m}$ στην $\widehat{m}'$. Μάλιστα, ο αντίστροφος του P είναι ο πίνακας αλλαγής βάσης $P^{-1} = (I_M : \widehat{m}', \widehat{m})$

Πράγματι

$$PP^{-1} = (I_M : \widehat{m}, \widehat{m}')(I_M : \widehat{m}', \widehat{m}) = (I_M \circ I_M : \widehat{m}', \widehat{m}') = I_M$$

και αντίστοιχα

$$P^{-1}P = (I_M : \widehat{m}', \widehat{m})(I_M : \widehat{m}, \widehat{m}') = (I_M \circ I_M : \widehat{m}, \widehat{m}) = I_M$$

(ii) (**Ισοδυναμία Πινάκων**) Έστω M, N δύο πεπερασμένα παραγόμενα ελεύθερα R-πρότυπα και $f : M \to N$ ένας ομομορφισμός. Έστω $\widehat{m}, \widehat{m}'$ δύο διατεταγμένες βάσεις τουυ M και $\widehat{n}, \widehat{n}'$ δύο διατεταγμένες βάσεις του N. Τότε, οι πίνακες $A = (f : \widehat{m}, \widehat{n})$ και $A' = (f : \widehat{m}', \widehat{n}')$ είναι ισοδύναμοι, δηλαδή υπάρχουν αντιστρέψιμοι πίνακες P, Q ώστε $A' = PAQ$.

Πράγματι, η f είναι η σύνθεση

$$M \xrightarrow{I_M} M \xrightarrow{f} N \xrightarrow{I_N} N$$

και άρα $A' = (f : \widehat{m}', \widehat{n}') = (I_M \circ f \circ I_N : \widehat{m}', \widehat{n}') = (I_N : \widehat{n}, \widehat{n}')(f : \widehat{m}, \widehat{n})(I_M : \widehat{m}, \widehat{m}')$.

Πρόταση 3.1.2. *Έστω R μεταθετικός δακτύλιος με $1_R \neq 0_R$. Τότε υπάρχει σώμα $\mathbb{F}$ και ομομορφισμός δακτυλίων $\phi : R \to \mathbb{F}$ με $\phi(1) = 1$.*

Απόδειξη. Έστω

$$\mathfrak{X} = \{I \subseteq R \,|\, I \text{ ιδεώδη με } 1 \notin I\}$$

Μπορούμε να επιλέξουμε ένα $I \in \mathfrak{X}$ έτσι ώστε για κάθε $J \in \mathfrak{X}$ με $J \supseteq I$ να είναι $J = I$.

Ισχυριζόμαστε ότι ο δακτύλιος-πηλίκο R/I είναι σώμα, οπότε η απεικόνιση-πηλίκο $R \to R/I$ είναι ο ζητούμενος ομομορφισμός δακτυλίων.

Ο δακτύλιος-πηλίκο R/I είναι μεταθετικός και έχει μονάδα. Έστω $r + I \in R/I$ ώστε $r + I \neq 0 + I$. Τότε, $r \notin I$. Θεωρούμε το ιδεώδες

$$J = I + (r) = \{r \in R \,|\, \exists y \in I, a \in R : x = y + ar\}$$

και παρατηρούμε ότι $I \subseteq J$. Επιπλέον, $I \subset J$, γιατί $r \in J$, αλλά $r \notin I$.

Από την επιλογή του I, έπεται ότι $J \notin \mathfrak{X}$, και άρα $1 \in J$. Συνεπώς, υπάρχουν $y_0 \in I, a_0 \in R$ τέτοια ώστε $1 = y_o + a_0 r$.

Τότε, όμως, $1 - a_0 r = y_0 \in I$ και άρα $(a_0 + I)(r + I) = a_o r + I = 1 + I$, οπότε $a_0 + 1 = (r + I)^{-1}$. □

Πρόταση 3.1.3. *Έστω R μεταθετικός δακτύλιος.*

(i) Δεν υπάρχουν $n, m \in \mathbb{N}$ με $n \neq m$ και πίνακες $A \in R^{n\times m}, B \in R^{m\times n}$ ώστε $AB = I_n$ και $BA = I_m$.

(ii) Δεν υπάρχουν $n, m \in \mathbb{N}$ με $n \neq m$ ώστε $R^n \simeq R^m$.

Απόδειξη. (i) Έστω ότι υπάρχουν $n, m \in \mathbb{N}$ με $n \neq m$ και πίνακες $A \in R^{n\times m}, B \in R^{m\times n}$ ώστε $AB = I_n$ και $BA = I_m$.

Γνωρίζουμε ότι υπάρχει σώμα $\mathbb{F}$ και ομομορφισμός δακτυλίων $\phi : R \to \mathbb{F}$. Θεωρούμε τους πίνακες $A' \in \mathbb{F}^{n\times m}, B' \in \mathbb{F}^{m\times n}$, που προκύπτουν από τους A, B εφαρμοζοντας τον ϕ σε κάθε εγγραφή. Τότε, αφού η ϕ είναι προσθετική, πολλαπλασιαστική και $\phi(1) = 1$ είναι $A'B' = I_n \in \mathbb{F}^{n\times n}, B'A' = I_m \in \mathbb{F}^{m\times m}$.

Αυτό δεν μπορεί να συμβεί καθώς στον $\mathbb{F}$-διανυσματικό χώρο $\mathbb{F}^n \not\simeq \mathbb{F}^m$.
(ii) Υποθέτουμε ότι υπάρχουν $n, m \in \mathbb{N}$ με $n \neq m$ ώστε $R^n \simeq R^m$. Τότε, υπάρχουν R-ομομορφισμοί $f : R^n \to R^m, g : R^m \to R^n$, με $f \circ g = I_{R^m}, g \circ f = I_{R^n}$.

θεωρούμε διατεταγμένες βάσεις, $\widehat{u}$ του R^n, $\widehat{v}$ του R^m και τους πίνακες $B = (f : \widehat{v}, \widehat{u}) \in R^{m\times n}, A = (g : \widehat{v}, \widehat{u}) \in R^{n\times m}$. Τότε,

$$AB = (g : \widehat{v}, \widehat{u})(f : \widehat{v}, \widehat{u}) = (g \circ f : \widehat{u}, \widehat{u}) = (I_{R^n} : \widehat{u}, \widehat{u}) = I_n$$

και

$$BA = (f : \widehat{v}, \widehat{u})(g : \widehat{v}, \widehat{u}) = (f \circ g : \widehat{v}, \widehat{v}) = (I_{R^m} : \widehat{v}, \widehat{v}) = I_m$$

-άτοπο από (i). □

Ορισμός 3.1.2. Αν R είναι ένας μεταθετικός δακτύλιος και M ένα πεπερασμένα παραγόμενο ελεύθερο R-πρότυπο, τότε το πλήθος των στοιχείων μιας πεπερασμένης βάσης του M καλείται **διάσταση** (ή τάξη) του M και συμβολίζεται με $\operatorname{rank} M$.

Παρατήρηση 3.1.1. Το πλήθος των στοιχείων μιας πεπερασμένης βάσης ενός R-προτύπου δεν εξαρτάται από την επιλογή της βάσης.

Πράγματι, αν B_1, B_2 δύο βάσεις του M με n_1, n_2 στοιχεία αντίστοιχα, τότε υπάρχουν ισομορφισμοί $M \simeq R^{n_1}, M \simeq R^{n_2}$. Τότε, $R^{n_1} \simeq R^{n_2}$ άρα $n_1 = n_2$.

Λήμμα 3.1.1. *Έστω R ΠΚΙ, M ένα R-πρότυπο και $f : M \to R$ ένας ομομορφισμός R-προτύπων. Τότε, υπάρχει ισομομορφισμός R-προτύπων*

$$M \simeq \ker f \oplus \operatorname{im} f$$

Απόδειξη. Αν $f = 0$, τότε $\operatorname{im} f = 0$, $\ker f = M$ και

$$\ker f \oplus \operatorname{im} f = M \oplus 0 \simeq M$$

Υποθέτουμε ότι $f \neq 0$ και άρα $0 \neq \operatorname{im} f \subseteq R$. Η $\operatorname{im} f$ είναι ένα υποπρότυπο του R, δηλαδή ένα ιδεώδες.

Συνεπώς, υπάρχει $a \in \operatorname{im} f$ τέτοιο ώστε $\operatorname{im} f = \langle a \rangle$. Παρατηρούμε ότι $a \neq 0$. Επιπλέον, υπάρχει $m_a \in M$ με $a = f(m_0)$. Θεωρούμε την απεικόνιση

$$\lambda : \ker f \oplus \operatorname{im} f \to M, \quad \lambda(m, ra) = m + rm_a, \quad \forall (m, ra) \in \ker f \oplus \operatorname{im} f$$

Η λ είναι καλά ορισμένη.

Αν $m, m' \in \ker f$ και $ra, r'a \in \operatorname{im} f$ με $(m, ra) = (m', r'a)$, τότε $m = m' \in \ker f$ και $ra = r'a \in \operatorname{im} f = \langle a \rangle \subseteq R$.

Συνεπώς, $r = r' \in R$ άρα $m + rm_a = m' + r'm_a$.

Η λ είναι ομομορφισμός R-προτύπων. Έστω $(m, ra), (m', r'a) \in \ker f \oplus \operatorname{im} f$, $k \in R$. Τότε

$$\begin{aligned}
\lambda[(m, ra) + (m', r'a)] &= \lambda[(m + m', ra + r'a)] \\
&= \lambda[(m + m', (r + r')a] \\
&= m + m' + (r + r')m_a \\
&= m + m' + rm_a + r'm_a \\
&= (m + rm_a) + (m' + r'm_a) \\
&= \lambda(m, ra) + \lambda(m', r'a)
\end{aligned}$$

και

$$\begin{aligned}
\lambda[k(m, ra)] &= \lambda(km, kra) \\
&= km + krm_a \\
&= k(rm + rm_a) \\
&= k\lambda(m, ra)
\end{aligned}$$

Η λ είναι 1-1. Έστω $(m, ra), (m', r'a) \in \ker f \oplus \operatorname{im} f$ με $\lambda(m, ra) = \lambda(m', r'a)$. Τότε, $m + rm_a = m' + r'm_a$ άρα $f(m + rm_a) = f(m' + rm_a) \in R$ και $ra = r'a$, οπότε $r = r'$, $m = m'$. Συνεπώς, $(m, ra) = (m', r'a) \in \ker f \oplus \operatorname{im} f$.

Η λ είναι επί. Έστω $m \in M$. Τότε, $f(m) \in imf = \langle a \rangle$ άρα $f(m) = ra$. Θεωρούμε το στοιχείο $m - rm_a \in M$ και παρατηρούμε ότι $f(m - rm_a) = f(m) - rf(m_a) = ra - ra = 0$, άρα $m - rm_a \in \ker f$. Έτσι ορίζεται $(m - rm_a, f(m)) \in \ker f \oplus imf$ με

$$\lambda(m - rm_a, f(m)) = \lambda(m - rm_a, ra) = m - rm_a + rm_a = m$$

□

Πρόταση 3.1.4. *Έστω R ΠΚΙ, $n \in \mathbb{N}$ και $M \subseteq R^n$ ένα R-υποπρότυπο. Τότε, υπάρχει $k \leq n$ ώστε $M \simeq R^k$.*

Απόδειξη. Υποθέτουμε ότι το ζητούμενο ισχύει για το $n \in \mathbb{N}$ και θα δείξουμε ότι κάθε R-υποπρότυπο $M \subseteq R^{n+1}$ είναι ισόμορφο με το R^k, για κάποιο $k \leq n+1$. Θεωρούμε την απεικόνιση $f : M \to R$

$$M \xrightarrow{i} R^{n+1} = R^n \oplus R \xrightarrow{\pi_{n+1}} R$$

$$f(r_1, r_2, \ldots, r_n, r_{n+1}) = r_{n+1}, \quad \forall (r_1, r_2, \ldots, r_n, r_{n+1}) \in M \subseteq R^{n+1}$$

Η f είναι ομομορφισμός R-προτύπων. Έστω $(r_1, r_2, \ldots, r_n, r_{n+1}), (r'_1, r'_2, \ldots, r'_n, r'_{n+1}) \in M$, $r \in R$. Υπολογίζουμε

$$\begin{aligned} &f[(r_1, r_2, \ldots, r_n, r_{n+1}) + (r'_1, r'_2, \ldots, r'_n, r'_{n+1}) \\ &= (r_1 + r'_1, r_2 + r'_2, \ldots, r_n + r'_n, r_{n+1} + r'_{n+1}) \\ &= r_{n+1} + r'_{n+1} \\ &= f(r_1, r_2, \ldots, r_n, r_{n+1}) + f(r'_1, r'_2, \ldots, r'_n, r'_{n+1}) \end{aligned}$$

και

$$\begin{aligned} f[r(r_1, r_2, \ldots, r_n, r_{n+1})] &= f(rr_1, rr_2, \ldots, rr_n, rr_{n+1}) \\ &= rr_{n+1} \\ &= rf(r_1, r_2, \ldots, r_n, r_{n+1}) \end{aligned}$$

Συνεπώς, από το Λήμμα 3.1.1 έπεται ότι υπάρχει ισομορφισμός

$$M \simeq \ker f \oplus \operatorname{im} f$$

Επίσης,

$$\begin{aligned} \ker f &= \{(r_1, r_2, \ldots, r_n, r_{n+1}) \in M : r_{n+1} = 0 \in R\} \\ &= \{(r_1, r_2, \ldots, r_n, 0) \in R^{n+1} : (r_1, r_2, \ldots, r_n, 0) \in M\} \\ &= M \cap \{(r_1, r_2, \ldots, r_n, 0) : r_1, r_2, \ldots, r_n \in R^n\} \\ &= M \cap R^n \end{aligned}$$

Έπεται ότι ο $\ker f$ είναι ένα υποπρότυπο του R^n.

Άρα, από την επαγωγική υπόθεση, $\ker f \simeq R^k$, για κάποιο $k \in \mathbb{N}$. Καθώς η εικόνα $\operatorname{im} f \subseteq R$ είναι ένα ιδεώδες, $\operatorname{im} f = 0$ ή $\operatorname{im} f = \langle a \rangle$, για κάποιο $a \in R^*$.

Αν $\operatorname{im} f = \langle a \rangle$, για κάποιο $a \in R^*$, τότε η απεικόνιση

$$\mu : R \to \operatorname{im} f, \quad \mu(r) = ra, \quad \forall r \in R$$

είναι ισομορφισμός R-προτύπων. Έτσι, $\operatorname{im} f \simeq R^{k'}$, με $k' \leq 1$. Τελικά,

$$M \simeq \ker f \oplus \operatorname{im} f \simeq R^k \oplus R^{k'} = R^{k+k'}, \quad k + k' \leq n+1$$

□

Πόρισμα 3.1.1. *Έστω R μια ΠΚΙ και M ένα πεπερασμένα παραγόμενο και ελεύθερο R-πρότυπο. Αν $N \subseteq M$ είναι ένα R-υποπρότυπο του M, τότε το N είναι επίσης πεπερασμένα παραγόμενα και ελεύθερο.*

Απόδειξη. Γνωρίζουμε ότι υπάρχει $n \in \mathbb{N}$ ώστε $M \simeq R^n$. Συνεπώς υπάρχει $k \in \mathbb{N}$, $k \leq n$ με $N' \simeq R^k$.

Τότε, όμως, $N \simeq N' \simeq R^k$ και έτσι το N είναι πεπερασμένα παραγόμενο και ελεύθερο.

