Εισαγωγή στη Μη Μεταθετική Άλγεβρα

$$
\begin{tikzcd}
 & & \bigoplus_{[g]\in\mathcal{C}(G)} \mathbf{C}[g] \arrow[dd, bend left, "{``\chi_V''}"] \\
\mathbf{C}G \arrow[urr, "F"] \arrow[r, "\pi"] \arrow[drr, "\chi_V"'] & {\mathbf{C}G\big/[\mathbf{C}G,\mathbf{C}G]} \arrow[ur, "\overline{F}"] \arrow[dr, "\overline{\chi}_V"] & \\
 & & \mathbf{C}
\end{tikzcd}
$$

Πρόχειρες Σημειώσεις

Τμήμα Μαθηματικών ΕΚΠΑ
Αθήνα, 2025

Πρόλογος

Στο Εαρινό εξάμηνο του ακαδημαϊκού έτους 2022-2023 παρακολούθησα το μεταπτυχιακό μάθημα "Αλγεβρα ΙΙ" που διδάχθηκε από τον Ιωάννη Εμμανουήλ στο Τμήμα Μαθηματικών του ΕΚΠΑ. Το παρόν αρχείο προέκυψε από τις σημειώσεις που κράτησα κατά τη διάρκεια του μαθήματος, στις οποίες πρόσθεσα επιπλέον κεφάλαια, προτάσεις, παρατηρήσεις, πορίσματα και μια "τελική εξέταση" για αυτοαξιολόγηση. Δεν μπορώ, βέβαια, να εγγυηθώ ότι έκανα αυτολεξεί αντιγραφή από τις παραδόσεις, αλλά μπορώ να εγγυηθώ ότι το παρόν κείμενο έχει διορθωθεί επανειλημμένα από έμενα τον ίδιο, συνεπώς είμαι υπεύθυνος για τα λάθη που μπορεί να υπάρχουν και θα ήμουν ευγνώμων αν ο αναγνώστης εντόπιζε κάποιο και μου το επισήμανε στο e-mail μου[1].

Δημήτρης Γιαννακάρας
Σεπτέμβριος 2025

[1] giannakarasdimitris@gmail.com

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Δακτύλιοι και Πρότυπα

1.1 Δακτύλιοι

Ορισμός 1.1.1. *Έστω $(R, +, \cdot)$ ένας δακτύλιος. Ορίζω $R^{op} = (R, +, *)$ τον αντίστροφο δακτύλιο να είναι ο δακτύλιος ορισμένος στο ίδιο σύνολο R, με την ίδια πρόσθεση και με πολλαπλασιασμό $a * b := b \cdot a$ για κάθε $a, b \in R$.*

Ορισμός 1.1.2. *Έστω $R = (R, +, \cdot)$ ένας δακτύλιος. Μια αβελιανή υποομάδα $(I, +) \subseteq (R, +)$ καλείται :*

- *Αριστερό ιδεώδες αν για κάθε $r \in R$ και $x \in I$ είναι $r \cdot x \in I$*
- *Δεξιό ιδεώδες αν για κάθε $r \in R$ και $x \in I$ είναι $x \cdot r \in I$*
- *Αμφίπλευρο ιδεώδες αν για κάθε $r \in R$ και $x \in I$ είναι $r \cdot x \in I$ και $x \cdot r \in I$.*

Ορισμός 1.1.3. *Ένας δακτύλιος D καλείται διαιρετικός, αν κάθε $d \in D$ έχει αντίστροφο, δηλαδή υπάρχει $d' \in D$ με $dd' = d'd = 1$. Ένας μεταθετικός διαιρετικός δακτύλιος καλείται σώμα.*

Παραδείγματα (Δακτυλίων). *(i) Έστω R δακτύλιος και $n \in \mathbf{N}$, θεωρώ το σύνολο των $n \times n$ πινάκων με εγγραφές από τον δακτύλιο R :*

$$\mathbf{M}_n(R) = \{A = (a_{ij}) : a_{ij} \in R \text{ και } 1 \leq i, j \leq n\}$$

Ο $\mathbf{M}_n(R)$ αποτελεί δακτύλιος με πράξεις την πρόσθεση και πολλαπλασιασμό πινάκων. Η αναστροφή πινάκων $A \longmapsto A^T$ επάγει ισομορφισμό δακτυλίων $\mathbf{M}_n(R^{op}) \simeq (\mathbf{M}_n(R))^{op}$.

(ii) Έστω $(M, +)$ μια αβελιανή ομάδα , όριζω

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

Το σύνολο των ενδομορφισμών του M εφοδιάζεται με την δομή δακτυλίου με μονάδα, με πράξεις την κατα σημείο πρόσθεση και σύνθεση απεικονίσεων. Μονάδα είναι η ταυτοτική απεικόνιση $1_M : M \to M$.

(iii) Εστω $\mathbf{F}$ σώμα και V ένας διανυσματικός χώρος επί του $\mathbf{F}$, τότε το σύνολο

$$\mathcal{L}(V) = \{f : V \to V \mid f \ \ \mathbf{F}\text{-γραμμικη}\}$$

αποτελεί δακτύλιος και αν $\dim_{\mathbf{F}} V = n$, τότε $\mathcal{L}(V) \simeq \mathbf{M}_n(\mathbf{F})$

(iv) Αν $(\mathcal{H}, \langle \cdot, \cdot \rangle)$ χώρος Hilbert, θεωρώ το σύνολο των φραγμένων τελεστών :

$$B(\mathcal{H}) = \{f : \mathcal{H} \to \mathcal{H} \mid f \text{ γραμμικη και συνεχής}\}$$

Ο $B(\mathcal{H})$ αποτελεί δακτύλιος με πράξεις την πρόσθεση και σύνθεση τελεστών.

Ορισμός 1.1.4. *Έστω $\Bbbk$ μεταθετικός δακτύλιος και G ομαδα. Για κάθε απεικόνιση $f : G \to \Bbbk$ θεωρούμε τον φορέα (support) supp$(f) := \{g \in G : f(g) \neq 0_{\Bbbk}\}$. Ορίζουμε*

$$\Bbbk G := \{f : G \to \Bbbk \mid \#\mathit{supp}(f) < \infty\}$$

Δίνουμε στο σύνολο $\Bbbk G$ δομή δακτυλίου με τις εξής πράξεις :

- *Πρόσθεση (κατά σημείο) : $f + h \in \Bbbk G$, καθώς supp$(f + h) \subseteq$ supp$(f) \cup$ supp(h)*
- *Πολλαπλασιασμός (συνέλιξη) : $f * h \in \Bbbk G$, καθώς supp$(f * h) \subseteq$ supp$(f) \cdot$ supp(h), όπου*

$$(f * h)(g) = \sum_{x,y\in G, xy=g} f(x)g(y)$$

- *Μόναδα την συνάρτηση dirac στο μοναδιαίο στοιχείο $e \in G$:*

$$\delta_e(g) = \begin{cases} 1 & g = e \\ 0 & g \neq e \end{cases}$$

Ο δακτύλιος $(\Bbbk G, +, *)$ ονομάζεται ομαδοδακτύλιος.

Παρατήρηση. *Το να ορίσω μια απεικόνιση $f : G \to \Bbbk$ είναι ακριβώς το να πω ότι στην θέση g, έχουμε την τιμή $f(g) \in \Bbbk$. Έτσι, μπορούμε να δούμε τον $\Bbbk G$ σαν τα τυπικά αθροίσματα :*

$$\Bbbk G = \left\{ \sum_{g\in G} \lambda_g g : \lambda_g \in \Bbbk \text{ για κάθε } g \in G \text{ και } \lambda_g \neq 0_{\Bbbk} \text{ για πεπερασμένα } g \in G \right\}$$

Η αντίστοιχη πρόσθεση και πολλαπλασιασμός είναι :

$$\sum_{g\in G} \lambda_g g + \sum_{g\in G} \mu_g g = \sum_{g\in G} (\lambda_g + \mu_g) g$$

$$\left(\sum_{g\in G} \lambda_g g\right) * \left(\sum_{g\in G} \mu_g g\right) = \sum_{g,h\in g} \lambda_g \mu_h \cdot gh = \sum_{x\in G} \left(\sum_{gh=x} \lambda_g \mu_h\right) \cdot x$$

με μονάδα να είναι $1_{\Bbbk} \cdot e$.

Παράδειγμα. *Έστω η ομάδα S_3 των μεταθέσεων με 3 σύμβολα και θεωρώ τον δακτύλιο $\mathbf{C}S_3$, τότε τα στοιχεία $\alpha = \sqrt{3} \cdot (1\ 2) + i \cdot (1\ 2\ 3) + 2 \cdot (1\ 3)$ και $\beta = (1 + i) \cdot (1\ 2) + 7 \cdot (1\ 2\ 3)$ ανήκουν στον δακτύλιο $\mathbf{C}S_3$ και έχουν άθροισμα και γινόμενο*

$$\alpha + \beta = (\sqrt{3} + 1 + i) \cdot (1\ 2) + (7 + i) \cdot (1\ 2\ 3) + 2 \cdot (1\ 3)$$

$$\alpha\beta = \sqrt{3}(1 + i) \cdot 1_{S_3} + (-1 + i) \cdot (1\ 3) + 2(1 + i) \cdot (1\ 2\ 3) + 7\sqrt{3} \cdot (2\ 3) + 7i \cdot (1\ 3\ 2) + 14 \cdot (1\ 2)$$

αντίστοιχα.

Ορισμός 1.1.5 (Πράξεις μεταξύ ιδεωδών). *Έστω R δακτύλιος και $I, J \subseteq R$ αριστερά ιδεώδη τότε ορίζονται*

- *το $I \cap J \subseteq R$ είναι αριστερό ιδεώδες και μάλιστα είναι το μέγιστο ιδεώδες που περιέχεται στα I, J*
- *το $I + J \subseteq R$ είναι αριστερό ιδεώδες και μάλιστα είναι το έλαχιστο ιδεώδες που περιέχει και το I και το J*
- *το $IJ := \left\{ \sum_{i=1}^{n} x_i y_i : n \in \mathbf{N},\ x_i \in I, y_i \in J \right\}$ είναι ένα αριστερό ιδεώδες.*

1.2 Πρότυπα

Ορισμός 1.2.1. *Έστω R ένας δακτύλιος. Ένα αριστερό R-πρότυπο είναι μια αβελιανή ομάδα $(M, +)$ εφοδιασμένη με έναν ομομορφισμό δακτυλίων $\ell : R \to \mathrm{End}(M, +)$. Ισοδύναμα, η αβελιανή ομάδα $(M, +)$ εφοδιάζεται με έναν εξωτερικό πολλαπλασιασμό από τον δακτύλιο R, τέτοιος ώστε*

- $1_R \cdot x = x$ *για κάθε* $x \in M$.
- $(r + s) \cdot x = r \cdot x + s \cdot x$ *για κάθε* $x \in M$ *και κάθε* $r, s \in R$.
- $r \cdot (x + y) = r \cdot x + r \cdot y$ *για κάθε* $x, y \in M$ *και κάθε* $r \in R$.
- $(rs) \cdot x = r \cdot (s \cdot x)$ *για κάθε* $x \in M$ *και κάθε* $r, s \in R$.

Αν ορίσουμε έναν εξωτερικό πολλαπλασιασμό, όπως παραπάνω, τότε ο αντιστοιχός ομομορφισμός $\ell : R \to \mathrm{End}(M, +)$ είναι αυτός με $\ell(r) = (r \longmapsto r \cdot x) \in \mathrm{End}(M, +)$. Αντίστροφα, αν μας δωθεί ένας ομομορφισμός $\ell : R \to \mathrm{End}(M, +)$, τότε εύκολα βλέπουμε ότι η πράξη $r \cdot x := \ell(r)(x)$ ικανοποιεί τα παραπάνω. Τέλος, ένα δεξί R-πρότυπο είναι ένα αριστερό R^{op}-πρότυπο και σε αυτήν την περίπτωση γράφουμε την πράξη από τα δεξιά, δηλαδή $x \cdot r$. Αν ο R είναι μεταθετικός, τα αριστερά R-πρότυπα ταυτίζονται με τα δεξιά, αφού τότε $R \simeq R^{op}$.

Ορισμός 1.2.2. *Ο μηδενιστής $ann_R M$ ενός R-προτύπου ορίζεται ως εξής :*

$$ann_R M := \{r \in R : rx = 0_M\} = \ker[R \xrightarrow{\ell} \mathrm{End}(M, +)]$$

όπου ℓ ο ομομορφισμός που δίνει την δομή του R-προτύπου στην αβελιανή ομάδα $(M, +)$. Είναι προφανές ότι ο μηδενιστής αποτελεί ιδεώδες.

Παραδείγματα. (i) *Αν $\mathbf{F}$ σώμα, τότε τα $\mathbf{F}$-πρότυπα είναι ακριβώς οι $\mathbf{F}$-διανυσματικοί χώροι.*

(ii) *Τα $\mathbf{Z}$-πρότυπα είναι ακριβώς οι αβελιανές ομάδες. Υπάρχει ένας μοναδικός ομομορφισμός δακτυλίων $\ell : \mathbf{Z} \to \mathrm{End}(M, +)$. Πράγματι,*

$$\ell(n) = \ell(n \cdot 1) = n \cdot \ell(1) = n \cdot 1_M \in \mathrm{End}(M, +)$$

(iii) *Έστω $\mathbf{F}$ σώμα, ένας $\mathbf{F}$-διανυσματικός χώρος V και $\varphi : V \to V$ μια γραμμική απεικόνιση. Ορίζω στην αβελιανή ομάδα $(V, +)$ την δομή ενός $\mathbf{F}[x]$-προτύπου, θέτοντας :*

$$f(x) \bullet v = f(\varphi(v))$$

για κάθε $f(x) \in \mathbf{F}[x]$ και $v \in V$. Για παράδειγμα $(2x^2 - x + 16) \bullet v = 2\varphi^2(v) - \varphi(v) + 16v$.

(iv) *Έστω R ένας δακτύλιος και $I \subseteq R$ ένα αριστερό ιδεώδες. Το I είναι ένα αριστερό R-πρότυπο με πρόσθεση και βαθμωτό πολλαπλασιασμό του R.*

(v) *Σε μια αβελιανή ομάδα $(M, +)$, μπορώ να ορίσω μια φυσιολογική δομή $\mathrm{End}(M, +)$-προτύπου, ως εξής :*

$$f \bullet x = f(x) \in M$$

για κάθε $f \in \mathrm{End}(M, +)$ και $x \in M$. Ειδικές περιπτώσεις του παραδείγματος αυτού είναι :

- *Έστω R δακτύλιος και n φυσικός αριθμός, τότε ο R^n λαμβάνει την δομή $\mathbf{M}_n(R)$-προτύπου θέτοντας $A \bullet v := Av$ για κάθε $A \in \mathbf{M}_n(R)$ και $v \in R^n$*
- *Αν $\mathcal{H}$ χώρος Hilbert, τότε ο $\mathcal{H}$ λαμβάνει την δομή $B(\mathcal{H})$-προτύπου θέτοντας $T \bullet v = T(v) \in \mathcal{H}$ για κάθε $T \in B(\mathcal{H})$ και $v \in H$*

(vi) *Έστω R δακτύλιος και $(M_\lambda)_{\lambda\in\Lambda}$ οικογένεια R-προτύπων. Το καρτεσιανό γινόμενο $M = \prod_\lambda M_\lambda$ λαμβάνει την δομή R-προτύπου, θέτοντας :*

$$(x_\lambda)_\lambda + (y_\lambda)_\lambda = (x_\lambda + y_\lambda)_\lambda$$

$$r(x_\lambda)_\lambda = (rx_\lambda)_\lambda$$

Το υποσύνολο

$$M' = \{(x_\lambda)_\lambda \in M : x_\lambda \neq 0_{M_\lambda} \text{ για πεπερασμένα το πλήθος } \lambda \in \Lambda\} \subseteq M$$

με τις ίδιες πράξεις, αποτελεί R-πρότυπο. Το υποσύνολο αυτό καλείται το το ευθύ άθροισμα της οικογένειας $(M_\lambda)_{\lambda\in\Lambda}$ και συμβολίζεται :

$$M' = \bigoplus_{\lambda\in\Lambda} M_\lambda$$

Παρατηρώ ότι αν $\#\Lambda < \infty$, τότε $M' = M$.

(vii) *Έστω $\varphi : S \to R$ ομομορφισμός δακτυλίων και M ένα R-πρότυπο. Μπορώ να ορίσω στην αβελιανή ομάδα $(M, +)$ την δομή ενός S-προτύπου, θέτοντας :*

$$s \bullet x = \varphi(s) \cdot x$$

για κάθε $s \in S$ και $x \in M$. Δηλαδή οι ομομορφισμοί $\varphi : S \to R$ και $\ell : R \to \mathrm{End}(M, +)$, επάγουν τον ομομορφισμό $\ell \circ \varphi : S \to \mathrm{End}(M, +)$.

$(viii)$ *Έστω R δακτύλιος και $I \subseteq R$ ιδεώδες. Τα R/I-πρότυπα M είναι ακριβώς τα R-πρότυπα M, με $I \subseteq ann_R M$. Πράγματι, αν M ένα R/I-πρότυπο, μπορώ να ορίσω την δομή R-προτύπου μεσώ της απεικόνισης πηλίκο $\pi : R \to R/I$ με τον φυσιολογική τρόπο και παρατηρώ ότι για $r \in I$:*

$$r \bullet x = \pi(r)x = (r + I)x = 0_{R/I}x = 0_M$$

άρα $I \subseteq ann_R M$. Αντίστροφα, έστω M ένα R-πρότυπο με $I \subseteq ann_R M$, τότε θέτω :

$$(r + I) \bullet x = rx$$

Η πράξη είναι καλά ορισμένη. Πράγματι, αν $r_1 + I = r_2 + I$, τότε $r_1 - r_2 \in I \subseteq ann_R M$, άρα $(r_1 - r_2)x = 0_M \iff r_1 x = r_2 x \iff (r_1 + I) \bullet x = (r_2 + I) \bullet x$. Με λίγα λόγια αν $\ell : R \to \mathrm{End}(M, +)$ ένας ομομορφισμός και $I \subseteq R$ ένα ιδεώδες με $I \subseteq \ker \ell = ann_R M$, τότε ο ομομορφισμός ℓ παραγοντοποείται στον $\overline{\ell} : R/I \to \mathrm{End}(M, +)$.

Ορισμός 1.2.3. *Έστω M ένα R-πρότυπο. Ένα R-υποπρότυπο N είναι μια αβελιανή υποομάδα της $(M, +)$, τέτοια ώστε για κάθε $r \in R$ και $x \in N$, $rx \in N$.*

Παραδείγματα. (i) *Τα R-υποπρότυπα του R είναι τα ιδεώδη $I \subseteq R$.*

(ii) *Έστω $\mathbf{F}$ σώμα , V ένας $\mathbf{F}$-διανυσματικός χώρος και $\varphi : V \to V$ μια γραμμική απεικόνιση, τότε ορίζουμε το $\mathbf{F}[x]$-πρότυπο V. Τα $\mathbf{F}[x]$-υποπρότυπα είναι ακριβώς οι φ-αναλλοίωτοι υπόχωροι του V.*

Παρατήρηση. *Αν $A, B, C \subseteq M$ είναι υποπρότυπα, είναι αληθές ότι η πρόσθεση προτύπων μετατίθεται με την τομή, δηλαδή $(A \cap C) + (B \cap C) = (A + B) \cap C$; Ισχύει καθολικά ο εγκλείσμος $(A \cap C) + (B \cap C) \subseteq (A + B) \cap C$, δεν ισχύει όμως πάντα ισότητα. Πράγματι, έστω τα $\mathbf{R}$-πρότυπα ($\mathbf{R}$-διανυσματικοί χώροι)*

$$A = \{(x, 0) \in \mathbf{R}^2 \ : \ x \in \mathbf{R}\}, \ \ B = \{(0, y) \in \mathbf{R}^2 \ : \ y \in \mathbf{R}\} \ \ , C = \{(z, z) \in \mathbf{R}^2 \ : \ z \in \mathbf{R}\}$$

τότε παρατηρούμε ότι $(A \cap C) + (B \cap C) = 0 \subsetneq C = (A + B) \cap C$. *Αν όμως ισχύει ότι* $A \subseteq C$, *τότε έχουμε ισότητα. Αν* $z \in (A + B) \cap C$, *τότε υπάρχουν* $x \in A, y \in B$ *με* $z = x + y$ *και* $z \in C$. *Αφού* $A \subseteq C$, *έχουμε* $x \in C$ *και άρα* $y = x - z \in C$. *Τέλος* $x \in A \cap C$ *και* $y \in B \cap C$, *άρα* $z \in (A \cap C) + (B \cap C)$.

Πρόταση 1.2.1 (Ταυτότητα Modularity). *Έστω* M *ένα* R*-πρότυπο και* $A, C \subseteq M$ *υποπρότυπα με* $A \subseteq C$. *Αν υπάρχει υποπρότυπο* $B \subseteq M$, *με* $A \cap B = C \cap B$ *και* $A + B = C + B$, *τότε* $A = C$.

Απόδειξη : Από την προηγούμενη παρατήρηση, έχουμε $A+(B\cap C) = (A+B)\cap C$ και από υπόθεση $A \cap B = C \cap B$, άρα $A = A + (A \cap B) = A + (C \cap B) = (A + B) \cap C = (C + B) \cap C = C$ □

Ορισμός 1.2.4. *Έστω* M *ένα* R*-πρότυπο και* $A, B \subseteq C$ *υποπρότυπα του με* $A\cap B = 0$ *και* $A+B = M$. *Τότε λέμε ότι το* M *είναι το ευθύ άθροισμα των* A, B *και γράφουμε* $A \oplus B = M$.

Ορισμός 1.2.5. *Έστω* M *ένα* R*-πρότυπο και* $X \subseteq M$ *ένα αυθαίρετο σύνολο και* $x \in X$, *τότε*

- *Το υποπρότυπο* $Rx := \{rx : r \in R\}$ *είναι το μικρότερο πρότυπο του* M *που περιέχει το* $x \in M$. *Το υποπρότυπο* Rx *καλείται το κυκλικό πρότυπο που παράγεται από το στοιχείο* x.
- *Αν* $X \subseteq M$ *ένα σύνολο, το* $\sum_{x\in X} Rx := \left\{ \sum_{i=1}^{n} r_i x_i : n \in \mathbf{N},\ r_i \in R,\ x_i \in X \right\}$ *είναι το ελάχιστο υποπρότυπο που περιέχει το σύνολο* X. *Το υποπρότυπο* $\sum_{x\in X} Rx$ *καλείται το υποπρότυπο που παράγεται από το σύνολο* X.

Έστω M *ένα* R*-πρότυπο και* $(N_\lambda)_{\lambda\in\lambda}$ *μια οικογένεια υποπροτύπων του, τότε*

- *Η τομή* $\bigcap_{\lambda\in\Lambda} N_\lambda$ *είναι ένα υποπρότυπο του* M *και είναι το μεγαλύτερο υποπρότυπο που περιέχει όλα τα* N_λ.
- *Το άθροισμα* $\sum_{\lambda\in\Lambda} N_\lambda$ *λέγεται ευθύ άθροισμα και γράφω* $\sum_{\lambda\in\Lambda} N_\lambda = \bigoplus_{\lambda\in\Lambda} N_\lambda$ *αν* $N_{\lambda_0} \cap \sum_{\lambda\in\Lambda\setminus\{\lambda_0\}} N_\lambda = 0$ *για κάθε* $\lambda_0 \in \Lambda$. *Στην περίπτωση αυτή για κάθε* $x \in \sum_{\lambda\in\Lambda} N_\lambda$ *υπάρχουν μοναδικά* $x_\lambda \in N_\lambda$ *με* $x_\lambda \neq 0$ *για πεπερασμένα* $\lambda \in \Lambda$, *ώστε* $x = \sum_{\lambda\in\Lambda} x_\lambda$[1]

Ορισμός 1.2.6. *Το* R*-πρότυπο* M *καλείται πεπερασμένα παραγόμενο, αν υπάρχει πεπερασμένο σύνολο* $X \subseteq M$, *τέτοιο ώστε* $M = \sum_{x\in X} Rx$.

Παράδειγμα (Ένα πεπερασμένα παραγόμενο πρότυπο με μη πεπερασμένα παραγόμενο υποπρότυπο). *Έστω* R *ενας δακτύλιος, τότε το* R*-πρότυπο* R *είναι πεπερασμένα παραγόμενο από το μονοσύνολο* $\{1_R\}$. *Συνεπώς αρκεί να βρω έναν δακτύλιο με ένα μη πεπερασμένα παραγόμενο ιδεώδες. Έστω* $R = \mathcal{C}[0, 1] = \{f : [0, 1] \to \mathbf{R} : f$ *συνεχής*$\}$ *και θεωρώ το ιδεώδες* $I \subseteq R$ *με*

$$I = \{f \in R : \exists\, \varepsilon > 0,\ \text{ώστε } f(t) = 0 \text{ για κάθε } t \in [0, \varepsilon]\}$$

Το I *δεν είναι πεπερασμένα παραγόμενο. Πράγματι, έστω* $f_1, \dots, f_n \in I$, *τότε υπάρχουν* $\varepsilon_i > 0$, *ώστε* $f_i|_{[0,\varepsilon_i]} = 0$ *για κάθε* $i = 1, 2, \dots, n$. *Επιλέγω* $\varepsilon = \min\{\varepsilon_i : i = 1, 2, \dots, n\}$ *και συνεπώς* $f_i|_{[0,\varepsilon]} = 0$ *για κάθε* $i = 1, 2 \dots, n$. *Άρα για κάθε* $g \in \sum_{i=1}^{n} Rf_i$, *ισχύει* $g|_{[0,\varepsilon]} = 0$, *αλλά προφανώς υπάρχουν* $f \in I$ *με* $f|_{[0,\varepsilon]} \neq 0$, *οπότε* $\sum_{i=1}^{n} Rf_i \subsetneq I$ *για κάθε* $f_1, \dots, f_n \in I$ *και άρα το* I *δεν να είναι πεπερασμένα παραγόμενο.*

[1] Θα το αποδείξουμε αργότερα.

1.3 R-γραμμικές απεικονίσεις

Ορισμός 1.3.1. *Έστω M, N δύο R-πρότυπα, μια απεικόνιση $f : M \to N$ καλείται R-γραμμική αν :*

- $f(x+y) = f(x) + f(y)$ *για κάθε* $x, y \in M$
- $f(rx) = rf(x)$ *για κάθε* $x \in M$ *και* $r \in R$

και θέτουμε $\mathrm{End}_R M := \{f : M \to M : f \text{ είναι } R\text{-γραμμική}\} \subseteq \mathrm{End}_{\mathbf{Z}} M$

Παράδειγμα. *Έστω $\mathbf{F}$ σώμα, V ένας $\mathbf{F}$-διανυσματικός χώρος και $\varphi : V \to V$ μια γραμμική απεικόνιση. Έστω V_φ το $\mathbf{F}[x]$-πρότυπο. Τότε μια απεικόνιση $f : V_\varphi \to V_\varphi$ είναι $\mathbf{F}[x]$-γραμμική αν και μόνο αν η $f : V \to V$ είναι $\mathbf{F}$-γραμμική και $f \circ \varphi = \varphi \circ f$.*

Πρόταση 1.3.1. *Αν $f : M \to N$ μια R-γραμμική απεικόνιση, τότε ισχύουν τα εξής :*

- *Αν $M' \subseteq M$ ένα R-υποπρότυπο, τότε η εικόνα $f(M') \subseteq N$ είναι ένα R-υποπρότυπο. Συνεπώς η εικόνα $\mathrm{im} f = f(M) \subseteq N$ είναι ένα R-υποπρότυπο.*
- *Αν $N' \subseteq N$ ένα R-υποπρότυπο, τότε η αντίστροφη εικόνα $f^{-1}(N') \subseteq M$ είναι ένα R-υποπρότυπο. Συνεπώς ο πυρήνας $\ker f = f^{-1}(\{0\}) \subseteq M$ είναι ένα R-υποπρότυπο.*

Παρατήρηση. *Η R-γραμμική απεικόνιση $f : M \to N$ είναι 1-1 και επί αν και μόνο αν υπάρχει R-γραμμική απεικόνιση $g : N \to M$, ώστε $f \circ g = 1_N$ και $g \circ f = 1_M$.*

Θεώρημα 1.3.1 (1ο Θεώρημα Ισομορφισμών)**.** *Κάθε R-γραμμική απεικόνιση $f : M \to N$ παραγοντοποιείται με μοναδικό τρόπο :*

$$M \xrightarrow{\pi} M/\ker f \xrightarrow{\exists ! \tilde{f}} \mathrm{im} f \xhookrightarrow{i} N$$

Απόδειξη : Για την μοναδικότητα, αν υπάρχουν $\tilde{f}_1, \tilde{f}_2$, τέτοιες ώστε $f = i \circ \tilde{f}_1 \circ \pi = i \circ \tilde{f}_2 \circ \pi$, αφού η i και η π είναι 1-1 και επί αντιστοίχα, συνεπάγεται ότι $\tilde{f}_1 = \tilde{f}_2$. Για την υπάρξη, ορίζω $\tilde{f} : M/\ker f \to \mathrm{im} f$ με $\tilde{f}(x + \ker f) = f(x) \in \mathrm{im} f$ και έχουμε βλέπουμε ότι ο $\tilde{f}$ είναι ισομορφισμός. □

Θεώρημα 1.3.2 (2ο Θεώρημα Ισομορφισμών)**.** *Αν $K, L \subseteq M$ είναι R-υποπρότυπα, τότε υπάρχει ισομορφισμός*

$$\frac{K+L}{L} \simeq \frac{K}{K \cap L}$$

Απόδειξη. Έστω $f : K \to (K+L)/L$ με $f(x) = x + L \in (K+L)/L$. Η f είναι R-γραμμική, επί και $\ker f = K \cap L$ άρα από το 1ο θεώρημα ισομορφισμών :

$$\frac{K}{K \cap L} = K/\ker f \simeq \mathrm{im} f = \frac{K+L}{L}$$

□

Θεώρημα 1.3.3 (3ο Θεώρημα Ισομορφισμών)**.** *Έστω $N \subseteq M$ ένα R-υποπρότυπο, τότε :*

- *Κάθε υποπρότυπο $\tilde{L} \subseteq M/N$ είναι της μορφής $\tilde{L} = L/N$ για κάποιο υποπρότυπο $L \subseteq M$, με $N \subseteq L$.*
- *Για κάθε υποπρότυπο $L \subseteq M$ με $N \subseteq L$, το $L/N \subseteq M/N$ είναι υποπρότυπο και υπάρχει ισομορφισμός $\dfrac{M/N}{L/N} \simeq \dfrac{M}{L}$.*

Απόδειξη : Έστω $\pi : M \to M/N$ η απεικόνιση πηλικό και θέτω $L = \pi^{-1}(\tilde{L})$. Τότε $N = \ker \pi = \pi^{-1}(\{0\}) \subseteq \pi^{-1}(\tilde{L}) = L$ και αφού π επί, έχουμε $\tilde{L} = \pi(\pi^{-1}(\tilde{L})) = \pi(L) = L/N$.
Τέλος για την άλλη ισότητα θεωρώ τον ομομορφισμό $\varrho : M/N \to M/L$ με $\varrho(x+N) = x + L \in M/L$. Τότε η ϱ είναι γραμμική, επί και $\ker \varrho = L/N$. Άρα το $L/N \subseteq M/N$ είναι υποπρότυπο και από το 1ο θεώρημα ισομορφισμών :

$$\frac{M/N}{L/N} = \frac{M/N}{\ker \varrho} \simeq \mathrm{im}\varrho = \frac{M}{L}$$

□

Η αβελιανή ομάδα των R-γραμμικών απεικονίσεων $M \to N$

Ορισμός 1.3.2. *Έστω M, N δύο R-πρότυπα. Θεωρώ το σύνολο των R-γραμμικών απεικονίσεων $M \to N$:*

$$\mathrm{Hom}_R(M, N) := \{f : M \to N : f \textit{ είναι } R\textit{-γραμμική}\}$$

Το σύνολο $\mathrm{Hom}_R(M, N)$ αποτελεί αβελιανή ομάδα. Το σύνολο των ενδομορφισμών $M \to M$, το συμβολίζω $\mathrm{End}_R M := \mathrm{Hom}_R(M, M)$ και αποτελεί στην πραγματικότητα δακτύλιος με πράξεις την πρόσθεση και σύνθεση ενδομορφισμών.

Πρόταση 1.3.2. (i) *Αν $(N_\lambda)_\lambda$ είναι μια οικογένεια R-προτύπων και $N = \prod_\lambda N_\lambda$ με $p_\lambda : N \to N_\lambda$ η φυσική απεικόνιση, τότε η απεικόνιση $\mathrm{Hom}_R(M, N) \to \prod_\lambda \mathrm{Hom}(M, N_\lambda)$ με $f \longmapsto (p_\lambda \circ f)_\lambda$ είναι ισομορφισμός αβελιανών ομάδων. Η αντίστροφη απεικόνιση είναι αυτή που απεικονίζει μια οικογένεια $(f_\lambda)_\lambda \in \prod_\lambda \mathrm{Hom}(M, N_\lambda)$ στην γραμμική απεικόνιση $M \to N$ με $x \longmapsto (f_\lambda(x))_\lambda$. Συνεπώς,*

$$\mathrm{Hom}_R(M, \prod_{\lambda\in\Lambda} N_\lambda) \simeq \prod_{\lambda\in\Lambda} \mathrm{Hom}_R(M, N_\lambda)$$

(ii) *Αν $(M_\lambda)_\lambda$ είναι μια οικογένεια R-προτύπων και $M = \bigoplus_\lambda N_\lambda$ με εμφυτεύσεις $L_\lambda : M_\lambda \to M$ τότε η απεικόνιση $\mathrm{Hom}_R(M, N) \to \prod_\lambda \mathrm{Hom}(M_\lambda, N)$ με $f \longmapsto (f \circ L_\lambda)_\lambda$ είναι ισομορφισμός αβελιανών ομάδων. Η αντίστροφη απεικόνιση απεικονίζει την οικογένεια $(f_\lambda)_\lambda \in \prod_\lambda \mathrm{Hom}_R(M_\lambda, N)$ στην γραμμική απεικόνιση $(\sum_\lambda x_\lambda \longmapsto \sum_\lambda f_\lambda(x_\lambda))$. Συνεπώς*

$$\mathrm{Hom}_R(\bigoplus_{\lambda\in\Lambda} M_\lambda, N) \simeq \prod_{\lambda\in\Lambda} \mathrm{Hom}_R(M_\lambda, N)$$

Παρατηρήσεις. (i) *Από την προηγούμενη πρόταση, έπεται ότι αν θεωρήσω πεπερασμένες οικογένειες R-προτύπων $(M_i)_{i=1}^n$ και $(N_j)_{j=1}^m$, τότε υπάρχει ισομορφισμός αβελιανών ομάδων*

$$\mathrm{Hom}_R(\bigoplus_{i=1}^n M_i, N) \simeq \bigoplus_{i=1}^n \mathrm{Hom}_R(M_i, N) \qquad \mathrm{Hom}_R(M, \bigoplus_{j=1}^m N_j) \simeq \bigoplus_{j=1}^m \mathrm{Hom}_R(M, N_j)$$

(ii) *Ισχύει ότι*

$$\mathrm{Hom}_{\mathbf{Z}}(\bigoplus_{n\geq 2} \mathbf{Z}_n, \bigoplus_{m\geq 2} \mathbf{Z}_m) \not\simeq \bigoplus_{n\geq 2} \mathrm{Hom}_{\mathbf{Z}}(\mathbf{Z}_n, \bigoplus_{m\geq 2} \mathbf{Z}_m)$$

Πράγματι, η αβελιανή ομάδα στα αριστερά έχει ένα στοιχείο άπειρης τάξης, την ταυτοτική απεικόνιση. Η δεξία αβελιανή ομάδα είναι ομάδα στρέψης, αφού για κάθε $f : \mathbf{Z}_n \to \bigoplus_{m\geq 2} \mathbf{Z}_m$ είναι $n \cdot f = 0$.

