ΚΕΦΑΛΑΙΟ 2: Ημιαπλοί Δακτύλιοι

Είδαμε στο κύριο θεώρημα του προηγούμενου κεφαλαίου ότι κάθε δακτύλιος διαίρεσης έχει την ιδιότητα “κάθε πρότυπο είναι ευθύ άθροισμα απλών προτύπων”. Εδώ θα χαρακτηρίσουμε όλους τους δακτύλιους με την ιδιότητα αυτή. Η κλάση των δακτυλίων αυτών (ημιαπλοί δακτύλιοι) παίζει σημαντικότατο ρόλο στη θεωρία αναπαραστάσεων πεπερασμένων ομάδων, πράγμα που θα δούμε στο κεφάλαιο 7. Το κύριο θεώρημα του παρόντος κεφαλαίου είναι αυτό του Wedderburn που χαρακτηρίζει τους ημιαπλούς δακτύλιους.

2.1. Θεώρημα του Wedderburn

Ένα R-πρότυπο λέγεται **ημιαπλό** αν είναι ευθύ άθροισμα απλών προτύπων. Ο R λέγεται **ημιαπλός** δακτύλιος αν είναι ημιαπλό ως R-πρότυπο.

2.1.1 Παραδείγματα

1. Κάθε D-πρότυπο είναι ημιαπλό, όπου D είναι δακτύλιος διαίρεσης (Θεώρημα 1.5.1). Ειδικά κάθε k-διανυσματικός χώρος (πεπερασμένης ή άπειρης διάστασης) είναι ημιαπλό k-πρότυπο.
2. Για κάθε πρώτο αριθμό p, το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_p$ είναι απλό και άρα ημιαπλό. Επίσης και το $\mathbb{Z}_p \oplus ... \oplus \mathbb{Z}_p$ είναι ημιαπλό.
3. Έστω $p \neq q$ δυο πρώτοι αριθμοί. Τότε το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_{pq}$ είναι ημιαπλό αφού έχουμε έναν ισομορφισμό $\mathbb{Z}$-προτύπων $\mathbb{Z}_{pq} \simeq \mathbb{Z}_p \oplus \mathbb{Z}_q$.
4. Έστω p ένας πρώτος αριθμός. Το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_{p^2}$ δεν είναι ημιαπλό. Πράγματι, αν ήταν ημιαπλό θα είχαμε έναν ισομορφισμό $\mathbb{Z}$-προτύπων της μορφής $\mathbb{Z}_{p^2} \simeq \bigoplus_{i \in I} M_i$, όπου κάθε M_i είναι απλό $\mathbb{Z}$-πρότυπο. Τότε κάθε M_i θα ήταν ισόμορφο με απλό $\mathbb{Z}$- υποπρότυπο του $\mathbb{Z}_{p^2}$, δηλαδή θα ήταν ισόμορφο με το $\mathbb{Z}_p$ (από την ταξινόμηση υποομάδων πεπερασμένης κυκλικής ομάδας). Τότε $\mathbb{Z}_{p^2} \simeq \bigoplus_{i \in I} \mathbb{Z}_p$ που είναι άτοπο.
5. Το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_n$ είναι ημιαπλό αν και μόνο αν το n δεν διαιρείται με το τετράγωνο ακεραίου >1 (γιατί;)

6. Αν R και S είναι ημιαπλοί δακτύλιοι τότε και ο $R\times S$ είναι ημιαπλός. Πράγματι, γράφοντας $R=\underset{i\in I}{\oplus}R_i$, $S=\underset{j\in J}{\oplus}S_j$, όπου τα R_i και S_j είναι απλά ιδεώδη των R και S αντίστοιχα, βλέπουμε ότι τα απλά ιδεώδη $\overline{R}_i=R_i\times\{0\}$, $\overline{S}_j=\{0\}\times S_j$ του $R\times S$ έχουν την ιδιότητα $R\times S=\left(\underset{i\in I}{\oplus}\overline{R}_i\right)\oplus\left(\underset{j\in J}{\oplus}\overline{S}_j\right)$.

Μια οικογένεια $\{M_i\}_{i\in I}$ υποπροτύπων του M θα λέγεται **ανεξάρτητη** αν

$$\sum_i m_i=0\Rightarrow \quad \text{κάθε} \quad m_i=0,$$

όπου $m_i\in M_i$ είναι όλα σχεδόν μηδέν. Τότε ορίζεται το εσωτερικό ευθύ άθροισμα σύμφωνα με την Πρόταση 1.2.1 και ισχύει

$$\sum_{i\in I}M_i=\underset{i\in I}{\oplus}M_i.$$

2.1.2 Πρόταση. *i) Κάθε πρότυπο που παράγεται από απλά πρότυπα είναι ημιαπλό.*
ii) Έστω $0\to L\to M\to N\to 0$ μια ακριβής ακολουθία R-προτύπων, όπου το M είναι ημιαπλό. Τότε τα L, N είναι ημιαπλά R-πρότυπα και επιπλέον η ακολουθία διασπάται.

Απόδειξη: i) Έστω $M=\sum_{i\in I}M_i$, όπου τα M_i είναι απλά υποπρότυπα του M. Θα δείξουμε ότι $M=\underset{j\in J}{\oplus}M_j$, για κάποιο $J\subseteq I$. Με τη βοήθεια του λήμματος του Zorn, εύκολα επαληθεύεται ότι το σύνολο

$$\{J\subseteq I\mid\{M_j\}_{j\in J} \ \text{είναι ανεξάρτητο}\}$$

έχει μέγιστο στοιχείο, έστω J'. Ισχύει $M=\underset{j\in J'}{\oplus}M_j$. Πράγματι, $\underset{j\in J'}{\oplus}M_j\subseteq M$. Για την άλλη σχέση, θεωρούμε ένα τυχαίο M_i και παρατηρούμε ότι

$$M_i\cap\left(\underset{j\in J'}{\oplus}M_j\right)=0 \quad \text{ή} \quad M_i,$$

