ΚΕΦΑΛΑΙΟ 1: Πρότυπα

Στο κεφάλαιο αυτό θα υπενθυμίσουμε τις βασικές έννοιες που αφορούν πρότυπα πάνω από ένα δακτύλιο. Θα περιοριστούμε στα πλέον απαραίτητα για αυτά που ακολουθούν στα άλλα κεφάλαια. Η κατευθυντήρια γραμμή είναι να μελετήσουμε δακτυλίους μέσω των προτύπων τους. Ως ένα πρώτο απλούστατο παράδειγμα της γραμμής αυτής δίνουμε ένα χαρακτηρισμό δακτυλίων διαίρεσης.

1.1 Βασικές Έννοιες

Ένας **δακτύλιος** είναι ένα σύνολο R εφοδιασμένο με δύο πράξεις, $+: R\times R\to R$ και $\cdot: R\times R\to R$, έτσι ώστε

i) $(R,+)$ είναι αβελιανή ομάδα,

ii) $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ για κάθε $x,y,z\in R$,

iii) υπάρχει στοιχείο $1_R\in R$ με την ιδιότητα $1_R\cdot x = x\cdot 1_R = x$ για κάθε $x\in R$,

iv) $(x+y)\cdot z = x\cdot z + y\cdot z$, $x\cdot(y+z) = x\cdot y + x\cdot z$ για κάθε $x,y,z\in R$.

Στον παραπάνω ορισμό, θα λέμε ότι η πράξη $+: R\times R\to R$ είναι η πρόσθεση του R και $\cdot: R\times R\to R$ είναι ο πολλαπλασιασμός του R.

Στη συνέχεια θα γράφουμε xy στη θέση του $x\cdot y$ και 1 στη θέση του 1_R. Ένας δακτύλιος R καλείται **μεταθετικός** αν $xy = yx$ για κάθε $x,y\in R$. *Στις σημειώσεις αυτές οι δακτύλιοί μας θα είναι γενικά μη μεταθετικοί εκτός αν διατυπώνεται σαφώς το αντίθετο.*

Ένα στοιχείο $r\in R$ ενός δακτυλίου R καλείται **αντιστρέψιμο** αν υπάρχει $s\in R$ με $rs = sr = 1$. Το σύνολο των αντιστρέψιμων στοιχείων του R αποτελεί πολλαπλασιαστική ομάδα. Ένας δακτύλιος ονομάζεται **δακτύλιος διαίρεσης** αν $1\neq 0$ και κάθε $r\in R,\ r\neq 0$, είναι αντιστρέψιμο. **Σώμα** είναι ένας μεταθετικός δακτύλιος διαίρεσης.

Αριστερό ιδεώδες του δακτυλίου R είναι μια υποομάδα της $(R,+)$ που έχει την ιδιότητα $ra\in I$ για κάθε $r\in R$ και κάθε $\alpha\in I$. Αν αντικαταστήσουμε τη συνθήκη $ra\in I$ με $ar\in I$, προκύπτει η έννοια του δεξιού ιδεώδους. **Αμφίπλευρο** ιδεώδες είναι ένα αριστερό ιδεώδες που ταυτόχρονα είναι και δεξιό ιδεώδες. *Στα επόμενα, όταν λέμε ιδεώδες εννοούμε αριστερό ιδεώδες.*

Αν το I είναι αμφίπλευρο ιδεώδες, τότε η αβελιανή ομάδα R/I καθίσταται δακτύλιος με πολλαπλασιασμό που ορίζεται από τη σχέση $(r+I)(s+I) = rs+I$. Ο R/I ονομάζεται δακτύλιος πηλίκο.

Μια απεικόνιση δακτυλίων $f: R\to S$ ονομάζεται **ομομορφισμός** αν $f(r+r') = f(r)+f(r')$, $f(rr') = f(r)f(r')$ για κάθε $r,r'\in R$. Ο **πυρήνας** ενός ομομορφισμού f είναι $Kerf = \{r\in R \mid f(r)=0\}$ και αποτελεί αμφίπλευρο ιδεώδες του R. Ένας ομομορφισμός δακτυλίων λέγεται **μονομορφισμός** (αντίστοιχα, **επιμορφισμός**) αν είναι 1-1 απεικόνιση (αντίστοιχα, επί). Ένας ομομορφισμός δακτυλίων που είναι 1-1 και επί απεικόνιση λέγεται **ισομορφισμός** δακτυλίων.

Έστω $f: R\to S$ ομομορφισμός δακτυλίων. Υπενθυμίζουμε το πρώτο θεώρημα ισομορφισμών δακτυλίων, που λέει ότι η απεικόνιση $\overline{f}: R/\ker f\to \operatorname{Im} f,\ a+\ker f\to f(a)$, είναι ισομορφισμός δακτυλίων.

1.1.1 Ορισμός *Έστω R ένας δακτύλιος. Μια αβελιανή ομάδα $(M,+)$ εφοδιασμένη με μία απεικόνιση $R\times M\to M$, $(r,m)\to r\cdot m$, ονομάζεται **αριστερό R-πρότυπο** αν ισχύουν οι εξής ιδιότητες*

i) $r_1\cdot(r_2\cdot m) = (r_1r_2)\cdot m$ *για κάθε* $r_1,r_2\in R,\ m\in M$

ii) $(r_1+r_2)\cdot m = r_1\cdot m + r_2\cdot m$ *για κάθε* $r_1,r_2\in R,\ m\in M$

iii) $r\cdot(m_1+m_2) = r\cdot m_1 + r\cdot m_2$ *για κάθε* $r\in R,\ m_1,m_2\in M$

iv) $1\cdot m = m$ *για κάθε* $m\in M$.

Στον παραπάνω ορισμό θα ονομάζουμε την απεικόνιση $R \times M \to M$, $(r,m) \to r \cdot m$ τον **εξωτερικό πολλαπλασιασμό** του *R*. Στα παρακάτω θα γράφουμε *rm* στη θέση του $r \cdot m$.

Ανάλογα ορίζεται και η έννοια του δεξιού *R*-προτύπου: ο εξωτερικός πολλαπλασιασμός έχει τη μορφή $M \times R \to M$, $(m,r) \mapsto mr$, και τα αξιώματα i) – iv) γράφονται στη δεξιά μορφή τους, π.χ. $(m \cdot r_2) \cdot r_1 = m \cdot (r_2 r_1)$. *Στα παρακάτω όταν λέμε R-πρότυπο εννοούμε αριστερό R-πρότυπο.*

1.1.2 Παραδείγματα

- Έστω *k* ένα σώμα. Κάθε *k*-διανυσματικός χώρος είναι *k*-πρότυπο. Μάλιστα οι έννοιες *k*-διανυσματικός χώρος και *k*-πρότυπο ταυτίζονται.
- Κάθε αβελιανή ομάδα G είναι $\mathbb{Z}$-πρότυπο με εξωτερικό πολλαπλασιασμό $\mathbb{Z} \times G \to G, (r,m) \mapsto rm,$

$$rm = \begin{cases} m + ... + m \quad (r \quad \text{φορές}), \quad \text{αν} \quad r > 0 \\ 0, \quad \text{αν} \quad r = 0 \\ -(-r)m, \quad \text{αν} \quad r < 0. \end{cases}$$

- Κάθε ιδεώδες ενός δακτυλίου R είναι *R*-πρότυπο με εξωτερικό πολλαπλασιασμό τον πολλαπλασιασμό του *R*.
- Έστω *I* ένα ιδεώδες ενός δακτυλίου *R*. Η αβελιανή ομάδα R/I καθίσταται *R*-πρότυπο αν ορίσουμε $r(a+I) = ra + I$, όπου $r, a \in R$. (Σημείωση: Γενικά το R/I είναι μόνο πρότυπο και όχι δακτύλιος, εκτός αν το *I* είναι αμφίπλευρο ιδεώδες).
- Έστω $f : R \to S$ ένας ομομορφισμός δακτυλίων. Κάθε *S*-πρότυπο *M* γίνεται *R*-πρότυπο αν ορίσουμε $rm = f(r)m,\ r \in R,\ m \in M$.
- Έστω *R* ένας δακτύλιος. Με $M_n(R)$ συμβολίζουμε το δακτύλιο των $n \times n$ πινάκων με στοιχεία από το *R* (ως προς τις συνήθεις πράξεις). Είναι *R*-πρότυπο με εξωτερικό πολλαπλασιασμό $R \times M_n(R) \to M_n(R)$, $(r, A) \mapsto rA$, όπου rA είναι ο πίνακας που προκύπτει από τον A αν πολλαπλασιάσουμε κάθε στοιχείο του με το r.
- Έστω R δακτύλιος και $V = M_{n\times1}(R)$ το σύνολο των $n \times 1$ πινάκων με στοιχεία από το R. Το V είναι $M_n(R)$-πρότυπο με εξωτερικό πολλαπλασιασμό $M_n(R) \times V \to V$ το γινόμενο πινάκων.

Σ'ένα *R*-πρότυπο *M* εύκολα επαληθεύονται οι σχέσεις:

$$O_R m = O_M,\ rO_M = O_M,\ (-r)m = r(-m) = -rm \text{ για κάθε } r \in R \text{ και } m \in M.$$

Έστω *M*, *N* δύο *R*-πρότυπα. Μια απεικόνιση $f : M \to N$ ονομάζεται **ομομορφισμός *R*-προτύπων** αν

i) $f(m+m') = f(m) + f(m')$ για κάθε $m, m' \in M$, και

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

Παραδείγματα

- Αν το k είναι σώμα και U, V είναι *k*-διανυσματικοί χώροι, τότε ταυτίζονται οι έννοιες ομομορφισμός *k*-προτύπων $U \to V$ και *k*-γραμμική απεικόνιση $U \to V$.
- Αν $R = \mathbb{Z}$, τότε ταυτίζονται οι έννοιες ομομορφισμός *R*-προτύπων και ομομορφισμός (αβελιανών) ομάδων.
- Αν R είναι δακτύλιος και $a \in R$, τότε η απεικόνιση $f_a : R \to R, f_a(r) = ra,$ είναι ομομορφισμός R-προτύπων. Αντίθετα, η απεικόνιση $f_a : R \to R, f_a(r) = ar,$ δεν είναι γενικά ομομορφισμός R-προτύπων (γιατί;).

Ένας ομομορφισμός R-προτύπων λέγεται **μονομορφισμός** (αντίστοιχα **επιμορφισμός**) αν είναι 1-1 απεικόνιση (αντίστοιχα επί). **Ισομορφισμός** R-προτύπων είναι ομομορφισμός R-προτύπων που είναι 1-1 κι επί. Για έναν ομομορφισμό R-προτύπων $f: M \to N$ ισχύει: f μονομορφισμός $\Leftrightarrow$ $\ker f = \{0\}$ (άσκηση).

Ένα υποσύνολο N του R-προτύπου M καλείται ***R*-υποπρότυπο** του M (συμβολικά, $N \leq M$) αν είναι υποομάδα της M και $ra \in N$ για κάθε $r \in R$ και $a \in N$.

Για παράδειγμα, αν θεωρήσουμε ένα δακτύλιο R ως R-πρότυπο, τότε τα R- υποπρότυπά του είναι τα ιδεώδη του. Τα k-υποπρότυπα ενός k-διανυσματικού χώρου είναι οι υπόχωροι του. Αν $f: M \to N$ είναι ένας ομομορφισμός R-προτύπων, ο πυρήνας $\ker f$ είναι ένα υποπρότυπο του M, και η εικόνα $\operatorname{Im} f$ είναι ένα υποπρότυπο του N (άσκηση).

Είναι σαφές ότι κάθε υποπρότυπο N του R-προτύπου M είναι R-πρότυπο ως προς τον εξωτερικό πολλαπλασιασμό $R \times N \to N$.

Έστω M ένα R-πρότυπο και $a \in M$. Το σύνολο $(a) = \{ra \in M \mid r \in R\}$ είναι ένα υποπρότυπο του M και το καλούμε το υποπρότυπο του M που παράγεται από το a. Ένα υποπρότυπο N του M ονομάζεται **κυκλικό** αν $N = (a)$ για κάποιο $a \in N$. Για παράδειγμα, κάθε δακτύλιος R είναι κυκλικό R-πρότυπο αφού $R = (1)$. Τα κυκλικά υποπρότυπα του R είναι ακριβώς τα κύρια ιδεώδη του R.

Αν το N είναι υποπρότυπο του M, τότε στην αβελιανή ομάδα M/N ορίζεται η δομή R-προτύπου με εξωτερικό πολλαπλασιασμό που ορίζεται από

$$r(m+N) = rm + N,$$

όπου $r \in R, m \in M$. Πράγματι, ας δούμε ότι ο παραπάνω εξωτερικός πολλαπλασιασμός είναι καλά ορισμένος. Έστω $m_1 + N = m_2 + N$. Τότε $m_1 - m_2 \in N$ και επειδή $N \leq M$ παίρνουμε $r(m_1 - m_2) \in N$, οπότε $rm_1 + N = rm_2 + N$. Οι ιδιότητες στον ορισμό του προτύπου επαληθεύονται εύκολα. Το M/N ονομάζεται **πρότυπο πηλίκο** και η απεικόνιση

$$f: M \ni m \mapsto m + N \in M/N$$

είναι επιμορφισμός R-προτύπων που συνήθως ονομάζεται **φυσική προβολή** ή **φυσικός επιμορφισμός**.

Αν A,B είναι υποπρότυπα του R-προτύπου M, ορίζουμε $A + B = \{a + b \mid a \in A,\, b \in B\}$. Εύκολα επαληθεύουμε ότι το $A + B$ είναι ένα R-υποπρότυπο του M. Παρατηρούμε ότι αυτή η κατασκευή γενικεύει το άθροισμα ιδεωδών δακτυλίου, το άθροισμα υποχώρων διανυσματικού χώρου και το γινόμενο δυο υποομάδων αβελιανής ομάδας. Κατ'αναλογία με τους δακτυλίους έχουμε:

1.1.3 Πρόταση. *(1ο Θεώρημα Ισομορφισμών Προτύπων). Έστω $f: M \to N$ ένας ομομορφισμός R-προτύπων. Τότε η απεικόνιση $\bar{f}: M/\ker f \ni m + \ker f \mapsto f(m) \in \operatorname{Im} f$ είναι ισομορφισμός R-προτύπων.*
(2ο Θεώρημα Ισομορφισμών Προτύπων). Έστω A,B υποπρότυπα του R-προτύπου M. Τότε υπάρχει ισομορφισμός R-προτύπων

$$(A+B)/A \cong B/A \cap B.$$

(3ο Θεώρημα Ισομορφισμών Προτύπων). Έστω R-πρότυπα $C \leq B \leq A$. Τότε υπάρχει ισομορφισμός R-προτύπων

$$(A/C)/(B/C) \cong A/B.$$

Απόδειξη. i) Εύκολα επαληθεύουμε ότι η απεικόνιση $\bar{f}$ είναι καλά ορισμένος επιμορφισμός R-προτύπων. Ισχύει $\ker \bar{f} = \{m + \ker f \mid f(m) = 0\} = \{m + \ker f \mid m \in \ker f\} = \{\ker f\}$. Άρα ο $\bar{f}$ είναι ισομορφισμός.
ii) Η απεικόνιση

$$f: B \to (A+B)/A, \quad f(b) = b + A$$

είναι επιμορφισμός R-προτύπων. Ισχύει $\ker \varphi = \{b \in B \mid b + A = A\} = A \cap B$. Άρα από το 1ο θεώρημα ισομορφισμών προκύπτει $B / A \cap B \cong (A+B)/A$.

iii) Εφόσον $C \leq B$ η απεικόνιση

$$f : A/C \to A/B, \quad f(a+C) = a+B$$

είναι καλά ορισμένος επιμορφισμός R-προτύπων. Ισχύει $\ker f = \{a+C \mid a+B = B\} = B/C$. Άρα από το 1ο θεώρημα ισομορφισμών έχουμε $(A/C)/(B/C) \cong A/B$.

1.1.4 Ορισμός. *Έστω A ένα R-πρότυπο, όπου το R είναι μεταθετικός δακτύλιος. Αν το A είναι δακτύλιος με την ιδιότητα*

$$r(aa') = (ra)a' = a(ra') \quad \textit{για κάθε} \quad a, a' \in A, \ r \in R$$

*τότε λέμε ότι το A είναι μια **R-άλγεβρα**.*

Παρατήρηση. Αν η A είναι R-άλγεβρα, τότε $(r1_A)a = a(r1_A)$ για κάθε $r \in R$ και κάθε $a \in A$.

Για παράδειγμα, κάθε δακτύλιος είναι $\mathbb{Z}$-άλγεβρα. Το $\mathbb{C}$ είναι $\mathbb{R}$-άλγεβρα. Οι $n \times n$ πίνακες $M_n(k)$ με στοιχεία από ένα σώμα k αποτελούν k-άλγεβρα. Ο δακτύλιος των πολυωνύμων $k[x]$ με συντελεστές από σώμα k είναι ομοίως k-άλγεβρα, όπως και κάθε πηλίκο του $k[x_1,..,x_n]$ με ιδεώδες. Ακολουθούν δύο παραδείγματα που είναι σημαντικά για τα επόμενα κεφάλαια.

1.1.5 Παράδειγμα. i) (Δακτύλιος ομάδας). Έστω G μια ομάδα και k σώμα. Με $k[G]$ συμβολίζουμε τον k-διανυσματικό χώρο με βάση τα στοιχεία της G όπου η πρόσθεση και ο εξωτερικός πολλαπλασιασμός ορίζονται ως εξής: το τυπικό στοιχείο του $k[G]$ συμβολίζεται $\sum_{g \in G} r_g g$, όπου όλα σχεδόν τα $r_g \in k$ είναι μηδέν - δηλαδή όλα τα r_g είναι μηδέν εκτός ενδεχομένως από ένα *πεπερασμένο* πλήθος. Θέτουμε

$$\begin{aligned} \sum_{g \in G} r_g g + \sum_{g \in G} r'_g g &= \sum_{g \in G} (r_g + r'_g) g \\ r(\sum_{g \in G} r_g g) &= \sum_{g \in G} (r r_g) g. \end{aligned}$$

Ο διανυσματικός χώρος $k[G]$ καθίσταται δακτύλιος ως προς την πρόσθεση που είδαμε πριν και τον πολλαπλασιασμό που ορίζεται από

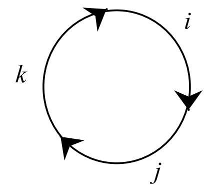
$$(\sum_{g \in G} r_g g)(\sum_{h \in G} s_h h) = \sum_{u \in G} t_u u,$$

όπου $t_u = \sum_{\substack{g,h \in G \\ u = gh}} r_g s_h$. Η μονάδα του δακτυλίου είναι το ουδέτερο στοιχείο $1 \in G$ της ομάδας G. Με τις πιο πάνω πράξεις, το $k[G]$ γίνεται μια k-άλγεβρα.

Παρατηρούμε ότι κάθε στοιχείο της G είναι αντιστρέψιμο στο δακτύλιο $k[G]$. Αν η $G = \{g_1, ..., g_n\}$ είναι πεπερασμένη ομάδα τάξης $n > 1$, τότε ο δακτύλιος $k[G]$ περιέχει διαιρέτες του μηδενός, αφού για παράδειγμα έχουμε $(1-g)(1+g+...+g^{n-1}) = 1 - g^n = 0$.

ii) (**Quaternions** επί του $\mathbb{R}$). Έστω $\mathbb{H}$ ένας $\mathbb{R}$-διανυσματικός χώρος διάστασης 4 και $\{1, i, j, k\}$ μια βάση του $\mathbb{H}$. Ορίζουμε έναν πολλαπλασιασμό στοιχείων του $\mathbb{H}$ ως εξής: απαιτούμε το 1 να είναι μοναδιαίο στοιχείο και θέτουμε

$$i^2 = j^2 = k^2 = -1$$
$$ij = -ji = k$$
$$jk = -kj = i$$
$$ki = -ik = j$$



Πολλαπλασιάζουμε τυχαία στοιχεία $a + bi + cj + dk$ και $a' + b'i + c'j + d'k$, χρησιμοποιώντας επιμερισμό και τον προηγούμενο πίνακα. Για παράδειγμα, $(1+2i)(1-3j) = 1 + 2i - 3j - 6k$. Λαμβάνουμε έτσι μία $\mathbb{R}$-άλγεβρα. Παρατηρούμε ότι ο δακτύλιος $\mathbb{H}$ είναι δακτύλιος διαίρεσης. Πράγματι, αν $q = a + bi + cj + dk$, θέτουμε $\overline{q} = a - bi - cj - dk$ (ο '**συζυγής**' του *q*). Εύκολα επαληθεύεται ότι $q\overline{q} = \overline{q}q = a^2 + b^2 + c^2 + d^2$. Θέτουμε $|q| = \sqrt{q\overline{q}}$. Παρατηρούμε ότι αν $q \neq 0$, τότε $q\frac{\overline{q}}{|q|^2} = \frac{\overline{q}}{|q|^2}q = 1$, δηλαδή το *q* είναι αντιστρέψιμο.

1.1.6 Σημείωση. Θα δούμε στο Κεφάλαιο 6 ότι οι $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ είναι οι μόνες πεπερασμένης διάστασης $\mathbb{R}$-άλγεβρες με διαίρεση.

Αν *M*, *N* είναι δύο *R*-πρότυπα το σύνολο

$$Hom_R(M,N) = \{f : M \to N \mid f \text{ ομομορφισμός } R\text{-προτύπων}\}$$

είναι αβελιανή ομάδα με πρόσθεση που ορίζεται από $(f + f')(m) = f(m) + f'(m)$. Δεν είναι γενικά *R*-πρότυπο. Αν $M = N$, το σύνολο $Hom_R(M,M)$ συνήθως συμβολίζεται με $End_R(M)$ (το σύνολο των *R*-ενδομορφισμών του *M*) και αποτελεί δακτύλιο με πολλαπλασιασμό τη σύνθεση συναρτήσεων.

Ένα μη μηδενικό *R*-πρότυπο *M* λέγεται **απλό** αν δεν υπάρχει υποπρότυπο *N* με την ιδιότητα $O \underset{\neq}{\subseteq} N \underset{\neq}{\subseteq} M$.

Παραδείγματα

- Ένας k-διανυσματικός χώρος είναι απλό k-πρότυπο αν και μόνο αν έχει διάσταση 1.
- Για κάθε πρώτο αριθμό p, το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_p$ είναι απλό, αφού κάθε υποομάδα του $\mathbb{Z}_p$ είναι η τετριμμένη υποομάδα ή η $\mathbb{Z}_p$. Το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_4$ δεν είναι απλό αφού ένα υποπρότυπό του είναι το $\{[0],[2]\}$.
- Το $\mathbb{Z}$-πρότυπο $\mathbb{Q}$ δεν περιέχει απλό υποπρότυπο, γιατί αν $N \leq \mathbb{Q}$ με *N* απλό, τότε για κάποια $m, n \in \mathbb{Z} - \{0\}$ θα είχαμε $\frac{m}{n} \in N$ και άρα $m \in N$. Τότε $m\mathbb{Z} \subseteq N$ και λόγω της απλότητας θα είχαμε $m\mathbb{Z} = N$. Όμως είναι σαφές ότι το $m\mathbb{Z}$ δεν είναι απλό, καθώς αν $m \neq 0$, τότε $0 \underset{\neq}{\subset} 2m\mathbb{Z} \underset{\neq}{\subset} m\mathbb{Z}$.
- Έστω D δακτύλιος διαίρεσης και $V = M_{n\times 1}(D)$. Ξέρουμε ότι το V είναι $M_n(D)$-πρότυπο με εξωτερικό πολλαπλασιασμό το γινόμενο πινάκων. Θα δείξουμε ότι το V είναι απλό $M_n(D)$-πρότυπο. Έστω $E_{ij} \in M_n(D)$ ο πίνακας με 0 παντού εκτός από τη θέση (i,j) όπου υπάρχει το στοιχείο 1. Έστω $E_i \in M_{n\times 1}(D)$ ο πίνακας στήλη με 0 παντού εκτός από τη θέση i όπου υπάρχει το στοιχείο 1. Έστω $U \leq V$ και

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_j \\ \vdots \\ v_n \end{pmatrix} \in U \text{ με } v \neq 0.$$

Τότε $v_j \neq 0$ για κάποιο j. Από τον πολλαπλασιασμό πινάκων έπεται ότι για κάθε i ισχύει $E_{ij}v = v_j E_i$. Άρα $E_i = (v_j^{-1}E_{ij})v \in U$. Συνεπώς $d_1E_1 + ... + d_nE_n \in U$ για κάθε $d_1,...,d_n \in D$. Άρα $V \subseteq U$ και $V = U$.

Δακτύλιοι διαίρεσης εμφανίζονται συχνά ως ενδομορφισμοί απλών προτύπων όπως δείχνει το επόμενο αποτέλεσμα

1.1.7 Λήμμα. *(Λήμμα του Schur). Έστω M ένα απλό R-πρότυπο. Τότε ο $End_R(M)$ είναι δακτύλιος διαίρεσης.*

Απόδειξη. Έστω $f \in End_R(M)$, $f \neq 0$. (Υπάρχει τέτοιο *f* αφού $M \neq 0$, π.χ. $f = 1_M$). Επειδή $\ker f \neq M$, ισχύει $\ker f = 0$. Επειδή $\operatorname{Im} f \neq 0$, ισχύει $\operatorname{Im} f = M$. Άρα ο f είναι ισομορφισμός οπότε είναι αντιστρέψιμο στοιχείο του δακτυλίου $End_R(M)$.

Το ακόλουθο αποτέλεσμα υποδεικνύει τη σημασία των δακτυλίων $M_n(k)$.

1.1.8 Πρόταση. *Έστω k ένα σώμα και A μια k-άλγεβρα με $\dim_k A = n < \infty$. Τότε ο δακτύλιος A είναι ισόμορφος με υποδακτύλιο του $M_n(k)$.*

Απόδειξη. Έστω $a \in A$ και $f_a : A \to A, x \mapsto ax$. Τότε $f_a \in End_k(A)$ και η απεικόνιση $A \to End_k(A), a \mapsto f_a$, είναι μονομορφισμός δακτυλίων. Συνεπώς ο *A* είναι ισόμορφος με υποδακτύλιο του $End_k(A)$. Επιλέγοντας μια βάση του διανυσματικού χώρου *A*, λαμβάνουμε έναν ισομορφισμό δακτυλίων $End_k(A) \simeq M_n(k)$.

Μια απεικόνιση *R*-αλγεβρών είναι **ομομορφισμός** *R*-αλγεβρών αν είναι ταυτόχρονα ομομορφισμός δακτυλίων και *R*-προτύπων. Ανάλογα ορίζεται η έννοια του ισομορφισμού R-αλγεβρών.

Μια *R*-**υποάλγεβρα** μιας *R*-άλγεβρας A είναι ένας υποδακτύλιος του A που είναι και R-υποπρότυπο του A. Για παράδειγμα, η $\mathbb{R}$ υποάλγεβρα της $\mathbb{H}$ που αποτελείται από τα $q = a + bi + cj + dk$ για τα οποία $b = c = d = 0$ είναι ισόμορφη με το $\mathbb{R}$. Ομοίως η $\mathbb{R}$-υποάλγεβρα της $\mathbb{H}$ που αποτελείται από τα $q = a + bi + cj + dk$ για τα οποία $c = d = 0$ είναι ισόμορφη με το $\mathbb{C}$.

Το **κέντρο** μιας *R*-άλγεβρας *A* είναι η *R*-υποάλγεβρα

$$C(A) = \{x \in A \mid ax = xa \quad \text{για κάθε} \quad a \in A\}.$$

Για παράδειγμα, το κέντρο της $M_2(k)$, όπου το *k* είναι σώμα, είναι $C(M_2(k)) = \left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in M_2(k)\right)$.

Πράγματι, είναι σαφές ότι $\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in M_2(k)\right) \subseteq C(M_2(k))$. Έστω $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C(M_2(k))$. Τότε έχουμε

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow c = b = 0.$ Επίσης $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow a = d.$

1.2 Άθροισμα και Γινόμενο Προτύπων, Ακριβείς Ακολουθίες

Αν $(M_\lambda)_{\lambda\in\Lambda}$ είναι μια οικογένεια *R*-προτύπων, τότε το σύνολο των ακολουθιών $(x_\lambda)_{\lambda\in\Lambda}$, με $x_\lambda \in M_\lambda$, είναι ένα *R*-πρότυπο με πρόσθεση και εξωτερικό πολλαπλασιασμό που ορίζονται από τις σχέσεις $(x_\lambda)_{\lambda\in\Lambda}+(y_\lambda)_{\lambda\in\Lambda}=(x_\lambda+y_\lambda)_{\lambda\in\Lambda}$, $r(x_\lambda)_{\lambda\in\Lambda}=(rx_\lambda)_{\lambda\in\Lambda}$. Το συμβολίζουμε με $\prod\limits_{\lambda\in\Lambda} M_\lambda$ και το ονομάζουμε το **ευθύ γινόμενο** των M_λ, $\lambda\in\Lambda$. Στην περίπτωση που το *Λ* είναι πεπερασμένο, $\Lambda=\{1,2,...,n\}$, θα γράφουμε και $M_1\times...\times M_n$ στη θέση του $\prod\limits_{\lambda\in\Lambda} M_\lambda$. Αν επιπλέον $M_1=...=M_n=M$, θα γράφουμε και M^n.

Ορίζουμε τώρα ένα υποπρότυπο του $\prod\limits_{\lambda\in\Lambda} M_\lambda$. Έστω $\bigoplus\limits_{\lambda\in\Lambda} M_\lambda$ το υποσύνολο του $\prod\limits_{\lambda\in\Lambda} M_\lambda$ που αποτελείται από εκείνες τις ακολουθίες $(x_\lambda)_{\lambda\in\Lambda}$ όπου $x_\lambda=0$ εκτός το πολύ ένα πεπερασμένο πλήθος $\lambda\in\Lambda$. Ονομάζεται **ευθύ άθροισμα** των M_λ. Στην περίπτωση που το *Λ* είναι πεπερασμένο ισχύει βέβαια $\bigoplus\limits_{\lambda\in\Lambda} M_\lambda$ $=\prod\limits_{\lambda\in\Lambda} M_\lambda$.

Έστω $(N_\lambda)_{\lambda\in\Lambda}$ μια οικογένεια *R*-υποπροτύπων του *R*-προτύπου *M*. Θα λέμε ότι το *M* είναι το **εσωτερικό ευθύ άθροισμα** των N_λ, $\lambda\in\Lambda$, αν κάθε $x\in M$ γράφεται μοναδικά ως άθροισμα της μορφής $x=y_{\lambda_1}+...+y_{\lambda_t}$, με $y_{\lambda_i}\in N_{\lambda_i}$, $t\geq 1$. Στην περίπτωση αυτή θα γράφουμε $N=\bigoplus\limits_{\lambda\in\Lambda} N_\lambda$.

Σημείωση. Η χρήση του ίδιου συμβολισμού $\bigoplus\limits_{\lambda\in\Lambda} N_\lambda$ για δύο διαφορετικά πράγματα δεν πρέπει να δημιουργεί σύγχυση γιατί το εσωτερικό ευθύ άθροισμα των N_λ (όταν ορίζεται) είναι ισόμορφο με το ευθύ γινόμενο των N_λ (που πάντα ορίζεται).

Αν $X\subseteq M$ είναι ένα υποσύνολο του *R*-προτύπου *M*, με $<X>$ ή (X) συμβολίζουμε το υποπρότυπο του *M*, $(X)=\{r_1x_1+...+r_tx_t\in M \mid t\geq 1,\ r_i\in R,\ x_t\in M\}$. Ονομάζεται δε το υποπρότυπο του *M* που **παράγει** το *X*. Ταυτίζεται με την τομή όλων των υποπροτύπων του *M* που περιέχουν το *X* (γιατί;). Αν $(N_\lambda)_{\lambda\in\Lambda}$ είναι μια οικογένεια υποπροτύπων του *M*, το υποπρότυπο $(\bigcup\limits_{\lambda\in\Lambda} N_\lambda)$ που παράγουν τα N_λ, $\lambda\in\Lambda$, συμβολίζεται με $\sum\limits_{\lambda\in\Lambda} N_\lambda$. Ισχύει $\sum\limits_{\lambda\in\Lambda} N_\lambda=\{x_{\lambda_1}+...+x_{\lambda_t} \mid t\geq 1,\ x_{\lambda_i}\in N_{\lambda_i}\}$. Για παράδειγμα, έχουμε $m\mathbb{Z}+n\mathbb{Z}=d\mathbb{Z}$, όπου $d=\mu\kappa\delta(m,n)$ (άσκηση).

1.2.1 Πρόταση. *Έστω $(N_\lambda)_{\lambda\in\Lambda}$ μια οικογένεια R-υποπροτύπων του R-προτύπου M. Τότε ισχύει $M=\bigoplus\limits_{\lambda\in\Lambda} N_\lambda$ αν και μόνο αν*

i) $M=\sum\limits_{\lambda\in\Lambda} N_\lambda$, και

ii) για κάθε $\lambda\in\Lambda$ ισχύει $N_\lambda\cap\sum\limits_{\mu\neq\lambda} N_\mu=0$.

Απόδειξη. Έστω $x\in M$ και $x=y_{\lambda_1}+...+y_{\lambda_t}=y'_{\lambda_1}+...+y'_{\lambda_t}$, όπου $y_{\lambda_i}, y'_{\lambda_i}\in N_{\lambda_i}$. Τότε $N_{\lambda_1}\ni y_{\lambda_1}-y'_{\lambda_1}=(y'_{\lambda_t}-y_{\lambda_t})+...+(y'_{\lambda_t}-y_t)\in\sum\limits_{\mu\neq\lambda_1} N_\mu$. Αν ισχύει η συνθήκη (ii), παίρνουμε $y_{\lambda_1}=y'_{\lambda_1}$. Συνεπώς αν ισχύουν οι συνθήκες (i) και (ii) λαμβάνουμε $M=\bigoplus\limits_{\lambda\in\Lambda} N_\lambda$. Το αντίστροφο είναι επίσης άμεσο: αν $N_\lambda\cap\sum\limits_{\mu\neq\lambda} N_\mu\neq 0$, τότε θα είχαμε $y_\lambda=y_{\lambda_1}+...+y_{\lambda_t}$ με $y_{\lambda_i}\in N_{\lambda_i}$ και $\lambda\neq\lambda_i$, δηλαδή θα είχαμε δύο εκφράσεις για το y_λ, άτοπο.

1.2.2 Πρόταση. *Έστω M,N R-πρότυπα και* $(M_\lambda)_{\lambda\in\Lambda}$, $(N_\lambda)_{\lambda\in\Lambda}$ *οικογένειες R-προτύπων. Τότε υπάρχουν ισομορφισμοί αβελιανών ομάδων*

i) $Hom_R\left(\underset{\lambda\in\Lambda}{\oplus} M_\lambda, N\right) \simeq \prod_{\lambda\in\Lambda} Hom_R(M_\lambda, N)$

ii) $Hom_R\left(M, \prod_{\lambda\in\Lambda} N_\lambda\right) \simeq \prod_{\lambda\in\Lambda} Hom_R(M, N_\lambda)$.

Απόδειξη. (i) Έστω $(g_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} Hom_R(M_\lambda, N)$, όπου $g_\lambda \in Hom_R(M_\lambda, N)$. Έστω $g : \underset{\lambda\in\Lambda}{\oplus} M_\lambda \to N$ η απεικόνιση που ορίζεται από $g(x_\lambda)_{\lambda\in\Lambda} = \sum_{\lambda\in\Lambda} g_\lambda(x_\lambda)$. Ο ορισμός έχει νόημα γιατί $x_\lambda = 0$ για όλα τα $\lambda\in\Lambda$ εκτός από ένα πεπερασμένο πλήθος. Η *g* είναι βέβαια ομομορφισμός *R*-προτύπων, $g \in Hom_R\left(\underset{\lambda\in\Lambda}{\oplus} M_\lambda, N\right)$.

Έστω $\Psi : \prod_{\lambda\in\Lambda} Hom_R(M_\lambda, N) \to Hom_R\left(\underset{\lambda\in\Lambda}{\oplus} M_\lambda, N\right)$, $(g_\lambda)_{\lambda\in\Lambda} \mapsto g$. Είναι ομομορφισμός αβελιανών ομάδων. Στην αντίθετη κατεύθυνση ορίζουμε $\Phi : Hom_R(\oplus M_\lambda, N) \to \prod_{\lambda\in\Lambda} Hom_R(M_\lambda, N)$, $f \mapsto (f_\lambda)_{\lambda\in\Lambda}$, όπου για κάθε $\lambda\in\Lambda$ $f_\lambda(x_\lambda) = f(\ldots,0,x,0,\ldots)$ και το $x\in M_\lambda$ βρίσκεται στην *λ* συνιστώσα του $(\ldots,0,x,0,\ldots) \in \underset{\lambda\in\Lambda}{\oplus} M_\lambda$. Η *Φ* είναι ομομορφισμός αβελιανών ομάδων και ισχύει $\Phi\circ\Psi$ και $\Psi\circ\Phi$ είναι οι αντίστοιχες ταυτοτικές απεικονίσεις. Συνεπώς *Φ* είναι ισομορφισμός.

ii) Παρόμοια με την (i).

Σημείωση. Δεν ισχύει γενικά ότι $Hom_R\left(\prod_{\lambda\in\Lambda} M_\lambda, N\right) \simeq \prod_{\lambda\in\Lambda} Hom(M_\lambda, N)$ (Άσκηση 12).

1.2.3 Πρόταση. *Έστω M ένα R-πρότυπο. Υπάρχει ισομορφισμός R-προτύπων*

$$Hom_R(R, M) \cong M.$$

Απόδειξη. Πρώτα παρατηρούμε ότι η αβελιανή ομάδα $Hom_R(R,M)$ είναι (αριστερό) *R*-πρότυπο, $(rf)(r') = f(r'r)$. Εύκολα επαληθεύεται ότι η απεικόνιση $\Phi : Hom_R(R,M) \ni f \mapsto f(1) \in M$ είναι ομομορφισμός *R*-προτύπων. Επίσης η απεικόνιση $\Psi : M \mapsto Hom_R(R,M)$, $\Psi(m)(r) = rm$ είναι ομομορφισμός *R*-προτύπων. Ισχύει $\Psi\circ\Phi = 1_{Hom_R(R,M)}$, $\Phi\circ\Psi = 1_M$, και άρα ο *Φ* είναι ισομορφισμός.