□

3.2 Κανονική Μορφή Smith

Δύο πίνακες $A, B \in R^{n\times m}$ καλούνται ισοδύναμοι αν υπάρχουν αντιστρέψιμοι πίνακες $P \in R^{n\times n}, Q \in R^{m\times m}$ με $B = PAQ$.

Η ισοδυναμία πινάκων είναι μιά σχέση διάταξης:

(α) Αν $A \in R^{n\times m}$, τότε $A = I_n A I_m$ και άρα ο A είναι ισοδύναμος με τον εαυτό του.

(β) Αν $A, B \in R^{n\times m}$ και $B = PAQ$, για κάποιους αντιστρέψιμους πίνακες $P \in R^{n\times n}, Q \in R^{m\times m}$, τότε $A = P^{-1}BQ^{-1}$, και άρα ο B είναι ισοδύναμος με τον A.

(γ) Αν $A, B, C \in R^{n\times m}$ και $B = PAQ$ και $C = P'BQ'$, για κάποιους αντιστρέψιμους πίνακες $P, P' \in R^{n\times n}, Q, Q' \in R^{m\times m}$, τότε $C = (P'P)A(QQ')$ και άρα, καθώς οι πίνακες $P'P \in R^{n\times n}$ και $QQ' \in R^{m\times m}$ είναι αντιστρέψιμοι, ο A είναι ισοδύναμος με τον C.

Εναλλακτικά, δύο πίνακες $A, B \in R^{n\times m}$ είναι ισοδύναμοι ανν υπάρχει R-γραμμική απεικόνιση, δηλαδή ομομορφισμός R-προτύπων, $f : R^m \to R^n$ και διατεταγμένες βάσεις $\widehat{u}$ του R^m και $\widehat{v}$ του R^n ώστε $A = (f : \widehat{e}_m, \widehat{e}_n)$ και $B = (f : \widehat{u}, \widehat{v})$.

Πράγματι, ας υποθέσουμε ότι υπάρχουν αντιστρέψιμοι πίνακες $P \in R^{n\times n}, Q \in R^{m\times m}$ ώστε $B = PAQ$. Θεωρούμε την γραμμική απεικόνιση $f : R^m \to R^n$ με $(f : \widehat{e}_m, \widehat{e}_n) = A$ και τις διατεταγμένες βάσεις $\widehat{u}$ και $\widehat{v}$ των R^m και R^n αντίστοιχα με $P = (I_{d_{R^m}} : \widehat{e}_n, \widehat{v})$ και $Q = (I_{d_{R^m}} : \widehat{u}, \widehat{e}_m)$. Τότε υπολογίζουμε

$$\begin{aligned} B &= PAQ \\ &= (I_{d_{R^m}} : \widehat{e}_n, \widehat{v})(f : \widehat{e}_m, \widehat{e}_n)(I_{d_{R^m}} : \widehat{u}, \widehat{e}_m) \\ &= (I_{d_{R^m}} \circ f \circ I_{d_{R^n}} : \widehat{u}, \widehat{v}) \\ &= (f : \widehat{u}, \widehat{v}) \end{aligned}$$

Αντίστροφα, γνωρίζουμε ότι οι πίνακες μιας R-γραμμικής απεικόνισης $f : R^m \to R^n$ ως προς διαφορετικές επιλογές διατεταγμένων βάσεων των R^m και R^m αντίστοιχα είναι ισοδύναμοι.

Παρατηρήσεις 3.2.1. (i) Για κάθε πίνακα $A = (a_{ij})_{ij} \in R^{n\times m}$, θεωρούμε το ιδεώδες

$$I(A) = (a_{11}, a_{12}, \ldots, a_{1n}, a_{21}, a_{22}, \ldots) \subseteq R$$

Αν οι πίνακες $A, B \in R^{n\times m}$ είναι ισοδύναμοι, τότε $I(A) = I(B)$.

Γνωρίζουμε ότι υπάρχουν αντιστρέψιμοι πίνακες $P \in R^{n\times n}, Q \in R^{m\times m}$ ώστε $B = PAQ$. Τότε για κάθε (ij) είναι $b_{ij} \in I(A)$ και άρα $I(B) \subseteq I(A)$.

Λόγω συμμετρίας έπεται ότι $I(A) \subseteq I(B)$ άρα $I(A) = I(B)$.

(ii) Για κάθε $i, j \in \{1, 2, \ldots, n\}$ με $i \neq j$ θεωρούμε τον πίνακα H_{ij} ο οποίος προκύπτει από τον I_n εναλλάσοντας την i-γραμμή με την j-γραμμή.

Για κάθε $i \in \{1, 2, \ldots, n\}, u \in U(R)$ θεωρούμε τον πίνακα $D_i(u)$ ο οποίος προκύπτει από τον I_n πολλαπλασιάζοντας την i-γραμμή με u.

Για κάθε $i, j \in \{1, 2, \ldots, n\}$ με $i \neq j$ και $a \in R$ θεωρούμε τον πίνακα $A_{ij}(a)$ ο οποίος προκύπτει από τον I_n προσθέτοντας το a-πλάσιο της i-γραμμής στην i-γραμμή.

Οι παραπάνω πίνακες είναι αντιστρέψιμοι με

$$H_{ij}^{-1} = H_{ij}, \quad D_i(u)^{-1} = D_i(u^{-1}), \quad A_{ij}(a)^{-1} = A_{ij}(-a)$$

Συνεπώς για κάθε πίνακα $A \in R^{n\times m}$, μπορούμε να βρούμε ισοδύναμούς του πίνακες, τους εξής:

(α) $H_{ij} \cdot A$: ο πίνακας που προκύπτει από τον A εναλλάσοντας την i-γραμμή με την j-γραμμή.

(β) $D_i(u) \cdot A$: ο πίνακας που προκύπτει από τον A πολλαπλασιάζοντας την i-γραμμή με u.

(γ) $A_{ij}(a) \cdot A$: ο πίνακας που προκύπτει από τον A προσθέτοντας το a-πλάσιο της i-γραμμής στην i-γραμμή.

Συνεπώς μπορώ να βρω ισοδύναμους πίνακες του A εφαρμόζοντας στον A "πράξεις γραμμών".

Αντίστοιχα, πολλαπλασιάζοντας τον A από τα δεξιά με τους στοιχειώδεις πίνακες $H_{ij}, D_i(u), A_{ij}(a)$ μπορώ να βρω ισοδύναμους πίνακες του A εφαρμόζοντας σε αυτόν "πράξεις στηλών".

(iii) Έστω R μια ΠΚΙ και $a, b \in R, a, b \neq 0$ με $\delta = \text{μκδ}(a, b)$.

Τότε $\begin{pmatrix} a & b \\ * & * \end{pmatrix} \backsim \begin{pmatrix} \delta & 0 \\ * & * \end{pmatrix}$ και $\begin{pmatrix} a & * \\ b & * \end{pmatrix} \backsim \begin{pmatrix} \delta & * \\ 0 & * \end{pmatrix}$.

Υπάρχουν $x, y \in R$ ώστε $\delta = ax + by$. Μπορούμε να γράψουμε $a = \delta a', b = \delta b'$, οπότε $\delta = \delta a'x + \delta b'y$ και άρα $a'x + b'y = 1$. Θεωρούμε τον πίνακα $Q = \left(\begin{smallmatrix} x & -b' \\ y & a' \end{smallmatrix}\right)$ και παρατηρούμε ότι είναι αντιστρέψιμος, με $Q^{-1} = \left(\begin{smallmatrix} a' & b' \\ -y & x \end{smallmatrix}\right)$, και

$$\begin{pmatrix} a & b \\ * & * \end{pmatrix} \begin{pmatrix} x & -b' \\ y & a \end{pmatrix} = \begin{pmatrix} ax + by & -ab' + a'b \\ * & * \end{pmatrix} = \begin{pmatrix} \delta & 0 \\ * & * \end{pmatrix}$$

Ανάλογα, θεωρούμε τον αντιστρέψιμο πίνακα $P = \left(\begin{smallmatrix} x & y \\ b' & a' \end{smallmatrix}\right)$ και παρατηρούμε ότι

$$\begin{pmatrix} x & y \\ b' & -a' \end{pmatrix} \begin{pmatrix} a & * \\ b & * \end{pmatrix} = \begin{pmatrix} \delta & * \\ 0 & * \end{pmatrix}$$

Θεώρημα 3.2.1 (Κανονική Μορφή Smith). *Έστω R μια ΠΚΙ και $A \in R^{n\times m}$. Τότε ο A είναι ισοδύναμος με έναν πίνακα της μορφής* $\begin{pmatrix} d_1 & & \\ & d_2 & \\ & & \ddots \end{pmatrix}$, *για κάποια $d_1, d_2, \ldots \in R$, με $d_1|d_2, d_2|d_3, \ldots$*

Απόδειξη. Γράφουμε $A = (a_{ij})$ και υποθέτουμε ότι $a_{11} \neq 0$. Θεωρούμε την απεικόνιση $\lambda : R^* \to \mathbb{N}$, με $\lambda(r) = n$ αν το $r \in R^*$ είναι γινόμενο n το πλήθος αναγώγων στοιχείων. Χρησιμοποιώντας επαγωγή στο $\lambda(a_{11})$ θα δείξουμε ότι ο A είναι ισοδύναμος με έναν πίνακα της μορφής

$$\left(\begin{array}{c|c} c & 0\cdots 0 \\ \hline 0 & \\ \vdots & \mathrm{B} \\ 0 & \end{array}\right)$$

για κάποιον $B \in R^{(n-1)\times(m-1)}$, ώστε $c|b$ για κάθε εγγραφή b του B. Αν $\lambda(a_{11}) = 0$, τότε $a_{11} \in U(R)$. Εφαρμόζοντας κατάλληλες πράξεις στηλών μπορούμε να υποθέσουμε ότι $a_{12} =$

$a_{13} = \cdots = 0$. Όμοια, εφαρμόζοντας κατάλληλες γραμμοπράξεις μπορούμε να υποθέσουμε ότι $a_{21} = a_{31} = \cdots = 0$. Καθώς $a \in U(R)$ έπεται ότι το a_{11} διαιρεί κάθε εγγραφή b του πίνακα-"υπόλοιπο" B.

Υποθέτουμε ότι $\lambda(a_{11}) > 0$ και ότι η ζητούμενη αναγωγή είναι δυνατή για πίνακες με $< \lambda(a_{11})$. Αν $a_{11}|a_{ij}$ για κάθε i, j, τότε μπορούμε όπως πριν να προχωρήσουμε βρίσκοντας έναν πίνακα ισοδύναμο με τον A της μορφής

$$\left(\begin{array}{c|c} a_{11} & 0\cdots 0 \\ \hline \begin{matrix}0\\ \vdots \\ 0\end{matrix} & \text{B} \end{array}\right)$$

όπου $a_{11}|b$ για κάθε εγγραφή b του πίνακα B.

Αν υπάρχουν (ij) ώστε $a_{11} \nmid a_{ij}$, υποθέτουμε ότι $i = 1, j = 2$. Θεωρούμε $\delta = \text{μκδ}(a_{11}, a_{12})$ και παρατηρουμε ότι $\delta|a_{11}$, αλλά $a_{11} \nmid \delta$, συνεπώς $\lambda(\delta) < \lambda(a_{11})$. Μπορούμε να πολλαπλασιάσουμε τον A από τα δεξιά με έναν πίνακα της μορφής

$$P = \left(\begin{array}{cc|c} x & y & \mathbb{O} \\ a & b & \\ \hline \multicolumn{2}{c|}{\mathbb{O}} & \text{I} \end{array}\right)$$

έτσι ώστε $bx + ay = 1$ και

$$AP = \begin{pmatrix} \delta & 0 & * & \dots & * \\ * & * & * & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \dots & * \end{pmatrix}$$

Τότε, όμως, ο A είναι ισοδύναμος με τον AP και $\lambda(\delta) < \lambda(a_{11})$.

Τελειώνουμε χρησιμοποιώντας την επαγωγική υπόθεση. Μπορούμε να βρούμε αντιστρέψιμους πίνακες $P \in R^{n\times n}, Q \in R^{m\times m}$, με

$$PAQ = \left(\begin{array}{c|c} c & 0\cdots 0 \\ \hline \begin{matrix}0\\ \vdots \\ 0\end{matrix} & \text{B} \end{array}\right)$$

για κάποιον $B \in R^{(n-1)\times(m-1)}$, έτσι ώστε $c|b$ για κάθε εγγραφή b του B.

Χρησιμοποιώντας επαγωγή στη διάσταση του πίνακα, $n + m$, μπορούμε να βρούμε αντιστρέψιμους πίνακες $P' \in R^{(n-1)\times(n-1)}, Q' \in R^{(m-1)\times(m-1}$, έτσι ώστε

$$P'BQ' = \begin{pmatrix} d_1 & & \\ & d_2 & \\ & & \ddots \end{pmatrix}$$

για κάποια $d_1, d_2, \ldots \in R$ με $d_1|d_2, d_2|d_3, \ldots$

Παρατηρούμε ότι $c|d_1$ και οι

$$\left(\begin{array}{c|c} 1 & 0\cdots 0 \\ \hline \begin{matrix}0\\ \vdots \\ 0\end{matrix} & \text{P'} \end{array}\right) \in R^{n\times m}, \left(\begin{array}{c|c} 1 & 0\cdots 0 \\ \hline \begin{matrix}0\\ \vdots \\ 0\end{matrix} & \text{Q'} \end{array}\right) \in R^{m\times m}$$

είναι αντιστρέψιμοι.
Έπεται ότι ο A είναι ισοδύναμος με τον

$$\begin{pmatrix} 1 & \mathbb{O} \\ \mathbb{O} & P' \end{pmatrix} PAQ \begin{pmatrix} 1 & \mathbb{O} \\ \mathbb{O} & Q' \end{pmatrix} = \begin{pmatrix} 1 & \mathbb{O} \\ \mathbb{O} & P' \end{pmatrix} \begin{pmatrix} c & \mathbb{O} \\ \mathbb{O} & B \end{pmatrix} \begin{pmatrix} 1 & \mathbb{O} \\ \mathbb{O} & Q' \end{pmatrix}$$
$$= \begin{pmatrix} 1 \cdot c \cdot 1 & \mathbb{O} \\ \mathbb{O} & P'BQ' \end{pmatrix}$$
$$= \begin{pmatrix} c & & \mathbb{O} & \\ & d_1 & & \\ \mathbb{O} & & d_2 & \\ & & & \ddots \end{pmatrix}$$

□

Παραδείγματα 3.2.1. (i) Έστω $R = \mathbb{Z}$. Τότε

$$\begin{pmatrix} 14 & 10 & -2 \\ 3 & 2 & 1 \\ 17 & 10 & 13 \\ 7 & 4 & 9 \end{pmatrix} \sim \begin{pmatrix} 3 & 2 & 1 \\ 14 & 10 & -2 \\ 17 & 10 & 13 \\ 7 & 4 & 9 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ -2 & 10 & 14 \\ 13 & 10 & 17 \\ 9 & 4 & 7 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 14 & 20 \\ 0 & -16 & -22 \\ 0 & -14 & -20 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 14 & 20 \\ 0 & -16 & -22 \\ 0 & -14 & -20 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & -4 & 6 \\ 0 & -2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Με βάση τη γενική θεωρία, η πέμπτη ισοδυναμία παραπάνω προκύπτει πολλαπλασιάζοντας από τα δεξιά με τον πίνακα

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & -10 \\ 0 & -2 & 7 \end{pmatrix} \in SL_3(\mathbb{Z})$$

Πράγματι, έχουμε $\text{μκδ}(14, 20) = 2 = 14 \cdot 3 + 20 \cdot (-2) \in \mathbb{Z}$ και $1 = 7 \cdot 3 + 10 \cdot (-2)$.