1.4 Ελεύθερα πρότυπα

Ορισμός 1.4.1 (Καθολική ιδιότητα των ελεύθερων προτύπων.). *Έστω B ένα αυθαίρετο σύνολο. Ένα αριστερό R-πρότυπο F λέγεται ελεύθερο στο σύνολο B, αν υπάρχει μια απεικόνιση $i : B \to F$, τέτοια ώστε για κάθε αριστερό R-πρότυπο M, κάθε απεικόνιση $\gamma : B \to M$ να επεκτείνεται μοναδικά σε μια R-γραμμική απεικόνιση $g : F \to M$.*

$$\begin{tikzcd}
B \arrow[d, "i"'] \arrow[dr, "\gamma"] & \\
F \arrow[r, dashed, "g"'] & M
\end{tikzcd}$$

δηλαδή $g \circ i = \gamma$. Στην περίπτωση αυτή, λέμε ότι το F είναι ένα αριστερό ελεύθερο R-πρότυπο με γεννήτορες $i : B \to F$.

Ορισμός 1.4.2. *Έστω R δακτύλιος και B ένα αυθαίρετο σύνολο. Για μια συνάρτηση $f : B \to R$ θεωρώ τον φορέα supp$(f) = \{\beta \in B : f(\beta) \neq 0\}$. Παρατηρώ ότι για $f, g : B \to R$ και $r \in R$ το κατά σημείο άθροισμα $f + g : B \to R$ και το κατα σήμειο γινόμενο $rf : B \to R$ ικανοποιούν supp$(f+g) \subseteq$ supp$(f) \cup$ supp(g) και supp$(rf) \subseteq$ supp(f). Ορίζω το R-πρότυπο F ως εξής :*

$$F = \{f : B \to R : \#\mathit{supp}(f) < \infty\}$$

Για κάθε $\beta \in B$, θεωρώ την απεικόνιση $e_\beta \in M$, όπου $e_\beta(\beta') = \begin{cases} 1 & \beta = \beta' \\ 0 & \beta \neq \beta' \end{cases}$ και έτσι παρατηρώ ότι κάθε $x \in F$ γράφεται σαν $x = \sum_{\beta \in B} x(\beta) e_\beta$.

Πρόταση 1.4.1. *Με τον παραπάνω συμβολισμό, το R-πρότυπο $F = \{f : B \to R : \#\mathit{supp}(f) < \infty\}$ μαζί με την ένθεση $i : B \hookrightarrow F$, όπου $i(\beta) = e_\beta$ είναι ένα ελεύθερο R-πρότυπο στο σύνολο B*

Απόδειξη : Έστω ένα R-πρότυπο M και $\gamma : B \to M$ μια απεικόνιση. Κάθε $x \in F$, έχει μοναδική γραφή $x = \sum_{\beta \in B} x(\beta) e_\beta$. Ορίζω $g(x) = \sum_{\beta \in B} x(\beta)\gamma(b)$ και παρατηρώ ότι τότε $(g \circ i)(\beta) = g(i(\beta)) = g(e_\beta) = \gamma(b)$. Αν τώρα $\theta : F \to M$ μια άλλη R-γραμμική απεικόνιση με $\theta(e_\beta) = \theta(i(\beta)) = \gamma(\beta)$ για κάθε $\beta \in B$, τότε για τυχαίο $x = \sum_{\beta \in B} x(\beta) e_\beta \in F$, έχω $\theta(x) = \theta(\sum_{\beta \in B} x(\beta) e_\beta) = \sum_{\beta \in B} x(\beta)\theta(e_\beta) = \sum_{\beta \in B} x(\beta)\gamma(\beta) = g(x)$, δηλαδή $\theta = g$. □

Πρόταση 1.4.2. *Έστω F, F' δύο ελεύθερα R-πρότυπα στο σύνολο B. Τότε τα F, F' είναι ισόμορφα*

Απόδειξη : Θεωρώ το μεταθετικό διάγραμμα :

$$\begin{tikzcd}
F' & & & & F \\
F \arrow[u, dashed, "g"] & & B \arrow[ll, "i"] \arrow[rr, "i'"'] \arrow[ull, "i'"'] \arrow[urr, "i"] & & F' \arrow[u, dashed, "f"']
\end{tikzcd}$$

Υπάρχουν μοναδικές R-γραμμικές απεικονίσεις $f : F' \to F$ και $g : F \to F'$ με $f \circ i = i'$ και $g \circ i' = i$. Ειδικότερα, είναι $(f \circ g) \circ i' = f \circ i = i'$ και $(g \circ f) \circ i = g \circ i' = i$, αλλά οι μόνες απεικονίσεις με αυτήν την ιδιότητα είναι οι ταυτοτικές. Συνεπώς $f \circ g = 1_{F'}$ και $g \circ f = 1_F$, ισοδύναμα $F \simeq F'$ □

Παρατήρηση. *Έστω F το ελεύθερο πρότυπο στο σύνολο B. Τότε υπάρχει ισομορφισμός R-προτύπων $f : F \longrightarrow \bigoplus_{\beta\in\beta} R$ με :*

$$f : \sum_{\beta\in B} x(\beta)e_\beta \longmapsto (x(\beta))_{\beta\in B}$$

Επίσης, όπως και στην περίπτωση του ομαδοδακτυλίου, μπορώ να δω το αριστερό ελεύθερο R-πρότυπο F σαν το σύνολο

$$F = \left\{ \sum_{i=1}^{n} r_i\beta_i : n \in \mathbf{N},\ r_i \in R,\ \beta_i \in B \right\}$$

Θεώρημα 1.4.1. *Κάθε αριστερό R-πρότυπο M είναι πηλίκο ενός ελεύθερου αριστερού R-προτύπου F. Επίσης το M είναι πεπερασμένα παραγόμενο αν και μόνο αν το F μπορεί να επιλεχθεί πεπερασμένα παραγόμενο.*

Απόδειξη : . Έστω F να είναι το ευθύ άθροισμα $\#M$ το πλήθος αντιτύπων του R (οπότε το F είναι ένα ελεύθερο αριστερό R-πρότυπο) και $(x_m)_{m\in M}$ μια βάση του F. Από την καθολική ιδιότητα των ελεύθερων προτύπων, υπάρχει μια μοναδική R-γραμμική απεικόνιση $g : F \to M$ που επεκτείνει την αντιστοιχία $x_m \mapsto m$ (δηλαδή $g(x_m) = m$ για κάθε $m \in M$). Προφανώς η g είναι επιμορφισμός, άρα από το πρώτο θεώρημα ισομορφισμών $F/\ker g \simeq M$. Τέλος, αν το M είναι πεπερασμένα παραγόμενο, τότε $M = \sum_{i=1}^{n} Rm_i$ για κάποια $m_i \in M$ $i = 1, 2, \ldots, n$. Θεωρούμε το ελεύθερο αριστερό R-πρότυπο F με βάση $\{x_1, \ldots, x_n\}$, τότε η R-γραμμική απεικόνιση $g : F \to M$ με $g(x_i) = m_i$ για κάθε $i = 1, 2, \ldots, n$ είναι προφανώς επί. □

Παρατήρηση (Ένα παράδειγμα δακτυλίου S, με την ιδιότητα $S \simeq S^2 \simeq S^3 \simeq \ldots$ σαν S-πρότυπα). *Θα ήταν εύλογο κάποιος να σκεφτεί ότι οι κλάσεις ισομορφίας ελεύθερων R-προτύπων καθορίζονται από την πληθικότητα του συνόλου βάσης B. Κάτι τέτοιο όμως δεν ισχύει εν γένει. Έστω N ένα R-πρότυπο και $S = \mathrm{End}_R N$ ο δακτύλιος των R-γραμμικών ενδομορφισμών $s : N \to N$. Εύκολα δείχνετε ότι για κάθε R-πρότυπο M, η αβελιανή ομάδα $\mathrm{Hom}_R(M, N)$ λαμβάνει δομή S-προτύπου και για κάθε δύο R-πρότυπα M_1, M_2, υπάρχει ισομορφισμός S-προτύπων $\mathrm{Hom}_R(M_1 \oplus M_2, N) \simeq \mathrm{Hom}_R(M_1, N) \oplus \mathrm{Hom}_R(M_2, N)$. Συνεπώς, αν επιλέξουμε το N να είναι τέτοιο ώστε $N \simeq N^2$,[2] τότε*

$$S = \mathrm{End}_R N = \mathrm{Hom}_R(N, N) \simeq \mathrm{Hom}_R(N^2, N) \simeq \mathrm{Hom}_R(N, N) \oplus \mathrm{Hom}_R(N, N) \simeq S^2$$

και επαγωγικά αν $S \simeq S^n$, τότε $S \simeq S^n \simeq S \oplus S^{n-1} \simeq S^2 \oplus S^{n-1} \simeq S^{n+1}$

Θεώρημα 1.4.2. *Έστω R ένας μεταθετικός δακτύλιος. Θεωρώ ένα ελεύθερο R-πρότυπο F με γεννήτορες $i : B \longrightarrow F$. Υποθέτουμε ότι το R-πρότυπο F είναι ελεύθερο και με γεννήτορες $j : B' \hookrightarrow F$, τότε $\#B = \#B'$. Στην περίπτωση αυτή, ορίζουμε την τάξη του ελεύθερου R-προτύπου F, με $\mathrm{rank}(F) := \#B$ και δύο ελεύθερα R-πρότυπα F, F' είναι ισόμορφα αν και μόνο αν $\mathrm{rank}(F) = \mathrm{rank}(F')$*

Απόδειξη : Από το λήμμα του Zorn, εγγυείται η ύπαρξη μεγιστικού ιδεώδους $m \subsetneq R$[3]. Θεωρώ, το R-υποπρότυπο του F

$$m \cdot F := \left\{ \sum_{i=1}^{n} m_i x_i : n \in \mathbf{N},\ m_i \in m,\ x_i \in F \right\}$$

Το αντίστοιχο πηλίκο $F/m \cdot F$ λαμβάνει την φυσική δομή R/m-διανυσματικού χώρου (R/m-προτύπου), καθώς $m \subseteq ann_R F/m \cdot F$. Ισχυριζόμαστε, ότι το R/m-πρότυπο $F/m \cdot F$ είναι ελεύθερο με γεννήτορες $\pi \circ i : B \to F/m \cdot F$, αλλά και με γεννήτορες $\pi \circ j : B' \to F/m \cdot F$ όπου $\pi : F \to F/m \cdot F$ η απεικόνιση πηλίκο. Στην περίπτωση αυτή, θα είναι $F/m \cdot F \simeq \bigoplus_{\beta\in B} R/m \simeq$

[2] Ενα παράδειγμα τέτοιου N είναι το R-πρότυπο $N = \bigoplus_{i\geq 1} R$

[3] Έδω χρησιμοποιείται η υπόθεση ότι ο R είναι μεταθετικός. Υπαρχούν δακτύλιοι που δεν έχουν αμφίπλευρα (μεγιστικά) ιδεώδη. Για παράδειγμα ο $\mathbf{M}_n(D)$, όπου D διαιρετικός.

$\bigoplus_{\beta' \in B'} R/\mathfrak{m}$ και άρα $\#B' = \dim_{R/\mathfrak{m}} F/\mathfrak{m} \cdot F = \#B$. Πράγματι, έστω V ένας $R/\mathfrak{m}$-διανυσματικός χώρος και $\gamma : B \to V$ μια απεικόνιση. Ο διανυσματικός χώρος V λαμβάνει την φυσική δομή R-προτύπου με $\mathfrak{m} \subseteq ann_R V$ και άρα, αφού το F είναι ελεύθερο R-πρότυπο, υπάρχει μοναδική R-γραμμική απεικόνιση $g : F \to V$ με $g \circ i = \gamma$. Παρατηρούμε ότι, αν $m \in \mathfrak{m}$ και $x \in F$, τότε $g(mx) = mg(x) = 0 \in V$, άρα $\mathfrak{m} \cdot F \subseteq \ker g$, οπότε η g παραγοντοποείται σε μια $\bar{g} : F/\mathfrak{m} \cdot F \to V$ $(\bar{g} \circ \pi = g)$. Βλέπουμε ότι $\bar{g} \circ (\pi \circ i) = (\bar{g} \circ \pi) \circ i = g \circ i = \gamma$. Για την μοναδικότητα, έστω $\bar{\theta} : F/\mathfrak{m} \cdot F \to V$ μια άλλη $R/\mathfrak{m}$-γραμμική απεικόνιση, τέτοια ώστε $\bar{\theta} \circ (\pi \circ i) = \gamma$. Άρα η $\theta := \bar{\theta} \circ \pi : F \to V$, έχει την ιδιότητα $\theta \circ i = \gamma$, συνεπώς $\theta = g$, δηλαδή $\bar{\theta} \circ \pi = \bar{g} \circ \pi \Rightarrow \bar{\theta} = \bar{g}$, αφου η π είναι επί. Αντίστοιχα για τους γεννήτορες $j : B' \to F$. □

1.5 Τανυστικό γινόμενο

Έστω $f : S \longrightarrow R$ ένας ομομορφισμός δακτυλίων (ειδικότερα μια επέκταση δακτυλίων) και M ένα αριστερό R-πρότυπο, τότε το M έχει και την φυσιολογική δομή S-προτύπου που επάγεται από την $f : S \longrightarrow R$ Αντίστροφα, αν N ένα S-πρότυπο, με ενδιαφέρει να επεκτείνω την αβελιανή ομάδα $(N, +)$ σε μια "μεγαλύτερη" $(N', +)$, ώστε η N' να αποτελεί R-πρότυπο και να πέρνει υπόψιν την δομή του S-προτύπου N. Το τανυστικό γινόμενο προτύπων $R \otimes_S N$ πετυχένει ακριβώς αυτό.

Ορισμός 1.5.1. *Έστω R ένας δακτύλιος, A_R ένα δεξί R-πρότυπο, ${}_RB$ ένα αριστερό R-πρότυπο και G μια αβελιανή ομάδα. Μια συνάρτηση $f : A \times B \to G$ λέγεται R-διπροσθετική αν για κάθε $a, a' \in A$, $b, b' \in B$ και $r \in R$ ισχύει ότι :*

- $f(a + a', b) = f(a, b) + f(a', b)$
- $f(a, b + b') = f(a, b) + f(a, b')$
- $f(ar, b) = f(a, rb)$

Αν ο R είναι μεταθετικός και έχω R-πρότυπα A, B και M, τότε μια R-διπροσθετική απεικόνιση $f : A \times B \to M$ λέγεται R-διγραμμική αν επίσης $f(ar, b) = f(a, rb) = rf(a, b)$.

Ορισμός 1.5.2 (Τανυστικό γινόμενο). *Έστω R ένας δακτύλιος και πρότυπα A_R και ${}_RB$. Το τανυστικό γινόμενο τους είναι μια αβελιανή ομάδα T μαζί με την R-διπροσθετική απεικόνιση $h : A \times B \to T$ ώστε για κάθε άλλη αβελιανή ομάδα $(G, +)$ και R-διπροσθετική απεικόνιση $f : A \times B \to G$, να υπάρχει μια μοναδική $\mathbf{Z}$-γραμμική $\bar{f} : T \to G$ που κάνει το παρακάτω διάγραμμα μεταθετικό.*

$$\begin{tikzcd} & T \arrow[dr, dashed, "\bar{f}"] & \\ A \times B \arrow[ur, "h"] \arrow[rr, "f"'] & & G \end{tikzcd}$$

δηλαδή $\bar{f} \circ h = f$.

Πρόταση 1.5.1 (Μοναδικότητα). *Έστω A_R και ${}_RB$ δύο R-πρότυπα. Αν το τανυστικό γινόμενο τους υπάρχει, τότε είναι μοναδικό ως προς ισομορφισμό.*

Proof. Έστω R-πρότυπα A_R και ${}_RB$ με τανυστικά γινόμενα $(T, h : A \times B \to T)$, $(T', h : A \times B \to T')$, θα δείξουμε ότι $T \simeq T'$. Έιναι

$$\begin{tikzcd} T' & & & & T \\ T \arrow[u, "f"] & & A \times B \arrow[ll, "h"] \arrow[ull, "h'"'] \arrow[urr, "h"] \arrow[rr, "h'"'] & & T' \arrow[u, "g"'] \end{tikzcd}$$

υπάρχουν μοναδικές $f : T \to T'$ και $g : T' \to T$, ώστε $f \circ h = h'$ και $g \circ h' = h$. Παρατηρούμε, ότι $(g \circ f) \circ h = g \circ (f \circ h) = g \circ h' = h$ και $(f \circ g) \circ h' = f \circ (g \circ h') = f \circ h = h'$ και ταυτόχρονα οι $1_T : T \to T$ και $1_{T'}$ είναι οι μοναδικές $\mathbf{Z}$-γραμμικές με $1_T \circ h = h$ και $1_{T'} \circ h' = h'$. Συνεπώς $f \circ g = 1_T$ και $g \circ f = 1_{T'}$ □

Πρόταση 1.5.2. *Έστω R ένας δακτύλιος και R-πρότυπα A_R και ${}_RB$, τότε το τανυστικό τους γινόμενο υπάρχει και το συμβολίζουμε $A \otimes_R B$.*

Απόδειξη : Έστω F το ελεύθερο $\mathbf{Z}$-πρότυπο στο σύνολο $A \times B$, δηλαδή

$$F = \left\{ \sum_{i=1}^{r} n_i \cdot (a_i, b_i) : r \in \mathbf{N},\ n_i \in \mathbf{Z},\ (a_i, b_i) \in A \times B \right\}$$

Έστω S η υποομάδα του F που παράγεται από τα παρακάτω στοιχεία

$$(a + a', b) - (a, b) - (a', b) \qquad (a, b + b') - (a, b) - (a, b') \qquad (ar, b) - (a, rb)$$

για κάθε $a, a' \in A$ $b, b' \in B$ και $r \in R$. Ορίζω $A \otimes_R B := F/S$, συμβολίζω το σύμπλοκο $(a, b) + S$ με $a \otimes b$ και θεωρώ

$$h : A \times B \to A \otimes_R B$$

$$h : (a, b) \longmapsto a \otimes b$$

(δηλαδή $h = \pi\,|_{A\times B}$, όπου $\pi : F \to F/S$ η απεικόνιση πηλίκο). Συνεπώς ισχύουν οι παρακάτω σχέσεις στην $A \otimes_R B$:

$$(a + a') \otimes b = a \otimes b + a' \otimes b$$

$$a \otimes (b + b') = a \otimes b + a \otimes b'$$

$$(ar) \otimes b = a \otimes (rb)$$

Η h είναι προφανώς R-διπροσθετική. Έστω τώρα $(G, +)$ μια αβελιανή ομάδα και $f : A \times B \to G$ μια R-διπροσθετική απεικόνιση. Από την καθολική ιδιότητα των ελεύθερων προτύπων, υπάρχει μια μοναδική $\mathbf{Z}$-γραμμική απεικόνιση $g : F \to G$ που επεκτείνει την f. Παρατηρούμε ότι $S \subseteq \ker g$ και άρα παραγοντοποιείται μέσω τις απεικόνισης πηλίκο σε μια $\bar{f} : A \otimes_R B \to G$.

$$\begin{tikzcd}
& F \arrow[d, "\pi"] \arrow[ddr, bend left, "g"] & \\
& A \otimes_R B \arrow[dr, "\bar{f}"] & \\
A \times B \arrow[uur, bend left, "i"] \arrow[ur, "h"] \arrow[rr, "f"'] & & G
\end{tikzcd}$$

Υπάρχει δηλαδή, $\mathbf{Z}$-γραμμική $\bar{f} : A \otimes_R B \to G$, ώστε $\bar{f} \circ \pi = g$. Η $\bar{f}$ είναι αυτή που κάνει την δουλειά. Πράγματι $(\bar{f} \circ h)(a, b) = \bar{f}(a \otimes b) = \bar{f}(\pi(a, b)) = g(a, b) = f(a, b)$, δηλαδή $\bar{f} \circ h = f$. Για την μοναδικότητα της $\bar{f}$, έστω $\bar{\theta} : A \otimes_R B \to G$ μια άλλη προσθετική απεικόνιση, τέτοια ώστε $\bar{\theta} \circ h = f$. Ορίζω $\theta := \bar{\theta} \circ \pi : F \to G$, τότε παρατηρώ $\theta \circ i(a, b) = \bar{\theta} \circ \pi \circ i(a, b) = \bar{\theta} \circ h(a, b) = f(a, b)$ και άρα από την μοναδικότητα της g, έχω $\theta = g$. Ισοδύναμα $\bar{\theta} \circ \pi = \bar{f} \circ \pi$ και αφού η π είναι επί, έχω $\bar{\theta} = \bar{f}$. □

Παρατηρήσεις. *(i) Η αβελιανή ομάδα $A \otimes_R B$ παράγεται από το σύνολο $\{a \otimes b : (a,b) \in A \times B\}$, δηλαδή κάθε $u \in A \otimes_R B$ έχει την μορφή $u = \sum_{i=1}^{n} a_i \otimes b_i$. Όμως η γραφή αυτή δεν είναι μοναδική. Πράγματι, για παράδειγμα το $0 \in A \otimes_R B$ έχει τις διαφορετικές γραφές :*

$$0 = (a + a') \otimes b - a \otimes b - a' \otimes b = a \otimes (b + b') - a \otimes b - a \otimes b'$$

$$= (ar) \otimes b - a \otimes (rb)$$

για κάθε $a \in A, b \in B$

(ii) Αν A μια αβελιανή ομάδα, τότε για να ορίσουμε καλά μια $f : M \otimes_R N \to A$, δεν αρκεί να ορίσουμε την εικόνα των γεννητόρων $m \otimes n$ για κάθε $m \in M$ και $n \in N$, καθώς κάθε στοιχείο $u \in M \otimes_R N$ έχει πόλλες διαφορετικές γραφές με βάση αυτούς τους γεννήτορες. Ο πιο ασφαλής και απλός τρόπος είναι να ορίσουμε πρώτα μια $\bar{f} : M \times N \to A$, τέτοια ώστε $S \subseteq \ker \bar{f}$ και έτσι να παραγοντοποίειται σε μια $f : M \otimes_R N \to A$.

Πρόταση 1.5.3. *Έστω R-γραμμικές $f : M_R \to M'_R$ και $g : {}_RN \to {}_RN'$ απεικονίσεις δεξιών και αριστερών R-προτύπων αντίστοιχα. Τότε υπάρχει μια μοναδική $\mathbf{Z}$-γραμμική απεικόνιση, που συμβολίζεται $f \otimes g : M \otimes_R N \to M' \otimes_R N'$, με*

$$f \otimes g : m \otimes n \longmapsto f(m) \otimes g(n)$$

Απόδειξη : Η απεικόνιση $\gamma : M \times N \to M' \otimes_R N'$, με $(m,n) \overset{\gamma}{\longmapsto} f(m) \otimes g(n)$ είναι R-διπροσθετική, συνεπώς επάγει μια μοναδική $\mathbf{Z}$-γραμμική απεικόνιση $M \otimes_R N \to M' \otimes_R N'$ με $m \otimes n \longmapsto f(m) \otimes g(n)$. □

Πόρισμα 1.5.1. *Έστω R-γραμμικές απεικονίσεις δεξιών R-προτύπων $M \overset{f'}{\to} M' \overset{f''}{\to} M''$ και αριστερών R-προτύπων $N \overset{g'}{\to} N' \overset{g''}{\to} N''$, τότε έχουμε*

$$(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$$

Απόδειξη : Και οι δύο απεικονίσεις απεικονίζουν $m \otimes n \longmapsto f'(f(m)) \otimes g'(g(n))$, οπότε απο την μοναδικότητα έχουμε ισότητα. □

Πρόταση 1.5.4.

(i) *Έστω ένα διπρότυπο ${}_SM_R$ και ένα αριστερό πρότυπο ${}_RB$. Το τανυστικό $M \otimes_R N$ εφοδιάζεται με την δομή αριστερού S-προτύπου, με δράση $s(m \otimes n) = (sm) \otimes n$*

(ii) *Έστω ένα δεξί πρότυπο M_R και ένα διπρότυπο ${}_RN_S$. Το τανυστικό $M \otimes_R N$ εφοδιάζεται με την δομή δεξιού S-προτύπου, με δράση $(m \otimes n)s = m \otimes (ns)$*

Παρατηρήσεις. *(i) Αν ο R μεταθετικός, τότε το τανυστικό γινόμενο $M \otimes_R N$ αποτελεί R-πρότυπο και ισχύει $r(m \otimes n) = (rm) \otimes n = (m) \otimes (rn)$*

(ii) Το τανυστικό γινόμενο δεν σέβεται τις ένθεσεις. Πράγματι, έστω η ένθεση $\mathbf{Z} \hookrightarrow \mathbf{Q}$ τότε $\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}_2 \simeq \mathbf{Z}$, αλλά $\mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Z}_2 = 0$, αφού αν $q \otimes a \in \mathbf{Q} \otimes_{\mathbf{Z}} \mathbf{Z}_2$, τότε $q \otimes a = (q/2) \otimes 2a = (q/2) \otimes 0 = 0$

Πρόταση 1.5.5. *Για κάθε αριστερό R-πρότυπο M, υπάρχει ισομορφισμός R-προτύπων*

$$\vartheta_M : R \otimes_R M \longrightarrow M$$

$$r \otimes m \longmapsto rm$$

Απόδειξη. Θεωρούμε την R-γραμμική απεικόνιση $\varphi_M : M \to R \otimes_R M$ με $\varphi_M : m \longmapsto 1_R \otimes m$. Εύκολα βλέπουμε ότι $\varphi_M \vartheta_M = 1_{R \otimes_R M}$ και $\vartheta_M \varphi_M = 1_M$. □

Θεώρημα 1.5.1. *(i) Έστω ένα δεξί R-πρότυπο A και αριστερά πρότυπα $\{B_i \,:\, i \in I\}$, τότε υπάρχει ισομορφισμός αβελιανών ομάδων*

$$A \otimes_R \left(\bigoplus_{i \in I} B_i \right) \xrightarrow{\varphi} \bigoplus_{i \in I} (A \otimes_R B_i)$$

με $\varphi : a \otimes (b_i) \longmapsto (a \otimes b_i)$.

(ii) Έστω αριστερό R-πρότυπο ${}_R B$ και αριστερά R-πρότυπα $\{A_i \,:\, i = 1, 2, \ldots, n\}$, τότε υπάρχει ισομορφισμός αβελιανών ομάδων

$$\left(\bigoplus_{i=1}^{n} A_i \right) \otimes_R B \xrightarrow{\psi} \bigoplus_{i=1}^{n} (A_i \otimes_R B)$$

με $\psi : (a_i)_{i=1}^n \otimes b \longmapsto (a_i \otimes b)_{i=1}^n$

Πόρισμα 1.5.2. *Έστω $\mathbf{F}$ σώμα και U, V δύο $\mathbf{F}$-διανυσματικοί χώροι διάστασης n και m αντίστοιχα. Έστω $u_1, \ldots, u_n$ μια βάση του U και $v_1, \ldots, v_m$ μια βάση του V. Τότε το τανυστικό γινόμενο τους $U \otimes_{\mathbf{F}} V$ είναι ένας $\mathbf{F}$-διανυσματικός χώρος διάστασης nm και μια βάση του είναι η $u_i \otimes v_j$ για $i = 1, 2, \ldots, n$ και $j = 1, 2, \ldots, m$.*

Απόδειξη : Προφανώς, η συλλογή των στοιχείων $u_i \otimes v_j$ για $i = 1, 2, \ldots, n$ και $j = 1, 2, \ldots, m$ παράγει τον $U \otimes_{\mathbf{F}} V$ και είναι πληθικότητας nm. Μένει να δείξουμε ότι $\dim_{\mathbf{F}} U \otimes_{\mathbf{C}} V = nm$. Πράγματι, αφού $\dim_{\mathbf{F}} U = n$ και $\dim_{\mathbf{F}} V = m$, τότε $U \simeq \mathbf{F}^n$ και $V \simeq \mathbf{F}^m$. Συνεπώς,

$$U \otimes_{\mathbf{F}} V \simeq \mathbf{F}^n \otimes_{\mathbf{F}} V \simeq \bigoplus_{i=1}^{n} \mathbf{F} \otimes_{\mathbf{F}} V \simeq \bigoplus_{i=1}^{n} V \simeq V^n \simeq \mathbf{F}^{nm}$$

άρα $\dim_{\mathbf{F}} U \otimes_{\mathbf{C}} V = nm$. □

Παρατήρηση. *(i) Έστω $\mathbf{F}$ ένα σωμά, U ένας $\mathbf{F}$-διανυσματικός χώρος με $\dim_{\mathbf{F}} U = 2$ και θεωρώ τον $\mathbf{F}$-διανυσματικό χώρο $U \otimes_{\mathbf{F}} U$. Υπάρχουν στοιχεία στον $U \otimes_{\mathbf{F}} U$ που δεν είναι την μορφής $u_1 \otimes u_2$. Πράγματι, έστω $\{u_1, u_2\}$ μια βάση του U, τότε μια βάση του $U \otimes_{\mathbf{F}} U$ είναι η $\{u_1 \otimes u_1, u_1 \otimes u_2, u_2 \otimes u_1, u_2 \otimes u_2\}$. Ισχυρίζομαι ότι δεν υπάρχουν $v, w \in U$ με $v \otimes w = u_1 \otimes u_2 + u_2 \otimes u_1$. Αν υπήρχαν, τότε για κάποια $a, b, c, d \in \mathbf{F}$ θα ήταν*

$$u_1 \otimes u_2 + u_2 \otimes u_1 = v \otimes w = (au_1 + bu_2) \otimes (cu_1 + du_2) =$$

$$ac(u_1 \otimes u_1) + ad(u_1 \otimes u_2) + bc(u_2 \otimes u_1) + bd(u_2 \otimes u_2)$$

Συνεπώς, από γραμμική ανεξαρτησία $ac = bd = 0$ και $ad = bc = 1$. Έπεται ότι $0 = 1$ #

Πρόταση 1.5.6. *Έστω $\mathbf{F}$ σώμα και U, V δύο $\mathbf{F}$-διανυσματικοί χώροι διάστασης n και m αντίστοιχα. Σταθεροποιώ μια βάση $u_1, \ldots, u_n$ του U, μια βάση $v_1, \ldots, v_m$ του V και θεωρώ την επαγόμενη βάση $u_i \otimes v_j$ για $i = 1, 2, \ldots, n$ και $j = 1, 2, \ldots, m$ του τανυστικού γινομένουν $U \otimes_{\mathbf{F}} V$. Αν $f : U \to U$ και $g : V \to V$ δύο $\mathbf{F}$-γραμμικές απεικονίσεις, τότε ισχύει*

$$\mathrm{tr}(f : U \to U) \cdot \mathrm{tr}(g : V \to V) = \mathrm{tr}(f \otimes g : U \otimes_{\mathbf{F}} V \to U \otimes_{\mathbf{F}} V)$$

Απόδειξη : Υπάρχουν αριθμοί $a_{i,j}, b_{i,j} \in \mathbf{F}$ με

$$f(u_j) = \sum_{i=1}^{n} a_{i,j} u_i \qquad g(v_j) = \sum_{i=1}^{m} b_{i,j} v_i$$

Συνεπώς,

$$(f \otimes g)(u_k \otimes v_\ell) = f(u_k) \otimes g(v_\ell) = \left(\sum_{i=1}^{n} a_{i,k} u_i\right) \otimes \left(\sum_{j=1}^{m} b_{j,\ell} v_i\right) = \sum_{i,j} a_{i,k} b_{j,\ell} u_i \otimes v_j$$

και άρα

$$\operatorname{tr}(f \otimes g : U \otimes_{\mathbf{F}} V \to U \otimes_{\mathbf{F}} V) = \sum_{i,j} a_{i,i} b_{j,j} = \operatorname{tr}(f : U \to U) \cdot \operatorname{tr}(g : V \to V)$$

$\square$

ΚΕΦΑΛΑΙΟ 2

Θεωρία Wedderburn-Artin

2.1 Πρότυπα της Noether και του Artin

Ορισμός 2.1.1. *Έστω M ένα R-πρότυπο. Λέμε ότι το M ικανοποιεί :*

- *την συνθήκη αύξουσας άλυσης αν κάθε ακολουθία υποπροτύπων της μορφής*

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots \subseteq N_m \subseteq N_{m+1} \subseteq \dots$$

είναι τελικά σταθερή, δηλαδή υπάρχει ένα φυσικός k, ώστε $N_k = N_{k+1} = \dots$

- *την συνθήκη φθίνουσας άλυσης αν κάθε ακολουθία υποπροτύπων της μορφής*

$$L_1 \supseteq L_2 \supseteq L_3 \supseteq \cdots \supseteq L_m \supseteq L_{m+1} \supseteq \dots$$

είναι τελικά σταθερή, δηλαδή υπάρχει ένα φυσικός k, ώστε $L_k = L_{k+1} = \dots$

Πρόταση 2.1.1. *Οι επόμενες συνθήκες είναι ισοδύναμες για ένα R-πρότυπο M :*

(i) Κάθε υποπρότυπο $N \subseteq M$ είναι πεπερασμένα παραγόμενο.

(ii) Ισχύει η συνθήκη αύξουσας άλυσης

(iii) Για κάθε μη κενή συλλογή $\mathscr{X}$ υποπροτύπων του M, υπάρχει μεγιστικό στοιχείο.