γιατί το M_i είναι απλό. Η πρώτη περίπτωση δεν ισχύει λόγω του μεγίστου του J'. Συνεπώς

$$M_i\cap\left(\underset{j\in J'}{\oplus}M_j\right)=M_i$$

για κάθε $i\in I$. Άρα $M_i\subseteq\underset{j\in J'}{\oplus}M_j$ για κάθε i και $M\subseteq\underset{j\in J'}{\oplus}M_j$.

ii) Έστω $g: M \to N$ ο επιμορφισμός της δοθείσας ακριβούς ακολουθίας. Γράφουμε $M \subseteq \bigoplus_{i \in I} M_i$, όπου κάθε M_i είναι απλό, και παρατηρούμε ότι $g(M_i) = 0$ ή $g(M_i) \cong M_i$. Άρα η εικόνα $g(M) = N$ παράγεται από κάποια απλά πρότυπα, οπότε λόγω του i) είναι ημιαπλό πρότυπο. Το ίδιο ισχύει και για τον πυρήνα $Kerg = L$, δηλαδή το $\ker g \simeq \bigoplus_{j \in J} M_j$ για κάποιο $J \subseteq I$. Τέλος, ο $\ker g$ είναι ευθύς προσθετέος του M και συνεπώς η ακριβής ακολουθία διασπάται (Πρόταση 1.2.4).

■

Σημειώνουμε ότι, σύμφωνα με την προηγούμενη πρόταση, κάθε υποπρότυπο και κάθε πηλίκο ημιαπλού προτύπου είναι ημιαπλό πρότυπο.

Τονίζουμε ότι δεν ισχύει το αντίστροφο του πρώτου ισχυρισμού της Πρότασης 2.1.2 ii). Για παράδειγμα, αν p είναι πρώτος, το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_{p^2}$ δεν είναι ημιαπλό ενώ το $\mathbb{Z}_p$ είναι ημιαπλό και έχουμε την ακριβή ακολουθία

$0 \to \mathbb{Z}_p \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p \to 0.$

2.1.3 Θεώρημα Weddeburn. *Για κάθε δακτύλιο R οι παρακάτω συνθήκες είναι ισοδύναμες.*

1) R είναι ημιαπλός

2) κάθε R-πρότυπο είναι ημιαπλό

3) κάθε ακριβής ακολουθία $0 \to A \to B \to C \to 0$ *R-προτύπων διασπάται*

4) κάθε R-πρότυπο είναι προβολικό

5) κάθε R-πρότυπο είναι εμφυτευτικό

6) ως δακτύλιοι $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s)$, *όπου κάθε* D_i *είναι δακτύλιος διαίρεσης.*

Απόδειξη. $1) \Rightarrow 2)$.

Από την υπόθεση και την Πρόταση 1.3.1 i) κάθε ελεύθερο *R*-πρότυπο είναι ημιαπλό. Από την Πρόταση 1.3.1 ii) προκύπτει ότι κάθε *R*-πρότυπο είναι ημιαπλό.

$2) \Rightarrow 3)$.

Επειδή το *B* είναι ημιαπλό, η ακριβής ακολουθία $0 \to A \to B \to C \to 0$ διασπάται σύμφωνα με την Πρόταση 2.1.1 ii).

$3) \Rightarrow 1)$.

Παρατήρηση: Με την υπόθεση 3) ισχύει ότι κάθε ιδεώδες $I \neq 0$ του *R* περιέχει ένα απλό ιδεώδες.

Απόδειξη: Έστω $a \in I,\ a \neq 0$. Έστω ότι το κύριο ιδεώδες (a) δεν είναι απλό. Τότε υπάρχει ιδεώδες J με $0 \underset{\neq}{\subseteq} J \underset{\neq}{\subseteq} (a)$. Χρησιμοποιώντας το λήμμα του Zorn, συμπεραίνουμε ότι υπάρχει μέγιστο τέτοιο *J*. (Η απόδειξη είναι πανομοιότυπη με αυτή της Πρότασης 1.4.2 με την παρατήρηση ότι το ρόλο του 1 παίζει εδώ το α). Η ακριβής ακολουθία *R*-προτύπων

$$0 \to J \to (a) \to (a)/J \to 0$$

διασπάται σύμφωνα με την υπόθεση. Έτσι το $(a)/J$ είναι ισόμορφο ως *R*-πρότυπο με ιδεώδες του *R*, που είναι απλό λόγω του μεγίστου του *J*.

Επιστρέφουμε τώρα στην απόδειξη $3) \Rightarrow 1)$. Έστω *I* το ιδεώδες που παράγεται απ'όλα τα απλά ιδεώδη του *R*. Είναι $I \neq 0$ λόγω της παρατήρησης. Από την ακριβή ακολουθία

$$0 \to I \to R \to R/I \to 0$$

και την υπόθεση παίρνουμε ότι το R/I είναι ισόμορφο με ιδεώδες *J* του *R*. Ισχύει $I \cap J = 0$, γιατί η προηγούμενη ακολουθία διασπάται. Αν $J \neq 0$, η παρατήρηση μας πληροφορεί ότι το *J* περιέχει απλό ιδεώδες και κατά συνέπεια ο ορισμός του *I* δίνει $I \cap J \neq 0$, άτοπο. Άρα $R/I = 0$, δηλαδή $R = I$. Από τον ορισμό του *I* και την Πρόταση 2.1.2 i) παίρνουμε ότι το *R* είναι ημιαπλός.

$(3) \Leftrightarrow (4) \Leftrightarrow (5)$

Έπεται αμέσως από την Πρόταση 1.3.3 ii) και τον ορισμό στη Σημείωση 1.3.6.

$(1) \Rightarrow (6)$

Ξεκινάμε με τρεις απλές παρατηρήσεις.

α) Υπάρχει ισομορφισμός δακτυλίων $R^{op} \cong End_R(R),\ r \mapsto f_r$, όπου $f_r(a) = ar$ (πολλαπλασιασμός από δεξιά), $a, r \in R$. (Άσκηση 1.3).