(ii) Έστω $R = \mathbb{Q}[x]$. Τότε

$$\begin{pmatrix} x+2 & 2 & -6 \\ 1 & x & -3 \\ 1 & 1 & x-4 \end{pmatrix} \sim \begin{pmatrix} 1 & x & -3 \\ x+2 & 2 & -6 \\ 1 & 1 & x-4 \end{pmatrix} \sim \begin{pmatrix} 1 & x & -3 \\ 0 & -x^2-2x+2 & 3x \\ 0 & -x+1 & x-1 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -x^2-2x+2 & 3x \\ 0 & -x+1 & x-1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3x & -x^2-2x+2 \\ 0 & x-1 & -x+1 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\frac{1}{3}x^2+\frac{1}{3}x-\frac{1}{3} \\ 0 & 0 & x^3-2x^2-x+2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^3-2x^2-x+2 \end{pmatrix}$$

Με βάση τη γενική θεωρία, η πέμπτη ισοδυναμία παραπάνω προκύπτει πολλαπλασιάζοντας από τα αριστερά με τον πίνακα

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{3} & -1 \\ 0 & -x+1 & 3x \end{pmatrix} \in SL_3(\mathbb{Q}[x])$$

Πράγματι, έχουμε μκδ$(3x, x-1) = 1 = 3x \cdot \frac{1}{3} + (x-1)\cdot(-1) \in \mathbb{Q}[x]$.

(iii) Έστω $R = \mathbb{Z}[i]$. Τότε

$$\begin{pmatrix} 4+4i & -2+2i & 4i \\ -14-2i & 8 & 1-i \\ 4-4i & 2+4i & 4+2i \end{pmatrix} \sim \begin{pmatrix} -14-2i & 8 & 1-i \\ 4+4i & -2+2i & 4i \\ 4-4i & 2+4i & 4+2i \end{pmatrix} \sim \begin{pmatrix} 1-i & 8 & -14-2i \\ 4i & -2+2i & 4+4i \\ 4+2i & 2+4i & 4-4i \end{pmatrix}$$
$$\sim \begin{pmatrix} 1-i & 8 & -14-2i \\ 0 & 14-14i & -28+28i \\ 0 & -6-20i & 12+40i \end{pmatrix} \sim \begin{pmatrix} 1-i & 0 & 0 \\ 0 & 14-14i & -28+28i \\ 0 & -6-20i & 12+40i \end{pmatrix}$$
$$\sim \begin{pmatrix} 1-i & 0 & 0 \\ 0 & -6-20i & 12+40i \\ 0 & 14-14i & -28+28i \end{pmatrix} \sim \begin{pmatrix} 1-i & 0 & 0 \\ 0 & 2 & -4 \\ 0 & 0 & 0 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1-i & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Με βάση τη γενική θεωρία, η έκτη ισοδυναμία παραπάνω προκύπτει πολλαπλασιάζοντας από τα αριστερά με τον πίνακα

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -6-i & 4-5i \\ 0 & -7+7i & -3-10i \end{pmatrix} \in SL_3(\mathbb{Z}[i])$$

Πράγματι, έχουμε μκδ$(-6-20i, 14-14i) = 2 = (-6-20i)\cdot(-6-i)+(14-14i)\cdot(4-5i) \in \mathbb{Z}[i]$ και $1 = (-3-10i)\cdot(-6-i)+(7-7i)\cdot(4-5i)$.

Πρόταση 3.2.1. *Έστω R μια ΠΚΙ, F ένα πεπερασμένα παραγόμενο και ελεύθερο R-πρότυπο και $M \subseteq N$ ένα υποπρότυπο. Τότε υπάρχουν $k, n \in \mathbb{N}$, με $k \leq n$ και κατάλληλες βάσεις $u_1, u_2, \ldots, u_k$ του M, $v_1, v_2, \ldots, v_n$ του F, έτσι ώστε $u_1 = d_1v_1, u_2 = d_2v_2, \ldots, u_k = d_kv_k$, για κάποια $d_1, d_2, \ldots, d_k \in R$ με $d_1|d_2, d_2|d_3, \ldots, d_{k-1}|d_k$.*

Απόδειξη. Έστω $\widehat{v}' = (v_1', v_2', \ldots, v_k')$ μια διατεταγμένη βάση του F.

Γνωρίζουμε ότι το υποπρότυπο $M \subseteq F$ είναι επίσης πεπερασμένα παραγόμενο και ελεύθερο και μάλιστα έχει μια βάση με k στοιχεία, για κάποιο $k \in \mathbb{N}$. Έστω $\widehat{u} = (u_1', u_2', \ldots, u_k')$ μια διατεταγμένη βάση του M.

Θεωρούμε τη γραμμική απεικόνιση $i : M \to F$, με $i(m) = m$ για κάθε $m \in M$. Θεωρούμε τον πίνακα $A = (i : \widehat{u}', \widehat{v}') \in R^{n\times k}$. Γνωρίζουμε ότι ο A είναι ισοδύναμος με έναν πίνακα της μορφής

$$\left(\begin{array}{ccc} d_1 & & \\ & d_2 & \\ & & \ddots \\ & & d_k \\ \hline \multicolumn{3}{c}{\mathbb{O}} \end{array}\right)$$

για κάποιους $d_1, d_2, \ldots, d_k \in R$ με $d_1|d_2, d_2|d_3, \ldots, d_{k-1}|d_k$.

Καθώς ισοδύναμοι πίνακες παριστάνουν την ίδια απεικόνιση ως προς κατάλληλες επιλογές βάσεων, υπάρχουν διατεταγμένες βάσεις $\widehat{u} = (u_1, u_2, \ldots, u_k)$ του M, και $\widehat{v} = (v_1, v_2, \ldots, v_n)$ του F ώστε $(i : \widehat{u}, \widehat{v}) = B$. Τότε $u_1 = i(u_1) = d_1 v_1, u_2 = d_2 v_2, \ldots, u_k = d_k v_k$. □

3.3 Ασκήσεις

1.

Κεφάλαιο 4

Θεωρήματα Δομής

4.1 Μηδενιστής και τάξη

Ορισμός 4.1.1. Έστω R δακτύλιος και M ένα R-πρότυπο. Θεωρούμε το υποσύνολο $\operatorname{ann}_R M \subseteq R$, το οποίο ονομάζουμε **μηδενιστή** του R-προτύπου M, με

$$\operatorname{ann}_R M = \{r \in R : rm = 0 \in M, \quad \forall m \in M\}$$

Παρατηρήσεις 4.1.1. (i) Ο μηδενιστής $\operatorname{ann}_R M$ κάθε R-προτύπου M είναι ένα ιδεώδες του R.

Πράγματι, θεωρούμε τον ομομορφισμό δακτυλίων

$$\rho : R \to \operatorname{End}(M, +)$$

με $\rho(r) = rm$ για κάθε $r \in R$, $m \in m$ και παρατηρουμε ότι $\operatorname{ann}_R M = \ker \rho$.

(ii) Έστω M, N δύο R-πρότυπα και $M \oplus N$ το ευθύ τους άθροισμα. Τότε

$$\operatorname{ann}_R(M \oplus N) = \operatorname{ann}_R M \cap \operatorname{ann}_R N$$

Αν $r \in R$, τότε

$$\begin{aligned} r \in \operatorname{ann}_R(M \oplus N) &\Leftrightarrow r(m, n) = (0, 0), \quad \forall (m, n) \in M \oplus N \\ &\Leftrightarrow (rm, rn) = (0, 0), \quad \forall (m, n) \in M \oplus N \\ &\Leftrightarrow rm = 0, \quad \forall m \in M \text{ και } rn = 0 \quad \forall n \in N \\ &\Leftrightarrow r \in \operatorname{ann}_R M \cap \operatorname{ann}_R N \end{aligned}$$

Ορισμός 4.1.2. Έστω R μια ΠΚΙ και M ένα R-πρότυπο. Τότε υπάρχει $r \in R$ τέτοιο ώστε $\operatorname{ann}_R M = (r)$. Λέμε ότι το r είναι μια **τάξη** του M και γράφουμε $r = o(M)$.

Παρατηρήσεις 4.1.2. (i) Αν r μια τάξη του R-προτύπου M, όπου R ΠΚΙ, τότε κάθε συντροφικό στοιχείο του r είναι επίσης μια τάξη του M.

(ii) Αν M είναι μια κυκλική ομάδα $M = \langle m_0 \rangle$, $M = \mathbb{Z}m_0$, τότε η τάξη του M (όπως ορίστηκε παραπάνω) συμπίπτει με την τάξη του στοιχείου m_0 (όπως αυτή ορίζεται στη Θεωρία Ομάδων).

(iii) Έστω $\mathbb{F}$ ένα σώμα, V ένα $\mathbb{F}$-διανυσματικός χώρος με $\dim_{\mathbb{F}} V < \infty$ και ϕ μια $\mathbb{F}$-γραμμική απεικόνιση.

Θεωρούμε τον V ως $\mathbb{F}[x]$-πρότυπο κατά τα γνωστά.

Τότε η τάξη του $\mathbb{F}[x]$-προτύπου είναι το ελάχιστο πολυώνυμο $\mu_\phi(x) \in \mathbb{F}[x]$ της γραμμικής απεικόνισης ϕ.

Πράγματι,

$$\begin{aligned}\operatorname{ann}_{\mathbb{F}[x]} V &= \{f(x) \in \mathbb{F}[x] : f(x)v = 0, \quad \forall v \in V\} \\ &= \{f(x) \in \mathbb{F}[x] : [f(\phi)](v) = 0, \quad \forall v \in V\} \\ &= \{f(x) \in \mathbb{F}[x] : f(\phi) = 0 : V \to V\} \\ &= \mu_\phi(x)\end{aligned}$$

Πρόταση 4.1.1. *Έστω R μεταθετικός δακτύλιος και M ένα κυκλικό R-πρότυπο. Τότε υπάρχει ισομορφισμός R-προτύπων $M \simeq R/\operatorname{ann}_R M$.*

Απόδειξη. Υπάρχει $m_0 \in M$ με $M = \langle m_0 \rangle = Rm_0$. Θεωρούμε την απεικόνιση

$$f : R \to M, \quad f(r) = rm_0, \quad \forall r \in R$$

Η f είναι ομομορφισμός R-προτύπων. Αν $r, r_1, r_2 \in R$, τότε

$$\begin{aligned}f(r_1 + r_2) &= (r_1 + r_2)m_0 \\ &= r_1 m_0 + r_2 m_0 \\ &= f(r_1) + f(r_2)\end{aligned}$$

και

$$\begin{aligned}f(rr_1) &= (rr_1)m_0 \\ &= r(r_1 m_0) \\ &= rf(r_1)\end{aligned}$$

Η f είναι προφανώς επί, γιατί $M = \langle m_0 \rangle$.

Επιπλέον $\ker f = \operatorname{ann}_R M$. Αν $r \in \ker f$, τότε $rm_0 = f(r) = 0 \in M$. Αν τώρα $m \in M$, έχουμε $m = km_0$, για κάποιο $k \in R$. Τότε $rm = rkm_0 = (rk)m_0 = krm_0 = k0 = 0 \in M$ άρα $r \in \operatorname{ann}_R M$.

Αντίστροφα, έστω $r \in \operatorname{ann}_R M$. Τότε $rm = 0 \in M$ για κάθε $m \in M$. Ειδικότερα $rm_0 = 0 \in M$ άρα $r \in \ker f$.

Έτσι, από το 1ο Θεώρημα Ισομορφισμών προτύπων υπάρχει ισομορφισμός

$$R/\operatorname{ann}_R M = R/\ker f \simeq \operatorname{im} f = M$$

□

Πόρισμα 4.1.1. *Έστω R μια ΠΚΙ και M ένα κυκλικό R-πρότυπο. Τότε υπάρχει ισομορφισμός $M \simeq R/(r)$, όπου r είναι μιά τάξη του M.*

Παρατηρήσεις 4.1.3. (i) Έστω $f : M \to N$ ένας ισομορφισμός R-προτύπων. Υποθέτουμε ότι υπάρχουν R-υποπρότυπα $M_1, M_2 \subseteq M$ ώστε η γραμμική απεικόνιση

$$a : M_1 \oplus M_2 \to M, \quad (x_1, x_2) \mapsto x_1 + x_2$$

είναι ισομορφισμός.

Θεωρούμε τα υποπρότυπα $N_1, N_2 \subseteq N$, με $N_1 = f(M_1), N_2 = f(M_2)$. Τότε η απεικόνιση

$$b : N_1 \oplus N_2 \to N, \quad (y_1, y_2) \mapsto y_1 + y_2$$

είναι επίσης ισομορφισμός.

Μπορούμε να θεωρήσουμε τους ισομορφισμούς R-προτύπων $f_1 = f|_{M_1} : M_1 \to N_1, f_2 = f|_{M_2} : M_2 \to N_2$ και έτσι έχουμε το μεταθετικό τετράγωνο:

$$\begin{array}{ccc} M_1 \oplus M_2 & \xrightarrow{\text{a}} & M \\ \Big\downarrow{\scriptstyle f_1 \oplus f_2} & & \Big\downarrow{\scriptstyle \text{f}} \\ N_1 \oplus N_2 & \xrightarrow{\text{b}} & N \end{array}$$

Συνεπώς η b είναι η σύνθεση των ισομορφισμών $(f_1 \oplus f_2), a$ και f, άρα η b είναι ισομορφισμός.

(ii) Έστω M ένα R-πρότυπο και $m_1, m_2, \ldots, m_n$ μια βάση του. Τότε η απεικόνιση

$$\langle m_1 \rangle \oplus \langle m_2 \rangle \oplus \cdots \oplus \langle m_n \rangle \to M$$

με

$$(r_1 m_1, r_2 m_2, \ldots, r_n m_n) \mapsto \sum_{i=1}^{n} r_i m_i$$

είναι ισομορφισμός R-προτύπων.

Γνωρίζουμε ότι η απεικόνιση

$$I : R^n \to M, \quad f(r_1, r_2, \ldots, r_n) = \sum_{i=1}^{n} r_i m_i$$

είναι ισομορφισμός προτύπων.

Είναι επίσης προφανές ότι για την κανονική βάση $e_1, e_2, \ldots, e_n$ του R^n η απεικόνιση

$$\langle e_1 \rangle \oplus \langle e_2 \rangle \oplus \cdots \oplus \langle e_n \rangle \to R^n$$

με

$$(r_1 e_1, r_2 e_2, \ldots, r_n e_n) \mapsto (r_1, r_2, \ldots, r_n)$$

είναι ισομορφισμός.

Καθώς $\langle m_i \rangle = \langle f(e_i) \rangle = f(\langle e_i \rangle)$, το ζητούμενο έπεται από την παρατήρηση (i).