Στην περίπτωση αυτή, το M καλείται Noetherian (πρότυπο της Noether)

Απόδειξη: $(i) \to (ii)$: Έστω $(N_k)_k$ μια αύξουσα ακολουθία υποπροτύπων του M. Στην περίπτωση αυτή το $N = \bigcup_k N_k$ αποτελεί R-υποπρότυπο του N. Τότε από την υπόθεση είναι πεπερασμένα παραγόμενο, άρα υπάρχουν $x_1, \dots, x_k \in N$, τέτοια ώστε $N = \sum_{i=1}^k Rx_i$. Καθώς, $x_i \in N = \cup_k N_k$, υπάρχουν $k_1, \dots, k_n$, τέτοια ώστε $x_i \in N_{k_i}$, για $i = 1, 2, \dots, n$. Θέτω $k_0 = \max_i k_i$, και παρατηρώ :

$$N \subseteq N_{k_0} \subseteq N_{k_0+1} \subseteq \cdots \subseteq \cup_k N_k = N$$

άρα για κάθε $n \geq k_0$ $N_k = N_{k_0}$

$(ii) \to (iii)$: Υποθέτουμε ότι ισχύει η συνθήκη αύξουσας άλυσης και έστω, ως προς άτοπο, ότι υπάρχει μια μη κενή συλλογή υποπροτύπων $\mathscr{X}$, που δεν έχει μεγιστικό στοιχείο. Καθώς η συλλογή δεν είναι κενή, επιλέγω $N_0 \in \mathscr{X}$, και αφού δεν έχει μεγιστικό στοιχείο, υπάρχει $N_1 \in \mathscr{X}$, τέτοιο ώστε $N_0 \subsetneq N_1$. Το $N_1 \in \mathscr{X}$ και αφού το η $\mathscr{X}$ δεν έχει μεγιστικό στοιχείο, υπάρχει ένα $N_2 \in \mathscr{X}$, τέτοιο ώστε $N_1 \subsetneq N_2$. Συνεχίζοντας επαγωγικά κατασκευάζω μια γνησίως αύξουσα ακολουθία υποπροτύπων $\#$

$(iii) \to (i)$: Έστω $N \subseteq M$ ένα υποπρότυπο και $\mathscr{X}$ η συλλογή των πεπερασμένα παραγόμενων υποπροτύπων του N. Η οικόγενεια $\mathscr{X}$ είναι μη κένη, καθώς $0 \in \mathscr{X}$. Έστω N' το μεγιστικό στοιχείο της $\mathscr{X}$. θα δείξω ότι $N' = N$. Προφανώς, $N' \subseteq N$, αν υπήρχε $x \in N \setminus N'$, τότε για το υποπρότυπο $Q = N' + Rx$, ισχύει ότι $Q \subseteq N$. Επίσης $N' \subsetneq Q$ και Q προφανώς πεπερασμένα παραγόμενο, άρα $N' \in \mathscr{X}$, αλλά N μεγιστικό #

□

Πρόταση 2.1.2. *Οι επόμενες συνθήκες είναι ισοδύναμες για ένα R-πρότυπο M :*

(i) Ισχύει η συνθήκη φθίνουσας άλυσης για τα υποπρότυπα του M.

(ii) Κάθε μη κενή συλλογή $\mathscr{X}$ υποπροτύπων του M έχει ελαχιστικό στοιχείο.

Στην περίπτωση αυτή, το M καλείται Artinian (πρότυπο του Artin)

Απόδειξη. $(i) \to (ii)$: Εντελώς ανάλογα όπως πριν.

$(ii) \to (i)$: Έστω $N_0 \supseteq N_1 \supseteq \cdots \supseteq N_k \supseteq N_{k+1} \supseteq \ldots$ μια φθίνουσα ακολουθία υποπροτύπων του M και θέτω $\mathscr{X} = \{N_k : k \in \mathbf{N}\}$. Η $\mathscr{X}$ προφανώς μη κενή, άρα από υπόθεση έχει ελαχιστικό στοιχείο N_{t_0}, αλλά για κάθε $t > t_0$, έχω $N_t \subseteq N_{t_0}$ και $N_t \in \mathscr{X}$. Από τον ελαχιστικό χαρακτήρα παίρνουμε $N_t = N_{t_0}$, για κάθε $t \geq t_0$. □

Παραδείγματα. (i) *Το $\mathbf{Z}$-πρότυπο $\mathbf{Z}$ είναι της Noether, αλλά όχι του Artin. Πράγματι, υπάρχει γνησίως φθίνουσα ακολουθία ιδεωδών*

$$2\mathbf{Z} \supsetneq 4\mathbf{Z} \supsetneq 8\mathbf{Z} \supsetneq 16\mathbf{Z} \supsetneq \ldots$$

και καθώς ο δακτύλιος $\mathbf{Z}$ είναι περιοχή κυρίων ιδεωδών είναι εύκολο να δειχθεί ότι κάθε γνησίως αύξουσα ακολουθία $\mathbf{Z}$-υποπροτύπων του τερματίζει.

(ii) *Σταθεροποιώ έναν πρώτο αριθμό p και θεωρώ το $\mathbf{Z}$-πρότυπο :*

$$\mathscr{C}(p^\infty) = \{z \in \mathbf{C} : z^{p^n} = 1 \text{ για κάποιο } n \in \mathbf{N}\}$$

Το $\mathbf{Z}$-πρότυπο $\mathscr{C}(p^\infty)$ είναι του Artin, αλλά όχι της Noether. Πράγματι, για κάθε $t \in \mathbf{N}$, όριζω την υποομάδα $\mathcal{C}_t \in \mathscr{C}(p^\infty)$, ως εξής :

$$\mathcal{C}_t = \{z \in \mathbf{C} : z^{p^t} = 1\} = \left\langle \exp \frac{2\pi i}{p^t} \right\rangle \simeq \mathbf{Z}_{p^t}$$

δηλαδή κυκλίκη τάξεως p^t. Ισχύει ότι :

$$\mathcal{C}_0 \subsetneq \mathcal{C}_1 \subsetneq \mathcal{C}_2 \subsetneq \cdots \subsetneq \mathcal{C}_t \subsetneq \mathcal{C}_{t+1} \subsetneq \ldots$$

και άρα το $\mathbf{Z}$-πρότυπο $\mathscr{C}(p^\infty)$ δεν είναι της Noether. Οι γνήσιες υποόμαδες της $\mathscr{C}(p^\infty)$[1] είναι ακριβώς οι $(\mathcal{C}_t)_t$. Πράγματι[2] έστω $A \subsetneq \mathscr{C}(p^\infty)$ γνήσια υποόμαδα. Τότε υπάρχει $t \in \mathbf{N}$, ώστε $C_t \subsetneq A$. Καθώς $\mathcal{C}_0 \subseteq A$, επιλέγω τον μικρότερο t_0, τέτοιο ώστε $\mathcal{C}_{t_0} \subseteq A$ και $\mathcal{C}_{t_0+1} \not\subseteq A$. Τότε ισχύριζομαι ότι $A = \mathcal{C}_{t_0}$, δηλαδή ότι $A \subseteq \mathcal{C}_{t_0}$. Έστω $\alpha \in A \subseteq \mathscr{C}(p^\infty)$ και $o(\alpha) = p^\lambda$. Τότε $\langle \alpha \rangle = \{z \in \mathbf{C} : z^{p^\lambda} = 1\} = C_\lambda$. Αν $\lambda \geq t_0+1$, τότε $\mathcal{C}_{t_0+1} \subseteq \mathcal{C}_\lambda \subseteq A$ #. Αν $\lambda \leq t_0$, τότε $\alpha \in \langle \alpha \rangle = \mathcal{C}_\lambda \subseteq \mathcal{C}_{t_0}$. Συνεπώς είναι του Artin.

[1] Οι οικογένεια των $\mathbf{Z}$-προτύπων (υποομάδων) $\{\mathcal{C}_t : t \in \mathbf{N}\}$ έχουν την ιδιότητα ότι για κάθε $n, m \in \mathbf{N}$, υπάρχει $\ell \in \mathbf{N}$ τέτοιο ώστε $\mathcal{C}_n \cup \mathcal{C}_m \subseteq \mathcal{C}_\ell$. Είναι εύκολο να δειχθεί ότι σε αυτήν την περίπτωση, η ένωση $\bigcup_{t=1}^{\infty} \mathcal{C}_t$ αποτελέι $\mathbf{Z}$-πρότυπο και στην πραγματικότητα $\mathscr{C}(p^\infty) = \bigcup_{t=1}^{\infty} \mathcal{C}_t$

[2] Στην πραγματικότητα οι πεπερασμένα παραγόμενες ομάδες οι οποίες είναι πλήρως διατεταγμένα σύνολα (με διάταξη τον εγκλεισμό συνόλων) είναι ακριβώς οι κυκλικές $\mathbf{Z}_{p^n}$, όπου $n \in \mathbf{N}$ και p πρώτος.

(iii) *Αν $\mathbf{F}$ σώμα και V ένας $\mathbf{F}$-διανυσματικός χώρος, τότε ο V είναι $\mathbf{F}$-πρότυπο του Artin αν και μονο αν είναι $\mathbf{F}$-πρότυπο της Noether αν και μονο αν $\dim_{\mathbf{F}} V < \infty$. Πράγματι, είναι φανερό ότι αν $\dim_{\mathbf{F}} V < \infty$, τότε ισχύουν οι συνθήκες της Noether και του Artin. Αν $\dim_{\mathbf{F}} V = \infty$ και $\{e_i : i \in \mathbf{N}\}$ μια βάση του, τότε έχω τις γνησίως μονότονες ακολουθίες :*

$$0 \subsetneq \langle e_1 \rangle \subsetneq \langle e_1, e_2 \rangle \subsetneq \langle e_1, e_2, e_3 \rangle \subsetneq \dots$$

άρα δεν ειναι της Noether.

$$V \supsetneq \langle e_2, e_3, \cdots \rangle \supsetneq \langle e_3, e_4, \cdots \rangle \supsetneq \dots$$

άρα ούτε του Artin.

(iv) *Έστω $\mathbf{F} \subseteq \mathbf{E}$ δυο σώματα και V ένας $\mathbf{E}$-διανυσματικός χώρος. Θεωρώ τον δακτύλιο :*

$$\begin{pmatrix} \mathbf{E} & V \\ O & \mathbf{F} \end{pmatrix} := \left\{ \begin{pmatrix} e & v \\ 0 & f \end{pmatrix} : e \in \mathbf{E}, f \in \mathbf{F} \text{ και } v \in V \right\}$$

με πρόσθεση και πολλαπλασιασμό :

$$\begin{pmatrix} e & v \\ 0 & f \end{pmatrix} + \begin{pmatrix} e' & v' \\ 0 & f' \end{pmatrix} = \begin{pmatrix} e+e' & v+v' \\ 0 & f+f' \end{pmatrix} \qquad \begin{pmatrix} e & v \\ 0 & f \end{pmatrix} \cdot \begin{pmatrix} e' & v' \\ 0 & f' \end{pmatrix} = \begin{pmatrix} ee' & ev'+f'v \\ 0 & ff' \end{pmatrix}$$

Παρατηρώ επίσης ότι υπάρχει επιμορφισμός δακτυλίων :

$$g : \begin{pmatrix} \mathbf{E} & V \\ O & \mathbf{F} \end{pmatrix} \to \mathbf{E} \times \mathbf{F}, \text{ με } \begin{pmatrix} e & v \\ 0 & f \end{pmatrix} \xmapsto{g} (e, f)$$

με πυρήνα $\ker g = \begin{pmatrix} O & V \\ O & O \end{pmatrix}$ Θεωρώ τώρα τον δακτύλιο :

$$R = \begin{pmatrix} \mathbf{R} & \mathbf{R} \\ O & \mathbf{Q} \end{pmatrix} \subseteq \mathbf{M}_2(\mathbf{R})$$

Ο R δεν είναι δεξία του Artin, ούτε της Noether (το δεξί R-πρότυπο R). Καθώς $\dim_{\mathbf{Q}} \mathbf{R} = \infty$ μπορώ να βρώ ακολουθίες $\mathbf{Q}$-διανυσματικών υπόχωρων τέτοιοι ώστε :

$$U_0 \subsetneq U_1 \subsetneq \cdots \subsetneq U_k \subsetneq \cdots \subsetneq \mathbf{R} \supsetneq W_0 \supseteq W_1 \supsetneq \cdots \supsetneq W_k \supsetneq \dots$$

και έτσι πρόκυπτουν ακολουθίες δεξιών ιδεωδών :

$$\begin{pmatrix} 0 & U_0 \\ 0 & 0 \end{pmatrix} \subsetneq \begin{pmatrix} 0 & U_1 \\ 0 & 0 \end{pmatrix} \subsetneq \begin{pmatrix} 0 & U_2 \\ 0 & 0 \end{pmatrix} \subsetneq \cdots \subsetneq \begin{pmatrix} 0 & \mathbf{R} \\ 0 & 0 \end{pmatrix} \subsetneq R$$

$$R \supsetneq \begin{pmatrix} 0 & \mathbf{R} \\ 0 & 0 \end{pmatrix} \supsetneq \begin{pmatrix} 0 & W_0 \\ 0 & 0 \end{pmatrix} \supsetneq \begin{pmatrix} 0 & W_1 \\ 0 & 0 \end{pmatrix} \supsetneq \begin{pmatrix} 0 & W_2 \\ 0 & 0 \end{pmatrix} \supsetneq \dots$$

Ομώς ο R είναι αριστέρα του Artin και της Noether (το αριστερό R-πρότυπο R). Πράγματι, το αριστέρο ιδεώδες (R-υποπρότυπο) $\begin{pmatrix} 0 & \mathbf{R} \\ 0 & 0 \end{pmatrix}$ έχει μόνο δύο R-υποπρότυπα, τον ευατό του και το 0. Συνεπώς, είναι της Noether και του Artin. Ταυτόχρονα, το πρότυπο πηλίκο :

$$R/\begin{pmatrix} 0 & \mathbf{R} \\ 0 & 0 \end{pmatrix} = R/\ker g \simeq \mathbf{R} \times \mathbf{Q}$$

είναι επίσης αριστερά της Noether και αριστερά του Artin. Έχει ακριβώς τέσσερα ιδεώδη :

$$\mathbf{R} \times 0,\ 0 \times \mathbf{Q}, \mathbf{R} \times \mathbf{Q}, 0 \times 0$$

Από την επόμενη πρόταση ο δακτύλιος R είναι αριστερά του Artin και της Noether.

Πρόταση 2.1.3. *Αν M ενα R-πρότυπο και $N \subseteq M$ ένα υποπρότυπο, τότε τα επομενα είναι ισοδύναμα:*

(i) *Το M είναι της Noether (Artin)*

(ii) *Το N και M/N είναι της Noether (Artin)*

Απόδειξη : $(i) \to (ii)$: Θα δείξω ότι τα υποπρότυπα του N και M/N είναι πεπερασμένα παραγόμενα. Εστώ L υποπρότυπο του N. Αφού $L \subseteq N \subseteq M$, δηλαδή το L είναι και υποπρότυπο του M, το L είναι πεπερασμένα παραγόμενο και άρα το N είναι της Noether. Αν $\tilde{K}$ υποπρότυπο του M/N, από το θεώρημα αντιστοιχίας, υπάρχει υποπρότυπο K του M, τέτοιο ώστε $N \subseteq K \subseteq M$ και $K/N \simeq \tilde{K}$. Αφού K είναι υποπρότυπο M και το M της Noether, το K είναι πεπερασμένα παραγόμενο, δηλαδή $K = \sum_{i=1}^{n} Rx_i$, για κάποια $x_i \in K$. Είναι εύκολο να δειχθεί ότι $\tilde{K} \simeq K/N = \sum_{i=1}^{n} R(x_i + N)$

$(ii) \to (i)$: Θα αποδείξουμε την συνθήκη αύξουσας άλυσης για το M. Έστω $M_1 \subseteq M_2 \subseteq M_3 \subseteq \dots$ μια αύξουσα ακολουθία υποπροτύπων. Από αυτήν έπονται δύο αύξουσες ακολουθίες

$$M_1 \cap N \subseteq M_2 \cap N \subseteq M_3 \cap N \subseteq \dots \qquad \frac{M_1 + N}{N} \subseteq \frac{M_2 + N}{N} \subseteq \frac{M_3 + N}{N} \subseteq \dots$$

των προτύπων N και M/N αντίστοιχα. Αφού για τα N και M/N ισχύει η συνθήκη αύξουσας άλυσης, υπάρχει $k \in \mathbf{N}$, τέτοιο ώστε

$$M_k \cap N = M_{k+1} \cap N = \dots \qquad \frac{M_k + N}{N} = \frac{M_{k+1} + N}{N} = \dots$$

Έστω $n \geq k$, τότε $M_n \subseteq M_{n+1}$, $M_n \cap N = M_{n+1} \cap N$ και $M_n + N = M_{n+1} + N$. Από την modularity, παίρνω $M_n = M_{n+1}$. □

Παρατήρηση. *Έστω V ένας $\mathbf{F}$-διανυσματικός χώρος με $\dim_{\mathbf{F}} V < \infty$. Σε ένα μάθημα γραμμικής άλγεβρας μαθαίνει κάποιος (μέσω της ισότητας $\dim_{\mathbf{F}} \ker f + \dim_{\mathbf{F}} \mathrm{im} f = \dim_{\mathbf{F}} V$) ότι ένας ενδομορφισμός $f : V \to V$ είναι 1-1 αν και μόνο αν είναι επί. Στην πραγματικότητα, αυτό συμβαίνει διότι το $\mathbf{F}$-πρότυπο V ικανοποιεί τις συνθήκες άλυσης, δηλαδή είναι ταυτόχρονα της Noether και του Artin. Πράγματι, έστω ένα R-πρότυπο M της Noether και $f : M \to M$ ένας επιμορφισμός.Θα δείξω ότι είναι 1-1, θεωρώ την ακολουθία*

$$\ker f \subseteq \ker f^2 \subseteq \ker f^3 \subseteq \dots$$

Από την συνθήκη αύξουσα άλυσης υπάρχει $n \in \mathbf{N}$ με $\ker f^n = \ker f^{n+1} = \dots$. Έστω $x \in \ker f^n$ και αφού f^n επί (η f είναι επί και από αυτό έπεται ότι η f^n είναι επίσης επί) υπάρχει $y \in M$, με $f^n(y) = x$. Συνεπώς $f^{2n}(y) = f^n(x) = 0$ και άρα $y \in \ker f^{2n} = \ker f^n$, δηλαδή $x = f^n(y) = 0$. Έπεται $\ker f \subseteq \ker f^n = 0 \Rightarrow \ker f = 0$. Ανάλογα αν N ένα R-πρότυπο του Artin και $g : N \to N$ ένας μονομορφισμός, τότε αυτός είναι και επί.

2.2 Απλοί και ημιαπλοί δακτύλιοι.

Πρόταση 2.2.1. *Οι επόμενες συνθήκες είναι ισοδύναμες για ένα R-πρότυπο M.*

(i) *Το M είναι μη μηδενικό και δεν έχει γνήσια, μη μηδενικά υποπρότυπα.*

(ii) *Για κάθε $x \in M \setminus \{0\}$ είναι $M = Rx$*

(iii) *$M \simeq R/m$ για κάποιο γνήσιο μεγιστικό αριστερό ιδεώδες $m \subseteq R$*

Στην περίπτωση αυτή το R-πρότυπο M λέγεται απλό.

Απόδειξη : $(i) \to (ii)$: Για κάθε $x \in M \setminus \{0\}$, το $Rx \subseteq M$ είναι ένα μη μηδενικό R-υποπρότυπο και άρα από υπόθεση $M = Rx$.

$(ii) \to (iii)$: Σταθεροποιώ ένα $x \in M \setminus \{0\}$ και έστω η R-γραμμική απεικόνιση $f : R \to M$ με $f(r) = rx$. Από υπόθεση, έπεται ότι f επί, άρα από το πρώτο θεώρημα ισομορφισμών $R/m \simeq M$, όπου $m = \ker f$. Αρκεί να δειχθεί ότι m μεγιστικό. Έστω J ιδεώδες με $m \subsetneq J$ και $r \in J \setminus m$. Το υποπρότυπο $R(r+m) \subseteq R/m$ είναι μη μηδενικό και άρα από υπόθεση $R(r+m) = R/m$. Άρα υπάρχει $s \in R$, ώστε $sr + m = 1 + m \iff 1 - sr \in m \subseteq J$, οπότε $1 = (1 - sr) + sr \in J \Rightarrow 1 \in J \iff J = R$

$(iii) \to (i)$: Άμεσο από το θεώρημα της αντιστοιχίας. □

Παράδειγμα. *Τα απλά $\mathbf{Z}$-πρότυπα είναι οι κυκλικές ομάδες $\mathbf{Z}_p$, όπου p πρώτος.*

Πρόταση 2.2.2 (Λήμμα του Schur). *Έστω $f : M \to N$ μια γραμμική απεικόνιση μεταξύ απλών R-προτύπων. Τότε $f = 0$ ή f ισομορφισμός. Ειδικότερα, αν M απλό, ο δακτύλιος $\mathrm{End}_R(M)$ είναι διαιρετικός.*

Απόδειξη : Αν $f \neq 0$, τότε $\ker f \neq M$ και $\mathrm{im} f \neq 0$. Αφού M, N απλά R-πρότυπα και $\ker f \subseteq M$ και $\mathrm{im} f \subseteq N$, η f είναι 1-1 και επί. □

Παράδειγμα (Το αντίστροφο του λήμματος του Schur δεν ισχύει). *Υπάρχουν S-πρότυπα M που δεν είναι απλά, αλλά ο δακτύλιος $\mathrm{End}_S M$ να είναι διαιρετικός. Θεωρώ το $\mathbf{Z}$-πρότυπο $\mathbf{Q}$. Το $\mathbf{Q}$ προφανώς δεν είναι απλό $\mathbf{Z}$-πρότυπο, για παράδειγμα το $\mathbf{Z}$ είναι ένα γνήσιο $\mathbf{Z}$-υποπρότυπο. Ο δακτύλιος των ενδομορφισμών $\mathrm{End}_{\mathbf{Z}}\mathbf{Q}$ είναι διαιρετικός. Στην πραγματικότητα είναι $\mathrm{End}_{\mathbf{Z}}\mathbf{Q} \simeq \mathbf{Q}$. Παρατηρούμε, ότι για κάθε $f : \mathbf{Q} \to \mathbf{Q}$ προσθετική είναι*

$$mf(1) = f(m) = f\left(n\frac{m}{n}\right) = nf\left(\frac{m}{n}\right) \Rightarrow f\left(\frac{m}{n}\right) = f(1)\frac{m}{n}$$

Συνεπώς, είναι προφανές ότι η απεικόνιση

$$\mathrm{End}_{\mathbf{Z}}\mathbf{Q} \longrightarrow \mathbf{Q}$$

$$f \longmapsto f(1)$$

είναι ισομορφισμός δακτυλίων.

Ορισμός 2.2.1. *Το R-πρότυπο M καλείται ημιαπλό, αν για κάθε υποπρότυπο $N \subseteq M$ υπάρχει υποπρότυπο $K \subseteq M$, με $M = N \oplus K$.*

Πρόταση 2.2.3. *Αν το M είναι ημιαπλό R-πρότυπο και $N \subseteq M$ υποπρότυπο, τότε τα R-πρότυπα N και M/N είναι ημιαπλά.*

Απόδειξη : Έστω K υποπρότυπο του N, άρα K υποπρότυπο και του M. Αφού το M είναι ημιαπλό R-πρότυπο, υπάρχει $L \subseteq M$ υποπρότυπο τέτοιο ώστε $M = K \oplus L$. Εύκολα αποδεικνείεται ότι $N = K \oplus (N \cap L)$, άρα το N είναι ημιαπλό R-πρότυπο. Θα δείξω τώρα ότι το R-πρότυπο M/N είναι ημιαπλό. Γνωρίζουμε, ότι υπάρχει R-πρότυπο N', τέτοιο ώστε $M = N \oplus N'$, άρα $M/N = (N \oplus N')/N \simeq N'$. Το N' είναι ημιαπλό σαν υποπρότυπο ημιαπλού προτύπου. □

Πρόταση 2.2.4. *Έστω M ένα ημιαπλό R-πρότυπο με $M \neq 0$. Τότε υπάρχει απλό R-πρότυπο $N \subseteq M$.*

Απόδειξη. Έστω $x \in M \setminus \{0\}$. Χωρίς βλάβη της γενικότητας, μπορώ να υποθέσω ότι $M = Rx$. Έστω το σύνολο

$$\mathscr{X} = \{K \subseteq M : K \text{ υποπρότυπο και } x \notin K\}$$

και το εφοδιάζω με την μερική διάταξη του περιέχεστε. $\mathscr{X} \neq \emptyset$, καθώς $0 \in \mathscr{X}$ και από το λήμμα του Zorn, επιλέγω μεγιστικό στοιχείο $K \in \mathscr{X}$. Από υπόθεση υπάρχει υποπρότυπο $N \subseteq M$, με $N \oplus K = M$. Θα δείξω ότι το N είναι απλό. Αρχικά $N \neq 0$, καθως αν $N = 0$, τότε $M = K \oplus N = K$ και άρα $x \in K$ #. Έστω τώρα $N' \subseteq N$ με $N' \neq 0$, θα δείξω ότι $N' = N$. Είναι $K \subsetneq N' + K$, γιατί αν $K = K + N'$, τότε $N' \subseteq K$ αλλά και $N' \subseteq N$, συνεπώς $N' \subseteq N \cap K = 0$ #. Αφού $K \subsetneq K + N'$ και K μεγιστικό στοιχείο της $\mathscr{X}$, έπεται $K + N' \notin \mathscr{X}$ και άρα $x \in K + N' \overset{M=Rx}{\Rightarrow} K + N' = M$ αλλά και $N' + K = M = N + K$ άρα $N' \cap K \subseteq N \cap K = 0$, οπότε $N' \cap K = 0 = N \cap K$. Από την modularity έπεται ότι $N' = N$. □

Πρόταση 2.2.5. *Έστω M ένα R-πρότυπο και $M_1, M_2, \dots, M_n \subseteq M$ υποπρότυπα του. Οι επόμενες συνθήκες είναι ισοδύναμες :*

(i) $M_i \cap \left(\sum_{j \neq i} M_j\right) = 0$ *για κάθε* $i = 1, 2, \dots, n$

(ii) κάθε $x \in \sum_{i=1}^n M_i$ *γράφεται με μοναδικό τρόπο ως* $x = \sum_i x_i$*, όπου* $x_i \in M_i$.

Σε αυτή την περίπτωση, τα υποπρότυπα $M_1, \dots, M_n$ λέγονται γραμμικά ανεξάρτητα.

Απόδειξη. $(i) \to (ii)$ Έστω $x = \sum_i x_i = \sum_i x_i'$, τότε για κάθε $j = 1, 2, \dots, n$, έχουμε $x_j - x_j' = \sum_{i \neq j} x_i' - x_i$, άρα $x_j - x_j' \in M_i \cap \left(\sum_{j \neq i} M_j\right) = 0$ για κάθε j, δηλαδή $x_j = x_j'$ για κάθε j.

$(ii) \to (i)$ Έστω $x_i \in M_i \cap \left(\sum_{j \neq i} M_j\right)$, άρα υπάρχουν $x_j \in M_j$ για κάθε $j \neq i$, τέτοια ώστε $x_i = \sum_{j \neq i} x_j \iff x_1 + x_2 + \dots + x_{j-1} - x_j + x_{j+1} + \dots + x_n = 0$, αλλά από υπόθεση το 0 γράφεται κατά μοναδικό τρόπο, άρα $x_j = 0$ για κάθε j. □

Ορισμός 2.2.2. *Μια οικογένεια υποπροτύπων $(M_\lambda)_{\lambda \in \Lambda}$ λέγεται γραμμικά ανεξάρτητη αν για κάθε πεπερασμένο υποσύνολο $\{\lambda_1, \lambda_2, \dots \lambda_n\} \subseteq \Lambda$ τα υποπρότυπα $M_{\lambda_1}, M_{\lambda_2}, \dots, M_{\lambda_n}$ είναι γραμμικά ανεξάρτητα.*

Πρόταση 2.2.6. *Για κάθε οικογένεια υποπροτύπων $(M_\lambda)_{\lambda \in \Lambda}$, υπάρχει μεγιστικό υποσύνολο $\Lambda' \subseteq \Lambda$, ώστε η υποοικογένεια $(M_\lambda)_{\lambda \in \Lambda'}$ να είναι γραμμικά ανεξάρτητη.*

Απόδειξη. Άμεσο πόρισμα του Λήμματος του Zorn. □

Παρατήρηση. *Αν $(M_\lambda)_{\lambda \in \Lambda}$ είναι μια οικογένεια υποπροτύπων και $(M_\lambda)_{\lambda \in \Lambda'}$ είναι μια μεγιστική γραμμικά ανεξάρτητη υποοικογένεια τότε ενδέχεται ο εγκλεισμός :*

$$\bigoplus_{\lambda \in \Lambda'} M_\lambda = \sum_{\lambda \in \Lambda'} M_\lambda \subseteq \sum_{\lambda \in \Lambda} M_\lambda$$

να είναι γνήσιος. Πράγματι, έστω $U, V \subseteq \mathbf{R}^3$ δυο υπόχωροι διάστασης 2, με $U \neq V$, τότε $U + V = \mathbf{R}^3$, αλλά μια μεγιστική υποοικογένεια της $\{U, V\}$ είναι η $\{U\}$ και προφανώς $U \neq \mathbf{R}^3 = U + V$.

Πρόταση 2.2.7. *Έστω $(M_\lambda)_{\lambda \in \Lambda}$ μια οικογένεια απλών R-υποπροτύπων του M και $(M_\lambda)_{\lambda \in \Lambda'}$, μια μεγιστική γραμμικά ανεξάρτητη υποοικογένεια. Τότε :*

$$\bigoplus_{\lambda \in \Lambda'} M_\lambda = \sum_{\lambda \in \Lambda'} M_\lambda = \sum_{\lambda \in \Lambda} M_\lambda$$

Απόδειξη. Για να δείξω ότι $\sum_{\lambda \in \Lambda} M_\lambda \subseteq \sum_{\lambda \in \Lambda'} M_\lambda$, αρκεί να δειχθεί ότι για κάθε $\ell \in \Lambda \setminus \Lambda'$ ισχύει ότι $M_\ell \subseteq \sum_{\lambda \in \Lambda'} M_\lambda = M'$. Έστω, ως προς άτοπο, ότι υπάρχει $\ell \notin \Lambda'$, τέτοιο ώστε $M_\ell \nsubseteq M'$, τότε $M_\ell \cap M' \subsetneq M_\ell$. Αφού το M_ℓ είναι απλό, έπεται ότι $M' \cap M_\ell = 0$ και άρα το άθροισμα $M' + M_\ell$ είναι ευθύ, όμως :

$$M_\ell + M' = M_\ell \oplus M' = M_\ell \oplus \left(\bigoplus_{\lambda \in \Lambda'} M_\lambda\right) = \bigoplus_{\lambda \in \Lambda' \cup \{\ell\}} M_\lambda$$

Αυτό όμως αντίκειται στον μεγιστικό χαρακτήρα του Λ'. □

Πρόταση 2.2.8. *Τα επόμενα είναι ισοδύναμα για ένα R-πρότυπο M :*

(i) Το M ειναι ημιαπλό.

(ii) $M = \sum_{i \in I} M_i$ για κάποια οικογένεια $(M_i)_{i \in I}$ απλών υποπροτύπων του M.

(iii) $M = \bigoplus_{i \in I'} M_i$ για κάποια γραμμικά ανεξάρτητη οικογένεια $(M_i)_{i \in I'}$ απλών υποπροτύπων του M.

Απόδειξη : $(ii) \leftrightarrow (iii)$: Από τα προηγούμενα.

$(i) \to (ii)$: Έστω $(M_i)_{i \in I}$ η συλλογή όλων των απλών υποπροτύπων του M και $M' = \sum_{i \in I} M_i$. Γνωρίζω ότι υπάρχει $M'' \subseteq M$ τέτοιο ώστε $M'' \oplus M' = M$. Θα δείξω ότι $M'' = 0$ και τότε $M = M' = \sum_{i \in I} M_i$. Έστω, ως προς άτοπο ότι $M'' \neq 0$, τότε το M'' είναι ημιαπλό και άρα υπάρχει ένα απλό υποπρότυπο $N \subseteq M''$. Προφανώς το N είναι απλό υποπρότυπο και του M και άρα $N \subseteq \sum_{i \in I} M_i = M'$. Είναι άρα $N \subseteq M' \cap M'' = 0$ #

$(ii) \to (i)$: Έστω $N \subseteq M$ υποπρότυπο και έστω

$$\mathscr{X} = \left\{ J \subseteq I : \left(\sum_{i \in J} M_i \right) \cap N = 0 \right\}$$

Το $\mathscr{X}$ είναι διάφορο του κενού, καθώς $\emptyset \in \mathscr{X}$. Από το λήμμα του Zorn, υπάρχει μεγιστικό στοιχείο $J_0 \in \mathscr{X}$. Θα δείξω ότι $N + \sum_{i \in J_0} M_i = M$. Πράγματι αρκεί να δείξω ότι $M \subseteq N + \sum_{i \in J_0} M_i = M'$, δηλαδή ότι για κάθε $t \in I$ είναι $M_t \subseteq M'$. Έστω, ως προς άτοπο, ότι υπάρχει $t \in I$, με $M_t \nsubseteq M'$. Καθώς $M_t \cap M' \subsetneq M_t$ και το M_t είναι απλό, έπεται $M_t \cap M' = 0$ και άρα το άθροισμα $M_t + M' = M_t + \sum_{i \in J_0} M_i$ είναι ευθύ. Παρατηρώ ότι

$$M_t \oplus M' = M_t \oplus \left(N \oplus \bigoplus_{i \in J_0} M_i \right) = N \oplus \left(M_t \oplus \bigoplus_{i \in J_0} M_i \right) = N \oplus \left(\bigoplus_{i \in J_0 \cup \{t\}} M_i \right)$$

Συνεπώς $J_0 \cup \{t\} \in \mathscr{X}$. Αυτό, όμως αντίκειται στο μεγιστικό χαρακτήρα του J_0 #. □

Πρόταση 2.2.9. *Οι επόμενοι ισχυρισμοί είναι ισοδύναμοι για έναν δακτύλιο R:*

(i) Κάθε R-πρότυπο R είναι ημιαπλό.

(ii) Κάθε πεπερασμένα παραγόμενο R-πρότυπο είναι ημιαπλό.

(iii) για κάθε αριστερό ιδεώδες $I \subseteq R$ το R-πρότυπο R/I είναι ημιαπλό

(iv) Το R-πρότυπο R είναι ημιαπλό.

Στην περίπτωση αυτή, ο δακτύλιος R καλείται (αριστερά)[3] ημιαπλός.

Απόδειξη : $(i) \to (ii) \to (iii) \leftrightarrow (iv)$: Έχουν δειχθεί.