β) Έστω *M* ένα *R*-πρότυπο. Τότε υπάρχει ισομορφισμός δακτυλίων

$$End_R(M^n) \cong M_n(End_R(M)).$$

Πράγματι, αν $g \in End_R(M^n)$ θέτουμε $g_{ij} \in End_R(M)$,

$$g_{ij} : M \xrightarrow{\varepsilon_j} M \oplus \ldots \oplus \xrightarrow{g} M \oplus \ldots \oplus M \xrightarrow{\pi_i} M$$

όπου $\varepsilon_j(m) = (0,\ldots,m,\ldots,0)$ είναι η εμφύτευση στη *j* συνιστώσα και $\pi_i(m_1,\ldots,m_n) = m_i$ είναι η προβολή στην *i* συνιστώσα. Ορίζεται έτσι ομομορφισμός δακτυλίων

$$\Phi : End_R(M^n) \to M_n(End_R(M)), \quad (g) \mapsto (g_{ij}).$$

Στην αντίθετη κατεύθυνση ορίζουμε ομομορφισμό δακτυλίων

$$\Psi : M_n(End_R(M)) \to End_R(M^n), \ (f_{ij}) \mapsto f$$

όπου, $f(m_1,...,m_n) = \left(\sum_k f_{1k}(m_k),...,\sum_k f_{nk}(m_k) \right)$. (Συμβολικά, $f(m_1,...,m_n)$ $= (f_{ij}) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$ "πολλαπλασιασμός" πινάκων). Είναι θέμα ρουτίνας να επαληθεύσουμε ότι οι συνθέσεις $\Phi \circ \Psi$ και $\Psi \circ \Phi$ είναι οι αντίστοιχες ταυτοτικές συναρτήσεις.

γ) Έστω *M, N* δυο *R*-πρότυπα με $Hom_R(M,N) = Hom_R(N,M) = 0$. Τότε υπάρχει ισομορφισμός δακτυλίων $End_R(M \oplus N) \cong End_R(M) \times End_R(N)$. Πράγματι, λόγω της Πρότασης 1.2.2 και της υπόθεσης στα *M, N* υπάρχει ισομορφισμός αβελιανών ομάδων $End_R(M \oplus N) \cong End_R(M) \times End_R(N)$. Αυτός ο συγκεκριμένος ισομορφισμός (δες την απόδειξη της Πρότασης 1.2.2) εύκολα επαληθεύεται ότι είναι ισομορφισμός δακτυλίων.

Επιστρέφουμε τώρα στην απόδειξη $(1) \Rightarrow (6)$. Έστω $R = \bigoplus_{i \in I} M_i$, όπου τα M_i είναι απλά ιδεώδη. Επειδή το *R* είναι πεπερασμένα παραγόμενο *R*-πρότυπο το ίδιο συμβαίνει για το $\bigoplus_{i \in I} M_i$. Άρα μόνο πεπερασμένου πλήθους συνιστώσες του $\bigoplus_{i \in I} M_i$ είναι μη-μηδενικές, δηλαδή το *I* είναι πεπερασμένο. Μπορούμε έτσι να γράψουμε

$$R \cong \bigoplus_{i=1}^{s} M_i^{n_i} \quad \text{όπου} \quad M_i \cong M_j \Leftrightarrow i = j .$$

Έχουμε τώρα διαδοχικά ισομορφισμούς δακτυλίων

$$\begin{aligned}
R &\cong (R^{op})^{op} \\
&\cong (End_R(R))^{op} && \text{(παρατήρηση α)} \\
&= \left(End_R\left(\bigoplus_{i=1}^{s} M_i^{n_i} \right) \right)^{op} \\
&\cong \left(\prod_{i=1}^{s} End_R(M_i^{n_i}) \right)^{op} && \text{(γιατί } Hom_R(M_i^{n_i}, M_j^{n_j}) = 0 \text{ αν } i \neq j\text{. Παρατήρηση γ)} \\
&\cong \prod_{i=1}^{s} \left(End_R(M_i^{n_i})^{op} \right) && \left((R \times S)^{op} \cong R^{op} \times S^{op} \right)
\end{aligned}$$

$\cong \prod_{i=1}^{s}\left(M_{n_i}(End_R(M_i)^{op})\right)$. (παρατήρηση β και άσκηση 1.3.3 iii)).

Από το λήμμα του Schur (Λήμμα 1.1.7), κάθε $End_R(M_i)$ είναι δακτύλιος διαίρεσης και συνεπώς κάθε $D_i := End_R(M_i)^{op}$ είναι δακτύλιος διαίρεσης. Έχουμε $R \cong \prod_{i=1}^{s} M_{n_i}(D_i)$.

$(6) \Rightarrow (1)$

Λόγω του Παραδείγματος 2.1.1 6), για να δείξουμε ότι $(6) \Rightarrow (1)$ αρκεί να δείξουμε ότι: D δακτύλιος διαίρεσης $\Rightarrow M_n(D)$ ημιαπλός δακτύλιος.

Έστω I_k το (αριστερό) ιδεώδες του $M_n(D)$ που αποτελείται από πίνακες της μορφής

$$\begin{pmatrix} 0 & \cdots a_1 \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots a_n \cdots & 0 \end{pmatrix}$$

όπου τα a_i υπάρχουν στην k στήλη. Προφανώς $M_n(D) = I_1 \oplus \ldots \oplus I_n$. Θα δείξουμε ότι κάθε I_k είναι απλό. Έστω $\alpha \in (\alpha_{ij}) = I_k$, $\alpha \neq 0$, και $\beta \in I_k$. Με E_{ij} συμβολίζουμε τον $n \times n$ πίνακα που έχει μηδέν παντού εκτός από τη θέση (i, j), όπου το στοιχείο είναι 1. Αφού $\alpha \neq 0$ υπάρχει i_0 με $\alpha_{i_0 k} \neq 0$. Αν γράψουμε $\beta = \sum_j \beta_j E_{jk}$, τότε εύκολα ελέγχουμε με πράξεις πινάκων ότι

$$\beta = \left(\sum_j \beta_j \alpha_{i_0 k}^{-1} E_{j i_0}\right)\alpha .$$

Άρα το I_k παράγεται σαν ιδεώδες από το τυχαίο μη μηδενικό στοιχείο του. Η απόδειξη είναι πλήρης.