(iii) Γνωρίζουμε ότι αν $M_1, M_2, \ldots, M_n$ είναι R-πρότυπα και $N_1 \subseteq M_1, N_2 \subseteq M_2, \ldots, N_n \subseteq M_n$ είναι R-υποπρότυπα, τότε το $\bigoplus_{i=1}^{n} N_i$ είναι ένα R-υποπρότυπο του $\bigoplus_{i=1}^{n} M_i$ και υπάρχει ισομορφισμός

$$\bigoplus_{i=1}^{n} M_i / \bigoplus_{i=1}^{n} N_i \simeq \bigoplus_{i=1}^{n} (M_i / N_i)$$

4.2 Θεώρημα Δομής Ι

Θεώρημα 4.2.1. *Έστω R μια ΠΚΙ και M ένα πεπερασμένα παραγόμενο R-πρότυπο. Τότε υπάρχουν μη-μηδενικά κυκλικά υποπρότυπα $M_1, M_2, \ldots, M_n \subseteq M$ ώστε:*

(i) $M \simeq M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

(ii) $R \supseteq \operatorname{ann} M_1 \supseteq \operatorname{ann} M_2 \supseteq \ldots \supseteq \operatorname{ann} M_n$.

(ii) Αν $\operatorname{ann} M_i = (d_i)$ *για κάποιο* $d_i \in R \backslash U(R)$, *τότε* $d_1 | d_2, d_2 | d_3, \ldots, d_{n-1} | d_n$.

Απόδειξη. Καθώς το M είναι πεπερασμένα παραγόμενο, γνωρίζουμε ότι υπάρχει ισομορφισμός $M \simeq F/K$, για κάποιο πεπερασμένα παραγόμενο και ελεύθερο R-πρότυπο F και κάποιο R-υποπρότυπο $K \subseteq F$.

Καθώς ο R είναι ΠΚΙ, υπάρχουν $k, n \in \mathbb{N}$, $k \leq n$, βάσεις $u_1, u_2, \ldots, u_k$ του K και $v_1, v_2, \ldots, v_n$ του F και στοιχεία $d_1, d_2, \ldots, d_k \in R$ με $u_1 = d_1 v_1, u_2 = d_2 v_2, \ldots, u_k = d_k v_k$ και $d_1 | d_2, d_2 | d_3, \ldots, d_{k-1} | d_k$. Άρα

$$F \simeq \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus \cdots \oplus \langle v_k \rangle \oplus \langle v_{k+1} \rangle \oplus \cdots \oplus \langle v_n \rangle$$

και

$$\begin{aligned} K &\simeq \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \cdots \oplus \langle u_k \rangle \\ &= \langle d_1 v_2 \rangle \oplus \langle d_2 v_2 \rangle \oplus \cdots \oplus \langle d_k v_k \rangle \\ &\simeq \langle d_1 v_2 \rangle \oplus \langle d_2 v_2 \rangle \oplus \cdots \oplus \langle d_k v_k \rangle \oplus 0 \oplus \cdots \oplus 0 \end{aligned}$$

Συνεπώς

$$\begin{aligned} M = F/K &\simeq \frac{\langle v_1 \rangle}{\langle d_1 v_1 \rangle} \oplus \cdots \oplus \frac{\langle v_k \rangle}{\langle d_k v_k \rangle} \oplus \frac{\langle v_{k+1} \rangle}{0} \oplus \cdots \oplus \frac{\langle v_n \rangle}{0} \\ &= \frac{\langle v_1 \rangle}{\langle d_1 v_1 \rangle} \oplus \cdots \oplus \frac{\langle v_k \rangle}{\langle d_k v_k \rangle} \oplus \frac{\langle v_{k+1} \rangle}{\langle 0 v_{k+1}} \rangle \oplus \cdots \oplus \frac{\langle v_n \rangle}{\langle 0 v_n \rangle} \end{aligned}$$

Ορίζουμε $M_1 \subseteq M$ το κυκλικό R-υποπρότυπο που παράγει η εικόνα του V_i. Έτσι

$$M_i \simeq \frac{\langle v_1 \rangle}{\langle d_i v_i \rangle} \simeq \frac{R}{(d_1)}$$

δηλαδή $\operatorname{ann} M_i = (d_i)$. Θέτοντας $d_{k+1} = \cdots = d_n = 0$ έχουμε τελειώσει. □

Πόρισμα 4.2.1. *Έστω G μια πεπερασμένα παραγόμενη αβελιανή ομάδα. Τότε υπάρχουν $n \in \mathbb{N}$ και $d_1, d_2, \ldots, d_n \in \mathbb{Z}$ με $d_1 | d_2, \ldots d_{n-1} | d_n$ και*

$$G \simeq \mathbb{Z}/(d_1) \oplus \mathbb{Z}/(d_2) \oplus \cdots \oplus \mathbb{Z}/(d_n)$$

Σχόλιο 4.2.1. Αν $d_i = \pm 1$, τότε $\mathbb{Z}/(d_i) = \mathbb{Z}/\mathbb{Z} = 0$.

Αν $d_n = 0$, τότε $\mathbb{Z}/(d_n) = \mathbb{Z}/0 = \mathbb{Z}$.

Πόρισμα 4.2.2. *Έστω G μια πεπερασμένη αβελιανή ομάδα. Τότε υπάρχουν μη-μηδενικά στοιχεία $d_1, d_2, \ldots, d_n \in \mathbb{Z}$ με $d_1 | d_2, \ldots, d_{n-1} | d_n$ και*

$$G = \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_n}$$

Σχόλιο 4.2.2. Θα πρέπει $|G| = d_1 d_2 \cdots d_n$.

Παραδείγματα 4.2.1. (i) Έστω G αβελιανή ομάδα με $|G| = 36$. Τότε

$$G \simeq \mathbb{Z}_{36} \,\acute{\eta}\, G \simeq \mathbb{Z}_6 \oplus \mathbb{Z}_6 \,\acute{\eta}\, G \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_{12} \,\acute{\eta}\, G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{18}$$

Ερώτημα: Μήπως η λίστα αυτή των τεσσάρων ομάδων μπορεί να "μικρύνει";

Θα δούμε ότι τα d_i ως προς τη συντροφικότητα είναι μονοσήμαντα ορισμένα και άρα οι ομάδες αυτές δεν είναι ισόμορφες.

(ii) Έστω $A \subseteq \mathbb{Z}^4$ η υποομάδα που παράγεται από τα στοιχεία $(14, 3, 17, 7), (10, 2, 10, 4)$ και $(-2, 1, 13, 9)$. Θεωρούμε, επίσης, την $G = \mathbb{Z}^4/A$.

Ορίζουμε τον πίνακα

$$\begin{pmatrix} 14 & 10 & -2 \\ 3 & 2 & 1 \\ 17 & 10 & 13 \\ 7 & 4 & 9 \end{pmatrix}$$

Γνωρίζουμε ότι ο πίνακας αυτός είναι ισοδύναμος με τον

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Συνεπώς υπάρχει μια βάση u_1, u_2, u_3 της A και μια βάση v_1, v_2, v_3, v_4 της $\mathbb{Z}^4$ ώστε $u_1 = 1v_1, u_2 = 2v_2, u_3 = 6v_3$. Έτσι

$$\mathbb{Z}^4 = \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \mathbb{Z}v_3 \oplus \mathbb{Z}v_4$$

και

$$A = \mathbb{Z}u_1 \oplus \mathbb{Z}u_2 \oplus \mathbb{Z}u_3 = \mathbb{Z}1v_1 \oplus \mathbb{Z}2v_2 \oplus \mathbb{Z}6v_3 \oplus 0$$

Άρα

$$\mathbb{Z}^4/A \simeq \frac{\mathbb{Z}v_1}{\mathbb{Z}1v_1} \oplus \frac{\mathbb{Z}v_2}{\mathbb{Z}2v_2} \oplus \frac{\mathbb{Z}v_3}{\mathbb{Z}6v_3} \oplus \frac{\mathbb{Z}v_4}{0} = 0 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}$$

δηλαδή

$$G \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}$$

Πρόταση 4.2.1. *Έστω $\mathbb{F}$ σώμα με $|\mathbb{F}| < \infty$. Τότε η πολλαπλασιαστική ομάδα $(\mathbb{F}^*, \cdot)$ είναι κυκλική.*

Απόδειξη. Γνωρίζουμε ότι υπάρχουν κυκλικές ομάδες $A_1, A_2, \ldots, A_n$ με τάξεις $d_1, d_2, \ldots, d_n$ αντίστοιχα, ώστε

$$\mathbb{F} \simeq A_1 \oplus A_2 \oplus \cdots \oplus A_n$$

και $d_1 | d_2, \ldots, d_{n-1} | d_n$.

Γνωρίζουμε ότι $\operatorname{ann}_{\mathbb{Z}} \mathbb{F}^* = (d_n)$ και ότι $|\mathbb{F}^*| = d_1 d_2 \cdots d_n$. Τότε $a^{d_n} = 1 \in \mathbb{F}^*$ για κάθε $a \in \mathbb{F}^*$. Όμως το πολυώνυμο $x^{d_n} - 1 \in \mathbb{F}[x]$, έχει το πολύ d_n ρίζες. Άρα

$$d_1 d_2 \cdots d_n = |\mathbb{F}^*| \leq d_n$$

και έτσι $d_1 d_2 \cdots d_{n-1} \leq 1$, οπότε $d_1 = d_2 = \cdots = d_{n-1} = 1$. Τελικά,

$$A_1 = A_2 = \cdots = A_{n-1} = \{*\}$$

άρα η $\mathbb{F}^* \simeq A_n$ είναι κυκλική. □

Πρόταση 4.2.2. *Έστω R ΠΚΙ και M ένα πεπερασμένα παραγόμενο R-πρότυπο. Τότε υπάρχουν $n \in \mathbb{N}$ και ισομορφισμός προτύπων $M \simeq M_t \oplus R^n$.*

Απόδειξη. Γνωρίζουμε ότι υπάρχει ισομορφισμός προτύπων

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

όπου το R-πρότυπο M_i είναι κυκλικό για κάθε $i = 1, 2, \ldots, k$. Συνεπώς

$$M_t \simeq (M_1 \oplus M_2 \oplus \cdots \oplus M_k)_t = (M_1)_t \oplus (M_2)_t \oplus \cdots \oplus (M_k)_t$$

Για κάθε $i = 1, 2, \ldots, k$ υπάρχει $d_i \in R$ με $M_i \simeq R/(d_i)$. Αν $d_i = 0$, τότε $M_i \simeq R$ και $(M_i)_t = 0$. Αν $d_i \neq 0$, τότε $d_i \ell = 0$ για κάθε $\ell \in M_i = R/(d_i)$ και άρα $M_i = (M_i)_t$.

Συνεπώς, υποθέτοντας ότι $d_1, d_2, \ldots, d_\lambda \neq 0$ και $d_{\lambda+1} = d_{\lambda+2} = \cdots = d_k = 0$ έπεται ότι

$$M_t = M_1 \oplus \cdots \oplus M_\lambda \oplus 0 \oplus \cdots \oplus 0 = M_1 \oplus \cdots \oplus M_\lambda$$

Έτσι

$$\begin{aligned} M &\simeq M_1 \oplus \cdots \oplus M_k \\ &= (M_1 \oplus \cdots \oplus M_\lambda) \oplus (M_{\lambda+1} \oplus \cdots \oplus M_k) \\ &= M_t \oplus R^{k-\lambda} \end{aligned}$$

□

Πόρισμα 4.2.3. *Έστω M ένα πεπερασμένο παραγόμενο R-πρότυπο τέτοιο ώστε*

$$M \simeq M_1 \oplus \cdots \oplus M_n$$

και

$$M \simeq M_1' \oplus \cdots \oplus M_n'$$

για κάποια κυκλικά πρότυπα M_i, $i = 1, 2, \ldots, n$ και M_j', $j = 1, 2, \ldots, n'$ με

$$\operatorname{ann} M_1 \supseteq \operatorname{ann} M_2 \supseteq \ldots \supseteq \operatorname{ann} M_n$$

και

$$\operatorname{ann} M_1' \supseteq \operatorname{ann} M_2' \supseteq \ldots \supseteq \operatorname{ann} M_{n'}'$$

Τότε, αν $k = \#\{i : \operatorname{ann} M_i = 0\}$ και $\lambda = \#\{j : \operatorname{ann} M_j' = 0\}$ ισχύει $k = \lambda$.

Απόδειξη. Είδαμε ότι $M \simeq M_t \oplus R^k$ και $M \simeq M_t \oplus R^\lambda$. Συνεπώς $M/M_t \simeq R^k$ και $M/M_t \simeq R^\lambda$. Έτσι $R^k \simeq R^\lambda$, άρα $= \lambda$. □

Πόρισμα 4.2.4. *Έστω M ένα πεπερασμένα παραγόμενο R-πρότυπο.*

(i) Το R-πρότυπο M/M_t είναι ελεύθερο.

(ii) Αν το M είναι ελεύθερο στρέψεως, τότε το M είναι ελεύθερο.

Παρατηρήσεις 4.2.1. (i) Το $\mathbb{Z}$-πρότυπο $\mathbb{Q}$ είναι ελεύθερο στρέψεως αλλά όχι ελεύθερο. Είναι απαραίτητη προυπόθεση να είναι το M πεπερασμένα παραγόμενο.

(ii) Αν $R = \mathbb{Z}[x]$ και $I = (2, x)$, τότε το I δεν είναι ελεύθερο R-πρότυπο αν και είναι πεπερασμένα παραγόμενο και ελεύθερο στρέψεως. Είναι απαραίτητη προυπόθεση ο R να είναι ΠΚΙ.

(iii) Θεωρούμε έναν μεταθετικό δακτύλιο R, ένα R-πρότυπο M και ένα ιδεώδες $I \subseteq R$ τέτοιο ώστε $rx = 0$ για κάθε $r \in I$, $x \in M$, δηλαδή $IM = 0$.

Θεωρούμε τον δακτύλιο-πηλίκο R/I και ορίζουμε στην αβελιανή ομάδα M τη δομή ενος R/I-προτύπου με εξωτερικό πολλαπλασιασμό

$$R/I \times M \to M, \quad (r+I, x) \mapsto (r+I) \cdot x := rx$$

Ο εξωτερικός πολλαπλασιασμός είναι καλά ορισμένος. Έστω $r, r' \in R$ με $r + I = r' + I \in R/I$ και $x \in M$. Τότε $r - r' \in I$, άρα $(r' - r)x = 0$ οπότε $r'x - rx = 0 \in M$ και $rx = r'x \in M$.

Ισχύουν οι ιδιότητες του R/I-προτύπου.

Έστω $r + I, r' + I \in R/I$, $x \in M$. Τότε

$$\begin{aligned}[(r+I)(r'+I)] \cdot x &= (rr' + I) \cdot x \\ &= (rr')x \\ &= r(r'x) \\ &= (r+I) \cdot (r'x) \\ &= (r+I)[(r'+I) \cdot x]\end{aligned}$$

Ανάλογα, δείχνονται και οι άλλες 3 ιδιότητες.

Πρόταση 4.2.3. *Έστω R ΠΚΙ και $p \in R$ ένα ανάγωγο στοιχείο.*

(i) Ο δακτύλιος $R/(p)$ είναι σώμα.

(ii) Αν M είναι ένα R-πρότυπο, τότε η αβελιανή ομάδα M/pM μπορεί να θεωρηθεί ως $R/(p)$-διανυσματικός χώρος.

(iii) Αν το M είναι ένα κυκλικό R-πρότυπο με $o(M) = d$, τότε $\dim_{R/(p)} M/pM$ είναι 1 αν $p|d$ και 0 αν $p \nmid d$.