Για παράδειγμα, αν G είναι αβελιανή ομάδα, τότε υπάρχει ισομορφισμός ομάδων $Hom_{\mathbb{Z}}(\mathbb{Z}, G) \cong G$.

Έστω $f : L \to M$, $g : M \to N$ ομομορφισμοί *R*-προτύπων. Η ακολουθία

$$L \xrightarrow{f} M \xrightarrow{g} N$$

λέγεται **ακριβής** στο *M* αν ισχύει $\ker g = \operatorname{Im} f$. (Παρατηρούμε ότι στην περίπτωση αυτή έχουμε $g\circ f = 0$, γιατί η τελευταία σχέση είναι ισοδύναμη με τη $\operatorname{Im} f \subseteq \ker g$. Όμως η ακρίβεια στο M μας λέει κάτι ισχυρότερο.

Πιο γενικά, μια ακολουθία *R*-προτύπων και *R*-ομομορφισμών

$$\ldots \to M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \ldots$$

λέγεται **ακριβής** αν είναι ακριβής σε κάθε M_i.

Μια ακριβής ακολουθία της μορφής

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

λέγεται **βραχεία**. Ένα παράδειγμα είναι $0 \longrightarrow \mathbb{Z} \xrightarrow{\alpha} \mathbb{Z} \xrightarrow{\beta} \mathbb{Z}_m \longrightarrow 0$, όπου η απεικόνιση α είναι ο πολλαπλασιασμός με το m και β η φυσική προβολή. Παρατηρούμε ότι ο f είναι μονομορφισμός, γιατί $\ker f = \mathrm{Im}(0 \to L) = 0$. Επίσης ο g είναι επιμορφισμός, γιατί $\mathrm{Im}\, g = \ker(N \to 0) = N$. Ισχύει (λόγω του 1ου θεωρήματος ισομορφισμών) $N = \mathrm{Im}\, g \simeq M / \ker g \simeq M / L$, δηλαδή $N \cong M / L$. Αντίστροφα, αν L είναι υποπρότυπο του M, παίρνουμε μια ακριβή ακολουθία $0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} M / L \longrightarrow 0$, όπου $\alpha(x) = x$, $\beta(y) = y + L$ για $x \in L$, $y \in M$. (Ο β είναι ο φυσικός επιμορφισμός). Συνεπώς βλέπουμε ότι μια βραχεία ακριβής ακολουθία αποτελεί έναν τρόπο καταγραφής του 1ου θεωρήματος ισομορφισμών.

Αν $L \xrightarrow{f} M$ είναι μονομορφισμός, παίρνουμε την ακριβή ακολουθία $0 \longrightarrow L \xrightarrow{f} M \xrightarrow{\beta} M / \mathrm{Im}\, f \longrightarrow 0$, όπου β είναι ο φυσικός επιμορφισμός. Αν $M \xrightarrow{g} N$ είναι επιμορφισμός, παίρνουμε την ακριβή ακολουθία $0 \longrightarrow \ker g \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$, όπου $\alpha(x) = x$ είναι η φυσική εμφύτευση.

1.2.4 Πρόταση. *Έστω $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ βραχεία ακριβής ακολουθία R-προτύπων. Οι παραπάνω συνθήκες είναι ισοδύναμες*

(i) υπάρχει R-ομομορφισμός $\alpha' : B \to A$ με την ιδιότητα $\alpha' \circ \alpha = 1_A$

(ii) υπάρχει R-ομομορφισμός $\beta' : C \to B$ με την ιδιότητα $\beta \circ \beta' = 1_C$

(iii) η εικόνα $\mathrm{Im}\, a$ είναι ευθύς προσθετέος του B.

Απόδειξη. $\text{(i)} \Rightarrow \text{(iii)}$. Σύμφωνα με την Πρόταση 1.2.1. αρκεί να δείξουμε ότι $B = \mathrm{Im}\,\alpha + \ker\alpha'$ και $\mathrm{Im}\,\alpha \cap \ker\alpha' = 0$. Έστω $b \in B$. Γράφουμε

$$b = \alpha \circ \alpha'(b) + (b - \alpha \circ \alpha'(b)).$$

Ισχύει βέβαια $\alpha \circ \alpha'(b) \in \mathrm{Im}\,\alpha$. Επειδή $\alpha'(b - \alpha \circ \alpha'(b)) = \alpha'(b) - \alpha' \circ \alpha \circ \alpha'(b) = \alpha'(b) - \alpha'(b) = 0$, ισχύει $b - \alpha \circ a'(b) \in \ker\alpha'$. Άρα $B = \mathrm{Im}\,\alpha + \ker\alpha'$. Έστω τώρα $x \in \mathrm{Im}\,\alpha \cap \ker\alpha'$. Τότε $\alpha'(x) = 0$ και $x = \alpha(y)$ για κάποιο $y \in A$. Συνεπώς έχουμε $\alpha'(\alpha(y)) = 0$, δηλαδή $y = 0$ οπότε $x = 0$. Άρα $\mathrm{Im}\,\alpha \cap \ker\alpha' = 0$.

$\text{(iii)} \Rightarrow \text{(i)}$ Έστω $B = \mathrm{Im}\,\alpha \oplus N$ για κάποιο υποπρότυπο N του B. Αν $b \in B$, τότε $b = \alpha(x) + y$ για κάποιο $x \in A$, $y \in N$. Επιπλέον τα x, y είναι μοναδικά ορισμένα γιατί ο α είναι μονομορφισμός και $\mathrm{Im}\,\alpha \cap N = 0$. Θέτουμε $\alpha' : B \to A$, $\alpha'(b) = x$, που είναι καλά ορισμένος R-ομομορφισμός. Ισχύει βέβαια $\alpha' \circ \alpha = 1_A$.

$\text{(ii)} \Rightarrow \text{(iii)}$ Θα δείξουμε ότι $B = \ker\beta \oplus \mathrm{Im}\,\beta'$ απ'όπου προκύπτει το ζητούμενο γιατί $\ker\beta = \mathrm{Im}\,\alpha$. Έστω $b \in B$. Γράφουμε

$$b = (b - \beta' \circ \beta(b)) + \beta' \circ \beta(b)$$

και παρατηρούμε ότι $b - \beta' \circ \beta(b) \in \ker\beta$ (αφού $\beta(b - \beta' \circ \beta(b)) = \beta(b) - \beta \circ \beta' \circ \beta(b) = \beta(b) - \beta(b) = 0$) και $\beta' \circ \beta(b) \in \mathrm{Im}\,\beta'$. Αν $x \in \ker\beta \cap \mathrm{Im}\,\beta'$, τότε $\beta(x) = 0$ και επειδή $x = \beta'(y)$ για κάποιο C, έχουμε $\beta \circ \beta'(y) = 0$, δηλαδή $y = 0$.

$\text{(iii)} \Rightarrow \text{(ii)}$ Έστω $B = \mathrm{Im}\,\alpha \oplus N$ για κάποιο υποπρότυπο N του B. Τότε $B = \ker\beta \oplus N$. Ο περιορισμός του β στο N είναι ισομορφισμός, $\beta|_N : N \to C$. Πράγματι, αφού $B = \ker\beta + N$, ο $\beta|_N$ είναι επί. Αν $\beta(y) = 0$ για κάποιο $y \in N$, τότε $y \in \ker\beta$ και άρα $y = 0$, αφού $\ker\beta \cap N = 0$. Θέτοντας $\beta' = \beta|_N$ προκύπτει το ζητούμενο.

Μια βραχεία ακολουθία που ικανοποιεί μια συνθήκη της προηγούμενης πρότασης καλείται

διασπώμενη, και θα λέμε ότι η βραχεία ακολουθία **διασπάται**.

Στην περίπτωση που η ακριβής ακολουθία $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ διασπάται, ισχύει $B \simeq A \oplus C$. Πράγματι, από την απόδειξη της Πρότασης 1.2.4 έχουμε $B = \ker \beta \oplus \operatorname{Im} \beta'$. Ισχύει $A \simeq \operatorname{Im} \alpha$ και $C \simeq \operatorname{Im} \beta'$ γιατί οι α και β' είναι μονομορφισμοί.

1.2.5 Παραδείγματα

- Η ακριβής ακολουθία $\mathbb{Z}$-προτύπων
$$0 \longrightarrow \mathbb{Z} \xrightarrow{m} \mathbb{Z} \longrightarrow \mathbb{Z}_m \longrightarrow 0,$$
όπου η απεικόνιση $\mathbb{Z} \xrightarrow{m} \mathbb{Z}$ είναι πολλαπλασιασμός με το $m \in \mathbb{Z} - \{0\}$, δεν διασπάται όταν $m \neq \pm 1$ (γιατί;).
- Έστω k ένα σώμα. Τότε κάθε ακριβής ακολουθία k-διανυσματικών χώρων πεπερασμένης διάστασης $0 \longrightarrow V_1 \longrightarrow V_2 \longrightarrow V_3 \longrightarrow 0$ διασπάται, γιατί κάθε σύνολο γραμμικώς ανεξαρτήτων του διανυσμάτων V_2 μπορεί να επεκταθεί σε βάση του V_2.
- Έστω k ένα σώμα. Η ακριβής ακολουθία $0 \longrightarrow (x) \longrightarrow k[x] \longrightarrow k \longrightarrow 0$ διασπάται, αν θεωρηθεί ως ακολουθία k-προτύπων: ορίζουμε $\alpha' \ : \ k[x] \to (x)$, $f_0 + f_1 x + \ldots + f_r x^n \mapsto f_1 x + \ldots + f_r x^n$. Τότε ο α' είναι ομομορφισμός k-προτύπων και ο περιορισμός του στο $\langle x \rangle$ είναι η ταυτοτική απεικόνιση. Όμως η παραπάνω ακριβής ακολουθία **δεν** διασπάται αν θεωρηθεί ως ακολουθία $k[x]$-προτύπων. Πράγματι, έστω $\alpha' \ : \ k[x] \to (x)$ ένας ομομορφισμός $k[x]$ προτύπων που είναι η ταυτοτική απεικόνιση στο $\langle x \rangle$. Έστω $\alpha'(1) = xf(x)$, $f(x) \in k[x]$. Τότε $\alpha'(x) = x\alpha'(1) = x^2 f(x)$, δηλαδή $x = x^2 f(x)$. Φυσικά δεν υπάρχει τέτοιο $f(x)$.

1.3. Ελεύθερα και Προβολικά Πρότυπα

Μια οικογένεια $(e_\lambda)_{\lambda \in \Lambda}$ στοιχείων ενός R-προτύπου M καλείται **βάση** του M αν κάθε $m \in M$ γράφεται κατά μοναδικό τρόπο ως $m = \sum_{\lambda \in \Lambda} r_\lambda e_\lambda$, όπου $r_\lambda \in R$ είναι όλα μηδέν εκτός το πολύ ένα πεπερασμένο πλήθος.

Ένα R-πρότυπο λέγεται **ελεύθερο** αν έχει μια τουλάχιστον βάση. Για παράδειγμα, το R είναι ελεύθερο R-πρότυπο με βάση το σύνολο $\{1\}$. Για κάθε $n > 1$, το $\mathbb{Z}_n$ δεν είναι ελεύθερο $\mathbb{Z}$-πρότυπο γιατί $na = 0$ για κάθε $a \in \mathbb{Z}_n$, δηλαδή το 0 δεν γράφεται κατά μοναδικό τρόπο όπως απαιτεί ο ορισμός. Κάθε k-διανυσματικός χώρος είναι ελεύθερο k-πρότυπο. Το $M_n(R)$ είναι ελεύθερο R-πρότυπο με μια βάση τα στοιχεία $E_{ij} \in M_n(R)$, $i, j = 1, \ldots, n$, όπου E_{ij} είναι ο πίνακας με μηδέν παντού εκτός από τη θέση (i, j) όπου υπάρχει το 1.

1.3.1 Πρόταση. *i) Ένα R-πρότυπο M είναι ελεύθερο αν και μόνο αν είναι ισόμορφο με ένα πρότυπο της μορφής* $\bigoplus_{\lambda \in \Lambda} R_\lambda$, *όπου* $R_\lambda = R$ *για κάθε* $\lambda \in \Lambda$.
ii) Κάθε R-πρότυπο είναι ομομορφική εικόνα ελεύθερου R-προτύπου.

Απόδειξη. i) Αν το M είναι ελεύθερο με βάση $(e_\lambda)_{\lambda \in \Lambda}$, τότε ορίζεται ένας ισομορφισμός $\varphi : M \ni m \mapsto (r_\lambda)_{\lambda \in \Lambda} \in \bigoplus_{\lambda \in \Lambda} R_\lambda$, όπου $m = \sum_{\lambda \in \Lambda} r_\lambda e_\lambda$. Αντίστροφα, το $\bigoplus_{\lambda \in \Lambda} R_\lambda$ είναι ελεύθερο γιατί μία βάση του είναι το σύνολο $\{\varepsilon_\lambda \mid \lambda \in \Lambda\}$, όπου ε_λ είναι η ακολουθία $\varepsilon_\lambda = (\varepsilon_\lambda)_\mu$ με $\varepsilon_{\lambda\mu} = 0$ αν $\lambda \neq \mu$ και $\varepsilon_{\lambda\lambda} = 1$.
ii) Έστω $Λ$ ένα σύνολο γεννητόρων του M, π.χ. $\Lambda = M$. Κατά τον προφανή τρόπο ορίζεται ένας

επιμορφισμός $\underset{\lambda\in\Lambda}{\oplus} R_\lambda \to M$.

1.3.2 Πρόταση. *Έστω* $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ *μια ακριβής ακολουθία R-προτύπων. Αν το C είναι ελεύθερο, τότε αυτή διασπάται.*

Απόδειξη. Έστω $\{e_\lambda\}_{\lambda\in\Lambda}$ μια βάση του *C*. Επιλέγουμε για κάθε $\lambda\in\Lambda$ ένα στοιχείο $b_\lambda \in B$, έτσι ώστε $\beta(b_\lambda)=e_\lambda$ (ο β είναι επιμορφισμός). Ορίζουμε έναν *R*-ομομορφισμό $\beta' : C \to B$ από τις σχέσεις $\beta'(e_\lambda)=b_\lambda$. Ισχύει $\beta\circ\beta' = 1_C$ και άρα (Πρόταση 1.2.4) η ακολουθία διασπάται.

Ερχόμαστε τώρα στα προβολικά πρότυπα. Θα περιοριστούμε στα πλέον απαραίτητα για τα κεφάλαια που ακολουθούν.

1.3.3 Πρόταση. *Έστω P ένα R-πρότυπο. Τα ακόλουθα είναι ισοδύναμα:*
i) Για κάθε ομομορφισμό $f : P \to B$ *R-προτύπων και για κάθε επιμορφισμό R-προτύπων* $p : A \to B$, *υπάρχει ομομορφισμός* $g : P \to A$ *R-προτύπων που καθιστά το διάγραμμα μεταθετικό*

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "g"'] \arrow[d, "f"] & \\
A \arrow[r, "p"'] & B \arrow[r] & 0
\end{tikzcd}$$

ii) Κάθε ακριβής ακολουθία $0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$ *διασπάται.*
iii) Το P είναι ευθύς προσθετέος κάποιου ελεύθερου R-προτύπου (δηλαδή $P\oplus X = F$, *για κάποια R-πρότυπα X, F όπου το F είναι ελεύθερο).*

Απόδειξη. $\text{i)} \Rightarrow \text{ii)}$. Προκύπτει άμεσα θεωρώντας το διάγραμμα

$$\begin{tikzcd}
 & P \arrow[dl, dashed, "g"'] \arrow[d, "1_P"] & \\
M \arrow[r, "p"'] & P \arrow[r] & 0
\end{tikzcd}$$

$\text{ii)} \Rightarrow \text{iii)}$. Έστω $F \to P \to 0$ επιμορφισμός *R*-προτύπων, όπου το *F* είναι ελεύθερο (δες την πρόταση 1.3.1 ii)), και $N=\ker(F\to P)$. Η ακριβής ακολουθία $0 \longrightarrow N \longrightarrow F \longrightarrow P \longrightarrow 0$ διασπάται, και άρα $F \cong N\oplus P$.
$\text{iii)} \Rightarrow \text{i)}$. Έστω $P\oplus X$ ελεύθερο *R*-πρότυπο για κάποιο *R*-πρότυπο *X*. Θεωρούμε το διάγραμμα *R*-ομομορφισμών.

Φ

$$\begin{tikzcd}
 & P\oplus X \arrow[ddl, "f"'] \arrow[d, shift right, "i"'] & \\
 & P \arrow[u, shift right, "\pi"'] \arrow[d] & \\
A \arrow[r, "p"'] & B \arrow[r] & 0
\end{tikzcd}$$

όπου $\pi(a,x)=a$ και $i(a)=(a,0)$, $a\in P$, $x\in X$. Επειδή το $P\oplus X$ είναι ελεύθερο, εύκολα διαπιστώνουμε ότι υπάρχει R-ομομορφισμός $\Phi: P\oplus X\to A$ που καθιστά μεταθετικό το διάγραμμα (αν $(e_i)_{i\in I}$ είναι μια βάση του $P\oplus X$, ορίζουμε $\Phi(e_i)=z_i$, όπου $p(z_i)=f\circ\pi(e_i)$). Τώρα η ζητούμενη απεικόνιση $g: P\to A$ είναι η σύνθεση

$$P\xrightarrow{i}P\oplus X\xrightarrow{\Phi}A.$$

Ένα R-πρότυπο P που ικανοποιεί μια από τις συνθήκες της προηγούμενης πρότασης καλείται **προβολικό**. Η πρόταση 1.3.2 (ή η απόδειξη της Πρότασης 1.3.3) μας πληροφορεί ότι:

1.3.4 Πόρισμα. *Κάθε ελεύθερο πρότυπο είναι προβολικό.*

Το αντίστροφο δεν ισχύει. Από $\mathbb{Z}_2\oplus\mathbb{Z}_3\simeq\mathbb{Z}_6$ (ως $\mathbb{Z}_6$-πρότυπα) συμπεραίνουμε ότι το $\mathbb{Z}_2$ είναι προβολικό $\mathbb{Z}_6$-πρότυπο. Όμως δεν είναι ελεύθερο $\mathbb{Z}_6$-πρότυπο (γιατί;).

Η επόμενη πρόταση μας πληροφορεί ότι τα προβολικά πρότυπα 'συμπεριφέρονται καλά' ως προς το ευθύ άθροισμα.

1.3.5 Πρόταση. *Έστω $(P_\lambda)_{\lambda\in\Lambda}$ μια οικογένεια R-προτύπων. Τότε το $\underset{\lambda\in\Lambda}{\oplus}P_\lambda$ είναι προβολικό αν και μόνο αν κάθε P_λ είναι προβολικό.*

Απόδειξη. Αν το $\underset{\lambda\in\Lambda}{\oplus}P_\lambda$ είναι προβολικό, τότε $\underset{\lambda\in\Lambda}{\oplus}P_\lambda\oplus X$ είναι ελεύθερο για κάποιο X. Άρα κάθε P_λ είναι ευθύς προσθετέος ελεύθερου προτύπου. Αντίστροφα, αν για κάθε $\lambda\in\Lambda$ υπάρχει πρότυπο X και ελεύθερο πρότυπο F_λ με την ιδιότητα $P_\lambda\oplus X_\lambda=F_\lambda$, τότε $\left(\underset{\lambda\in\Lambda}{\oplus}P\right)\oplus\left(\underset{\lambda\in\Lambda}{\oplus}X_\lambda\right)=\underset{\lambda\in\Lambda}{\oplus}F_\lambda$ που είναι ελεύθερο R-πρότυπο (πρόταση 1.3.1 i) για παράδειγμα).

1.3.6. Σημείωση. Δεν θα ασχοληθούμε εδώ με τη 'δυϊκή' έννοια του προβολικού προτύπου πέρα από τον ορισμό του: ένα R-πρότυπο I λέγεται **εμφυτευτικό** αν κάθε ακριβής ακολουθία R-προτύπων της μορφής $0\to I\to A\to B\to 0$ διασπάται (σύγκρινε με την Πρόταση 1.3.3 ii)). Στις σημειώσεις αυτές η έννοια του εμφυτευτικού προτύπου εμφανίζεται μόνο στο Θεώρημα 2.1.2.

1.4 Λήμμα του Zorn και Μέγιστα Ιδεώδη

Μια σχέση $\le$ σε ένα (μη κενό) σύνολο X ονομάζεται **σχέση μερικής διάταξης** αν i) $x\le x\ \forall x\in X$, ii) $x\le y,\ y\le z\Rightarrow x\le z$, και iii) $x\le y,\ y\le x\Rightarrow x=y$. Το X ονομάζεται τότε **μερικά διατεταγμένο** σύνολο. Ένα μερικά διατεταγμένο σύνολο X στο οποίο ισχύει η πρόσθετη συνθήκη iv) για κάθε $x,y\in X$ είτε $x\le y$ είτε $y\le x$, ονομάζεται **ολικά διατεταγμένο**.

Έστω Y ένα υποσύνολο του μερικά διατεταγμένου συνόλου X. Ένα στοιχείο $x\in X$ ονομάζεται **άνω φράγμα** του Y στο X αν $y\le x$ για κάθε $y\in Y$.

Ένα στοιχείο $x\in X$ του μερικά διατεταγμένου συνόλου X ονομάζεται **μέγιστο** (ή **μεγιστικό**) αν δεν υπάρχει $x'\in X$ με $x\le x',\ x\ne x'$.

1.4.1 Λήμμα του Zorn. *Έστω X ένα μη κενό μερικά διατεταγμένο σύνολο του οποίου κάθε μη κενό ολικά διατεταγμένο υποσύνολο έχει ένα άνω φράγμα στο X. Τότε το X έχει ένα τουλάχιστον μέγιστο στοιχείο.*

Αποδεικνύεται στη Θεωρία Συνόλων ότι το Λήμμα του Zorn είναι ισοδύναμο με το Αξίωμα Επιλογής. Βέβαια εμείς εδώ θα το δεχτούμε ως αξίωμα. Ακολουθεί μια τυπική εφαρμογή. Θυμίζουμε πρώτα ότι ένα γνήσιο ιδεώδες I του R λέγεται **μέγιστο** αν δεν υπάρχει άλλο ιδεώδες J με την ιδιότητα $I \subsetneqq J \subsetneqq R$.

1.4.2 Πρόταση. *Κάθε δακτύλιος $R \neq 0$ έχει ένα τουλάχιστον μέγιστο ιδεώδες.*

Απόδειξη. Έστω X το σύνολο των γνήσιων ιδεωδών του R. Ισχύει $X \neq \varnothing$ αφού $(0) \in X$. Έστω Y ένα μη κενό ολικά διατεταγμένο υποσύνολο του X. (Η σχέση μερικής διάταξης στο X είναι η σχέση υποσυνόλου). Θέτουμε

$$J = \bigcup_{I \in Y} I$$

και παρατηρούμε ότι είναι ιδεώδες του R. Πράγματι, αν $a, b \in J$ τότε $a \in I_1$ και $b \in I_2$ για κάποια $I_1, I_2 \in Y$. Επειδή το Y είναι ολικά διατεταγμένο, ισχύει $I_1 \subseteq I_2$ ή $I_2 \subseteq I_1$. Συνεπώς $a + b \in J$. Επίσης $ra \in I_1$ για κάθε $r \in R$. Άρα $ra \in J$. Το J είναι γνήσιο, γιατί αν $J = R$ θα είχαμε $1 \in J$, δηλαδή $1 \in I$ για κάποιο $I \in Y$, δηλαδή $R \in Y \subseteq X$, άτοπο. Άρα το J είναι ένα άνω φράγμα του Y στο X. Από το Λήμμα του Zorn, το X έχει ένα μέγιστο στοιχείο, που φυσικά είναι μέγιστο ιδεώδες.

1.4.3 Πρόταση. *Κάθε δακτύλιος $R \neq 0$ έχει ένα τουλάχιστον απλό R-πρότυπο.*

Απόδειξη. Έστω I ένα μέγιστο ιδεώδες του R (Πρόταση 1.4.2). Το R-πρότυπο R / I είναι απλό, γιατί κάθε υποπρότυπό του έχει τη μορφή J / I όπου $J \supseteq I$ είναι ιδεώδες του R.

1.5 Δακτύλιοι Διαίρεσης

Ένας αποτελεσματικός τρόπος μελέτης δακτυλίου είναι να εξετάσουμε ιδιότητες των προτύπων του. Ένα απλούστατο παράδειγμα παρέχει το παρακάτω θεώρημα. Κάθε σώμα k έχει την ιδιότητα ότι όλα τα k-πρότυπα είναι ελεύθερα. Ποιοι δακτύλιοι έχουν την ιδιότητα αυτή;

1.5.1 Θεώρημα. *Ένας δακτύλιος $R \neq 0$ είναι δακτύλιος διαίρεσης αν και μόνο αν κάθε R-πρότυπο είναι ελεύθερο.*

Για την απόδειξη, χρειαζόμαστε τον ακόλουθο λήμμα.

1.5.2 Λήμμα. *Έστω $M \neq 0$ ένα R-πρότυπο, όπου R είναι δακτύλιος διαίρεσης. Τότε υπάρχει γραμμικά ανεξάρτητο υποσύνολο του M μέγιστο ως προς τη σχέση υποσυνόλου.*

Απόδειξη. Έστω X το σύνολο των γραμμικά ανεξάρτητων υποσυνόλων του M. (Ισχύει $X \neq \varnothing$, γιατί κάθε μονοσύνολο $\{a\}$ με $a \in M$, $a \neq 0$, είναι γραμμικά ανεξάρτητο, αφού έχουμε $ra = 0,\ r \neq 0 \Rightarrow a = 1a = r^{-1}(ra) = 0$). Θεωρούμε τη μερική διάταξη στο X που δίνεται από τη σχέση υποσυνόλου. Έστω Y ένα ολικά διατεταγμένο υποσύνολο του X. Ορίζοντας

$$\Omega = \bigcup_{A \in Y} A$$

εύκολα επαληθεύουμε ότι το Ω είναι γραμμικά ανεξάρτητο. Δηλαδή το Ω είναι ένα άνω φράγμα του Y στο X. Το ζητούμενο προκύπτει από το Λήμμα του Zorn.

Απόδειξη του Θεωρήματος 1.5.1.
"$\Rightarrow$" Έστω R δακτύλιος διαίρεσης και M ένα R-πρότυπο. Έστω B ένα μέγιστο γραμμικά ανεξάρτητο υποσύνολο του M (Λήμμα 1.5.2). Έστω $m \in M$ το οποίο δεν γράφεται ως γραμμικός συνδυασμός των στοιχείων του B. Θα φθάσουμε σε άτοπο, πράγμα που σημαίνει ότι το B είναι βάση του M. Το $\{m\} \cup B$ είναι γραμμικά εξαρτημένο από τον ορισμό του B. Άρα

$$rm + \sum r_i b_i = 0, \quad r \neq 0$$

για κάποια $r_i \in R$ και $b_i \in B$. Συνεπώς

$$m = -r^{-1}\left(\sum r_i b_i\right) = -\sum r^{-1} r_i b_i ,$$

που είναι άτοπο.

"$\Leftarrow$" Πρώτα παρατηρούμε ότι το το R είναι απλό R-πρότυπο. Πράγματι, έστω I ένα μέγιστο ιδεώδες του R (Πρόταση 1.4.2). Τότε το R-πρότυπο $M = R/I$ είναι απλό. Από την υπόθεση είναι και ελεύθερο. Άρα έχει βάση αποτελούμενη από ένα στοιχείο. Συνεπώς $M \cong R$, δηλαδή το R είναι απλό R-πρότυπο.

Έστω $x \in R,\ x \neq 0$. Για το κύριο ιδεώδες (x) του R έχουμε, λόγω της απλότητας του R, $(x) = R$ και επομένως υπάρχει $y \in R$ με $yx = 1$. Μένει να δείξουμε ότι $xy = 1$. Όπως πριν έχουμε $(y) = R$ και επομένως $zy = 1$ για κάποιο $z \in R$. Αλλά $yx = 1 \Rightarrow zyx = z \Rightarrow x = z$.

Έστω R ένας δακτύλιος διαίρεσης και $M \neq 0$ ένα R-πρότυπο. Το M είναι ελεύθερο σύμφωνα με το προηγούμενο θεώρημα. Έστω ότι έχει μια βάση με $n < \infty$ στοιχεία. Όπως ακριβώς στη Γραμμική Άλγεβρα (δηλαδή με τη χρήση του "λήμματος της ανταλλαγής") αποδεικνύεται και εδώ ότι κάθε άλλη βάση θα έχει n στοιχεία. Έτσι ορίζεται η **τάξη** του M, που συμβολίζεται $\dim M$ ή rkM, ως ο πληθάριθμος μιας βάσης του. (Στην περίπτωση που το M έχει μια βάση με άπειρα στοιχεία θα γράφουμε $\dim M = \infty$).

Η προηγούμενη ιδιότητα δεν ισχύει για γενικούς δακτυλίους όπως δείχνει το επόμενο παράδειγμα.

1.5.3 Παράδειγμα. Έστω $R = End_{\mathbb{Z}}\left(\bigoplus_{i\in\mathbb{N}} \mathbb{Z}\right)$. Ως R-πρότυπο, το R είναι ελεύθερο μια βάση το μονοσύνολο $\{1\}$. Θα κατασκευάσουμε τώρα μια άλλη βάση του R με δύο στοιχεία! Έστω $\{e_1, e_2, ...\}$ η κανονική βάση του $\bigoplus_{i\in\mathbb{N}} \mathbb{Z}$ ως $\mathbb{Z}$-πρότυπο, δηλαδή $e_1 = (1,0,0,...)$, $e_2 = (0,1,0,...)$ κλπ. Έστω $f, g \in R$ που ορίζονται από τις σχέσεις

$$f(e_i) = \begin{cases} e_n, & \text{αν } i = 2n \\ 0, & \text{αν } i = 2n-1 \end{cases}$$

$$g(e_i) = \begin{cases} 0, & \text{αν } \ i = 2n \\ e_n, & \text{αν } \ i = 2n-1. \end{cases}$$

Τότε κάθε $\varphi \in R$ γράφεται μοναδικά ως $\varphi = \alpha f + \beta g$, $\alpha, \beta \in R$. (Μάλιστα ισχύει $\alpha(e_i) = \varphi(e_{2i})$, $\beta(e_i) = \phi(e_{2i-1})$). Άρα μία βάση του R είναι το $\{f, g\}$.

Σημείωση. Αποδεικνύεται ότι σε μη μηδενικούς μεταθετικούς δακτυλίους η έννοια της τάξης ελεύθερου προτύπου είναι καλά ορισμένη.

Αν M είναι ένα R-πρότυπο και X υποσύνολο του M. Θέτουμε $Ann(X) = \left\{ r \in R \middle| rx = 0\ \forall x \in X \right\}$. Το $Ann(X)$ ονομάζεται ο **μηδενιστής** του M και είναι ιδεώδες του R (άσκηση). Αν το X είναι υποπρότυπο του M, τότε το $Ann(X)$ είναι αμφίπλευρο ιδεώδες του R (άσκηση). Για παράδειγμα, για το $\mathbb{Z}$-πρότυπο $M = \mathbb{Z}_6 \oplus \mathbb{Z}_8$, έχουμε $Ann(M) = (24)$. Στην περίπτωση που το σύνολο $X = \{x\}$ έχει μόνο ένα στοιχείο, θα γράφουμε $Ann(x)$ στη θέση του $Ann(X)$.

Ασκήσεις

Στα παρακάτω, R παριστάνει δακτύλιο.

1. Ένα στοιχείο $e \in R$ λέγεται **αυτοδύναμο** αν $e^2 = e$. Έστω $e \in R$ αυτοδύναμο στοιχείο που ανήκει στο κέντρο του R. Τότε τα κύρια (αριστερά) ιδεώδη (e) και $(1-e)$ είναι αμφίπλευρα και μάλιστα υποδακτύλιοι του R. Ως δακτύλιοι ισχύει $R \simeq (e) \times (1-e)$. Επίσης το (e) είναι προβολικό R-πρότυπο.

2. Έστω $e_1, \ldots, e_n$ αυτοδύναμα στοιχεία του R (βλ. προηγούμενη άσκηση) για τα οποία $e_i e_j = 0 \ (i \neq j)$, $e_i \in C(R)$ και $e_1 + \ldots + e_n = 1$. Τότε ως δακτύλιοι $R \cong R_1 \times \ldots \times R_n$, όπου $R_i = (e_i)$.

3. Αν R είναι δακτύλιος, με R^{op} συμβολίζουμε το δακτύλιο όπου ως σύνολο $R^{op} = R$, η πρόσθεση είναι αυτή του R αλλά ο πολλαπλασιασμός ορίζεται "ανάποδα" $r \cdot s = sr$. Δείξετε ότι

i) $k[G]^{op} \simeq k[G]$ (G ομάδα, k σώμα)

ii) $\mathbb{H}^{op} \simeq \mathbb{H}$

iii) $M_n(R)^{op} \simeq M_n(R^{op})$

iv) $End_R(R) \simeq R^{op}$.

4. Έστω $R \subseteq M_2(\mathbb{C})$, $R = \left\{ \begin{pmatrix} \bar{a} & b \\ -\bar{b} & a \end{pmatrix} \middle| \ a, b \in \mathbb{C} \right\}$. Ως $\mathbb{R}$-άλγεβρες, $R \simeq \mathbb{H}$.

5. Έστω $m > 1$. Το $\mathbb{Z}$-πρότυπο $\mathbb{Z}_m$ είναι απλό αν και μόνο αν ο m είναι πρώτος.

6. Έστω $R \neq 0$ ένας δακτύλιος. Τα ακόλουθα είναι ισοδύναμα.

i) R είναι δακτύλιος διαίρεσης

ii) κάθε R-πρότυπο είναι ελεύθερο

iii) κάθε κυκλικό R-πρότυπο είναι ελεύθερο.

7. Έστω I, J δυο ιδεώδη του R. Δείξτε τα εξής.

i) Υπάρχει ακριβής ακολουθία R-προτύπων της μορφής

$$0 \to I \cap J \to R \to R/I \times R/J \to R/(I+J) \to 0.$$

ii) (**Κινεζικό θεώρημα υπολοίπων**) Αν τα I, J είναι αμφίπλευρα ιδεώδη και ισχύει $I + J = R$, τότε οι δακτύλιοι $R/I \cap J$ και $R/I \times R/J$ είναι ισόμορφοι.

8. i) Έστω $0 \to A \to B \to C \to 0$ μια ακριβής ακολουθία R-προτύπων. Αν τα A και C είναι πεπερασμένα παραγόμενα, τότε και το B είναι πεπερασμένα παραγόμενο.

ii) Έστω M, N υποπρότυπα ενός τρίτου R-προτύπου. Αν τα $M + N$ και $M \cap N$ είναι πεπερασμένα παραγόμενα, τότε και τα M, N είναι πεπερασμένα παραγόμενα.

9. Έστω V ένα D-πρότυπο πεπερασμένης τάξης, όπου D-δακτύλιος διαίρεσης. Θέτουμε $R = End_D(V)$.

i) Το V είναι R-πρότυπο με εξωτερικό πολλαπλασιασμό $f \cdot v = f(v), \ f \in R, \ v \in V$.

ii) Το V είναι απλό R-πρότυπο.

iii) Υπάρχει ισομορφισμός $D \simeq End_R(V)$, $d \mapsto \varphi_d$, όπου $\varphi_d(v) = dv$.

10. Έστω R, S δυο δακτύλιοι. Θυμίζουμε ότι το κέντρο του R είναι ο υποδακτύλιος $C(R) = \{r \in R \mid rs = sr$ για κάθε $s \in R\}$. Δείξτε τα εξής.

i) $C(R \times S) = C(R) \times C(S)$

ii) $C(M_n(R)) \simeq C(R)$

iii) D δακτύλιος διαίρεσης $\Rightarrow C(D)$ σώμα.

iv) Έστω D ένας δακτύλιος διαίρεσης και $V \neq 0$ ένα D-πρότυπο. Τότε $C(End_D(V)) \simeq C(D)$.

11. Έστω M ένα R-πρότυπο. Τα ακόλουθα είναι ισοδύναμα

i) Το M είναι απλό.

ii) Για κάθε $m \in M, m \neq 0, \ M = (m)$.

iii) Το $M \simeq R/I$ για κάποιο μέγιστο ιδεώδες I του R.

12. Δείξτε με παράδειγμα ότι γενικά **δεν** ισχύει $Hom_R(\prod_{\lambda \in \Lambda} M_\lambda, N) \simeq \prod_{\lambda \in \Lambda} Hom(M_\lambda, N)$. Υπόδειξη: Έστω Λ =

$\mathbb{N}$, $M = N = R =$ σώμα. Χρησιμοποιήστε το γεγονός ότι αν ένας διανυσματικός χώρος είναι ισόμορφος με τον δυϊκό του, τότε είναι πεπερασμένης διάστασης.

13. Έστω k σώμα, G μια πεπερασμένη ομάδα, $a \in G$ και $C = \{gag^{-1} | g \in G\}$. Δείξτε ότι το στοιχείο $\sum_{c \in C} c$ ανήκει στο κέντρο της άλγεβρας $k[G]$.

14. Έστω G μια πεπερασμένη κυκλική ομάδα τάξης n και k ένα σώμα. Αποδείξτε ότι υπάρχει ισομορφισμός k-αλγεβρών $k[G] \simeq \dfrac{k[x]}{(x^n - 1)}$.

15. Αποδείξτε ότι υπάρχει ισομορφισμός δακτυλίων $End(\mathbb{Z} \oplus \mathbb{Z}) \simeq M_2(\mathbb{Z})$.

16. Έστω R ένας δακτύλιος.

i) Έστω I αμφίπλευρο ιδεώδες του R. Δείξτε ότι το $M_n(I)$ είναι αμφίπλευρο ιδεώδες του $M_n(R)$ και $M_n(R)/M_n(I) \simeq M_n(R/I)$.

ii) Αποδείξτε ότι κάθε αμφίπλευρο ιδεώδες του $M_n(R)$ είναι της μορφής $M_n(I)$, όπου I είναι αμφίπλευρο ιδεώδες του R.

17. Έστω $m, n > 0$. Αποδείξτε ότι υπάρχει ισομορφισμός ομάδων $Hom_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) \simeq \mathbb{Z}_d$, όπου $d = \mu\kappa\delta(m,n)$.