$(iii) \to (i)$: Έστω M ένα R-πρότυπο. Για κάθε $x \in M$, θεωρώ την R-γραμμική απεικόνιση $f : R \to M$ με $f(r) = rx$. Από το πρώτο θεώρημα ισομορφισμών, υπάρχει ιδεώδες $I \subseteq R$ με $R/I \simeq Rx$. Συνεπώς για κάθε $x \in M$ το $Rx \subseteq M$ είναι ημιαπλό. Τέλος, αφού το $M = \sum_{x \in M} Rx$ είναι άθροισμα ημιαπλών προτύπων και αυτά είναι άθροισμα απλών προτύπων, με την σειρά του το M είναι άθροισμα απλών. □

[3] Θα δείξουμε ότι οι αριστερά ημιαπλοί είναι ακριβώς οι δεξιά ημιαπλοί.

Λήμμα 2.2.1. *Έστω R δακτύλιο με $R = \bigoplus_{\lambda\in\Lambda} I_\lambda$ για κάποια οικογένεια ελαχιστικών αριστερών ιδεωδών $(I_\lambda)_{\lambda\in\Lambda}$. Τότε $\#\Lambda < \infty$.*[4]

Απόδειξη : Αφού $1_R \in \bigoplus_{\lambda\in\Lambda} I_\lambda$, υπάρχουν $\lambda_1, \lambda_2, \ldots, \lambda_n \in \Lambda$ και $e_i \in I_{\lambda_i}$ με $\sum_{i=1}^n e_i = 1_r$. Θα δείξω ότι $\Lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_n\} = \Lambda'$. Έστω, ως προς άτοπο ότι υπάρχει $\ell \in \Lambda \setminus \Lambda'$, τότε επιλέγω $x \in I_\ell$ και έχω $x = x \cdot 1_r = \sum_{i=1}^n xe_i \in I_\ell \cap (\sum_{i=1}^n I_{\lambda_i}) = 0$. Άρα $I_\ell = 0$ #. □

Παρατηρήσεις. *(i) Αν R αριστερά ημιαπλός, τότε ο R είναι αριστερά της Noether και του Artin. Πράγματι, γνωρίζουμε ότι υπάρχουν ελαχιστικά ιδεώδη $I_1, \ldots, I_n \subseteq R$ τέτοια ώστε $R = \bigoplus_{i=1}^n I_i = \sum_{i=1}^n I_i$. Τα ιδεώδη I_i είναι απλά R-πρότυπα, δηλαδή δεν έχουν μη τετριμμένα υποπρότυπα, συνεπώς είναι της Noether και του Artin και άρα και το πεπερασμένο άθροισμα τους είναι της Noether και του Artin.*

(ii) Αν R, S αριστερά ημιαπλοί, τότε ο $R \times S$ είναι αριστερά ημιαπλός. Πράγματι, γνωρίζουμε ότι $R = \bigoplus_{i=1}^n I_i$ και $S = \bigoplus_{i=1}^m J_i$ για κάποια ελαχιστικά ιδεώδη $I_1, \ldots, I_n \subseteq R$ και $J_1, \ldots, J_n \subseteq S$. Τότε έχω $R \times S = (R \times 0) \oplus (0 \times S) = \bigoplus_{i=1}^n (I_i \times 0) \oplus \bigoplus_{i=1}^m (0 \times J_i)$

Παράδειγμα. *Αν $\mathbf{F}_1, \ldots, \mathbf{F}_n$ σώματα, τότε $\mathbf{F}_1 \times \cdots \times \mathbf{F}_n$ αριστερά ημιαπλός.*

Ορισμός 2.2.3. *Ένας δάκτυλιος R λέγεται απλός αν για κάθε αμφίπλευρο ιδεώδες I, ισχύει ότι $I = 0$ ή $I = R$.*

2.3 Το θεώρημα Wedderburn-Artin

Πρόταση 2.3.1. *Έστω D ένας διαιρετικός δακτύλιος και θέτουμε $R = \mathbf{M}_n(D)$. Ισχύουν τα παρακάτω:*

(i) Ο R είναι ένας απλός δακτύλιος.

(ii) Ο R είναι αριστερά της Noether και του Artin.

(iii) Η αβελιανή ομάδα $V = D^n = \{(d_1, \ldots, d_n)^T : d_1, \ldots, d_n \in D\}$ είναι ένα απλό R-πρότυπο με την φυσιολογική δράση.

(iv) Υπάρχει ισομορφισμός R-προτύπων $\mathrm{End}_R V \simeq D^{op}$

Απόδειξη : (i) Έστω I ένα αμφίπλευρο ιδεώδες με $I \neq 0$ και $A \in I$,με $A \neq 0$. Γράφω $A = (a_{ij}) = \sum_{i,j} a_{i,j} E_{i,j}$, όπου $E_{i,j}$ η συνήθης βάση του $\mathbf{M}_n(D)$. Αφού $A \neq 0$, υπάρχουν $\kappa, \lambda \in \mathbf{N}$ με $a_{\kappa,\lambda} \neq 0$. Για να δείξουμε ότι $I = \mathbf{M}_n(D)$, αρκεί να δείξουμε ότι $E_{\alpha\beta} \in I$ για κάθε $\alpha, \beta \in \{1, 2, \ldots, n\}$, μιας και τότε για κάθε $X = (x_{i,j}) \in \mathbf{M}_n(D)$ ισχύει ότι $X = \sum_{i,j} x_{i,j} E_{i,j} = \sum_{i,j} (x_{i,j} I_n) E_{i,j} \in I$. Παρατηρούμε ότι

$$E_{\alpha\beta} = E_{\alpha\kappa}(\alpha_{\kappa\lambda}^{-1} I_n) A E_{\lambda\beta} \in I$$

καθώς ισχύει $E_{\alpha\kappa} E_{ij} E_{\lambda\beta} = \begin{cases} E_{\alpha\beta} & \kappa = i \text{ και } j = \lambda \\ 0 & \text{αλλιώς} \end{cases}$

(ii) Ο D εμφυτεύεται ως υποδακτύλιος του $\mathbf{M}_n(D)$ μέσω του ομομορφισμού $d \longmapsto d \cdot I_n \in \mathbf{M}_n(D)$, $d \in D$. Συνεπώς κάθε αριστερό ιδεώδες είναι ένας D-διανυσματικός υπόχωρος του $R = \mathbf{M}_n(D)$. Όμως $\dim_D \mathbf{M}_n(D) = n^2 < \infty$

(iii) Αρκεί να δείξω ότι για κάθε $v \in V/\{0\}$ ισχύει ότι $Rv = V$. Έστω $v = \sum_{i=1}^n v_i e_i \in V$ ένα μη μηδενικό στοιχείο, τότε υπάρχει $i = 1, 2, \ldots, n$ με $v_i \neq 0$. Τότε για κάθε $k = 1, 2, \ldots, n$

$$e_k = (v_i^{-1} E_{k,i}) v \in V$$

[4] Η ύπαρξη μονάδας σε έναν δακτύλιο είναι μια έννοια συμπάγειας.

(iv) Για κάθε $d \in D$, θεωρώ την R-γραμμική απεικόνιση $r_d : V \to V$ όπου

$$r_d \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} = \begin{pmatrix} d_1 \cdot d \\ \vdots \\ d_n \cdot d \end{pmatrix} \in V$$

Η r_d είναι R-γραμμική. Πράγματι, για κάθε $A \in \mathbf{M}_n(D)$ και $v = (d_1, \ldots, d_n)^T \in V$ είναι :

$$r_d(Av) = r_d \begin{pmatrix} \sum_j a_{1,j} d_j \\ \vdots \\ \sum_j a_{n,j} d_j \end{pmatrix} = \begin{pmatrix} (\sum_j a_{1,j} d_j) \cdot d \\ \vdots \\ (\sum_j a_{n,j} d_j) \cdot d \end{pmatrix} = \begin{pmatrix} \sum_j a_{1,j} (d_j \cdot d) \\ \vdots \\ \sum_j a_{n,j} (d_j \cdot d) \end{pmatrix} = A \cdot \begin{pmatrix} d_1 \cdot d \\ \vdots \\ d_n \cdot d \end{pmatrix} = A \cdot r_d \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$$

δηλαδή $r_d \in \mathrm{End}_R V$ για κάθε $d \in D$. Η απεικόνιση $r : D^{op} \to \mathrm{End}_R V$ είναι 1-1, επί, προσθετική, απεικονίζει το 1_D στην $1_V : V \to V$ και $r(d_1 \cdot d_2) = r(d_2) \circ r(d_1)$. Θα δείξουμε το 1-1 και επί, τα υπόλοιπα αφήνονται σαν άσκηση. Έχουμε :

- 1-1 : Έστω $d_1, d_2 \in D$ με $r_{d_1} = r_{d_2}$, τότε $r_{d_1}(1, 0, \ldots, 0)^T = r_{d_2}(1, 0, \ldots, 0)^T \iff d_1 = d_2$.
- επί : Έστω $f : V \to V$ μια προσθετική απεικόνιση με $f(A \cdot v) = A \cdot f(v) \in V$ για κάθε $A \in \mathbf{M}_n(D)$ και $v \in V$. Θεωρώ το $f(1, 0, \ldots, 0)^T = (d, *, \ldots, *) \in V$, όπου $d \in D$. Τότε για κάθε $v = (d_1, \ldots, d_n)^T \in V$ είναι :

$$f(v) = f \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} = f \left(\begin{pmatrix} d_1 & 0 & \ldots & 0 \\ d_2 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ d_n & 0 & \ldots & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \right) = \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ d_2 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ d_n & 0 & \ldots & 0 \end{pmatrix} f \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} =$$

$$= \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ d_2 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ d_n & 0 & \ldots & 0 \end{pmatrix} \begin{pmatrix} d \\ * \\ \vdots \\ * \end{pmatrix} = \begin{pmatrix} d_1 \cdot d \\ d_2 \cdot d \\ \vdots \\ d_n \cdot d \end{pmatrix} = r_d \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}$$

□

Πόρισμα 2.3.1. *Έστω $n \in \mathbf{N}$, $D_1, D_2, \ldots, D_r$ διαιρετικοί δακτύλιοι και $n_1, \ldots, n_r \in \mathbf{N}$. Τότε ο δακτύλιος $R = \mathbf{M}_{n_1}(D_1) \times \cdots \times \mathbf{M}_{n_r}(D_r)$ είναι ημιαπλός.*

Πόρισμα 2.3.2. *Το αριστερό R-πρότυπο R είναι ${}_R R \simeq \bigoplus_{i=1}^n V = V^n$ και αφού το R-πρότυπο V είναι απλό, επέται ότι ο δακτύλιος R είναι ημιαπλός.*

Απόδειξη : Παρατηρούμε ότι $R \simeq I_1 \oplus \cdots \oplus I_n$, όπου $I_k \subseteq R$ είναι το σύνολο των $n \times n$ πινάκων που έχουν παντού μηδενικά, εκτός από την k-στήλη, δηλαδή

$$I_k = \{A = (a_{i,j}) \in R : a_{i,j} = 0 \text{ για κάθε } j \neq k\}$$

Είναι προφανώς $I_k \simeq V$ για κάθε $k = 1, 2, \ldots, n$ και άρα ${}_R R \simeq \bigoplus_{k=1}^n I_k \simeq V^n$ □

Πρόταση 2.3.2. *Έστω D διαιρετικός δακτύλιος, $R = \mathbf{M}_n(D)$ και $V = D^n$. Τότε κάθε απλό R-πρότυπο είναι ισόμορφο με το V.*

Απόδειξη : Έστω U ένα απλό R-πρότυπο με $U \not\simeq V$. Είναι $U \neq 0$ και $U \simeq R/m$ για κάποιο μεγιστικό αριστερό ιδεώδες $m \subseteq R$. Η απεικόνιση πηλίκο $p : R \to R/m = U$ δεν είναι η μηδενική απεικόνιση και άρα $\mathrm{Hom}_R(R, U) \neq 0$, όμως ${}_R R = V \oplus \cdots \oplus V$ και άρα

$$\mathrm{Hom}_R(R, U) = \mathrm{Hom}_R(V \oplus \cdots \oplus V, U) = \mathrm{Hom}_R(V, U) \oplus \cdots \oplus \mathrm{Hom}_R(V, U)$$

Από το λήμμα του Schur, έχουμε $\mathrm{Hom}_R(V, U) = 0$ και άρα $\mathrm{Hom}_R(R, U) = 0$ #. □

Πρόταση 2.3.3. *Υπάρχει ισομορφισμός δακτυλίων* $\mathrm{End}_R(M^n) \simeq \mathbf{M}_n(\mathrm{End}_R M)$.

Απόδειξη : Αν $M_1, \ldots, M_m$ και $N_1, \ldots, N_n$ R-πρότυπα και $M = \bigoplus_{j=1}^m M_j$, $N = \bigoplus_{i=1}^n N_i$. Για κάθε $f : M \to N$, θεωρούμε την απεικόνιση $p_i \circ f \circ v_j : M_j \to N_i$, όπου $p_i : N \to N_i$ η προβολή και $v_j : N_j \to N$ η ένθεση. Ισχύει ότι υπάρχει ισομορφισμός αβελιανών ομάδων

$$\mathrm{Hom}_R(M, N) \simeq \bigoplus_{i=1}^n \mathrm{Hom}_R(M, N_i) \simeq \bigoplus_{i=1}^n \bigoplus_{j=1}^n \mathrm{Hom}_R(M_j, N_i)$$

$$f \longrightarrow (p_i \circ f)_i \longrightarrow (p_i \circ f \circ v_j)_{i,j}$$

Είναι $\mathrm{Hom}_R(M, N) \simeq (n \times m$ πίνακες με την ομάδα $\mathrm{Hom}_R(M_j, N_i)$ στην $(i, j) -$ θέση). Η αντιστοιχία αυτή αντιστοιχεί στη σύνθεση γραμμικών απεικονίσεων το γινόμενο πινάκων. Πράγματι, έστω $M = \bigoplus_{j=1}^m M_j$, $N = \bigoplus_{i=1}^n N_i$, $L = \bigoplus_{k=1}^l L_k$ και R-γραμμικές απεικονίσεις $f : M \to N$, $g : N \to L$. Τότε η σύνθεση $g \circ f : M \to L$ αντιστοιχεί στον πίνακα $(\sum_{k=1}^n g_{k,i} \circ f_{i,j})_{k,j}$. Είναι $f(m_j) = \sum_{i=1}^n f_{i,j}(m_j)$ και $g(n_i) = \sum_{k=1}^l g_{k,i}(n_i)$ για κάθε $m_j \in M_j$ και $n_i \in N_i$. Άρα για κάθε $j = 1, 2, \ldots, m$ και $m_j \in M_j$ είναι

$$(g \circ f)(m_j) = g\left(\sum_{i=1}^n f_{i,j}(m_j)\right) = \sum_{i=1}^n g(f_{i,j}(m_j)) = \sum_{i=1}^n \sum_{k=1}^l g_{k,i}(f_{i,j}(m_j))$$

□

Πόρισμα 2.3.3. *Αν* $M = \bigoplus_{i=1}^n M_i$ *και* $\mathrm{Hom}_R(M_i, M_j) = 0$ *για κάθε* $i \neq j$, *τότε* $\mathrm{End}_R(M) \simeq \prod_{i=1}^n \mathrm{End}_R(M_i)$

Απόδειξη : Είναι

$$\mathrm{End}_R(M) := \mathrm{Hom}_R(M, M) \simeq \bigoplus_{i,j=1}^n \mathrm{Hom}_R(M_i, M_j) = \left(\bigoplus_{i=j} \mathrm{Hom}_R(M_i, M_i)\right) \oplus \left(\bigoplus_{i \neq j} \mathrm{Hom}_R(M_i, M_j)\right)$$

$$= \bigoplus_{i=1}^n \mathrm{Hom}_R(M_i, M_i) = \bigoplus_{i=1}^n \mathrm{End}_R(M_i)$$

□

Πρόταση 2.3.4. *Αν ο* R *είναι ένας δακτύλιος, τότε* $\mathrm{End}_R R \simeq R^{op}$

Απόδειξη. Έστω $r \in R$ και $f_r : R \to R$ η απεικόνιση με $f_r(x) = x \cdot r$ για κάθε $x \in R$. Η f_r είναι R-γραμμική. Η απεικόνιση $f : R^{op} \to \mathrm{End}_R R$ με $r \longmapsto f_r$ είναι ισομορφισμός δακτυλίων. Είναι εύκολο να δειχθεί ότι η f είναι προσθετική, πολλαπλασιαστική και στέλνει την μονάδα στην ταυτοτική απεικόνιση . Θα δείξω ότι η f είναι αμφιμονοσήμαντη. Για το 1-1, έστω $r \in R$ με $f_r = 0 \in \mathrm{End}_R R$, τότε $f_r(1) = 0 \iff r = 0$. Τέλος για το επί, ισχύει ότι για κάθε $g \in \mathrm{End}_R R$ είναι $g = f_{g(1)}$. Πράγματι, για κάθε $x \in R$ $g(x) = g(x \cdot 1) = x \cdot g(1) = f_{g(1)}(x)$. □

Θεώρημα 2.3.1 (Wedderburn-Artin). *Έστω* R *ένας ημιαπλός δακτύλιος. Τότε υπάρχουν* $n_1, \ldots, n_r$ *φυσικοί αριθμοί και* $D_1, \ldots, D_r$ *διαιρετικοί δακτύλιοι, ώστε* $R \simeq \prod_{i=1}^r \mathbf{M}_{n_i}(D_i)$. *Επιπλέον το* r *και η* r*-αδα* $(D_1, n_1), \ldots, (D_r, n_r)$ *είναι μοναδικά ως προς αναδιάταξη.*

Απόδειξη : Μπορώ να γράψω ${}_R R = V_1^{n_1} \oplus \cdots \oplus V_r^{n_r}$, όπου τα $V_1, \ldots, V_r$ είναι απλά πρότυπα, ανά δύο μη ισόμορφα και $n_1, \ldots, n_r \geq 1$. Είναι

$$R^{op} \simeq \mathrm{End}_R R \simeq \mathrm{End}_R\left(\bigoplus_{i=1}^r V_i^{n_i}\right) \simeq \prod_{i=1}^r \mathrm{End}_R(V_i^{n_i}) \simeq \prod_{i=1}^r \mathbf{M}_{n_i}(\mathrm{End}_R V_i)$$

Συνεπώς

$$R \simeq \left(\prod_{i=1}^{r} \mathbf{M}_{n_i}(\mathrm{End}_R V_i)\right)^{op} \simeq \prod_{i=1}^{r} (\mathbf{M}_{n_i}(\mathrm{End}_R V_i))^{op} \simeq \prod_{i=1}^{r} \mathbf{M}_{n_i}((\mathrm{End}_R V_i)^{op})$$

Θέτοντας $D_i = (\mathrm{End}_R V_i)^{op}$ έχουμε την διάσπαση Wedderburn-Artin. Για την μοναδικότητα της διάσπασης, θα χρησιμοποιήσουμε το επόμενο λήμμα

Λήμμα 2.3.1. *Έστω R ενας δακτύλιος που διασπάται σαν*

$$R = \prod_{i=1}^{n} R_i \qquad\qquad R = \prod_{j=1}^{m} S_j$$

όπου οι $R_1, \ldots, R_n, S_1, \ldots, S_m$ απλοί υποδακτύλιοι, τότε $n = m$ και $R_i =$ [5] *S_i modulo κάποια αμφιμονοσήμαντη αντιστοιχία. για κάθε $i = 1, 2, \ldots, n$*

Απόδειξη λήμματος : Μπορώ να δω τους R_i και S_j σαν αμφίπλευρα ιδεώδη του R. Παρατηρώ, ότι $R_iR = R_i$ και εφαρμόζοντας το στην ισότητα $R = \prod_{j=1}^{m} S_j$, έχω $R_i = \prod_{j=1}^{m} R_iS_j$. Το R_iS_j είναι αμφίπλευρο ιδεώδες του S_j, άρα είτε είναι το 0 ή ο ίδιος ο S_j. Αφού $R \neq 0$, υπάρχει ένα $j = 1, 2, \ldots, m$, ώστε $R_iS_j = S_j$. Όμως το R_iS_j είναι και αμφίπλευρο ιδεώδες του R_i, άρα $R_i = R_iS_j = S_j$. □

Έστω ότι υπάρχουν φυσικοί $s, k_1, \ldots, k_s \in \mathbf{N}$ και διαιρετικοί δακτύλιοι $\Delta_1, \ldots, \Delta_s$, ώστε

$$R \simeq \prod_{i=1}^{r} \mathbf{M}_{n_i}(D_i) \simeq \prod_{i=1}^{s} \mathbf{M}_{k_i}(\Delta_i)$$

από το παραπάνω, παίρνω ότι $r = s$ και $\mathbf{M}_{n_i}(D_i) \simeq \mathbf{M}_{k_i}(\Delta_i)$ για κάθε $i = 1, 2, \ldots, r$. Για κάθε i, έχω

$$D_i^{n_i} \simeq D_i \cdot I_{n_i} \overset{!}{=} Z(\mathbf{M}_{n_i}(D_i)) \simeq Z(\mathbf{M}_{k_i}(\Delta_i)) \overset{!}{=} \Delta_i \cdot I_{k_i} \simeq \Delta_i^{k_i}$$

εφαρμόζοντας πάλι το προηγούμενο λήμμα, έχω $n_i = k_i$ και $\Delta_i \simeq D_i$. □

Παρατήρηση. *Στην παραπάνω απόδειξη, στην ισότητα $Z(\mathbf{M}_n(D)) = D \cdot I_n$ χρησιμοποιείται ουσιωδώς, ότι ο δακτύλιος D είναι διαιρετικός. Πράγματι, έστω $A = (a_{i,j}) \in \mathbf{M}_n(D)$ ένας πίνακας που μετατίθεται με όλους τους πίνακες, ειδικότερα για κάθε k, ℓ είναι $E_{k,\ell}A = AE_{k,\ell}$. Συνεπώς,*

$$Ae_k = AE_{k,\ell}e_\ell = E_{k,\ell}Ae_\ell \Rightarrow \begin{pmatrix} a_{1,k} \\ a_{2,k} \\ \vdots \\ a_{n,k} \end{pmatrix} = E_{k,\ell} \begin{pmatrix} a_{1,\ell} \\ a_{2,\ell} \\ \vdots \\ a_{n,\ell} \end{pmatrix} \Rightarrow \sum_{i=1}^{n} a_{i,k}e_i = a_{\ell,\ell}e_k$$

Από γραμμική ανεξαρτησία, παίρνουμε ότι για κάθε k, ℓ είναι $a_{k,k} = a_{\ell,\ell}$ και $a_{k,i} = 0$ για κάθε $i \neq \ell$. Αν R, S δακτύλιοι και $n, m \in \mathbf{N}$ με $\mathbf{M}_n(R) \simeq \mathbf{M}_m(S)$ δεν είναι απαραίτητο ότι $n = m$ και $R \simeq S$. Για να ισχύει αυτό πρέπει οι R, S να είναι διαιρετικοί. Για παράδειγμα $\mathbf{M}_2(\mathbf{M}_2(\mathbf{Z})) \simeq \mathbf{M}_4(\mathbf{Z})$.

[5] Ισχύει κάτι παραπάνω από ισομορφία. Ισχυει ισότητα.

2.4 Έφαρμογές

Πόρισμα 2.4.1. *Ο R είναι ημιαπλός αν και μόνο αν ο R^{op} είναι ημιαπλός. Συνεπώς ο R είναι αριστερά ημιαπλός αν και μόνο αν είναι δεξία ημιαπλός.*

Απόδειξη : Από την διάσπαση Wedderburn-Artin, υπάρχουν $n_1, \ldots, n_r \in \mathbf{N}$ και $D_1, \ldots, D_r$ διαιρετικοί δακτύλιοι τέτοιοι ώστε $R \simeq \prod_{i=1}^r \mathbf{M}_{n_i}(D_i)$. Είναι

$$R^{op} \simeq \left(\prod_{i=1}^r \mathbf{M}_{n_i}(D_i)\right)^{op} \simeq \prod_{i=1}^r (\mathbf{M}_{n_i}(D_i))^{op} \simeq \prod_{i=1}^r \mathbf{M}_{n_i}(D_i^{op})$$

□

Πόρισμα 2.4.2. *Οι μεταθετικοί ημιαπλό δακτύλιοι είναι ακριβώς της μορφής $\mathbf{F}_1 \times \cdots \times \mathbf{F}_r$, όπου $r \in \mathbf{N}$ και τα $\mathbf{F}_1, \ldots, \mathbf{F}_r$ είναι σώματα.*

Πρόταση 2.4.1 (Θεώρημα Δομής των απλών δακτυλιών του Artin.). *Τα επόμενα είναι ισοδύναμα για έναν δακτύλιο R :*

(i) $R = \mathbf{M}_n(D)$ *για κάποιο φυσικό $n \geq 1$ και D διαιρετικό δακτύλιο.*

(ii) *Ο R είναι απλός και ημιαπλός.*

(iii) *Ο R είναι απλός και αριστερά του Artin.*

(iv) *Ο R είναι απλός και δεξιά του Artin.*

(v) *Ο R έχει ενα απλό και πιστό αριστερό R-πρότυπο M και είναι αριστερά του Artin.*

Απόδειξη : $(i) \to (ii)$: Έχει δειχθεί.

$(ii) \to (i)$ ο R είναι ημιαπλός, συνεπώς από το θεώρημα Wedderburn-Artin $R \simeq \prod_{i=1}^r \mathbf{M}_{n_i}(D_i)$, για κάποιους διαιρετικούς δακτύλιος $D_1, \ldots, D_r$. Όμως ο R είναι απλός αν και μόνο αν $r = 1$.

$(ii) \to (iii), (ii) \to (iv)$: Έχει δειχθεί.

$(iii) \to (ii)$: Έστω $I \subseteq R$ ένα ελαχιστικό ιδεώδες του R, που υπάρχει λόγο της συνθήκης του Artin. Θεωρώ $\mathscr{X} = \{I' \subseteq R : I'$ αριστερό ιδεώδες και $I' \simeq I$ ως R-πρότυπα$\}$ και ορίζω

$$J = \sum_{I' \in \mathscr{X}} I'$$

Θα δείξω ότι το J είναι αμφίπλευρο ιδεώδες, καθώς τότε $0 \neq I \subseteq J$ και αφού ο R είναι απλός, είναι ${}_RR = {}_RJ$ είναι άθροισμα απλών προτύπων, δηλαδή το R-πρότυπο R είναι ημιαπλό. Αρκεί να δείξω ότι το J είναι δεξί ιδεώδες, δηλαδή ότι για κάθε $r \in R$ και αριστερό ιδεώδες $I' \in \mathscr{X}$ είναι $I' \cdot r \subseteq J$. Θεωρώ την απεικόνιση $\delta_r : I' \to R$, η οποία είναι R-γραμμική, με $\delta_r(x) = xr$. Προφανώς είναι $\mathrm{im}\delta_r = I' \cdot r$ και $\ker \delta_r \subseteq I'$. Από το ελαχιστικό χαρακτήρα του I', είναι $\ker \delta_r = 0$, που τότε $I' \simeq I' \cdot r \Rightarrow I' \cdot r \in \mathscr{X}$, είτε $\ker \delta_r = I'$ και άρα $I' \cdot r \subseteq J$.

$(iv) \to (ii)$: Δυϊκά με πριν.

$(i) \to (v)$: Γνωρίζουμε ότι ο R είναι απλός και το R-πρότυπο D^n είναι πιστό και απλό.

$(v) \to (i)$: Έστω M ένα πιστό και απλό R-πρότυπο, τότε αρκεί να δείξουμε ότι υπάρχει φυσικός n με ${}_RR \simeq M^n$, καθώς τότε $R^{op} \simeq \mathrm{End}_R R \simeq \mathrm{End}_R M^n \simeq \mathbf{M}_n(\mathrm{End}_R M)$ και άρα $R \simeq \mathbf{M}_n(D)$, όπου $D = (\mathrm{End}_R M)^{op}$ και ο D διαιρετικός από το λήμμα του Schur. Έστω η οικογένεια

$$\mathcal{F} = \{f : R \to M^n : f \text{ είναι } R\text{-γραμμική και } n \in \mathbf{N}\}$$

και θεωρώ την οικογένεια των αντίστοιχων πυρήνων

$$\mathcal{F}' = \{\ker f : f \in \mathcal{F}\}$$

Από την συνθήκη του Artin, η $\mathcal{F}'$ έχει ελαχιστικό στοιχείο και έστω η $f : R \to M^n$ που πετυχαίνει τον αντίστοιχο πυρήνα. Ισχυρίζομαι ότι ο η f είναι 1-1. Έστω ως προς άτοπο, ότι υπάρχει $r \neq 0$ με $f(r) = 0$, τότε αφού το M είναι πιστό, υπάρχει $m \in M$ με $rm \neq 0$. Θεωρώ την απεικόνιση

$$R \xrightarrow{\varphi} M^n \oplus M$$

$$\varphi : x \longmapsto (f(x), xm)$$

τότε $\ker \varphi \in \mathcal{F}'$ και $\ker \varphi = \ker f \cap \ker(x \longmapsto xm) \subsetneq \ker f$, αφού $r \in \ker f$ και $r \notin \ker \varphi$. Από το ελαχιστικό χαρακτήρα του $\ker f$ #. $\square$

Παράδειγμα (Ένας δακτύλιος γεμάτος αντιπαραδείγματα). *Έστω $\mathbf{F}$ σώμα, V ένας $\mathbf{F}$-διανυσματικός χώρος με βάση $\{e_n : n \in \mathbf{N}\}$ και $R = \mathrm{End}_{\mathbf{F}} V$. Θεωρώ το σύνολο $I = \{f \in R : \dim_{\mathbf{F}} \mathrm{im} f < \infty\} \subseteq R$. Το I είναι αμφίπλευρο ιδεώδες[6] και θεωρώ τον αντίστοιχο δακτύλιο πηλίκο*

$$S = R/I$$

Ο δακτύλιος S είναι ένας απλός δακτύλιος που δεν είναι αριστερά του Artin :
Θα δείξω ότι για κάθε $s \in S$ με $s \neq 0$, υπάρχουν $s_1, s_2 \in S$ με $s_1 \cdot s \cdot s_2 = 1_S$. Αρκεί να δείξω ότι για κάθε $f \notin I$, υπάρχουν $g, h \in R$ με $g \circ f \circ h = 1_V : V \to V$. Αφού $\dim \mathrm{im} f = \infty$, υπάρχουν $u_n \in V$, τέτοια ώστε $\mathrm{im} f = \langle f(u_n) : n \in \mathbf{N}\rangle$. Ορίζω $g, h : V \to V$ με $h(e_n) = u_n$ και $g(f(u_n)) = e_n$, τότε $(g \circ f \circ h)(e_n) = g(f(h(e_n))) = g(f(u_n)) = e_n$, συνεπώς $g \circ f \circ h = 1_V$. Συνεπώς, αν $J \subseteq S$ ένα αμφίπλευρο ιδεώδες με $J \neq 0$, τότε $1_S \in J$ και άρα $J = S$. Θα δείξω τώρα, ότι ο R δεν είναι αριστερά του Artin. Για κάθε υπόχωρο $U \subseteq V$, ορίζω

$$I_U = \{f \in R : f\big|_U = 0\} \subseteq R$$

Εύκολα βλέπουμε ότι το I_U είναι αριστερό ιδεώδες και για κάθε $U_1 \subseteq U_2$ είναι $I_{U_2} \subseteq I_{U_1}$. Ισχυρίζομαι, ότι αν $U \subseteq W \subseteq V$ με $\dim W/U = \infty$, τότε ο εγκλεισμός $I + I_W \subseteq I + I_U$ είναι γνήσιος. Πράγματι, έστω $(u_n)_n$ μια βάση του U και την επεκτείνω σε μια βάση $(u_n)_n \cup (w_n)_n$ του W. Γνωρίζω, ότι υπάρχει $f \in R$ με $f|_U = 0$ και $f(w_i) = w_i$ για κάθε $i = 1, 2, 3, \ldots$. Είναι βεβαίως $f \in I_U \subseteq I + I_U$, αλλά $f \notin I + I_W$, γιατί διαφορετικά θα υπήρχε $g \in I$ και $h \in I_W$ με $f = g + h$ και τότε θα είχα $w_i = f(w_i) = g(w_i) + h(w_i) = g(w_i) \subseteq \mathrm{im} g$, δηλαδή $w_i \in \mathrm{im} g$ για κάθε i. Αυτό είναι άτοπο, καθώς τότε $W \subseteq \mathrm{im} g$ και $\dim img < \infty$. Θεωρόντας τώρα μια αύξουσα ακολουθία υποχώρων $U_1 \subseteq U_2 \subseteq \ldots U_n \subseteq U_{n+1} \subseteq \ldots$ με $\dim U_{i+1}/U_i = \infty$ για κάθε $i \geq 1$, προκύπτει μια γνήσια φθίνουσα ακολουθία αριστερών ιδεωδών του $S = R/I$:

$$\frac{I + I_{U_1}}{I} \supsetneq \frac{I + I_{U_2}}{I} \supsetneq \cdots \supsetneq \frac{I + I_{U_n}}{I} \supsetneq \frac{I + I_{U_{n+1}}}{I} \supsetneq \ldots$$

Τελικά ο δακτύλιος $S = R/I$ είναι ένας απλός δακτύλιος, ο οποίος δεν είναι αριστερά του Artin και ειδικότερα δεν είναι ημιαπλός.

[6] Έστω $f, g \in I$, τότε $\mathrm{im}(f+g) \subseteq \mathrm{im} f + \mathrm{im} g$ και $\mathrm{im}(f \circ g) \subseteq \mathrm{im}(f),\ \mathrm{im}(g \circ f) \subseteq \mathrm{im} g$.

ΚΕΦΑΛΑΙΟ 3

Το ριζικό του Jacobson.

Το νόημα της θεωρίας προτύπων είναι καταλάβουμε την δομή των δακτυλίων μέσα από τις δράσεις τους σε αβελιανές ομάδες. Στην περίπτωση τον ημιαπλών προτύπων, ενδέχεται όμως να υπάρχουν στοιχεία που έχουν τετριμμένη δράση, δηλαδή $rM = 0$ για κάθε ημιαπλό πρότυπο M. Το σύνολο αυτό των παθογεννών στοιχειών $J(R)$ το ονομάζουμε ριζικό του Jacobson. Στο κεφάλαιο αυτό, θα δείξουμε ότι το ριζικό $J(R)$ είναι ένα αμφίπλευρο ιδεώδες και θα χαρακτηρίσουμε τα στοιχεία του.