Απόδειξη. (i) Έστω $k \in R/(p)$ με $k \neq 0$. Τότε $k = r + (p)$, για κάποιο $r \in R$, $r \notin (p)$. Τότε, όμως, $p \nmid r$ και άρα μκδ$(p, r) = 1$. Συνεπώς υπάρχουν $a, b \in R$ με $1 = ap + br$.

Αν $n = b + (p)$, τότε

$$kn = [r + (p)][b + (p)] = rb + (p) = 1 + (p) \in R/(p)$$

Άρα το k είναι αντιστρέψιμο και συνεπώς ο $R/(p)$ είναι σώμα.
(ii) Αρκεί να δείξουμε ότι για κάθε $k \in R/(p)$ και $x \in M/pM$ είναι $kx = 0 \in M/pM$.

Γράφουμε $k = ap$ για κάποιο $a \in R$ και $x = m + pM$ για κάποιο $m \in M$. Τότε

$$kx = ap(m + pM) = apm + pM = 0 + pm \in M/pM$$

(iii) Ισχύει $M \simeq R/(d)$ και άρα

$$rM \simeq (p) + (d)/(d) = (p, d)/(d) = (\delta)/(d)$$

όπου $\delta =$ μδκ(p, d).

Συνεπώς

$$M/pM \simeq \frac{R/(d)}{(\delta)/(d)} \simeq R/(\delta)$$

από το 3ο θεώρημα Ισομορφισμών.

Αν $p|d$, τότε $\delta = \text{μκδ}(p,d) = p$ και άρα $M/pM \simeq R/(p)$. Συνεπώς

$$\dim_{R/(p)} M/pM = \dim_{R/(p)} R/(p) = 1$$

Αν $p \nmid d$, τότε $\delta = \text{μκδ}(p,d) = 1$ και άρα $M/pM = R/(\delta) = R/(1) = R/R = 0$. Συνεπώς

$$\dim_{R/(p)} M/pM = 0$$

□

Πόρισμα 4.2.5. *Έστω R ΠΚΙ και M ένα πεπερασμένα παραγόμενο R-πρότυπο στρέψεως. Αν*

$$M \simeq M_1 \oplus \cdots \oplus M_k$$

και

$$M = N_1 \oplus \cdots \oplus N_\lambda$$

όπου τα M_j, N_i είναι κυκλικά μη-μηδενικά και

$$\operatorname{ann} M_1 \supseteq \operatorname{ann} M_2 \supseteq \ldots \supseteq \operatorname{ann} M_n$$

και

$$\operatorname{ann} N_1 \supseteq \operatorname{ann} N_2 \supseteq \ldots \supseteq \operatorname{ann} N_\lambda$$

τότε $k = \lambda$.

Απόδειξη. Γράφουμε $M_i \simeq R/(d_i)$, $i = 1, 2, \ldots, k$ και έχουμε $d_1|d_2, \ldots, d_{k-1}|d_k$ και, όμοια, $N_i \simeq R/(\delta_j)$, $j = 1, 2, \ldots, \lambda$ και έχουμε $\delta_1|\delta_2, \ldots, \delta_{\lambda-1}|\delta_\lambda$. θα δείξουμε ότι $k \leq \lambda$ και $\lambda \leq k$.

Καθώς $M_i \neq 0$ ισχύει $d_1 \notin U(R)$. Επιλέγουμε ένα ανάγωγο στοιχείο $p \in R$ με $p|d_1$. Τότε $p|d_i$ για κάθε $i = 1, 2, \ldots, k$. Συνεπώς

$$\begin{aligned}
\dim_{R/(p)} M/pM &= \dim_{R/(p)} \frac{M_1 \oplus \cdots \oplus M_k}{pM_1 \oplus \cdots \oplus pM_k} \\
&= \dim_{R/(p)} \left[\frac{M_1}{pM_1} \oplus \cdots \oplus \frac{M_k}{pM_k} \right] \\
&= \dim_{R/(p)} M_1/rM_1 + \dim_{R/(p)} M_2/pM_2 + \cdots + \dim_{R/(p)} M_k/pM_k \\
&= k
\end{aligned}$$

Έτσι είναι

$$\begin{aligned}
k &= \dim_{R/(p)} M/pM \\
&= \dim_{R/(p)} N_1/pN_1 + \dim_{R/(p)} N_2/pN_2 + \cdots + \dim_{R/(p)} N_\lambda/pN_\lambda \\
&\leq \lambda
\end{aligned}$$

Ανάλογα έπεται ότι $\lambda \leq k$. □

Πρόταση 4.2.4. *Έστω R ΠΚΙ, M ένα πεπερασμένα παραγόμενο R-πρότυπο στρέψεως. Αν*

$$M \simeq M_1 \oplus \cdots \oplus M_k$$

και

$$M = N_1 \oplus \cdots \oplus N_k$$

όπου τα M_i, N_i είναι κυκλικά μη-μηδενικά και

$$\operatorname{ann} M_1 \supseteq \operatorname{ann} M_2 \supseteq \ldots \supseteq \operatorname{ann} M_n$$

και

$$\operatorname{ann} N_1 \supseteq \operatorname{ann} N_2 \supseteq \ldots \supseteq \operatorname{ann} N_k$$

τότε

$$\operatorname{ann} M_i = \operatorname{ann} N_i, \quad \forall i = 1, 2, \ldots, k$$

δηλαδή αν $\operatorname{ann} M_i = (d_i)$, $\operatorname{ann} N_i = (\delta_i)$, *τότε* $d_i \sim \delta_i$.

Απόδειξη. Έστω $i \in \{1, 2, \ldots, k\}$. Για να δείξουμε ότι $d_i \sim \delta_i$, αρκεί να δείξουμε ότι $d_i | \delta_i$ και $\delta_i | d_i$.

Θεωρούμε το R-πρότυπο $d_i M$. Είναι

$$\begin{aligned} d_i M &\simeq d_i M_1 \oplus \cdots \oplus d_i M_i \oplus d_i M_{i+1} \oplus \cdots \oplus d_i M_k \\ &= d_i M_{i+1} \oplus \cdots \oplus d_i M_k \end{aligned}$$

και

$$d_i M \simeq d_i N_1 \oplus d_1 N_2 \oplus \cdots \oplus d_i N_k$$

Άρα, τουλάχιστον i από τα R-πρότυπα $d_i N_1, \ldots, d_i N_k$ είναι 0.

Αν όμως $d_i N_j = 0$, τότε $d_i \in \operatorname{ann} N_j$ οπότε $d_i \in N_{j-1}, \ldots$ και άρα $d_i N_{j-1} = 0 d_i N_{j-1} = 0, \ldots$. Έτσι $d_i N_i = 0$, άρα $d_i \in \operatorname{ann} N_i = (\delta_i)$ και άρα $\delta_i | d_i$. Όμοια $d_i | \delta_i$. □

Παράδειγμα 4.2.1. Θεωρούμε την αβελιανή ομάδα

$$M = \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}^2$$

Έστω ότι

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

όπου $k \in \mathbb{N}$, $M_i \neq 0$ κυκλική για κάθε $i = 1, 2, \ldots, n$ και

$$\operatorname{ann} M_1 \supseteq \operatorname{ann} M_2 \supseteq \ldots \supseteq \operatorname{ann} M_k$$

(α) Έχουμε

$$N = M_t = \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_{120}$$

άρα

$$M/M_t \simeq \mathbb{Z} \oplus \mathbb{Z} = \mathbb{Z}^2$$

Συνεπώς $\#\{i : \operatorname{ann} M_i = 0\} = 2$ δηλαδή $\operatorname{ann} M_{k-1} = \operatorname{ann} M_k = 0$ και $\operatorname{ann} M_{k-1} \neq 0$. Άρα

$$N = M_t \simeq M_1 \oplus M_2 \oplus \cdots \oplus M_{k-2}$$

(β) Επιλέγουμε $p = 2$, που να διαιρεί τον d_1. Τότε

$$\begin{aligned} N/2N &= \frac{\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_{120}}{2\mathbb{Z}_2 \oplus 2\mathbb{Z}_6 \oplus 2\mathbb{Z}_{24} \oplus 2\mathbb{Z}_{120}} \\ &\simeq \frac{\mathbb{Z}_2}{2\mathbb{Z}_2} \oplus \frac{\mathbb{Z}_6}{2\mathbb{Z}_6} \oplus \frac{\mathbb{Z}_{24}}{2\mathbb{Z}_{24}} \oplus \frac{\mathbb{Z}_{120}}{2\mathbb{Z}_{120}} \\ &\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \end{aligned}$$

Άρα $\dim_{\mathbb{Z}_2} N/2N = 4$.

Όμοια $N/2N \simeq \bigoplus_{i=1}^{k-2} \frac{M_i}{2M_i}$.

Καθώς $\dim_{\mathbb{Z}_2} M_i/2M_i \leq 1$ και $\sum_{i=1}^{k-2} \dim_{\mathbb{Z}_2} M_i/2M_i = 4$ έπεται ότι $k-2 \geq 4$.

Ανάλογα έπεται ότι $k-2 \leq 4$ και άρα $k-2 = 4$. Τελικά $k = 6$.

Έχουμε, λοιπόν,

$$N = M_1 \oplus M_2 \oplus M_3 \oplus M_4 = \mathbb{Z}_{\delta_1} \oplus \mathbb{Z}_{\delta_2} \oplus \mathbb{Z}_{\delta_3} \oplus \mathbb{Z}_{\delta_4}$$

όπου $\delta_1 | \delta_2, \delta_2 | \delta_3, \delta_3 | \delta_4$.

(γ) Θα δείξουμε ότι $\delta_1 = \pm 2, \delta_2 = \pm 6, \delta_3 = \pm 24, \delta_4 = \pm 120$. Ας δείξουμε παραδείγματος χάριν ότι $\delta_2 = \pm 6$. Όμοια αποδεικύονται και τα υπόλοιπα.

Έχουμε

$$\begin{aligned} 6N &= 6\mathbb{Z}_2 \oplus 6\mathbb{Z}_6 \oplus 6\mathbb{Z}_{24} \oplus 6\mathbb{Z}_{120} \\ &= 0 \oplus 0 \oplus 6\mathbb{Z}_{24} \oplus 6\mathbb{Z}_{120} \\ &\simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2 0 \end{aligned}$$

Καθώς

$$\begin{aligned} 6N &= 6M_1 \oplus 6M_2 \oplus 6M_3 \oplus 6M_4 \\ &= \underbrace{6\mathbb{Z}_{\delta_1} \oplus 6\mathbb{Z}_{\delta_2}}_{0} \oplus 6\mathbb{Z}_{\delta_3} \oplus 6\mathbb{Z}_{\delta_4} \end{aligned}$$

είναι

$$\operatorname{ann} 6\mathbb{Z}_{\delta_1} \subseteq \operatorname{ann} 6\mathbb{Z}_{\delta_2} \subseteq \operatorname{ann} 6\mathbb{Z}_{\delta_3} \subseteq \operatorname{ann} 6\mathbb{Z}_{\delta_4}$$

Ειδικότερα, πρέπει $6\mathbb{Z}_{\delta_2} = 0$ άρα $\delta_2 | 6$.

Ανάλογα, έπεται ότι $6 | \delta_2$ άρα $\delta_2 \sim 6$.

Τελικά, $\delta_2 = \pm 6$.

4.3 Θεώρημα Δομής II

Θεώρημα 4.3.1 (Κινέζικο Θεώρημα Υπολοίπων). *Έστω R μεταθετικός δακτύλιος και $I, J \subseteq R$ ιδεώδη με $I + J = R$. Τότε*

(i) $IJ = I \cap J$

(ii) Υπάρχει ισομορφισμός R-προτύπων

$$R/IJ \simeq R/I \oplus R/J$$

Απόδειξη. (i) Είναι $IJ \subseteq I$ και $IJ \subseteq J$. Συνεπώς $IJ \subseteq I \cap J$.

Αντίστροφα, θεωρούμε $a \in I \cap J$. Καθώς $I + J = R$, έχουμε ότι $1 \in I + J$, άρα υπάρχουν $i \in I, j \in J$ με $1 = i + j$. Τότε $a = a \cdot 1 = a(i + j) = ai + aj = ia + aj \in IJ$, άρα $I \cap J \subseteq IJ$.

(ii) Θεωρούμε την απεικόνιση

$$f : R \to R/I \oplus R/J$$

με

$$f(r) = (r + I, r + J) \in R/I \oplus R/J, \quad \forall r \in R$$

Η f είναι R-γραμμική. Έστω $r, r' \in R$ και $a \in R$. Τότε

$$\begin{aligned} f(r) &= ((r + r') + I, (r + r') + J) \\ &= ((r + I) + (r' + I), (r + J) + (r' + J)) \\ &= (r + I, r + J) + (r' + I, r' + J) \\ &= f(r) + f(r') \end{aligned}$$

και

$$\begin{aligned} f(ar) &= (ar + I, ar + J) = (a(r + I), a(r + J)) \\ &= a(r + I, r + J) = af(r) \end{aligned}$$

Η f είναι επί. Θεωρούμε $(a + I, b + J) \in R/I \oplus R/J$, όπου $a, b \in R$.

Αν επιλέξουμε $i \in I$ και $j \in J$ ώστε $1 = i + j$, τότε θεωρούμε το $c = aj + bi \in R$ και παρατηρούμε ότι

$$a - c = a(i + j) - c = ai + aj - c = ai - bi \in I$$

και

$$b - c = b(i + j) - c = bi + bj - c = bj - aj \in J$$

Συνεπώς $f(c) = (c + I, c + J) = (a + I, b + J) \in R/I \oplus R/J$.

Τέλος,

$$\begin{aligned} \ker f &= \{r \in R : f(r) = 0\} \\ &= \{r \in R : f(r) = (0 + I, 0 + J) \in R/I \oplus R/J\} \\ &= \{r \in R : (r + I, r + J) = (0 + I, 0 + J) \in R/I \oplus R/J\} \\ &= \{r \in R : r + I = 0 + I \in R/I, r + J = 0 + J \in R/J\} \\ &= \{r \in R : r \in I, r \in J\} \\ &= I \cap J = IJ \end{aligned}$$

Άρα από το 1ο Θεώρημα Ισομορφισμών υπάρχει ισομορφισμός R-προτύπων

$$R/IJ = R/\ker f \xrightarrow{\sim} \operatorname{im} f = R/I \oplus R/J$$

□

Πόρισμα 4.3.1. *Έστω R ΠΚΙ και $a, b \in R$ με μκδ$(a, b) = 1$. Τότε υπάρχει ισομορφισμός R-προτύπων*

$$R/(ab) \simeq R/(a) \oplus R/(b)$$

Απόδειξη. Θεωρούμε τα ιδεώδη $I = (a), J = (b)$ και παρατηρούμε ότι $I + J = (d)$, $d = \text{μκδ}(a, b)$. Όμως, $d = 1$ άρα $I + J = (1) = R$.

Το ζητούμενο έπεται από το Κινέζικο Θεώρημα Υπολοίπων καθώς $IJ = (ab)$. □

Πόρισμα 4.3.2. *Έστω R ΠΚΙ και $a_1, a_2, \ldots, a_n \in R$ με μκδ$(a_i, a_j) = 1$ για κάθε $i \neq j$. Αν $a = \prod_{i=1}^{n} a^i$, τότε υπάρχει ισομορφισμός R-προτύπων*

$$R/(a) \simeq \bigoplus_{i=1}^{n} R/(a_i)$$

Πρόταση 4.3.1. *Έστω R ΠΚΙ και M ένα πεπερασμένα παραγόμενο R-πρότυπο. Τότε υπάρχουν κυκλικά πρότυπα $M_1, M_2 \ldots, M_n$ ώστε*

$$M \simeq \bigoplus_{i=1}^{n} M_i$$

και $M_i \simeq R$ ή $M_i \simeq R/(p_i^{n_i})$ για κάθε $i = 1, 2, \ldots, n$, για κάποιο ανάγωγο $p_i \in R$ και κάποιο $n_i > 0$.