■

Σημειώνουμε ότι η συνθήκη 6) στο Θεώρημα του Wedderburn είναι ιδιαίτερα σημαντική καθώς μας παρέχει πληροφορίες για τη ‘δομή’ του δακτυλίου R.

2.1.4 Παρατήρηση. Στην προηγούμενη απόδειξη, είδαμε ότι κάθε ημιαπλός δακτύλιος έχει πεπερασμένο πλήθος απλά ιδεώδη και επιπλέον είναι το ευθύ άθροισμά τους.

2.2 Εφαρμογή: Θεώρημα του Maschke.

Το επόμενο αποτέλεσμα μας πληροφορεί πότε ο δακτύλιος $k[G]$ μιας πεπερασμένης ομάδας G (όπου k είναι σώμα) είναι ημιαπλός, πράγμα που θα χρησιμοποιηθεί στο κεφάλαιο 7 (αναπαραστάσεις πεπερασμένων ομάδων).

2.2.1 Θεώρημα *(Maschke). Έστω G μια πεπερασμένη ομάδα τάξης n και k σώμα χαρακτηριστικής p. Αν $p = 0$ ή αν $p > 0$ και το p δεν διαιρεί το n, τότε ο δακτύλιος $k[G]$ είναι ημιαπλός. Αντίστροφα, αν p διαιρεί το n, τότε ο δακτύλιος $k[G]$ δεν είναι ημιαπλός.*

Απόδειξη: "$\Rightarrow$" Έστω

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \qquad (*)$$

μια ακριβής ακολουθία $k[G]$-προτύπων. Θα δείξουμε ότι διασπάται (Θεώρημα 2.1.3 3)). Θεωρώντας την (*) ως ακολουθία k-διανυσματικών χώρων αυτή διασπάται (Πρόταση 1.3.2). Έτσι υπάρχει k-γραμμική απεικόνιση $\beta' : C \to B$ με την ιδιότητα $\beta \circ \beta' = 1_C$. Από την β' κατασκευάζουμε έναν ομομορφισμό $k[G]$-προτύπων[1]

$$\overline{\beta} : C \to B, \quad \overline{\beta}(c) = \frac{1}{n} \sum_{g \in G} g\beta'(g^{-1}c).$$

Παρατηρούμε εδώ ότι στο k έχουμε $n \neq 0$ λόγω της υπόθεσης στο p. Η απεικόνιση $\overline{\beta}$ είναι πράγματι ομομορφισμός $k[G]$-προτύπων, γιατί αν $h \in G$ τότε

$$\begin{aligned}
\overline{\beta}(hc) &= \frac{1}{n} \sum_{g \in G} g\beta'(g^{-1}hc) \\
&= h\left(\frac{1}{n} \sum_{g \in G} h^{-1}g\beta'(g^{-1}hc)\right) \\
&= h\left(\frac{1}{n} \sum_{g' \in G} g'\beta'((g')^{-1}c)\right) \qquad \text{(γιατί καθώς το } g \text{ διατρέχει τη } G\text{, το } h^{-1}g = g' \text{ διατρέχει τη } G\text{).} \\
&= h(\overline{\beta}(c)).
\end{aligned}$$

Δηλαδή $\overline{\beta}(hc) = h\overline{\beta}(c)$ για κάθε $h \in G$ και $c \in G$. Επειδή η $\overline{\beta}$ είναι προφανώς προσθετική προκύπτει ότι η $\overline{\beta}$ είναι ομομορφισμός $k[G]$-προτύπων. Τέλος έχουμε

[1] Η ιδέα είναι να αντικαταστήσουμε την απεικόνιση β', που είναι μόνο ομομορφισμός k – προτύπων, με άλλη που είναι ομομορφισμός $k[G]$ - προτύπων. Αυτό επιτυγχάνεται λαμβάνοντας το 'μέσο όρο' της β' υπεράνω της ομάδας G.

$\beta \circ \overline{\beta} = 1$, γιατί αν $c \in k[G]$ τότε

$$\beta\overline{\beta}(c) = \frac{1}{n}\sum_{g \in G} \beta(g\beta'(g^{-1}c))$$

$$= \frac{1}{n}\sum_{g \in G} g(\beta\beta'(g^{-1}c)) \quad \text{(γιατί } \beta \text{ είναι ομομορφισμός } k[G]\text{-προτύπων)}$$

$$= \frac{1}{n}\sum_{g \in G} g1_C(g^{-1}c)$$

$$= \frac{1}{n}(nc) = c.$$

"$\Leftarrow$" Έστω τώρα ότι το $p > 0$ διαιρεί το *n*. Θεωρούμε το *k* ως *k*[*G*]-πρότυπο, $\left(\sum_{g \in G} r_g g\right) v = \left(\sum_{g \in G} r_g\right) v$ για κάθε $v \in k$. Θα δείξουμε ότι η ακριβής ακολουθία

$$0 \longrightarrow \ker \varepsilon \longrightarrow k[G] \xrightarrow{\varepsilon} k \longrightarrow 0$$

δεν διασπάται, όπου $\varepsilon : k[G] \to k$ είναι ο ομομορφισμός *k*[*G*]-προτύπων $\varepsilon\left(\sum_{g \in G} r_g g\right) = \sum_{g \in G} r_g$. Έστω για άτοπο ότι υπάρχει ομομορφισμός *k*[*G*]-προτύπων $\varepsilon' : k \to kG$ με $\varepsilon\varepsilon' = 1_k$ και έστω $\varepsilon'(1) = \sum_{g \in G} r_g g$. Τότε για κάθε $h \in G$ ισχύει $\varepsilon'(1) = \varepsilon'(h \cdot 1) = h\varepsilon'(1) = h\sum_{g \in G} r_g g$. Άρα

$$\sum_{g \in G} r_g g = h\sum_{g \in G} r_g g \quad \text{για κάθε} \quad h \in G.$$

Συνεπώς $r_g = r_{g'}$ για κάθε $g, g' \in G$ (γιατί;). Άρα υπάρχει $r \in k$ με $\varepsilon'(1) = r\left(\sum_{g \in G} g\right)$.