18. Έστω k ένα σώμα, $R = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in M_2(k) \right\}$ και $I = \left\{ \begin{pmatrix} 0 & 0 \\ b & c \end{pmatrix} \in R \right\}$. Εξετάστε αν το I είναι αμφίπλευρο ιδεώδες του R. Αληθεύει ότι το I είναι απλό R-πρότυπο; Αν όχι, να βρεθεί ένα απλό R-υποπρότυπο του I.

19. Έστω $0 \to M \to N \to R \to 0$ ακριβής ακολουθία R-προτύπων. Δείξτε ότι οι αβελιανές ομάδες $Hom_R(N, M)$ και $Hom_R(M, M) \oplus M$ είναι ισόμορφες.

20. Έστω D μια $\mathbb{R}$ - άλγεβρα διαίρεσης. Δείξτε ότι αν ο $\dim_{\mathbb{R}} D < \infty$, τότε για κάθε $d \in D$ υπάρχει $\lambda \in \mathbb{R}$ με $d^2 + \lambda d \in \mathbb{R}$.

21. Έστω R μια k-άλγεβρα, όπου k σώμα. Τότε R κεντρική αν και μόνο αν $M_n(R)$ κεντρική.

22. Δείξτε ότι ο δακτύλιος $T_n(R)$ των $n \times n$ άνω τριγωνικών πινάκων είναι ισόμορφος με το δακτύλιο $L_n(R)$ των $n \times n$ κάτω τριγωνικών πινάκων;

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 (θεώρημα του Wedderburn). Η κλάση των δακτυλίων αυτών παίζει σημαντικό ρόλο στη θεωρία αναπαραστάσεων πεπερασμένων ομάδων, πράγμα που θα δούμε στο κεφάλαιο 7.

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. Δεχόμαστε ότι ο μηδενικός δακτύλιος είναι ημιαπλός.

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 $\mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$ 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 $R = \bigoplus_{i \in I} R_i$, $S = \bigoplus_{j \in J} S_j$, 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 $R \times S = \left(\bigoplus_{i \in I} \overline{R}_i \right) \oplus \left(\bigoplus_{j \in J} \overline{S}_j \right)$.

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

$$\sum_{i \in I} M_i = \bigoplus_{i \in I} M_i .$$

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 $M = \bigoplus_{j\in J} M_j$, 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 $M = \bigoplus_{j\in J'} M_j$. Πράγματι, $\bigoplus_{j\in J'} M_j \subseteq M$. Για την άλλη σχέση, θεωρούμε ένα τυχαίο M_i και παρατηρούμε ότι

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

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

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

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

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 $g(M_i) \simeq M_i$. Άρα η εικόνα $g(M) = N$ παράγεται από κάποια απλά πρότυπα, οπότε λόγω του i) είναι ημιαπλό πρότυπο. Ο περιορισμός της g σε κάθε απλό προσθετέο είναι ισομορφισμός ή μηδενική απεικόνιση. Από αυτό έπεται ότι η ακριβής ακολουθία $0 \to L \to M \to N \to 0$ διασπάται (Πρόταση 1.2.4). Άρα το $Ker g = L$ είναι ισόμορφο με ευθύ προσθετέο του M και συνεπώς είναι ισόμορφο με πηλίκο του M. Από αυτό που αποδείξαμε πριν, έπεται ότι το L είναι ημιαπλό.

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 $R \cong M_{n_1}(D_1) \times ... \times M_{n_s}(D_s)$, 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 $R^{op} \simeq End_R(R),\ r \mapsto f_r$, 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

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

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

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

όπου $\varepsilon_j(m) = (0,...,m,...,0)$ είναι η εμφύτευση στη *j* συνιστώσα και $\pi_i(m_1,...,m_n) = m_i$ 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 $End_R(M \oplus N) \simeq End_R(M) \times End_R(N)$. Πράγματι, λόγω της Πρότασης 1.2.2 και της υπόθεσης στα *M*, *N* υπάρχει ισομορφισμός αβελιανών ομάδων $End_R(M \oplus N) \simeq End_R(M) \times End_R(N)$. 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 $\underset{i\in I}{\oplus} M_i$ είναι μη-μηδενικές, δηλαδή το I είναι πεπερασμένο. Μπορούμε έτσι να γράψουμε

$$R \simeq \overset{s}{\underset{i=1}{\oplus}} M_i^{n_i} \quad \text{όπου} \quad M_i \simeq M_j \Leftrightarrow i = j\,.$$

Έχουμε τώρα διαδοχικά ισομορφισμούς δακτυλίων

$$\begin{aligned}
R &\simeq (R^{op})^{op} \\
&\simeq (End_R(R))^{op} && \text{(παρατήρηση α)} \\
&= \left(End_R \left(\overset{s}{\underset{i=1}{\oplus}} M_i^{n_i} \right) \right)^{op} \\
&\simeq \left(\prod_{i=1}^{s} End_R(M_i^{n_i}) \right)^{op} && \text{(γιατί } Hom_R(M_i^{n_i}, M_j^{n_j}) = 0 \text{ αν } i \neq j\text{. Παρατήρηση γ)} \\
&\simeq \prod_{i=1}^{s} \left(End_R(M_i^{n_i})^{op} \right) && \left((R \times S)^{op} \simeq R^{op} \times S^{op} \right) \\
&\simeq \prod_{i=1}^{s} \left(M_{n_i}(End_R(M_i)^{op}) \right). && \text{(παρατήρηση β και άσκηση 1.3.3 iii)).}
\end{aligned}$$

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 $R \simeq \prod_{i=1}^{s} M_{n_i}(D_i)$.

$(6) \Rightarrow (1)$

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. Ισχύει

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

Αν γράψουμε $\beta = \sum_j \beta_j E_{jk}$, τότε εύκολα ελέγχουμε με τη βοήθεια των προηγουμένων σχέσεων (άσκηση) 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 σε κάθε ημιαπλό δακτύλιο R υπάρχουν ιδεώδη $I_1,...,I_k$ (πεπερασμένο πλήθος) με $R = I_1 \oplus ... \oplus I_k$ και I_i απλό για κάθε i.

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.

***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 (για παράδειγμα, βλ. 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

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

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

$$\begin{aligned}
\beta\overline{\beta}(c) &= \frac{1}{n}\sum_{g \in G} \beta(g\beta'(g^{-1}c)) \\
&= \frac{1}{n}\sum_{g \in G} g(\beta\beta'(g^{-1}c)) && \text{(γιατί } \beta \text{ είναι ομομορφισμός } k[G]\text{-προτύπων)} \\
&= \frac{1}{n}\sum_{g \in G} g1_C(g^{-1}c) \\
&= \frac{1}{n}(nc) = c.
\end{aligned}$$

[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.

"$\Leftarrow$" 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. Από το θεώρημα του Wedderburn έχουμε $R\simeq M_{n_1}(D_1)\times\ldots\times M_{n_s}(D_s)$, όπου κάθε D_i είναι δακτύλιος διαίρεσης. Είναι οι ακέραιοι $n_1,\ldots,n_s$, s μονοσήμαντα ορισμένοι;

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 αν 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 $k,\ \ell$. Για τους στοιχειώδεις πίνακες E_{ij} ισχύει

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

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 $I=R$.

Αν $R\simeq M_{n_1}(D_1)\times\ldots\times M_{n_s}(D_s)$ όπως στο Θεώρημα του Wedderburn, τότε $R\simeq R_1\times\ldots\times R_s$, όπου κάθε $R_i=M_{n_1}(D_i)$ είναι αμφίπλευρο ιδεώδες του R και επιπλέον απλός δακτύλιος από το προηγούμενο λήμμα.

2.3.2 Λήμμα. *Έστω $R\simeq R_1\times\ldots\times R_m$ και $R\simeq R_1'\times\ldots\times R_n'$ όπου τα R_i και R_i' είναι αμφίπλευρα ιδεώδη του R. Αν* *οι R_i και R_i' απλοί δακτύλιοι, τότε $m = n$.*

Απόδειξη: Μια γενική παρατήρηση (άσκηση): Κάθε αμφίπλευρο ιδεώδες I του $R_1' \times \ldots \times R_n'$ είναι της μορφής $I = I_1' \times \ldots \times I_n'$, όπου I_i' αμφίπλευρο ιδεώδες του R_i'.

Έχουμε ισομορφισμό δακτυλίων

$$R_1 \times \ldots \times R_m \to R_1' \times \ldots \times R_n'.$$

Έστω $m \le n$. Θα δείξουμε ότι $m = n$ με επαγωγή στο m. Για $m = 1$ έχουμε ισομορφισμό $R_1 \to R_1' \times \ldots \times R_n'$ και επειδή ο R_1 είναι απλός παίρνουμε ότι ο $R_1' \times \ldots \times R_n'$ είναι απλός, οπότε $n = 1$.

Έστω $m \ge 2$. Η εικόνα του $R_1 \times 0 \times \ldots \times 0$ είναι αμφίπλευρο ιδεώδες του $R_1' \times \ldots \times R_n'$, άρα της μορφής $I_1' \times \ldots \times I_n'$ σύμφωνα με την παρατήρηση. Επειδή ο $R_1 \times 0 \times \ldots \times 0$ είναι απλός, η εικόνα είναι της μορφής $0 \times \ldots \times I_k' \times \ldots \times 0$ και επειδή ο R_k' είναι απλός η εικόνα είναι $0 \times \ldots \times R_k' \times \ldots \times 0$. Από τον ισομορφισμό $R_1 \times \ldots \times R_m \to R_1' \times \ldots \times R_n'$ επάγεται ισομορφισμός $\dfrac{R_1 \times \ldots \times R_m}{R_1 \times 0 \times \ldots \times 0} \to \dfrac{R_1' \times \ldots \times R_n'}{0 \times \ldots \times R_k' \times \ldots \times 0}$, δηλαδή ισομορφισμός $R_2 \times \ldots \times R_m \to R_1' \times \ldots \times R_{k-1}' \times R_{k+1}' \times \ldots \times R_n'$. Από την επαγωγική υπόθεση $m - 1 = n - 1$.

Τα δύο προηγούμενα λήμματα δίνουν αμέσως το εξής:

2.3.3 Πόρισμα. *Έστω R ένας ημιαπλός δακτύλιος οπότε*

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

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 $r_1 \in R_1$. 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*

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

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

$$\begin{array}{ccccc} & & \text{στήλη } j & & \\ & & \downarrow & & \end{array}$$

$$\begin{pmatrix} 0 & \cdots & a_1 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & a_{n_i} & \cdots & 0 \end{pmatrix} \in M_{n_i}(D_i)$$

(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 $\overline{V_{ij}} \not\simeq \overline{V_{i'j'}}$ 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

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

παίρνουμε

$$R \simeq \overline{V}_{11}^{n_1} \oplus \ldots \oplus \overline{V}_{s1}^{n_s}. \tag{**}$$

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), το γεγονός ότι τα $\overline{V}_{i1}$ είναι απλά και το γεγονός ότι το V είναι απλό δίνουν ότι το V είναι ισόμορφο με ένα από τα $\overline{V}_{i1}$.

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*

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

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 2.16. Η σχέση $n_i = \dim_{D_i} V_i$ είναι σαφής.

Εφαρμογή στις πεπερασμένες ομάδας

Χρειαζόμαστε την ακόλουθη εκδοχή του Λήμματος του Schur.

2.3.7 Πρόταση *Έστω R μια k-άλγεβρα, όπου k αλγεβρικά κλειστό σώμα, και M ένα απλό R-πρότυπο με*

$\dim_k M < \infty$. *Τότε* $End_R(M) \simeq k$.

Απόδειξη: Έστω $f \in End_R(M)$. Ως γραμμική απεικόνιση πεπερασμένης διάστασης διανυσματικού χώρου πάνω από αλγεβρικά κλειστό σώμα, η f έχει ιδιοτιμή $\lambda_f \in k$. Τότε $f - \lambda_f 1_M \in End_R(M)$. Επειδή το M είναι απλό R -πρότυπο, έχουμε $\ker(f - \lambda_f 1_M) = M$, οπότε $f = \lambda_f 1_M$. Είναι σαφές ότι η απεικόνιση $f \mapsto \lambda_f$ είναι ισομορφισμός δακτυλίων.

Αν στην απόδειξη του θεωρήματος Wedderburn ,$1) \Rightarrow 6)$, χρησιμοποιήσουμε την προηγούμενη πρόταση στη θέση του Λήμματος του Schur, παίρνουμε το εξής αποτέλεσμα. Έστω k αλγεβρικά κλειστό σώμα και R k-άλγεβρα με $dim_k R < \infty$. Αν ο R είναι ημιαπλός, τότε υπάρχει ισομορφισμός k-αλγεβρών $R \simeq M_{n_1}(k) \times ... \times M_{n_s}(k)$. Ειδικά για άλγεβρες ομάδων έχουμε:

2.3.8 Πόρισμα *Έστω k ένα αλγεβρικά κλειστό σώμα και G μια πεπερασμένη ομάδα τέτοια ώστε ο δακτύλιος* $k[G]$ *είναι ημιαπλός. Τότε*

- *i)* $k[G] \simeq M_{n_1}(k) \times ... \times M_{n_s}(k)$ *(ως k-άλγεβρες),*
- *ii)* $n = n_1^2 + ... + n_s^2$, *όπου* $n = |G|$,
- *iii)* $s =$ *πλήθος των ανά δύο μη ισόμορφων απλών* $k[G]$ *προτύπων,*
- *iv)* $n_1, ..., n_s$ *είναι οι διαστάσεις των δύο μη ισόμορφων απλών* $k[G]$ *προτύπων.*

Απόδειξη: Τα i), iii) και iv) είναι γνωστά. Το ii) προκύπτει από το i) λαμβάνοντας διαστάσεις k-χώρων.

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. Επειδή το $\mathbb{C}$ είναι αλγεβρικά κλειστό, η Πρόταση 2.3.8 δίνει $\mathbb{C}[G] \simeq M_{n_1}(\mathbb{C}) \times ... \times M_{n_s}(\mathbb{C})$. Επειδή η G είναι αβελιανή παίρνουμε $n_1 = ... = n_s = 1$. Αφού $\dim_{\mathbb{C}} \mathbb{C}[G] = n$ έχουμε $s = n$ και $\mathbb{C}[G] \simeq \mathbb{C} \times ... \times \mathbb{C}$ (n φορές).

Σημείωση: Στο παράδειγμα αυτό 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 $\mathbb{C}[G] \simeq \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$.
Πράγματι, όπως πριν έχουμε $\mathbb{C}[G] \simeq M_{n_1}(\mathbb{C}) \times ... \times M_{n_s}(\mathbb{C})$. Από την Πρόταση 2.3.8 ii) παίρνουμε ότι $8 = n_1^2 + ... + n_s^2$ οπότε έχουμε τις εξής περιπτώσεις

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

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.

3) Εδώ θεωρούμε κυκλική ομάδα G τάξης 4. Για $k=\mathbb{C}$ από το Παράδειγμα 1 έχουμε

$$\mathbb{C}[G]\simeq \mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}.$$

Για το σώμα $k=\mathbb{Q}$ ισχύει $\mathbb{Q}[G]\simeq \mathbb{Q}[x]/(x^4-1)$ σύμφωνα με ην άσκηση 1.14. Επειδή έχουμε την ανάλυση $x^4-1=(x-1)(x+1)(x^2+1)$ σε γινόμενο αναγώγων στο $\mathbb{Q}[x]$, to Κινεζικο θεωρημα υπολοίπων (βλ. άσκηση 1.7) δίνει $\mathbb{Q}[x]/(x^4-1)\simeq \mathbb{Q}[x]/(x-1)\times\mathbb{Q}[x]/(x-1)\times\mathbb{Q}[x]/(x^2+1)$ και άρα

$$\mathbb{Q}[G]\simeq \mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}(i).$$

Ασκήσεις

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

Έστω $R=\left\{\begin{pmatrix} a & b\\ 0 & c\end{pmatrix} \middle|\ a,b,c\in\mathbb{C}\right\}$. 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 ετα 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 το 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.

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. i) Αληθεύει ότι για κάθε ακέραιο $n>1$ υπάρχει πεπερασμένος ημιαπλός δακτύλιος τάξης n ;

ii) Να ταξινομηθούν ως προς ισομορφισμό οι ημιαπλοί δακτύλιοι τάξης 5^4.

9. Έστω $R\simeq M_{n_1}(D_1)\times\ldots\times M_{n_s}(D_s)$ 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 $i \neq j$,

$e_1 + ... + e_n = 1$,

$e_i\, v = v$ για κάθε v 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 $\Phi : D^{op} \to End_R(V), \Phi(d)(v) = vd$ 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 $V = (v)$. 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 1.9 iii).

17. Αν ο R είναι ημιαπλός δακτύλιος, τότε και ο $M_n(R)$ είναι ημιαπλός.

18. Έστω k σώμα και $A \in M_n(k)$. Με $k[A]$ συμβολίζουμε τον υποδακτύλιο $\{a_0 I_n + a_1 A + ... + a_m A^m \,|\, m \in \mathbb{N}, a_i \in k\}$ του $A \in M_n(k)$.

i) Δείξτε ότι αν ο A είναι διαγωνίσιμος, τότε ο $k[A]$ είναι ημιαπλός.

ii) Για $n = 2$ και $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ αληθεύει ότι $k[A]$ είναι ημιαπλός;

iii) Δείξτε ότι αν το k είναι αλγεβρικά κλειστό, τότε ισχύει το αντίστροφο του i).

ΚΕΦΑΛΑΙΟ 3: Συνθήκες Αλυσίδων

Μελετάμε εδώ τη συνθήκη της αύξουσας αλυσίδας υποπροτύπων και τη συνθήκη της φθίνουσας αλυσίδας υποπροτύπων. Αυτές συνδέονται μεταξύ τους με την έννοια της συνθετικής σειράς (Θεώρημα 3.2.3). Το κύριο αποτέλεσμα σχετίζεται με το Κεφάλαιο 2 και περιγράφει τη δομή των απλών δακτυλίων του Artin (Θεώρημα Wedderburn-Artin).

3.1 Πρότυπα της Noether και πρότυπα του Artin

3.1.1 Ορισμός

- *Ένα R-πρότυπο M λέγεται πρότυπο της **Noether** (αντίστοιχα, του **Artin**) αν κάθε αύξουσα $M_0 \subseteq M_1 \subseteq ...$ (αντίστοιχα, φθίνουσα $M_0 \supseteq M_1 \supseteq ...$) ακολουθία υποπροτύπων του M γίνεται τελικά σταθερή, δηλαδή αν $M_n = M_{n+1} = ...$ για κάποιο n.*
- *Ένας δακτύλιος καλείται δακτύλιος της **Noether** (αντίστοιχα, του **Artin**) αν ικανοποιεί την αντίστοιχη συνθήκη ως R-πρότυπο, δηλαδή αν κάθε αύξουσα (αντίστοιχα, φθίνουσα) ακολουθία ιδεωδών του R γίνεται τελικά σταθερή.*

Παραδείγματα

1) Ο δακτύλιος $\mathbb{Z}$ είναι της Noether, γιατί η μοναδική παραγοντοποίηση ενός $a \neq 0, \pm 1$ σε γινόμενο πρώτων αριθμών σημαίνει ότι το ιδεώδες (α) περιέχεται σε πεπερασμένου πλήθους ιδεώδη. (Για μια άλλη δικαιολόγηση, δες την Πρόταση 3.1.2 (iii) παρακάτω). Με παρόμοιο τρόπο, βλέπουμε ότι κάθε περιοχή κυρίων ιδεωδών είναι δακτύλιος της Noether.

2) Ο $\mathbb{Z}$ δεν είναι του Artin αφού $(2) \underset{\neq}{\supset} (2^2) \underset{\neq}{\supset} (2^3) \underset{\neq}{\supset} ...$.

3) Κάθε πεπερασμένος δακτύλιος είναι και της Noether και του Artin, γιατί το πλήθος των ιδεωδών είναι πεπερασμένο. Για τον ίδιο λόγο κάθε δακτύλιος διαίρεσης είναι και της Noether και του Artin.

4) Ο δακτύλιος των πολυωνύμων $\mathbb{Z}[x_1, x_2, ...]$ στις απείρου πλήθους μεταβλητές $x_1, x_2 ...$ δεν είναι ούτε της Noether ούτε του Artin, γιατί έχουμε τις αλυσίδες ιδεωδών $(x_1) \underset{\neq}{\subset} (x_1, x_2) \underset{\neq}{\subset} (x_1, x_2, x_3) \underset{\neq}{\subset} ...$ και $(x_1) \underset{\neq}{\supset} (x_1^2) \underset{\neq}{\supset} (x_1^3) \underset{\neq}{\supset} ...$.

5) Κάθε k-άλγεβρα R πεπερασμένης διάστασης πάνω από το k είναι δακτύλιος και της Noether και του Artin, γιατί κάθε ακολουθία ιδεωδών του R είναι ακολουθία διανυσματικών χώρων και οι διαστάσεις αυτών είναι μεταξύ του 0 και n, όπου $n = \dim_k R$.

3.1.2 Πρόταση. *Έστω M* ένα *R*-πρότυπο. Τα ακόλουθα είναι ισοδύναμα.

(i) Το M είναι της Noether.
(ii) Κάθε μη κενό υποσύνολο προτύπων του M έχει μέγιστο στοιχείο.
(iii) Κάθε υποπρότυπο του M είναι πεπερασμένα παραγόμενο.

Απόδειξη: (i) $\Rightarrow$ (ii) . Έστω $X \neq \varnothing$ ένα σύνολο υποπροτύπων του *M*. Έστω $M_0 \in M$. Αν το M_0 δεν είναι μέγιστο, τότε υπάρχει $M_1 \in X$ με $M_0 \underset{\neq}{\subset} M_1$. Αν το M_1 δεν είναι μέγιστο, τότε υπάρχει $M_2 \in X$ με $M_0 \underset{\neq}{\subset} M_1 \underset{\neq}{\subset} M_2$. Συνεχίζουμε λαμβάνοντας μια αύξουσα ακολουθία υποπροτύπων του *M*. Από την υπόθεση αυτή κάπου τερματίζει, $M_n = M_{n+1} = ...$ Προφανώς το M_n είναι μέγιστο στοιχείο του *X*.

(ii) $\Rightarrow$ (iii) . Έστω *N* υποπρότυπο του *M* και *X* το σύνολο των πεπερασμένα παραγόμενων υποπροτύπων του

N. Φυσικά $X \neq \varnothing$. Έστω N_0 ένα μέγιστο στοιχείο του X σύμφωνα με την υπόθεση. Θα δείξουμε ότι $N = N_0$. Αρκεί να δείξουμε $N \subseteq N_0$: Έστω $a \in N$. Το πρότυπο $N_0 + \langle a \rangle$ είναι πεπερασμένα παραγόμενο και $N_0 \subseteq N_0 + (a)$. Άρα $N_0 + (a) = N_0$, απ'όπου παίρνουμε $a \in N_0$. Άρα $N \subseteq N_0$.
(iii) $\Rightarrow$ (i). Έστω $M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots$ μια αύξουσα ακολουθία υποπροτύπων του M. Το πρότυπο $N = \bigcup_i M_i$ είναι πεπερασμένα παραγόμενο από την υπόθεση, $N = (a_1,\ldots,a_n)$. Υπάρχουν m_i με $a_i \in M_{m_i}$, $i = 1,\ldots,n$. Θέτοντας $m = \max\{m_1,\ldots,m_n\}$ έχουμε $\bigcup_i M_i = M_m$ λόγω της αλυσίδας. Άρα $M_m = M_{m+1} = \ldots$.

Με ανάλογο τρόπο αποδεικνύεται η εξής πρόταση.

3.1.3 Πρόταση. *Έστω M ένα R-πρότυπο. Τα ακόλουθα είναι ισοδύναμα.*
(i) Το M είναι του Artin.
(ii) Κάθε μη κενό σύνολο υποπροτύπων του M έχει ελάχιστο στοιχείο.

Απόδειξη: Άσκηση.

Συνεπώς σ' ένα δακτύλιο της Noether (αντίστοιχα, του Artin) κάθε μη κενό σύνολο ιδεωδών έχει μέγιστο (αντίστοιχα, ελάχιστο) στοιχείο. Επίσης σ' ένα δακτύλιο της Noether κάθε ιδεώδες είναι πεπερασμένα παραγόμενο.

3.1.4 Πρόταση. *Έστω*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

μια ακριβής ακολουθία R-προτύπων. Τότε το M είναι πρότυπο της Noether (αντίστοιχα, του Artin) αν και μόνο αν τα L και N είναι πρότυπα της Noether (αντίστοχα, του Artin).

Απόδειξη: Θα ασχοληθούμε με πρότυπα της Noether μόνο καθώς η περίπτωση των προτύπων του Artin είναι παρόμοια. Έστω ότι το M είναι της Noether. Θεωρούμε αύξουσες αλυσίδες

$$L_0 \subseteq L_1 \subseteq \ldots \quad \text{και} \quad N_0 \subseteq N_1 \subseteq \ldots \tag{1}$$

υποπροτύπων του L και N αντίστοιχα. Παίρνουμε αντίστοιχες ακολουθίες υποπροτύπων του M

$$f(L_0) \subseteq f(L_1) \subseteq \ldots \quad \text{και} \quad g^{-1}(N_0) \subseteq g^{-1}(N_1) \subseteq \ldots, \tag{2}$$

που τελικά είναι σταθερές λόγω της υπόθεσης στο M. Αν $f(L_n) = f(L_{n+1}) = \ldots$ παίρνουμε $L_n = L_{n+1} = \ldots$, γιατί ο f είναι μονομορφισμός. Επίσης αφού το g είναι επιμορφισμός, έχουμε $g^{-1}(N_m) = g^{-1}(N_{m+1}) = \ldots \Rightarrow N_m = N_{m+1} = \ldots$. Αντίστροφα, έστω ότι τα L,N είναι της Noether, και έστω $M_0 \subseteq M_1 \subseteq \ldots$ αύξουσα ακολουθία υποπροτύπων του M. Απ'αυτή παίρνουμε τις ακολουθίες

$$f^{-1}(M_0) \subseteq f^{-1}(M_1) \subseteq \ldots,\ g(M_0) \subseteq g(M_1) \subseteq \ldots$$

που είναι τελικά σταθερές. Άρα υπάρχει n με

$$f^{-1}(M_n) = f^{-1}(M_{m+1}) = \ldots,\ g(M_n) = g(M_{n+1}) = \ldots\ .$$

Θα δείξουμε ότι $M_n = M_{n+1} = \ldots$. Έστω $x \in M_{k+1}$, όπου $k \geq n$. Τότε $g(x) \in g(M_{k+1}) = g(M_k)$. Άρα $g(x) = g(y)$, για κάποιο $y \in M_k$. Συνεπώς $g(x-y) = 0$ και $x - y \in \ker g = \operatorname{Im} f$. Άρα $x - y \in \operatorname{Im} f \cap M_{k+1}$ και $f^{-1}(x-y) \in$ $f^{-1}(M_{k+1}) = f^{-1}(M_k)$, απ'όπου παίρνουμε $x - y \in M_k$. Άρα $x \in M_k$. Αποδείξαμε ότι $M_{k+1} \subseteq M_k$, και συνεπώς $M_{k+1} = M_k$.

Σύμφωνα με τη μια κατεύθυνση της προηγούμενης πρότασης, οι ιδιότητες ‘πρότυπο της Noether’ και ‘πρότυπο του Artin’ κληρονομούνται στα υποπρότυπα και στα πηλίκα.

3.1.5 Πόρισμα. *Έστω* $M_1,\ldots,M_n$ *R-πρότυπα. Τότε το* $\overset{n}{\underset{i=1}{\oplus}} M_i$ *είναι της Noether (αντίστοιχα, του Artin) αν και μόνο αν κάθε* M_i *είναι της Noether (αντίστοιχα, του Artin).*

Απόδειξη: Επαγωγή στο *n*. Για $n=1$ το πόρισμα είναι προφανές. Έστω $n>1$ και θεωρούμε την ακριβή ακολουθία

$$0 \longrightarrow M_1 \xrightarrow{i} M_1 \oplus \ldots \oplus M_n \xrightarrow{\pi} M_2 \oplus \ldots \oplus M_n \longrightarrow 0$$

όπου $i(a_1)=(a_1,0,\ldots,0)$ και $\pi(a_1,\ldots,a_n)=(a_2,\ldots,a_n)$, $a_i \in M_i$. Από την Πρόταση 3.1.4, το $M_1 \oplus \ldots \oplus M_n$ είναι της Noether (αντίστοιχα, του Artin) αν και μόνο αν τα M_1 και $M_2 \oplus \ldots \oplus M_n$ είναι της Noether (αντίστοιχα, του Artin). Αλλά από την επαγωγική υπόθεση, το $M_2 \oplus \ldots \oplus M_n$ είναι της Noether (αντίστοιχα, του Artin) αν και μόνο αν τα $M_2,\ldots,M_n$ είναι της Noether (αντίστοιχα, του Artin).

3.1.6 Πόρισμα. *Κάθε ημιαπλός δακτύλιος είναι και της Noether και του Artin.*

Απόδειξη: Επειδή κάθε απλό πρότυπο είναι προφανώς και της Noether και του Artin, το ζητούμενο προκύπτει από το Πόρισμα 3.1.5 και την Παρατήρηση 2.1.4.

3.1.7 Πόρισμα. *Έστω R ένας δακτύλιος της Noether (αντίστοιχα, του Artin). Τότε κάθε πεπερασμένα παραγόμενα R-πρότυπο είναι της Noether (αντίστοιχα, του Artin).*

Απόδειξη: Έστω *M* ένα πεπερασμένα παραγόμενο *R*-πρότυπο. Τότε υπάρχει επιμορφισμός $F \to M$, όπου το *F* είναι ελεύθερο και μάλιστα της μορφής $F \simeq \overset{n}{\underset{i=1}{\oplus}} R$, $n<\infty$. (Πρόταση 1.3.1 ii) και η απόδειξή της). Από το Πόρισμα 3.1.5 το *F* είναι της Noether (αντίστοιχα, του Artin) και άρα (Πρόταση 3.1.4) το *M* είναι της Noether (αντίστοιχα, του Artin).

Σημείωση: Το Πόρισμα 3.1.5 δεν ισχύει για $n=\infty$. Για παράδειγμα, ενώ το $\mathbb{Z}$ ως $\mathbb{Z}$-πρότυπο είναι της Noether, το $\mathbb{Z}$-πρότυπο $\underset{i\in\mathbb{N}}{\oplus}\mathbb{Z}$ δεν είναι της Noether καθώς έχουμε την αύξουσα ακολουθία υποπροτύπων $\mathbb{Z}\oplus 0\oplus 0\oplus\ldots \subseteq \mathbb{Z}\oplus\mathbb{Z}\oplus 0\oplus\ldots \subseteq \mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\oplus 0\oplus\ldots \subseteq \ldots$. Επίσης το Πόρισμα 3.1.7 δεν ισχύει γενικά για πρότυπα που δεν είναι πεπερασμένα παραγόμενα (γιατί;).

3.2. Συνθετικές Σειρές

Ποιά πρότυπα είναι *και* της Noether *και* του Artin. Το θεώρημα που θα αποδείξουμε εδώ χαρακτηρίζει τα προαναφερθέντα πρότυπα και θα εφαρμοστεί στην απόδειξη του Θεωρήματος 4.2.4 του επόμενου κεφαλαίου.

3.2.1 Ορισμός. *Μια* ***συνθετική σειρά*** *ενός R-προτύπου M είναι μια (πεπερασμένη) ακολουθία υποπροτύπων του M*

$$0 = M_n \subseteq ... \subseteq M_1 \subseteq M_0 = M$$

όπου κάθε πηλίκο M_i / M_{i+1} *είναι απλό πρότυπο.*

Παραδείγματα

1) Έστω D δακτύλιος διαίρεσης και V ένα πεπερασμένο παραγόμενο D-πρότυπο. Από το κεφάλαιο 1 ξέρουμε ότι το V είναι ελεύθερο πρότυπο και έχει πεπερασμένη βάση, έστω $\{v_1,...,v_n\}$. Αν V_i είναι το υποπρότυπο του V που παράγεται από τα $v_1,...,v_{n-i}$, τότε έχουμε την ακολουθία $0 = V_n \subseteq ... \subseteq V_1 \subseteq V_0 = V$ και κάθε διαδοχικό πηλίκο V_i / V_{i+1} είναι απλό D-πρότυπο αφού έχει διάσταση 1.

2) Κάθε ημιαπλός δακτύλιος έχει συνθετική σειρά: αν $R = I_1 \oplus ... \oplus I_n$, όπου κάθε I_i είναι απλό ιδεώδες (Παρατήρηση 2.1.4), τότε έχουμε τη συνθετική σειρά

$$0 \subseteq I_1 \subseteq I_1 \oplus I_2 \subseteq ... \subseteq I_1 \oplus ... \oplus I_n = R.$$

3) Έστω k σώμα. Μια συνθετική σειρά του $k[x]/(x^3)$ ως $k[x]/(x^3)$-πρότυπο είναι

$$0 \subseteq (x^2)/(x^3) \subseteq (x)/(x^3) \subseteq k[x]/(x^3).$$

4) Έστω $p \neq q$ πρώτοι. Μια συνθετική σειρά του $\mathbb{Z}$-προτύπου $\mathbb{Z}_{pq}$ είναι

$$0 \subseteq ([p]) \subseteq \mathbb{Z}_{pq}$$

και μια άλλη είναι

$$0 \subseteq ([q]) \subseteq \mathbb{Z}_{pq}.$$

Άρα οι όροι σε μια συνθετική σειρά δεν είναι μοναδικοί. Στην πρώτη συνθετική σειρά τα διαδοχικά πηλίκα (από αριστερά στα δεξιά) είναι $\mathbb{Z}_q, \mathbb{Z}_p$ και στη δεύτερη συνθετική σειρά είναι $\mathbb{Z}_p, \mathbb{Z}_q$. Βλέπουμε ότι το μήκος και τα διαδοχικά πηλίκα (εκτός από τη σειρά τους) είναι μοναδικά. Σχετικά ισχύει το εξής αποτέλεσμα:

3.2.2 Θεώρημα *(Jordan Hölder). Έστω δύο συνθετικές σειρές του M*

$$0 \subseteq M_m \subseteq ... \subseteq M_1 \subseteq M_0 = M$$

$$0 \subseteq M'_n \subseteq ... \subseteq M'_1 \subseteq M'_0 = M.$$

Τότε $m = n$ *και υπάρχει μετάθεση π, έτσι ώστε*

$$M_i / M_{i+1} \simeq M'_{\pi(i)} / M'_{\pi(i)+1}.$$

Η απόδειξη του προηγούμενου θεωρήματος είναι λέξη προς λέξη ίδια για τις ομάδες που περιέχεται σε κάθε εισαγωγικό βιβλίο θεωρίας ομάδων και δεν θα μας απασχολήσει εδώ. Δεν θα χρησιμοποιήσουμε το προηγούμενο θεώρημα παρά μόνο σε ασκήσεις.

Ερχόμαστε τώρα να απαντήσουμε στο ερώτημα που θέσαμε πριν.

3.2.3 Θεώρημα. *Ένα πρότυπο έχει συνθετική σειρά αν και μόνο αν είναι πρότυπο και της Noether και της Artin.*

Απόδειξη: Θα δώσουμε μια απόδειξη ανεξάρτητη από το θεώρημα Jordan-Hölder.
"$\Rightarrow$" Έστω ότι το *M* έχει συνθετική σειρά και έστω *n* το μήκος της. Θα εφαρμόσουμε επαγωγή στο *n* ξεκινώντας από την τετριμμένη περίπτωση $n = 0$. Έστω $n \geq 1$ και η συνθετική σειρά

$$0 = M_n \subseteq ... \subseteq M_1 \subseteq M_0 = M.$$

Από το 3ο θεώρημα ισομορφισμών προτύπων (Πρόταση 1.1.3. iii) διαπιστώνουμε ότι

$$0=\frac{M_{n-1}}{M_{n-1}}\subseteq\ldots\subseteq\frac{M_1}{M_{n-1}}\subseteq\frac{M_0}{M_{n-1}}=\frac{M}{M_{n-1}}$$

είναι μια συνθετική σειρά του M/M_{n-1}. Αφού το μήκος είναι $n-1$, η επαγωγική υπόθεση δίνει ότι το M/M_{n-1} είναι πρότυπο και της Noether και του Artin. Το ίδιο συμβαίνει και για το M_{n-1} γιατί είναι απλό. Από την ακριβή ακολουθία

$$0\longrightarrow M_{n-1}\longrightarrow M\longrightarrow M/M_{n-1}\longrightarrow 0$$

και την Πρόταση 3.1.4 συμπεραίνουμε ότι το M είναι και της Noether και του Artin.

"$\Leftarrow$" Έστω ότι το M είναι και της Noether και του Artin. Έστω ότι δεν είναι απλό. Κατασκευάζουμε μια συνθετική σειρά κατά τον ακόλουθο προφανή τρόπο: Έστω M_1 μέγιστο γνήσιο υποπρότυπο του M (υπάρχει τέτοιο λόγω της Πρότασης 3.1.2) οπότε το πηλίκο M/M_1 είναι απλό. Αν το M_1 δεν είναι απλό, έστω M_2 ένα μέγιστο γνήσιο υποπρότυπο του M_1 (υπάρχει, γιατί το M_1 ως υποπρότυπο προτύπου της Noether είναι της Noether-Πρόταση 3.1.4) οπότε το πηλίκο M_1/M_2 είναι απλό. Συνεχίζουμε

$$\ldots\underset{\neq}{\subseteq}M_2\underset{\neq}{\subseteq}M_1\underset{\neq}{\subseteq}M_0=M\ .$$

Η διαδικασία τερματίζει μετά από πεπερασμένο αριθμό βημάτων γιατί το M είναι πρότυπο του Artin.

3.3. Απλοί δακτύλιοι του Artin

Υπενθυμίζουμε ότι ο δακτύλιος $M_n(D)$, όπου D δακτύλιος διαίρεσης, είναι απλός (Λήμμα 2.3.1) και δακτύλιος του Artin (Πόρισμα 3.1.6). Το Θεώρημα των Wedderburn-Artin λέει ότι πέρα από τους $M_n(D)$ δεν υπάρχουν άλλοι απλοί δακτύλιοι του Artin.