Απόδειξη. Γνωρίζουμε ότι το R-πρότυπο M μπορεί να γραφτεί ως ευθύ άθροισμα κυκλικών προτύπων της μορφής $R/(d)$.

Γράφουμε $d = up_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, όπου $u \in U(R)$, τα p_i είναι ανάγωγα και ανά δυο μη-συντροφικά και $n_1, n_2 \ldots, n_k \in \mathbb{N}$. Τότε μκδ$(p_i^{n_i}, p_j^{n_j}) = 1$ για κάθε $i \neq j$ και άρα

$$R/(d) = R/(u^{-1}d) = R/(\prod_{i=1}^{k} p_i^{n_i}) \simeq \bigoplus_{i=1}^{k} R/(p_i^{n_i})$$

□

Πόρισμα 4.3.3. *Κάθε πεπερασμένα παραγόμενη αβελιανή ομάδα είναι ισόμορφη με ένα ευθύ άθροισμα της μορφής*

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n$$

όπου κάθε M_i είναι είτε η άπειρη κυκλική ομάδα $\mathbb{Z}$ είτε μια κυκλική ομάδα τάξης $p_i^{n_i}$, για κάποιον p_i πρώτο και κάποιο $n_i \in \mathbb{N}$.

Παράδειγμα 4.3.1. Έστω G αβελιανή ομάδα με $|G| = 36$. Γνωρίζουμε ότι η G είναι ισόμορφη με μια από τις

$$\mathbb{Z}_{36} \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_9$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{18} \simeq \mathbb{Z}_2 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_9)$$

$$\mathbb{Z}_3 \oplus \mathbb{Z}_{12} \simeq \mathbb{Z}_3 \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_3)$$

$$\mathbb{Z}_6 \oplus \mathbb{Z}_6 \simeq (\mathbb{Z}_2 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_3)$$

Ορισμός 4.3.1. Έστω R ΠΚΙ, M ένα R-πρότυπο και $p \in R$ ένα ανάγωγο στοιχείο. Θεωρούμε το υποσύνολο $M(p) \subseteq M$ με

$$M(p) = \{m \in M : p^k m = 0 \,\text{για κάποιο}\, k \in \mathbb{N}\}$$

Παρατήρηση 4.3.1. Το $M(p) \subseteq M$ είναι ένα R-υποπρότυπο του M.

Πράγματι, έστω $m, m' \in M(p)$ και $r \in R$. Τότε, υπάρχει $k \in \mathbb{N}$ τέτοιο ώστε $p^k m = 0$ και $p^k m' = 0$. Συνεπώς

$$p^k(m \pm m') = p^k m \pm p^k m' = 0 \pm 0 = 0 \in M$$

και

$$p^k(rm) = (rp^k)m = r(p^k m) = r0 = 0 \in M$$

Επίσης $0 \in M(p)$.

Πρόταση 4.3.2. *Έστω R ΠΚΙ, $p \in R$ ανάγωγο και M, N δύο R-πρότυπα. Τότε*

$$(M \oplus N)(p) = M(p) \oplus N(p)$$

Απόδειξη. Πρέπει να δείξουμε ότι αν $(x, y) \in M \oplus N$, τότε $(x, y) \in (M \oplus N)(p)$ ανν $x \in M(p)$ και $y \in N(p)$.

Αν $(x, y) \in (M \oplus N)(p)$, τότε υπάρχει $k \in \mathbb{N}$ με $(p^k x, p^k y) = p^k(x, y) = (0, 0) \in M \oplus N$ άρα $p^k x = 0 \in M$ και $p^k y = 0 \in N$, δηλλαδή $x \in M(p)$ και $y \in N(p)$.

Κάθως $x \in M(p)$ και $y \in N(p)$, μπορούμε να βρούμε $k \in \mathbb{N}$ με $p^k x = 0 \in M$ και $p^k y = 0 \in N$. Τότε $p^k(x, y) = (p^k x, p^k y) = (0, 0) \in M \oplus N$ και άρα $(x, y) \in (M \oplus N)(p)$. □

Πρόταση 4.3.3. *Έστω R ΠΚΙ, $p \in R$ ένα ανάγωγο στοιχείο και M ένα κυκλικό R-πρότυπο με $\operatorname{ann} M = (q^n)$ για κάποιο ανάγωγο στοιχείο $q \in R$ και κάποιο $n \in \mathbb{N}$.*

(i) Αν $p \sim q$ είναι $M(p) = M$.

(ii) Αν $p \not\sim q$ είναι $M(p) = 0$.

Απόδειξη. (i) Αν $p \sim q$ μπορούμε να βρούμε $u \in U(R)$ με $p = uq$. Τότε $p^n = u^n q^n$ και άρα για κάθε $x \in M$ είναι $p^n x = u^n q^n x = u^n 0 = 0 \in M$. Άρα $M(p) = M$.

(ii) Έστω $x \in M(p)$. Τότε $p^m x = 0$ για κάποιο $m \in \mathbb{N}$. Καθώς $p \not\sim q$ έχουμε μκδ$(p^m, q^n) = 1$. Συνεπώς, υπάρχουν $\lambda, \mu \in R$ με $1 = \lambda p^m + \mu q^n$. Συνεπώς $x = 1x = (\lambda p^m + \mu q^n)x = \lambda p^m x + \mu q^n x = 0$, άρα $M(p) = 0$. □

Θεώρημα 4.3.2. *Έστω R ΠΚΙ και M ένα πεπερασμένα παραγόμενο R-πρότυπο. Υποθέτουμε ότι*

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

και

$$M \simeq N_1 \oplus N_2 \oplus \cdots \oplus N_\lambda$$

όπου τα M_i, N_j είναι κυκλικά μη-μηδενικά και οι μηδενιστές $\operatorname{ann} M_i, \operatorname{ann} N_j$ είναι είτε 0 είτε της μορφής (p^s), για κάποιο ανάγωγο $p \in R$ και κάποιο $s > 0$. Τότε $k = \lambda$ και η ακολουθία $(\operatorname{ann} M_1, \ldots, \operatorname{ann} M_k)$ είναι μια αναδιάταξη της ακολουθίας $(\operatorname{ann} N_1, \ldots, \operatorname{ann} N_\lambda)$.

Απόδειξη. Γνωρίζουμε ότι το πλήθος των i με $\operatorname{ann} M_i = 0$ είναι η τάξη του ελεύθερου R-προτύπου M/M_t. Αντίστοιχα, το πλήθος των j με $\operatorname{ann} N_j = 0$ είναι η τάξη του M/M_t. Συνεπώς $\#\{i : \operatorname{ann} M_i = 0\} = \#\{j : \operatorname{ann} N_j = 0\}$.

Επιλέγουμε $p \in R$ ανάγωγο και υποθέτουμε ότι $\operatorname{ann} M_1 = (p^{k_1}), \ldots, \operatorname{ann} M_s = (p^{k_s})$ και αν $i > s$ τότε $\operatorname{ann} M_i = (q_i^{a_i})$ για κάποια ανάγωγα στοιχεία $q_i \in R$ με $p \not\sim q_i$ ή $\operatorname{ann} M_i = 0$. Επιπλέον, υποθέτουμε ότι $k_1 \leq k_2 \leq \ldots \leq k_s$.

Όμοια υποθέτουμε ότι $\operatorname{ann} N_1 = (p^{\lambda_1}), \ldots, \operatorname{ann} N_\sigma = (p^{\lambda_\sigma})$ και αν $j > \sigma$ τότε $\operatorname{ann} N_j = (\theta_j^{b_i})$ για κάποια ανάγωγα στοιχεία $\theta_j \in R$ με $p \not\sim \theta_j$ ή $\operatorname{ann} N_j = 0$.

θα δείξουμε ότι $s = \sigma$ και $(k_1, \ldots, k_s) = (\lambda_1, \ldots, \lambda_\sigma)$.

Παρατηρούμε ότι

$$\begin{aligned} M(p) &\simeq M_1(p) \oplus M_2(p) \oplus \cdots \oplus M_k(p) \\ &= M_1 \oplus M_2 \oplus \cdots \oplus M_s \oplus 0 \oplus \cdots \oplus 0 \end{aligned}$$

Έτσι

$$M(p) \simeq M_1 \oplus M_2 \oplus \cdots \oplus M_s$$

Όμοια βλέπουμε ότι

$$M(p) \simeq N_1 \oplus N_2 \oplus \cdots \oplus N_\sigma$$

Καθώς

$$\operatorname{ann} M_1 \supseteq \operatorname{ann} M_2 \supseteq \ldots \supseteq \operatorname{ann} M_s$$

και

$$\operatorname{ann} N_1 \supseteq \operatorname{ann} N_2 \supseteq \ldots \supseteq \operatorname{ann} N_\sigma$$

από τη μοναδικότητα της διάσπασης που έχουμε δει, έπεται ότι $s = \sigma$ και

$$k_1 = \lambda_1, k_2 = \lambda_2, \ldots, k_s = \lambda_\sigma$$

□

Πρόταση 4.3.4. *Έστω R ΠΚΙ και M ένα πεπερασμένα παραγόμενο R-πρότυπο στρέψεως. Αν $\operatorname{ann} M = (d)$ και $d = up_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, όπου τα $p_i \in R$ είναι ανάγωγα και τα $a_i > 0, u \in U(R)$, τότε*

$$M \simeq M(p_1) \oplus \cdots \oplus M(p_n)$$

Απόδειξη. Μπορούμε να γράψουμε

$$M \simeq \bigoplus_{i=1}^{k} M_i$$

όπου τα M_i είναι κυκλικά R-πρότυπα και

$$\operatorname{ann} M_1 \supseteq \operatorname{ann} M_2 \supseteq \ldots \supseteq \operatorname{ann} M_k$$

Αν $\operatorname{ann} M_i = (d_i)$ έχουμε ότι $d_1 | p_1 a_1 p_2^{a_2} \cdots p_n^{a_n}$. Συνεπώς μπορούμε να γράψουμε ότι $d_i \sim p_1^{a_1^{(i)}} \cdots p_n^{a_n^{(i)}}$, για κάποια $a_1^{(i)}, \ldots, a_n^{(i)} \geq 0$. (Το i δεν δηλώνει εκθέτη).

Έτσι, μπορούμε να έχουμε μια διάσπαση

$$M \simeq \bigoplus_{j=1}^{\lambda} N_j$$

όπου $\operatorname{ann} N_j = (q^a)$, για κάποιο $q \in \{p_1, p_2, \ldots, p_n\}$ και $a > 0$.

Αναδιατάσσοντας το j μπορούμε να υποθέσουμε ότι $\operatorname{ann} N_j = (p_1^{b_j})$, για $j = 1, \ldots, \lambda_1$ και $\operatorname{ann} N_j = (p_2^{\gamma_j})$, για $j = \lambda_1 + 1, \ldots, \lambda_1 + \lambda_2, \ldots$ και τέλος $\operatorname{ann} N_j = (p_n^{\delta_j})$ για $j = \lambda_1 + \lambda_2 + \cdots + \lambda_{n-1} + 1, \ldots, \lambda_1 + \cdots + \lambda_{n-1} + \lambda_n = \lambda$.

Έτσι,

$$M(p_1) = \bigoplus_{j=1}^{\lambda_1} N_j(p_1)$$

$$M(p_2) = \bigoplus_{j=\lambda_1+1}^{\lambda_+\lambda_2} N_j(p_2)$$

$$\vdots$$

$$M(p_n) = \bigoplus_{j=\lambda_1+\ldots+\lambda_{n-1}+1}^{\lambda_1+\ldots+\lambda_{n-1}+\lambda_n} N_j(p_n)$$

Άρα

$$M \simeq M(p_1) \oplus M(p_2) \oplus \cdots \oplus M(p_n)$$

□

Παράδειγμα 4.3.2. Έστω

$$M = \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}^4$$

Εδώ

$$M_t = \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_{120}$$

και $\operatorname{rank} M/M_t = 4$. Συνεπώς $\operatorname{ann} M_t = 120$. Έχουμε

$$\mathbb{Z}_3 = \mathbb{Z}_3$$

$$\mathbb{Z}_6 = \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

$$\mathbb{Z}_{24} = \mathbb{Z}_8 \oplus \mathbb{Z}_3$$

$$\mathbb{Z}_{120} = \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

άρα

$$M = \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}^4$$

Για να βρούμε την 2η διάσπαση του M βρίσκουμε τους πρώτους που εμφανίζονται στην παράπανω ανάλυση του M και επιλέγουμε κάθε φορά αυτούς στην μεγαλύτερη δύναμη που εμφανίζονται, δηλαδή

$$\begin{aligned} M &= (\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_8 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_3 \oplus \mathbb{Z}^4 \\ &= \mathbb{Z}_{120} \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}^4 \\ &= \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{24} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}^4 \end{aligned}$$

Επίσης είναι

$$M_2 = \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8$$

$$M_3 = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

και

$$M_5 = \mathbb{Z}_5$$

4.4 Δυο Εφαρμογές

Όπως γνωρίζουμε το αντίστροφο του θεωρήματος Lagrange δεν ισχύει εν γένει. Για παράδειγμα αν θεωρήσουμε την ομάδα A_4 δεν υπάρχει υποομάδα $M \subseteq A_4$ με $|M| = 6|12 = |A_4|$. Όπως βλέπουμε παρακάτω το αντίστροφο του θεωρήματος Lagrange ισχύει αν μιλάμε για αβελιανές ομάδες.

Πρόταση 4.4.1 (Αντίστροφο του Θεωρήματος Lagrange). *Έστω G μια αβελιανή ομάδα με $|G| = n < \infty$ και $m \in \mathbb{N}$ με $m|n$. Τότε υπάρχει υποομάδα $H \subseteq G$ με $|H| = m$.*

Απόδειξη. Γράφουμε $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, όπου p_i είναι διακεκριμένοι πρώτοι και $a_i > 0$ για κάθε i. Γνωρίζουμε ότι $G = \bigoplus_{i \leq k} G_{p_i}$ και $G_p = 0$ αν $p \notin \{p_1, p_2, \ldots, p_k\}$. Άρα

$$G = G_{p_1} \oplus G_{p_2} \oplus \cdots \oplus G_{p_k}$$

και $|G_{p_i}| = p_i^{a_i}$. Έτσι

$$|G| = \prod_{i=1}^{k} |G_i| = \prod_{i=1}^{k} p_i^{a_i}$$

Καθώς $m|n$ μπορούμε να γράψουμε $m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, όπου $0 \leq b_i \leq a_i$ για κάθε $i \leq k$.

Αν δείξουμε ότι για κάθε $i \leq k$ υπάρχει υποομάδα $H_i \subseteq G_{p_i}$ με $|H_i| = p_i^{b_i}$, τότε για την

$$H = \bigoplus_{i=1}^{k} H_i \subseteq \bigoplus_{i=1}^{k} G_{p_i} = G$$

θα έχουμε ότι

$$|H| = \prod_{i=1}^{k} |H_i| = \prod_{i=1}^{k} p_i^{b_i} = m$$

Μπορούμε, λοιπόν, να υποθέσουμε ότι $|G| = p^a$, για κάποιον p πρώτο και κάποιο $a > 0$, ενώ $m = p^b$, για κάποιο $b \leq a$.