Όμως τότε $\varepsilon\varepsilon'(1) = r\varepsilon\left(\sum_{g \in G} g\right) = rn = 0$, που είναι άτοπο γιατί $\varepsilon\varepsilon' = 1_k$.

■

2.3. Παρατηρήσεις στο Θεώρημα του Wedderburn

Έστω *R* ένας ημιαπλός δακτύλιος. Θα ασχοληθούμε εδώ με τα εξής ερωτήματα. Από το θεώρημα του Wedderburn έχουμε $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s)$, όπου κάθε D_i είναι δακτύλιος διαίρεσης. Είναι οι αριθμοί $n_1, \ldots, n_s$, s μονοσήμαντα ορισμένοι; (Θα δούμε ότι η απάντηση είναι ναι). Πόσα ανά δύο μη ισόμορφα απλά πρότυπα έχει ο *R*;

Ένας δακτύλιος $R \neq 0$ λέγεται **απλός** αν δεν έχει αμφίπλευρα ιδεώδη $\neq 0, R$. Σημειώνουμε ότι, αν R είναι απλός, τότε δεν έπεται αναγκαστικά ότι είναι απλό R-πρότυπο. Αν όμως είναι απλό R-πρότυπο, τότε είναι απλός δακτύλιος.

Για παράδειγμα κάθε δακτύλιος διαίρεσης είναι απλός. Πιο γενικά έχουμε:

2.3.1 Λήμμα. *Ο $M_n(D)$ είναι απλός όταν ο D είναι δακτύλιος διαίρεσης.*

Απόδειξη: Έστω $I \neq 0$ αμφίπλευρο ιδεώδες του R. Θα δείξουμε ότι $I = R$. Έστω $\alpha = (\alpha_{ij}) \in I$ με $\alpha \neq 0$. Τότε $\alpha_{ke} \neq 0$ για κάποιους δείκτες k, ℓ. Για τους στοιχειώδεις πίνακες E_{ij} ισχύει

$$E_{ij}E_{pq} = \begin{cases} 0 & , \text{αν } \ j \neq p \\ E_{iq}, & \text{αν } \ j = p. \end{cases} \qquad (*)$$

Γράφοντας $\alpha = \sum_{i,j} \alpha_{ij} E_{ij}$ παίρνουμε από την προηγούμενη σχέση

$$E_{\ell k}\alpha E_{\ell k} = \sum_{i,j} \alpha_{ij}(E_{\ell k}E_{ij})E_{\ell k} = \sum_{j} \alpha_{kj}E_{\ell j}E_{\ell k} = \alpha_{k\ell}E_{\ell k} .$$

Άρα το I περιέχει το $\alpha_{k\ell}E_{\ell k}$ και συνεπώς το $E_{\ell k} = \alpha_{k\ell}^{-1}(\alpha_{k\ell}E_{\ell k})$. Από την (*) προκύπτει ότι $E_{ij} \in I$ για κάθε i, j. Άρα $I = R$.

■

2.3.2 Λήμμα. *Έστω $R = R_1 \times \ldots \times R_m$ και $R = R_1' \times \ldots \times R_n'$ όπου οι R_i και R_i' είναι απλοί δακτύλιοι. Τότε $m = n$ και (μετά από κάποια αρίθμηση) $R_1 = R_1', \ldots, R_m = R_m'$.*

Απόδειξη: Επαγωγή στο $d = \min\{m, n\}$. Η περίπτωση $d = 1$ είναι προφανής. Θεωρώντας τα R_i και R_j' ως αμφίπλευρα ιδεώδη του R έχουμε $R_1R = R_1R_1' \times \ldots \times R_1R_n'$ και άρα $R_1 = R_1R_1' \times \ldots \times R_1R_n'$. Δεν μπορεί να ισχύει $R_1R_j' = 0$ για κάθε j γιατί $R_1 \neq 0$ και άρα για κάποιο j έχουμε $R_1R_j' \neq 0$. Τότε το μη μηδενικό αμφίπλευρο ιδεώδες R_1R_j' περιέχεται και στο R_1 και στο R_j'. Συνεπώς από την υπόθεση περί απλών δακτυλίων παίρνουμε $R_1 = R_j'$. Υποθέτοντας χωρίς βλάβη της γενικότητας ότι $j = 1$, παίρνουμε $R_2 \times \ldots \times R_m = R_2' \times \ldots \times R_n'$ οπότε εφαρμόζει η επαγωγική υπόθεση.

■

Τα δύο προηγούμενα λήμματα δίνουν αμέσως το εξής:

2.3.3 Πόρισμα. *Έστω R ένας ημιαπλός δακτύλιος οπότε*

$$R \cong M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s)$$

όπου κάθε D_i *είναι δακτύλιος διαίρεσης. Τότε ο αριθμός* s *είναι μονοσήμαντα ορισμένος.*

■

Το s στο παραπάνω πόρισμα είναι ο *αριθμός των απλών συνιστωσών του R*. Θα δώσουμε παρακάτω ένα άλλο χαρακτηρισμό του s (Πρόταση 2.3.5) που θα βρει εφαρμογή στην απόδειξη του Θεωρήματος 3.3.1.

Έστω I_1, I_2 ιδεώδη των δακτυλίων R_1, R_2 αντίστοιχα Τα σύνολα $I_1 \times 0$ και $0 \times I_2$ είναι $R_1 \times R_2$-πρότυπα. (ως ιδεώδη του $R_1 \times R_2$).