Υπενθυμίζουμε ότι αν M είναι ένα R-πρότυπο, ο μηδενιστής του M είναι

$$AnnM=\{r\in R\mid rm=0,\forall m\in M\}.$$

Το $AnnM$ είναι ένα αμφίπλευρο ιδεώδες του M.

Ορισμός *Ένα R-πρότυπο λέγεται* ***πιστό*** *αν* $AnnM=0$.

Παραδείγματα

1) Κάθε μη μηδενικό πρότυπο πάνω από δακτύλιο διαίρεσης είναι πιστό. Πιο γενικά, κάθε μη μηδενικό πρότυπο M πάνω από απλό δακτύλιο R είναι πιστό, αφού το $AnnM$ είναι μη μηδενικό αμφίπλευρο ιδεώδες του R και άρα τετριμμένο.

2) Για κάθε $m\neq 0$, το $\mathbb{Z}_m$ δεν είναι πιστό $\mathbb{Z}$-πρότυπο.

3) Το $\mathbb{Q}/\mathbb{Z}$ είναι πιστό $\mathbb{Z}$-πρότυπο.

4) Κάθε μη μηδενικό ελεύθερο πρότυπο είναι πιστό.

3.3.1 Θεώρημα (Wedderburn-Artin). *Για ένα δακτύλιο R τα ακόλουθα είναι ισοδύναμα:*

1) R είναι απλός δακτύλιος του Artin

2) R έχει απλό πιστό πρότυπο και είναι δακτύλιος του Artin.

3) $R\simeq M^n$*, για κάποιο απλό πρότυπο M*

4) R είναι ημιαπλός και όλα τα απλά πρότυπα είναι ισόμορφα

5) $R\simeq M_n(D)$*, όπου* D *είναι δακτύλιος διαίρεσης*

Απόδειξη: $1) \Rightarrow 2)$. Παρατηρούμε ότι αν $M \neq 0$ είναι ένα R-πρότυπο, τότε $AnnM = 0$, γιατί το $AnnM$ είναι ένα μη μηδενικό αμφίπλευρο ιδεώδες του απλού δακτυλίου R. Έστω τώρα $M \neq 0$ ένα υποπρότυπο του R. Αν το M είναι απλό, δεν υπάρχει τίποτα να αποδείξουμε. Αν όχι, τότε υπάρχει $M_1 \subsetneq M$, με M_1 μη μηδενικό. Αν το M_1 είναι απλό δεν υπάρχει κάτι να αποδείξουμε. Αν όχι, συνεχίζουμε. Με τον τρόπο αυτό λαμβάνουμε μια φθίνουσα ακολουθία ιδεωδών $M \supsetneq M_1 \supsetneq ....$ Από την υπόθεση του Artin, η ακολουθία αυτή είναι της μορφής

$$M \supsetneq M_1 \supsetneq .... \supsetneq M_n \supsetneq 0$$

Το M_n είναι απλό.

$2) \Rightarrow 3)$ Έστω M πιστό και απλό. Θα δείξουμε ότι ο R είναι ισόμορφο με υποπρότυπο του M^k για κάποιο k και άρα είναι ισόμορφο με M^n για κάποιο $n \leq k$. Θεωρούμε όλους του R-ομομορφισμούς $R \to M^k$, όπου $k \in \mathbb{N}$, και επιλέγουμε έναν με ελάχιστο πυρήνα, έστω $f : R \to M^k$. (Η υπόθεση της συνθήκης του Artin το επιτρέπει, Πρόταση 3.1.3). Ισχυριζόμαστε ότι ο f είναι μονομορφισμός. Πράγματι αν $f(r) = 0$ με $r \neq 0$, τότε υπάρχει $m \in M$ με $rm \neq 0$, γιατί το M είναι πιστό. Ορίζουμε έναν ομομορφισμό

$$g : R \to M^k \oplus M, \quad x \mapsto (f(x), xm).$$

Ισχύει $\ker g \subsetneq \ker f$, γιατί $r \notin \ker g$. Αυτό είναι άτοπο. Έτσι ο f είναι μονομορφισμός.

$3) \Rightarrow 4)$ Ο R είναι ημιαπλός από την Πρόταση 2.1.1. Ότι όλα τα απλά πρότυπά του είναι ισόμορφα έπεται για παράδειγμα, από την παρατήρηση ότι κάθε απλό πρότυπο είναι της μορφής R/I (I μέγιστο ιδεώδες του R, άσκηση 1.10) και συνεπώς είναι πηλίκο του M^n, και άρα είναι ισόμορφο με το M.

$4) \Rightarrow 5)$ Πρόταση 2.3.4.

$5) \Rightarrow 1)$ Λήμμα 2.3.1 και Πόρισμα 3.1.6.

3.3.2 Σημείωση Στα επόμενα κεφάλαια θα εφαρμόσουμε μια μικρή παραλλαγή του θεωρήματος των Wedderburn-Artin που αναφέρεται σε άλγεβρες. Έστω k σώμα και R πεπερασμένης διάστασης k-άλγεβρα. Υποθέτουμε ότι ο δακτύλιος R απλός. Τότε ο R είναι δακτύλιος του Artin, καθώς $\dim_k R < \infty$, και από το θεώρημα Wedderburn-Artin υπάρχει δακτύλιος διαίρεσης D με $R \simeq M_n(D)$. Από την απόδειξη του '$1 \Rightarrow 6$' στο θεώρημα 2.1.3, είναι σαφές ότι ο D (που είναι μοναδικός ως προς ισομορφισμό – βλ.πόρισμα 2.3.6) είναι k-άλγεβρα και επιπλέον ο ισομορφισμός $R \simeq M_n(D)$ είναι ισομορφισμός k-αλγεβρών. Αν V είναι D-πρότυπο τάξης n, τότε όπως ακριβώς στη Γραμμική Άλγεβρα με την αντιστοιχία πινάκων και γραμμικών απεικονίσεων, η επιλογή βάσης του V δίνει ισομορφισμό k-αλγεβρών $M_n(D) \simeq End_D(V)$. Έτσι το συμπέρασμα στο 5) του θεωρήματος Wedderburn-Artin μπορεί να διατυπωθεί ως εξής: Με τις προϋποθέσεις στο R που αναφέραμε πριν, υπάρχει ισομορφισμός k-αλγεβρών $R \simeq End_D(V)$, όπου D πεπερασμένης διάστασης k-άλγεβρα διαίρεσης και V πεπερασμένης τάξης D-πρότυπο.

Είδαμε ότι κάθε απλός δακτύλιος του Artin είναι ημιαπλός. Στο επόμενο παράδειγμα έχουμε έναν απλό δακτύλιο που *δεν* είναι ημιαπλός.

3.3.3 Παράδειγμα Θεωρούμε την άλγεβρα $\mathbb{C}\{x, y\}$ των πολυωνύμων στις μη μεταθετικές μεταβλητές[1] x, y.

---

[1] Μια βάση διανυσματικού χώρου $\mathbb{C}\{x, y\}$ αποτελεί το σύνολο των λέξεων $x^{a_1}y^{b_1}...x^{a_k}y^{b_k}$, όπου $a_i, b_i \geq 0$. Ο πολλαπλασιασμός της άλγεβρας $\mathbb{C}\{x, y\}$ δίνεται από την παράθεση λέξεων.

Έστω I το αμφίπλευρο ιδεώδες του $\mathbb{C}\{x,y\}$ που παράγεται από το $yx-xy-1$ και $R=\mathbb{C}\{x,y\}/I$. Τότε ο R είναι απλός αλλά όχι ημιαπλός.
Περιγράφουμε παρακάτω τα κύρια βήματα της απόδειξης και αφήνουμε τις λεπτομέρειες για άσκηση. Με X,Y συμβολίζουμε τις εικόνες $x+I, y+I$ των x, y αντίστοιχα στο R. Τότε έχουμε τη σχέση $YX-XY=1$.

0. Ως διανυσματικός χώρος ο R παράγεται από τα 'μονώνυμα' X^mY^n, $m,n\geq 0$.
1. $YX^mY^n = X^mY^{n+1}+mX^{m-1}Y^n$ για κάθε $m,n\geq 0$.
2. $Y^nX = XY^n + nY^{n-1}$ για κάθε $n\geq 0$.
3. Έστω I ένα αμφίπλευρο ιδεώδες του R και $f\in I$, $f\neq 0$. Έστω $Z=X^mY^n$ το 'μονώνυμο' μεγίστου βαθμού που εμφανίζεται στο f (σε μια ανάλυση του f που προβλέπεται από το 0.) ως προς τη διάταξη
$$X^aY^b\leq X^cY^d \Leftrightarrow 1)\ a<c \text{ ή } 2)\ a=c \text{ και } b\leq d .$$
Ορίζουμε τα εξής στοιχεία του I.
$X_1 = YZ-ZY$
$X_2 = YX_1 - X_1Y$
...
$X_m = YX_{m-1}-X_{m-1}Y$
Τότε χρησιμοποιώντας τη σχέση 1. προκύπτει ότι το X_m είναι 'πολυώνυμο' του Y 'βαθμού' n (δεν εμφανίζεται X).
4. Με τους προηγούμενους συμβολισμούς ορίζουμε τα εξής στοιχεία του I.
$Y_1 = X_mX - XX_m$
$Y_2 = Y_1X - XY_1$
...
$Y_n = Y_{n-1}X - XY_{n-1}$.
Τότε χρησιμοποιώντας το 2. και 3. προκύπτει ότι το Y_n είναι μια μη μηδενική σταθερά και άρα $I=R$. Συνεπώς ο R είναι απλός δακτύλιος.
5. Ο R δεν είναι ημιαπλός. Πράγματι, από το Πόρισμα 3.1.6 αρκεί να δείξουμε ότι ο R δεν είναι δακτύλιος του Artin. Έχουμε την αλυσίδα ιδεωδών
$$(Y)\supsetneqq(Y^2)\supsetneqq(Y^3)\supsetneqq\dots .$$
Σημείωση: Θεωρούμε την άλγεβρα $\mathbb{C}[x]$ των πολυωνύμων μιας μεταβλητής. Αποδεικνύεται ότι η άλγεβρα R του παραδείγματος είναι ισόμορφη με την υποάλγεβρα B της $End_{\mathbb{C}}(\mathbb{C}[x])$ που παράγεται από τις γραμμικές απεικονίσεις 1) $h=$'πολλαπλασιασμός με το x' και 2) $\frac{d}{dx}=$'παραγώγιση ως προς x'. Ο δε ισομορφισμός $R\simeq B$ επάγεται από την αντιστοιχία $X\mapsto h, Y\mapsto\frac{d}{dx}$. Έχουμε $\frac{d}{dx}\circ h - h\circ\frac{d}{dx}=1_{\mathbb{C}[x]}$, πράγμα που 'εξηγεί' τη σχέση $YX-XY=1$ στο R.
Η άλγεβρα B είναι ένα παράδειγμα των 'αλγεβρών Weyl'. Αυτές έχουν σημαντικές εφαρμογές στην Άλγεβρα, Ανάλυση και Κβαντική Φυσική.

Ασκήσεις

1. Εξετάστε αν το R πρότυπο M είναι της Noether ή/και του Artin.
- $M=\mathbb{Q},\ R=\mathbb{Q}$.
- $M=\mathbb{Q},\ R=\mathbb{Z}$.
- $M=\mathbb{Q}/\mathbb{Z},\ R=\mathbb{Z}$.

2. Θεωρώντας αύξουσες αλυσίδες δεξιών ιδεωδών ορίζεται η έννοια του δακτυλίου που είναι δεξιά της Noether. Αποδείξετε ότι ο δακτύλιος

$$\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a\in\mathbb{Z},\ \ b,c\in\mathbb{Q}\right\}$$

είναι δεξιά της Noether αλλά όχι αριστερά της Noether.

3. Αν ο R είναι δακτύλιος της Noether (αντ. Artin) τότε ο $M_n(R)$ είναι της Noether (αντ. Artin).

4. Έστω M R-πρότυπο και $f:M\to M$ ομομορφισμός.

i) Αν το M είναι πρότυπο του Artin και ο f μονομορφισμός, τότε ο f είναι ισομορφισμός.

ii) Αν το M είναι πρότυπο της Noether και ο f επιμορφισμός, τότε ο f είναι ισομορφισμός.

iii) Αν το M έχει συνθετική σειρά, τότε: f μονομορφισμός $\Leftrightarrow$ f επιμορφισμός.

Υπόδειξη για τα i) και ii): $\operatorname{Im} f\supseteq \operatorname{Im} f^2\supseteq\dots$ και $\ker f\subseteq \ker f^2\subseteq\dots$

5. Αν το M έχει συνθετική σειρά, ονομάζουμε το **μήκος** του M (συμβολικά $\ell(M)$) το μήκος της. Είναι καλά ορισμένο από το θεώρημα Jordan-Hölder. Αν η ακολουθία R-προτύπων

$$0\to M_n\to\dots\to M_1\to 0$$

είναι ακριβής και κάθε M_i έχει συνθετική σειρά, τότε $\sum_{i=1}^{n}(-1)^i\,\ell(M_i)=0$.

6. Έστω N_1,N_2 υποπρότυπα του N που έχει συνθετική σειρά τότε,

i) $\ell(N_1+N_2)=\ell(N_1)+\ell(N_2)-\ell(N_1\cap N_2)$

ii) $\ell(N/N_1\cap N_2)=\ell(N/N_1)+\ell(N/N_2)-\ell(N/N_1+N_2)$.

7. Ποιό είναι το μήκος του $M_2(\mathbb{H})$ ως $M_2(\mathbb{H})-$πρότυπο; Ως $\mathbb{H}$-πρότυπο; Ως $\mathbb{C}$-πρότυπο;

8. Έστω R μία $\mathbb{C}$-άλγεβρα και M ένα απλό R-πρότυπο με $\dim_{\mathbb{C}} M<\infty$. Αποδείξτε τα εξής.

i) $End_R(M)=\mathbb{C}$.

ii) Η απεικόνιση $R\to End_{\mathbb{C}}(M),\quad r\mapsto$ "πολλαπλασιασμός" με το r, είναι επί.

Υπόδειξη: για το ii) εφαρμόστε το θεώρημα Wedderburn-Artin θεωρώντας το M ως πιστό $R/AnnM$-πρότυπο.

9. Αληθεύει ότι κάθε απλός δακτύλιος του Artin έχει πεπερασμένο πλήθος ιδεωδών;
Υπόδειξη: $R=M_2(\mathbb{R})$.

10. Έστω R ένας δακτύλιος της Noether και $a,b\in R$ τέτοια ώστε $ab=1$. Αποδείξτε ότι $ba=1$.
Υπόδειξη: άσκηση 3 ii).

11. (Λήμμα του Fitting) Έστω M ένα R-πρότυπο μήκους n (βλ. άσκηση 4). Αποδείξτε ότι για κάθε $f\in End_R M$, έχουμε $M\simeq \operatorname{Im}(f^n)\oplus\ker(f^n)$.

12. Ένα πρότυπο λέγεται **μη αναλύσιμο** αν κάθε μη μηδενικό γνήσιο υποπρότυπό του δεν είναι ευθύς προσθετέος του. Για παράδειγμα, το $\mathbb{Z}$ είναι μη αναλύσιμο $\mathbb{Z}$-πρότυπο ενώ το $\mathbb{Z}_6$ δεν είναι μη αναλύσιμο $\mathbb{Z}$-πρότυπο αφού $\mathbb{Z}_6\simeq\mathbb{Z}_2\oplus\mathbb{Z}_3$.

Έστω M ένα μη αναλύσιμο R-πρότυπο με μήκος n (βλ. άσκηση 6) και $f\in End_R M$. Οι ακόλουθες προτάσεις είναι ισοδύναμες.

1. η f είναι 1-1
2. η f είναι επί
3. η f δεν είναι μηδενοδύναμη.

Υπόδειξη: άσκηση 11.

13. i) Αληθεύει ότι κάθε μη μηδενικό R-πρότυπο περιέχει γνήσιο μεγιστικό υποπρότυπο;
ii) Αληθεύει ότι κάθε μη μηδενικό R-πρότυπο περιέχει ελάχιστο μη μηδενικό μεγιστικό υποπρότυπο;

14. Δώστε ένα παράδειγμα δακτυλίου του Artin που δεν έχει απλό πιστό πρότυπο.

15. Έστω $\mathbb{Q}_2 = \{\frac{m}{2^n} \in \mathbb{Q} \,|\, m \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\}$. Το $\mathbb{Z}$-πρότυπο $\mathbb{Q}_2/\mathbb{Z}$ είναι του Artin αλλά όχι της Noether.

16. Αν το R-πρότυπο M είναι ημιαπλό και πεπερασμένα παραγόμενο, τότε ο δακτύλιος $End_R M$ είναι της Noether και του Artin.

17. Έστω M πιστό R-πρότυπο.
i) Δείξτε ότι αν το M είναι πρότυπο της Noether, τότε ο δακτύλιος R είναι της Noether.
ii) Αληθεύει ότι αν το M είναι πρότυπο της Artin, τότε ο δακτύλιος R είναι της Artin;
Υπόδειξη για το ii). $R = \mathbb{Z}$ και $M = \mathbb{Q}/\mathbb{Z}$.

18. Έστω k σώμα και $T_3(k)$ ο υποδακτύλιος των άνω τριγωνικών πινάκων του $M_3(k)$. Δείξτε ότι μια συνθετική σειρά του $V = M_{3\times 1}(k)$ ως $T_3(k)$-πρότυπο είναι

$$0 \subseteq \{\begin{pmatrix} * \\ 0 \\ 0 \end{pmatrix}\} \subseteq \{\begin{pmatrix} * \\ * \\ 0 \end{pmatrix}\} \subseteq V \ .$$

Αληθεύει ότι κάθε δύο ανάγωγα $T_3(k)$-πρότυπα είναι ισόμορφα;

19. Θεωρούμε την k-άλγεβρα $R = \{(a_{ij}) \in M_3(k) \,|\, a_{12} = a_{13} = 0\}$ και το R-πρότυπο $V = M_{3\times 1}(k)$ με εξωτερικό πολλαπλασιασμό τον πολλαπλασιασμό πινάκων.
i) Να βρεθεί μια συνθετική σειρά του R-προτύπου V.
ii) Αληθεύει ότι το V είναι ημιαπλό R-πρότυπο;

20. Έστω R ημιαπλή $\mathbb{C}$-άλγεβρα με $\dim_{\mathbb{C}} R < \infty$.
i) Να ταξινομηθούν ως προς ισομορφισμό οι R με $\dim_{\mathbb{C}} R = 5$. Σε κάθε περίπτωση να βρεθεί το μήκος $\ell(R)$ του R ως R-πρότυπο.
ii) Δείξτε ότι ο R είναι απλός αν και μόνο αν για κάθε μη μηδενικά R-πρότυπα M, N ισχύει $Hom_R(M,N) \neq 0$.

21. Έστω k σώμα. Δείξτε ότι υπάρχει ομομορφισμός k-αλγεβρών $M_m(k) \to M_n(k)$ αν και μόνο αν το m διαιρεί το n.

22. Έστω R απλός δακτύλιος του Artin. Αν I, J είναι απλά ιδεώδη του R, τότε υπάρχει $r \in R$ με $I = Jr$.
Υπόδειξη: Από το θεώρημα Wedderburn-Artin μπορούμε να υποθέσουμε ότι $R = M_n(D)$, όπου D δακτύλιος διαίρεσης.

ΚΕΦΑΛΑΙΟ 4: Ριζικό του Jacobson

Στο κεφάλαιο αυτό μελετάμε δακτυλίους του Artin χρησιμοποιώντας το ριζικό του Jacobson. Ως εφαρμογή αποδεικνύουμε ότι κάθε δακτύλιος του Artin είναι και της Noether.

4.1. Δακτύλιοι του Artin

Τι εμποδίζει ένα δακτύλιο του Artin να είναι ημιαπλός;

4.1.1 Πρόταση *Έστω R δακτύλιος. Τότε*

$$\bigcap_{M \text{ απλό}} AnnM = \bigcap_{I \text{ μέγιστο}} I,$$

όπου το M διατρέχει τα απλά R-πρότυπα και το I διατρέχει τα μέγιστα ιδεώδη του R.

***Απόδειξη**:* Έστω $r \in R$ τέτοιο ώστε $rM = 0$ για κάθε απλό R-πρότυπο M. Τότε $r\frac{R}{I} = 0_{R/I}$ για κάθε μέγιστο ιδεώδες I του R. Άρα $rR \subseteq I \Rightarrow r \in I$. Συνεπώς $\bigcap_{M \text{ απλό}} AnnM \subseteq \bigcap_{I \text{ μέγιστο}} I$.

Έστω $r \in R$ τέτοιο ώστε $r \in I$ για κάθε μέγιστο ιδεώδες I του R. Έστω M απλό R-πρότυπο και $m \in M, m \neq 0$. Η απεικόνιση $f_m : R \to M, x \mapsto xm,$ είναι ομομορφισμός R-προτύπων και επειδή το M είναι απλό είναι επί. Συνεπώς $R/\ker f_m \simeq M$ που σημαίνει ότι ο $\ker f_m$ είναι μέγιστο ιδεώδες οπότε $r \in Kerf_m$. Δηλαδή $rm = 0$ και επειδή αυτό ισχύει για κάθε $m \in M$ παίρνουμε $r \in AnnM$. Άρα $\bigcap_{I \text{ μέγιστο}} I \subseteq \bigcap_{M \text{ απλό}} AnnM$.

Το $\bigcap_{I \text{ μέγιστο}} I$ ονομάζεται **το ριζικό του Jacobson** του R και συμβολίζεται συνήθως με $J(R)$. Η προηγούμενη πρόταση λέει ότι το ιδεώδες $J(R)$ είναι *αμφίπλευρο* ιδεώδες του R αφού κάθε $AnnM$ είναι αμφίπλευρο ιδεώδες του R.

Παραδείγματα

1. $J(\mathbb{Z}) = 0$. Πράγματι, τα μέγιστα ιδεώδη του $\mathbb{Z}$ είναι τα (p),όπου p πρώτος, και είναι σαφές ότι η τομή αυτών είναι το μηδενικό ιδεώδες.
2. Αν $n = p_1^{n_1}...p_k^{n_k}$, όπου p_i διακεκριμένοι πρώτοι και $n_i > 0$, τότε $J(\mathbb{Z}_n) = (a)$, όπου $a = [p_1 p_2 ... p_k]$. Αυτό έπεται από το ότι τα μέγιστα ιδεώδη του $\mathbb{Z}_n$ είναι τα $([p_i])$, $i = 1,...,k$.
3. Αν D είναι δακτύλιος διαίρεσης, τότε $J(M_n(D)) = 0$ γιατί ο δακτύλιος $M_n(D)$ είναι απλός και το ριζικό του Jacobson είναι γνήσιο αμφίπλευρο ιδεώδες.
4. Αν R, S είναι δακτύλιοι, τότε $J(R \times S) = J(R) \times J(S)$. Αυτό έπεται από το γεγονός ότι τα μέγιστα ιδεώδη του $R \times S$ είναι τα $I \times S$, όπου I μέγιστο ιδεώδες του R, και τα $R \times J$, όπου J μέγιστο ιδεώδες του S.
5. Αν R είναι ημιαπλός δακτύλιος, τότε $J(R) = 0$. Πράγματι, από το Θεώρημα του Wedderburn έχουμε $R \simeq M_{n_1}(D_1) \times ... \times M_{n_s}(D_s)$, όπου D_i δακτύλιοι διαίρεσης, οπότε από τα προηγούμενα δύο παραδείγματα έχουμε $J(R) \simeq J(M_{n_1}(D_1)) \times ... \times J(M_{n_s}(D_s)) = 0$.

Το παρακάτω θεώρημα λέει ότι το ιδεώδες $J(R)$ "μετράει" κατά πόσο ένας δακτύλιος του Artin απέχει από το να είναι ημιαπλός. Παρέχει μια απάντηση στο ερώτημα που θέσαμε στην αρχή του κεφαλαίου.

4.1.2 Θεώρημα. *Ο δακτύλιος R είναι ημιαπλός αν και μόνο αν ο R είναι δακτύλιος του Artin και* $J(R)=0$.

Για την απόδειξη χρειαζόμαστε το ακόλουθο αποτέλεσμα.

4.1.3 Λήμμα. *Αν R είναι δακτύλιος του Artin, τότε υπάρχουν πεπερασμένου πλήθους μέγιστα ιδεώδη* $I_1,\ldots,I_n$ *με*

$$J(R)=I_1\cap\ldots\cap I_n.$$

Απόδειξη: Από την υπόθεση του Artin, το μη κενό (πρόταση 1.4.2) σύνολο ιδεωδών

$$\{\cap I_i \,/\, \{I_i\} \text{ πεπερασμένη οικογένεια μέγιστων ιδεωδών}\}$$

έχει ελάχιστο στοιχείο, έστω J. Θα δείξουμε ότι $J(R)=J$. Από τον ορισμό του $J(R)$ αρκεί να δείξουμε ότι $J\subseteq J(R)$. Έστω I μέγιστο ιδεώδες. Τότε $I\cap J\subseteq J$, οπότε ο ορισμός του J δίνει $I\cap J=J$. Άρα $J\subseteq I$ και επειδή αυτό ισχύει για κάθε μέγιστο ιδεώδες, παίρνουμε $J\subseteq J(R)$.

Απόδειξη του Θεωρήματος 4.1.2.
"$\Rightarrow$" Το είδαμε πριν στα παραδείγματα.
"$\Leftarrow$" Έστω ότι ο *R* είναι δακτύλιος του Artin με $J(R)=0$. Θα δείξουμε ότι ο *R* είναι υποπρότυπο ημιαπλού προτύπου, οπότε από την πρόταση 2.1.1 ii) θα είναι ημιαπλός δακτύλιος. Από την υπόθεση και το λήμμα 4.1.3 παίρνουμε $0=I_1\cap\ldots\cap I_n$ για κάποια μέγιστα ιδεώδη I_k. Συνεπώς ο ομομορφισμός *R*-προτύπων

$$R\to R/I_1\times\ldots\times R/I_n,\ r\mapsto(r+I_1,\ldots,r+I_n)$$

είναι μονομορφισμός. Όμως κάθε R/I_k είναι απλό R-πρότυπο, γιατί το I_k είναι μέγιστο. Άρα το $R/I_1\times\ldots\times R/I_n$ είναι ημιαπλό πρότυπο.

4.1.4 Πόρισμα. *R δακτύλιος του Artin* $\Rightarrow R/J(R)$ *ημιαπλός δακτύλιος.*

Απόδειξη: Ο $R/J(R)$ είναι του Artin, γιατί ο *R* είναι του Artin. Επιπλέον $J(R/J(R))=0$. Πράγματι, τα μέγιστα ιδεώδη του $R/J(R)$, είναι ακριβώς τα $I_i/J(R)$, όπου τα I_i είναι τα μέγιστα ιδεώδη του *R* που περιέχουν το $J(R)$, δηλαδή όλα τα μέγιστα ιδεώδη του *R*. Έτσι

$$J(R/J(R))=\bigcap_i(I_i/J(R))=J(R)/J(R)=0.$$

4.1.5 Πόρισμα. *Αν R δακτύλιος και* I *αμφίπλευρο ιδεώδες του* R *τέτοιο ώστε ο δακτύλιος* R/I *είναι ημιαπλός, τότε* $J(R)\subseteq I$.

Απόδειξη: Επειδή ο R/I είναι ημιαπλός έχουμε $J(R/I)=0$. Άρα $\bigcap\limits_{\substack{I'\,\text{μέγιστο}\\ I'\supseteq I}} I'=I.$ Επομένως $J(R)\subseteq I.$

Τα τελευταία δύο πορίσματα λένε ότι για δακτύλιο του Artin R, το $J(R)$ *είναι το ελάχιστο αμφίπλευρο ιδεώδες του* R *τέτοιο ώστε ο δακτύλιος* $R/J(R)$ *είναι ημιαπλός.*

4.2. Ιδιότητες του ριζικού του Jacobson και μια εφαρμογή

Στα παρακάτω μελετάμε το ριζικό του Jacobson και δίνουμε μια σημαντική εφαρμογή του.

Ένα ιδεώδες λέγεται **μηδενοδύναμο** αν $I^n=0$ για κάποιο *n*, δηλαδή αν $r_1\ldots r_n=0$ για κάθε $r_i\in I$. Για παράδειγμα, το ιδεώδες $I=([6])$ του $\mathbb{Z}_{24}$ είναι μηδενοδύναμο αφού $I^3=0$. Όμοια, αν $n=p_1^{n_1}...p_k^{n_k}$, όπου p_i διακεκριμένοι πρώτοι και $n_i>0$, τότε το ιδεώδες $I=([a])$, όπου $a=[p_1p_2...p_k]$, είναι μηδενοδύναμο καθώς $I^n=0$, όπου $n=\max\{n_1,...,n_k\}$.

4.2.1 Λήμμα. *Για κάθε $r\in J(R)$, το $1-r$ έχει αριστερό αντίστροφο.*

Απόδειξη: Αν το $1-r$ δεν έχει αριστερό αντίστροφο, τότε το κύριο ιδεώδες $(1-r)$ περιέχεται σε κάποιο μέγιστο ιδεώδες του R, $(1-r)\subseteq M$. Όμως $r\in J(R)\subseteq M$ και άρα $1=1-r+r\in M$, άτοπο.

4.2.2 Θεώρημα.
1) Το $J(R)$ περιέχει κάθε μηδενοδύναμο ιδεώδες του R.
2) Αν ο R είναι δακτύλιος του Artin, τότε το $J(R)$ είναι μηδενοδύναμο.

Απόδειξη: 1) Έστω μηδενοδύναμο ιδεώδες *I* που δεν περιέχεται σε κάποιο μέγιστο ιδεώδες *M*. Τότε $I+M=R$, και άρα υπάρχει $x\in M$, έτσι ώστε το $1-x$ είναι μηδενοδύναμο. Επομένως για κάποιο *n* ισχύει $(1-x)^n=0$ δηλαδή

$$1+\sum_{i=1}^{n}(-1)^i\binom{n}{i}x^i=0,$$

οπότε $1\in M$, άτοπο
2) Η ακολουθία

$$J(R)\supseteq J(R)^2\supseteq J(R)^3\supseteq ...$$

κάπου γίνεται σταθερή. Έστω ότι $J(R)^n=J(R)^{n+1}=...$. Θα δείξουμε ότι $J(R)^n=0$. Έστω $J(R)^n\neq 0$. Από την υπόθεση του Artin, το σύνολο των ιδεωδών *I* που έχουν τις ιδιότητες

$$I\subseteq J(R)^n \quad \text{και} \quad J(R)^n I\neq 0$$

(που είναι μη κενό γιατί περιέχει το $J(R)^n$) έχει ελάχιστο στοιχείο που το συμβολίζουμε πάλι με *I*. Τότε υπάρχει $x\in I$ με $J(R)^n x\neq 0$. Το ιδεώδες $J(R)^n x$ περιέχεται στο I και ικανοποιεί τις προηγούμενες ιδιότητες, οπότε λόγω του ελαχίστου έχουμε

$$J(R)^n x=I.$$

Συνεπώς υπάρχει $y\in J(R)^n$ με $yx=x$. Έτσι $(1-y)x=0$. Αλλά το $1-y$ έχει αριστερό αντίστροφο (Λήμμα 4.2.1) αφού $y\in J(R)^n\subseteq J(R)$. Τότε η σχέση $(1-y)x=0$ δίνει $x=0$, άτοπο.

Το προηγούμενο θεώρημα λέει ότι για δακτύλιο R του Artin, το $J(R)$ είναι το 'μεγαλύτερο' μηδενοδύναμο ιδεώδες του.

Παράδειγμα Έστω k σώμα και $T_n(k)$ ο δακτύλιος των $n\times n$ άνω τριγωνικών πινάκων με στοιχεία από το k. Θα βρούμε το $J(T_n(k))$.

Εύκολα επαληθεύεται ότι το σύνολο $I\subseteq T_n(k)$ των άνω τριγωνικών πινάκων με 0 στη διαγώνιο είναι αμφίπλευρο ιδεώδες του R. Ο δακτύλιος πηλίκο R/I είναι ισόμορφος με τον $k\times...\times k=k^n$ (γιατί;) που είναι ημιαπλός. Από την Πόρισμα 4.1.6, $J(T_n(k))\subseteq I$. Αφήνουμε ως άσκηση την επαλήθευση ότι $I^n=0$. Από το Θεώρημα 4.2.2, $J(T_n(k))\supseteq I$ και επομένως $J(T_n(k))=I$.

Από το Θεώρημα 4.1.2 έπεται ότι ο δακτύλιος $T_n(k)$ δεν είναι ημιαπλός αν $n>1$.

Ως άμεσο πόρισμα του Θεωρήματος 4.2.2 λαμβάνουμε ένα ακόμα χαρακτηρισμό ημιαπλών δακτυλίων.

4.2.3 Πόρισμα. *Ένας δακτύλιος είναι ημιαπλός αν και μόνο αν είναι δακτύλιος του Artin και δεν έχει μη τετριμμένα μηδενοδύναμα ιδεώδη.*

Δίνουμε τώρα την εφαρμογή που μνημονεύσαμε στην αρχή του κεφαλαίου.

4.2.4 Θεώρημα. *Κάθε δακτύλιος του Artin είναι και της Noether.*

Απόδειξη: Θα δείξουμε ότι ο R έχει συνθετική σειρά, οπότε θα είναι της Noether σύμφωνα με το Θεώρημα 3.2.3. Γνωρίζουμε ότι

i) το $J(R)$ είναι μηδενοδύναμο (Θεώρημα 4.2.2) και

ii) ο $R/J(R)$ είναι ημιαπλός (Πόρισμα 4.1.4).

Από το i) υπάρχει $n \in \mathbf{N}$ με

$$0 = J(R)^n \subseteq \ldots \subseteq J(R)^2 \subseteq J(R) \subseteq R \qquad (*)$$

Το R-πρότυπο $J(R)^i / J(R)^{i+1}$ γίνεται $R/J(R)$-πρότυπο με εξωτερικό πολλαπλασιασμό $r(x + J(R)^{i+1}) = rx + J(R)^{i+1}$ (γιατί;). Ο $R/J(R)$ είναι ημιαπλός και συνεπώς το $J(R)^i / J(R)^{i+1}$ είναι ευθύ άθροισμα απλών $R/J(R)$ – προτύπων. Ισχυριζόμαστε ότι αυτό το ευθύ άθροισμα έχει πεπερασμένο πλήθος προσθετέων. Προς τούτο αρκεί να δειχτεί ότι κάθε $J(R)^i / J(R)^{i+1}$ είναι $R/J(R)$ – πρότυπο του Artin, ή ισοδύναμα ότι είναι R-πρότυπο του Artin (γιατί τα R-υποπρότυπα του $J(R)^i / J(R)^{i+1}$ ταυτίζονται με τα $R/J(R)$ – υποπρότυπα του $J(R)^i / J(R)^{i+1}$). Αλλά R δακτύλιος του Artin $\Rightarrow$ $J(R)^i$ είναι R-πρότυπο του Artin (αφού είναι υποπρότυπο του R) και κατά συνέπεια το πηλίκο $J(R)^i / J(R)^{i+1}$ είναι R-πρότυπο του Artin (Πρόταση 3.1.4).

Από τον ισχυρισμό έπεται ότι κάθε $J(R)^i / J(R)^{i+1}$ έχει συνθετική σειρά ως $R/J(R)$-πρότυπο και άρα ως R-πρότυπο σύμφωνα με την Παρατήρηση 4.1.5 iii) παρακάτω. Παρεμβάλλοντας τότε όρους στην (*), εύκολα βλέπουμε ότι το R έχει συνθετική σειρά και συνεπώς το R είναι R-πρότυπο της Noether.

4.2.5 Παρατήρηση Έστω $\varphi : R \to S$ ομομορφισμός δακτυλίων και M S-πρότυπο.

i) Το M είναι R-πρότυπο με εξωτερικό πολλαπλασιασμό που ορίζεται από $r \cdot m = \varphi(r)m,\ r \in R,\ m \in M$

ii) Αν ο φ είναι επιμορφισμός και το M απλό S-πρότυπο, τότε το M είναι απλό R-πρότυπο.

Πράγματι, αν $m \in M, m \neq 0,$ τότε $\{r \cdot m \mid r \in R\} = \{\varphi(r)m \mid r \in R\} = \{sm \mid s \in S\} = M$.

iii) Αν ο φ είναι επιμορφισμός και το M έχει συνθετική σειρά ως S-πρότυπο, τότε έχει συνθετική σειρά ως R-πρότυπο.

Αυτό έπεται άμεσα από τα προηγούμενα.

Ασκήσεις

1. Βρείτε το $J(R)$ στις ακόλουθες περιπτώσεις.

i) $R=\mathbb{Q}[x]$.

ii) $R=\mathbb{Q}[x]/(x^2)$.

iii) $R=\mathbb{Q}[x]/(x^2(x^2-2))$.

iv) $R=\left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a,b,d\in S\right\}$, όπου S είναι δακτύλιος.

2. Κάθε δακτύλιος του Artin που δεν έχει μη μηδενικά μηδενοδύναμα στοιχεία είναι ισόμορφος με ευθύ γινόμενο δακτυλίων διαίρεσης.

3. Ένας δακτύλιος είναι δακτύλιος διαίρεσης αν και μόνο αν είναι του Artin και $xy\neq 0$ για κάθε $x,y\neq 0$.

4. Κάθε μεταθετικός δακτύλιος του Artin έχει πεπερασμένο πλήθος μεγίστων ιδεωδών. Δώστε ένα παράδειγμα δακτυλίου του Artin που έχει άπειρο πλήθος μεγίστων ιδεωδών.

5. Αν ο R είναι μεταθετκός δακτύλιος του Artin, τότε

i) ο $R/J(R)$ είναι ευθύ γινόμενο σωμάτων,

ii) $J(R)=\{r\in R \mid r^n=0, \textit{κάποιο } n\in\mathbb{N}\}$

6. Έστω k σώμα χαρακτηριστικής p και $R=k[x]/(x^n-1)$.

i) Για ποια p,n ο R είναι ημιαπλός;

ii) Ποιο είναι το $J(R)$;

7. Έστω R δακτύλιος του Artin και M R-πρότυπο. Το M είναι ημιαπλό αν και μόνο αν $J(R)M=0$.