3.1 Το ριζικό

Παρατήρηση. *Αν $I \subseteq R$ είναι ένα γνήσιο αριστερό (ή δεξί) ιδεώδες, τότε υπάρχει ένα αριστερό (ή δεξί) μεγιστικό ιδεώδες $m \subsetneq R$, με $I \subseteq m$. Πράγματι, έστω το σύνολο*

$$\mathcal{F} := \{J \subseteq R : J \text{ γνήσιο ιδεώδες και } I \subseteq J\}$$

με διάταξη τον εγκλεισμό συνόλων. Αν $\mathcal{F}' = \{J_1 \subseteq J_2 \subseteq \cdots \subseteq J_n \subseteq J_{n+1} \subseteq \dots\} \subseteq \mathcal{F}$ ένα πλήρως διατεταγμένο υποσύνολο, τότε η ένωση $J = \bigcup_{n\geq 1} J_n$ αποτελεί ιδεώδες με $J \in \mathcal{F}$ και $J_n \subseteq J$ για κάθε n, δηλαδή το J είναι άνω φράγμα. Συνεπώς, από το λήμμα του Zorn, υπάρχει μεγιστικό στοιχείο $m \in \mathcal{F}$. Το m είναι μεγιστικό ιδεώδες. Πράγματι, αν $m \subseteq K$ για κάποιο ιδεώδες $K \subseteq R$, τότε $K \supseteq m \supseteq I$ και άρα $K \in \mathcal{F}$. Αφού το m είναι μεγιστικό στοιχείο, έπεται $m = K$.

Πρόταση 3.1.1. *Οι επόμενες συνθήκες είναι ισοδύναμες για το $r \in R$*

(i) *$r \in m$ για κάθε μεγιστικό αριστερό ιδεώδες $m \subseteq R$*

(ii) *$1 - xr$ είναι αριστερά αντιστρέψιμο για κάθε $x \in R$*

(iii) *$rM = 0$ για κάθε απλό R-πρότυπο*

(iv) *$rM = 0$ για κάθε ημιαπλό R-πρότυπο*

Απόδειξη: $(i) \to (ii)$: Έστω ως προς άτοπο, ότι υπάρχει $x \in R$ ώστε το $1 - xr$ να μην είναι αντιστρέψιμο. Τότε το ιδεώδες $R(1 - xr)$ είναι γνήσιο και άρα υπάρχει μεγιστικό ιδεώδες m με $R(1 - xr) \subseteq m$. Από υπόθεση $r \in m$ και άρα $xr \in m$, οπότε $1 = (1 - xr) + xr \in m$ #

$(ii) \to (iii)$ Έστω, ως προς άτοπο, ότι υπάρχει απλό R-πρότυπο M με $rM \neq 0$, ισοδύναμα υπάρχει $a \in M$ με $ra \neq 0$. Το M είναι απλό, άρα ισχύει ότι $M = Rra$. Συνεπώς υπάρχει $x \in R$ με $a = xra$ ισοδύναμα $(1 - xr)a = 0$. Από υπόθεση το στοιχείο $1 - xr$ είναι αριστερά αντιστρέψιμο, έπεται ότι $a = 0$ #.

$(iii) \leftrightarrow (iv)$ ΄Αμεσο.

$(iii) \rightarrow (i)$ Έστω $m \subseteq R$ μεγιστικό ιδεώδες, τότε το R-πρότυπο R/m είναι απλό. Από υπόθεση $r(R/m) = 0 \iff r(1+m) = 0 \iff r \in m$. $\square$

Ορισμός 3.1.1. *Το ριζικό του δακτυλίου R είναι το σύνολο*

$$J(R) := \bigcap \{m : m \text{ μεγιστικό αριστερό ιδεώδες του } R\}$$

Πρόταση 3.1.2. *Το ριζικό $J(R)$ είναι αμφίπλευρο ιδεώδες του R.*

Απόδειξη: Από την Πρόταση 3.3.1,

$$\mathrm{rad}R = \bigcap_{M \text{ απλό}} ann_R M = \bigcap_{M \text{ ημιαπλό}} ann_R M$$

Οι μηδενιστές είναι πυρήνες, ειδικότερα αμφίπλευρα ιδεώδη. $\square$

Πρόταση 3.1.3. *Τα επόμενα είναι ισοδύναμα :*

(i) $r \in J(R)$

(ii) $1 - xry \in \mathbf{U}(R)$ *για κάθε* $x, y \in R$.

Απόδειξη : $(ii) \rightarrow (i)$: ΄Αμεσο για $y = 1$.

$(i) \rightarrow (ii)$ Έστω $x, y \in R$ και $r \in J(R)$ τότε $ry \in J(R)$ και άρα το στοιχείο $1 - xry$ είναι αριστερά αντιστρέψιμο. Ισοδύναμα, υπάρχει $s \in R$ με $s(1 - xry) = 1 \iff s = 1 + sxry$. Το στοιχείο $-sxr \in J(R)$, άρα το $s = 1 - (-sxr)y$ είναι αριστερά αντιστρέψιμο, δηλαδή υπάρχει $u \in R$ με $us = 1$. Ισχύει επίσης $su = 1$, πράγματι

$$1 - xry = 1 \cdot (1 - xry) = (us) \cdot (1 - xry) = u(s(1 - xry)) = u \cdot 1 = u$$

άρα $su = s(1 - xry) = 1$. $\square$

Πόρισμα 3.1.1. $J(R) = \bigcap \{m : m \subseteq R \text{ μεγιστικό δεξιό ιδεώδες}\}$

Ορισμός 3.1.2. *Ο R καλείται Jacobson ημιαπλός αν* $J(R) = 0$

Παρατηρήσεις. (i) *Αν* $I \subseteq R$ *είναι ένα ιδεώδες με* $I \subseteq J(R)$*, τότε* $J(R/I) = J(R)/I$*. Πράγματι, από το θεώρημα της αντιστοιχίας, τα αριστερά μεγιστικά ιδεώδη* $\overline{m} \subseteq R/I$ *είναι ακριβώς τα ιδεώδη* m/I *για ένα αριστερό μεγιστικό ιδεώδες* $m \supseteq I$*. Συνεπώς:*

$$\begin{aligned} J(R/I) &= \bigcap \{m/I \ : \ m \subseteq R \text{ μεγιστικό αριστερό ιδεώδες}\} \\ &= \left(\bigcap \{m : m \subseteq R \text{ μεγιστικό αριστερό ιδεώδες}\} \right) /I \\ &= J(R)/I \end{aligned}$$

(ii) *Παρατηρούμε ότι* $J(R/J(R)) = J(R)/J(R) = 0$*, άρα ο* $R/J(R)$ *είναι πάντα Jacobson ημιαπλός.*

(iii) Οι δακτύλιοι R και $R/J(R)$ έχουν ακριβώς τα ίδια απλά πρότυπα. Πράγματι, κάθε απλό $R/J(R)$-πρότυπο είναι R-πρότυπο, μέσω του ομομορφισμού πηλίκο $R \twoheadrightarrow R/J(R)$ το οποίο είναι προφανώς απλό. Αντίστροφα, έστω N ένα απλό R-πρότυπο. Ο ομομορφισμός δακτυλίων $R \longrightarrow \mathrm{End}(N,+)$ μηδενίζει στο $J(R)$ και άρα παραγοντοποιείται, μέσω τις απεικόνισης πηλίκο $R \twoheadrightarrow R/J(R)$.

$$\begin{tikzcd} R \arrow[d, "\pi"] \arrow[dr, "\ell"] & \\ R/J(R) \arrow[r, "\bar{\ell}"] & \mathbf{End}_{\mathbf{Z}}(M,+) \end{tikzcd}$$

(iv) Τα αντιστρέψιμα στοιχεία του πηλίκου $R/J(R)$ είναι ακριβώς αυτά που έχουν αντιστρέψιμο αντιπρόσωπο, δηλαδή $\mathbf{U}(R/J(R)) = \{r + J(R) : r \in \mathbf{U}(R)\}$. Πράγματι ο εκλεισμός $\supseteq$ είναι προφανής. Για τον άλλον, έστω $r \in R$ με $r + J(R) \in \mathbf{U}(R/J(R))$, τότε υπάρχει $s \in R$ με $(r+J(R))(s+J(R)) = (s + J(R))(r + J(R)) = 1 + J(R) \iff 1 - sr, 1 - rs \in J(R)$. Συνεπώς

$$1 - rs \in J(R) \Rightarrow 1 - 1 \cdot (1 - rs) \in \mathbf{U}(R) \Rightarrow rs \in \mathbf{U}(R) \Rightarrow r \text{ δεξία αντιστρέψιμο}$$

$$1 - sr \in J(R) \Rightarrow 1 - 1 \cdot (1 - sr) \in \mathbf{U}(R) \Rightarrow sr \in \mathbf{U}(R) \Rightarrow r \text{ αριστερά αντιστρέψιμο}$$

άρα $r \in \mathbf{U}(R)$.

Μηδενοδύναμα στοιχεία και το ριζικό.

Ορισμός 3.1.3. *Το $r \in R$ καλείται μηδενοδύναμο αν $r^n = 0$ για κάποιο $n > 0$. Το αριστερό ή δεξίο ή αμφίπλευρο ιδεώδες $I \subseteq R$ καλείται nil αν κάθε $r \in I$ είναι μηδενοδύναμο. Το αριστερό ή δεξίο ή αμφίπλευρο ιδεώδες $I \subseteq R$ καλείται μηδενοδύναμο αν $I^n = 0$ για κάποιο $n > 0$, όπου*

$$I^n = \left\{ \sum x_{i_1} \ldots x_{i_n} : x_{i_j} \in I \text{ για κάθε } j = 1, 2, \ldots, n \right\}$$

Παράδειγμα. *Έστω $\Bbbk$ σώμα, θεώρω τον δακτύλιο $R = \mathcal{T}_n(\Bbbk)$ των άνω τριγωνικών $n \times n$ πινάκων με εγγραφές από το $\Bbbk$. Το ιδεώδες*

$$I = \{A = (a_{ij}) : a_{ij} = 0 \text{ για κάθε } i \geq j\}$$

τών άνω τριγωνικών πινάκων με μηδενικά στην διαγώνιο είναι ένα μηδενοδύναμο αμφίπλευρο ιδεώδες του R.

Πρόταση 3.1.4. *Έστω $I \subseteq R$ ένα αριστερό (ή δεξίο ή αμφίπλευρο) ιδεώδες. Τότε :*

(i) Αν το I είναι μηδενοδύναμο, τότε είναι nil.

(ii) Αν I είναι nil, τότε $I \subseteq J(R)$

Απόδειξη : (i) Προφανές.

(ii) Έστω $r \in I$ και $x \in R$, τότε $xr \in I$ και αφού το I είναι nil, $(xr)^n = 0$ για κάποιο $n > 0$. Παρατηρώ ότι

$$(1 - xr)(1 + xr + \cdots + (xr)^{n-1}) = (1 + xr + \cdots + (xr)^{n-1})(1 - xr) = 1 - (xr)^n = 1$$

άρα το $1 - xr \in \mathbf{U}(R)$, ειδικότερα το $1 - xr$ είναι αριστερά αντιστρέψιμο. □

Πρόταση 3.1.5. *Έστω $I_1, \dots I_n \subseteq R$ αριστερά (δεξία ή αμφίπλευρα) ιδεώδη, τα οποία είναι μηδενοδύναμα, τότε το ιδεώδες $I = \sum_{k=1}^{n} I_k$ είναι μηδενοδύναμο.*

Απόδειξη : Αρκεί να δείξω ότι αν τα I_1, I_2 είναι μηδενοδύναμα ιδεώδη, τότε το $I_1 + I_2$ είναι μηδενοδύναμο ιδεώδες και μετά επαγωγικά παίρνω το ζητούμενο. Έστω $I_1^n = 0$ και $I_2^m = 0$, θα δείξω ότι $(I_1 + I_2)^{n+m-1} = 0$. Ισοδύναμα, για κάθε $x_1, \dots x_{n+m-1} \in I_1$ και $y_1, \dots, y_{n+m-1} \in I_2$ είναι $\prod_{i=1}^{n+m-1}(x_i + y_i) = 0$. Υπολογίζω :

$$\prod_{i=1}^{n+m-1}(x_i + y_i) = \sum_j a_{1,j}a_{2,j}\cdots a_{n+m-1,j}$$

όπου κάθε $a_{i,j} = x_i$ ή y_i. Συνεπώς αφού κάθε γινόμενο έχει $n+m-1$ παράγοντες, αν έχω λιγότερο απο m γινόμενα y_i, έχω τουλάχιστον n από x_i και αντίστροφα, άρα πράγματι το τελικό γινόμενο είναι μηδέν. $\square$

Παράδειγμα. *Υπάρχουν nil ιδεώδη τα οποία δεν είναι μηδενοδύναμα. Πράγματι, θεωρώ τον μεταθετικό δακτύλιο*

$$R = \frac{\mathbf{Z}[X_1, X_2, X_3, \dots]}{(X_1^2, X_2^3, X_3^4, \dots)}$$

και το ιδεώδες $I = (x_1, x_2, x_3, \dots)$, όπου $x_i \in R$ η κλάση του X_i στο πηλίκο. Το I είναι nil, αφού κάθε στοιχείο του γράφετε σαν άθροισμα μηδενοδύναμων στοιχείων. Δεν είναι όμως μηδενοδύναμο, αφού για κάθε φυσικό $N \gg 0$, υπάρχει στοιχείο $x_N \in I$ μηδενοδύναμης τάξης N. Στις επόμενες προτάσεις εξετάζουμε υπό ποιες προϋποθέσεις μπορεί να ισχύει και το αντίστροφο.

Πρόταση 3.1.6. *Αν ο R είναι μεταθετικός δακτύλιος της Noether, τότε κάθε nil ιδεώδες $I \subseteq R$ είναι μηδενοδύναμο.*

Απόδειξη : Έστω $I \subseteq R$ ένα nil ιδεώδες, τότε αφού ο R είναι της Noether, το I είναι πεπερασμένα παραγόμενο, δηλαδή υπάρχουν $a_i \in I$ για $i = 1, 2, \dots, n$, ώστε $I = \sum_{i=1}^{n} Ra_i$. Αφού τα $a_i \in I$ για $i = 1, 2, \dots, n$ είναι μηδενοδύναμα και ο R είναι μεταθετικός, τα ιδεώδη Ra_i είναι μηδενοδύναμα. Συνεπώς από την Πρόταση 3.2.2. το $I = \sum_{i=1}^{n} Ra_i$ είναι μηδενοδύναμο. $\square$

Πρόταση 3.1.7. *Αν ο R είναι αριστερά του Artin, τότε το $J(R) \subseteq R$ είναι μηδενοδύναμο.*

Απόδειξη : Έστω $I = J(R) \subseteq R$ και θεωρούμε την φθίνουσα ακολουθία :

$$I \supseteq I^2 \supseteq I^3 \supseteq \dots$$

Ο R είναι του Artin, συνεπώς από την συνθήκη φθίνουσας άλυσης, υπάρχει $n \in \mathbf{N}$, ώστε $I^n = I^{n+1}$. Θα δείξω ότι $I^n = 0$. Έστω ως προς άτοπο, ότι $I^n \neq 0$, τότε θεωρούμε την συλλογή

$$\mathscr{X} := \{J \subseteq R \ : \ J \text{ αριστερό ιδεώδες με } I^n J \neq 0\}$$

Από υπόθεση το $\mathscr{X} \neq \emptyset$ ($R \in \mathscr{X}$). Καθώς ο R είναι του Artin η συλλογή $\mathscr{X}$ έχει ελαχιστικό στοιχείο J_0. Αφού $J_0 \in \mathscr{X}$, ισχύει ότι $I^n J_0 \neq 0$ και άρα υπάρχει $r \in J_0$ με $I^n r \neq 0$. Παρατηρώ ότι $I^n r \subseteq J_0$ και $I^n(I^n r) = I^{2n} r = I^n r \neq 0$, συνεπώς $I^n r \in \mathscr{X}$. Από την ελαχιστικότητα του J_0, έχουμε $J_0 = I^n r$. Έχουμε $r \in J_0 = I^n r$, επομένως υπάρχει $x \in I^n$ με $r = xr \iff (1-x)r = 0$. Αφού $x \in I^n \subseteq I = J(R)$, το στοιχείο $1 - x \in R$ είναι αντιστρέψιμο και άρα $r = 0$, δηλαδή $I^n r = 0$ # $\square$

Πόρισμα 3.1.2. *Αν ο R είναι αριστερά του Artin, τότε κάθε nil αριστερό ιδεώδες είναι μηδενοδύναμο.*

Απόδειξη : Έστω R ένας δακτύλιος του Artin και $I \subseteq R$ ένα nil ιδεώδες. Αφού το I είναι nil, ισχύει ότι $I \subseteq J(R)$ και καθώς ο R είναι του Artin υπάρχει $n \in \mathbf{N}$ με $(J(R))^n = 0$. Συνεπως $I \subseteq J(R) \Rightarrow I^n \subseteq (J(R))^n = 0$, άρα $I^n = 0$. $\square$

Παρατήρηση. *Αν ο R είναι αριστερά του Artin, τότε το ριζικό του Jacobson είναι το μέγιστο μηδενοδύναμο ιδεώδες.*

Πρόταση 3.1.8. *Τα επόμενα είναι ισοδύναμα για έναν δακτύλιο R.*

(i) *Ο R είναι ημιαπλός.*

(ii) *Ο R είναι αριστερά του Artin και Jacobson ημιαπλός.*

Απόδειξη : $(i) \to (ii)$: Έστω R ημιαπλός και $r \in J(R)$. Το R-πρότυπο R είναι ημιαπλό, συνεπώς $r \cdot R = 0$ και άρα $r = r \cdot 1_R = 0$. Για την συνθήκη φθίνουσας άλυσης, γνωρίζουμε ότι $R = \sum_{k=1}^{n} I_k$. Τα I_k είναι απλά R-πρότυπα, συνεπώς του Artin και το άθροισμα R-προτύπων του Artin είναι του Artin.

$(ii) \to (i)$: Θα δείξω ότι ο R είναι το ευθύ άθροισμα ελαχιστικών ιδεωδών. Αφού ο R είναι του Artin, υπάρχει ελαχιστικό ιδεώδες $I_1 \subseteq R$. Καθώς $I_1 \nsubseteq 0 = J(R)$, υπάρχει αριστερό μεγιστικό ιδεώδες m_1 ώστε $I_1 \nsubseteq m_1$ και άρα $I_1 \cap m_1 \subsetneq I_1$. Από την ελαστικότητα του I_1, έχουμε $I_1 \cap m_1 = 0$ και αφού $m_1 \subseteq m_1 \oplus I_1$ συνεπάγετε ότι $m_1 \oplus I_1 = R$. Αν $m_1 = 0$ τελείωσαμε. Αν όχι επιλέγω ελαχιστικό ιδεώδες $I_2 \subseteq m_1$. Όπως πριν υπάρχει υπάρχει μεγιστικό αριστερό ιδεώδες $m_2' \subseteq R$ ώστε $m_2' \oplus I_2 = R$. Ισχύει ότι $m_1 = I_2 \oplus (m_2' \cap m_1)$. Θέτω $m_2 = m_2' \cap m_1$ και έχω $R = I_1 \oplus I_2 \oplus m_2$. Αν $m_2 = 0$ τελείωσα. Αν όχι, βρίσκω ελαχιστικό $I_3 \subseteq m_2$ και έχω μεγιστικό αριστερό ιδεώδες $m_3' \subseteq R$ με $I_3 \nsubseteq m_3'$. Όμοια με πριν, έχω $m_2 = I_3 \oplus (m_3' \cap m_2)$ και θέτοντας $m_3 := m_3' \cap m_2$ έχω $R = I_1 \oplus I_2 \oplus I_3 \oplus m_3$. Παρατηρώ ότι η διαδικασία αυτή παράγει μια γνησίωες φθίνουσα ακολουθία ιδεώδων

$$m_1 \supsetneq m_2 \supsetneq m_3 \supsetneq \dots$$

και αφού ο R είναι του Artin, τερματίζει σε πεπερασμένα βήματα.

Μια δεύτερη απόδειξη για το $(ii) \to (i)$: Θα χρησιμοποιοήσουμε το εξής λήμμα :

Λήμμα 3.1.1. *Αν R ένας δακτύλιος του Artin, τότε υπάρχουν αριστερά μεγιστικά ιδεώδη $m_1, \dots, m_n$, τέτοια ώστε $J(R) = \bigcap_{i=1}^{n} m_i$*

Απόδειξη λήμματος : Θεωρούμε την οικόγενεια των :

$$\mathcal{X} := \left\{ \bigcap_{i=1}^{n} m_i : m_1, \dots, m_n \text{ αριστερά μεγιστικά ιδεώδη} \right\}$$

Αν $\mathcal{X} = \varnothing$, δεν έχουμε να δείξουμε τίποτα. Αν $\mathcal{X} \neq \varnothing$, τότε από την συνθήκη του Artin, υπάρχει ελαχιστικό στοιχείο $J \in \mathcal{X}$. Ισχύει ότι $J = J(R)$. Πράγματι, προφανώς $J(R) \subseteq J$ και παρατηρούμε ότι για κάθε αριστερό μεγιστικό ιδεώδες m είναι $m \cap J \subseteq J$ και $m \cap J \in \mathcal{X}$, συνεπώς από τον ελαχιστικό χαρακτήρα του J, είναι $J \cap m = J$, ισοδύναμα $J \subseteq m$ για κάθε αριστερό μεγιστικό ιδεώδες m. Έπεται άμεσα ότι $J = J(R)$. Τέλος, αφού $J(R) = J \in \mathcal{X}$, παίρνουμε το ζητούμενο. □

Έστω R ένας δακτύλιος του Artin, τέτοιος ώστε $J(R) = 0$. Θα δείξω ότι το R-πρότυπο R είναι ημιαπλό και για αυτό αρκεί να δείξω ότι είναι υποπρότυπο ημιαπλού προτύπου. Από το λήμμα, υπάρχουν αριστερά μεγιστικά ιδεώδη $m_1, \dots, m_n$, τέτοια ώστε $\bigcap_{i=1}^{n} m_i = J(R) = 0$. Καθώς τα αριστερά ιδεώδη m_i είναι μεγιστικά, τα αριστερά R-πρότυπα R/m_i είναι απλά για κάθε $i = 1, 2, \dots, n$. Η φυσική R-γραμμική απεικόνιση

$$R \longrightarrow \bigoplus_{i=1}^{n} R/m_i$$

έχει πυρήνα $\bigcap_{i=1}^{n} m_i = 0$ και παίρνω το ζητούμενο. □

Πόρισμα 3.1.3. *Αν R αριστερά του Artin, τότε ο $R/J(R)$ είναι ημιαπλός.*

Απόδειξη : Αφού $J(R/J(R)) = 0$, έπεται άμεσα από την προηγούμενο πρόταση. □

Παρατηρήσεις. *(i) Έστω S ένας δακτύλιος και M ένα ημιαπλό S-πρότυπο, τότε το M είναι της Noether αν και μόνο αν είναι του Artin. Πράγματι, γράφω το $M = \bigoplus_{i\in I} M_i$ για κάποια απλά S-πρότυπα M_i. Αν το M είναι του Artin, τότε $\#I < \infty$, καθώς διαφορετικά, θα μπορούσα να κατασκευάσω γνήσιως φθίνουσα ακολουθία υποπροτύπων :*

$$M \supsetneq \bigoplus_{i\neq i_0} M_i \supsetneq \bigoplus_{i\neq i_0, i_1} M_i \supsetneq \dots$$

για κάποια διακεκριμένα $i_0, i_1, \dots \in I$. Συνεπώς το M είναι το ευθύ άθροισμα απλών S-πρότυπων και άρα είναι της Noether. Αντίστροφα, αν M είναι της Noether, ισχύει επίσης ότι $\#I < \infty$, καθώς διαφορετικά μπορώ να κατασκευάσω μια γνησίως αύξουσα ακολουθία υποπροτύπων :

$$0 \subsetneq M_{i_0} \subsetneq M_{i_0} \oplus M_{i_1} \subsetneq \dots$$

για κάποια διακεκριμένα $i_0, i_1, \dots \in I$. Συνεπώς το M είναι το ευθύ άθροισμα απλών S-πρότυπων και άρα είναι του Artin. Ειδικότερα, αν S ένας ημιαπλός δακτύλιος και M ένα R-πρότυπο, τότε το M είναι του Artin αν και μόνο αν είναι της Noether.

(ii) Έστω S ένας δακτύλιος, $J \subseteq S$ ιδεώδες και M ένα S/J-πρότυπο. Μπορώ να θεωρήσω το M σαν S-πρότυπο, ώστε $J \cdot M = 0$. Τότε μια υποομάδα N της $(M, +)$ είναι S-υποπρότυπο αν και μόνο αν η N είναι ένα S/J-υποπρότυπο. Συνεπώς, το S-πρότυπο M είναι της Noether (του Artin) αν και μόνο το S/J-πρότυπο είναι είναι της Noether (του Artin).

(iii) Έστω R ένας δακτύλιος και M ένα R-πρότυπο, εφοδιασμένο με μια φθίνουσα ακολουθία υποπροτύπων

$$M = M_0 \supseteq M_1 \supseteq \dots \supseteq M_n \supseteq M_{n+1} = 0$$

Τότε το M είναι του Artin (της Noether) αν και μόνο αν M_i/M_{i+1} είναι του Artin (της Noether) για κάθε $i = 0, 1, \dots, n$. Πράγματι, αν το M είναι του Artin (της Noether), τότε τα M_i είναι του Artin (της Noether) και άρα και τα M_i/M_{i+1} είναι του Artin (της Noether). Αντίστροφα, αν $M_0/M_1, M_1/M_2, \dots, M_n/M_{n+1}$ είναι του Artin (της Noether), ειδικότερα το $M_n/M_{n+1} = M_n$, M_{n-1}/M_n είναι του Artin (της Noether), συνεπώς το M_{n-1} είναι του Artin (της Noether). Το M_{n-1} και το M_{n-2}/M_{n-1} είναι του Artin (της Noether), συνεπώς το M_{n-2} είναι του Artin (της Noether). Επαγωγικά βρίσκω ότι το $M_0 = M$ είναι του Artin (της Noether).

Πρόταση 3.1.9 (Θεώρημα του Hopkin)**.** *Τα επόμενα είναι ισοδύναμα για έναν δακτύλιο R :*

(i) Ο R είναι αριστερά του Artin.

(ii) Ο R είναι αριστερά της Noether, το ριζικό $J(R)$ είναι μηδενοδύναμο και ο $R/J(R)$ είναι ημιαπλός.

Συγκεκριμένα αν ο R είναι του Artin τότε είναι και της Noether.

Απόδειξη. Αρκεί να δειχθεί το εξής : Αν το ριζικό $J(R)$ είναι μηδενοδύναμο και ο $R/J(R)$ είναι ημιαπλός, τότε ο R είναι της Noether αν και μόνο αν Ο R είναι του Artin. Θέτω $I = J(R)$, με $I^{n+1} = 0$. Ισχύει ότι ο $\overline{R} = R/I$ είναι ημιαπλός. Θεωρώ το αριστερό R-πρότυπο R και την ακολουθία ιδεωδών

$$R =: I^0 \supseteq I \supseteq I^2 \supseteq \dots \supseteq I^n \supseteq I^{n+1} = 0$$

Γνωρίζω ότι ο R είναι της Noether αν και μόνο αν τα R-πρότυπα I^k/I^{k+1} για $k = 0, 1, \dots, n$ είναι της Noether αν και μόνο αν τα R/I-πρότυπα I^k/I^{k+1} για $k = 0, 1, \dots, n$ είναι της Noether αν και μόνο αν τα R-πρότυπα I^k/I^{k+1} για $k = 0, 1, \dots, n$ είναι του Artin αν και μόνο αν ο R είναι του Artin. □

Λήμμα 3.1.2 (Υπολογίζοντας το ριζικό). *Αν S δακτύλιος, $I \subseteq S$ ιδεώδες και $J(S/I) = 0$, τότε $J(S) \subseteq I$. Δηλαδή το ριζικό $J(S)$ είναι το μικρότερο ιδεώδες I για το οποίο $J(S/I) = 0$.*

Απόδειξη. Αφού $J(S/I) = 0$, έχουμε ότι $\bigcap\{m : m \subseteq S$ μεγιστικό αριστερό ιδεώδες με $I \subseteq m\}/I = 0$ και άρα $I = \bigcap\{m : m \subseteq S$ μεγιστικό αριστερό ιδεώδες με $I \subseteq m\} \supseteq J(S)$. □

Παράδειγμα. (i) *Ο δακτύλιος $R = \begin{pmatrix} \mathbf{R} & \mathbf{R}[x] \\ 0 & \mathbf{R} \end{pmatrix} \subseteq \mathbf{M}_2(\mathbf{R}[x])$ έχει μηδενοδύναμο ριζικό, ο $R/J(R)$ είναι ημιαπλός, αλλά δεν είναι ουτε αριστερά ούτε δεξία της Noether (του Artin). Πράγματι, θεωρώ το ιδεώδες $I = \begin{pmatrix} 0 & \mathbf{R}[x] \\ 0 & 0 \end{pmatrix} \subseteq R$ και παρατηρώ ότι $I^2 = 0 \Rightarrow I \subseteq J(R)$. Από την άλλη ο $R/I \simeq \mathbf{R} \times \mathbf{R}$ είναι ημιαπλός και άρα και Jacobson ημιαπλός. Από το προηγούμενο λήμμα $J(R) \subseteq I$ και άρα $J(R) = I$. Τέλος παρατηρώ ότι για κάθε διανυσματικό υπόχωρο $U \subseteq \mathbf{R}[x]$ το $\begin{pmatrix} 0 & U \\ 0 & 0 \end{pmatrix}$ είναι αμφίπλευρο ιδεώδες του R. Συνεπώς, αφού $\dim_{\mathbf{R}} \mathbf{R}[x] = \infty$, ο R δεν είναι ούτε αριστερά ούτε δεξία της Noether (του Artin).*

Ένας άλλος χαρακτηρισμός του ριζικού

Ορισμός 3.1.4. *Έστω R ένας δακτύλιος και $r \in R$. Θα λέμε ότι το στοιχείο r δεν παράγει τον δακτύλιο R, αν για κάθε υποσύνολο $S \subseteq R$ τέτοιο ώστε το $S \cup \{r\}$ να παράγει τον R, να ισχύει ότι το S παράγει τον R.*

Πρόταση 3.1.10. *Έστω R ένας δακτύλιος. Τότε $J(R) = \{x \in R :$ το x δεν παράγει τον $R\}$.*

Απόδειξη : $\subseteq$: Αν $x \in J(R)$ και S ένα υποσύνολο του R, τέτοιο ώστε το $S \cup \{x\}$ να παράγει το R, τότε υπάρχουν $r_0, r_1, \ldots, r_n \in R$ και $s_1, \ldots, s_n \in S$, ώστε

$$r_0 x + r_1 s_1 + \cdots + r_n s_n = 1$$

Αν $r_0 = 0 \in R$, τότε το S παραγεί τον R. Αν $r_0 \neq 0$, τότε το στοιχείο $1 - r_0 x$ είναι αντιστρέψιμο και άρα

$$(1 - r_0 x)^{-1} r_1 s_1 + \cdots + (1 - r_0 x)^{-1} r_n s_n = 1$$

οπότε και πάλι το S παράγει τον R.

$\supseteq$: Έστω $x \in R$ ένα στοιχείο που δεν παράγει τον R και έστω ως προς άτοπο ότι $x \notin J(R)$. Τότε, υπάρχει ένα μεγιστικό αριστερό ιδεώδες $m \subseteq R$, τέτοιο ώστε $x \notin m$. Ισχύει, ότι $m \subseteq \langle m \cup \{x\} \rangle$, συνεπώς από τον μεγιστικό χαρακτήρα του m το σύνολο $m \cup \{x\}$ παράγει τον δακτύλιος R, έπεται ότι το σύνολο m παράγει τον R, δηλαδή $m = R$ #. □

Λήμμα του Nakayama

Ορισμός 3.1.5. *Έστω M ένα αριστερό R-πρότυπο και $I \subseteq R$ ένα αριστερό ιδεώδες. Το σύνολο*

$$IM := \left\{ \sum_{i=1}^{n} r_i x_i : n \in \mathbf{N},\ r_i \in I, x_i \in I \right\}$$

αποτελεί R-υποπρότυπο του M

Πρόταση 3.1.11 (Λήμμα του Nakayama). *Έστω M ένα πεπερασμένα παραγόμενο R-πρότυπο και $I \subseteq J(R)$ ιδεώδες.*

(i) *Αν $I \cdot M = M$, τότε $M = 0$.*

(ii) *Αν N ένα υποπρότυπο του M, με $M = N + I \cdot M$, τότε $M = N$*

Απόδειξη : (i) Έστω, ως προς άτοπο, ότι $M \neq 0$, τότε επιλέγω τον ελάχιστο φυσικό n, τέτοιο ώστε να υπάρχει σύνολο $\{e_1, \ldots, e_n\}$ που παράγει το υποπρότυπο M. Αφού $e_1 \in M = I \cdot M$, υπάρχουν $a_1, \ldots, a_n \in J(R)$, τέτοια ώστε

$$e_1 = a_1 e_1 + \cdots + a_n e_n \iff$$

$$(1 - a_1)e_1 = a_2 e_2 + \cdots + a_n e_n$$

Αφού $a_1 \in I \subseteq J(R)$, το στοιχείο $1 - a_1$ είναι αντιστρέψιμο και άρα το σύνολο $\{e_2, \ldots, e_n\}$ παράγει το R-πρότυπο M. Άτοπο, από τον ελαχιστικό χαρακτήρα του n.

(ii) Η φυσική R-γραμμική απεικόνιση $I \cdot M \longrightarrow I \cdot M/N$ έχει πυρήνα τον $N \cap IM$, άρα

$$I\frac{M}{N} \simeq \frac{IM}{N \cap IM} \simeq \frac{N + IM}{N} = \frac{M}{N}$$

από το (i), παίρνω $M/N = 0$, ισοδύναμα $M = N$. □

Παρατηρήσεις. (i) *Αν το ριζικό $J(R)$ είναι μηδενοδύναμο, τότε το πόρισμα του λήμματος Nakayama ισχύει τετριμμένα. Πράγματι, αν υπάρχει $n \gg 0$, τέτοιο ώστε $I^n \subseteq J(R)^n = 0$, τότε $M = IM = I^2 M = \cdots = I^n M = 0$. Ειδικότερα, αν ένας δακτύλιος R είναι του Artin, τότε ισχύει το πόρισμα του λήμματος του Nakayama.*

(ii) *Η υπόθεση το πρότυπο M να είναι πεπερασμένα παραγόμενο στο Λήμμα του Nakayama είναι απαραίτητη. Πράγματι, είναι εύκολο να δειχθεί ότι ο δακτύλιος $R = \{a/b \in \mathbf{Q} : b \text{ περιττός}\}$ είναι ένας τοπικός δακτύλιος με μοναδικό μεγιστικό ιδεώδες το $m = (2)$. Θεωρούμε το R-πρότυπο $\mathbf{Q}$ και έχουμε ότι $J(R) \cdot \mathbf{Q} = m \cdot \mathbf{Q} = \mathbf{Q}$*

Ορισμός 3.1.6. *Έστω $I \subseteq R$ ένα ιδεώδες, M ένα R-πρότυπο και $IM \subseteq M$ το αντίστοιχο υποπρότυπο. Αν $f : M \to M'$ μια R-γραμμική απεικόνιση, τότε είναι $f(IM) \subseteq f(IM')$ και άρα επάγεται μια απεικόνιση*

$$M/IM \longrightarrow M'/IM'$$

$$m + IM \longmapsto f(m) + IM'$$

Σταθεροποιούμε $I = J(R)$ και εφαρμόζουμε τα παραπάνω. Συμβολίζουμε με $\overline{M}$ το $R/J(R)$-πρότυπο $M/J(R)M$ και αν $f : M \to M'$ μια R-γραμμική απεικόνιση με $\overline{f} : \overline{M} \to \overline{M'}$ την επαγόμενη $R/J(R)$-γραμμική απεικόνιση.