2.3.4 Λήμμα. *Με τους προηγούμενους συμβολισμούς ισχύει ότι κάθε ομομορφισμός* $R_1 \times R_2$*-προτύπων* $I_1 \times 0 \to 0 \times I_2$ *είναι ο μηδενικός.*

Απόδειξη: Έστω ομομορφισμός $R_1 \times R_2$-προτύπων, $\varphi\colon I_1 \times 0 \to 0 \times I_2$ και έστω $r_1 \in R_1$. Αν $\varphi(r_1, 0) = (0, r_2)$, τότε

$$\varphi(r_1,0) = \varphi((e_1,0)(r_1,0) = (e_1,0)\varphi(r_1,0) = (e_1,0)(0,r_2) = (0,0),$$

όπου e_1 είναι το μοναδιαίο στοιχείο του R_1.

■

2.3.5 Πρόταση. *Έστω R ένας ημιαπλός δακτύλιος οπότε*

$$R \cong M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s),$$

όπου κάθε D_i *είναι δακτύλιος διαίρεσης. Τότε το πλήθος των ανά δύο μη ισόμορφων απλών R-προτύπων είναι* s.

Απόδειξη: Πρώτα θα δείξουμε ότι ο *R* έχει *τουλάχιστον* s ανά δύο μη ισόμορφα απλά πρότυπα.

Έστω V_{ij} το απλό $M_{n_i}(D_i)$-πρότυπο που αποτελείται από πίνακες της μορφής

$$\begin{array}{c} \text{στήλη } i \\ \begin{pmatrix} 0 & \cdots & a_1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & a_{n_i} & \cdots & 0 \end{pmatrix} \end{array} \in M_{n_i}(D_i)$$

(Το ότι το V_{ij} είναι απλό αποδείχτηκε στο (6)$\Rightarrow$(1) του Θεωρήματος του Wedderburn). Έστω

$$\overline{V_{ij}} = 0\times\ldots\times V_{ij}\times\ldots\times 0 \subseteq M_{n_1}(D_1)\times\ldots\times M_{n_s}(D_s)$$

όπου το V_{ij} βρίσκεται στην i συνιστώσα. Τότε βέβαια το $\overline{V_{ij}}$ είναι απλό $M_{n_1}(D_1)\times\ldots\times M_{n_s}(D_s)$-πρότυπο. Από το Λήμμα 2.3.4 (με την προφανή γενίκευση για πεπερασμένο πλήθος συνιστώσες R_i) προκύπτει ότι $\overline{V_{ij}} \ncong \overline{V_{i'j'}}$ για $i \neq i'$.

Θα δείξουμε τώρα ότι ο R έχει το *πολύ* s ανά δύο μη ισόμορφα απλά πρότυπα. Έστω V απλό R-πρότυπο. Επειδή ισχύει

$$M_{n_i}(D_i) = V_{i1}\oplus\ldots\oplus V_{in_i}$$

και

$$V_{i1}\cong\ldots\cong V_{in_i} \text{ ως } M_{n_i}(D_i)\text{-πρότυπα}$$

παίρνουμε

$$R \cong \overline{V}_{11}^{n_1}\oplus\ldots\oplus\overline{V}_{s1}^{n_s}. \qquad (**)$$

Επειδή τώρα το V είναι απλό θα είναι πηλίκο του R (άσκηση 1.11) και συνεπώς πηλίκο του δεξιού σκέλους της (**). Η Πρόταση 2.1.2 ii) και το γεγονός ότι το V είναι απλό δίνει ότι το V είναι ισόμορφο με ένα από τα V_{i1}.

■

Γνωρίζουμε λοιπόν ότι σε έναν ημιαπλό δακτύλιο R κάθε απλή συνιστώσα του $M_{n_i}(D_i)$ συνεισφέρει ακριβώς ένα απλό R-πρότυπο V_i και το σύνολο αυτών είναι ακριβώς ένα σύνολο των ανά δύο μη ισόμορφων απλών R-προτύπων.

2.3.6 Πόρισμα. *Έστω R ημιαπλός δακτύλιος οπότε*

$$R \cong M_{n_1}(D_1)\times\ldots\times M_{n_s}(D_s),$$

όπου κάθε D_i είναι δακτύλιος διαίρεσης. Έστω $V_1,\ldots,V_s$ τα αντίστοιχα απλά R-πρότυπα. Τότε για κάθε i

- *υπάρχει ισομορφισμός δακτυλίων $End_R(V_i)\simeq D_i^{op}$ και συνεπώς οι D_i είναι μονοσήμαντα ορισμένοι*
- $n_i = \dim_{D_i} V_i$*, και συνεπώς οι αριθμοί n_i είναι μονοσήμαντα ορισμένοι.*

Απόδειξη: Για τον ισομορφισμό $End_R(V_i) \simeq D_i^{op}$ βλ άσκηση 16. Η σχέση $n_i = \dim_{D_i} V_i$ είναι σαφής.

■

Για τα παραδείγματα που ακολουθούν χρειαζόμαστε την εξής πρόταση.

2.3.7 Πρόταση *Έστω A μια k-άλγεβρα διαίρεσης, όπου k αλγεβρικά κλειστό σώμα, με* $\dim_k A = n < \infty$. *Τότε* $A = k$.

Απόδειξη: Έστω $a \in A$ και $\ker \Phi = \left(f(x) \right)$ ο πυρήνας του ομομορφισμού αλγεβρών $\Phi : k[x] \to A,\ \Phi(g(x)) = g(a),\ g(x) \in k[x]$. Λαμβάνουμε έναν μονομομορφισμό αλγεβρών $k[x]/\left(f(x) \right) \to A$. Επειδή τα στοιχεία $1, a, a^2, ..., a^n$ είναι γραμμικά εξαρτημένα υπεράνω του *k*, έχουμε $\deg f(x) \geq 1$. Επειδή ο *A* δεν έχει διαιρέτες του μηδενός, το $f(x)$ είναι ανάγωγο, και αφού το *k* είναι αλγεβρικά κλειστό έχουμε $\deg f(x) = 1$. Άρα $f(x) = f_0 + f_1 x$, όπου $f_0, f_1 \in k$, οπότε $f_0 + af_1 = 0$ και επομένως $a \in k$.