8. Αν R δακτύλιος, τότε $J(M_n(R))=M_n(J(R))$. Ποιο είναι το $J(R)$ αν $R=M_2(\mathbb{Z})\times M_2(\mathbb{Z}_8)$;

9. Δείξτε ότι $J(R)=\{r\in R \mid \forall a\in R, \exists b\in R, b(1-ar)=1\}$.

10. Έστω k σώμα και $T_n(k)$ ο δακτύλιος των $n\times n$ άνω τριγωνικών πινάκων με στοιχεία από το k. Στο Παράδειγμα μετά το Θεώρημα 4.2.2 προσδιορίσαμε το $J(T_n(k))$.

i) Ποιος είναι ο ημιαπλός δακτύλιος $T_n(k)/J(T_n(k))$; Με τη βοήθεια αυτού δείξτε ότι το πλήθος των ανά δύο μη ισόμορφων απλών $T_n(k)$-προτύπων είναι ίσο με n και καθένα από αυτά έχει διάσταση 1.

ii) Βρείτε μια συνθετική σειρά του $V=M_{n\times 1}(k)$ ως $T_n(k)$-πρότυπο.

11. Έστω k σώμα και $L_n(k)$ ο δακτύλιος των $n\times n$ άνω τριγωνικών πινάκων (a_{ij}) με στοιχεία από το k τέτοιων ώστε $a_{11}=a_{22}=...=a_{nn}$. Δείξτε τα εξής.

i) $J(L_n(k))=\{(a_{ij})\in L_n(k) \mid a_{11}=a_{22}=...=a_{nn}=0\}$.

ii) Κάθε δύο απλά $L_n(k)$-πρότυπα είναι ισόμορφα.

ΚΕΦΑΛΑΙΟ 5: Τανυστικά Γινόμενα

Στο κεφάλαιο αυτό εισάγουμε την έννοια του τανυστικού γινομένου προτύπων. Θα περιοριστούμε στις προτάσεις που θα βρουν εφαρμογές σε παρακάτω κεφάλαια.

5.1. Ορισμοί

Έστω R ένας δακτύλιος. Για να δηλώσουμε ότι το M είναι ένα αριστερό R-πρότυπο, θα χρησιμοποιούμε το συμβολισμό ${}_R M$. Ανάλογα, ο συμβολισμός M_R σημαίνει ότι το M είναι δεξιό R-πρότυπο.

Έστω M_R, ${}_R N$ δύο R-πρότυπα. Μια απεικόνιση

$$f : M \times N \to G,$$

όπου G είναι αβελιανή ομάδα, λέγεται ***R*-διπροσθετική** αν

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

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

(iii) $f(mr,n) = f(m,rn)$

για κάθε $m,m' \in M$, $n,n' \in N$ και $r \in R$.

5.1.1 Ορισμός. *Έστω R ένας δακτύλιος και* M_R, ${}_R N$ *δύο πρότυπα.* ***Τανυστικό γινόμενο*** *των* M_R, ${}_R N$ *είναι ένα* $\mathbb{Z}$*-πρότυπο G και μια R-διπροσθετική απεικόνιση* $f : M \times N \to G$ *που έχει την ιδιότητα: για κάθε* $\mathbb{Z}$*-πρότυπο* G' *και κάθε R-διπροσθετική απεικόνιση* $f' : M \times N \to G'$

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "f'"'] & G \arrow[dl, dotted, "h"] \\ G' & \end{tikzcd}$$

υπάρχει μοναδικός ομομορφισμός $\mathbb{Z}$*-πρότυπων* $h : G \to G'$ *που καθιστά το διάγραμμα μεταθετικό (δηλαδή* $hf = f'$*).*

5.1.2 Πρόταση *(Μοναδικότητα). Έστω* M_R, ${}_R N$ *δύο R-πρότυπα. Αν* $f : M \times N \to G$ *και* $f' : M \times N \to G'$ *είναι δύο τανυστικά γινόμενα των M και N, τότε* $G \simeq G'$.

Απόδειξη: Από τα διαγράμματα

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "f'"'] & G \arrow[dl, dashed, "h"] \\ G' & \end{tikzcd} \qquad \begin{tikzcd} M \times N \arrow[r, "f'"] \arrow[d, "f"'] & G' \arrow[dl, dashed, "h'"] \\ G & \end{tikzcd}$$

συμπεραίνουμε ότι υπάρχουν ομομορφισμοί h, h' με τις ιδιότητες $hf = f'$ και $h'f' = f$ αντίστοιχα. Άρα $f' = (hh')f'$. Συγκρίνοντας τώρα τα μεταθετικά διαγράμματα

$$\begin{tikzcd} M \times N \arrow[r, "f'"] \arrow[d, "f'"'] & G' \arrow[dl, dashed, "hh'"] \\ G' & \end{tikzcd} \qquad \begin{tikzcd} M \times N \arrow[r, "f'"] \arrow[d, "f'"'] & G' \arrow[dl, dashed, "1_{G'}"] \\ G' & \end{tikzcd}$$

η μοναδικότητα στον Ορισμό 5.1.1 δίνει $hh' = 1_{G'}$. Με ανάλογο τρόπο παίρνουμε $h'h = 1_G$. Άρα ο h είναι ισομορφισμός.

***5.1.3 Πρόταση** (Υπαρξη)**.** Έστω M_R και ${}_RN$ δύο R-πρότυπα. Τότε υπάρχει τανυστικό γινόμενό τους.*

Απόδειξη: Έστω F το ελεύθερο $\mathbb{Z}$-πρότυπο $\bigoplus_{\lambda\in M\times N}\mathbb{Z}_\lambda$, όπου για κάθε λ ισχύει $\mathbb{Z}_\lambda=\mathbb{Z}$. Έστω $\{e_\lambda\}_{\lambda\in M\times N}$ βάση του F. Με F' συμβολίζουμε το υποπρότυπο του F που παράγεται από τα στοιχεία

$$e_{(m+m',n)}-e_{(m,n)}-e_{(m',n)}$$
$$e_{(m,n+n')}-e_{(m,n)}-e_{(m,n')}$$
$$e_{(mr,n)}-e_{(m,rn)}$$

για όλες τις επιλογές των $m,m'\in M$, $n,n'\in N$ και $r\in R$.

Θέτουμε $M\underset{R}{\otimes}N=F/F'$ και συμβολίζουμε το στοιχείο $e_{(m,n)}+F'$ του F/F' με $m\otimes n$. Η απεικόνιση

$$f: M\times N\ni(m,n)\mapsto m\otimes n\in M\underset{R}{\otimes}N$$

είναι R-διπροσθετική. Θα δείξουμε ότι ικανοποιεί τη συνθήκη του Ορισμού 5.1.1. Έστω $f': M\times N\to G'$ R-διπροσθετική απεικόνιση. Έστω $f'': F\to G'$ η $\mathbb{Z}$-γραμμική επέκταση της f' (δηλαδή ο ομομορφισμός $\mathbb{Z}$-προτύπων που ορίζεται από $f''(e_{(m,n)})=f'(m,n)$). Επειδή η f' είναι R-διπροσθετική ισχύει $f''(F')=0$. Επομένως η f'' επάγει μια απεικόνιση

$$h: F/F'\to G',$$

όπου $h(m\otimes n)=f'(m,n)$ για κάθε $m\in M$, $n\in N$. Ισχύει βέβαια $hf=f'$.

Το ότι ο ομομορφισμός h είναι μοναδικός ως προς την ιδιότητα $hf=f'$ συνάγεται από το γεγονός ότι τα στοιχεία $f(m,n)$, όπου $m\in M$, $n\in N$, παράγουν το $\mathbb{Z}$-πρότυπο F/F'.

5.1.4 Παρατήρηση.

i) Ως $\mathbb{Z}$-πρότυπο, το $M\underset{R}{\otimes}N$ παράγεται από τα στοιχεία $m\otimes n$, όπου $m\in M$, $n\in N$. Δηλαδή κάθε στοιχείο του $M\underset{R}{\otimes}N$ είναι της μορφής $r_1\left(m_1\otimes n_1\right)+\dots+r_k\left(m_k\otimes n_k\right)$ όπου $k\geq 1, r_i\in\mathbb{Z}, m_i\in M, n_i\in N$. Γενικά δεν αληθεύει ότι κάθε στοιχείο του $M\underset{R}{\otimes}N$ είναι της μορφής $m\otimes n$.

ii) Από την απόδειξη της πρότασης 5.1.3 είναι σαφές ότι στο $M\underset{R}{\otimes}N$ ισχύουν οι σχέσεις[1]

$$\boxed{\begin{aligned}(m+m')\otimes n&=m\otimes n+m'\otimes n\\ m\otimes(n+n')&=m\otimes n+m\otimes n'\\ mr\otimes n&=m\otimes rn\end{aligned}}$$

για κάθε $m,n'\in M$, $n,n'\in N$ και $r\in R$. Από αυτές προκύπτουν οι σχέσεις (άσκηση)

$$\boxed{\begin{aligned}&m\otimes 0_N=0_M\otimes n=0_{M\underset{R}{\otimes}N},\\ &(-m)\otimes n=m\otimes(-n)=-\left(m\otimes n\right)\end{aligned}}$$

για κάθε $m\in M, n\in N$.

iii) Είναι δυνατόν να ισχύει $m\otimes n=0$ με $m\neq 0$, $n\neq 0$, ή ακόμα να ισχύει $M\underset{R}{\otimes}N=0$ με $M\neq 0$ και $N\neq 0$. Για παράδειγμα έστω $M=\mathbb{Z}_m$ και $N=\mathbb{Z}_n$ με μ.κ.δ $(m,n)=1$. Θα δείξουμε ότι $\mathbb{Z}_m\underset{\mathbb{Z}}{\otimes}\mathbb{Z}_n=0$. Πράγματι, υπάρχουν $x,y\in\mathbb{Z}$ με την ιδιότητα $1=mx+yn$. Έτσι για κάθε $a\in\mathbb{Z}_m$ και $b\in\mathbb{Z}_n$

[1] Σε πράξεις με τανυσικά γινόμενα μπορούμε να χρησιμοποιούμε τις σχέσεις αυτές 'αγνοώντας' την κατασκευή της Πρότασης 5.1.3.

$$
\begin{aligned}
&a\otimes b=\\
&a1\otimes b=\\
&(amx+ayn)\otimes b=\\
&amx\otimes b+ayn\otimes b=\\
&amx\otimes b+ay\otimes nb=\\
&0\otimes b+ay\otimes 0=\\
&0.
\end{aligned}
$$

Επειδή τα $a\otimes b$, όπου $a,b\in\mathbb{Z}$, παράγουν το $\mathbb{Z}_m\underset{\mathbb{Z}}{\otimes}\mathbb{Z}_n$, παίρνουμε $\mathbb{Z}_m\underset{\mathbb{Z}}{\otimes}\mathbb{Z}_n=0$.

5.2 Ιδιότητες

Το τανυστικό γινόμενο $M\underset{R}{\otimes}N$ (όταν ορίζεται) είναι $\mathbb{Z}$-πρότυπο. Θα δούμε τώρα συνθήκες κάτω από τις οποίες καθίσταται πιο γενικό πρότυπο.

Έστω R, S δυο δακτύλιοι. Έστω M ένα $\mathbb{Z}$-πρότυπο που είναι ταυτόχρονα αριστερό S-πρότυπο και δεξιό R-πρότυπο. Το M ονομάζεται (S,R) **-διπρότυπο** αν ισχύει $(sm)r=s(mr)$ για κάθε $s\in S$, $m\in M$ και $r\in R$. Τότε θα συμβολίζουμε το M με ${}_SM_R$.

5.2.1 Πρόταση. *Έστω R, S δυο δακτύλιοι. Ισχύουν τα εξής.*
i) Για πρότυπα ${}_SM_R$ και ${}_RN$ το $M\underset{R}{\otimes}N$ είναι αριστερό S-πρότυπο με εξωτερικό πολλαπλασιασμό που ορίζεται από $s(m\otimes n)=sm\otimes n$.
ii) Για πρότυπα M_R και ${}_RN_S$ το $M\underset{R}{\otimes}N$ είναι δεξιό S-πρότυπο με εξωτερικό πολλαπλασιασμό που ορίζεται από $(m\otimes n)s=m\otimes ns$.

Απόδειξη: i) Για σταθερό s, η απεικόνιση

$$M\times N\ni(m,n)\mapsto sm\otimes n\in M\underset{R}{\otimes}N$$

είναι R-διπροσθετική. Επομένως (Ορισμός 5.1.1) επάγει έναν ομομορφισμό ομάδων

$$M\underset{R}{\otimes}N\ni m\otimes n\mapsto sm\otimes n\in M\underset{R}{\otimes}N.$$

Ορίζεται έτσι μια απεικόνιση

$$S\times M\underset{R}{\otimes}N\to M\underset{R}{\otimes}N,\ (s,m\otimes n)\mapsto sm\otimes n$$

που εύκολα ελέγχουμε ότι καθιστά την αβελιανή ομάδα $M\underset{R}{\otimes}N$ S-πρότυπο. Η απόδειξη του ii) είναι παρόμοια.

Σημείωση Έστω ότι ο δακτύλιος R είναι μεταθετικός. Τότε κάθε αριστερό πρότυπο M καθίσταται δεξιό πρότυπο με εξωτερικό πολλαπλασιασμό που ορίζεται από $m\cdot r=rm$, όπου $m\in M, r\in R,$ και επομένως το M είναι ένα (R,R)- διπρότυπο. Έτσι το $M\underset{R}{\otimes}N$ ορίζεται και είναι ένα R-πρότυπο.

5.2.2 Πρόταση. *Για κάθε δεξιό R-πρότυπο M υπάρχει ισομορφισμός δεξιών R-προτύπων $M\underset{R}{\otimes}R\simeq M$, και για κάθε αριστερό R-πρότυπο N υπάρχει ισομορφισμός αριστερών R-προτύπων $R\underset{R}{\otimes}N\simeq N$.*

Απόδειξη: Το R είναι (R,R)-διπρότυπο και συνεπώς (Πρόταση 5.2.1) το $M\underset{R}{\otimes}R$ είναι δεξιό R-πρότυπο. Επειδή η απεικόνιση

$$M \times R \to M, \quad (m,r) \mapsto mr$$

είναι R-διπροσθετική, λαμβάνουμε έναν ομομορφισμό ομάδων (Ορισμός 5.1.1)

$$\varphi : M \underset{R}{\otimes} R \to M, \quad m \otimes r \mapsto mr.$$

O φ είναι ομομορφισμός (δεξιών) R-προτύπων. Ορίζοντας τον ομομορφισμό R-προτύπων

$$\psi : M \to M \underset{R}{\otimes} R, \quad m \mapsto m \otimes 1$$

εύκολα επαληθεύουμε ότι $\varphi \circ \psi = 1_M$ και $\psi \circ \varphi = 1_{M \otimes R}$, και άρα ο φ είναι ισομορφισμός. Ο άλλος ισομορφισμός της πρότασης αποδεικνύεται με παρόμοιο τρόπο.

Παράδειγμα Σύμφωνα με την προηγούμενη πρόταση έχουμε $\mathbb{Z} \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \simeq \mathbb{Q} \simeq \mathbb{Q} \underset{\mathbb{Q}}{\otimes} \mathbb{Q}$.

5.2.3 Πρόταση. *i) Έστω πρότυπα M_R, N_R και ${}_R L$. Τότε υπάρχει ισομορφισμός $\mathbb{Z}$-προτύπων*

$$(M \oplus N) \underset{R}{\otimes} L \simeq M \underset{R}{\otimes} L \oplus N \underset{R}{\otimes} L.$$

Ειδικά,

- *αν έχουμε την κατάσταση ${}_S M_R$, ${}_S N_R$ και ${}_R L$, τότε ο παραπάνω ισομορφισμός είναι ισομορφισμός αριστερών S-προτύπων και*
- *αν έχουμε την κατάσταση M_R, N_R και ${}_R L_S$, τότε ο παραπάνω ισομορφισμός είναι ισομορφισμός δεξιών S-προτύπων.*

ii) Έστω ${}_R M$, ${}_R N$ και L_R. Τότε υπάρχει ισομορφισμός $\mathbb{Z}$-προτύπων

$$L \underset{R}{\otimes} (M \oplus N) \simeq L \underset{R}{\otimes} M \oplus L \underset{R}{\otimes} N.$$

Ειδικά,

- *αν έχουμε την κατάσταση ${}_R M$, ${}_R N$ και ${}_S L_R$, τότε ο παραπάνω ισομορφισμός είναι ισομορφισμός αριστερών S-προτύπων και*
- *αν έχουμε την κατάσταση ${}_R M_S$, ${}_R N_S$ και L_R, τότε ο παραπάνω ισομορφισμός είναι ισομορφισμός δεξιών S-προτύπων και*

Απόδειξη: i) Η απεικόνιση

$$(M \oplus N) \times L \to M \underset{R}{\otimes} L \oplus N \underset{R}{\otimes} L$$

$$((m,n),l) \mapsto (m \otimes l, \ n \otimes l)$$

είναι R-διπροσθετική και άρα υπάρχει καλά ορισμένος ομομορφισμός $\mathbb{Z}$-προτύπων (Ορισμός 5.1.1)

$$f : (M \oplus N) \underset{R}{\otimes} L \to M \underset{R}{\otimes} L \oplus N \underset{R}{\otimes} L$$

$$(m,n) \otimes l \mapsto (m \otimes l, \, n \otimes l).$$

Στην αντίθετη κατεύθυνση, οι R-διπροσθετικές απεικονίσεις

$$M \times L \ni (m,l) \mapsto (m,0) \otimes l \in (M \oplus N) \underset{R}{\otimes} L$$

$$N \times L \ni (n,l) \mapsto (0,n) \otimes l \in (M \oplus N) \underset{R}{\otimes} L$$

δίνουν καλά ορισμένους ομομορφισμούς $\mathbb{Z}$-προτύπων

$$g_M : M \otimes L \to (M \oplus N) \underset{R}{\otimes} L$$

$$g_N : N \otimes L \to (M \oplus N) \underset{R}{\otimes} L.$$

Ορίζουμε τον ομομορφισμό $\mathbb{Z}$-προτύπων

$$g: M\underset{R}{\otimes}L\oplus N\underset{R}{\otimes}L\to(M\oplus N)\underset{R}{\otimes}L$$
$$(m\otimes l, n\otimes l')\mapsto g_M(m\otimes l)+g_N(n\otimes l')$$

και επαληθεύουμε (άσκηση) ότι οι fg και gf είναι οι αντίστοιχες ταυτοτικές συναρτήσεις.
Είναι σαφές ότι ισχύουν οι ειδικές περιπτώσεις της εκφώνησης.
ii) Παρόμοια.

Ως άσκηση στους συμβολισμούς (!) αφήνουμε την απόδειξη της ιδιότητα $\left(\underset{i}{\oplus}M_i\right)\underset{R}{\otimes}L\simeq\underset{i}{\oplus}\left(M_i\underset{R}{\otimes}L\right)$.

Όμως προσοχή: δεν ισχύει γενικά $\left(\prod\limits_i M_i\right)\underset{R}{\otimes}L\simeq\prod\limits_i\left(M_i\underset{R}{\otimes}L\right)$. Βλ. άσκηση 1.

5.2.4 Πόρισμα. *Έστω k σώμα και πεπερασμένης διάστασης k-διανυσματικοί χώροι V και W με αντίστοιχες βάσεις $\{v_1,...,v_m\}$ και $\{w_1,...,w_n\}$. Τότε μία βάση του k-διανυσματικού χώρου $V\underset{k}{\otimes}W$ είναι το* $\{v_1\otimes w_1,...,v_m\otimes w_n\}$.

Απόδειξη: Επειδή τα στοιχεία $v_i\otimes w_j$ παράγουν το $V\underset{k}{\otimes}W$, αρκεί να δείξουμε ότι $\dim_k(V\underset{k}{\otimes}W)=mn$.
Έχουμε ισομορφισμό διανυσματικών χώρων $V\simeq k^m$ και επομένως

$$V\otimes W\simeq k^m\underset{k}{\otimes}W\simeq\left(k\underset{k}{\otimes}W\right)\oplus\left(k\underset{k}{\otimes}W\right)\oplus...\oplus\left(k\underset{k}{\otimes}W\right)\simeq W\oplus W\oplus...\oplus W$$

λόγω των Προτάσεων 5.2.3 και 5.2.2. Άρα $\dim_k(V\underset{k}{\otimes}W)=m\dim_k W$.

Σημείωση Χρειάζεται προσοχή στο δακτύλιο R του τανυστικού γινομένου '$\underset{R}{\otimes}$'. Για παράδειγμα, ενώ $\dim_{\mathbb{R}}(\mathbb{C}\underset{\mathbb{C}}{\otimes}\mathbb{C})=2$, έχουμε $\dim_{\mathbb{R}}(\mathbb{C}\underset{\mathbb{R}}{\otimes}\mathbb{C})=4$.

5.2.5 Παραδείγματα

1. Έστω G μια πεπερασμένα παραγόμενη αβελιανή ομάδα. Τότε η G είναι πεπερασμένη αν και μόνο αν $G\underset{\mathbb{Z}}{\otimes}\mathbb{Q}=0$.

   Πράγματι, αν η G είναι πεπερασμένη τάξης n, τότε για κάθε $g\in G, a\in\mathbb{Z}, b\in\mathbb{Z}, b\neq 0$ έχουμε

   $$g\otimes\frac{a}{b}=g\otimes\frac{na}{nb}=ng\otimes\frac{a}{nb}=0_G\otimes\frac{a}{nb}=0$$

   και άρα $G\underset{\mathbb{Z}}{\otimes}\mathbb{Q}=0$.

   Αντίστροφα, έστω ότι $G\underset{\mathbb{Z}}{\otimes}\mathbb{Q}=0$. Επειδή η G είναι πεπερασμένα παραγόμενη αβελιανή ομάδα, έχουμε

   $$G\simeq H\oplus\mathbb{Z}^m,$$

   όπου H πεπερασμένη υποομάδα της G και $m\geq 0$ (σύμφωνα με το θεώρημα ταξινόμησης των πεπερασμένα παραγόμενων αβελιανών ομάδων). Τώρα από την Πρόταση 5.2.3 έχουμε

   $$G\underset{\mathbb{Z}}{\otimes}\mathbb{Q}\simeq\left(H\underset{\mathbb{Z}}{\otimes}\mathbb{Q}\right)\oplus\left(\mathbb{Z}^m\underset{\mathbb{Z}}{\otimes}\mathbb{Q}\right)$$

   και με τη βοήθεια της Πρότασης 5.2.2 έχουμε

$$0=\mathbb{Z}^m \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \simeq \left(\mathbb{Z} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}\right) \oplus \ldots \oplus \left(\mathbb{Z} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}\right) \simeq \mathbb{Q} \oplus \ldots \oplus \mathbb{Q}.$$

Άρα $m=0$. Τότε $G=H$ που είναι πεπερασμένη.

2. Έστω R ένας μεταθετικός δακτύλιος και I, J ιδεώδη του R. Τότε υπάρχει ισομορφισμός R-προτύπων $(R/I) \underset{R}{\otimes} (R/J) \simeq R/(I+J)$.

   Πράγματι, η απεικόνιση
   $$f:(R/I)\times(R/J)\to R/(I+J),\ (r+I, r'+J)\mapsto rr'+I+J,$$
   είναι διπροσθετική και άρα υπάρχει καλά ορισμένος ομομορφισμός αβελιανών ομάδων
   $$\Phi:(R/I)\underset{R}{\otimes}(R/J)\to R/(I+J),\ (r+I)\otimes(r'+J)\mapsto rr'+I+J.$$
   Εύκολα επαληθεύεται ότι ο Φ είναι ομομορφισμός R-προτύπων.

   Στην αντίθετη κατεύθυνση, παρατηρούμε ότι ο ομομορφιαμός R-προτύπων
   $$g:R\to(R/I)\underset{R}{\otimes}(R/J),\ r\mapsto(r+I)\otimes(1+J),$$
   έχει την ιδιότητα $I+J\subseteq\ker g$. Συνεπώς επάγεται ένας ομομορφισμός R-προτύπων
   $$\Psi:R/(I+J)\to(R/I)\underset{R}{\otimes}(R/J),\ r+I+J\mapsto(r+I)\otimes(1+J).$$
   Εύκολα επαληθεύεται ότι οι συνθέσεις $\Phi\Psi$, $\Psi\Phi$ είναι οι αντίστοιχες ταυτοτικές συναρτήσεις και άρα ο Φ είναι ισομορφισμός.

3. Έχουμε $\mathbb{Z}_m \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_n \cong \mathbb{Z}_d$, όπου $d=\text{μκδ}(m,n)$.

   Αυτό προκύπτει άμεσα από το προηγούμενο παράδειγμα για $R=\mathbb{Z}, I=(m), J=(n)$.

Έστω R μεταθετικός δακτύλιος. Αν A και B είναι δύο R-άλγεβρες, τότε το τανυστικό γινόμενο $A\underset{R}{\otimes}B$ καθίσταται R-άλγεβρα με πολλαπλασιασμό που ορίζεται από $(a\otimes b)(a'\otimes b')=aa'\otimes bb'$, όπου $a,a'\in A$ και $b,b'\in B$ (γιατί είναι καλά ορισμένος;).

Ασκήσεις

1. Έστω p πρώτος αριθμός. Οι αβελιανές ομάδες $\left(\prod_i \mathbb{Z}_{p^i}\right)\underset{\mathbb{Z}}{\otimes}\mathbb{Q}$ και $\prod_i\left(\mathbb{Z}_{p^i}\underset{\mathbb{Z}}{\otimes}\mathbb{Q}\right)$ δεν είναι ισόμορφες.

2. i) Ποιο είναι το $\dfrac{\mathbb{Q}}{\mathbb{Z}}\underset{\mathbb{Z}}{\otimes}\mathbb{Q}$;

ii) Έστω R ένας μεταθετικός δακτύλιος, I ένα ιδεώδες του R και M ένα R- πρότυπο. Τότε υπάρχει ισομορφισμός R-προτύπων $\dfrac{R}{I}\underset{R}{\otimes}M\simeq\dfrac{M}{IM}$. Με βάση αυτό δώστε μια νέα απόδειξη του Παραδ. 5.2.5 3.

3. Έστω R ένας δακτύλιος.

i) Το τανυστικό γινόμενο δυο ελεύθερων R-προτύπων είναι ελεύθερο.

ii) Αν ο R είναι μεταθετικός, τότε το τανυστικό γινόμενο δυο προβολικών R-προτύπων είναι προβολικό.

4. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.

i) Η $\mathbb{R}$-άλγεβρα $\mathbb{C}\underset{\mathbb{R}}{\otimes}\mathbb{C}$ είναι δακτύλιος διαίρεσης.

ii) Η $\mathbb{Z}$-άλγεβρα $\mathbb{Q}\underset{\mathbb{Z}}{\otimes}\mathbb{Q}$ είναι δακτύλιος διαίρεσης.

iii) Οι δακτύλιοι $\mathbb{C}\underset{\mathbb{R}}{\otimes}\mathbb{C}$ και $\mathbb{C}\times\mathbb{C}$ είναι ισόμορφοι.

5. Για κάθε πρώτο p οι $\mathbb{Z}_p$-άλγεβρες $\mathbb{Z}_p\underset{\mathbb{Z}}{\otimes}M_n(\mathbb{Z})$ και $M_n(\mathbb{Z}_p)$ είναι ισόμορφες. Ποιο γενικά, αν S είναι R-άλγεβρα, όπου R-μεταθετικός δακτύλιος, τότε οι R-άλγεβρες $S\underset{R}{\otimes}M_n(R)$ και $M_n(S)$ είναι ισόμορφες.

6. Έστω A, B δυο k-άλγεβρες.

i) Αν I και J είναι αμφίπλευρα ιδεώδη των A, B αντίστοιχα, τότε το $I\underset{k}{\otimes}J$ είναι αμφίπλευρο ιδεώδες της άλγεβρας $A\underset{k}{\otimes}B$.

ii) Έστω ότι $\dim_k A<\infty$ και $\dim_k B<\infty$. Αν η A δεν είναι ημιαπλή, τότε η $A\underset{k}{\otimes}B$ δεν είναι απλή.

Υπόδειξη: Θεώρημα 4.1.4.

7. Έστω k ένα σώμα και V, W δύο πεπερασμένης διάστασης k-διανυσματικοί χώροι.

i) Δείξτε ότι οι k-άλγεβρες $End_k(V)\underset{k}{\otimes}End_k(W)$ και $End_k(V\underset{k}{\otimes}W)$ είναι ισόμορφες. Άρα οι k-άλγεβρες $M_m(k)\underset{k}{\otimes}M_n(k)$ και $M_{mn}(k)$ είναι ισόμορφες.

ii) Δώστε μια άλλη απόδειξη του ισομορφισμού k-αλγεβρών $M_m(k)\underset{k}{\otimes}M_n(k)\simeq M_{mn}(k)$ με βάση την άσκηση 5 πιο πάνω.

8. Έστω k ένα αλγεβρικά κλειστό σώμα. Τότε το τανυστικό γινόμενο $A\underset{k}{\otimes}B$ δύο απλών k-αλγεβρών του Artin A, B είναι απλή k-άλγεβρα του Artin.

Υπόδειξη: Προηγούμενη άσκηση, Θεώρημα Wedderburn-Artin και Πρόταση 2.3.7.

9. i) Έστω G, H δυο πεπερασμένες ομάδες και k σώμα. Τότε υπάρχει ισομορφισμός k-αλγεβρών $k[G\times H]\simeq k[G]\underset{k}{\otimes}k[H]$.

ii) Έστω G μια πεπερασμένη αβελιανή ομάδα τάξης m. Ποιο είναι το πλήθος των ανά δύο μη ισόμορφων απλών $\mathbb{C}[G\times S_3]$-προτύπων, όπου S_3 είναι η ομάδα μεταθέσεων 3 συμβόλων; Πόσα από αυτά έχουν διάσταση 1;

10. Έστω G πεπερασμένη αβελιανή ομάδα τάξης n και p^k η μέγιστη δύναμη του πρώτου p που διαιρεί το n. Δείξτε ότι η αβελιανή ομάδα $\mathbb{Z}_{p^k}\underset{\mathbb{Z}}{\otimes}G$ είναι ισόμορφη με την p-Sylow υποομάδα της G.

11. Δείξτε ότι στο $\mathbb{Z}\underset{\mathbb{Z}}{\otimes}\mathbb{Z}_2$ ισχύει $2\otimes 1=0$ ενώ στο $2\mathbb{Z}\underset{\mathbb{Z}}{\otimes}\mathbb{Z}_2$ ισχύει $2\otimes 1\neq 0$.

12. Δείξτε ότι $\mathbb{Q}/\mathbb{Z}\underset{\mathbb{Z}}{\otimes}\mathbb{Q}/\mathbb{Z}=0$ και $\mathbb{Q}\underset{\mathbb{Z}}{\otimes}\mathbb{Q}\neq 0$. Αληθεύει ότι οι $\mathbb{Q}$-διανυσματικοί χώροι $\mathbb{Q}\underset{\mathbb{Z}}{\otimes}\mathbb{Q}$ και $\mathbb{Q}\underset{\mathbb{Q}}{\otimes}\mathbb{Q}$ είναι ισόμορφοι;

13. Δείξτε ότι $\mathbb{Z}[i]\underset{\mathbb{Z}}{\otimes}\mathbb{R}\simeq\mathbb{C}$ (ισομορφισμός δακτυλίων).

14. Έστω A, B, C R-πρότυπα, όπου R μεταθετικός. Δείξτε ότι υπάρχει ισομορφισμός R-προτύπων $Hom_R(A\underset{R}{\otimes}B, C)\simeq Hom_R(A, Hom_R(B, C))$.

15. Έστω R μεταθετικός δακτύλιος. Για τους δακτύλιους πολυωνύμων $R[x], R[y], R[x,y]$ δείξτε ότι $R[x]\underset{R}{\otimes}R[y]\simeq R[x,y]$.

ΚΕΦΑΛΑΙΟ 6: Κεντρικές Απλές Άλγεβρες

Χρησιμοποιώντας τανυστικά γινόμενα και εφαρμόζοντας το θεώρημα των Wedderburn-Artin (§ 3.3) θα αποδείξουμε δύο θεμελιώδη θεωρήματα που αφορούν κεντρικές απλές άλγεβρες

* θεώρημα Skolem-Noether
* θεώρημα του διπλού κεντροποιητή.

Αμέσως μετά θα εφαρμόσουμε τα αποτελέσματα αυτά για να πάρουμε άλλα δύο φημισμένα θεωρήματα: την ταξινόμηση των πραγματικών αλγεβρών διαίρεσης που έχουν πεπερασμένη διάσταση (Frobenius), και το γεγονός ότι κάθε πεπερασμένος δακτύλιος διαίρεσης είναι μεταθετικός (Wedderburn).

6.1 Θεώρημα των Skolem-Noether

Έστω k ένα σώμα και R μια k-άλγεβρα. Το **κέντρο** της R είναι $C(R)=\{x\in R \mid rx=xr\ \forall r\in R\}$. Είναι μια μεταθετική υποάλγεβρα της R που περιέχει το k. Η άλγεβρα R λέγεται **κεντρική** αν $C(R)=k$ δηλαδή αν το κέντρο είναι το μικρότερο δυνατό. Υπενθυμίζουμε ότι μια άλγεβρα λέγεται απλή αν δεν έχει γνήσια μη τετριμμένα αμφίπλευρα ιδεώδη.

Παραδείγματα

1. Η $M_n(k)$ είναι κεντρική k-άλγεβρα αφού το κέντρο της είναι $C\left(M_n(k)\right)=\left\{aI \middle| a\in k\right\}$. Η $M_n(k)$ είναι απλή. Η k-άλγεβρα $M_n(k)\times M_n(k)$ δεν είναι κεντρική, αφού το κέντρο της είναι $\left\{(aI,bI) \middle| a,b\in k\right\}\neq\left\{(aI,aI) \middle| a\in k\right\}$.
2. Η άλγεβρα των quaternions $\mathbb{H}$ (Παράδειγμα 1.1.5) είναι κεντρική απλή $\mathbb{R}$-άλγεβρα.
3. Η $\mathbb{C}$ ως $\mathbb{R}$-άλγεβρα είναι απλή αλλά όχι κεντρική ενώ ως $\mathbb{C}$-άλγεβρα είναι απλή και κεντρική.
4. Η πολυωνυμική άλγεβρα $k[x]$ δεν είναι ούτε κεντρική ούτε απλή.

Έστω R μια k-άλγεβρα. Υπενθυμίζουμε ότι μια υποάλγεβρα A του R είναι ένας υποδακτύλιος του R (και άρα περιέχει το 1_R σύμφωνα με τις παραδοχές μας) που είναι και k-υπόχωρος του R. Επίσης, ένας ομομορφισμός k-αλγεβρών είναι ομομορφισμός δακτυλίων που είναι και ομομορφισμός k-διανυσματικών χώρων. Ένας ομομορφισμός k-αλγεβρών $R\to R$ που είναι 1-1 και επί θα λέγεται k-**αυτομορφισμός** της R ή απλά αυτομορφισμός της R, αν είναι σαφές πιο k θεωρούμε.

6.1.1 Θεώρημα (Skolem-Noether). *Έστω R μια κεντρική απλή k-άλγεβρα πεπερασμένης διάστασης και A απλή υποάλγεβρα της R. Αν $f: A\to R$ είναι ομομορφισμός k-αλγεβρών, τότε υπάρχει αντιστρέψιμο $c\in R$ με την ιδιότητα*

$$f(a)=cac^{-1} \quad \text{για κάθε } a\in A. \tag{1}$$

6.1.2 Πόρισμα. *Κάθε αυτομορφισμός μιας κεντρικής απλής άλγεβρας πεπερασμένης διάστασης είναι της μορφής (1).*

Ο ομομορφισμός στην (1) δύναται να οριστεί σε όλο το R (με τον ίδιο τύπο). Ένας αυτομορφισμός της μορφής $R\to R, a\mapsto cac^{-1}$, λέγεται **εσωτερικός αυτομορφισμός**. Το θεώρημα των Skolem Noether λέει ότι κάθε ομομορφισμός $f: A\to R$ είναι ο περιορισμός κάποιου εσωτερικού αυτομορφισμού της R.

Παρατηρήσεις

1. Η υπόθεση στο πόρισμα ότι η άλγεβρα είναι κεντρική είναι απαραίτητη. Για παράδειγμα ο αυτομορφισμός $\mathbb{C}\to\mathbb{C}$, $z\to\overline{z}$ (συζυγής του z) της $\mathbb{R}$-άλγεβρας $\mathbb{C}$ δεν είναι της μορφής (1).
2. Ο αυτομορφισμός $\mathbb{C}\times\mathbb{C}\to\mathbb{C}\times\mathbb{C}, (a,b)\mapsto(b,a)$, δεν είναι εσωτερικός.

3. Το πόρισμα μας πληροφορεί ότι η ομάδα των αυτομορφισμών της k-άλγεβρας $M_n(k)$ είναι ισόμορφη με τη $GL_n(k)/N$, όπου $N=\{aI\in M_n(k)\,|\,a\in k, a\neq 0\}$ (άσκηση).

Στην απόδειξη του Θεωρήματος 6.1.1 υπεισέρχεται με ουσιαστικό τρόπο η έννοια του τανυστικού γινομένου. Υπενθυμίζουμε ότι αν *A*, *B* είναι *k*-άλγεβρες, ο διανυσματικός χώρος $A\underset{k}{\otimes}B$ καθίσταται *k*-άλγεβρα αν θέσουμε

$$(a\otimes b)(a'\otimes b')=aa'\otimes bb'.$$

Το ταυτοτικό στοιχείο του $A\underset{k}{\otimes}B$ είναι το $1_A\otimes 1_B$. Στα παρακάτω θα γράφουμε $A\otimes B$ στη θέση του $A\underset{k}{\otimes}B$.

6.1.3 Λήμμα. *Έστω R δακτύλιος και πρότυπα M_R και $_RF$ όπου το F είναι ελεύθερο με βάση X. Τότε κάθε $u\in M\underset{R}{\otimes}F$ γράφεται κατά μοναδικό τρόπο ως*

$$u=\sum_{i=1}^{n} m_i\otimes x_i,$$

όπου $m_i\in M$ και τα $x_i\in X$ είναι ανά δύο διάφορα.(Σημ. Στη μοναδικότητα δεν λαμβάνονται υπόψη μηδενικοί όροι $0_M\otimes x_j$.)