Πρόταση 3.1.12 (Λήμμα Nakayama). *Έστω M ένα R-πρότυπο. Τότε $M = 0$ αν και μόνο αν $\overline{M} = 0$.*

Πρόταση 3.1.13. *Έστω M' ένα πεπερασμένα παραγόμενο R-πρότυπο και $f : M \to M'$ μια R-γραμμική απεικόνιση. Η $f : M \to M'$ είναι επί αν και μόνο αν η $\overline{f} : \overline{M} \to \overline{M'}$ είναι επί.*

Απόδειξη : Το ευθύ είναι άμεσο. Για το αντίστροφο, έστω ένα $m' \in M'$, τότε αφού η $\overline{f} : \overline{M} \to \overline{M'}$ είναι επί, υπάρχει ένα $m \in M$, τέτοιο ώστε $f(m) + J(R)M' = m' + J(R)M'$, ισοδύναμα $m' - f(m) \in J(R)M$. Συνεπώς, $m' = f(m) + m' - f(m) \in \mathrm{im} f + J(R)M'$, δηλαδή $M' = \mathrm{im} f + J(R)M'$ και αφού το M' είναι πεπερασμένα παραγόμενο, από το λήμμα του Nakayama, παίρνω $\mathrm{im} f = M'$. □

Πόρισμα 3.1.4. *Έστω M ένα πεπερασμένα παραγόμενο R-πρότυπο και $\{x_i\}_{i \in I}$ μια συλλογή στοιχείων του. Τότε τα στοιχεία $\{x_i\}_{i \in I} \subseteq M$ παράγουν το R-πρότυπο M, αν και μόνο αν τα αντίστοιχα στοιχεία στο πηλίκο $\{\overline{x_i}\} \subseteq \overline{M}$ παράγουν το $R/J(R)$-πρότυτο $\overline{M}$.*

Απόδειξη. Έστω $M' := \langle x_i : i \in I \rangle$ και θεωρώ την ένθεση $M' \longrightarrow M$. Το M παράγεται από την σύνολο $\{x_i\}_{i \in I}$ αν και μόνο αν η ένθεση $M' \longrightarrow M$ επί αν και μόνο αν η επαγόμενη απεικόνιση $\overline{M'} \longrightarrow \overline{M}$ είναι επί αν και μόνο αν το M' παράγεται από την σύνολο $\{\overline{x_i}\}_{i \in I}$ □

3.2 Von Neumann Κανονικότητα

Έχουμε δείξει ότι η συνθήκη αύξουσας άλυσης (Noether) είναι πιο πλούσια από την συνθήκη φθίνουσας άλυσης (Artin) στους δακτυλίους, η έννοια του ημιαπλού δακτυλίου επάγει και τις δύο συνθήκες άλυσης και η συνθήκη φθίνουσας άλυσης μαζί με την Jacobson ημιαπλότητα είναι ισοδύναμες με το ο δακτύλιος να είναι ημιαπλός. Θέλουμε τώρα να ορίσουμε μια νέα εννοία που μαζί με την συνθήκη της Noether να είναι ισοδύναμη με την ημιαπλότητα. Η έννοια αυτή είναι οι Von Neumann κανονικοί δακτύλιοι. Ο John Von Neumann τους όρισε για πρώτη φορά το 1936 στην θεωρία της κβαντικής μηχανικής.

$$
\begin{tikzcd}
\textit{Noether} \arrow[d, hook] & & \textit{Artin} \arrow[ll] \arrow[d, hook] \\
\begin{matrix}\textit{Noether}\\ +\\ \textit{Von Neumann}\\ \textit{Κανονικότητα}\end{matrix} \arrow[r, leftrightarrow] & \begin{matrix}\textit{Ημιαπλός}\\ \textit{Δακτύλιος}\end{matrix} \arrow[ul] \arrow[ur] \arrow[dl] \arrow[dr] \arrow[r, leftrightarrow] & \begin{matrix}\textit{Artin}\\ +\\ \textit{Jacobson}\\ \textit{Ημιαπλός}\end{matrix} \\
\begin{matrix}\textit{Von Neumann}\\ \textit{Κανονικότητα}\end{matrix} \arrow[u, hook] \arrow[rr] & & \begin{matrix}\textit{Jacobson}\\ \textit{Ημιαπλός}\end{matrix} \arrow[u, hook]
\end{tikzcd}
$$

Πρόταση 3.2.1. *Οι επόμενες συνθήκες είναι ισοδύναμες για έναν δακτύλιο R :*

(i) *Για κάθε $\alpha \in R$, υπάρχει $\beta \in R$, ώστε $\alpha = \alpha\beta\alpha$.*

(ii) *Για κάθε $\alpha \in R$, υπάρχει $e^2 = e \in R$, ώστε $R\alpha = Re$*

(iii) *Για κάθε πεπερασμένα παραγόμενο ιδεώδες $I \subseteq R$, υπάρχει $e^2 = e \in R$, ώστε $I = Re$.*

Στην περίπτωση αυτή ο R καλείται Von-Neumann κανονικός.

Απόδειξη : $(i) \to (ii)$: Θεωρώ $\alpha \in R$ και $\beta \in R$, ώστε $\alpha = \alpha\beta\alpha$. Τότε παρατηρώ ότι $\beta\alpha = \beta\alpha\beta\alpha = (\beta\alpha)^2$. Θέτω $e = \beta\alpha$ και άρα $Re \subseteq R\alpha$. Όμοια $\alpha = \alpha e$, οπότε $R\alpha \subseteq Re$. Τελικά $R\alpha = Re$ και $e^2 = e$.

$(ii) \to (i)$ Θεωρώ $\alpha \in R$ και επιλέγω $e^2 = e \in R$, με $R\alpha = Re$. Υπάρχουν $x, y \in R$ με $\alpha = xe$ και $e = y\alpha$, οπότε $\alpha = xe = xee = xey\alpha = \alpha y\alpha$

$(ii) \to (iii)$: Αρκεί να δείξω ότι το ιδεώδες $Re + Rf$ για ταυτοδύναμα στοιχεία $e, f \in R$ γράφεται σαν Rs για κάποιο ταυτοδύναμο στοιχείο $s \in R$ και επαγωγικά θα πάρω το ζητούμενο. Στόχος μου είναι να βρω ένα νέο ταυτοδύναμο στοιχείο $e' \in R$, τέτοιο ώστε $Re + Rf = Re' + Rf$ και επιπλεόν $e'f = 0$. Αν το καταφέρω αυτό , τότε θα είναι $Re + Rf = Re' + Rf = Rs$, όπου $s = e' + f - fe'$ και το στοιχείο s είναι ταυτοδύναμο.

• Για την ύπαρξη του στοιχείου e' : Αρχικά, ισχύει η ισότητα $Re(1-f) + Rf = Re + Rf$, πράγματι αφού

$$e(1-f) = e + (-e)f \in Re + Rf \text{ και } f \in Re + Rf \Rightarrow Re(1-f) + Rf \subseteq Re + Rf$$

$$e = e(1-f) + ef \in Re(1-f) + Rf \text{ και } f \in Re(1-f) + Rf \Rightarrow Re + Rf \subseteq Re(1-f) + Rf$$

Από την υπόθεση, υπάρχει ταυτοδύναμο στοιχείο $e' \in R$, τέτοιο ώστε $Re' = Re(1-f)$. Είναι $Re + Rf = Re(1-f) + Rf = Re' + Rf$ και τέλος υπάρχει $x \in R$ ώστε $e' = xe(1-f)$, άρα $e'f = xe(1-f)f = xe(f-f^2) = 0$.

• Για την ισότητα $Re' + Rf = Rs$ και την ταυτοδυναμία του s : Το στοιχείο s είναι πράγματι ταυτοδύναμο, αφού

$$s^2 = (e'+f-fe')^2 = e'^2 + e'f - e'fe' + fe' + f^2 - f^2e' - fe'^2 - fe'f + fe'fe' = e' + f - fe' = s$$

Για την ισότητα των ιδεωδών, ο ένας εγκλεισμός είναι προφανής, για τον άλλον παρατηρώ ότι $e' = e's \in Rs$ και $f = fs \in Rs$.

$(iii) \to (ii)$: Προφανές. $\square$

Πρόταση 3.2.2. *Έστω R Von Neumann κανονικός δακτύλιος, τότε ο R είναι Jacobson ημιαπλός.*

Απόδειξη : Έστω $x \in J(R)$, τότε υπάρχει $y \in R$ με $x = xyx \iff x(1-yx) = 0$. Όμως το $1 - yx$ είναι αντιστρέψιμο και άρα $x = 0$. $\square$

Πρόταση 3.2.3. *Τα επόμενα είναι ισοδύναμα για έναν δακτύλιο R*

(i) *ο R είναι ημιαπλός.*

(ii) *ο R είναι αριστερά της Noether και Von Neumann κανονικός.*

Απόδειξη : $(i) \to (ii)$ Έστω $I \subseteq R$ ένα πεπερασμένα παραγόμενο ιδεώδες θα δείξω ότι υπάρχει $e^2 = e \in R$ με $I = Re$. Αφού R ημιαπλός, υπάρχει $J \subseteq R$ ιδεώδες ώστε $R = I \oplus J$. Τότε υπάρχουν $e \in I, f \in J$ ώστε $1 = e + f$. Παρατηρώ ότι $e - e^2 = e(1-e) = ef \in I \cap J = 0$ συνεπώς $e = e^2$. Ακόμα αν $r \in I$, τότε $r = r \cdot 1 = re + rf$ και άρα $r - re = rf \in I \cap J = 0$ συνεπώς $r = re$ και τελικά $I = Re$. Τέλος, όπως και έχει δειχθεί, η ημιαπλότητα συνεπάγει τις συνθήκες άλυσης.

$(ii) \to (i)$ Έστω $I \subseteq R$ ιδεώδες, θα δείξω ότι έχει συμπλήρωμα. Αφού ο R είναι της Noether, το I είναι πεπερασμένα παραγόμενο και καθώς είναι και Von Neumann κανονικός, υπάρχει στοιχείο $e^2 = e \in R$, ώστε $I = Re$. Είναι $I = Re \oplus R(1-e)$, πράγματι προφανώς $Re + R(1-e) = R$ και αν $x \in Re \cap R(1-e)$, τότε υπάρχουν $\alpha, \beta \in R$ με $x = \alpha e = \beta(1-e)$, όμως $x = \alpha e = \alpha ee = \beta(1-e)e = 0$, συνεπώς $Re \cap R(1-e) = 0$ $\square$

Παρατηρήσεις. *Η Πρόταση 3.3.2. ήταν αναμενόμενη. Από την Πρόταση 3.3.3. παίρνω το διάγραμμα*

$$\begin{array}{c} \textit{Artin} \\ + \\ \textit{Jacobson Ημιαπλός} \end{array} \longleftrightarrow \begin{array}{c} \textit{Noether} \\ + \\ \textit{Von Neummann} \\ \textit{Κανονικός} \end{array}$$

και αφού η συνθήκη της Noether είναι πιο "πλούσια" από την συνθήκη του Artin, για να "υπάρχει ισορροποία στο παραπάνω διάγραμμα" οφείλει η Jacobson ημιαπλότητα να περιέχει περισσότερη δομή από την Von Neummann κανονικότητα .[1]

[1] Ένας τρόπος να καταλάβουμε πόσο πιο πλούσια είναι η έννοια της Noether από του Artin : Στην θεωρία της Αλγεβρικής Γεωμετρίας, μελετάμε επιφάνειες που τα στοιχεία τους είναι λύσεις πολυωνυμικών συστημάτων και υπάρχει μια αντιστοιχία μεταξύ επιφανειών και αλγεβρικών αντικειμένων. Στο πλαίσιο αυτό κάθε επιφάνεια είναι της Noether (μέσω αυτής της αντιστοιχίας), ενώ του Artin είναι μόνο τα σύνολα με πεπερασμένο το πλήθος σημεία.

Παραδείγματα. (i) *Ο δακτύλιος $\mathcal{C}[0,1]$ των συνεχών συναρτήσεων στο $[0,1]$ είναι Jacobson ημιαπλός, αλλά όχι Von Neumann κανονικός. Πράγματι, σταθεροποιώ ένα $a \in [0,1]$ και θεωρώ τον ομομορφισμό εκτίμισης $ev_a : \mathcal{C}[0,1] \to \mathbf{C}$ με $ev_a(f) = f(a) \in \mathbf{C}$. Ο ev_a είναι επί, συνεπώς $\mathcal{C}[0,1]/m_a \simeq \mathbf{C}$, όπου $m_a := \ker ev_a$ ο πυρήνας. Το ιδεώδες m_a είναι μεγιστικό για κάθε $a \in \mathbf{C}$ και άρα $J(\mathcal{C}[0,1]) \subseteq \bigcap_a m_a = 0$, δηλαδή ο $\mathcal{C}[0,1]$ είναι Jacobson ημιαπλός. Για την Von Neumann κανονικότητα, θεωρώ την $f \in \mathcal{C}[0,1]$, όπου $f(t) = t$ για κάθε $t \in [0,1]$ και έστω, ως προς άτοπο ότι υπάρχει $g \in \mathcal{C}[0,1]$ με $f = fgf$. Συνεπώς για κάθε $t > 0$ είναι $g(t) = 1/t$, δηλαδή υπάρχει συνεχής επέκταση της $g(t) = 1/t$ στο $[0,1]$ $\#$.*

(ii) *Έστω M ένα αριστερά ημιαπλό R-πρότυπο και $S = \mathrm{End}_R M$. Τότε ο S είναι Von Neumann κανονικός. Θεωρώ $f \in S$ και τα $\ker f$, $imf \subseteq M$. Αφού M ημιαπλός, υπάρχουν R-υποπρότυπα $N, K \subseteq M$ με $R = \ker f \oplus N = imf \oplus K$. Ισχύει ότι ο $f|_N : N \to imf$ είναι ισομορφισμός. Πράγματι, έστω $x \in N$ με $f|_N(x) = 0 \Rightarrow f(x) = 0 \Rightarrow x \in \ker f \cap N = 0$. Συνεπώς η $f|_N$ είναι 1-1. Έστω τώρα $y = f(z) \in imf$, άρα υπάρχουν $z_1 \in \ker f$, $z_2 \in N$ με $z_1 + z_2 = z$ και $y = f(z) = f(z_1 + z_2) = f(z_1) + f(z_2) = f(z_2) = f|_N(z_2)$, επομένως $y \in imf|_N$, δηλαδή η $f|_N$ είναι επί. Θεωρώ τώρα την αντίστροφη $\gamma : imf \to N$ και ορίζω $g : M \to M$ την σύνθεση*

$$\begin{tikzcd} M = \mathrm{im} f \oplus K \arrow[r, "\pi"] \arrow[rrr, bend right, "g"'] & \mathrm{im} f \arrow[r, "\gamma"] & N \arrow[r, hook, "i"] & \ker f \oplus N = M \end{tikzcd}$$

Θα δείξω ότι $f = f \circ g \circ f : M \to M$. Πράγματι, αφού $M = \ker f \oplus N$ παίρνω περιπτώσεις.

- *Αν $x \in \ker f$, τότε $f(x) = 0 = (f \circ g \circ f)(x)$.*
- *Αν $x \in N$, τότε $(f \circ g \circ f)(x) = (f \circ g \circ f|_N)(x) = (f \circ \gamma \circ f|_N)(x) = f(x)$.*

3.3 Ο δακτύλιος $\mathbf{C}G$ είναι Jacobson ημιαπλός για κάθε ομάδα G

Στο επόμενο κεφάλιο θα αποδείξουμε ότι για πεπερασμένες ομάδες, ο δακτύλιος $\mathbf{C}G$ είναι ημιαπλός, ειδικότερα είναι Jacobson ημιαπλός. Αν και ο δακτύλιος $\mathbf{C}G$ δεν είναι ποτέ ημιαπλός για άπειρες ομάδες, στην παράγραφο αυτή θα δείξουμε ότι παραμένει Jacobson ημιαπλός.

Ορισμός 3.3.1. *Ονομάζω ενέλιξη (involution) την απεικόνιση $\mathbf{C}G \to \mathbf{C}G$ με $a \longmapsto a^*$, όπου για $a = \sum_{g \in G} \lambda_g g \in \mathbf{C}G$ είναι*

$$a^* = \sum_{g \in G} \bar{\lambda}_g g^{-1}$$

Η ενέλιξη έχει τις εξής ιδιότητες :

- $(\alpha + \beta)^* = \alpha^* + \beta^*$ *για κάθε* $\alpha, \beta \in \mathbf{C}G$
- $(\alpha\beta)^* = \beta^* \alpha^*$ *για κάθε* $\alpha, \beta \in \mathbf{C}G$
- $(\lambda\alpha)^* = \bar{\lambda}\alpha^*$ *για κάθε* $\alpha \in \mathbf{C}G$ *και* $\lambda \in \mathbf{C}$

και ορίζω το κανονικό ίχνος να είναι η γραμμική απεικόνιση

$$\mathbf{C}G \xrightarrow{\tau} \mathbf{C}$$

$$\tau : \sum_g \lambda_g g \longmapsto \lambda_e \in \mathbf{C}$$

όπου $e \in G$ το μοναδιαίο στοιχείο.

Πρόταση 3.3.1. *Έστω $\tau : \mathbf{C}G \to \mathbf{C}$ το κανονικό ίχνος, τότε :*

(i) η τ είναι γραμμική, δηλαδή $\tau(\alpha+\beta) = \tau(\alpha) + \tau(\beta)$ για κάθε $\alpha, \beta \in \mathbf{C}G$.

(ii) Η τ είναι ίχνος, δηλαδή $\tau(\alpha\beta) = \tau(\beta\alpha)$ για κάθε $\alpha, \beta \in \mathbf{C}G$.

(iii) Αν $\alpha \in \mathbf{C}G$ με $\tau(\alpha^*\alpha) = 0$, τότε $\alpha = 0$.

(iv) Για κάθε $a \in \mathbf{C}G$, ισχύει ότι $\tau(aa^*) \in \mathbf{R}$ και $|\tau(a)|^2 \leq \tau(aa^*)$.

Απόδειξη : Το (i) και (ii) είναι άμεσα, θα δείξω το (iii) και το (iv). Έστω $a = \sum_{g\in G} \lambda_g g$, τότε

$$aa^* = \left(\sum_{g\in G} \lambda_g g\right) \cdot \left(\sum_{g\in G} \bar{\lambda}_g g^{-1}\right) = \sum_{x\in G}\left(\sum_{gh=x} \lambda_g \bar{\lambda}_{h^{-1}}\right) x$$

και άρα $\tau(aa^*) = \sum_{gh=e} \lambda_g\bar{\lambda}_{h^{-1}} = \sum_{g\in G} |\lambda_g|^2$. Συνεπώς, αν $\tau(aa^*) = 0$, τότε $\sum_{g\in G} |\lambda_g|^2 = 0$, άρα $\lambda_g = 0$ για κάθε $g \in G$, δηλαδή $a = 0$. Τέλος, προφανώς $\tau(aa^*) = \sum_{g\in G} |\lambda_g|^2 \in \mathbf{R}$ και

$$\tau(aa^*) = \sum_{g\in G} |\lambda_g|^2 \geq |\lambda_e|^2 = |\tau(a)|^2$$

□

Πόρισμα 3.3.1. *Αν $a = a^* \in \mathbf{C}G$, τότε για κάθε φυσικό $n \geq 1$ είναι $\tau(a^{2^n}) \in \mathbf{R}$ και $\tau(a^{2^n}) \geq |\tau(a)|^{2^n}$*

Απόδειξη : Παρατηρώ, ότι $\tau(a^2) = \tau(aa^*) \in \mathbf{R}$ και $(a^{2^{n-1}})^* = a^{2^{n-1}}$, άρα $\tau(a^{2^n}) = \tau(a^{2^{n-1}}(a^{2^{n-1}})^*) \in \mathbf{R}$. Για την ανισότητα, θα κάνω επαγωγή στο $n \geq 1$. Για $n = 1$, είναι $\tau(a^2) = \tau(aa^*) \geq |\tau(a)|^2$. Για το επαγωγικό βήμα, έστω ότι $\tau(a^{2^n}) \geq |\tau(a)|^{2^n}$ και έχω ότι

$$\tau(a^{2^{n+1}}) = \tau(a^{2^n} \cdot a^{2^n}) \stackrel{!}{=} \tau(a^{2^n} \cdot (a^{2^n})^*) \geq |\tau(a^{2^n})|^2 \geq (|\tau(a)|^{2^n})^2 = |\tau(a)|^{2^{n+1}}$$

□

Πρόταση 3.3.2. *Αν $J(\mathbf{C}G) \neq 0$, τότε υπάρχει $a \in J(\mathbf{C}G)$ με $\tau(a^{2^n}) \in \mathbf{R}$ και $\tau(a^{2^n}) \geq 1$ για κάθε φυσικό $n \geq 1$.*

Απόδειξη : Έστω ότι $J(\mathbf{C}G) \neq 0$, τότε υπάρχει $t \in J(\mathbf{C}G)$ με $t \neq 0$. Άρα $\tau(t^*t) \neq 0$. Θεωρώ το στοιχείο $a = t^*t/\tau(t^*t) \in J(\mathbf{C}G)$ και παρατηρούμε ότι

$$\tau(a) = \tau\left(\frac{1}{\tau(t^*t)} t^*t\right) = \frac{\tau(t^*t)}{\tau(t^*t)} = 1$$

αφού $\tau(t^*t) \in \mathbf{R}$. Ακόμα βλέπουμε ότι

$$a^* = \left(\frac{1}{\tau(t^*t)} t^*t\right)^* = \frac{1}{\overline{\tau(t^*t)}}(t^*t)^* = \frac{1}{\tau(t^*t)} t^*t = a$$

Συνεπώς από τα προηγούμενα, έχουμε $\tau(a^{2^n}) \in \mathbf{R}$ και $\tau(a^{2^n}) \geq \tau(a)^{2^n} = 1$ για κάθε φυσικό $n \geq 1$. □

Ορισμός 3.3.2. *Για κάθε $a \in \mathbf{C}G$, με $a = \sum_{g\in G} \lambda_g g$, θέτω*

$$\|a\| := \sum_{g\in G} |\lambda_g|$$

Πρόταση 3.3.3. *Για κάθε $a, b \in \mathbf{C}G$ και $\lambda \in \mathbf{C}$, ισχύουν τα παρακάτων για την $\|\cdot\| : \mathbf{C}G \to \mathbf{C}$:*

- *Για $a \in \mathbf{C}G$, ισχύει $\|a\| \geq 0$ και $\|a\| = 0$ αν και μόνο αν $a = 0$*
- $\|\lambda \cdot a\| = |\lambda| \cdot \|a\|$ *για κάθε $a \in \mathbf{C}G$ και $\lambda \in \mathbf{C}$*
- $\|a + b\| \leq \|a\| + \|b\|$ *για κάθε $a, b \in \mathbf{C}G$*
- $\|ab\| \leq \|a\| \cdot \|b\|$ *για κάθε $a, b \in \mathbf{C}G$*
- $|\tau(a)| \leq \|a\|$ *για κάθε $a \in \mathbf{C}G$*

Συνεπώς, η $\|\cdot\|$ είναι νόρμα στον γραμμικό χώρο $\mathbf{C}G$.

Παρατήρηση. *Για $a \in J(\mathbf{C}G)$, έχω ότι για κάθε $z \in \mathbf{C}$ το $1 - za \in \mathbf{C}G$ είναι αντιστρέψιμο. Συνεπώς η απεικόνιση*

$$\varphi : (\mathbf{C}, |\cdot|) \longrightarrow (\mathbf{C}G, \|\cdot\|)$$
$$z \longmapsto (1 - za)^{-1}$$

είναι καλά ορισμένη.

Πρόταση 3.3.4. *Η $\varphi : (\mathbf{C}, |\cdot|) \to (\mathbf{C}G, \|\cdot\|)$ με $\varphi(z) = (1 - za)^{-1}$ είναι τοπικά $2\|a\|\|\varphi(z_0)\|^2$-Lipschitz σε κάθε $z_0 \in \mathbf{C}$ με, δηλαδή για κάθε $z_0 \in \mathbf{C}$, υπάρχει $\delta = \delta(z_0) > 0$, τέτοιο ώστε για κάθε $z \in \mathbf{C}$ με $|z - z_0| < \delta$ να ισχύει*

$$\|\varphi(z) - \varphi(z_0)\| \leq 2\|a\|\|\varphi(z_0)\|^2|z - z_0|$$

Απόδειξη : Για κάθε $z, z_0 \in \mathbf{C}$ ισχύει προφανώς ότι $\varphi(z) \cdot \varphi(z_0) = \varphi(z_0) \cdot \varphi(z)$ και άρα υπολογίζω :

$$\varphi(z) - \varphi(z_0) = (1 - z_0 a)\varphi(z_0)\varphi(z) - (1 - za)\varphi(z_0)\varphi(z) =$$
$$= ((1 - z_0 a) - (1 - za))\varphi(z_0)\varphi(z) = (z - z_0)a\varphi(z)\varphi(z_0)$$

Τελικά έχω

$$\varphi(z) - \varphi(z_0) = (z - z_0)a\varphi(z)\varphi(z_0)$$

για κάθε $z, z_0 \in \mathbf{C}$. Επίσης είναι $\|(z - z_0)a\varphi(z_0)\| = |z - z_0| \cdot \|a\varphi(z_0)\| \xrightarrow{z \to z_0} 0$ και άρα για z αρκετά κοντά στο z_0, ισχύει ότι $1 - \|(z - z_0)a\varphi(z_0)\| \geq 1/2$. Συνεπώς, για z αρκετά κοντά στο z_0, ισχύει ότι $\|\varphi(z)\| \leq 2\|\varphi(z_0)\|$, αφού

$$\varphi(z) = \varphi(z_0) + (z - z_0)a\varphi(z)\varphi(z_0) \Rightarrow$$

$$\|\varphi(z)\| = \|\varphi(z_0) + (z - z_0)a\varphi(z)\varphi(z_0)\| \leq \|\varphi(z_0)\| + \|(z - z_0)a\varphi(z_0)\| \cdot \|\varphi(z)\|$$
$$\Rightarrow \|\varphi(z)\| \cdot (1 - \|(z - z_0)a\varphi(z_0)\|) \leq \|\varphi(z_0)\| \Rightarrow \|\varphi(z)\| \leq 2\|\varphi(z_0)\|$$

Άρα τελικά για z αρκετά κοντά στο z_0

$$\|\varphi(z) - \varphi(z_0)\| = \|(z - z_0)a\varphi(z)\varphi(z_0)\| \leq |z - z_0| \cdot \|a\| \cdot \|\varphi(z)\| \cdot \|\varphi(z_0)\| \leq 2|z - z_0| \cdot \|a\| \cdot \|\varphi(z_0)\|^2$$

□

Πόρισμα 3.3.2. *Έστω $a \in J(\mathbf{C}G)$ και $\varphi : (\mathbf{C}, |\cdot|) \to (\mathbf{C}G, \|\cdot\|)$ με $\varphi(z) = (1 - za)^{-1}$, τότε ισχύουν τα εξής :*

- *Η φ είναι συνεχής σε κάθε $z \in \mathbf{C}$.*

- *Η φ είναι "παραγωγίσιμη" με την έννοια του ότι*

$$\frac{1}{z-z_0}(\varphi(z)-\varphi(z_0)) \overset{z\to z_0}{\longrightarrow} a\varphi(z_0)^2$$

Απόδειξη : Η φ σαν τοπικά Lipschitz είναι συνεχής και "παραγωγίσιμη". Για την τιμή της παραγώγου στο $z_0 \in \mathbf{C}$, έχω :

$$\frac{1}{z-z_0}(\varphi(z)-\varphi(z_0)) = a\varphi(z)\varphi(z_0) \Rightarrow \frac{1}{z-z_0}(\varphi(z)-\varphi(z_0)) \overset{z\to z_0}{\longrightarrow} a\varphi(z_0)^2$$

□

Παρατήρηση. *Το κανονικό ίχνος $\tau : (\mathbf{C}G, \|\cdot\|) \to (\mathbf{C}, |\cdot|)$ είναι συνεχής, μιας και για κάθε $a \in \mathbf{C}G$ ισχύει ότι $|\tau(a)| \leq \|a\|$.*

Πρόταση 3.3.5. *Έστω $a \in J(\mathbf{C}G)$, $\varphi : (\mathbf{C}, |\cdot|) \to (\mathbf{C}G, \|\cdot\|)$ με $\varphi(z) = (1-za)^{-1} \in \mathbf{C}G$ και $\tau : (\mathbf{C}G, \|\cdot\|) \to (\mathbf{C}, |\cdot|)$ το κανονικό ίχνος. Τότε η σύνθεση $(\tau \circ \varphi)(z) : (\mathbf{C}, |\cdot|) \to (\mathbf{C}, |\cdot|)$ είναι ολόμορφη και για $|z| < 1/\|a\|$ ισχύει ότι*

$$(\tau\circ\varphi)(z) = \sum_{n=0}^{\infty} \tau(a^n) z^n$$

Απόδειξη : Η τ είναι προσθετική και ομογενής, άρα

$$\frac{1}{z-z_0}(\tau(\varphi(z)) - \tau(\varphi(z_0))) = \tau\left(\frac{1}{z-z_0}(\varphi(z)-\varphi(z_0))\right) \overset{z\to z_0}{\longrightarrow} \tau(a\varphi(z_0)^2)$$

άρα $(\tau\circ\varphi)'(z) = \tau(a\varphi(z)^2)$ για κάθε $z \in \mathbf{C}$. Για το δεύτερο μέρος της πρότασης, αρκεί να δείξω ότι για $\|za\| < 1$ ισχύει

$$\varphi(z) = \sum_{n=0}^{\infty} a^n z^n$$

και το αποτέλεσμα προκύπτει άμεσα από την ομογένεια και προσθετικότητα της τ (Το στοιχείο $\sum_{n=0}^{\infty} a^n z^n \in \mathbf{C}G$ είναι το $\|\cdot\|$-όριο της ακολουθίας $(\sum_{n=0}^{N} a^n z^n)_N \subseteq \mathbf{C}G$). Πράγματι :

$$\left\|\varphi(z) - \sum_{n=0}^{N} z^n a^n\right\| = \left\|\varphi(z) - \varphi(z)(1-za)\sum_{n=0}^{N} z^n a^n\right\| \leq \left\|\varphi(z)\cdot\left(1-(1-za)\sum_{n=0}^{N} z^n a^n\right)\right\| =$$

$$= \|\varphi(z)\cdot(1-(1-z^{N+1}a^{N+1}))\| = \|\varphi(z)(za)^{N+1}\| \leq \|\varphi(z)\|\cdot\|za\|^{N+1} \overset{N\to\infty}{\longrightarrow} 0$$

□

Πόρισμα 3.3.3. *Έστω $\tau : (\mathbf{C}G, \|\cdot\|) \to (\mathbf{C}, |\cdot|)$ το κανονικό ιχνός και $a \in J(\mathbf{C}G)$, τότε $\lim_{n\to\infty} \tau(\alpha^n) = 0$. Πράγματι, από την προηγούμενη πρόταση, έχω*

$$\sum_{n=0}^{\infty} \tau(a^n) = (\tau\circ\varphi)(1) \in \mathbf{C}$$

και άρα $\lim_{n\to\infty} \tau(a^n) = 0$ για κάθε $a \in J(\mathbf{C}G)$.

Θεώρημα 3.3.1. *Για κάθε ομάδα G ο δακτύλιος $\mathbf{C}G$ είναι Jacobson ημιαπλός.*

Απόδειξη : Έστω, ως προς άτοπο, ότι υπάρχει $t \in J(\mathbf{C}G)$ με $t \neq 0$. Τότε δείξαμε ότι για το στοιχείο

$$a = \frac{1}{\tau(t^*t)} t^*t \in \mathbf{C}G$$

ισχύει $a^* = a$, $\tau(a^{2^n}) \in \mathbf{R}$ και $\tau(a^{2^n}) \geq 1$. Όμως από την προηγούμενη πρόταση $\lim_{n\to\infty} \tau(a^{2^n}) = 0$ #. □

ΚΕΦΑΛΑΙΟ 4

Θεωρία Αναπαραστάσεων Πεπερασμένων Ομάδων.