■

2.3.8 Πόρισμα *Έστω k ένα αλγεβρικά κλειστό σώμα και G μια πεπερασμένη ομάδα τέτοια ώστε ο δακτύλιος* $k[G]$ *είναι ημιαπλός, οπότε* $k[G] \cong M_{n_1}(D_1) \times ... \times M_{n_s}(D_s)$ *για κάποιους δακτύλιους διαίρεσης* D_i. *Τότε για κάθε i έχουμε* $D_i = k$.

2.3.9 Παραδείγματα

1) Έστω G μια αβελιανή ομάδα με $|G| = n < \infty$. Τότε $\mathbb{C}[G] \simeq \mathbb{C} \times ... \times \mathbb{C}$ (*n* φορές).
Πράγματι, από το Θεώρημα του Maschke, ο δακτύλιος $\mathbb{C}[G]$ είναι ημιαπλός. Από το Θεώρημα του Wedderburn έχουμε $\mathbb{C}[G] \cong M_{n_1}(D_1) \times ... \times M_{n_s}(D_s)$, όπου D_i δακτύλιοι διαίρεσης. Από το Πόρισμα 2.3.8 έχουμε $\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times ... \times M_{n_s}(\mathbb{C})$. Επειδή η *G* είναι αβελιανή παίρνουμε $n_1 = ... = n_s = 1$. Αφού $\dim_{\mathbb{C}} \mathbb{C}[G] = n$ έχουμε $s = n$ και $\mathbb{C}[G] \simeq \mathbb{C} \times ... \times \mathbb{C}$.

Σημείωση: Από το προηγούμενο παράδειγμα φαίνεται ότι υπάρχει ισομορφισμός αλγεβρών $\mathbb{C}[\mathbb{Z}_4] \simeq \mathbb{C}[\mathbb{Z}_2 \times \mathbb{Z}_2]$ αν και οι ομάδες $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ δεν είναι ισόμορφες.

2) Έστω G μια μη αβελιανή ομάδα τάξης 8. Τότε $\mathbb{C}[G]\cong\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times M_2(\mathbb{C})$. Πράγματι, όπως πριν έχουμε $\mathbb{C}[G]\cong M_{n_1}(\mathbb{C})\times\ldots\times M_{n_s}(\mathbb{C})$. Θεωρώντας διαστάσεις διανυσματικών χώρων παίρνουμε $8=n_1^2+\ldots+n_s^2$ οπότε έχουμε τις εξής περιπτώσεις

$i)$ $n_1=\ldots=n_8=1$
$ii)$ $n_1=n_2=2$
$iii)$ $n_1=\ldots=n_4=1, n_5=2.$

Η περίπτωση i) απορρίπτεται γιατί η G δεν είναι αβελιανή. Η περίπτωση ii) απορρίπτεται γιατί κάποιο n_i πρέπει να είναι ίσο με 1 σύμφωνα με το Πόρισμα 2.3.6, αφού υπάρχει απλό $\mathbb{C}[G]$-πρότυπο διάστασης 1: το $\mathbb{C}$ με εξωτερικό πολλαπλασιασμό $\left(\sum_{g\in G} r_g g\right)v=\left(\sum_{g\in G} r_g\right)v$ για κάθε $v\in\mathbb{C}$ (βλ. την απόδειξη του $'\Leftarrow'$ του Θεωρήματος του Maschke). Από την περίπτωση iii) προκύπτει το ζητούμενο.

Ασκήσεις

1. (Οι άνω τριγωνικοί πίνακες δεν είναι γενικά ημιαπλοί δακτύλιοι).

Έστω $R=\left\{\left.\begin{pmatrix} a & b\\ 0 & c\end{pmatrix}\right| \; a,b,c\in\mathbb{C}\right\}$. Αποδείξτε ότι ο R δεν είναι ημιαπλός.

Υπόδειξη: Ένας τρόπος είναι να θέσουμε $M=\mathbb{C}^2$ με εξωτερικό πολλαπλασιασμό τον πολλαπλασιασμό πινάκων $\begin{pmatrix} a & b\\ 0 & c\end{pmatrix}\begin{pmatrix} x\\ y\end{pmatrix}=\begin{pmatrix} ax+by\\ cy\end{pmatrix}$. Έστω L το υποπρότυπο του M που παράγεται από το $\begin{pmatrix} 1\\ 0\end{pmatrix}$. Τότε η ακριβής ακολουθία $0\to L\to M\to M/L\to 0$ δεν διασπάται.

2. Έστω M ένα πεπερασμένο παραγόμενο D-πρότυπο, όπου D δακτύλιος διαίρεσης. Ποιά μορφή έχουν τα $End_D(M)$-πρότυπα;

Υπόδειξη: Αποδείξτε ότι ο $End_D(M)$ είναι δακτύλιος πινάκων με στοιχεία από δακτύλιο διαίρεσης και εφαρμόστε αποτελέσματα σχετικά με τη θεωρία των δακτυλίων αυτών.

3. Ποιοι από τους παρακάτω δακτύλιους είναι ημιαπλοί; Για του ημιαπλούς δακτύλιους ποιά μορφή έχουν είναι τα απλά πρότυπα;

1) $\mathbb{Z}$, 2) $\mathbb{Q}$, 3) $\mathbb{C}[x]$, 4) $\mathbb{C}[x,y]$, 5) $\mathbb{Q}[x]/(x^2-2)$.

Υπόδειξη για το $\mathbb{C}[x]$: ένας από τους πολλούς τρόπους απόδειξης είναι να παρατηρήσουμε ότι αν ήταν ημιαπλός, τότε από ο Θεώρημα του Wedderburn έπεται ότι $s=1, n_1=1$ και άρα ο $\mathbb{C}[x]$ είναι δακτύλιος διαίρεσης, άτοπο.

4. Ένα *R*-πρότυπο είναι ημιαπλό αν και μόνο αν κάθε κυκλικό υποπρότυπό του είναι ημιαπλό.