Απόδειξη: Το ότι το *u* έχει μία έκφραση της ζητούμενης μορφής προκύπτει άμεσα από το γεγονός ότι το *X* παράγει το F ως *R*-πρότυπο και ότι το τανυστικό γινόμενο $M\underset{R}{\otimes}F$ είναι πάνω από το R. Για τη μοναδικότητα, αν $x\in X$ γράφουμε $R_x=R$ και $M_x=M$. Τότε υπάρχει ισομορφισμός αβελιανών ομάδων

$$\theta : M\underset{R}{\otimes}F\to \underset{x\in X}{\oplus} M_x$$

$M\underset{R}{\otimes}F\simeq M\underset{R}{\otimes}\left(\underset{x\in X}{\oplus}R_x\right)\simeq \underset{x\in X}{\oplus}\left(M\underset{R}{\otimes}R_x\right)\simeq \underset{x\in X}{\oplus}M_x$, όπου οι δύο τελευταίοι ισομορφισμοί είναι από την παράγραφο 5.2. Ισχύει $\theta(m\otimes y)=i_y(m)$, $m\in M$, $y\in X$,, όπου $i_y : M_y\to \underset{x\in X}{\oplus}M_x$ είναι η εμφύτευση στην *y* συντεταγμένη. Από τον ορισμό του ευθέως αθροίσματος κάθε στοιχείο του $\underset{x\in X}{\oplus}M_x$ γράφεται μοναδικά στη μορφή

$$i_{x_1}(m_1)+\ldots+i_{x_n}(m_n)=\theta(m_1\otimes x_1)+\ldots+\theta(m_n\otimes x_n)=\theta\left(\sum m_i\otimes x_i\right),$$

όπου τα x_i είναι ανά δύο διάφορα στοιχεία του *X*. Η μοναδικότητα προκύπτει από το γεγονός ότι ο θ είναι μονομορφισμός.

Το παρακάτω αποτέλεσμα θα χρησιμοποιηθεί πολλές φορές.

6.1.4 Θεώρημα. *Έστω A, B απλές k-άλγεβρες. Αν η A είναι κεντρική τότε η $A\otimes B$ είναι απλή k-άλγεβρα.*

Απόδειξη: Έστω $I\neq 0$ αμφίπλευρο ιδεώδες του $A\otimes B$. Θα δείξουμε ότι $I=A\otimes B$.

Ισχυρισμός 1. $\exists\, v\in I-\{0\}$ της μορφής $v=1_A\otimes b,\ b\in B$.

Έστω προς στιγμή ότι ισχύει ο ισχυρισμός. Το $BbB=\{b_1bb_1'+\ldots+b_nbb_n'\in B\,|\ n>0, b_i, b_i'\in B\}$ είναι μη μηδενικό αμφίπλευρο ιδεώδες του *B*. Άρα $B=BbB$. Έχουμε

$$1_A\otimes B=1_A\otimes BbB\subseteq(1_A\otimes B)(1_A\otimes b)(1_A\otimes B)\subseteq(1_A\otimes B)v(1_A\otimes B),$$

και συνεπώς $1_A\otimes B\subseteq I$. Επίσης

$$A \otimes B = (A \otimes 1_B)(1_A \otimes B) \subseteq (A \otimes 1_B)I \subseteq I,$$

και συνεπώς $A \otimes B = I$.

Απόδειξη του Ισχυρισμού 1. Έστω Y μια βάση του B. Έστω $u \in I$, $u \neq 0$

$$u = \sum_{i=1}^{n} a_i \otimes y_i, \tag{1}$$

όπου $a_i \in A - \{0\}$, $y_i \in Y$ και τα y_i είναι ανά δύο διάφορα.

Επιλέγουμε μια έκφραση (1) με n ελάχιστο (καθώς το $u \neq 0$ διατρέχει το *I*). Λόγω της υπόθεσης της απλότητας έχουμε

$$Aa_1A = A.$$

Άρα

$$1_A = \sum_j r_j a_1 s_j,$$

για κάποια $r_i, s_j \in A$. Θέτουμε

$$v = \sum_j (r_j \otimes 1_B) u (s_j \otimes 1_B) \in I.$$

Εκτελώντας πράξεις έχουμε

$$\begin{aligned} v &= \sum_{i,j} (r_j \otimes 1_B)(a_i \otimes y_i)(s_j \otimes 1_B) \\ &= \sum_{i,j} r_j a_j s_j \otimes y_i \\ &= \sum_j r_j a_1 s_j \otimes y_1 + \sum_{i \neq 1} \left(\sum_j r_j a_i s_j \right) \otimes y_i \\ &= 1_A \otimes y_1 + \sum_{i \neq 1} \left(\sum_j r_j a_i s_j \right) \otimes y_i. \end{aligned} \tag{2}$$

Έστω $\overline{a}_i$ η ποσότητα στην τελευταία παρένθεση. Για να δείξουμε τον ισχυρισμό 1 αρκεί να δείξουμε ότι $\overline{a}_i \in k$ γιατί τότε θα έχουμε από την (2)

$$\begin{aligned} v &= 1_A \otimes y_1 + \sum_{i \neq 1} \overline{a}_i \otimes y_i \\ &= 1_A \otimes y_1 + 1_A \otimes \left(\sum_{i \neq 1} \overline{a}_i y_i \right) \\ &= 1_A \otimes \left(y_1 + \sum_{i \neq 1} \overline{a}_i y_i \right), \end{aligned} \tag{3}$$

οπότε θέτουμε $b = y_1 + \sum_{i \neq 1} \overline{a}_i y_i$.

Επειδή η *A* είναι κεντρική, αρκεί να δείξουμε ότι:

Ισχυρισμός 2. $\overline{a}_i \in C(A)$.

Απόδειξη: Έστω $a \in A$. Θέτουμε

$$w = (a \otimes 1_B)v - v(a \otimes 1_B) \in I.$$

Αντικαθιστώντας το *v* από τη (2) παίρνουμε

$$w = a \otimes y_1 + \sum_{i \neq 1} a\,\overline{a}_i \otimes y_i - \left[a \otimes y_1 + \sum_{i \neq 1} \overline{a}_i a \otimes y_i \right] = \sum_{i \neq 1} (a\,\overline{a}_i - \overline{a}_i a) \otimes y_i.$$

Από το ελάχιστο στον ορισμό του v παίρνουμε $w=0$. Από το Λήμμα 6.1.3 έπεται ότι $a\,\overline{a}_i - \overline{a}_i a = 0$, δηλαδή $\overline{a}_i \in C(A)$.

6.1.5 Σημείωση. Αποδεικνύεται ότι αν στις υποθέσεις του θεωρήματος 6.1.4 προσθέσουμε την υπόθεση ότι η B είναι απλή, τότε το συμπέρασμα είναι ότι η $A\otimes B$ είναι απλή **και** κεντρική. Αυτό δεν θα χρησιμοποιηθεί στις σημειώσεις αυτές.

Στην απόδειξη του θεωρήματος των Skolem-Noether θα χρησιμοιποιήσουμε το εξής πόρισμα του θεωρήματος Wedderburn-Artin.

6.1.6 Λήμμα. *Έστω A απλή k-άλγεβρα πεπερασμένης διάστασης. Αν M και N είναι A-πρότυπα με* $\dim_k M = \dim_k N$ *, τότε* $M \simeq N$ *ως A-πρότυπα.*

Απόδειξη: Η A είναι του Artin, αφού $\dim_k A < \infty$. Είναι και απλή. Από το θεώρημα Wedderburn-Artin (§ 3.3), το A έχει μοναδικό απλό πρότυπο (με προσέγγιση ισομορφισμού εννοείται), έστω L. Έχουμε

$$M \simeq L^m \quad \text{και} \quad N \simeq L^n,$$

(που είναι ισομορφισμοί A-προτύπων). Από τη σχέση $\dim_k M = \dim_k N$ παίρνουμε $m=n$ (αφού $\dim_k L < \infty$, γιατί το L είναι πηλίκο του A). Άρα $M \simeq N$ ως A-πρότυπα.

Απόδειξη του θεωρήματος Skolem-Noether.

Έστω $E = R\otimes A^{op}$. Η E είναι πεπερασμένης διάστασης k-άλγεβρα και, σύμφωνα με το Θεώρημα 6.1.4, απλή. Συνεπώς κάθε δύο E-πρότυπα με ίσες πεπερασμένες διαστάσεις ως k-διανυσματικοί χώροι είναι ισόμορφα (Λήμμα 6.1.6).

Καθιστούμε την αβελιανή ομάδα R ένα E-πρότυπο με δύο διαφορετικούς τρόπους:

(*) $(r\otimes a)\cdot x = rxa$,

(**) $(r\otimes a)\circ x = rxf(a)$,

όπου $r\in R, a\in A, x\in R$. Συνεπώς υπάρχει ισομορφισμός αβελιανών ομάδων $R \xrightarrow{h} R$ έτσι ώστε $(r\otimes a)\cdot h(x) = h((r\otimes a)\circ x)$, δηλαδή

$$rh(x)a = h(rxf(a)) \tag{3}$$

για κάθε $r,x\in R, a\in A$. Για $a=x=1$ παίρνουμε

$$rh(1) = h(r)$$

για κάθε $r\in R$.

Από αυτό έπεται ότι το $c=h(1)$ είναι αντιστρέψιμο. Πράγματι, επειδή η απεικόνιση h είναι επί, υπάρχει $y\in R$ με $yc=1$. Παρατηρούμε ότι η σχέση $cy=1$ ισοδυναμεί με τη $h(cy)=h(1)$, δηλαδή με τη $cyc=c$ που προφανώς αληθεύει.

Από την (3) έχουμε $h(1)a = h(f(a)) = f(a)h(1)$ και επομένως $f(a)=cac^{-1}$ για κάθε $a\in R$.

6.2 Θεώρημα Διπλού Κεντροποιητή

Έστω R μια k-άλγεβρα και $S\subseteq R$ ένα υποσύνολο του R. Ο **κεντροποιητής** του S στο R είναι η υποάλγεβρα

$$C_R(S) = C(S) = \{r\in R \mid rs = sr \quad \text{για κάθε} \quad s\in S\}.$$

Ισχύει $S\subseteq C(C(S))$. Το επόμενο θεώρημα περιγράφει μια κατάσταση όπου ισχύει ισότητα.

***6.2.1 Θεώρημα** (Διπλού κεντροποιητή).* *Έστω R κεντρική απλή k-άλγεβρα πεπερασμένης διάστασης και S απλή υποάλγεβρα. Τότε*

i) $C(S)$ *είναι απλή k-άλγεβρα,*

ii) $\dim_k R = (\dim_k S)(\dim_k C(S))$,

iii) $C(C(S)) = S$.

Απόδειξη: Δίνουμε πρώτα ένα χαρακτηρισμό του $C(S)$. Η R είναι απλή k-άλγεβρα του Artin. Συνεπώς (θεώρημα Wedderburn-Artin και Σημείωση 3.3.2) $R = End_D V$, όπου το V είναι πεπερασμένης διάστασης D-πρότυπο, D k-άλγεβρα διαίρεσης. Το V γίνεται $D \otimes S -$ πρότυπο με δράση

$$(d \otimes s)v = d(s(v)).$$

Ισχυριζόμαστε ότι $End_{D\otimes S} V = C(S)$. Πράγματι, έχουμε

$$End_{D\otimes S}(v) = \{ f \in End_D V \mid f((d\otimes s)v) = (d \otimes s) f(v),\ \forall v \in V,\ d \in D,\ s \in S \}.$$

Αλλά για κάθε $v \in V,\ d \in D,\ s \in S$,

$$f((d\otimes s)v) = (d\otimes s) f(v) \Leftrightarrow f(d(s(v)) = d(s(f(v))) \Leftrightarrow$$
$$df(s(v)) = d(s(f(v)) \Leftrightarrow f(s(v)) = sf(v) \Leftrightarrow fs = sf \Leftrightarrow f \in C(S).$$

Ερχόμαστε τώρα στην απόδειξη των i)-iii).

i) Επειδή η S είναι απλή και η D είναι απλή και κεντρική, από το θεώρημα 6.1.4 η $D \otimes S$ είναι απλή. Είναι και του Artin (αφού $\dim_k D < \infty$ και $\dim_k S < \infty$ καθώς $\dim_k R < \infty$). Από το θεώρημα Wedderburn-Artin

$$D \otimes S = End_{D'}(V'),$$

όπου V' είναι ένα D'-πρότυπο, D' k-άλγεβρα διαίρεσης. Επιπλέον γνωρίζουμε ότι το V' είναι το μοναδικό απλό $D \otimes S$-πρότυπο. Έτσι

$$V = (V')^m$$

για κάποιο m. Έχουμε

$$C(S) = End_{D\otimes S}(V) = End_{D\otimes S}((V')^m) \simeq M_m(End_{D\otimes S}(V')) \simeq M_m(D'), \tag{4}$$

όπου ο τελευταίος ισομορφισμός της (4) προέρχεται από την άσκηση 1.9 iii).

ii) Από την (4) έχουμε

$$\dim_k C(S) = m^2 \dim_k D' \tag{5}$$

και από $V = (V')^m$

$$m = \dim_k V / \dim_k V'. \tag{6}$$

Επειδή το V' είναι ελεύθερο D'-πρότυπο και το D' είναι ελεύθερο k-πρότυπο έχουμε (άσκηση)

$$\dim_k V' = \dim_{D'} V' \dim_k D'. \tag{7}$$

Αντικαθιστώντας τις (7) και (6) στην (5) παίρνουμε

$$\dim_k C(S) = (\dim_k V)^2 / (\dim_{D'} V)^2 \dim_k D'.$$

Ο παρονομαστής είναι $\dim_k End_{D'}(V') = \dim_k D \otimes S = (\dim_k D)(\dim_k S)$ και ο αριθμητής είναι $((\dim_D V)(\dim_k D))^2$. Άρα

$$\begin{aligned}\dim_k C(S) &= (\dim_D V)^2 \dim_k D / \dim_k S \\ &= \dim_k End_D(V) / \dim_k S \\ &= \dim_k R / \dim_k S.\end{aligned}$$

iii) Έχουμε $\dim_k R = \dim_k S \dim_k C(S)$ από το ii). Γράφοντας την ίδια σχέση για $C(S)$ στη θέση του S (επιτρεπτό αφού η $C(S)$ είναι απλή από το i)) παίρνουμε $\dim_k R = (\dim_k C(S))(\dim_k C(C(S)))$. Από τις δύο σχέσεις προκύπτει $\dim_k S = \dim_k C(C(S))$. Εφόσον ισχύει $S \subseteq C(C(S))$ και οι διαστάσεις είναι πεπερασμένες, προκύπτει το ζητούμενο.

6.3 Εφαρμογές

Θα αποδείξουμε εδώ δύο φημισμένα αποτελέσματα.

6.3.1 Θεώρημα *(Frobenius).* *Κάθε πραγματική άλγεβρα διαίρεσης πεπερασμένης διάστασης είναι ισόμορφη με μία από τις* $\mathbb{R}, \mathbb{C}, \mathbb{H}$.

6.3.2 Θεώρημα *(Wedderburn).* *Κάθε πεπερασμένος δακτύλιος διαίρεσης είναι μεταθετικός (δηλαδή σώμα).*

Ξεκινάμε με προκαταρκτικά που αφορούν δακτύλιους διαίρεσης.

6.3.3 Λήμμα. *Έστω D δακτύλιος διαίρεσης. Τότε*

i) Υπάρχει μέγιστο υπόσωμα του D (δηλ. σώμα που δεν περιέχεται γνήσια σε υπόσωμα του D).
ii) Κάθε μέγιστο υπόσωμα K περιέχει το κέντρο $C(D)$.
iii) Για κάθε μέγιστο υπόσωμα K ισχύει $C(K) = K$, όπου $C(K)$ είναι ο κεντροποιητής του K στο D.

Απόδειξη: i) Τυπική εφαρμογή του λήμματος του Zorn.
ii) Αν υπάρχει $d \in C(D),\ d \notin K$, τότε το σύνολο

$$K(d) = \left\{ \frac{f(d)}{g(d)} \,\middle|\, f(x), g(x) \in K[x], g(d) \neq 0 \right\}$$

είναι σώμα που περιέχει γνήσια το *K*, άτοπο.
iii) Αφού το *K* είναι μεταθετικό σύνολο, ισχύει $K \subseteq C(K)$. Αν υπάρχει $d \in C(K)$, $d \notin K$, τότε το σύνολο είναι σώμα που περιέχει γνήσια το *K*, άτοπο.

Το προηγούμενο λήμμα μαζί με το θεώρημα του διπλού κεντροποιητή δίνει αμέσως το εξής κομψό αριθμητικό αποτέλεσμα.

6.3.4 Πρόταση. *Έστω D κεντρική k-άλγεβρα διαίρεσης πεπερασμένης διάστασης και K μέγιστο υπόσωμα του D. Τότε* $\dim_k D = (\dim_k K)^2$.

Απόδειξη του θεωρήματος 6.3.1.
Έστω *K* μέγιστο υπόσωμα του *D*. Επειδή $\dim_{\mathbb{R}} K \le \dim_{\mathbb{R}} D < \infty$, η επέκταση σωμάτων $K/\mathbb{R}$ είναι αλγεβρική. Άρα

$$\dim_{\mathbb{R}} K = 1 \text{ ή } 2.$$

1η περίπτωση. $\dim_{\mathbb{R}} K = 1$.
Έχουμε

$$K = \mathbb{R} \quad \text{και} \quad K \supseteq C(D) \supseteq \mathbb{R}$$

οπότε $\mathbb{R} = C(D) = K$. Η πρόταση 6.3.4 δίνει $\dim_{\mathbb{R}} D = (\dim_{\mathbb{R}} K)^2 = 1$, και άρα $D = \mathbb{R}$.

2η περίπτωση. $\dim_{\mathbb{R}} K = 2$.
Άρα $K \simeq \mathbb{C}$. Θα ταυτίζουμε τα σώματα $K, \mathbb{C}$. Καθώς $\mathbb{R} \subseteq C(D) \subseteq \mathbb{C}$, διακρίνουμε τις περιπτώσεις:

$(\alpha)\quad C(D)=\mathbb{C},$

$(\beta)\quad C(D)=\mathbb{R}.$

Ας παρακολουθήσουμε το συλλογισμό στο διάγραμμα.

$$\left.\begin{array}{c} D \\ | \\ K=\mathbb{C} \\ | \\ C(D) \\ | \\ \mathbb{R} \end{array}\right.\qquad \begin{array}{c} K=\mathbb{C} \\ | \\ C(D) \\ | \end{array}\Bigg\}\, 2$$

(α) $C(D)=\mathbb{C}$.

Ισχύει $K=\mathbb{C}=C(D)$ και άρα (πρόταση 6.3.4) $\dim_{C(D)} D=(\dim_{C(D)} K)^2=1 \Rightarrow D=C(D)=\mathbb{C}$.

(β) $C(D)=\mathbb{R}$.

Θεωρούμε τον $\mathbb{R}$-ισομορφισμό

$$f: K \ni a+bi \mapsto a-bi \in K.$$

Από το θεώρημα Skolem-Noether, υπάρχει $x \in D$ με την ιδιότητα

$$x(a+bi)x^{-1}=a-bi \quad \text{για κάθε} \quad a,b \in \mathbb{R}. \tag{9}$$

Ισχυριζόμαστε ότι $x^2 \in \mathbb{R}$. Πράγματι, έχουμε

$$x^2(a+bi)x^{-2}=x(a-bi)x^{-1}=a+bi$$

που σημαίνει ότι $x^2 \in C(K)$. Έτσι $x^2 \in K$ (Λήμμα 6.3.3).

Τέλος η σχέση $f(x^2)=x^2$ δίνει $x^2 \in \mathbb{R}$.

Αν $x^2>0$, τότε $x^2=r^2$, $r\in\mathbb{R} \Rightarrow x=\pm r \in \mathbb{R}$, άτοπο λόγω της (9). Άρα $x^2<0$. Γράφουμε $x^2=-y^2$, $y\in\mathbb{R}$. Θέτουμε $j:=x/y$ και $k:=ij$.

Εύκολα ελέγχουμε ότι

$$i^2=j^2=k^2=-1$$

$$ij=-ji=k,\ jk=-kj=i,\ ki=-ik=j.$$

Ακόμα, η πρόταση 6.3.4 δίνει $\dim_{\mathbb{R}} D=(\dim_{\mathbb{R}} K)^2=4$. Εύκολα επαληθεύεται ότι τα στοιχεία $1, i, j, k$ είναι γραμμικά ανεξάρτητα πάνω από το $\mathbb{R}$ (άσκηση) και άρα αποτελούν βάση του D ως $\mathbb{R}$-διανυσματικός χώρος. Άρα $D \simeq \mathbb{H}$ ως $\mathbb{R}$-άλγεβρες (γιατί;).

Αποδεικνύουμε στη συνέχεια το θεώρημα 6.3.2.

6.3.5 Λήμμα. *Έστω G πεπερασμένη ομάδα και H γνήσια υποομάδα της G. Τότε*

$$G \neq \bigcup_{g\in G} gHg^{-1}.$$

Απόδειξη: Έστω X το σύνολο των υποομάδων της G. Θεωρούμε τη δράση της G το X που δίνεται από τη σχέση

$$G\times X \ni (g,H) \mapsto gHg^{-1} \in X.$$

Από γνωστό θεώρημα για δράσεις, ο πληθάριθμος της τροχιάς του $H\in X$ είναι ο δείκτης $[G:G_H]$, όπου G_H είναι ο σταθεροποιητής $G_H=\{g\in G \mid g\cdot H=H\}$. Ο ορισμός της δράσης δίνει

$$G_H = N(H)$$

όπου $N(H)$ είναι ο κανονικοποιητής της H στη G, $N(H) = \{g \in G \mid gHg^{-1} = H\}$. Συμπέρασμα: για σταθερό H, το πλήθος των διακεκριμένων υποομάδων της G της μορφής gHg^{-1}, $g \in G$, είναι $[G : N(H)]$. Μετράμε τώρα τα στοιχεία του συνόλου $\bigcup_{g \in G} gHg^{-1}$ που είναι διάφορα από το μοναδιαίο στοιχείο. Το πλήθος τους είναι

$$\begin{aligned}
&\leq [G : N(H)](|H| - 1) && \\
&\leq [G : H](|H| - 1) && (\text{γιατί } H \subseteq N(H)) \\
&= |G| - [G : H] && (\text{θεώρημα Lagrange}) \\
&< |G| - 1. && (\text{γιατί } H \neq G)
\end{aligned}$$

Άρα $G \neq \bigcup_{g \in G} gHg^{-1}$.

Παρατήρηση: Κάθε $d \in D$, όπου D είναι δακτύλιος διαίρεσης περιέχεται σε κάποιο μέγιστο υπόσωμα του D. Πράγματι το d περιέχεται στο σώμα $k(d) = \left\{ \dfrac{f(d)}{g(d)} \,\middle|\, f(x), g(x) \in k[x], g(d) \neq 0 \right\}$, όπου $k = C(D)$. Τώρα το ζητούμενο προκύπτει από μια τυπική εφαρμογή του λήμματος του Zorn.

Απόδειξη του θεωρήματος 6.3.2.

Έστω K μέγιστο υπόσωμα του D. Θα δείξουμε ότι $K = D$. Έστω $d \in D$. Από την προηγούμενη παρατήρηση το d περιέχεται σε κάποιο σώμα. Άρα ισχύει

$$D = \bigcup_K K, \quad K \text{ μέγιστο υπόσωμα.}$$

Ισχυρισμός: Κάθε δύο μέγιστα υποσώματα του D έχουν τον ίδιο πληθάριθμο. Πράγματι, έστω k το κέντρο του D οπότε το k είναι σώμα που περιέχεται στο K (λήμμα 6.3.3). Ως k-άλγεβρα η D έχει προφανώς πεπερασμένη τάξη. Η πρόταση 6.3.4 δίνει

$$\dim_k D = n^2,$$

όπου $n = \dim_k K$. Άρα $|K| = q^n$, όπου $q = |k|$ και $n^2 = \dim_k D$ δεν εξαρτώνται από το K.

Τώρα από τη θεωρία Galois, υπενθυμίζουμε ότι κάθε δύο πεπερασμένα σώματα της ίδιας τάξης είναι ισόμορφα και επιπλέον αν είναι επεκτάσεις του k υπάρχει ισομορφισμός που είναι ταυτοτικός στο k. Από το θεώρημα Skolem-Noether συμπεραίνουμε ότι κάθε δύο μέγιστα υποσώματα του D συνδέονται με μια σχέση της μορφής $K'' = xK'x^{-1}$, $x \in D$.

Συμπέρασμα:

$$D = \bigcup_{x \in D^*} xKx^{-1}.$$

Λαμβάνοντας τις πολλαπλασιαστικές ομάδες έχουμε

$$D^* = \bigcup_{x \in D^*} xK^*x^{-1}.$$

Από το λήμμα 6.3.5 αυτό είναι άτοπο εκτός αν $K^* = D^*$. Αλλά τότε $K = D$.

Ασκήσεις

Στα παρακάτω, k είναι σώμα. Επίσης $\otimes$ (χωρίς δείκτη) = $\underset{k}{\otimes}$.

1. Αληθεύει ότι υπάρχει πεπερασμένη ομάδα $G \neq 1$ ώστε η άλγεβρα $k[G]$ να είναι κεντρική;

2. Υπάρχει ισομορφισμός $\mathbb{R}$-αλγεβρών $\mathbb{H} \underset{\mathbb{R}}{\otimes} \mathbb{H} \simeq M_4(\mathbb{R})$.

3. Δείξτε ότι η ομάδα των αυτομορφισμών της k-άλγεβρας $M_n(k)$ είναι ισόμορφη με τη $GL_n(k)/N$, όπου $N = \{aI \in M_n(k) \mid a \in k, a \neq 0\}$. Ποια είναι η ομάδα των $\mathbb{R}$-αυτομορφισμών της $\mathbb{H}$;

4. Έστω A κεντρική απλή k-άλγεβρα και B k-άλγεβρα. Δείξτε τα εξής.
   a. Κάθε αμφίπλευρο ιδεώδες του $A \otimes B$ έχει τη μορφή $A \otimes I$, όπου το I είναι αμφίπλευρο ιδεώδες του B.
   b. $C(A \otimes B) = 1_A \otimes C(B)$.

5. Ποιο είναι το κέντρο της πραγματικής άλγεβρας $\mathbb{H} \underset{\mathbb{R}}{\otimes} M_2(\mathbb{C})$;

6. Ποιο είναι το πλήθος των απεικονίσεων $M_2(\mathbb{Z}_2) \to M_2(\mathbb{Z}_2)$ και πόσες από αυτές είναι ομομορφισμοί $\mathbb{Z}_2$-αλγεβρών;

7. Έστω A μια k-άλγεβρα. Τότε η A είναι κεντρική k-άλγεβρα αν και μόνο αν η $M_n(A)$ είναι κεντρική k-άλγεβρα για κάποιο n.

Ακολουθούν δύο κομψές εφαρμογές του Θεωρήματος Skolem-Noether.

8. Έστω D κεντρική k-άλγεβρα διαίρεσης πεπερασμένης διάστασης και $a, b \in D$. Αν οι k-γραμμικές απεικονίσεις

$$\varphi_a : D \to D, x \mapsto xa$$
$$\varphi_b : D \to D, x \mapsto xb$$

έχουν το ίδιο ελάχιστο πολυώνυμο, τότε $a = cbc^{-1}$ για κάποιο αντιστρέψιμο $c \in D$.

9. Ακολουθεί μια κομψή εφαρμογή του Θεωρήματος Skolem-Noether.
Έστω R δακτύλιος. Μια προσθετική απεικόνιση $d : R \to R$ λέγεται **παραγώγιση** αν $d(ab) = ad(b) + d(a)b$ για κάθε $a, b \in D$. Μια παραγώγιση d λέγεται **εσωτερική** αν είναι της μορφής $d(x) = xc - cx$ για κάποιο $c \in R$. Αποδείξετε ότι κάθε k-γραμμική παραγώγιση μιας πεπερασμένης διάστασης κεντρικής απλής k-άλγεβρας R είναι εσωτερική.
Υπόδειξη: Skolem-Noether στην απεικόνιση $f : A \to M_2(R)$ όπου

$$A = \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \middle| r \in R \right\} \text{ και } f : \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \mapsto \begin{pmatrix} r & d(r) \\ 0 & r \end{pmatrix}.$$

10.
   a. Αληθεύει ότι το τανυστικό γινόμενο δύο k-αλγεβρών διαίρεσης είναι πάντοτε k-άλγεβρα διαίρεσης;
   b. Έστω D, D' δύο k-άλγεβρες διαίρεσης πεπερασμένης διάστασης. Αν η D είναι κεντρική και επιπλέον μκδ$(\dim_k D, \dim_k D') = 1$, τότε η $D \otimes D'$ είναι k-άλγεβρα διαίρεσης.

11. Έστω $A \in M_n(k)$. Δείξτε ότι τα ακόλουθα είναι ισοδύναμα.
   a. Το χαρακτηριστικό πολυώνυμο και το ελάχιστο πολυώνυμο του A έχουν τον ίδιο βαθμό.
   b. Τα στοιχεία του $M_n(k)$ που αντιμετατίθενται με το A είναι ακριβώς τα πολυώνυμα του A.

12. Ταξινομήστε τους ημιαπλούς δακτυλίους που έχουν 2016 στοιχεία.

13. Έστω R απλή k-άλγεβρα. Δώστε στο R τη δομή $R \otimes R^{op}$ − προτύπου έτσι ώστε $C(R) \simeq End_{R \otimes R^{op}}(R)$.

14. Έστω $n \geq 2$. Είναι δυνατόν η $\mathbb{R}$-άλγεβρα $M_n(\mathbb{H})$ να περιέχει υπόσωμα K με $\mathbb{R} \subseteq K$ και $C(K) = K$;

15. Αν R είναι κεντρική απλή k-άλγεβρα πεπερασμένης διάστασης και S απλή κεντρική υποάλγεβρα της

R, τότε $R \simeq S \otimes C(S)$.

16. Έστω R k-αλγεβρα του Artin και S πεπερασμένης διάστασης k-άλγεβρα. Εξετάστε ποιες από τις ακόλουθες προτάσεις αληθεύουν.

a. $R \otimes S$ είναι δακτύλιος του Artin.

b. $C(R \otimes S) = k$ είναι κεντρική k-άλγεβρα.

c. Κάθε αυτομορφισμός της $R \otimes S$ είναι εσωτερικός.

d. Κάθε αυτομορφισμός της $S \otimes M_n(k)$ είναι εσωτερικός.

ΚΕΦΑΛΑΙΟ 7: Αναπαραστάσεις Πεπερασμένων Ομάδων I

Χρησιμοποιώντας το θεώρημα του Wedderburn για ημιαπλούς δακτυλίους, αναπτύσσουμε εδώ τις πρώτες προτάσεις από τη θεωρία των αναπαραστάσεων και χαρακτήρων πεπερασμένων ομάδων υπέρ του $\mathbb{C}$. Αυτές εφαρμόζονται στο επόμενο κεφάλαιο όπου αποδεικνύουμε ένα θεμελιώδες θεώρημα του Burnside που αφορά στην επιλυσιμότητα ομάδων τάξης $p^a q^b$ (p, q πρώτοι).

7.1 Αναπαραστάσεις

Έστω G ομάδα και k σώμα. Μια **αναπαράσταση** της G υπέρ του k είναι ένας ομομορφισμός ομάδων $\rho : G \to GL_n(k)$, για κάποιο n, όπου $GL_n(k)$ είναι η ομάδα των αντιστρέψιμων $n\times n$ πινάκων με στοιχεία από το k. Το n ονομάζεται ο **βαθμός** της αναπαράστασης.

Αν $\rho : G \to GL_n(k)$ είναι μια αναπαράσταση της G, τότε θέτοντας $V := k^n$ και ορίζοντας $gv = \rho(g)(v)$ λαμβάνουμε ένα $k[G]$-πρότυπο. Αντίστροφα αν V είναι ένα $k[G]$-πρότυπο διάστασης $n < \infty$, τότε σταθεροποιώντας μια βάση του V έχουμε $Aut(V) \simeq GL_n(k)$ και ορίζεται ένας ομομορφισμός ομάδων $\rho : G \to GL_n(k)$, όπου $\rho(g)$ είναι ο πίνακας της γραμμικής απεικόνισης $V \ni v \mapsto gv \in V$ ως προς τη συγκεκριμένη επιλογή βάση. Έτσι, στις σημειώσεις αυτές, θα χρησιμοποιούμε τους όρους αναπαράσταση της G και $k[G]$-πρότυπο χωρίς να γίνεται ιδιαίτερη διάκριση μεταξύ της ρ και του V.

7.1.1 Παράδειγμα

1. Για κάθε ομάδα G έχουμε την αναπαράσταση $\rho : G \to GL_1(k)$, όπου $\rho(g) = 1$ για κάθε $g \in G$. Αυτή λέγεται η **τετριμμένη αναπαράσταση** της G.

2. Για τη συμμετρική ομάδα $G = S_n$ έχουμε την αναπαράσταση $\rho : G \to GL_1(k)$, όπου $\rho(\sigma) = sign(\sigma)$ για κάθε $\sigma \in S_n$. Αυτή λέγεται η **αναπαράσταση προσήμου** της S_n.

3. Έστω G η ομάδα D_8 που δίνεται με γεννήτορες και σχέσεις από

$$D_8 = \left\langle a, b : a^4 = b^2 = 1,\ ab = ba^{-1} \right\rangle .$$

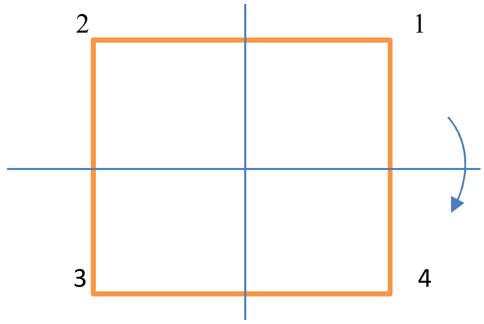
(Κάθε στοιχείο της D_8 γράφεται μοναδικά στη μορφή $a^i b^j$ με $0 \le i \le 1, 0 \le j \le 3$. Ειδικά, η D_8 έχει τάξη 8. Είναι μία από μια οικογένεια ομάδων που ονομάζονται διεδρικές. Γεωμετρικά, η D_8 περιγράφει τις συμμετρίες του τετραγώνου.) Θέτουμε

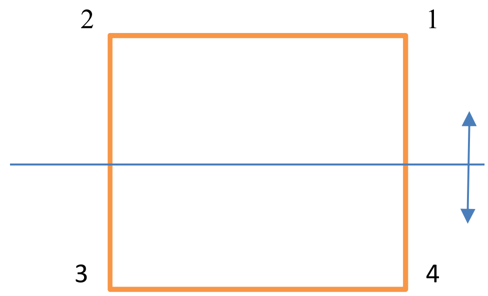
$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ελέγχουμε ότι $A^4 = B^2 = I$, $AB = BA^{-1}$. Συνεπώς ορίζεται μία αναπαράσταση G πάνω από το $\mathbb{C}$, $\rho : G \to GL_n(\mathbb{C})$, από τις σχέσεις

$$\rho(a^i b^j) = A^i B^j, \quad i = 0,...,3 \quad j = 0,1 .$$

Γεωμετρικά το A παριστάνει στροφή 90^{o} γύρω από την αρχή των αξόνων και το B ανάκλαση ως προς τον άξονα των x όπως φαίνεται στο παρακάτω σχήμα. Έτσι η συγκεκριμένη αναπαράσταση ρ “αναπαριστάνει” τη G ως ομάδα μετασχηματισμών του επιπέδου.





$$A:\begin{cases}1\to 4\\ 2\to 1\\ 3\to 2\\ 4\to 3\end{cases}\qquad\qquad B:\begin{cases}1\leftrightarrow 4\\ 2\leftrightarrow 3\end{cases}$$

Δύο αναπαραστάσεις $\rho,\rho' : G\to GL_n(k)$ λέγεται **ισοδύναμες** αν υπάρχει $T\in GL_n(k)$ με την ιδιότητα $\rho'(g)=T^{-1}\rho(g)T$ για κάθε $g\in G$. Για παράδειγμα η αναπαράσταση $\rho\ :\ D_8\to GL_2(\mathbb{C})$ του προηγούμενου παραδείγματος είναι ισοδύναμη με την $\rho'\ :\ D_8\to GL_2(\mathbb{C})$ που ορίζεται από τις σχέσεις

$$\rho'(a)=\begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix} \text{ και } \rho'(b)=\begin{pmatrix} 0 & 1\\ 1 & 0\end{pmatrix}.$$

Εδώ T είναι πίνακας που διαγωνοποιεί τον A, δηλαδή πίνακας των ιδιοδιανυσμάτων του A,

$$T=\begin{pmatrix} 1 & 1\\ i & -i\end{pmatrix}.$$

Έστω $\rho,\rho' : G\to GL_n(k)$ δύο αναπαραστάσεις της G με αντίστοιχα $k[G]$-πρότυπα V, V'. Τότε οι $\rho,\ \rho'$ είναι ισοδύναμες αν και μόνο αν υπάρχει ισομορφισμός $k[G]$-προτύπων $V\to V'$ (άσκηση).

Μία αναπαράσταση $\rho : G\to GL_n(k)$ λέγεται **ανάγωγη** αν το αντίστοιχο $k[G]$-πρότυπο V είναι απλό.

7.1.2 Παράδειγμα. Έστω $G=S_n$ η συμμετρική ομάδα των μεταθέσεων n στοιχείων. Έστω $V=k^n$ και μια βάση $\{v_1,\ldots,v_n\}$ του V. Το V είναι S_n-πρότυπο με δράση $\sigma v_i = v_{\sigma(i)}$. Δεν είναι απλό όταν $n>1$, γιατί ένα υποπρότυπό του είναι το $\langle v_1+\ldots+v_n\rangle$, το κυκλικό υποπρότυπο του V που παράγεται από το $v_1+\ldots+v_n$. Πράγματι, έχουμε $\sigma\left(v_1+\ldots+v_n\right)=v_{\sigma(1)}+\ldots+v_{\sigma(n)}=v_1+\ldots+v_n$ για κάθε $\sigma\in S_n$.