Γράφουμε

$$G = A_1 \oplus A_2 \oplus \cdots \oplus A_\lambda$$

όπου $A_i = \mathbb{Z}_{p^{k_i}}$, για κάποια $k_i \in \mathbb{N}$. Προφανώς

$$p^a = |G| = \prod_{i=1}^{\lambda} |A_i| = \prod_{i=1}^{\lambda} p^{k_i} = p^{\sum_{i=1}^{\lambda} k_i}$$

άρα $a = \sum_{i=1}^{\lambda} k_i$.

Τώρα, υπάρχει $\lambda_0 \leq \lambda$ και $0 \leq k \leq k_{\lambda_0+1}$ ώστε $b = k_1 + k_2 + \ldots + k_{\lambda_0} + k$. Η ομάδα A_{λ_0+1} έχει τάξη $p^{k_{\lambda_0}+1}$ και καθώς $p^k | p^{k_{\lambda_0+1}}$ υπάρχει υποομάδα $B \subseteq A_{\lambda_0+1}$ με $|B| = p^k$.

Ορίζουμε

$$H = A_1 \oplus A_2 \oplus \cdots \oplus A_{\lambda_0} \oplus B$$

οπότε

$$|H| = p^{k_1} p^{k_2} \cdots p_{\lambda_0} p^k = p^b$$

□

Έχουμε δει ότι αν πάρουμε μια $f : \mathbb{C}^m \to \mathbb{C}^m$ γραμμική απεικόνιση, τότε αυτή είναι ισομορφισμός ανν είναι 1-1 ανν είναι επί. Ειδικότερα αν η f είναι επί, τότε είναι 1-1. Αυτό, όπως αποδεικνύεται και παρακάτω, ισχύει και στο γενικότερο πλαίσιο των περιοχών κυρίων ιδεωδών.

Πρόταση 4.4.2. *Έστω R ΠΚΙ και $f : R^n \to R^n$ μια R-γραμμική απεικόνιση. Αν η f είναι επί, τότε η f είναι 1-1, και άρα ισομορφισμός.*

Απόδειξη. Γνωρίζουμε ότι υπάρχουν $d_1, d_2, \ldots, d_n \in R$ με $d_1 | d_2, \ldots, d_{n-1} | d_n$ και διατεταγμένες βάσεις $\widehat{u} = (u_1, u_2, \ldots, u_n)$ και $\widehat{v} = (v_1, v_2, \ldots, v_n)$ του R^n έτσι ώστε

$$(f : \widehat{u}, \widehat{v}) = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{pmatrix}$$

Με άλλα λόγια $f(u_1) = d_1 v_1, \ldots, f(u_n) = d_n v_n$. Έτσι για κάθε $\lambda_1, \lambda_2, \ldots, \lambda_n \in R$ ισχύει

$$f(\lambda_1 u_1 + \cdots + \lambda_n u_n) = \lambda_1 d_1 v_1 + \cdots + \lambda_n d_n v_n$$

Καθώς η f είναι επί, $v_n \in \operatorname{im} f$ και άρα υπάρχουν $\lambda_1^*, \lambda_2^*, \ldots, \lambda_n^* \in R$ ώστε

$$v_n = f(\lambda_1^* u_1 + \cdots + \lambda_n^* u_n) = \lambda_1^* d_1 v_1 + \cdots + \lambda_n^* d_n v_n$$

οπότε $1 = \lambda_n^* v_n$ και άρα $d_n \in U(R)$. Άρα $d_1, d_2, \ldots, d_n \in U(R)$ και έτσι η f είναι ισομορφισμός, άρα και 1-1, με αντίστροφο $f^{-1} : R^n \to R^n$ την απεικόνιση όπου

$$(f^{-1} : \widehat{v}, \widehat{u}) = \begin{pmatrix} d_1^{-1} & & & \\ & d_2^{-1} & & \\ & & \ddots & \\ & & & d_n^{-1} \end{pmatrix}$$

□

Πόρισμα 4.4.1. *Έστω R ΠΚΙ και $m, n \in \mathbb{N}$. Τότε υπάρχει R-γραμμική απεικόνιση $R^n \to R^m$ η οποία είναι επί ανν $n \geq m$.*

Απόδειξη. ($\Leftarrow$) Αν $n \geq m$, η απεικόνιση $f : R^n \to R^m$ με $f(r_1, \ldots, r_n) = (r_1, \ldots, r_m)$ -η προβολή στις πρώτες m συντεταγμένες- είναι R-γραμμική και επί.
($\Rightarrow$) Έστω ότι υπάρχουν $n, m \in \mathbb{N}$ με $n < m$ και μια R-γραμμική απεικόνιση $f : R^n \to R^m$, που είναι επί. Θεωρούμε τον $R^m = R^n \oplus R^{m-n}$ και την απεικόνιση $g : R^m = R^n \oplus R^{m-n} \to R^n$ με $g(r_1, r_2, \ldots, r_m) = f(r_1, r_2 \ldots, r_n)$ για κάθε $(r_1, r_2, \ldots, r_m) \in R^m$.

$$R^m = R^n \oplus R^{m-n} \xrightarrow{p_n} R^n \xrightarrow{f} R^m$$

Τότε η g είναι R-γραμμική ως σύνθεση R-γραμμικών απεικονίσεων και επί, άρα η g είναι 1-1.

Αυτό ,όμως, είναι άτοπο, γιατί $(0, 0, \ldots, 0, 1, 1, \ldots, 1) \in \ker g$. □

Κεφάλαιο 5

Εφαρμογές στη Γραμμική Άλγεβρα

Θεωρούμε ένα σώμα $\Bbbk$, V έναν $\Bbbk$-διανυσματικό χώρο με $\dim_{\Bbbk} V < \infty$ και $\phi : V \to V$ μια $\Bbbk$-γραμμική απεικόνιση. Τότε μπορούμε να θεωρήσουμε το V ως $\Bbbk[x]$-πρότυπο με $xv = \phi(v)$ για κάθε $v \in V$. Αυτό είναι το πλαίσιο στο οποίο δουλεύουμε σε αυτό το κεφάλαιο.

Παρατηρήσεις 5.0.1. (i) Το $\Bbbk[x]$-πρότυπο V είναι ένα πρότυπο στρέψεως.

Αν $v \in V$, τότε τα $v, \phi(v), \phi^2(v), \ldots$ είναι γραμμικά εξαρτημένα και άρα υπάρχουν $n \in \mathbb{N}$, $\lambda_0, \lambda_1, \ldots, \lambda_n \in k$ όχι όλα μηδενικά ώστε

$$\lambda_0 v + \lambda_1 \phi(v) + \ldots + \lambda_n \phi^n(v) = 0 \in V$$

Τότε

$$f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n \in \Bbbk[x] \backslash \{0\}$$

και

$$f(x)v = \lambda_0 v + \lambda_1 \phi(v) + \ldots + \lambda_n \phi^{n-1}(v) = 0 \in V$$

(ii) Για το ιδεώδες $\operatorname{ann}_{\Bbbk[x]} V \subseteq \Bbbk[x]$ ισχύει $\operatorname{ann}_{\Bbbk[x]} V = (\mu_\phi(x))$, όπου $\mu_\phi(x) \in \Bbbk[x]$ είναι το ελάχιστο πολυώνυμο της ϕ.

5.1 Ρητή Κανονική Μορφή

Πρόταση 5.1.1. *Έστω ότι το $\Bbbk[x]$-πρότυπο V είναι κυκλικό. Τότε:*

(i) $V \simeq \frac{\Bbbk[x]}{(\mu_\phi(x))}$, *όπου* $\mu_\phi(x) \in \Bbbk[x]$ *είναι το ελάχιστο πολυώνυμο της* ϕ.

(ii) $\dim_{\Bbbk[x]} V = \deg(\mu(x))$.

(iii) Υπάρχει διατεταγμένη βάση $\widehat{v}$ του V ώστε

$$(\phi : \widehat{v}, \widehat{v}) = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & \lambda_0 \\ 1 & 0 & 0 & \ldots & 0 & \lambda_1 \\ 0 & 0 & 1 & \ldots & 0 & \lambda_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & \lambda_{n-1} \end{pmatrix}$$

για κάποια $\lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in k$.

Απόδειξη. (i) Καθώς το $\Bbbk[x]$-πρότυπο V είνα κυκλικό γνωρίζουμε ότι υπάρχει ισομορφισμός $\Bbbk[x]$-προτύπων

$$V \simeq \frac{\Bbbk[x]}{\operatorname{ann}_{\Bbbk[x]} V}$$

Όμως $\operatorname{ann}_{\Bbbk[x]} V = (\mu(x))$.
(ii) Καθώς $V \simeq \frac{\Bbbk[x]}{\operatorname{ann}_{\Bbbk[x]} V}$ ως $\Bbbk$-διανυσματικοί χώροι έπεται ότι $\dim_{\Bbbk} V = \dim \frac{\Bbbk[x]}{\operatorname{ann}_{\Bbbk[x]} V}$.

Γράφουμε $\mu(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ και έχουμε ότι μια βάση του $\frac{\Bbbk[x]}{\operatorname{ann}_{\Bbbk[x]} V}$ αποτελείται από τα στοιχεία $1 + (\mu(x)), x + (\mu(x)), \ldots, x^{n-1} + (\mu(x))$.

Πράγματι, για κάθε $f(x) \in \Bbbk[x]$ μπορούμε να βρούμε $\pi(x) \in \Bbbk[x]$ και $b_0, b_1, \ldots, b_{n-1}$ ώστε

$$f(x) = \pi(x) \cdot \mu(x) + (b_0 + b_1 x + \ldots + b_{n-1}x^{n-1})$$

Συνεπώς

$$\begin{aligned} f(x) + (\mu(x)) &= (b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}) + (\mu(x)) \\ &= b_0(1 + (\mu(x))) + b_1(x + (\mu(x))) + \ldots + b_{n-1}(x^{n-1} + (\mu(x))) \end{aligned}$$

και άρα τα $1 + (\mu(x)), x + (\mu(x)), \ldots, x^{n-1} + (\mu(x))$ αποτελούν ένα σύνολο γεννητόρων.

Αν, τώρα, $c_0, c_1, \ldots, c_{n-1} \in \Bbbk$ και

$$c_0(1 + (\mu(x))) + c_1(x + (\mu(x))) + \ldots + c_{n-1}(x^{n+1} + (\mu(x))) = 0 + (\mu(x)) \in \frac{\Bbbk[x]}{\operatorname{ann}_{\Bbbk[x]} V}$$

τότε

$$(c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}) + (\mu(x)) = 0 + (\mu(x))$$

άρα

$$\mu(x) | c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$$

Καθώς, όμως, $\deg(\mu(x)) = n$ πρέπει να είναι

$$c_0 + c_1 x + \ldots + c_{n-1}x^{n-1} = 0 \in \Bbbk[x]$$

άρα $c_0 = \ldots = c_{n-1} = 0$.
(iii) Καθώς το $\Bbbk[x]$-πρότυπο V είναι κυκλικό υπάρχει $v \in V$ με $V = \Bbbk[x] \cdot v$.

Θα δείξουμε ότι τα διανύσματα $v, \phi(v), \ldots, \phi^{n-1}(v)$ αποτελουν μιά βάση του $\Bbbk$-διανυσματικού χώρου V. Καθώς $\dim_{\Bbbk} V = n$, αρκεί να δείξουμε ότι τα παραπάνω διανύσματα παράγουν τον διανυσματικό χώρο V.

Έστω $w \in V$. Τότε υπάρχει $f(x) \in \Bbbk[x]$ με $w = f(x)v$. Μπορούμε να γράψουμε

$$f(x) = \pi(x) \cdot \mu(x) + (\lambda_0 + \lambda_1 x + \ldots + \lambda_{n-1}x^{n-1})$$

για κάποιο $\pi(x) \in \Bbbk[x]$ και κάποια $\lambda_0, \lambda_1, \ldots, \lambda_{n-1} \in \Bbbk$.

Τότε

$$\begin{aligned} w &= \pi(x)\mu(x)v + (\lambda_0 + \lambda_1 x + \ldots + \lambda_{n-1}x^{n-1}) \\ &= \lambda_0 v + \lambda_1 \phi(v) + \ldots + \lambda_{n-1}\phi^{n-1}(v) \end{aligned}$$

Θα υπολογίσουμε τώρα τον πίνακα της ϕ ως προς την βάση $\widehat{v} = (v, \phi(v), \ldots, \phi^{n-1}(v))$. Είναι

$$\phi(v) = 0v + 1\phi(v) + \ldots + 0\phi^{n-1}(v)$$

$$\phi(\phi(v)) = 0v + 0\phi(v) + 1\phi^2(v) + \ldots + 0\phi^{n-1}(v)$$

$$\vdots$$

$$\begin{aligned}\phi(\phi^{n-2}(v)) &= 0v + 0\phi(v) + \ldots + 1\phi^{n-1}(v)\phi(\phi^{n-1}(v)) \\ &= -a_0 v - a_1\phi(v) - \ldots - a_{n-1}\phi^{n-1}(v)\end{aligned}$$

Έτσι

$$(\phi : \widehat{v}, \widehat{v}) = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

□

Ορισμός 5.1.1. Αν $\lambda(x) = x^n + \lambda_{n-1}x^{n-1} + \ldots + \lambda_1 x + \lambda_0 \in \Bbbk[x]$, ορίζουμε

$$\Sigma[\lambda(x)] = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -\lambda_0 \\ 1 & 0 & 0 & \ldots & 0 & -\lambda_1 \\ 0 & 0 & 1 & \ldots & 0 & -\lambda_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -\lambda_{n-1} \end{pmatrix}$$

τον **συνοδό πίνακα** του $\lambda(x)$.

Πρόταση 5.1.2. *Έστω ότι υπάρχει μια διατεταγμένη βάση $\widehat{v}$ του $\Bbbk$-διανυσματικού χώρου V και μονικό πολυώνυμο $\lambda(x) \in \Bbbk[x]$ έτσι ώστε $(\phi : \widehat{v}, \widehat{v}) = \Sigma[\lambda(x)]$. Τότε το $\Bbbk[x]$-πρότυπο V είναι κυκλικό και το $\lambda(x)$ είναι το ελάχιστο πολυώνυμο της ϕ.*

Απόδειξη. Έστω $\widehat{v} = (v_1, v_2, \ldots, v_n)$, οπότε $n = \dim_{\Bbbk} V$. Θα δείξουμε ότι $V = \Bbbk[x] \cdot v_1$.

Για το σκοπό αυτό, αρκεί να δείξουμε ότι $v_i \in \Bbbk[x] \cdot v_1$ για κάθε $i = 1, 2, \ldots, n$. Όμως

$$v_1 = 1v_1 \in \Bbbk[x] \cdot v_1$$

$$v_2 = \phi(v_1) = x \cdot v_1 \in \Bbbk[x] \cdot v_1$$

$$\vdots$$

$$v_n = \phi(v_{n-1}) = \ldots = \phi^{n-1}(v_1) = x^{n-1}v_1 \in \Bbbk[x] \cdot v_1$$

Συνεπώς, το $\Bbbk$-πρότυπο V είναι κυκλικό.