4.1 Αναπαραστάσεις Ομάδων

Παρατήρηση. *Έστω $\Bbbk$ ένας μεταθετικός δακτύλιος και G μια ομάδα. Τότε για τον ομαδοδακτύλιο $\Bbbk G$ ισχύει ότι : $\Bbbk \subseteq \Bbbk G$ σαν υποδακτύλιος και $G \subseteq \mathbf{U}(\Bbbk G)$ σαν υποομάδα. Αν R δακτύλιος και $f : \Bbbk G \to R$ ομομορφισμός δακτυλίων, τότε ορίζονται οι περιορισμοί :*

$$f\big|_{\Bbbk} : \Bbbk \to R \qquad f\big|_{G} : G \to \mathbf{U}(R)$$

καθώς $\lambda \cdot g = g \cdot \lambda \in \Bbbk G$ για κάθε $\lambda \in \Bbbk$ και $g \in G$ οι εικόνες $f(\Bbbk)$ και $f(G)$ μετατίθονται κατα σημείο. Αντίστροφα, αν $\varphi_1 : \Bbbk \to R$ ένας ομομορφισμός δακτυλίων και $\varphi_2 : G \to \mathbf{U}(R)$ ένας ομομορφισμός ομάδων, έτσι ώστε $\varphi_1(\lambda) \cdot \varphi_2(g) = \varphi_2(g) \cdot \varphi_1(\lambda)$ για κάθε $\lambda \in \Bbbk$ και $g \in G$, τότε η απεικόνιση $\varphi : \Bbbk G \to R$ με

$$\sum_{g \in G} \lambda_g g \xrightarrow{\quad \varphi \quad} \sum_{g} \varphi_1(\lambda_g)\varphi_2(g)$$

είναι ομομορφισμός δακτυλίων. Συνεπώς, ένα $\Bbbk G$-πρότυπο (ένας ομομορφισμός $\ell : \Bbbk G \to \mathrm{End}_{\mathbf{Z}} M$) είναι ακριβώς ένα $\Bbbk$-πρότυπο M (ένας ομομορφισμός $\ell|_{\Bbbk} : \Bbbk \to \mathrm{End}_{\mathbf{Z}} M$), το οποίο είναι εφοδιασμένο με έναν ομομορφισμό ομάδων $G \xrightarrow{\varrho} Aut_{\Bbbk} M := \mathbf{U}(\mathrm{End}(M, +))$, έτσι ώστε τα στοιχεία στην εικόνα της $G \xrightarrow{\varrho} Aut_{\Bbbk} M$ να μετατίθονται με τις ομοθεσίες $M \to M$ $(x \longmapsto \lambda x)$ για κάθε $\lambda \in \Bbbk$

Ο δακτύλιος $\mathbf{C}G$

Πόρισμα 4.1.1. *Ένα $\mathbf{C}G$-πρότυπο V είναι ακριβώς ο αντίστοιχος $\mathbf{C}$-διανυσματικός χώρος V εφοδιασμένος με έναν ομομορφισμό $\varrho : G \to GL(V)$. Τον ομομορφισμό $\varrho : G \to GL(V)$ τον ονομάζουμε αναπαράσταση.*

Ορισμός 4.1.1. *Έστω V ένα $\mathbf{C}G$-πρότυπο, ισοδύναμα μια αναπαράσταση $\varrho : G \to GL(V)$.*

- *Ορίζουμε την διάσταση της ϱ να είναι η διάσταση του $\mathbf{C}$-διανυσματικού χώρου V*
- *Η ϱ λέγεται ανάγωγη, αν το αντίστοιχο $\mathbf{C}G$-πρότυπο V είναι απλό. Ισοδύναμα, δεν υπάρχει $\mathbf{C}$-διανυσματικός υπόχωρος $U \subseteq V$, τέτοιος ώστε να είναι ϱ_g-αναλλοίωτος για κάθε $g \in G$.*

Παραδείγματα. (i) *Το τετριμμένο $\Bbbk G$-πρότυπο λαμβάνεται για $M = \Bbbk$ με τα αντίστοιχα στοιχεία της G να δρουν τετριμμένα, δηλαδή ο ομομορφισμός $G \to Aut(\Bbbk)$ είναι ο τετριμμένος, πιο συγκεκριμένα :*

$$\left(\sum_{g \in G} \lambda_g g \right) \cdot \lambda = \sum_{g \in G} \lambda_g \lambda$$

για κάθε $\sum_g \lambda_g g \in \Bbbk G$ *και* $\lambda \in \Bbbk$. *Ο αντίστοιχος ομομορφισμός δακτυλίων* $\Bbbk G \xrightarrow{\varepsilon} \Bbbk$ *καλείται ομομορφισμός επαύξησης, είναι* $\varepsilon(\sum_g \lambda_g g) = \sum_g \lambda_g$ *και ο πυρήνας του*

$$I_G(\Bbbk) = \ker(\Bbbk G \xrightarrow{\varepsilon} \Bbbk)$$

καλείται ιδεώδες επαύξησης

Πρόταση 4.1.1. *Το* $I_G(\Bbbk)$ *παράγεται ως* $\Bbbk$*-πρότυπο από τα στοιχεία* $g - e$, *για* $g \in G \setminus \{e\}$, *τα οποία μάλιστα αποτελούν μια βάση του* $\Bbbk G$*-προτύπου* $I_G(\Bbbk)$.

Απόδειξη : Έστω $\sum_g \lambda_g g \in I_G(\Bbbk)$, τότε $\lambda_e = -\sum_{g\neq e} \lambda_g$ και άρα

$$\sum_{g\in G} \lambda_g g = \lambda_e e + \sum_{g\in G\setminus\{e\}} \lambda_g g = -\sum_{g\in G\setminus\{e\}} \lambda_g e + \sum_{g\in G\setminus\{e\}} \lambda_g g = \sum_{g\in G\setminus\{e\}} \lambda_g (g-e)$$

Είναι άμεσο ότι τα στοιχεία $g - e$ για $g \in G \setminus \{e\}$ είναι γραμμικά ανεξάρτητα. $\square$

(ii) *Ο ομομορφισμός πρόσημο sign* : $S_n \to \{-1, 1\} \hookrightarrow \mathbf{U}(\Bbbk)$ *επάγει στο* $M = \Bbbk$ *την δομή ενός* $\Bbbk S_n$*-προτύπου, με*

$$\left(\sum_{\sigma\in S_n} \lambda_\sigma \sigma\right) \cdot \lambda = \sum_{\sigma\in S_n} \lambda_\sigma \cdot \mathit{sign}(\sigma)\lambda$$

(iii) *Η* $D_3 = \langle r, s : r^3 = s^2 = srsr = 1\rangle$ *έχει τη φυσική 2-διασταστή αναπαράσταση που ορίζεται μέσω της* $\varrho : D_3 \to GL_2(\mathbf{C})$ *με*

$$\varrho(r) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \varrho(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

δηλαδή η $\varrho : D_3 \to GL_2(\mathbf{C})$ *στέλνει την στροφή* $r \in D_3$, *στον πίνακα στροφής και την ανάκλαση* $s \in D_3$ *στον πίνακα ανάκλασης.*

(iv) *Η* S_n *έχει μια* n*-διάστατη αναπαράστατη στον* $\mathbf{C}^n = \bigoplus_{i=1}^n \mathbf{C}e_i$, *όπου* $\sigma e_i = e_{\sigma(i)}$. *Για παράδειγμα, για* $n = 3$ *:*

$$(1\ 2) \longmapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (1\ 2\ 3) \longmapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Η αναπαράσταση αυτή δεν είναι ανάγωγη, καθώς ο διανυσματικός υπόχωρος $U = \mathbf{C}(e_1 + \cdots + e_n)$ *είναι* S_n*-αναλλοίωτος και άρα είναι ένα* $\mathbf{C}S_n$*-υποπρότυπο του* $\mathbf{C}^n$.

(v) *Κάθε ομάδα* G *δρα στον ευατό της μέσων αριστερών πολλαπλασιασμών. Άρα η* G *δρα στον* $\mathbf{C}G = \bigoplus_{g\in G} \mathbf{C}g$ *ως εξής :* $x \cdot g = xg$ *για κάθε* $x, g \in G$. *Αυτή η αναπαράσταση ονομάζεται, αριστερή κανονική αναπαράσταση της* G.

Θεώρημα 4.1.1 (Maschke). *Ο δακτύλιος* $\Bbbk G$ *είναι ημιαπλός αν και μόνο αν ο* $\Bbbk$ *είναι ημιαπλός, η* G *είναι πεπερασμένη και* $\#G \cdot 1_\Bbbk \in \mathbf{U}(\Bbbk)$

Απόδειξη : • Ο $\Bbbk G$ είναι ημιαπλός $\Rightarrow$ ο $\Bbbk$ είναι ημιαπλός : Θεωρώ τον ομομορφισμό επαύξησης $\varepsilon : \Bbbk G \to \Bbbk$, ο οποίος είναι επί με πυρήνα $I_G(\Bbbk)$. Από το 1ο θεώρημα ομομορφισμών $\Bbbk G/I_G(\Bbbk) \simeq \Bbbk$. Καθώς τα πηλικά ημιαπλών δακτυλιών είναι ημιαπλοί δακτύλιοι, έπεται ότι $\Bbbk$ ημιαπλός

• Ο $\Bbbk G$ είναι ημιαπλός $\Rightarrow$ G είναι πεπερασμένη : Έστω, ως προς άτοπο, ότι G είναι άπειρη. Αφού ο $\Bbbk G$ είναι ημιαπλός, κάθε ιδεώδες έχει συμπλήρωμα, ειδικότερα για το ιδεώδες επαύξησης είναι $\Bbbk G = I_G(\Bbbk) \oplus J$ για κάποιο αριστερό ιδεώδες J. Παρατηρώ ότι για κάθε $x \in J$ και κάθε $g \in G$

είναι $(1-g)x \in I_G(\Bbbk) \cap J = 0$. Συνεπώς $gx = x$ για κάθε $g \in G$ και κάθε $x \in J$. Εξετάζοντας την συνιστώσα του $e \in G$, προκύπτει $x_e = x_{g^{-1}}$ για κάθε $g \in G$ και $x \in J$. Αφού $\#G = \infty$, οι μόνες σταθερές απεικονίσεις $x : G \to \Bbbk$ πεπερασμένου φορέα είναι οι μηδενικές, συνεπώς $J = 0$ # .

• Ο $\Bbbk G$ είναι ημιαπλός $\Rightarrow$ $G \cdot 1_\Bbbk \in \mathbf{U}(\Bbbk)$: Για αυτήν την συνεπαγωγή, θα χρησιμοποιήσω το εξής λήμμα

Λήμμα 4.1.1. *Έστω $g \in G$ με $o(g) = n$ και $x \in \Bbbk G$ με $(1-g)x = 0$, τότε υπάρχει $y \in \Bbbk G$ με $x = (1+g+g^2+\cdots+g^{n-1})y$*

Απόδειξη : Πράγματι έστω $x = \sum_h x_h h$ και έχω ότι $x = gx = \sum_h x_h(gh) = \sum_h x_{g^{-1}h}h$ άρα $x_h = x_{g^{-1}h}$. Επαγωγικά $x_h = x_{g^{-1}h} = x_{g^{-2}h} = \cdots == x_{g^{-(n-1)}h} \in \Bbbk$, $\forall h \in G$, δηλαδή $x_h = x_{h'}$ αν $\langle g\rangle h = \langle g\rangle h'$. Συνεπώς

$$x = \sum_{h\in G} x_h h = \sum_{\langle g\rangle h \in G/\langle g\rangle} \sum_{h' \in \langle g\rangle h} x_{h'}h' = \sum_{\langle g\rangle h \in G/\langle g\rangle} x_h \left(\sum_{h' \in \langle g\rangle h} h' \right) =$$

$$= \sum_{\langle g\rangle h \in G/\langle g\rangle} x_h(h+gh+g^2h+\cdots+g^{n-1}h) = (1+g+g^2+\cdots+g^{n-1})y$$

όπου $y = \sum_{\langle g\rangle h\in G/\langle g\rangle} x_h h$. □

Ο $\Bbbk G$ είναι ημιαπλός, ειδικότερα Von Neumann κανονικός. Έστω $g \in G$ με $o(g) = n$, τότε υπάρχει $\alpha \in \Bbbk G$, τέτοιο ώστε $1-g = (1-g)\alpha(1-g) \iff (1-g)(1-\alpha(1-g)) = 0$. Από λήμμα, υπάρχει $\beta \in \Bbbk G$, τέτοιο ώστε $1-\alpha(1-g) = (1+g+g^2+\cdots+g^{n-1})\beta$. Εφαρμόζοντας τον ομομορφισμό επαύξησης στην προηγούμενη ισότητα παίρνω $1 = n\varepsilon(\beta)$. Τελικά, για κάθε $g \in G$ με $o(g) = n$, ισχύει ότι $n \cdot 1_\Bbbk \in \mathbf{U}(\Bbbk)$. Γράφω $\#G = p_1p_2\cdots p_r$ για κάποιους (όχι αναγκαστηκά διακεκριμένους) πρώτους και επιλέγω στοιχεία ταξής p_i[1] για κάθε i, άρα $p_i \cdot 1_\Bbbk \in \mathbf{U}(\Bbbk)$ για κάθε $i = 1, 2, \ldots r$, έπεται $\#G \cdot 1_\Bbbk = (p_1 \cdot 1_\Bbbk)\ldots(p_r \cdot 1_\Bbbk) \in \mathbf{U}(\Bbbk)$

($\Leftarrow$) Θα δείξω ότι κάθε $\Bbbk G$-πρότυπο V είναι ημιαπλό. Έστω V λοιπόν ένα $\Bbbk G$-πρότυπο και $U \subseteq V$ ένα $\Bbbk G$-υποπρότυπο του. Προφανώς, το $U \subseteq V$ είναι ένα πρότυπο αναλλοίωτο ως προς την δράση της G, δηλαδή $gU \subseteq U$ για κάθε $g \in G$. Καθώς, ο $\Bbbk$ είναι ημιαπλός, υπάρχει $\Bbbk$-υποπρότυπο $U' \subseteq V$, τέτοιο ώστε $U \oplus U' = V$. Θεωρώ την $\Bbbk G$-γραμμική απεικόνιση $\varphi : V \to U$ με $\varphi|_U = 1_U$ και $U' \subseteq \ker\varphi$ και με την σειρά της την $\Bbbk$-γραμμική απεικόνιση $F : V \to U$ με

$$F(v) = \frac{1}{\#G}\sum_{g\in G} g^{-1}\varphi(gv)$$

Παρατηρώ ότι για $u \in U$

$$F(u) = \frac{1}{\#G}\sum_{g\in G} g^{-1}\varphi(gu) = \frac{1}{\#G}\sum_{g\in G} g^{-1}(gu) = \frac{1}{\#G}\sum_{g\in G} u = u$$

δηλαδή $F|_U = 1_U$. Επίσης η $F : V \to U$ είναι $\Bbbk G$-γραμμική. Πράγματι, έστω $h \in G$ και $v \in V$ τότε

$$F(hv) = \frac{1}{\#G}\sum_{g\in G} g^{-1}\varphi(ghv) = \frac{1}{\#G}\sum_{x\in G} hx^{-1}\varphi(xv) = hF(v)$$

Συνοψίζοντας η $F : V \to U$ είναι μια $\Bbbk G$-γραμμική απεικόνιση με $F|_U = 1_U$. Στην περίπτωση αυτή, ισχύει ότι $V = \ker F \oplus U$ και άρα το U έχει $\Bbbk G$-συμπλήρωμα. Πράγματι, για $v \in V$ είναι $v = v - F(v) + F(v)$ και παρατηρώ ότι $v - F(v) \in \ker F$ και $F(v) \in U$, συνεπώς $U + \ker F = V$. Αν τώρα $v \in U \cap \ker F$, τότε $v = F^2(v) = F(F(v)) = F(0) = 0$, άρα $U \oplus \ker F = V$. □

[1]Θεώρημα Cauchy : Έστω G πεπερασμένη ομάδα και p πρώτος αριθμός με $p \mid \#G$, τότε υπάρχει στοιχείο $g \in G$ με $o(g) = p$.

Πόρισμα 4.1.2. *Ο* $\mathbf{C}G$ *είναι ημιαπλός αν και μόνο αν* $\#G < \infty$.

Πρόταση 4.1.2 (Molien). *Έστω* k *ένα αλγεβρικά κλειστό σώμα και* R *ένας ημιαπλός δακτύλιος, τέτοιος ώστε* $k \hookrightarrow Z(R)$. *Τότε, η διάσπαση Wedderburn-Artin είναι* $R \simeq \prod_{i=1}^{r} \mathbf{M}_{n_i}(k)$.

1η Απόδειξη : Γνωρίζουμε ότι $R \simeq \prod_{i=1}^{r} \mathbf{M}_{n_i}(D_i)$, όπου $D_i = (\mathrm{End}_R V_i)^{op}$ και V_i τα απλά R-πρότυπα για $i = 1, 2, \ldots, r$. Έστω V ένα απλό R-πρότυπο και $f : V \to V$ μια R-γραμμική απεικόνιση, ειδικότερα ο V είναι k-διανυσματικός χώρος και η $f : V \to V$ είναι k-γραμμική. Αφού το k είναι αλγεβρικά κλειστό, ο ενδομορφισμός f έχει κάποια ιδιοτιμή $\lambda \in k$, με αντίστοιχο ιδιόχωρο $E_\lambda \subseteq V$. Ο E_λ είναι στην πραγματικότητα R-υποπρότυπο. Πράγματι, έστω $v \in E_\lambda$ και $r \in R$, τότε

$$f(rv) = rf(v) = r(\lambda v) = (r\lambda)v \overset{!}{=} (\lambda r)v = \lambda(rv)$$

δηλαδή $rv \in E_\lambda$. Αφού το V είναι απλό και ο E_λ μη μηδενικό R-υποπρότυπο, τότε $V = E_\lambda$, δηλαδή $f = \lambda \cdot 1_V : V \to V$. Συνεπώς, $D_i = (\mathrm{End}_R V_i)^{op} \simeq k^{op} \simeq k$ □

Πόρισμα 4.1.3. *Αν* $\#G < \infty$, *τότε* $\mathbf{C}G \simeq \prod_{i=1}^{r} \mathbf{M}_{n_i}(\mathbf{C})$.

Πόρισμα 4.1.4. *Αν* $\#G < \infty$ *και* $n_1, \ldots, n_r$ *οι βαθμοί των ανάγωγων αναπαραστάσεων, τότε* $\#G = \sum_{i=1}^{n} n_i^2$

Απόδειξη : Η διάσπαση Wedderburn-Artin είναι $\mathbf{C}G \simeq \prod_{i=1}^{r} \mathbf{M}_{n_i}(\mathbf{C})$, συνεπώς

$$\#G = \dim_{\mathbf{C}} \mathbf{C}G = \dim_{\mathbf{C}} \left\{ \prod_{i=1}^{r} \mathbf{M}_{n_i}(\mathbf{C}) \right\} = \sum_{i=1}^{r} n_i^2$$

□

Μονοδιάστατες Αναπαράστασεις

Στην παράγραφο αυτή, δοσμένης μιας πεπερασμένης ομάδας G, αναζητούμε ολα $\mathbf{C}G$-πρότυπα V με $\dim_{\mathbf{C}} V = 1$. Θα δείξουμε ότι το πλήθος των μονοδιάστατων αναπαραστάσεων είναι ίσο με $\#G_{ab}$ και οι πιθανοί ομομορφισμοί είναι $G \xrightarrow{\pi} G_{ab} \longrightarrow \mathbf{C}$. Τέλος, δείχνουμε ότι οι ανάγωγες αναπαραστάσεις μιας αβελιανής ομάδας A είναι όλες μονοδιάστατες.

Ορισμός 4.1.2. *Αν* A *είναι μια αβελιανή ομάδα, τότε η δυϊκή ομάδα* $\hat{A}$ *ορίζεται ώς*

$$\hat{A} = \{\varrho : A \to S^1 \ : \ \varrho \text{ ομομορφισμός}\}$$

Παρατηρήσεις. (i) *Αν* $A = \mathbf{Z}_n$, *τότε ένας ομομορφισμός* $\varrho : \mathbf{Z}_n \to S^1$ *καθορίζεται πλήρως από την εικόνα του γεννήτορα. Παρατηρώ ότι για κάθε* $k \in \mathbf{N}$, *μπορώ να ορίσω* $\varphi_k(\overline{1}) = e^{2\pi i k/n}$. *Συνεπώς,* $\mathbf{Z}_n \simeq \hat{\mathbf{Z}}_n$.

(ii) *Αν* A, B *αβελιανές ομάδες, τότε η απεικόνιση* $\widehat{A \oplus B} \longrightarrow \hat{A} \oplus \hat{B}$, *όπου*

$$(\varrho : A \oplus B \to S^1) \longmapsto (\varrho\big|_A : A \to S^1, \varrho\big|_B : B \to S^1)$$

είναι ισομορφισμός αβελιανών ομάδων.

(iii) *Αν* A *μια πεπερασμένη αβελιανή ομάδα, τότε η* $\hat{A}$ *είναι πεπερασμένη και μάλιστα* $\hat{A} \simeq A$. *Πράγματι, από το θεώρημα δομής* $A \simeq \bigoplus_{i=1}^{r} \mathbf{Z}_{p_i^{a_i}}$, *οπότε* $\hat{A} \simeq \bigoplus_{i=1}^{r} \widehat{\mathbf{Z}_{p_i^{a_i}}} \simeq \bigoplus_{i=1}^{r} \mathbf{Z}_{p_i^{a_i}} \simeq A$.

(iv) *Κάθε μονοδιάστατη αναπαράσταση είναι ανάγωγη, δηλαδή το αντίστοιχο* $\mathbf{C}G$ *είναι απλό.*

Πρόταση 4.1.3 (Καθολική ιδιότητα της αβελιανοποίησης). *Οι μονοδιάστατες μιγαδικές αναπαραστάσεις μιας ομάδας G, αντιστοιχούν σε ομομορφισμούς ομάδων $G \to \mathbf{C}^*$. Καθε τέτοιος ομομορφισμός απεικονίζει την παράγωγο υποομάδα $D(G) = \langle xyx^{-1}y^{-1} : x, y \in G\rangle$ στο τετριμμένο στοιχείο $1 \in \mathbf{C}^*$ και άρα παραγοντοποιείται μέσω της αβελιανοποιήσης $G_{ab} := G/D(G)$. Ειδικότερα, αν $\#G < \infty$, τότε $\{\varrho : G \to \mathbf{C}^* \mid \varrho$ ομομορφισμός$\} \overset{\simeq}{\longleftrightarrow} \{\bar{\varrho} : G_{ab} \to \mathbf{C}^* \mid \varrho$ ομομορφισμός$\} = \{\bar{\varrho} : G \to S^1 \mid \varrho$ ομομορφισμός$\} = \widehat{G_{ab}} \simeq G_{ab}$*

$$\begin{tikzcd} & G_{ab} \arrow[dr, "\bar{\varrho}"] & \\ G \arrow[ur, two heads, "\pi"] \arrow[rr, "\varrho"'] & & \mathbf{C} \end{tikzcd}$$

Συνεπώς το πλήθος των μιγαδικών μονοδιάστατων αναπαραστάσεων ισούται με $\#G_{ab}$

Παραδείγματα. (i) *Οι μονοδιάστατες αναπαραστάσεις της $S_n = \langle (1\,2), (1\;2\;\cdots\;n)\rangle$:*
Αναζητούμε ομομορφισμούς ομάδων $S_n \to \mathbf{C}^*$. Υπάρχουν τουλάχιστον δύο τέτοιοι ομομορφισμοί,

	e	$(1\,2)$	$(1\;2\;\cdots\;n)$	
ϱ_1	1	1	1	*(τετριμμένη)*
ϱ_2	1	-1	$(-1)^{n+1}$	*(αναπαράσταση πρόσημο)*

Με λίγη προσπάθεια, δείχνουμε ότι $D(S_n) = A_n$ και άρα $(S_n)_{ab} = S_n/A_n \simeq \mathbf{Z}_2$, συνεπώς τελικά υπάρχουν ακριβώς 2 μονοδιάστατες αναπαραστάσεις.

(ii) *Οι μονοδιάστατες αναπαραστάσεις της $A_4 = \langle (1\,2)(3\,4), (1\,2\,3)\rangle \simeq \langle a, b : a^2 = b^3 = 1, (ab)^3 = 1\rangle$*

Έστω $G = A_4$, θεωρώ την αβελιανοποιήση $G_{ab} = \langle a, b : a^2 = b^3 = 1, (ab)^3 = 1, ab = ba\rangle = \langle b : b^3 = 1\rangle \simeq \mathbf{Z}_3$, δηλαδή στο πηλίκο G_{ab} ο γεννήτορας $a = (1\,2)(3\,4)$ είναι το τετριμμένο στοιχείο και ο $b = (1\;2\;3)$ είναι στοιχείο τάξης 3. Αναζητούμε ομομορφισμούς $G_{ab} \to \mathbf{C}^*$. Οι πιθανοί ομομορφισμοί είναι $\#G_{ab} = 3$

	e	$(1\,2)(3\,4)$	$(1\;2\;3)$
ϱ_1	1	1	1
ϱ_2	1	1	ω
ϱ_3	1	1	ω^2

όπου $\omega = e^{2\pi i/3}$.

Πρόταση 4.1.4. *Έστω G αβελιανή ομάδα και V ένα απλό $\mathbf{C}G$-πρότυπο με $\dim_{\mathbf{C}} V < \infty$. Τότε $\dim_{\mathbf{C}} V = 1$.*

Απόδειξη. Έστω $g \in G$, αφού $\mathbf{C}$ είναι αλγεβρικά κλειστό, η γραμμική απεικόνιση $g : V \to V$ έχει ιδιοτιμή $\lambda_g \in \mathbf{C}$. Ο ιδιόχωρος $E_\lambda = \{v \in V : gv = \lambda_g v\} \neq 0$ είναι ένας διανυσματικός υπόχωρος του V και παρατηρούμε ότι είναι αναλλοίωτος στην δράση της G, δηλαδή $gE_\lambda \subseteq E_\lambda$ για κάθε $g \in G$. Συνέπως είναι ένα μη μηδενικό $\mathbf{C}G$-υποπρότυπο του V και αφού το V απλό, $V = E_\lambda$. Άρα για κάθε $g \in G$, υπάρχει $\lambda_g \in \mathbf{C}$, ώστε $g \cdot v = \lambda_g \cdot v$ για κάθε $v \in V$. Συνεπώς, κάθε $\mathbf{C}$-διανυσματικός υπόχωρος είναι G-αναλλοίωτος, άρα $\dim_{\mathbf{C}} V = 1$. $\square$

Πρόταση 4.1.5. *Έστω U, V δύο $\mathbf{C}G$-πρότυπα και $\varrho_U : G \to GL(U)$, $\varrho_V : G \to GL(V)$ οι αντίστοιχοι ομομορφισμοί. Τότε τα $\mathbf{C}G$-πρότυπα είναι ισόμορφα αν και μόνο αν υπάρχει ισομορφισμός $\mathbf{C}$-διανυσματικών χώρων $f : U \to V$ έτσι ώστε $\varrho_U = f^{-1} \circ \varrho_V \circ f$.*

Απόδειξη. ($\Rightarrow$) Έστω ότι U, V είναι ισόμορφα σαν $\mathbf{C}G$-πρότυπα και $f : U \to V$ ο $\mathbf{C}G$-ισομορφισμός ανάμεσα τους. Τότε $(f \circ \varrho_U(g))(u) = f(g \cdot u) = g \cdot f(u) = (\varrho_V(g))(f(u)) = (\varrho_V(g) \circ f)(u)$, δηλαδή $f \circ \varrho_U = \varrho_V \circ f$, ισοδύναμα $\varrho_U = f^{-1} \circ \varrho_V \circ f$.
($\Leftarrow$) Εύκολα δείχνουμε ότι η $\mathbf{C}$-γραμμική απεικόνιση $f : U \to V$ είναι στην πραγματικότητα $\mathbf{C}G$-γραμμική. $\square$

Πόρισμα 4.1.5. *Αν $U = V = \mathbf{C}$ δύο μονοδιάστατες αναπαραστάσεις της G με αντίστοιχούς ομομορφισμούς $\varrho_U : G \to \mathbf{C}^*$, $\varrho_V : G \to \mathbf{C}^*$, τότε τα $\mathbf{C}G$-πρότυπα U, V είναι ισόμορφα αν και μόνο αν $\varrho_U \equiv \varrho_V$.*

Πόρισμα 4.1.6. *Υπάρχει αμφιμονοσήμαντη αντιστοιχεία :*

$$\{\textit{κλάσεις ισομορφίας μονοδιάστατων αναπαραστάσεων}\} \longleftrightarrow \{\varrho : G \to \mathbf{C}^* : \varrho \textit{ ομομορφισμός ομάδων}\}$$

Παρατήρηση. *Η απεικόνιση πηλίκο $\pi : G \to G/D(G) = G_{ab}$ επάγει για κάθε ομάδα H, μια 1-1 απεικόνιση :*

$$\{f : G_{ab} \to H \ : \ f \textit{ ομομορφισμός}\} \xrightarrow{\pi^*} \{\varphi : G \to H \ : \ \varphi \textit{ ομομορφισμός}\}$$

Το 1-1 έπεται από το γεγονός ότι η π είναι επί ($f \circ \pi = f' \circ \pi' \Rightarrow f = f'$). Αν η H είναι αβελιανή, τότε η π^* είναι και επί.

4.2 Χαρακτήρες

Ορισμός 4.2.1. *Έστω G πεπερασμένη ομάδα και έστω V ένα $\mathbf{C}G$-πρότυπο με $\dim_{\mathbf{C}} V < \infty$. Ο χαρακτήρας χ_V του $\mathbf{C}G$-προτύπου V είναι η απεικόνιση $\chi_V : \mathbf{C}G \to \mathbf{C}$ με :*

$$\chi_V(\alpha) = \mathrm{tr}(V \xrightarrow{\alpha} V)$$

για κάθε $\alpha \in \mathbf{C}G$, δηλαδή $\chi_V(\alpha) = \mathrm{tr}(\varrho(a))$, όπου $\varrho : \mathbf{C}G \to \mathrm{End}_{\mathbf{C}}(V, +)$ ο ομομορφισμός που δίνει την δομή $\mathbf{C}G$-προτύπου στον V.

Παρατηρήσεις. (i) *Ο χαρακτήρας είναι γραμμική απεικόνιση, δηλαδή μια γραμμική μορφή του $\mathbf{C}$-διανυσματικόυ χώρου $\mathbf{C}G$.*

(ii) *Ο χαρακτήρας $\chi_V : \mathbf{C}G \to \mathbf{C}$ είναι ένα ίχνος, δηλαδή $\chi_V(\alpha\beta) = \chi_V(\beta\alpha)$ για κάθε $\alpha, \beta \in \mathbf{C}G$. Ειδικότερα $\chi_V(xy) = \chi_V(yx)$ για κάθε $x, y \in G$.*

(iii) *Παρατηρούμε ότι $\chi_V(g) = \chi_V(hgh^{-1})$ για κάθε $g, h \in G$, δηλαδή ο χαρακτήρας χ_V είναι σταθερός στις κλάσεις συζηγιας.*

(iv) *Οι επόμενοι τρεις ορισμοί είναι ισοδύναμοι :*

- *Έστω G πεπερασμένη ομάδα και έστω V ένα $\mathbf{C}G$-πρότυπο με $\dim_{\mathbf{C}} V < \infty$. Ο χαρακτήρας χ_V του $\mathbf{C}G$-προτύπου V είναι η απεικόνιση $\chi_V : \mathbf{C}G \to \mathbf{C}$ με : $\chi_V(\alpha) = \mathrm{tr}(V \xrightarrow{\alpha} V)$ για κάθε $\alpha \in \mathbf{C}G$, δηλαδή $\chi_V(\alpha) = \mathrm{tr}(\varrho(a))$, όπου $\varrho : \mathbf{C}G \to \mathrm{End}_{\mathbf{C}}(V, +)$ ο ομομορφισμός που δίνει την δομή $\mathbf{C}G$-προτύπου στον V.*

- *Έστω G πεπερασμένη ομάδα και έστω V ένα $\mathbf{C}G$-πρότυπο με $\dim_{\mathbf{C}} V < \infty$. Ο χαρακτήρας χ_V του $\mathbf{C}G$-προτύπου V είναι η απεικόνιση $\chi_V : G \to \mathbf{C}$ με : $\chi_V(g) = \mathrm{tr}(\varrho(g))$, όπου $\varrho : \mathbf{C}G \to \mathrm{End}_{\mathbf{C}}(V, +)$ ο ομομορφισμός που δίνει την δομή $\mathbf{C}G$-προτύπου στον V.*

- *Έστω G πεπερασμένη ομάδα και έστω V ένα $\mathbf{C}G$-πρότυπο με $\dim_{\mathbf{C}} V < \infty$. Ο χαρακτήρας χ_V του $\mathbf{C}G$-προτύπου V είναι η απεικόνιση $\chi_V : \mathcal{C}(G) \to \mathbf{C}$ με : $\chi_V([g]) = \mathrm{tr}(\varrho(g))$ όπου $\varrho : \mathbf{C}G \to \mathrm{End}_{\mathbf{C}}(V, +)$ ο ομομορφισμός που δίνει την δομή $\mathbf{C}G$-προτύπου στον V και $\mathcal{C}(G)$ το σύνολο των κλάσεων συζηγίας της G.*

Πρόταση 4.2.1. *Αν V ένα $\mathbf{C}G$-πρότυπο με $\dim_{\mathbf{C}} V < \infty$ και το $V' \subseteq V$ είναι $\mathbf{C}G$-υποπρότυπο, τότε $\chi_V = \chi_{V'} + \chi_{V/V'}$*

Απόδειξη. Θα δείξω ότι για κάθε $g \in G$, ισχύει ότι $\chi_V(g) = \chi_{V'}(g) + \chi_{V/V'}(g)$ δηλαδή ότι

$$\mathrm{tr}(V \xrightarrow{g} V) = \mathrm{tr}(V' \xrightarrow{g} V') + \mathrm{tr}(V/V' \xrightarrow{g} V/V')$$

Θεωρώ μια βάση $v_1, \ldots, v_n$ του V' και την επεκτείνω σε μια βάση $v_1, \ldots, v_n, v_{n+1}, \ldots v_r$ του V. Ο πίνακας της $g : V \to V$ ως προς την βάση αυτή έχει την μορφή :

$$\left(\begin{array}{c|c} A & B \\ \hline O & C \end{array}\right)$$

Συνεπώς $\mathrm{tr}(V \xrightarrow{g} V) = \mathrm{tr}(A) + \mathrm{tr}(C)$. Προφανώς ο A είναι ο πίνακας της $g : V' \to V'$ ως προς την βάση $v_1, \ldots, v_n$ του V', άρα $\mathrm{tr}(A) = \mathrm{tr}(V' \xrightarrow{g} V')$. Τέλος, αφού τα $v_{n+1} + V', \ldots, v_r + V'$ αποτελούν βάση του V/V', $\mathrm{tr}(C) = \mathrm{tr}(V/V' \xrightarrow{g} V/V)$ □

Πόρισμα 4.2.1. *Αν $V_1 \oplus V_2 = V$ ως $\mathbf{C}G$-πρότυπα και $\dim_{\mathbf{C}} V < \infty$, τότε $\chi_V = \chi_{V_1} + \chi_{V_2}$ και επαγωγικά έχουμε ότι για $V = \bigoplus_{i=1}^r V_i^{n_i}$ ισχύει ότι $\chi_V = \sum_{i=1}^r n_i \cdot \chi_{V_i}$.*

Παρατήρηση. *Αν $U = \mathbf{C}$ μονοδιάστατη αναπαράσταση με αντίστοιχο ομομορφισμό $\varrho_U : G \to \mathbf{C}^*$, τότε ο χαρακτήρας $\chi_U : G \to \mathbf{C}$ είναι η σύνθεση $G \xrightarrow{\varrho_U} \mathbf{C}^* \hookrightarrow \mathbf{C}$*