Ένα $k[G]$-πρότυπο V λέγεται **πλήρως αναλύσιμο** αν είναι ευθύ άθροισμα απλών υποπροτύπων του. Το θεώρημα του Maschke μας δίνει το εξής αποτέλεσμα.

7.1.3 Πόρισμα. *Έστω G μια πεπερασμένη ομάδα τάξης n. Αν η χαρακτηριστική του k είναι μηδέν, ή αν η χαρακτηριστική του k είναι p με $p\nmid n$, τότε κάθε $k[G]$-πρότυπο είναι πλήρως αναλύσιμο.*

Στα παρακάτω θα <u>ασχοληθούμε αποκλειστικά με την περίπτωση</u> $k=\mathbb{C}$, οπότε ισχύει το προηγούμενο πόρισμα. Επίσης, G <u>θα είναι πάντα πεπερασμένη ομάδα</u>.

Στο κεφάλαιο 2 είδαμε ότι υπάρχει ισομορφισμός αλγεβρών $\mathbb{C}[G] \simeq M_{n_1}(\mathbb{C}) \times ... M_{n_s}(\mathbb{C})$. Λαμβάνοντας διαστάσεις υπεράνω του $\mathbb{C}$ έχουμε

$$n_1^2 + ... + n_s^2 = |G|.$$

Υπενθυμίζουμε ότι το s είναι το πλήθος των ανά δυο μη ισόμορφων απλών $\mathbb{C}[G]$-προτύπων. Στη συνέχεια θα χαρακτηρίσουμε τον αριθμό s χρησιμοποιώντας ομαδοθεωρητικές έννοιες.

Υπενθυμίζουμε ότι η κλάση συζυγίας του $g \in G$ είναι το σύνολο $\{x^{-1}gx \mid x \in G\}$ και ότι δύο κλάσεις συζυγίας είτε ταυτίζονται είτε είναι ξένες. Έστω C μία κλάση συζυγίας. Θέτουμε

$$\overline{C} = \sum_{g \in C} g \in \mathbb{C}[G].$$

Θα δείξουμε ότι κάθε $\overline{C}$ ανήκει στο κέντρο της άλγεβρας $\mathbb{C}[G]$. Έστω $C = \{x_1^{-1}gx_1, ..., x_r^{-1}gx_r\}$ και $h \in G$. Έχουμε $\overline{C} = \sum_{i=1}^{r} x_i^{-1}gx$, οπότε

$$h^{-1}\overline{C}h = \sum_{i=1}^{r} h^{-1}x_i^{-1}gx_i h = \overline{C}, \tag{1}$$

γιατί καθώς το x_i διατρέχει τα στοιχεία $x_1, ..., x_r$ το $h^{-1}x_i^{-1}gx_i h$ διατρέχει τα στοιχεία του C (αφού $h^{-1}x_i^{-1}gx_i h = h^{-1}x_j^{-1}gx_j h \Leftrightarrow x_i^{-1}gx_i = x_j^{-1}gx_j \Leftrightarrow x_i = x_j$ λόγω του ορισμού των x_i στο σύνολο C). Από την (1) συνάγουμε ότι $\overline{C} \in C(\mathbb{C}[G])$.

7.1.4 Πρόταση. *Έστω $C_1, ..., C_m$ οι (ανά δύο διάφορες) κλάσεις συζυγίας της G. Τότε μία βάση του $\mathbb{C}$-διανυσματικού χώρου $C(\mathbb{C}[G])$ είναι η $\{\overline{C}_1, ..., \overline{C}_m\}$.*

Απόδειξη: Είδαμε πριν ότι $\overline{C}_i \in C(\mathbb{C}[G])$ για κάθε i.

i) Γραμμική ανεξαρτησία: Αν $\lambda_1\overline{C}_1 + ... + \lambda_m\overline{C}_m = 0$ με $\lambda_i \in \mathbb{C}$ παίρνουμε $\lambda_1 = ... = \lambda_m = 0$, γιατί τα $C_1, ..., C_m$ είναι ανά δύο ξένα υποσύνολα βάσης.

ii) Παράγουν το $C(\mathbb{C}[G])$: Έστω $\sum_g \lambda_g g \in C(\mathbb{C}[G])$. Τότε για κάθε $h \in G$ ισχύει $\sum_g \lambda_g h^{-1}gh = \sum_g \lambda_g g$ και επομένως

$$\sum_{x \in G} \lambda_{hxh^{-1}} x = \sum_g \lambda_g g,$$

οπότε παίρνουμε $\lambda_{hxh^{-1}} = \lambda_x$ για κάθε $x \in G$. Με άλλα λόγια, καθώς το g διατρέχει τα στοιχεία μια κλάσης συζυγίας C_i ο συντελεστής λ_g παραμένει σταθερός $\lambda_g = \lambda_i$. Έτσι γράφουμε $\sum_g \lambda_g g = \lambda_1\overline{C}_1 + ... + \lambda_m\overline{C}_m$.

Παράδειγμα Οι κλάσεις συζυγίας της συμμετρικής ομάδας $G = S_3 = \{1, \tau_1, \tau_2, \tau_3, \sigma, \sigma^2\}$, όπου τ_1, τ_2, τ_3 είναι οι κύκλοι μήκους δύο και σ, σ^2 είναι οι κύκλοι μήκους 3, είναι

$$C_1 = \{1\}, C_2 = \{\tau_1, \tau_2, \tau_3\}, C_3 = \{\sigma, \sigma^2\}.$$

(Γενικά ξέρουμε ότι δύο μεταθέσεις της S_n είναι συζυγή στοιχεία αν και μόνο αν έχουν τον ίδιο τύπο στην ανάλυση σε γινόμενο ξένων ανά δύο κύκλων). Άρα μια βάση του κέντρου της $\mathbb{C}$-άλγεβρας $\mathbb{C}[G]$ είναι

$$\overline{C}_1 = 1,$$
$$\overline{C}_2 = \tau_1 + \tau_2 + \tau_3,$$
$$\overline{C}_3 = \sigma + \sigma^2.$$

7.1.5 Πόρισμα. *Το πλήθος των ανά δύο μη ισόμορφων απλών $\mathbb{C}[G]$-προτύπων είναι το πλήθος των κλάσεων συζυγίας της G.*

Απόδειξη: Έχουμε $\mathbb{C}[G] \simeq M_{n_1}(\mathbb{C}) \times \ldots \times M_{n_s}(\mathbb{C})$ όπου s είναι το πλήθος των ανά δύο μη ισόμορφων απλών $\mathbb{C}[G]$-προτύπων. Υπολογίζοντας κέντρα παίρνουμε $C(\mathbb{C}[G]) \simeq \mathbb{C}^s$. Το ζητούμενο προκύπτει από την Πρόταση 7.1.4.

7.1.6 Πόρισμα. *Μια πεπερασμένη ομάδα G είναι αβελιανή αν και μόνο αν κάθε απλό $\mathbb{C}[G]$-πρότυπο έχει διάσταση ένα.*

Απόδειξη: Αν G αβελιανή, τότε η G έχει $|G|$ κλάσεις συζυγίας, οπότε η σχέση $|G| = n_1^2 + \ldots n_s^2$ δίνει $n_1 = \ldots = n_s = 1$. Αντίστροφα αν $n_1 = \ldots = n_s = 1$, τότε από τη σχέση $|G| = n_1^2 + \ldots + n_s^2$ έπεται ότι $|G| = s$, οπότε η G έχει $|G|$ κλάσεις συζυγίας και άρα είναι αβελιανή.

7.1.7 Παράδειγμα. (*Οι ανάγωγες αναπαραστάσεις αβελιανών ομάδων*). Έστω G αβελιανή ομάδα τάξης n. Από το θεώρημα ταξινόμησης των πεπερασμένων αβελιανών ομάδων γνωρίζουμε ότι η G είναι ισόμορφη με ευθύ γινόμενο κυκλικών ομάδων,

$$G = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r},$$

όπου n_i είναι θετικοί ακέραιοι. Μια παρουσίαση της G με γεννήτορες και σχέσεις είναι:

$$G = \left\langle g_1, \ldots, g_r : g_1^{n_1} = \ldots = g_r^{n_r} = 1,\ g_i g_j = g_j g_i\ \forall i, j \right\rangle.$$

Έστω $\lambda_1, \ldots, \lambda_r \in \mathbb{C}$ με $\lambda_i^{n_i} = 1$. Ορίζουμε την αναπαράσταση $\rho_{\lambda_1 \ldots \lambda_r} : G \to \mathbb{C}^*$

$$\rho_{\lambda_1 \ldots \lambda_r}(g_1^{i_1} \ldots g_r^{i_r}) = \lambda_1^{i_1} \ldots \lambda_r^{i_r}.$$

Το σύνολο $\{\rho_{\lambda_1 \ldots \lambda_r} \mid \lambda_i^{n_i} = 1,\ i = 1, \ldots, r\}$ έχει ακριβώς $n_1 \ldots n_r = n$ στοιχεία και αποτελεί το σύνολο των αναγώγων αναπαραστάσεων της G υπέρ του $\mathbb{C}$.

7.2 Χαρακτήρες

Ορισμός. *Έστω $\rho : G \to GL_n(k)$ αναπαράσταση της G. Ο **χαρακτήρας** του ρ είναι η απεικόνιση*

$$\chi_\rho : G \to k,\ \chi_\rho(g) = Tr(\rho(g)),$$

όπου $Tr(A)$ συμβολίζει το ίχνος $\sum_i a_{ii}$ του πίνακα $A = (a_{ij})$. Ο χαρακτήρας ενός $k[G]$-προτύπου είναι ο χαρακτήρας της αντίστοιχης αναπαράστασης.

Σημείωση. Επειδή όμοιοι πίνακες έχουν το ίδιο ίχνος, παρατηρούμε ότι ισοδύναμες αναπαραστάσεις έχουν τον ίδιο χαρακτήρα. Επιπλέον η τιμή $\chi_\rho(g)$ εξαρτάται μόνο από τη κλάση συζυγίας του g (και όχι από το g αυτό καθευατό).

Παράδειγμα Μετά από μερικές πράξεις με υπολογισμούς πινάκων και ιχνών, βλέπουμε ότι ο χαρακτήρας χ της αναπαράστασης $\rho : D_8 \to GL_2(\mathbb{C})$ του Παραδείγματος 7.1.3 είναι

g	1	a	a^2	a^3	b	ab	a^2b	a^3b
$\chi(g)$	2	0	-2	0	0	0	0	$0.$

Παρατηρούμε ότι αν χ είναι ο χαρακτήρας μιας αναπαράστασης ρ υπέρ του $\mathbb{C}$, $\rho : G \to GL_n(\mathbb{C})$, τότε:

i) Ο βαθμός της ρ είναι η τιμή $\chi(1)$.

ii) Αν m είναι η τάξη του στοιχείου $g \in G$, τότε το $\chi(g)$ είναι άθροισμα m-στών ριζών της μονάδας. Πράγματι, αφού $g^m = 1$ ισχύει $\rho(g)^m = I$ οπότε οι ιδιοτιμές του πίνακα $\rho(g)$ είναι m-στές ρίζες της μονάδας. Το ίχνος του $\rho(g)$ είναι το άθροισμα των ιδιοτιμών του.

iii) Ισχύει $\chi(g^{-1}) = \overline{\chi(g)}$ (ο συζυγής του $\chi(g)$), γιατί αν $\chi(g) = \omega_1 + ... + \omega_n$ με $\omega_i^m = 1$, τότε $\chi(g^{-1}) = \omega_1^{-1} + ... + \omega_n^{-1}$ και $\omega_i^{-1} = \overline{\omega_i}$ για κάθε i.

iv) $\chi(g) \in \mathbb{R}$ αν g και g^{-1} είναι συζυγή. Πράγματι, αν g και g^{-1} είναι συζυγή τότε ισχύει $\chi(g) = \chi(g^{-1}) = \overline{\chi(g)}$.

Ορισμός. *Έστω $\rho : G \to GL_m(\mathbb{C})$, $\rho' : G \to GL_n(\mathbb{C})$ δύο αναπαραστάσεις της G βαθμού m και n αντίστοιχα. Το **ευθύ άθροισμα** των ρ και ρ' είναι η αναπαράσταση $\rho \oplus \rho' : G \to GL_{m+n}(\mathbb{C})$ βαθμού $m+n$ που ορίζεται από*

$$(\rho \oplus \rho')(g) = \begin{pmatrix} \rho(g) & 0 \\ 0 & \rho'(g) \end{pmatrix}.$$

Παρατήρηση. Συνεπώς αν V, V' είναι τα αντίστοιχα $\mathbb{C}[G]$-πρότυπα των ρ, ρ' του παραπάνω ορισμού, τότε το αντίστοιχο $\mathbb{C}[G]$-πρότυπο της αναπαράστασης $\rho \oplus \rho'$ είναι το $V \oplus V'$. Θεωρώντας ίχνη παίρνουμε $\chi_{\rho\oplus\rho'} = \chi_\rho + \chi_{\rho'}$ (όπου στο δεξί μέλος έχουμε τη συνήθη πρόσθεση συναρτήσεων $G \to \mathbb{C}$, δηλαδή $(\chi_\rho + \chi_{\rho'})(g) = \chi_\rho(g) + \chi_{\rho'}(g)$ για κάθε $g \in G$).

Σημειώνουμε ότι η αναπαράσταση $\rho : G \to GL_n(\mathbb{C})$ είναι ανάγωγη αν και μόνο αν δεν υπάρχουν αναπαραστάσεις $\rho_1 : G \to GL_{n_1}(\mathbb{C})$, $\rho_2 : G \to GL_{n_2}(\mathbb{C})$, με $n = n_1 + n_2$ και $\rho = \rho_1 \oplus \rho_2$ (άσκηση).

Ορισμός. *Έστω $\chi, \psi : G \to \mathbb{C}$ συναρτήσεις (όχι αναγκαστικά χαρακτήρες). Ορίζουμε το **εσωτερικό γινόμενο** των χ και ψ*

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g\in G} \chi(g)\overline{\psi(g)}.$$

Παρατηρούμε ότι

i) $\langle \psi, \chi \rangle = \overline{\langle \chi, \psi \rangle}$

ii) $<,>$ είναι γραμμική στην πρώτη μεταβλητή, και

iii) $\langle \chi, \chi \rangle > 0$ αν $\chi \neq 0$.

Επίσης $\langle \chi, \lambda_1\psi_1 + \lambda_2\psi_2 \rangle = \overline{\lambda}_1 \langle \chi, \psi_1 \rangle + \overline{\lambda}_2 \langle \chi, \psi_2 \rangle$ για κάθε $\lambda_1, \lambda_2 \in \mathbb{C}$ και $\chi, \psi_1, \psi_2 : G \to \mathbb{C}$. Σε κάθε περίπτωση οι αποδείξεις είναι άμεσες.

Για χαρακτήρες μπορούμε να πούμε κάτι ισχυρότερο:

7.2.1 Πρόταση. *Έστω χ και ψ χαρακτήρες της G και $g_1, ..., g_s$ ανιιπρόσωποι των κλάσεων συζυγίας της G. Με $C(g_i)$ συμβολίζουμε την κεντροποιούσα ομάδα του g_i, $C(g_i) = \{x \in G \mid xg_i = g_i x\}$. Τότε* *(i)* $\langle \chi,\psi \rangle = \langle \psi,\chi \rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g)\psi(g^{-1}) \in \mathbb{R}$, *και*

(ii) $\langle \chi,\psi \rangle = \sum_{i=1}^{s}\frac{\chi(g_i)\overline{\psi(g_i)}}{|C(g_i)|}$.

Απόδειξη: i) Έχουμε

$$\langle \chi,\psi \rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} = \frac{1}{|G|}\sum_{g\in G}\chi(g)\psi(g^{-1}) = \frac{1}{|G|}\sum_{g^{-1}\in G}\chi(g^{-1})\psi(g) = \langle \psi,\chi \rangle .$$

Αφού $\langle \chi,\psi \rangle = \overline{\langle \psi,\chi \rangle}$, παίρνουμε $\langle \chi,\psi \rangle = \overline{\langle \chi,\psi \rangle}$ και άρα $\langle \chi,\psi \rangle \in \mathbb{R}$ (θα δούμε παρακάτω ότι ισχύει $\langle \chi,\psi \rangle \in \mathbb{N}$).

ii) Έστω C_i η κλάση συζυγίας του g_i. Επειδή $\chi(g)=\chi(g_i)$ και $\psi(g)=\psi(g_i)$ για κάθε $g\in C_i$ έχουμε

$$\langle \chi,\psi \rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\psi(g)} = \sum_{i=1}^{s}\frac{|C_i|}{|G|}\chi(g_i)\overline{\psi(g_i)} .$$

Θυμόμαστε από τις ομάδες (π.χ. δράσεις ομάδων) ότι $|C_i| = [G : C(G_i)]$ (ο πληθάριθμος μιας τροχιάς είναι ο δείκτης της αντίστοιχης σταθεροποιούσας ομάδας). Έτσι $\frac{|C_i|}{|G|} = \frac{1}{|C(g_i)|}$.

Μια συνάρτηση $\psi : G \to \mathbb{C}$ ονομάζεται **συνάρτηση κλάσεων** αν για κάθε $g\in G$ ισχύει $\psi(h^{-1}gh)=\psi(g)$ για κάθε $h\in G$, δηλαδή αν η ψ είναι σταθερή σε κάθε κλάση συζυγίας. Κάθε χαρακτήρας είναι συνάρτηση κλάσεων. Το $\mathbb{C}$-διανυσματικό χώρο των συναρτήσεων κλάσεων συμβολίζουμε με $cf(G)$. Θα αποδείξουμε στη συνέχεια το σημαντικό αποτέλεσμα ότι

οι χαρακτήρες των αναγώγων αναπαραστάσεων της *G* αποτελούν ορθοκανονική βάση του $cf(G)$ ως προς το εσωτερικό γινόμενο $<\ ,\ >$.

Αν $\psi : G \to \mathbb{C}$ είναι συνάρτηση, θα συμβολίζουμε πάλι με $\psi : \mathbb{C}[G] \to \mathbb{C}$ τη γραμμική επέκταση της $G\to\mathbb{C}$ στο $\mathbb{C}[G]\to\mathbb{C}$.

Έστω $V_1,...,V_s$ τα ανά δύο μη ισόμορφα απλά $\mathbb{C}[G]$-πρότυπα και $\chi_1,...,\chi_s$ οι χαρακτήρες τους αντίστοιχα. Οι χ_i ονομάζονται **ανάγωγοι** χαρακτήρες της *G*. Από την άσκηση 2.9 υπάρχουν κεντρικά αυτοδύναμα στοιχεία $e_1,...,e_s \in \mathbb{C}[G]$ με την ιδιότητα $1 = e_1 + ... + e_s$ και $e_i e_j = 0$ για $i \neq j$. Επιπλέον $e_i r_i = r_i$ για κάθε $r_i \in R_i$ και $e_i R_j = 0$ για κάθε $i\neq j$ και $e_i e_j = 0$ για κάθε $i \neq j$, όπου R_i είναι οι απλές συνιστώσες του $\mathbb{C}[G]$, $\mathbb{C}[G] \simeq R_1 \times ... \times R_s$. Συνεπώς ισχύει και $e_i v_i = v_i$ για κάθε $v_i \in V_i$ και $e_i V_j = 0$ για κάθε $i \neq j$.

7.2.2 Λήμμα. *Με τους προηγούμενους συμβολισμούς έχουμε*

$$\chi_i(e_j) = \begin{cases} \dim V_i & \text{αν} \quad i=j \\ 0 & \text{αν} \quad i\neq j \end{cases} .$$

Απόδειξη: Για $i \neq j$ έχουμε $e_j V_i = 0$ και άρα το ίχνος της δράσης του e_j στο V_i είναι μηδέν, δηλαδή $\chi_i(e_j)=0$. Γράφοντας τώρα $1 = e_1 + ... + e_s$ παίρνουμε $\chi_i(1) = \chi_i(e_1) + ... + \chi_i(e_s) \Rightarrow \dim V_i = \chi_i(e_i)$.

7.2.3 Λήμμα. *Έστω χ_{reg} ο χαρακτήρας του $\mathbb{C}[G]$-προτύπου $\mathbb{C}[G]$ (με δράση αριστερό πολλαπλασιασμό). Διατηρώντας τους προηγούμενους συμβολισμούς έχουμε:*

i) $\chi_{reg}(1) = |G|$ *και* $\chi_{reg}(g) = 0$ *για κάθε* $g \in G,\ g \neq 1$.

ii) $\chi_{reg} = \chi_1(1)\chi_1 + ... + \chi_s(1)\chi_s$.

Απόδειξη: i) $\chi_{reg}(1) = \dim \mathbb{C}[G] = |G|$. Έστω $g \in G,\ g \neq 1$. Θεωρούμε τη βάση $G = \{g_1 = g, g_2, ..., g_n\}$ του $\mathbb{C}[G]$. Ο αντίστοιχος πίνακας της δράσης του g έχει μη μηδενικό στοιχείο πάνω στη διαγώνιο αν και μόνο αν $gg_i = g_i$, δηλαδή αν $g = 1$.

ii) Το ζητούμενο προκύπτει αμέσως από τον ισομορφισμό $\mathbb{C}[G] \simeq V_1^{n_1} \oplus ... \oplus V_s^{n_s}$ (βλ. κεφάλαιο 2) και το γεγονός ότι $n_i = \dim V_i = \chi_i(1)$.

7.2.4 Πρόταση. *Με τους προηγούμενους συμβολισμούς ισχύει* $e_i = \dfrac{1}{|G|}\sum_{g \in G} \chi_i(1)\chi_i(g^{-1})g$.

Απόδειξη: Έστω $e_i = \sum_{g \in G} \lambda_g g$, $\lambda_g \in \mathbb{C}$. Θεωρώντας τον χαρακτήρα χ_{reg} της g υπολογίζουμε σύμφωνα με το Λήμμα 7.2.3 i). Έστω $h \in G$.

$$\chi_{reg}(h^{-1}e_i) = \sum_{g \in G} \lambda_g \chi_{reg}(h^{-1}g) = \lambda_h |G|.$$

Από το Λήμμα 7.2.3 ii) έχουμε

$$\chi_{reg}(h^{-1}e_i) = \sum_{j=1}^{s} \chi_j(1) x_j(h^{-1}e_i).$$

Επειδή $e_i R_j = 0$ για $i \neq j$, έχουμε $\chi_j(h^{-1}e_i) = 0$ για $i \neq j$. Για $i = j$ έχουμε $e_i v_i = v_i \quad \forall v_i \in R_i$ και άρα $\chi_i(h^{-1}e_i) = \chi_i(h^{-1})$. Τελικά αντικαθιστώντας έχουμε

$$\lambda_h = \frac{1}{|G|}\sum_{j=1}^{s} \chi_j(1)\chi_j(h^{-1}e_i) = \frac{1}{|G|}\chi_i(1)\chi_i(h^{-1}),$$

απ'όπου προκύπτει το ζητούμενο.

Είμαστε τώρα έτοιμοι να αποδείξουμε το πρώτο κύριο αποτέλεσμα αυτού του κεφαλαίου.

7.2.5 Θεώρημα. *Οι ανάγωγοι χαρακτήρες της G πάνω από το $\mathbb{C}$ αποτελούν ορθοκανονική βάση του $\mathbb{C}$-διανυσματικού χώρου $cf(G)$ ως προς το εσωτερικό γινόμενο $< , >$.*

Απόδειξη: Έστω $\chi_1, ..., \chi_s$ οι ανάγωγοι χαρακτήρες. Θα δείξουμε πρώτα ότι οι $\chi_1, ..., \chi_r$ αποτελούν βάση του $cf(G)$. Γνωρίζουμε ότι s είναι το πλήθος των κλάσεων συζυγίας της G (Πόρισμα 7.1.5). Επειδή η διάσταση του $cf(G)$ είναι s (μια βάση του $cf(G)$ είναι οι χαρακτηριστικές συναρτήσεις $f_i : G \to \mathbb{C}$ που ορίζονται από $f_i(C_j) = 0$ για $i \neq j$ και $f_i(g) = 1$ για κάθε $g \in C_i$) αρκεί να δείξουμε ότι οι $\chi_1, ..., \chi_s$ είναι γραμμικώς ανεξάρτητες. Έστω $\sum_{i=1}^{s} \lambda_i \chi_i = 0$. Από το Λήμμα 7.2.2 παίρνουμε τότε $\lambda_i \chi_i(e_i) = 0$, δηλαδή $\lambda_i \dim V_i = 0$, οπότε $\lambda_i = 0$. (Η γραμμική ανεξαρτησία των χ_i έπεται και από το γεγονός $< \chi_i, \chi_j > = \delta_{ij}$ που θα δείξουμε αμέσως παρακάτω). Θα δείξουμε τώρα ότι $< \chi_i, \chi_i > = 1$. Από τον τύπο της Πρότασης 7.2.4 συμπεραίνουμε ότι ο συντελεστής του $1 \in G$ στο e_i^2 είναι

$$\frac{1}{|G|^2}\chi_i(1)^2\sum_{g\in G}\chi_i(g)\chi_i(g^{-1})$$

που είναι (λόγω της Πρότασης 7.2.1 i)) ίσος με

$$\frac{1}{|G|}\chi_i(1)^2<\chi_i,\chi_i>.$$

Όμως $e_i^2=e_i$ οπότε ο συντελεστής του 1 στο e_i^2 είναι ίσος με (Πρόταση 7.2.4)

$$\frac{1}{|G|}\chi_i(1)^2.$$

Συγκρίνοντας τις δύο τελευταίες εκφράσεις παίρνουμε $<\chi_i,\chi_i>=1$.

Θα δείξουμε τώρα ότι $<\chi_i,\chi_j>=0$ για $i\neq j$. Από τη σχέση $e_ie_j=0$ παίρνουμε λόγω της Πρότασης 7.2.4 ότι

$$\sum_{g,h\in G}\chi_i(g^{-1})\chi_j(h^{-1})gh=0.$$

Ο συντελεστής του $1\in G$ στην προηγούμενη ισότητα δίνει

$$\sum_{g\in G}\chi_i(g)\chi_j(g^{-1})=0$$

οπότε $<\chi_i,\chi_j>=0$ από την πρόταση 7.2.1 i).

7.2.6 Πόρισμα. *Έστω V ένα $\mathbb{C}[G]$-πρότυπο με χαρακτήρα χ. Τότε το V είναι ανάγωγο αν και μόνο αν* $<\chi,\chi>=1$.

Απόδειξη: Αν V είναι ανάγωγο τότε $<\chi,\chi>=1$ από το προηγούμενο θεώρημα. Αντίστροφα, έστω $<\chi,\chi>=1$. Γράφοντας το V ως ευθύ άθροισμα αναγώγων προτύπων $V\simeq V_1^{m_1}\oplus\ldots\oplus V_r^{m_r}$ λαμβάνουμε $\chi=m_1\chi_1+\ldots+m_r\chi_r$ οπότε η σχέση $<\chi,\chi>=1$ δίνει

$$\sum_{i,j}m_im_j<\chi_i,\chi_j>=1.$$

Από το προηγούμενο θεώρημα έχουμε $<\chi_i,\chi_i>=1$ και $<\chi_i,\chi_j>=0$ για $i\neq j$, οπότε

$$m_1^2+\ldots+m_r^2=1.$$

Συνεπώς $m_j=1$ για κάποιο j και $m_i=0$ για $i\neq j$. Άρα $V=V_j$.

Το προηγούμενο πόρισμα είναι ιδιαίτερα χρήσιμο σε υπολογισμούς. Για παράδειγμα, ο χαρακτήρας χ της αναπαράστασης $\rho: D_8\to GL_2(\mathbb{C})$ του Παραδείγματος 7.1.2 υπολογίστηκε στην αρχή της παρούσας παραγράφου και βρήκαμε

g	1	a	a^2	a^3	b	ab	a^2b	a^3b
$\chi(g)$	2	0	-2	0	0	0	0	$0.$

Εύκολα επαληθεύουμε ότι $<\chi,\chi>=1$ και άρα η ρ είναι ανάγωγη.

Το ακόλουθο αποτέλεσμα δείχνει ότι οι χαρακτήρες αναπαραστάσεων επί του $\mathbb{C}$ 'χαρακτηρίζουν' τις αναπαραστάσεις.

7.2.7 Πόρισμα. *Δύο αναπαραστάσεις της G επί του $\mathbb{C}$ είναι ισοδύναμες αν και μόνο αν οι χαρακτήρες τους ταυτίζονται.*

Απόδειξη: Έστω ρ και ρ' αναπαραστάσεις με αντίστοιχους χαρακτήρες χ και χ'. Αν ρ και ρ' είναι ισοδύναμες τότε $\chi = \chi'$ όπως είπαμε στην αρχή της παραγράφου. Αντίστροφα, έστω $\chi = \chi'$. Για τα αντίστοιχα $\mathbb{C}[G]$-πρότυπα γράφουμε $V \simeq V_1^{m_1} \oplus ... \oplus V_r^{m_r}$, $V' \simeq V_1^{m_1} \oplus ... \oplus V_r^{m_r'}$ όπου $V_1,...,V_r$ είναι ανά δύο μη ισόμορφα ανάγωγα $\mathbb{C}[G]$-πρότυπα. Από $<\chi, \chi_i> = <\chi', \chi_i>$ παίρνουμε

$$m_1 < \chi_1, \chi_i > + ... + \; m_r < \chi_r, \chi_i > = \; m_1' < \chi_1, \chi_i > + ... + m_r < \chi_r', \chi_i >,$$

οπότε το Θεώρημα 7.2.5 δίνει $m_i = m_i'$ για κάθε *i*. Άρα $V \simeq V'$.

7.2.8 Πόρισμα. *Έστω V, V' $\mathbb{C}[G]$-πρότυπα με χαρακτήρες χ, χ' αντίστοιχα. Τότε*

$$< \chi, \chi' > = \; \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(V, V').$$

Απόδειξη: Γράφοντας $V \simeq V_1^{m_1} \oplus ... \oplus V_s^{m_s}$ και $V' \simeq V_1^{m_1'} \oplus ... \oplus V_s^{m_s'}$, το θεώρημα δίνει $< \chi, \chi' > = m_1 m_1' + ... + m_s m_s'$. Από την άλλη μεριά έχουμε από το Λήμμα του Schur για αλγεβρικά κλειστά σώματα ότι

$$\mathrm{Hom}_{\mathbb{C}[G]}(V_i, V_j) \cong \begin{cases} \mathbb{C}, & \text{αν} \;\; i = j \\ 0, & \text{αν} \;\; i \neq j \end{cases}.$$

Από την Πρόταση 1.2.2 παίρνουμε $\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(V, V') = m_1 m_1' + ... + m_s m_s'$.

Τονίζουμε ότι στην ειδική περίπτωση που στο προηγούμενο πόρισμα ο χαρακτήρας χ' είναι ανάγωγος, τότε ο μη αρνητικός ακέραιος $< \chi, \chi' >$ ισούται με την πολλαπλότητα του χ' στην παράσταση του χ ως $\mathbb{N}$ -γραμμικός συνδυασμός αναγώγων χαρακτήρων.

7.3 Σχέσεις Ορθογωνιότητας και Πίνακες Χαρακτήρων

Έστω $IrrG = \{\chi_1, ..., \chi_s\}$ το σύνολο των αναγώγων χαρακτήρων της G, $g_1, ..., g_s$ αντιπρόσωποι των κλάσεων συζυγίας της G και $C(g_i) = \{x \in G \mid xg_i = \; g_i x\}$ η κεντροποιούσα ομάδα του g_i. Με $\delta_{\alpha\beta}$ συμβολίζουμε το δέλτα του Kronecker, $\delta_{\alpha\beta} = 0$ εκτός αν $\alpha = \beta$ οπότε $\delta_{\alpha\alpha} = 1$.

7.3.1 Θεώρημα. *Με τους προηγούμενους συμβολισμούς έχουμε:*

*i) **(ορθογώνιες σχέσεις γραμμών)*** $\displaystyle\sum_{i=1}^{s} \frac{\chi_\alpha(g_i)\overline{\chi_\beta(g_i)}}{|C(g_i)|} = \delta_{\alpha\beta}$

*ii) **(ορθογώνιες σχέσεις στηλών)*** $\displaystyle\sum_{i=1}^{s} \chi_i(g_\alpha)\overline{\chi_i(g_\beta)} = \delta_{\alpha\beta} \, |C(g_\alpha)|.$

Απόδειξη: i) Από το Θεώρημα 7.2.5 έχουμε $< \chi_\alpha, \chi_\beta > = \delta_{\alpha\beta}$ οπότε το ζητούμενο προκύπτει από την Πρόταση 7.2.1 ii).

ii) Έστω $\psi_\beta \in cf(G)$ που ορίζεται από $\psi_\beta(g_\alpha) = \delta_{\alpha\beta}$. Λόγω του Θεωρήματος 7.2.5 γράφουμε $\psi_\beta = \lambda_1 \chi_1 + ... + \lambda_s \chi_s$ οπότε παίρνουμε

$$\lambda_i = <\psi_\beta, \chi_i> = \frac{1}{|G|}\sum_{g\in G}\psi_\beta(g)\overline{\chi_i(g)}.$$

Ισχύει $\psi_\beta(g)=1$ αν το g είναι συζυγές του g_β και $\psi_\beta(g)=0$ διαφορετικά. Επειδή επιπλέον ο πληθάριθμος της κλάσης συζυγίας του g_β είναι $|G|/|C(g_\beta)|$, παίρνουμε $\lambda_i = \frac{1}{|C(g_\beta)|}\overline{\chi_i(g_\beta)}$. Άρα

$$\delta_{\alpha\beta} = \psi_\beta(g_\alpha) = \lambda_1\chi_1(g_\alpha)+\ldots+\lambda_s\chi_s(g_\alpha) = \sum_{i=1}^{s}\frac{\chi_i(g_\alpha)\overline{\chi_i(g_\beta)}}{|C(g_\beta)|}.$$

Έστω $IrrG=\{\chi_1,\ldots,\chi_s\}$ και $g_1,\ldots,g_s$ αντιπρόσωποι των κλάσεων συζυγίας της G. Ο **πίνακας χαρακτήρων** της G είναι ένας $s\times s$ πίνακας που στη θέση (i,j) υπάρχει η τιμή $\chi_i(g_j)$.

Παραδείγματα 7.3.2

1. Ο πίνακας χαρακτήρων της κυκλικής ομάδας $\{1,a,a^2\}$ τάξης 3 είναι (Παράδειγμα 7.1.9),

g	1	a	a^2
χ_1	1	1	1
χ_2	1	ω	ω^2
χ_3	1	ω^2	ω

όπου $\omega^3=1$ με $\omega\neq 1$, δηλαδή $\omega^2+\omega+1=0$. Οι ορθογώνιες σχέσεις γραμμών

για τις πρώτες δύο γραμμές δίνουν $\frac{1}{3}+\frac{\overline{\omega}}{3}+\frac{\overline{\omega}^2}{3}=0$, και

για τη δεύτερη γραμμή με τον εαυτό της δίνουν $\frac{1}{3}+\frac{\omega\overline{\omega}}{3}+\frac{\omega^2\overline{\omega}^2}{3}=1$.

Οι ορθογώνιες σχέσεις στηλών

για τις δύο τελευταίες στήλες δίνουν $1+\omega\overline{\omega}^2+\omega^2\overline{\omega}=0$.

2. Οι ορθογώνιες σχέσεις επιτρέπουν συχνά τον προσδιορισμό ολόκληρου του πίνακα χαρακτήρων αν γνωρίζουμε μόνο κάποιο τμήμα του. Για παράδειγμα, ας υποθέσουμε ότι για μια ομάδα G τάξης 12 που έχει 4 κλάσεις συζυγίας γνωρίζουμε το ακόλουθο τμήμα του πίνακα χαρακτήρων

g_i	g_1	g_2	g_3	g_4
$\|C(g_i)\|$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4				

όπου $g_1,\ldots,g_4$ είναι αντιπρόσωποι των κλάσεων συζυγίας και $\omega^2+\omega+1=0$. Από τη σχέση $\chi_1(1)^2+\ldots+\chi_4(1)^2=12$ (θεώρημα 7.2.5 ή θεώρημα 7.3.1 i) για $\alpha=\beta=1$) παίρνουμε $\chi_4(1)=3$. Οι ορθογώνιες σχέσεις στηλών για τις στήλες 1 και 2 δίνουν

$$\sum_{i=1}^{4} \chi_i(g_1)\overline{\chi_i(g_2)} = 0 \Rightarrow 1+1+1+3\overline{\chi_4(g_2)} = 0 \Rightarrow \chi_4(g_2) = -1 .$$

Οι ορθογώνιες σχέσεις στηλών για τις στήλες 1 και 3 δίνουν

$$\sum_{i=1}^{4} \chi_i(g_1)\overline{\chi_i(g_3)} = 0 \Rightarrow 1+\omega+\omega^2 + 3\overline{\chi_4(g_3)} = 0 \Rightarrow \chi_4(g_3) = 0$$

και για τις στήλες 1 και 4 δίνουν

$$\sum_{i=1}^{4} \chi_i(g_1)\overline{\chi_i(g_4)} = 0 \Rightarrow 1+\omega+\omega^2 + 3\overline{\chi_4(g_4)} = 0 \Rightarrow \chi_4(g_4) = 0 .$$

Προσδιορίζεται κατά αυτόν τον τρόπο όλος ο πίνακας χαρακτήρων της G.

Ο προηγούμενος πίνακας χαρακτήρων είναι αυτός της ομάδας A_4.

3. Ως άλλο παράδειγμα ας θεωρήσουμε τη $G = S_3$ που έχει τρεις κλάσεις συζυγίας

$\{1\}$,

$\{(12, (23), (13)\}$,

$\{(123), (132)\}$.

Το Πόρισμα 7.1.5 δίνει $s = 3$ οπότε $n_1 = 1$, $n_2 = 1$, $n_3 = 2$. Μια ανάγωγη αναπαράσταση της S_3 είναι η $\rho : S_3 \ni \sigma \mapsto sign(\sigma) \in \mathbb{C}^*$ που έχει χαρακτήρα $\chi_2 = \chi_\rho$, που δίνεται από $\chi_2(1) = 1$, $\chi_2(12) = -1$, $\chi_2(123) = 1$. Συνεπώς ο πίνακας χαρακτήρων της S_3 έχει τη μορφή

g_i	1	(12)	(123)
$\lvert C(g_i)\rvert$	6	2	3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	a	b

.