5. i) Αν ο R είναι ημιαπλός, τότε το κέντρο του *R* είναι ημιαπλός δακτύλιος.
Υπόδειξη: Άσκηση 1.10.
ii) Κάθε μεταθετικός ημιαπλός δακτύλιος είναι ευθύ γινόμενο σωμάτων.

6.
i) Αληθεύει ότι γενικά μη μηδενικός υποδακτύλιος ημιαπλού δακτυλίου είναι ημιαπλός;
ii) Αποδείξτε ότι κάθε μη μηδενική επιμορφική εικόνα ημιαπλού δακτυλίου είναι ημιαπλός.
Υπόδειξη: Ίσως είναι χρήσιμη η παρατήρηση ότι κάθε αμφίπλευρο ιδεώδες του $R_1 \times \ldots \times R_s$ έχει τη μορφή $I_1 \times \ldots \times I_s$, όπου για κάθε *k*, το I_k είναι αμφίπλευρο ιδεώδες του R_k, σε συνδυασμό με το $1^{\text{ο}}$ θεώρημα ισομορφισμών δακτυλίων.

7. Έστω *k* σώμα και *G* πεπερασμένη ομάδα. Ο δακτύλιος *k*[*G*] είναι ημιαπλός αν και μόνο αν το *k* είναι προβολικό *k*[*G*]-πρότυπο.
Υπόδειξη: Βλ. την απόδειξη του Θεωρήματος του Maschke.

8. Υπάρχει πεπερασμένος ημιαπλός δακτύλιοι τάξης 2006;

9. Έστω $R \cong M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s)$ ημιαπλός δακτύλιος. Τότε υπάρχουν στοιχεία $e_1,\ldots,e_s$ στο R με τις ιδιότητες $e_i^2 = e_i$, $e_i e_j = 0$ για $i \neq j$,$e_1 + \ldots + e_n = 1$, $e_i v = v$ για κάθε ν στο $M_{n_i}(D_i)$, και $e_j \, M_{n_i}(D_i) = 0$.

10. Ένας δακτύλιος λέγεται **δεξιά ημιαπλός** αν είναι ευθύ άθροισμα απλών δεξιών ιδεωδών. Αποδείξετε ότι ένας δακτύλιος είναι δεξιά ημιαπλός αν και μόνο αν είναι (αριστερά) ημιαπλός. Ποιά είναι τα απλά δεξιά ιδεώδη του $M_n(D)$, όπου *D* δακτύλιος διαίρεσης;

11. Αν *M* είναι ένα *R*-πρότυπο, συμβολίζουμε με $soc_R(M)$ (το **βάθρο** του *M*) το υποπρότυπο του *M* που παράγεται από τα απλά υποπρότυπα του *M*. Αν το *M* δεν έχει απλά υποπρότυπα θέτουμε $soc_R(M)=0$. Παρατηρούμε ότι ένα μη μηδενικό *M* είναι ημιαπλό αν και μόνο αν $soc_R(M)=M$.

Ποια είναι τα $soc_{\mathbb{Z}}(\mathbb{Z})$, $soc_{\mathbb{Z}}(\mathbb{Z}_{p^2})$ όπου p πρώτος, $soc_{\mathbb{Z}}(\mathbb{Q})$;

12. Ένα ημιαπλό πρότυπο είναι πεπερασμένα παραγόμενο αν και μόνο αν είναι ευθύ άθροισμα πεπερασμένου πλήθους απλών προτύπων.

13. Αν το *M* είναι πεπερασμένα παραγόμενο ημιαπλό *R*-πρότυπο, τότε ο δακτύλιος $End_R(M)$ είναι ημιαπλός.

Υπόδειξη: Υπολογίστε τον $End_R(M)$. (Βλ.απόδειξη 1)$\Rightarrow$6) του Θεωρήματος του Wedderburn).

14. Έστω R ένας ημιαπλός δακτύλιος.

i) Η γραφή κάθε πεπερασμένα παραγόμενου *R*-προτύπου ως ευθύ άθροισμα απλών προτύπων είναι ουσιαστικά μοναδική.

ii) Η τάξη ελεύθερου *R*-προτύπου είναι καλά ορισμένη.

15. i) Να βρεθούν όλοι οι ημιαπλοί δακτύλιοι το κέντρο των οποίων είναι σώμα.

ii) Αποδείξτε ότι το κέντρο της $\mathbb{C}[S_3]$ έχει διάσταση 3, όπου S_3 είναι η ομάδα μεταθέσεων 3 συμβόλων.

iii) Έστω *G* μια ομάδα τάξης 10 για την οποία η άλγεβρα $\mathbb{C}[G]$ έχει τουλάχιστον 8 ανά δύο μη ισόμορφα απλά πρότυπα. Αποδείξτε ότι $G \simeq \mathbb{Z}_{10}$.

16. Έστω *D* ένας δακτύλιος διαίρεσης και *n* ένας θετικός ακέραιος. Θεωρούμε το δακτύλιο $R=M_n(D)$ και το *R*-πρότυπο $V=\left\{\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \middle| v_i \in D\right\}$ με εξωτερικό πολλαπλασιασμό τον πολλαπλασιασμό πινάκων.

i) Αποδείξτε ότι η απεικόνιση $\Phi : D^{op} \to End_R(V), \Phi(d)(v) = vd$ (προσοχή στη σειρά των *v*,*d*) είναι μονομορφισμός δακτυλίων.

ii) Αποδείξτε ότι η Φ είναι επί.

Υπόδειξη: Ένας οικονομικός τρόπος είναι ο εξής. Έστω $v = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in V$. Επειδή ως *R*-πρότυπο, το *V* είναι απλό, βλ. απόδειξη του Θεωρήματος Wedderburn, έχουμε $V = \langle v \rangle$. Αν $f \in End_R(V)$, τότε η *f* καθορίζεται από την εικόνα $f(v)$ και έχουμε $f(v) = f\left(E_{11}v\right) = E_{11} f(v) = dv = vd = \Phi(dv),$ για κάποιο $d \in D$. (Σημείωση: Η ίδια ιδέα εφαρμόζει και στην άσκηση 9 iii) του Κεφαλαίου 1).