Επιπλέον, έχουμε $\phi^n(v_1) = \phi(v_n) = -\lambda_0 v_1 - \lambda_1\phi(v_1) - \ldots - \lambda_{n-1}\phi^{n-1}(v_1)$ και άρα

$$\phi^n(v_1) + \lambda_{n-1}\phi^{n-1}(v_1) + \ldots + \lambda_1\phi(v_1) + \lambda_0 = 0 \in V$$

δηλαδή

$$(x^n + \lambda_{n-1}x^{n-1} + \ldots + \lambda_1 x + \lambda_0) \cdot v_1 = 0 \in V$$

Έτσι $\lambda(x) \cdot v_1 = 0 \in V$.

Συνεπώς

$$\lambda(x) \cdot v_i = \lambda(x) \cdot x^{i-1} \cdot v_1 = x^{i-1}(\lambda(x) \cdot v_1) = x^{i-1} \cdot 0 = 0 \in V$$

άρα $\lambda(x)\cdot v=0\in V$ για κάθε $v\in V$.

Έτσι, $\lambda(x)\in \operatorname{ann}_{\Bbbk[x]}V=(\mu(x))$ και άρα $\mu(x)|\lambda(x)$. Όπως δείξαμε πριν καθώς το $\Bbbk[x]$-πρότυπο V είναι κυκλικό, ισχύει $\dim_{\Bbbk}V=\deg(f\mu(x))$. Όμως $\dim_{\Bbbk}V=n=\deg(\lambda(x))$ και άρα $\deg(\mu(x))=\deg(\lambda(x))$.

Τελικά $\mu(x)=\lambda(x)$. □

Θεώρημα 5.1.1. *(i) Υπάρχει διατεταγμένη βάση $\widehat{v}$ του V και μονικά πολυώνυμα $d_1(x),d_2(x),\dots,d_k(x)\in\Bbbk[x]$ με $d_1(x)|d_2(x),\dots,d_{k-1}|d_k$ και*

$$(\phi:\widehat{v},\widehat{v})=\begin{pmatrix}\Sigma[d_1(x)] & & & \\ & \Sigma[d_2(x)] & & \\ & & \ddots & \\ & & & \Sigma[d_k(x)]\end{pmatrix}$$

(ii) Αν υπάρχουν μονικά πολυώνυμα $\delta_1(x),\delta_2(x),\dots,\delta_\lambda(x)\in\Bbbk[x]$ με $\delta_1(x)|\delta_2(x),\dots,\delta_{\lambda-1}|\delta_\lambda$ και διατεταγμένη βάση $\widehat{w}$ του V με

$$(\phi:\widehat{w},\widehat{w})=\begin{pmatrix}\Sigma[\delta_1(x)] & & & \\ & \Sigma[\delta_2(x)] & & \\ & & \ddots & \\ & & & \Sigma[\delta_\lambda(x)]\end{pmatrix}$$

τότε $k=\lambda$ και $\delta_i(x)=d_i(x)$ για κάθε $i=1,2,\dots,k$.

Απόδειξη. (i) Γνωρίζουμε ότι το $\Bbbk[x]$-πρότυπο V είναι το ευθύ άθροισμα κυκλικών υποπροτύπων $V_1,V_2,\dots,V_k$ με $\operatorname{ann}V_1\supseteq\operatorname{ann}V_2\supseteq\dots\supseteq\operatorname{ann}V_k$. Έτσι κάθε V_i είναι ένας ϕ-αναλλοίωτος υπόχωρος του V, ο οποίος είναι κυκλικό $\Bbbk[x]$-πρότυπο.

Για κάθε V_i υπάρχει διατεταγμένη βάση $\widehat{v_i}$ με $(\phi|_{V_i}:\widehat{v_i},\widehat{v_i})=\Sigma[d_i(x)]$, όπου $(d_i(x))=\operatorname{ann}V_i$.

Κατασκευάζουμε τη διατεταγμένη βάση $\widehat{v}=(\widehat{v_1},\widehat{v_2},\dots,\widehat{v_k})$ του V και έχουμε ότι

$$(\phi:\widehat{v},\widehat{v})=\begin{pmatrix}\Sigma[d_1(x)] & & & \\ & \Sigma[d_2(x)] & & \\ & & \ddots & \\ & & & \Sigma[d_k(x)]\end{pmatrix}$$

(ii) Με την υπόθεση του (ii), ο $\Bbbk$-διανυσματικός χώρος V είναι το ευθύ άθροισμα ϕ-αναλλοίωτων υπόχωρων $W_1,W_2,\dots,W_\lambda$ οι οποίοι έχουν διατεταγμένες βάσεις $\widehat{w_1},\widehat{w_2},\dots,\widehat{w_\lambda}$ αντίστοιχα, ώστε $(\phi|_{W_i}:\widehat{w_i},\widehat{w_i})=\Sigma[\delta_i(x)]$.

Άρα κάθε W_i είναι ένα κυκλικό $\Bbbk[x]$-υποπρότυπο του $\Bbbk[x]$-προτύπου V και $\operatorname{ann}W_i=(\delta_i(x))$, δηλαδή $\delta_i(x)=\mu_{\phi|_{W_i}}(x)$.

Καθώς $\delta_1(x)|\delta_2(x),\dots,\delta_{\lambda-1}|\delta_\lambda$ γνωρίζουμε ότι $k=\lambda$ και $d_i(x)=\delta_i(x)$ για κάθε $i=1,2,\dots,k$. □

Πόρισμα 5.1.1. *Έστω $\Bbbk$ σώμα και $A\in\Bbbk^{n\times n}$. Τότε ο A είναι όμοιος με έναν ακριβώς*

πίνακα της μορφής

$$\begin{pmatrix} \Sigma[d_1(x)] & & & \\ & \Sigma[d_2(x)] & & \\ & & \ddots & \\ & & & \Sigma[d_k(x)] \end{pmatrix} \in \Bbbk^{n\times n}$$

όπου τα $d_1(x), d_2(x), \ldots, d_k(x) \in \Bbbk[x]$ *είναι μονικά και* $d_1(x)|d_2(x), \ldots, d_{k-1}(x)|d_k(x)$.

Σχόλιο 5.1.1. Προφανώς, θα πρέπει να ισχύει $\deg(d_1(x)) + \deg(d_2(x)) + \ldots + \deg(d_k(x)) = n$.

Παράδειγμα 5.1.1. Ας βρούμε το πλήθος των κλάσεων ομοιότητας των 3×3 πινάκων επί του $\mathbb{Z}_2$.

Το πλήθος αυτό είναι σε αμφιμονοσήμαντη αντιστοιχία με το πλήθος των ακολουθιών μονικών πολυωνύμων $d_1(x), d_2(x), \ldots, d_k(x)$ όπου $d_1(x)|d_2(x), \ldots, d_{k-1}(x)|d_k(x)$.
Πρέπει $\sum_{i=1}^{k} \deg(d_i(x)) = 3$

Έστω $\deg(d_1(x)) = 1, \deg(d_2(x)) = 1, \deg(d_3(x)) = 1$ και $d_1(x) = d_2(x) = d_3(x)$. Υπάρχουν δύο επιλογές εδώ. Επιλέγουμε είτε το x είτε το $x + 1$.

Έστω $\deg(d_1(x)) = 1, \deg(d_2(x)) = 2$ και $d_2(x) = d_1(x)(x + a)$, για κάποιο $a \in \mathbb{Z}_2$. Σε αυτή την περίπτωση έχουμε 4 επιλογές. Δυο για το $d_1(x)$ και άλλες δυο για το a.

Έστω $\deg(d_1(x)) = 3$. Εδώ υπάρχουν 8 επιλογές.
Συνολικά, λοιπόν, υπάρχουν 14 κλάσεις ομοιότητας.

Παραδείγματος χάριν

Για $d_1(x) = x + 1$ και $d_2(x) = x^2 + x$ έχουμε τον αντιπρόσωπο

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Για $d_1(x) = d_2(x) = d_3(x) = x$ έχουμε τον αντιπρόσωπο

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Πρόταση 5.1.3. *Αν ο* $A \in \Bbbk^{n\times x}$ *είναι όμοιος με τον*

$$\begin{pmatrix} \Sigma[d_1(x)] & & & \\ & \Sigma[d_2(x)] & & \\ & & \ddots & \\ & & & \Sigma[d_k(x)] \end{pmatrix} \in \Bbbk^{n\times n}$$

όπου $d_1(x)|d_2(x), \ldots, d_{k-1}(x)|d_k(x)$, *τότε* $\mu_A(x) = d_k(x)$ *και* $\chi_A(x) = d_1(x)d_2(x)\cdots d_k(x)$.

Απόδειξη. Γνωρίζουμε ότι στη διάσπαση $V = V_1 \oplus V_2 \oplus \ldots \oplus V_k$ του αντίστοιχου $\Bbbk[x]$-προτύπου V όπου $\operatorname{ann} V_1 \supseteq \operatorname{ann} V_2 \supseteq \ldots \supseteq \operatorname{ann} V_k$ ισχύει $\operatorname{ann} V = \operatorname{ann} V_k$, και άρα $\mu(x) = d_k(x)$. Επίσης, γνωρίζουμε από την Γραμμική Άλγεβρα ότι $\chi_A(x) = \prod_{i=1}^{k} \chi_{\Sigma[d_i(x)]}(x) = \prod_{i=1}^{k} d_i(x)$. □

5.2 Κανονική Μορφή Jordan

Πρόταση 5.2.1. *Έστω ότι το $\Bbbk[x]$-πρότυπο V είναι κυκλικό και $\mu(x) = (x-\lambda)^n$ για κάποιο $\lambda \in \Bbbk$. Τότε υπάρχει διατεταγμένη βάση $\widehat{v}$ του V ώστε*

$$(\phi : \widehat{v}, \widehat{v}) = \begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & 1 & \ddots & \\ & & \ddots & \lambda \\ & & & 1 & \lambda \end{pmatrix}$$

*Ο πίνακας αυτός λέγεται **πίνακας Jordan** και συμβολίζεται με $J_{\lambda,n}$.*

Απόδειξη. Γνωρίζουμε ότι $V = \Bbbk[x] \cdot v$ για κάποιο $v \in V$. Θεωρούμε τα διανύσματα

$$v_1 = v, v_2 = (\phi - \lambda)v, \ldots, v_n = (\phi - \lambda)n - 1v$$

και ισχυριζόμαστε ότι αυτά αποτελούν βάση του V.

Καθώς $\dim_{\Bbbk} V = \deg(\mu(x)) = n$ αρκεί να δείξουμε ότι τα $v_1, v_2, \ldots, v_n$ είναι γραμμικά ανεξάρτητα.

Έστω $\lambda_1, \lambda_2, \ldots, \lambda_n \in \Bbbk$ με $\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n = 0$. Τότε

$$\lambda_1 v + \lambda_2(\phi - \lambda)v + \ldots + \lambda_n(\phi - \lambda)^{n-1}v = 0 \in V$$

και άρα

$$[\lambda_1 + \lambda_2(x - \lambda) + \ldots + \lambda_n(x - \lambda)^{n-1}]v = 0 \in V$$

Καθώς $V = \Bbbk[x] \cdot v$, για κάθε $u \in V$ μπορούμε να γράψουμε $u = g(x)v$ για κάποιο $g(x) \in \Bbbk[x]$. Έτσι

$$[\lambda_1 + \lambda_2(x - \lambda) + \ldots + \lambda_n(x - \lambda)^{n-1}]v = f(x)v = f(x)g(x)v = g(x)f(x)v = g(x) = 0 \in V$$

και άρα $f(x) \in \operatorname{ann} V = (\mu(x))$, οπότε $\mu(x) | f(x)$. Αφού, όμως, ο βαθμός του $f(x)$ είναι $\leq n-1$ έπεται ότι $f(x) = 0$, δηλαδή $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

Για να υπολογίσουμε τον πίνακα της ϕ ως προς τη διατεταγμένη βάση $\widehat{v} = (v_1, v_2, \ldots, v_n)$ παρατηρούμε ότι

$$\phi(v_1) = \phi(v) = \phi(v) - \lambda v + \lambda v = (\phi - \lambda)v + \lambda v = v_2 + \lambda v_1$$

$$\phi(v_2) = \phi(\phi - \lambda)(v) = (\phi - \lambda)\phi(v) = (\phi - \lambda)^2 v + \lambda(\phi - \lambda)(v) = v_3 + \lambda v_2$$

$$\vdots$$

$$\phi(v_n) = \phi(\phi - \lambda)^{n-1}(v) = (\phi - \lambda)^n(v) + \lambda(\phi - \lambda)^{n-1}(v) = \lambda v_n$$

Άρα

$$(\phi : \widehat{v}, \widehat{v}) = \begin{pmatrix} \lambda & & & \\ 1 & \lambda & & \\ & 1 & \ddots & \\ & & \ddots & \lambda \\ & & & 1 & \lambda \end{pmatrix}$$

□

Παράδειγμα 5.2.1. Έστω $\mu(x) = (x-4)^3 = x^3 - 12x^2 + 48x - 64$.

Ο συνοδός πίνακας είναι

$$\Sigma[\mu(x)] = \begin{pmatrix} 0 & 0 & 64 \\ 1 & 0 & -48 \\ 0 & 1 & 12 \end{pmatrix}$$

ενώ ο πίνακας Jordan είναι

$$J_{4,3} = \begin{pmatrix} 4 & 0 & 0 \\ 1 & 4 & 0 \\ 0 & 1 & 4 \end{pmatrix}$$

Αυτοί οι πίνακες είναι, προφανώς, όμοιοι.

Πρόταση 5.2.2. *Έστω ότι* $\mu_\phi(x) = \prod_{i=1}^{n}(x-\lambda_i) \in \Bbbk[x]$. *Τότε υπάρχει διατεταγμένη βάση* $\widehat{v}$ *του* V *και ζεύγη* (λ_i, n_i), $i = 1, 2, \ldots, k$ *όπου* $\lambda_i \in \Bbbk$ *και* $n_i \in \mathbb{N}$ *έτσι ώστε*

$$(\phi : \widehat{v}, \widehat{v}) = \begin{pmatrix} J\lambda_1, n_1 & & & \\ & J\lambda_2, n_2 & & \\ & & \ddots & \\ & & & J\lambda_k, n_k \end{pmatrix}$$

Απόδειξη. Καθώς το $\mu_\phi(x) = d_k(x)$ είναι γινόμενο πρωτοβάθμιων παραγόντων αυτό συμβαίνει για κάθε $d_i(x), i = 1, 2, \ldots, k-1$.

Έτσι μπορούμε να γράψουμε $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$, όπου τα $\Bbbk[x]$-υποπρότυπα V_i είναι κυκλικά και $\operatorname{ann} V_i = ((x-\lambda_i)^{n_i})$, για κάποια $\lambda_i \in k$ και $n_i \in \mathbb{N}$.

Με βάση την προηγούμενη πρόταση, μπορούμε να βρούμε μια βάση $\widehat{v_i}$ του V_i ώστε $(\phi|_{V_i} : \widehat{v_i}, \widehat{v_i}) = J_{l_i,n_i}$.

Έτσι, για τη διατεταγμένη βάση $\widehat{v} = (\widehat{v_1}, \widehat{v_2}, \ldots, \widehat{v_k})$ έχουμε

$$(\phi : \widehat{v}, \widehat{v}) = \begin{pmatrix} J\lambda_1, n_1 & & & \\ & J\lambda_2, n_2 & & \\ & & \ddots & \\ & & & J\lambda_k, n_k \end{pmatrix}$$

□

5.3 Ασκήσεις

1.