Οι ορθογώνιες σχέσεις στηλών για τις στήλες 1 και 2 δίνουν $1+(-1)+2a = 0$ οπότε $a = 0$. Για τις στήλες 1 και 3 δίνουν $1+1+2b = 0 \Rightarrow b = -1$.

4. Θεωρώντας το $\mathbb{C}[S_3]$ ως $\mathbb{C}[S_3]$-πρότυπο με το συνήθη τρόπο, ξέρουμε ότι ο χαρακτήρας του είναι (Λήμμα 7.2.3) $\chi_{reg} = \chi_1 + \chi_2 + 2\chi_3$ όπου οι ανάγωγοι χαρακτήρες χ_i υπολογίστηκαν στο προηγούμενο παράδειγμα.

Θεωρούμε τώρα το $\mathbb{C}[S_3]$ ως $\mathbb{C}[S_3]$-πρότυπο με διαφορετικό τρόπο: $\sigma \cdot \tau = \sigma^{-1}\tau\sigma$. Θα υπολογίσουμε το χαρακτήρα του, έστω ψ, ως γραμμικό συνδυασμό των χ_i.

Έστω $\sigma \in S_3$. Θεωρώντας τα στοιχεία της $S_3 = \{\sigma_1, ..., \sigma_6\}$ ως βάση του $\mathbb{C}[S_3]$, παρατηρούμε ότι ο πίνακας της γραμμικής απεικόνισης $\mathbb{C}[S_3] \to \mathbb{C}[S_3], \tau \to \sigma \cdot \tau$, έχει μη μηδενικό στοιχείο στη θέση i της διαγωνίου αν και μόνο αν $\sigma \cdot \sigma_i = \sigma_i$, δηλαδή αν και μόνο αν $\sigma_i \in C(\sigma)$. Από αυτό έπεται ότι $\psi(\sigma) = \lvert C(\sigma)\rvert$. Επομένως

$$\psi(1) = 6, \psi(12) = 2, \psi(123) = 3 .$$

Υπολογίζοντας με την Πρόταση 7.2.1 ii) βρίσκουμε

$$<\psi, \chi_3> = \frac{6\cdot 2}{6} + \frac{2\cdot 0}{2} + \frac{3\cdot(-1)}{3} = 1.$$

Όμοια $<\psi, \chi_1> = 3$ και $<\psi, \chi_2> = 1$. Άρα $\psi = 3\chi_1 + \chi_2 + \chi_3$.

Ασκήσεις

Στις παρακάτω ασκήσεις με G συμβολίζουμε μια πεπερασμένη ομάδα.

1. Το μη μηδενικό $\chi \in cf(G)$ είναι χαρακτήρας αν και μόνο αν $<\chi, \chi_i> \in \mathbb{N}$ για κάθε ανάγωγο χαρακτήρα χ_i.

2. Αν για τον χαρακτήρα χ ισχύει $\chi(g) = 0 \ \ \forall g \in G,\ g \neq 1$, τότε ο χ είναι της μορφής $m\chi_{reg},\ m \in \mathbb{N}$. Υπόδ: Υπολογίστε το $<\chi, \psi>$ όπου ψ ανάγωγος χαρακτήρας και χρησιμοποιείστε το Λήμμα 7.2.3).

3. Συμπληρώσετε τον πίνακα χαρακτήρων της D_8.

g_i	1	a	a^2	b	ab
$\lvert C(g_i)\rvert$	8	4			
χ_1	1	1		1	1
χ_2	1	1		-1	-1
χ_3	1	-1	1		
χ_4	1	-1	1	-1	
χ_5					

4.

i) Οι ορθογώνιες σχέσεις γραμμών είναι ισοδύναμες με τις ορθογώνιες σχέσεις στηλών.

ii) Έστω M ο πίνακας χαρακτήρων της G. Δείξετε ότι $\det M^2 = \prod_{i=1}^{s} \left|C(g_i)\right|$, όπου $g_1, ..., g_s$ είναι αντιπρόσωποι των κλάσεων συζυγίας της G.

Υπόδειξη: από τις σχέσεις ορθογωνιότητας προκύπτει ότι ο πίνακας $\overline{M}^t M$ είναι διαγώνιος.

iii) Έστω $Irr(G) = \{\chi_1, ..., \chi_s\}$. Τότε $C(G) = \left\{ g \in G \middle| \ \sum_{i=1}^{s} \chi_i(g)\overline{\chi_i(g)} = |G| \right\}$.

7. Έστω χ χαρακτήρας της G. Θέτουμε $\ker \chi = \{g \in G \mid \chi(g) = \chi(1)\}$. Τότε $\ker\chi$ είναι κανονική υποομάδα της G. Αντίστροφα κάθε κανονική υποομάδα της G είναι της μορφής $\ker \chi$ για κάποιο χαρακτήρα χ. Επιπλέον αν $\chi_1, ..., \chi_j$ είναι οι ανάγωγοι χαρακτήρες τότε

$$\ker \chi = \bigcap_j \ker \chi_j$$

όπου το χ_j διατρέχει τους ανάγωγους χαρακτήρες που έχουν την ιδιότητα $<\chi, \chi_j> > 0$. Συμπέρασμα: από τον πίνακα χαρακτήρων της G μπορούμε να βρούμε **όλες** τις κανονικές υποομάδες της G. Βρείτε τώρα όλες τις κανονικές υποομάδες της D_8 από την άσκηση 3.

8. Η G δεν είναι απλή αν και μόνο αν $\chi(g) = \chi(1)$ για κάποιον μη τετριμμένο ανάγωγο χαρακτήρα χ και κάποιο $g \in G,\ g \neq 1$. (Βλ. προηγούμενη άσκηση)

9. Για κάθε χαρακτήρα χ αβελιανής ομάδας ισχύει $<\chi, \chi> \geq \chi(1)$. Αληθεύει το συμπέρασμα για μη αβελιανές ομάδες;

10. Έστω χ ανάγωγος χαρακτήρας της G βαθμού n.

i) Για κάθε $g \in C(G)$ ισχύει $\left|\chi(g)\right| = n$.

ii) Ισχύει $n^2 \leq [G : C(G)]$.

11. Έστω H αβελιανή υποομάδα της G. Τότε κάθε ανάγωγος χαρακτήρας της G έχει βαθμό $\leq [G : H]$. Κατά συνέπεια κάθε ανάγωγος χαρακτήρας της διεδρικής ομάδας $D_{2n} =< a, b : a^n = b^2 = 1,\ ab = ba^{-1} >$ έχει βαθμό 1 ή 2.

12. Έστω $\mathbb{C}[G]$-πρότυπα V, W με αντίστοιχους χαρακτήρες χ, ψ. Τότε ο χαρακτήρας του $V \otimes_{\mathbb{C}} W$ είναι το γινόμενο $\chi\psi$. (Η δράση είναι $g(v\otimes w)=g(v)\otimes g(w)$). Υπόδειξη: υπολογίσετε το ίχνος της δράσης του g παίρνοντας βάσεις των V, W που αποτελούνται από ιδιοδιανύσματα της g.

13. Αν $\chi,\psi\in Irr(G)$ και $\deg\chi=1$, τότε $\chi\psi\in Irr(G)$. (Βλ. προηγούμενη άσκηση και Πόρισμα 7.2.6).

14. Έστω χ ο μοναδικός ανάγωγος χαρακτήρας της S_3 βαθμού 2. Βρείτε την ανάλυση του $\chi^2=\chi\chi$ σε άθροισμα αναγώγων χαρακτήρων.

15. Έστω $\rho: G\to GL_n(\mathbb{C})$ αναπαράσταση.

i) Αν υπάρχει $g\in G$ με $\det(\rho(g))=-1$, δείξτε ότι η G δεν είναι απλή.

ii) Αν το $g\in G$ έχει τάξη 2, τότε ισχύει ένα από τα εξής συμπεράσματα: a) $\chi(g)\equiv\chi(1)\bmod 4$ b) η G έχει κανονική υποομάδα δείκτη 2. Υπόδειξη: Αν V είναι το αντίστοιχο πρότυπο της ρ, μπορούμε να επιλέξουμε βάση του V τέτοια ώστε ο πίνακας της γραμμικής απεικόνισης $V\to V, v\mapsto gv$, είναι διαγώνιος με ±1 στη διαγώνιο.

16. Έστω V,W δυο ανάγωγα $\mathbb{C}[G]$-πρότυπα. Δείξτε ότι το $V\underset{\mathbb{C}}{\otimes}W$ (άσκηση12) εμφυτεύεται στην κανονική αναπαράσταση της G. Υπόδειξη: αρκεί να δειχτεί ότι αν $\chi,\psi,\zeta\in Irr(G)$, τότε $<\chi\psi,\zeta>\le\zeta(1)$.

17. Με το συμβολισμό του Παραδείγματος 7.1.2 έστω $k=\mathbb{C}$.

i) Δείξτε ότι το $\mathbb{C}[S_n]$-πρότυπο $V/\langle v_1+...+v_n\rangle$ είναι ανάγωγο.

ii) Δείξτε ότι $\langle\chi_V,\chi_1\rangle=1$ όπου χ_1 είναι ο τετριμμένος χαρακτήρας της S_n.

18. Να βρεθούν όλες οι ομάδες με ακριβώς 1,2 ή 3 ανάγωγους χαρακτήρες.

19. Έστω G πεπερασμένη υποομάδα της $GL_n(\mathbb{C})$. Αποδείξτε ότι αν $\sum_{g\in G}Tr(g)=0$, τότε $\sum_{g\in G}g=0$.

20. Έστω $\rho: G\to GL_2(\mathbb{C})$ μια αναπαράσταση τέτοια ώστε το 1 είναι ιδιοτιμή του $\rho(g)$ για κάθε $g\in G$. Δείξτε ότι η ρ δεν είναι ανάγωγη.

Υπόδειξη: Υπολογίστε το $\langle\chi,\chi_1\rangle$, όπου χ είναι ο χαρακτήρας της ρ και χ_1 ο τετριμμένος χαρακτήρας της G, συναρτήσει των ιδιοτιμών των $\rho(g)$.

21. Αποδείξτε ότι κάθε πεπερασμένη απλή ομάδα με τάξη όχι δύναμη πρώτου δεν έχει ανάγωγη αναπαράσταση βαθμού 2.

22. Έστω V_n ένας $\mathbb{C}$-διανυσματικός χώρος με $\dim_{\mathbb{C}}V_n=n\ge2$ και $\{v_1,...,v_n\}$ μια βάση του V_n. Ο V_n είναι $\mathbb{C}[S_n]$-πρότυπο με δράση $\sigma v_i=v_{\sigma(i)}$, $\sigma\in S_n$. Με χ_{V_n} συμβολίζουμε το χαρακτήρα του V_n.

Θέτουμε $Fix(\sigma)=\{i\in\{1,...,n\}\,|\,\sigma(i)=i\}$.

i) Δείξτε ότι $\chi_{V_n}(\sigma)=|Fix(\sigma)|$.

ii) Στο ερώτημα αυτό υποθέτουμε ότι $n=3$.

a. Υπολογίστε το εσωτερικό γινόμενο $<\chi_{V_3},\chi_{V_3}>$ και με βάση αυτό αποδείξτε ότι ο χ_{V_3} είναι άθροισμα δύο ανάγωγων χαρακτήρων της S_3. Υπολογίστε τους χαρακτήρες αυτούς.

b. Βρείτε το χαρακτήρα του $V_3\otimes V_3$ και παραστήστε τον ως άθροισμα ανάγωγων χαρακτήρων της S_3.

iii) Θεωρούμε τους υπόχωρους $U_n=\{a_1v_1+...+a_nv_n\,|\,a_1+...+a_n=0\}$ και $W_n=\{a(v_1+...+v_n)\,|\,a\in\mathbb{C}\}$ του V_n.

a. Δείξτε ότι οι παραπάνω υπόχωροι είναι $\mathbb{C}[S_n]$-υποπρότυπα του V_n και ότι $V_n=U_n\oplus W_n$.

b. Δείξτε ότι για κάθε $i=2,...,n$ ισχύει $v_i-v_{i-1}\in U_n$. Με βάση αυτό δείξτε ότι το U_n είναι απλό $\mathbb{C}[S_n]$-πρότυπο.

23. Έστω A ένας $\mathbb{C}$-διανυσματικός χώρος με $\dim_{\mathbb{C}}A=9$ και $\{v_{ij}\,|\,1\le i,j\le3\}$ μια βάση του A. . Ο A

είναι $\mathbb{C}[S_3]$-πρότυπο με δράση $\sigma v_{ij} = v_{\sigma(i)\,\sigma(i)}$, $\sigma \in S_3$. Για παράδειγμα, αν $\sigma = (12)$, τότε $\sigma v_{13} = v_{23}$. Δείξτε ότι $A \simeq \mathbb{C}[S_3] \oplus V_3$, όπου V_3 είναι το $\mathbb{C}[S_3]$-πρότυπο της προηγούμενης άσκησης.

24. Έστω n άρτιος θετικός ακέραιος, $n = 2m$. Ο διανυσματικός χώρος $\mathbb{C}[\mathbb{Z}_m \times \mathbb{Z}_m]$ είναι $\mathbb{C}[\mathbb{Z}_n]$ πρότυπο με εξωτερικό πολλαπλασιασμό που ορίζεται από $([a]_n, ([x]_m, [y]_m)) \mapsto ([a+x]_m, [a+y]_m)$. Παραστήστε το χαρακτήρα του $\mathbb{C}[\mathbb{Z}_m \times \mathbb{Z}_m]$ ως γραμμικό συνδυασμό των ανάγωγων χαρακτήρων της $\mathbb{Z}_n$.
Υπόδειξη: Ίσως είναι χρήσιμο να λύσετε αναλυτικά πρώτα την περίπτωση $m = 3$.

25. Οι αναπαραστάσεις της δικυκλικής ομάδας.

a. Έστω $\rho : G \to GL_2(\mathbb{C})$ μια αναπαράσταση τέτοια ώστε για κάποια $g, h \in G$ έχουμε $\rho(g)\rho(h) \neq \rho(h)\rho(g)$. Αποδείξτε ότι η ρ δεν είναι ανάγωγη.

b. Θεωρούμε την ομάδα (‘δικυκλική’) $T_{4n} = \left\langle a, b : a^{2n} = 1, a^n = b^2, b^{-1}ab = a^{-1} \right\rangle$ που έχει τάξη $4n$.

Έστω r ένας ακέραιος και $\varepsilon_r = e^{\frac{2\pi i r}{2n}} \in \mathbb{C}$. Δείξτε τα εξής.

i. Η αντιστοιχία $a \mapsto \begin{pmatrix} \varepsilon_r & 0 \\ 0 & \varepsilon_r^{-1} \end{pmatrix}$, $b \mapsto \begin{pmatrix} 0 & 1 \\ \varepsilon_r^{\,n} & 0 \end{pmatrix}$ ορίζει μια αναπαράσταση ρ_r της T_{4n}.

ii. Η ρ_r είναι ανάγωγη αν $\varepsilon_r \neq \pm 1$. (Υπόδειξη: ένας τρόπος είναι με το a.).

iii. Οι $\rho_1, \ldots, \rho_{n-1}$ είναι ανά δυο μη ισοδύναμες.

iv. Οι υπόλοιπες ανάγωγες ανά δυο μη ισοδύναμες αναπαραστάσεις της T_{4n} είναι βαθμού 1.

26. Υπολογίστε τον πίνακα χαρακτήρων της S_4 ως εξής.

a. Υπολογίστε τον αριθμό των κλάσεων συζυγίας χρησιμοποιώντας την ανάλυση μεταθέσεων σε γινόμενο ξένων κύκλων. Υπολογίστε τον πληθάριθμο κάθε κλάσης συζυγίας C_{g_i} και το $|C(g_i)| = [G : C_{g_i}]$.

b. Έστω χ_1, χ_2 ο τετριμμένος χαρακτήρας και ο χαρακτήρας προσήμου αντίστοιχα. Έστω χ_4 ο χαρακτήρας $\chi_V - \chi_1$ όπου χ_V ο χαρακτήρας του προτύπου στο παράδειγμα 7.1.2 για $n = 4$. Υπολογίστε τον χ_4 και δείξτε ότι είναι ανάγωγος.

c. Στη συνέχεια θέστε $\chi_5 = \chi_2 \chi_4$ (που είναι ανάγωγος από την άσκηση 13) και υπολογίστε τον. Βρείτε τον τελευταίο χαρακτήρα χ_3 από τις ορθογώνιες σχέσεις.

Δίνεται ο πίνακας χαρακτήρων της S_4 για επαλήθευση.

g_i	1	(12)	(123)	(12)(32)	(1234)
$\lvert C(g_i)\rvert$	24	4	3	8	4
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	-1	2	0
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	-1	1

ΚΕΦΑΛΑΙΟ 8: Εφαρμογή: Το θεώρημα του Burnside

Θα αποδείξουμε εδώ ότι κάθε ομάδα τάξης $p^a q^b$ (p, q πρώτοι) είναι επιλύσιμη. Το θεώρημα αυτό αποδείχτηκε από τον Burnside το 1904 ο οποίος χρησιμοποίησε τη νέα τότε θεωρία αναπαραστάσεων ομάδων που αναπτύχθηκε από τον Frobenius. Για σχεδόν 70 χρόνια δεν υπήρχε απόδειξη που να αποφεύγει χαρακτήρες και αναπαραστάσεις.

8.1 Αλγεβρικοί Ακέραιοι

Ξεκινάμε με ορισμένα στοιχεία που αφορούν αλγεβρικούς ακεραίους. Ένας αριθμός $a \in \mathbb{C}$ ονομάζεται **αλγεβρικός ακέραιος** αν είναι ρίζα ενός μονικού πολυωνύμου $p(x) \in \mathbb{Z}[x]$. Το σύνολο των αλγεβρικών ακεραίων συμβολίζεται με $\mathcal{O}$ και ο σκοπός μας είναι να δείξουμε ότι το $\mathcal{O}$ είναι υποδακτύλιος του $\mathbb{C}$.

8.1.1 Πρόταση. *Έστω $R \subseteq S$ δακτύλιοι και $s \in S$. Τότε τα παρακάτω είναι ισοδύναμα*

(i) το s είναι ακέραιο πάνω από το R (δηλαδή εξ ορισμού είναι ρίζα μονικού πολυωνύμου $p(x) \in R[x]$)

(ii) ο υποδακτύλιος $R[s]$ του S είναι πεπερασμένα παραγόμενο R-πρότυπο

(iii) υπάρχει υποδακτύλιος R' του S έτσι ώστε $R[s] \subseteq R'$ και το R' είναι πεπερασμένα παραγόμενο R-πρότυπο

(iv) υπάρχει πιστό $R[s]$-πρότυπο που είναι πεπερασμένα παραγόμενο R-πρότυπο.

Απόδειξη: (i)$\Rightarrow$(ii) Ως *R*-πρότυπο το $R[s]$ παράγεται από τα $1, s, s^2, \ldots$

Από την υπόθεση έχουμε

$$s^n + r_{n-1}s^{n-1} + \ldots + r_0 = 0$$

για κάποια $r_i \in R$. Άρα $s^n = -r_{n-1}s^{n-1} - \ldots - r_0$ και $s^{n+k} = -r_{n-1}s^{n+k-1} - \ldots - r_0 s^k$, οπότε μια προφανής επαγωγή στο *k* δείχνει ότι το s^{n+k} είναι *R*-γραμμικός συνδυασμός των $1, s, \ldots, s^{n-1}$.

(ii)$\Rightarrow$(iii) Προφανές

(iii)$\Rightarrow$(iv) Το R' είναι πιστό $R[s]$-πρότυπο

(iv)$\Rightarrow$(i) Έστω *M* πιστό $R[s]$-πρότυπο που παράγεται από $m_1, \ldots, m_n$.

Υπάρχουν $r_{ij} \in R$ με

$$\begin{aligned} sm_1 &= r_{11}m_1 + r_{12}m_2 + \ldots + r_{1n}m_n \\ &\cdots \\ sm_n &= r_{n1}m_1 + r_{n2}m_2 + \ldots + r_{nn}m_n, \end{aligned}$$

οπότε

$$\begin{aligned} 0 &= (r_{11} - s)m_1 + r_{12}m_2 + \ldots + r_{1n}m_n \\ &\cdots \\ 0 &= r_{n1}m_1 + r_{n2}m_2 + \ldots + (r_{nn} - s)m_n. \end{aligned}$$

Έστω *A* ο $n \times n$ πίνακας των συντελεστών των m_i στο τελευταίο σύστημα. Γράφουμε αυτό ως

$$0 = A\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

οπότε

$$0 = (adjA)A\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}.$$

Αλλά $(adjA)A = (\det A)I_n$, όπου I_n είναι ο ταυτοτικός $n \times n$ πίνακας, όπως θυμόμαστε από τη Γραμμική Άλγεβρα. (Η απόδειξη που δίνεται εκεί ισχύει και για μεταθετικούς δακτυλίους στη θέση σωμάτων). Άρα

$$(\det A)m_i = 0, \qquad i = 1,...,n .$$

Επειδή το M είναι πιστό $R[s]$-πρότυπο και τα m_i παράγουν το M παίρνουμε

$$\det A = 0 .$$

Το ανάπτυγμα της ορίζουσας $\det A$ δίνει τη ζητούμενη σχέση.

8.1.2 Πόρισμα. *Έστω $R \subseteq S$ δακτύλιοι και $s_1,...,s_n \in S$ στοιχεία ακέραια πάνω από το R. Τότε ο δακτύλιος $R[s_1,...,s_n]$ είναι πεπερασμένα παραγόμενο R-πρότυπο.*

Απόδειξη: Για $n = 1$ δες την προηγούμενη πρόταση. Για $n > 1$ γράφουμε

$$R[s_1,...,s_{n-1}] = R[s_1,...,s_{n-1}][s_n].$$

Το $R[s_1,...,s_{n-1}]$ είναι πεπερασμένα παραγόμενο R-πρότυπο από την υπόθεση της επαγωγής. Το $R[s_1,...,s_{n-1}][s_n]$ είναι πεπερασμένα παραγόμενο $R[s_1,...,s_{n-1}]$ πρότυπο (αφού το s_n είναι ακέραιο πάνω από το R). Συνεπώς το $R[s_1,...,s_n]$ είναι πεπερασμένα R-πρότυπο.

8.1.3 Πόρισμα. *Το σύνολο $\mathbb{C}$ είναι υποδακτύλιος του $\mathbb{C}$.*

Απόδειξη: Έστω $a,b \in \mathcal{O}$. Ο δακτύλιος $\mathbb{Z}[a,b]$ είναι πεπερασμένα παραγόμενο $\mathbb{Z}$-πρότυπο από το πόρισμα 8.1.2 για $R = \mathbb{Z}$ και $S = \mathcal{O}$. Από την πρόταση 8.1.1 συμπεραίνουμε ότι $a - b \in \mathcal{O}$ και $ab \in \mathcal{O}$.

8.1.4 Πρόταση. $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$.

Απόδειξη: Έστω $a/b \in \mathbb{Q}$ με $a,b \in \mathbb{Z}$, μ.κ.δ. $(a,b) = 1$. Αν $a/b \in \mathcal{O}$ τότε έχουμε μια σχέση της μορφής

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + ... + a_0, \quad a_i \in \mathbb{Z}$$

οπότε

$$a^n + a_{n-1}ba^{n-1} + ... + a_0 b^n = 0$$

πράγμα που δίνει ότι το b διαιρεί το a^n. Άρα $b = \pm 1$, οπότε $a/b \in \mathbb{Z}$. Η άλλη σχέση $\mathbb{Z} \subseteq \mathcal{O} \cap \mathbb{Q}$ είναι προφανής.

Επιστρέφουμε τώρα σε χαρακτήρες.

8.1.5 Πρόταση. *Έστω χ χαρακτήρας της G. Τότε για κάθε $g \in G$, $\chi(g) \in \mathcal{O}$.*

Απόδειξη: Κάθε ρίζα της μονάδας είναι αλγεβρικός ακέραιος ως ρίζα του $x^m - 1$. Γνωρίζουμε ότι το $\chi(g)$ είναι άθροισμα ριζών της μονάδας, οπότε το ζητούμε προκύπτει από το πόρισμα 8.1.3.

Κατά συνέπεια οι μόνοι ρητοί αριθμοί που εμφανίζονται στον πίνακα χαρακτήρων της G είναι οι ακέραιοι.

8.2 Θεώρημα του Burnside

8.2.1 Λήμμα. *Έστω V ανάγωγο $\mathbb{C}[G]$-πρότυπο και $z \in C(\mathbb{C}[G])$. Τότε υπάρχει $\lambda \in \mathbb{C}$ με την ιδιότητα $zv = \lambda v$ για κάθε $v \in V$.*

Απόδειξη: Επειδή $z \in C(\mathbb{C}[G])$, η συνάρτηση $f : V \ni v \mapsto zv \in V$ είναι $\mathbb{C}[G]$-ομομορφισμός. Επειδή το $\mathbb{C}$ είναι αλγεβρικά κλειστό και το V ανάγωγο, το ζητούμενο έπεται από το Λήμμα του Schur.

8.2.2 Πρόταση. *Έστω χ ανάγωγος χαρακτήρας της G και $g \in G$. Τότε*

$$\lambda = \frac{|G|}{|C(g)|}\frac{\chi(g)}{\chi(1)} \in \mathcal{O}.$$

Απόδειξη: Έστω $V \subseteq \mathbb{C}[G]$ ανάγωγο $\mathbb{C}[G]$**-**πρότυπο με χαρακτήρα χ και έστω $\overline{C}$ το άθροισμα των συζυγών του g. Από το προηγούμενο λήμμα, υπάρχει $\lambda \in \mathbb{C}$ με

$$\overline{C}v = \lambda v \text{ για κάθε } v \in V. \tag{1}$$

Λαμβάνοντας ίχνη η τελευταία σχέση δίνει $\sum \chi(g') = \lambda\chi(1)$, όπου το g' διατρέχει τα συζυγή στοιχεία του g. Επειδή $\chi(g') = \chi(g)$ και το πλήθος των g' είναι $|G|/C(g)|$ παίρνουμε

$$\lambda = \frac{|G|}{|C(g)|}\frac{\chi(g)}{\chi(1)}.$$

Θεωρούμε τώρα τη γραμμική απεικόνιση

$$f : \mathbb{C}[G] \ni z \mapsto \overline{C}z \in \mathbb{C}[G].$$

Ο πίνακας της f ως προς τη βάση $G = \{g_1,...,g_n\}$ έχει στοιχεία ακέραιους αριθμούς. Κάθε ιδιοτιμή ενός τέτοιου πίνακα είναι αλγεβρικός ακέραιος. Από το (1), το λ είναι ιδιοτιμή της f, και άρα το λ είναι αλγεβρικός ακέραιος.

Από την προηγούμενη πρόταση ο αριθμός $\dfrac{|G|}{|C(g)|}\dfrac{\chi(g)}{\chi(1)}$ είναι αλγεβρικός ακέραιος. Έστω ότι μκδ $\left(\dfrac{|G|}{|C(g)|},\ \chi(1)\right) = 1$. Τότε $a\dfrac{|G|}{|C(g)|} + \ b\,\chi(1) = 1$ για κάποια $a,b \in \mathbb{Z}$, οπότε

$$\frac{\chi(g)}{\chi(1)} = a\frac{|G|}{|C(g)|}\frac{\chi(g)}{\chi(1)} + b\,\chi(g)$$

που είναι αλγεβρικός ακέραιος (πόρισμα 8.1.3). Άρα δείξαμε το εξής.

8.2.4 Πόρισμα. *Με τους προηγούμενους συμβολισμούς, έστω μκδ$\left(\dfrac{|G|}{|C(g)|},\ \chi(1)\right) = 1$. Τότε $\chi(g)/\chi(1) \in \mathcal{O}$.*

Ερχόμαστε τώρα στο τελευταίο προπαρασκευαστικό αποτέλεσμα που αποτελεί το κλειδί για τα θεωρήματα που ακολουθούν. Εδώ θα χρησιμοποιήσουμε λίγη θεωρία Galois. Με $C(\rho(G))$ συμβολίζουμε το κέντρο της ομάδας $\rho(G)$.

8.2.5 Πόρισμα. *Με τους προηγούμενους συμβολισμούς, έστω μκδ$\left(\dfrac{|G|}{|C(g)|},\ \chi(1)\right) = 1$. Έστω $\rho : G \to GL_n(\mathbb{C})$ αναπαράσταση με χαρακτήρα χ. Τότε*

$$\text{ή } \rho(g) \in C(\rho(G)) \quad \text{ή } \chi(g) = 0.$$

Απόδειξη: Επειδή το $\chi(g)$ είναι αθροισμα ριζών της μονάδας (πλήθους $\chi(1)$) η τριγωνική ανισότητα δίνει

$$\left|\frac{\chi(g)}{\chi(1)}\right| \leq 1.$$

Αν ισχύει ισότητα, τότε αυτές οι ρίζες της μονάδας είναι ίσες μεταξύ τους (γιατί;) Ισχυριζόμαστε ότι $\rho(g) \in C(\rho(G))$. Πράγματι, έστω *m* η τάξη του *g*. Τότε $\rho(g)^m = I$, οπότε το ελάχιστο πολυώνυμο του πίνακα $\rho(g)$ διαιρεί το $x^m - 1$ και κατά συνέπεια έχει διακεκριμένες ρίζες. Άρα ο $\rho(g)$ είναι διαγωνίσιμος, και συνεπώς όμοιος με έναν πίνακα της μορφής ωI (γιατί οι ιδιοτιμές του $\rho(g)$ ταυτίζονται). Άρα $\rho(g) = \omega I$ που ανήκει στο κέντρο της $GL_n(\mathbb{C})$.

Έστω τώρα ότι $\left|\frac{\chi(g)}{\chi(1)}\right| < 1$. Θέτουμε $a = \frac{\chi(g)}{\chi(1)}$. Έστω ε μια πρωταρχική *m*-ρίζα της μονάδας, όπου *m* είναι η τάξη του *g*, και $K = \mathbb{Q}(\varepsilon)$ οπότε $a \in K$. Το K είναι επέκταση Galois του $\mathbb{Q}$.

Για κάθε $\sigma \in Gal(K/\mathbb{Q})$, ισχύει $\sigma(a) \leq 1$, γιατί

$$\sigma(a) = \frac{1}{\chi(1)}\sigma(\chi(g)) = \frac{1}{\chi(1)}(\omega_1 + ... + \omega_{\chi(1)})$$

όπου κάθε ω_i είναι *m*-ρίζα της μονάδας. Συνεπώς η υπόθεση $\left|\frac{\chi(g)}{\chi(1)}\right| < 1$ δίνει

$$\left|\prod_{\sigma \in Gal(K,\mathbb{Q})} \sigma(a)\right| < 1.$$

Επειδή $a \in \mathcal{O}$ (πόρισμα 8.2.4), κάθε $\sigma(a) \in \mathcal{O}$ και άρα το $b = \prod_{\sigma \in Gal(K,\mathbb{Q})} \sigma(a) \in \mathcal{O}$. Από την άλλη μεριά, το *b* είναι ρητός αριθμός, γιατί $\sigma(b) = b$ για κάθε $\sigma \in Gal(K,\mathbb{Q})$. Επομένως (πρόταση 8.1.4) $b \in \mathbb{Z}$. Αφού $|b| < 1$ παίρνουμε $b = 0$. Δηλαδή $\sigma(a) = 0$ για κάποιο *σ*, που δίνει βέβαια $a = 0$.

8.2.6 Θεώρημα *(Burnside).* *Έστω G πεπερασμένη ομάδα και C μια κλάση συζυγίας της G με $|C| = p^m$, p πρώτος $m > 0$. Τότε υπάρχει μη τετριμμένη ανάγωγη αναπαράσταση ρ της G με την ιδιότητα το $\rho(C) \subseteq C(\rho(G))$. Συνεπώς η G δεν είναι απλή.*

Απόδειξη: Έστω χ_{reg} ο χαρακτήρας του κανονικού $\mathbb{C}[G]$-προτύπου και $g \in G$, $g \neq 1$. Τότε (λήμμα 7.2.3)

$$0 = \chi_{reg}(g) = \chi_1(1)\chi_1(g) + ... + \chi_s(1)\chi_s(g) = 1 + \chi_2(1)\chi_2(g) + ... + \chi_s(1)\chi_s(g),$$

όπου χ_1 είναι ο χαρακτήρας της τετριμμένης αναπαράστασης. Γράφουμε την προηγούμενη σχέση ως

$$\sum_{i=2}^{s} \chi_i(g)\frac{\chi_i(1)}{p} = -\frac{1}{p}.$$

Επειδή $-\frac{1}{p} \notin \mathcal{O}$ (πρόταση 8.1.4), για κάποιο $i \geq 2$ έχουμε $\chi_i(g)\chi_i(1)/p \notin \mathcal{O}$ (πόρισμα 8.1.3). Επειδή $\chi_i(g) \in \mathcal{O}$ (πρόταση 8.1.5), $\chi_i(1)/p \notin \mathcal{O}$. Δηλαδή το *p* δεν διαιρεί το $\chi(1)$. Άρα

$$\chi_i(g) \neq 0 \text{ και } p \text{ δεν διαιρεί το } \chi_i(1).$$

Άρα μκδ$(|C|, \chi_i(1)) = 1$. Τότε το πόρισμα 8.2.5 δίνει ότι το $\rho(g)$ ανήκει στο κέντρο της $\rho(G)$ για κάθε $g \in C$, όπου *ρ* είναι η ανάγωγη αναπαράσταση με χαρακτήρα χ_i.

Θα δείξουμε τέλος ότι η *G* δεν είναι απλή. Έστω $H = Ker\rho$, που είναι μια κανονική υποομάδα της *G*. Αφού η *ρ* δεν είναι η τετριμμένη αναπαράσταση έχουμε $H \neq G$. Αν ισχύει $H = 1$, τότε $G \simeq \rho(G)$ και το κέντρο της $\rho(G)$ είναι μη τετριμμένο αφού περιέχει το σύνολο $\rho(C)$, όπως δείξαμε πριν. Αν

$C(\rho(G)) = \rho(G)$ τότε η G είναι αβελιανή, και αφού η τάξη της δεν είναι πρώτος (γιατί $|C|= p^m,\ m>0$) η G δεν είναι απλή. Αν $C(\rho(G)) \neq \rho(G)$, τότε το $C(\rho(G))$ είναι μια γνήσια μη τετριμμένη κανονική υποομάδα της $\rho(G)$, δηλαδή η $\rho(G)$ δεν είναι απλή.

Θυμίζουμε ότι μια ομάδα G ονομάζεται **επιλύσιμη** αν υπάρχουν υποομάδες της G

$$1 = G_0 < G_1 < \ldots < G_r < G$$

έτσι ώστε κάθε G_i είναι κανονική στη G_{i+1} και κάθε πηλίκο G_{i+1}/G_i είναι κυκλική τάξης πρώτου αριθμού. Ως ασκήσεις αφήνουμε τις αποδείξεις των εξής υπενθυμίσεων.

Παρατηρήσεις

1) Αν η υποομάδα H της G είναι κανονική με την ιδιότητα η H και η G/H είναι επιλύσιμες, τότε η G είναι επιλύσιμη.

2) Κάθε ομάδα τάξης p^a, p πρώτος, $a > 0$, δεν είναι απλή (υπόδειξη: $C(G) \neq 1$).

Ερχόμαστε τώρα στο φημισμένο θεώρημα του Burnside.

8.2.7 Θεώρημα (Burnside)*. Κάθε ομάδα τάξης $p^a q^b$, όπου p, q είναι πρώτοι αριθμοί, είναι επιλύσιμη.*

Απόδειξη: Το θεώρημα είναι προφανές για $a+b=1$ οπότε υποθέτουμε ότι $a+b \geq 2$. Θα δείξουμε πρώτα ότι η G δεν είναι απλή.

Αν $a=0$ ή $b=0$, τότε η G δεν είναι απλή από την παρατήρηση 2 που επισημάναμε πριν το θεώρημα. Έστω $a,b>1$. Έστω Q μια q-Sylow υποομάδα της G, οπότε $|Q|= q^b$. Τότε $C(Q) \neq 1$, από την παρατήρηση 2. Έστω $g \in C(Q),\ g \neq 1$. Τότε $Q \subseteq C_G(g)$ και άρα ο πληθάριθμος της κλάσεως συζυγίας του g, έστω C, είναι

$$|C|=[G:C_G(g)] = p^r$$

για κάποιο r. Αν $r=0$, τότε $g \in C(G)$, οπότε η G δεν είναι απλή, αφού $<g>$ είναι γνήσια μη τετριμμένη κανονική υποομάδα της G. Αν $r \neq 0$, τότε η G δεν είναι απλή από το θεώρημα 8.2.6.

Έχοντας αποδείξει ότι η G δεν είναι απλή, μια προφανής επαγωγή στο $a+b$ βασιζόμενη στην παρατήρηση 1 δίνει το αποτέλεσμα.

Όπως έχουν τονίσει ήδη, υπάρχουν αποδείξεις του θεωρήματος 8.2.7 που αποφεύγουν χαρακτήρες. Το ίδιο όμως δεν συμβαίνει για το θεώρημα 8.2.6 μέχρι σήμερα.

Ασκήσεις

1. Κάθε μη αβελιανή απλή ομάδα ταξης ≤ 69 έχει ταξη 60 (Υπόδειξη: για να αποκλείσετε τις περιπτώσεις 30 και 42 εφαρμόστε τα θεωρήματα Sylow).

2. Κάθε μη αβελιανή απλή ομάδα δεν έχει αβελιανή υποομάδα δείκτη p^r, p πρώτος.

3. Έστω χ ανάγωγος χαρακτήρας της G. Τότε το $\chi(1)$ διαιρεί $|G|$.

Υπόδειξη: Έστω $g_1, \ldots, g_s$ αντιπρόσωποι των κλάσεων συζυγίας. Από την πρόταση 8.2.2,

$$\sum_{i=1}^{s} \frac{|G|}{|C(g_i)|} \frac{\chi(g_i)\overline{\chi(g_i)}}{\chi(1)} \in \mathcal{O}.$$

4. Από τη στοιχειώδη θεωρία ομάδων γνωρίζετε ότι κάθε ομάδα τάξης p^2, p πρώτος, είναι αβελιανή. Δώστε μια άλλη απόδειξη.
Υπόδειξη: προηγούμενη άσκηση.

5. Ο πίνακας χαρακτήρων της S_n αποτελείται μόνο από ακέραιους αριθμούς.