Πίνακες Χαρακτήρων

Ορισμός 4.2.2. *Έστω G μια πεπερασμένη ομάδα. Πίνακας χαρακτήρων λέμε τον πίνακα που οι γραμμές του αντιστοιχούν στις ανάγωγες αναπαραστάσεις της G και οι στήλες του αντιστοιχούν στις κλάσεις συζηγίας της G. Η εγγραφή στην (i, j)-θέση είναι η τιμή του i-χαρακτήρα στην j-κλάση συζηγίας. Συνεπώς, αν σταθεροποιήσουμε αντιπροσώπους $g_1, g_2, g_3, \ldots$ των κλάσεων συζηγίας, τότε ο πίνακας χαρακτήρων είναι*

$\mathcal{C}(G)$	g_1	g_2	g_3	$\cdots$
χ_1	$\chi_1(g_1)$	$\chi_1(g_2)$	$\chi_1(g_3)$	$\cdots$
χ_2	$\chi_2(g_1)$	$\chi_2(g_2)$	$\chi_2(g_3)$	$\cdots$
χ_3	$\chi_3(g_1)$	$\chi_3(g_2)$	$\chi_3(g_3)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Παραδείγματα. *(i) Οι ανάγωγες αναπαραστάσεις τις $G = \mathbf{Z}_2 \oplus \mathbf{Z}_4$:*
Από την πρόταση 4.3.3, καθώς η G είναι αβελιανή, οι ανάγωγες αναπαραστάσεις της G είναι μονοδιάστατες. Αναζητώ ομομορφισμούς $\varrho : \mathbf{Z}_2 \oplus \mathbf{Z}_4 \to S^1$ και από τις προηγούμενες παρατηρήσεις, αρκεί να αναζητήσω ομομορφισμούς ομάδων $\varrho_1 = \varrho\,|_{\mathbf{Z}_2} : \mathbf{Z}_2 \to S^1$, $\varrho_2 = \varrho\,|_{\mathbf{Z}_4} : \mathbf{Z}_4 \to S^1$. Υπάρχουν συνολικά $\#\mathbf{Z}_2 = 2$ ομομορφισμοί $\varrho\,|_{\mathbf{Z}_2} : \mathbf{Z}_2 \to S^1$ και $\#\mathbf{Z}_4 = 4$ ομομορφισμοί $\varrho\,|_{\mathbf{Z}_4} : \mathbf{Z}_4 \to S^1$ ($\hat{\mathbf{Z}}_n \simeq \mathbf{Z}_n$), για συνολικά $4 \cdot 2 = 8$ ομομορφισμούς $\varrho : \mathbf{Z}_2 \oplus \mathbf{Z}_4 \to S^1$. Τέλος οι χαρακτήρες μονοδιάστατων $\mathbf{C}G$-προτύπων ταυτίζονται με τους αντίστοιχους ομομορφισμούς. Ο πίνακας χαρακτήρων είναι ο εξής :

	$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$
χ_1	1	1	1	1	1	1	1	1
χ_2	1	i	-1	$-i$	1	i	-1	$-i$
χ_3	1	-1	$-i$	1	1	-1	$-i$	1
χ_4	1	$-i$	1	i	1	$-i$	1	i
χ_1	1	1	1	1	-1	-1	-1	-1
χ_2	1	i	-1	$-i$	-1	$-i$	1	i
χ_3	1	-1	$-i$	1	-1	1	$-$	-1
χ_4	1	$-i$	1	i	-1	i	-1	$-i$

(ii). Οι ανάγωγες αναπαραστάσεις τις $G = S_3 = \langle (1,2),(1,3) \rangle = \langle a, b \mid a^2 = b^3 = 1,\ aba = b^{-1} \rangle$. Δείξαμε ότι οι μονοδιάστατες (ανάγωγες) αναπαραστάσεις είναι η εξής

	e	$(1\,2)$	$(1\,2\,3)$	
ϱ_1	1	1	1	*(τετριμμένη)*
ϱ_2	1	-1	1	*(αναπαράσταση πρόσημο)*

Με πίνακα χαρακτήρων :

$\mathcal{C}(S_3)$	e	$(1,2)$	$(1,2,3)$	*(κλάσεις συζηγίας)*
χ_1	1	1	1	*(τετριμμένη)*
χ_2	1	-1	1	*(αναπαράσταση πρόσημο)*

Για τις n-διάστατες αναπαραστάσεις για $n > 1$: Από το θεώρημα του Maschke ο δακτύλιος $\mathbf{C}S_3$ είναι ημιαπλός και άρα από το θεώρημα Wedderburn-Artin, υπάρχουν φυσικοί $n_i \geq 1$, ώστε $\mathbf{C}S_3 \simeq \mathbf{M}_{n_1}(\mathbf{C}) \times \cdots \times \mathbf{M}_{n_r}(\mathbf{C})$. Έχουμε δείξει ήδη ότι υπάρχουν ακριβώς δύο μονοδιάστατες αναπαραστάσεις, άρα αν υποθέσουμε ότι $n_1 = n_2 = 1$ έχουμε την σχέση

$$6 = \#S_3 = \dim_{\mathbf{C}} \mathbf{C}S_3 = \dim_{\mathbf{C}} \prod_{i=1}^{r} \mathbf{M}_{n_i}(\mathbf{C}) = 2 + \sum_{i=3}^{r} n_i^2$$

Αφού οι μονοδιάστατες αναπαραστάσεις είναι ακριβώς 2, δηλαδή $n_i \geq 2$ για $i = 3, 4, \ldots, r$ βλέπουμε ότι αναγκαστικά $r = 3$ και $n_3 = 2$, δηλαδή τελικά υπάρχουν ακριβώς 3 απλά $\mathbf{C}S_3$-πρότυπα, δύο μονοδιάστατα και ένα δισδιάστατο. Συνεπώς αναζητούμε τώρα μια 2-διάσταση αναπαράσταση $\varrho : S_3 \to GL(V) \simeq GL_2(\mathbf{C})$. Η $S_3 \simeq D_3$ δρα στις κορυφές του ισόπλευρου τριγώνου με στροφή 120^o και ανάκλαση. Απεικονίζουμε την "ανάκλαση" $(1\,2)$ και την "στροφή" $(1\,2\,3)$ στους πίνακες ανάκλασης και στροφής, δηλαδή :

$$\varrho(1\,2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \varrho(1\,2\,3) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

Με χαρακτήρα $\chi_V : S_3 \to \mathbf{C}$, όπου $\chi_V(1\,2) = 0$ και $\chi_V(1\,2\,3) = -1$. Το $\mathbf{C}S_3$-πρότυπο V είναι απλό. Πράγματι, αφού $\mathbf{C}S_3$ ημιαπλός, το V είναι ημιαπλό $\mathbf{C}S_3$-πρότυπο. Αν το V δεν είναι είναι απλό, τότε γράφεται σαν ευθύ άθροισμα των άλλων (μονοδιάστατων) δύο απλών προτύπων, αλλά $\chi_V \neq 2\chi_1,\ \chi_V \neq 2\chi_2,\ \chi_V \neq \chi_1 + \chi_2$, άρα V απλό. Άρα τελικά ο πίνακας χαρακτήρων είναι

$\mathcal{C}(G)$	e	$(1\,2)$	$(1\,2\,3)$
χ_1	1	1	1
χ_2	1	-1	1
χ_V	2	0	-1

Υπάρχει ακόμα ένας τρόπος να δούμε το 2-διαστατό απλό πρότυπο V : Θεωρούμε την δράση της S_3 στον $\mathbf{C}^3 = \mathbf{C}e_1 \oplus \mathbf{C}e_2 \oplus \mathbf{C}e_3$ με $\sigma \cdot e_i = e_{\sigma(i)}$ και επεκτείνουμε γραμμικά. Ο διανυσματικός χώρος $U = \mathbf{C}(e_1 + e_2 + e_3)$ είναι αναλλοίωτος από την παραπάνω δράση και άρα μπορώ να θεώρησω το $\mathbf{C}S_3$-πρότυπο πηλίκο $\mathbf{C}^3/U = \mathbf{C}\bar{e}_1 \oplus \mathbf{C}\bar{e}_2 \oplus \mathbf{C}\bar{e}_3$, όπου $\bar{e}_3 = -\bar{e}_1 - \bar{e}_2$. Παρατηρούμε :

$$(1\,2) \cdot \bar{e}_1 = \bar{e}_2 \qquad (1\,2) \cdot \bar{e}_2 = \bar{e}_1$$

$$(1\,2\,3)\cdot\bar{e}_1=\bar{e}_2 \qquad (1\,2\,3)\cdot\bar{e}_2=\bar{e}_3=-\bar{e}_1-\bar{e}_2$$

Άρα οι πίνακες τον γραμμικών απεικονίσεων $(1\,2),\ (1\,2\,3):\mathbf{C}^3/U\to\mathbf{C}^3/U$ *είναι*

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}\quad\begin{pmatrix}0&-1\\1&-1\end{pmatrix}$$

αντίστοιχα. Δηλαδή $V\simeq\mathbf{C}^3/U$.

(iii) *Ανάγωγες αναπαραστάσεις της* $A_4=\langle(1\,2)(3\,4),\ (1\,2\,3)\rangle\simeq\langle a,b\ :\ a^2=b^3=1,\ (ab)^3=1\rangle$
Δείξαμε ότι οι μονοδιάστατες (ανάγωγες) αναπαραστάσεις είναι

	e	$(1\,2)(3\,4)$	$(1\,2\,3)$
ϱ_1	1	1	1
ϱ_2	1	1	ω
ϱ_3	1	1	ω^2

όπου $\omega=e^{2\pi i/3}$. *Με πίνακα χαρακτήρων*

$\mathcal{C}(G)$	e	$(1\,2)(3\,4)$	$(1\,2\,3)$
χ_1	1	1	1
χ_2	1	1	ω
χ_3	1	1	ω^2

Συνεχίζοντας όπως πριν, μέχρι τώρα γνωρίζουμε ότι $\mathbf{C}A_4=\mathbf{C}\times\mathbf{C}\times\mathbf{C}\times\,?$. *Με λίγο σκέψη, βλέπουμε ότι λείπει μια 3-διάστατη αναπαράσταση. Από το μαγικό μου καπέλο την βγάζω : Θεωρώ* $\mathbf{C}^4=\mathbf{C}e_1\oplus\mathbf{C}e_2\oplus\mathbf{C}e_3\oplus\mathbf{C}e_4$ *με την φυσιολογική δράση της* S_4. *Θεωρώ το* $\mathbf{C}S_4$*-πρότυπο* $U=\mathbf{C}(e_1+e_2+e_3+e_4)$ *και το επαγόμενο πρότυπο πηλίκο* $M=\mathbf{C}^4/U$. *Θεωρώ το* M *ώς* $\mathbf{C}A_4$*-πρότυπο* $(\mathbf{C}A_4\subseteq\mathbf{C}S_4)$ *και είναι* $M=\mathbf{C}\bar{e}_1+\mathbf{C}\bar{e}_2+\mathbf{C}\bar{e}_3+\mathbf{C}\bar{e}_4$. *Τα στοιχεία* $(1\,2)(3\,4)$, $(1\,2\,3)$, $(1\,3\,2)$ *δρουν ως πίνακες :*

$$\begin{pmatrix}0&1&-1\\1&0&-1\\0&0&-1\end{pmatrix}\qquad\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\qquad\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$$

Το $\mathbf{C}A_4$*-πρότυπο* M *είναι απλό. Πράγματι*

	e	$(1\,2)(3\,4)$	$(1\,2\,3)$
χ_M	3	-1	0

και αποκλείεται ο χ_M *να γράφεται σαν άθροισμα των άλλων μονοδιάστατων προτύπων, καθώς* $\chi_M((1\,2)(3\,4))=-1<0<\sum_i n_i\chi_i((1\,2)(3\,4))$ *άρα το* M *είναι απλό.*

(iv) *Ανάγωγες αναπαραστάσεις της* $S_4=\langle(1\,2),\ (1\,2\,3\,4)\rangle$ *:*
Γνωρίζω ότι οι μονοδιάστατες αναπαραστάσεις έιναι οι εξής

	$(1\,2)$	$(1\,2\,3\,4)$
ϱ_1	1	1
ϱ_2	-1	-1

Για τις άλλες ανάγωγες τώρα, θεωρώ την κανονική σειρά $1\trianglelefteq\mathbf{V}\trianglelefteq A_4\trianglelefteq S_4$, *όπου* $\mathbf{V}$[2] *είναι η ομάδα του Klein. παρατηρώ ότι* $S_3\simeq S_4/\mathbf{V}$, *άρα η ανάγωγη 2-διάστατη αναπαράσταση της* S_3 *επάγει μια 2-διάστατη ανάγωγη αναπαράσταση στην* S_4

$$S_4\xrightarrow{\pi}S_4/\mathbf{V}\simeq S_3\xrightarrow{\varrho}GL_2(\mathbf{C})$$

[2] $\mathbf{V}=\{e,(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$

$$e \longmapsto \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad (1\,2) \longmapsto \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \quad (1\,2\,3) \longmapsto \begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$$

Τέλος, το προηγούμενο $\mathbf{C}A_4$-πρότυπο $M = \mathbf{C}^4/U$ είναι απλό και άρα είναι και $\mathbf{C}S_4$-απλό. Συνεπώς, μέχρι τώρα έχουμε των πίνακα χαρακτήρων :

$\mathcal{C}(G)$	e	$(1\,2)$	$(1\,2\,3)$	$(1\,2\,3\,4)$	$(1\,2)(3\,4)$
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1

και παρατηρούμε ότι $\mathbf{C}S_4 \simeq \mathbf{C} \times \mathbf{C} \times \mathbf{M}_2(\mathbf{C}) \times \mathbf{M}_3(\mathbf{C}) \times ?$. Εύκολα, βλέπουμε ότι μας λείπει μια ακόμα 3-διάστατη αναπαράσταση. Στην επόμενη παράγραφο θα την υπολογίσουμε.

4.2.1 Οι πίνακες χαρακτήρων είναι τετραγωνικοί

Ορισμός 4.2.3. *Αν R ένας δακτύλιος, ορίζω την υποομαδά $[R, R] \subseteq R$. ως την υποομάδα του $(R, +)$ που παράγεται από τα στοιχεία $rs - sr$, για $r, s \in R$*

Παρατήρηση. *Η υποομάδα $[\mathbf{C}G, \mathbf{C}G] \subseteq \mathbf{C}G$ είναι ένας $\mathbf{C}$-διανυσματικός υπόχωρος. Ο χαρακτήρας $\chi_V : \mathbf{C}G \to \mathbf{C}$ μηδενίζεται στον $\mathbf{C}$-διανυσματικό υπόχωρο $[\mathbf{C}G, \mathbf{C}G]$ και επάγει μια μοναδική $\mathbf{C}$-γραμμική απεικόνιση $\overline{\chi}_V : {}^{\mathbf{C}G}\big/_{[\mathbf{C}G, \mathbf{C}G]} \to \mathbf{C}$, όπου $\alpha + [\mathbf{C}G, \mathbf{C}G] \xmapsto{\overline{\chi}_V} \chi_V(\alpha)$. Ακόμα, η απεικόνιση πηλίκο $G \to \mathcal{C}(G)$ επάγει μια γραμμική απεικόνιση $F : \mathbf{C}G \longrightarrow \bigoplus_{[g]} \mathbf{C}[g]$ η οποία είναι επί και έχει $\ker F \overset{!}{=} [\mathbf{C}G, \mathbf{C}G]$. Συνεπώς από το πρώτο θεώρημα ισομορφισμών :*

$$\overline{F} : {}^{\mathbf{C}G}\big/_{[\mathbf{C}G, \mathbf{C}G]} \xrightarrow{\ \simeq\ } \bigoplus_{[g] \in \mathcal{C}(G)} \mathbf{C}[g]$$

σαν αποτέλεσμα

$$\dim_{\mathbf{C}} {}^{\mathbf{C}G}\big/_{[\mathbf{C}G, \mathbf{C}G]} = \dim_{\mathbf{C}} \bigoplus_{[g] \in \mathcal{C}(G)} \mathbf{C}[g] = \#\mathcal{C}(G)$$

και έχω το μεταθετικό διάγραμμα

$$\begin{tikzcd}
 & \bigoplus\limits_{[g] \in \mathcal{C}(G)} \mathbf{C}[g] \arrow[dd, bend left=60, "{}''\chi_V{}''"] \\
\mathbf{C}G \arrow[ur, "F"] \arrow[r, "\pi"] \arrow[dr, "\chi_V"'] & {}^{\mathbf{C}G}\big/_{[\mathbf{C}G, \mathbf{C}G]} \arrow[u, "\overline{F}"'] \arrow[d, "\overline{\chi}_V"'] \\
 & \mathbf{C}
\end{tikzcd}$$

Για το γεγονός ότι $\ker F = [\mathbf{C}G, \mathbf{C}G]$[3] *: Έστω $a = \sum \lambda_g g \in \mathbf{C}G$ και $\beta = \sum \mu_h h \in \mathbf{C}G$, τότε*

$$\alpha\beta - \beta\alpha = \sum_{g,h} \lambda_g \mu_h gh - \sum_{g,h} \lambda_g \mu_h hg = \sum_{g,h} \lambda_g \mu_h (gh - hg)$$

[3]Ισχύει ότι η G είναι αβελιανή αν και μόνο αν η F είναι 1-1. Δεν χρειάζεται καν να γνωρίζουμε ότι $\ker F = [\mathbf{C}G, \mathbf{C}G]$, καθώς εύκολα βλέπουμε ότι $\dim_{\mathbf{C}} \ker F = \#G - \#\mathcal{C}(G)$

Συνεπώς, ο μεταθέτης[4] $[G,G]$ *παράγει τον διανυσματικό χώρο* $[\mathbf{C}G,\mathbf{C}G]$ *και παρατηρούμε ότι για* $g,h\in G$ *είναι* $F(gh-hg)=F(gh)-F(hg)=[gh]-[hg]=0$, *δηλαδή* $[\mathbf{C}G,\mathbf{C}G]\subseteq\ker F$. *Για τον αντίστροφο εγκλεισμό, έστω* $\alpha\in\mathbf{C}G$ *με* $F(\alpha)=0$, *τότε*

$$0=F(\alpha)=\sum_{g\in G}a_g[g]=\sum_{[x]\in\mathcal{C}(G)}\sum_{g\in[x]}a_g[g]=\sum_{[x]\in\mathcal{C}(G)}\left(\sum_{g\in[x]}a_g\right)[x]$$

άρα $\alpha\in\ker F$ *αν και μόνο αν* $\sum_{g\in[x]}a_g=0$ *για κάθε* $[x]\in\mathcal{C}(G)$. *Θα δείξουμε τους εγκλεισμούς*

$$\ker F\subseteq\langle g-h:g\sim h\rangle\subseteq[\mathbf{C}G,\mathbf{C}G]$$

και έτσι θα έχουμε τελειώσει. Για τον πρώτο, έστω $\alpha\in\ker F$, *τότε*

$$\alpha=\sum_{g\in G}a_gg=\sum_{[x]\in\mathcal{C}(G)}\sum_{g\in[x]}a_gg=\sum_{[x]\in\mathcal{C}(G)}\sum_{g\in[x]}a_g(g-x)\in\langle g-h:g\sim h\rangle$$

αφού $\sum_{g\in[x]}a_g=0$ *για κάθε* $[x]\in\mathcal{C}(G)$. *Για τον δεύτερο εγκλεισμό, έστω* $g,h\in G$ *με* $g\sim h$, *τότε υπάρχει* $x\in G$ *με* $g=xhx^{-1}$ *και άρα*

$$g-h=xhx^{-1}-h=(x)(hx^{-1})-(hx^{-1})(x)\in[\mathbf{C}G,\mathbf{C}G]$$

Θεώρημα 4.2.1. *Αν* $\#G<\infty$, *με διάσπαση Wedderburn-Artin* $\mathbf{C}G\simeq\prod_{i=1}^r\mathbf{M}_{n_i}(\mathbf{C})$, *τότε* $r=\#\mathcal{C}(G)$

1η Απόδειξη : Αρχικά παρατηρούμε ότι

$$Z(\mathbf{C}G)\simeq Z\left(\prod_{i=1}^r\mathbf{M}_{n_i}(\mathbf{C})\right)\simeq\prod_{i=1}^r Z(\mathbf{M}_{n_i}(\mathbf{C}))\simeq\prod_{i=1}^r\mathbf{C}\cdot I_{n_i}\simeq\mathbf{C}^r$$

και άρα $\dim_{\mathbf{C}}Z(\mathbf{C}G)=r$, οπότε αρκεί να δείξουμε ότι $\dim_{\mathbf{C}}Z(\mathbf{C}G)=\#\mathcal{C}(G)$. Ας παρατηρήσουμε τα στοιχεία του κέντρου, έστω $a=\sum_g a_gg\in Z(\mathbf{C}G)$, άρα για κάθε $x\in G$ $ax=xa$, ισοδύναμα $a=xax^{-1}$. Δηλαδή

$$\sum_{g\in G}a_gg=a=xax^{-1}=\sum_{g\in G}a_g(xgx^{-1})=\sum_{g\in G}a_{x^{-1}gx}g$$

άρα για κάθε $g,x\in G$ $a_{xgx^{-1}}=a_g$, ισοδύναμα αν $g\sim h$, τότε $a_g=a_h$. Συνεπώς

$$a\in Z(\mathbf{C}G)\iff a=\sum_{\bar g\in\mathcal{C}(G)}\left(\sum_{x\in\bar g}a_xx\right)=\sum_{\bar g\in\mathcal{C}(G)}a_g\left(\sum_{x\in\bar g}x\right)$$

άρα τα στοιχεία $\sum_{x\in\bar g}x$ για $\bar g\in\mathcal{C}(G)$ αποτελούν μια βάση του $Z(\mathbf{C}G)$. Άρα $\dim_{\mathbf{C}}Z(\mathbf{C}G)=\#\mathcal{C}(G)$. □

2η Απόδειξη (Καλύτερη). Θα χρησιμοποιήσουμε το εξής λήμμα

Λήμμα 4.2.1. *Ισχύει ότι* $[\mathbf{M}_n(\mathbf{C}),\mathbf{M}_n(\mathbf{C})]=\{A\in\mathbf{M}_n(\mathbf{C}):\mathrm{tr}(A)=0\}$

Απόδειξη λήμματος : Έστω $(E_{i,j})_{i,j=1}^n$ η συνήθης βάση του $\mathbf{M}_n(\mathbf{C})$. Έχω τους εγκλεισμούς

$$\mathrm{span}\{E_{i,j},E_{1,1}-E_{k,k}:i\neq j,k\geq 2\}\subseteq[\mathbf{M}_n(\mathbf{C}),\mathbf{M}_n(\mathbf{C})]\subseteq\{A\in\mathbf{M}_n(\mathbf{C}):\mathrm{tr}(A)=0\}$$

Ο δεύτερος εγκλεισμός είναι προφανής, για τον πρώτο παρατηρώ ότι για κάθε $i\neq j$ είναι $E_{i,i}-E_{j,j}=E_{i,j}E_{j,i}-E_{j,i}E_{i,j}$ και $E_{i,j}=E_{i,m}E_{m,j}-E_{m,j}E_{i,j}$ για κάθε m. Η διάσταση του υπόχωρου των $n\times n$ πινάκων με μηδενικό ίχνος είναι n^2-1 και το πλήθος των γραμμικών ανεξάρτητων στοιχείων στο πρώτο σύνολο είναι επίσης n^2-1. Συνεπώς, έχουμε ισότητα των τριών υπόχωρων[5]. □

[4] Ο $[G,G]$ δεν είναι ο κλασσικός μεταθέτης. Εδώ εννοούμε $[G,G]=\{gh-hg:g,h\in G\}\subseteq\mathbf{C}G$

[5] Μέχρι το τέλος της απόδειξης δεν γνωρίζαμε καν ότι ο μεταθέτης $[\mathbf{M}_n(\mathbf{C}),\mathbf{M}_n(\mathbf{C})]$ είναι υπόχωρος.

Το ίχνος tr : $\mathbf{M}_n(\mathbf{C}) \to \mathbf{C}$ έχει πυρήνα τον υπόχωρο που παράγεται από τα στοιχεία $AB - BA$ για $A, B \in \mathbf{M}_n(\mathbf{C})$, άρα επάγει έναν ισομορφισμό $\mathbf{C}$-διανυσματικών χώρων :

$$\mathbf{M}_n(\mathbf{C})\Big/ [\mathbf{M}_n(\mathbf{C}, \mathbf{M}_n(\mathbf{C})\ ] \simeq \mathbf{C}$$

Επίσης $\mathbf{C}G \simeq \prod_{i=1}^{r} \mathbf{M}_n(\mathbf{C}) \Rightarrow\ [\mathbf{C}G, \mathbf{C}G\ ] \simeq \prod_{i=1}^{r} [\mathbf{M}_n(\mathbf{C}), \mathbf{M}_n(\mathbf{C})\ ]$, οπότε

$$\mathbf{C}G\Big/[\mathbf{C}G, \mathbf{C}G\ ] \simeq \frac{\prod_{i=1}^{r} \mathbf{M}_n(\mathbf{C})}{\prod_{i=1}^{r} [\mathbf{M}_n(\mathbf{C}), \mathbf{M}_n(\mathbf{C})\ ]} \simeq \prod_{i=1}^{r} \mathbf{M}_n(\mathbf{C})\Big/ [\mathbf{M}_n(\mathbf{C}, \mathbf{M}_n(\mathbf{C})\ ] \simeq \prod_{i=1}^{r} \mathbf{C} \simeq \mathbf{C}^r$$

Συνεπώς $\dim_{\mathbf{C}} \mathbf{C}G\Big/[\mathbf{C}G, \mathbf{C}G\ ] = r$ και από προηγούμενη παρατήρηση $\#\mathcal{C}(G) = \dim_{\mathbf{C}} \mathbf{C}G\Big/[\mathbf{C}G, \mathbf{C}G\ ]$. Τελικά $r = \#\mathcal{C}(G)$ $\square$

Πόρισμα 4.2.2. *Οι πίνακες των αναγώγων χαρακτήρων είναι τετραγωνικοί (Το πλήθος των κλάσεων ισομορφίας απλών $\mathbf{C}G$-προτύπων είναι ίσο με το πλήθος των κλάσεων συζηγίας)*

4.2.2 Σχέσεις Ορθογωνιότητας

Παρατήρηση. *Έστω X σύνολο και G ομάδα που δρά στο X. Ο $\mathbf{C}$-διανυσματικός χώρος*

$$\bigoplus_{x \in X} \mathbf{C}x$$

λαμβάνει την δομή ενός $\mathbf{C}G$-προτύπου, με $g \cdot e_x := e_{gx}$ για κάθε $g \in G$ και για κάθε $x \in X$

Παραδείγματα. (i) *Ο διανυσματικός χώρος $\mathbf{C}^n = \bigoplus_{i=1}^{n} \mathbf{C}e_i$ λαμβάνει την δομή ενός $\mathbf{C}S_n$-προτύπου από την φυσιολογική δράση $\sigma \cdot e_i = e_{\sigma(i)}$.*

(ii) *Ο $\mathbf{C}$-διανυσματικός $\mathbf{C}G = \bigoplus_{g \in G} \mathbf{C}g$ λαμβάνει την δομή ενός $\mathbf{C}G$- προτύπου από την φυσιολογική δράση της G στον ευατό της. Η αντιστοίχη αναπαράσταση ονομάζεται η αριστερά κανονική αναπαράσταση.*

Πρόταση 4.2.2. *Έστω X σύνολο και G ομάδα που δρά στο X. Θεωρώ το επαγόμενο $\mathbf{C}G$-πρότυπο $V = \bigoplus_{x \in X} \mathbf{C}x$. Για τον χαρακτήρα $\chi_V : G \to \mathbf{C}$ ισχύει ότι :*

$$\chi_V(g) = \#\mathrm{Fix}(g)$$

για κάθε $g \in G$, όπου $\mathrm{Fix}(g) = \{x \in X\ :\ gx = x\}$.

Απόδειξη : Αναπαριστώ τον πίνακα της γραμμικής απεικόνισης $g : V \to V$ ως προς την διατεταγμένη βάση $(e_x)_{x \in X}$, τότε παρατηρώ :

$$\mathrm{tr}(g) = \text{το πλήθος των 1 στην διαγώνιο} = \#\{x \in X\ :\ gx = x\}$$

$\square$

Πόρισμα 4.2.3. *Αν $\chi_{\mathrm{reg}} : G \to \mathbf{C}$ ο χαρακτήρας την κανονικής αριστερής αναπαράστασης, τότε*

$$\chi_{\mathrm{reg}}(g) = \begin{cases} \#G & g = e \\ 0 & g \neq e \end{cases}$$

Θεώρημα 4.2.2. *Έστω G πεπερασμένη ομάδα και έστω η διάσπαση Wedderburn-Artin του δακτυλίου $\mathbf{C}G \simeq \prod_{i=1}^{r} \mathbf{M}_{n_i}(\mathbf{C})$. Ισχύει ότι $Z(\mathbf{C}G) = \prod_{i=1}^{r} \mathbf{C} \cdot I_{n_i}$ και θέτω $C_{\bar{g}} := \sum_{x \in \bar{g}} x$ για κάθε $\bar{g} \in \mathcal{C}(G)$. Τέλος, θεωρώ τις βάσεις του $\mathbf{C}$-διανυσματικού χώρου $Z(\mathbf{C}G)$*

$$\hat{\mathbf{e}} = \{e_1, e_2, \ldots, e_r\} \qquad \hat{\mathbf{c}} = \{C_{\bar{g}} : \bar{g} \in \mathcal{C}(G)\}$$

όπου $\hat{\mathbf{e}}$ η κανονική βάση του $Z(\mathbf{C}G)$. Τότε ισχύουν τα εξής :

- $e_i = \dfrac{n_i}{\#G} \displaystyle\sum_{g \in G} \chi_i(g^{-1})g$ *για $i = 1, 2, \ldots, r$ όπου χ_i ο χαρακτήρας του i-οστού απλού $\mathbf{C}G$-προτύπου $V_i \simeq \mathbf{C}^{n_i}$ και παρατηρώ ότι* $e_i = \dfrac{n_i}{\#G} \displaystyle\sum_{g \in G} \chi_i(g^{-1})g = \sum_{\bar{g} \in \mathcal{C}(G)} \dfrac{n_i}{\#G} \chi_i(g^{-1}) C_{\bar{g}}$. *Συνεπώς, αν σταθεροποιήσουμε αντιπρόσωπους $g_1, \ldots, g_r$ των κλάσεων συζηγίας, ο πίνακας αλλαγής βάσης είναι*

$$A = (1_{Z(\mathbf{C}G)} : \hat{\mathbf{e}}, \hat{\mathbf{c}}) = \left(\frac{n_i}{\#G} \chi_i(g_j^{-1}) \right)_{1 \leq i,j \leq r}$$

- $C_{\bar{g}} = \displaystyle\sum_{j=1}^{r} \dfrac{\#\bar{g} \cdot \chi_j(g)}{n_j} e_j$ *για κάθε $\bar{g} \in \mathcal{C}(G)$. Συνεπώς, αν σταθεροποιήσουμε αντιπρόσωπους $g_1, \ldots, g_r$ των κλάσεων συζηγίας, ο αντίστροφος πίνακας είναι*

$$A^{-1} = (1_{Z(\mathbf{C}G)} : \hat{\mathbf{c}}, \hat{\mathbf{e}}) = \left(\frac{\#\overline{g_i}}{n_j} \chi_j(g_i) \right)_{1 \leq i,j \leq r}$$

Απόδειξη : Υπάρχουν $\lambda_{i,g} \in \mathbf{C}$, ώστε $e_i = \sum_{g \in G} \lambda_{i,g} g$ και άρα για $x \in G$ είναι $e_i x^{-1} = \sum_{g \in G} \lambda_{i,g} g x^{-1}$. Θεωρώ την κανονική αριστερή αναπαράσταση και υπολογίζω :

$$\chi_{\text{reg}}(e_i x^{-1}) = \sum_{g \in G} \lambda_{i,g} \chi_{\text{reg}}(g x^{-1}) = \lambda_{i,x} \#G$$

Είναι επίσης $\mathbf{C}G = V_1^{n_1} \oplus \cdots \oplus V_r^{n_r}$, όπου V_i τα απλά $\mathbf{C}G$-πρότυπα και άρα $\chi_{\text{reg}} = \sum_{i=1}^{r} n_i \chi_i$. Συνεπώς

$$\lambda_{i,x} \#G = \sum_{i=1}^{r} n_i \chi_i(e_i x^{-1}) = n_i \chi_i(x^{-1}) \Rightarrow \lambda_{i,x} = \frac{n_i \chi_i(x^{-1})}{\#G}$$

Για την άλλη σχέση, υπάρχουν $\mu_{\bar{g},i} \in \mathbf{C}$ ώστε $C_{\bar{g}} = \sum_{i=1}^{r} \mu_{\bar{g},i} e_i$. Υπολογίζω

$$\chi_j(C_{\bar{g}}) = \chi_j \left(\sum_{i=1}^{r} \mu_{\bar{g},i} e_i \right) = \sum_{i=1}^{r} \mu_{\bar{g},i} \chi_j(e_i) = \mu_{\bar{g},j} n_j$$

και ταυτόχρονα

$$\chi_j(C_{\bar{g}}) = \chi_j \left(\sum_{x \in \bar{g}} x \right) = \sum_{x \in \bar{g}} \chi_j(x) = \gamma_g \chi_j(g)$$

άρα τελικά $\mu_{\bar{g},j} = \gamma_g \chi_j(g)/n_j$. □

Πόρισμα 4.2.4 (Σχέσεις Ορθογωνιότητας).

- *(Ορθογωνιότητα γραμμών) Για κάθε* $i, j = 1, 2, \ldots, r$ *είνα* $\sum_{g \in G} \chi_i(g^{-1})\chi_j(g) = \begin{cases} \#G & i = j \\ 0 & i \neq j \end{cases}$
- *(Ορθογωνιότητα στηλών) Για κάθε* $g, h \in G$ *είναι* $\sum_{k=1}^{r} \chi_k(g)\chi_k(h^{-1}) = \begin{cases} \#C_G(g) & g \sim h \\ 0 & g \not\sim h \end{cases}$ *όπου* $C_G(g)$ *η κεντροποιούσα του* $g \in G$

Απόδειξη : Έστω $g_1, \ldots, g_r$ αντιπρόσωποι των κλάσεων συζηγίας. Από το προηγούμενο θεώρημα οι πίνακες

$$A = \left(\frac{n_i}{\#G}\chi_i(g_j^{-1})\right)_{1 \leq i,j \leq r} \qquad B = \left(\frac{\#\overline{g_i}}{n_j}\chi_j(g_i)\right)_{1 \leq i,j \leq r}$$

είναι ο αντίστροφος ένος του άλλου. Θεωρώ τα (i, j)-στοιχεία των πινάκων AB και BA και αφού $AB = BA = I_r$, έχω ότι :

$$(AB)_{i,j} = \sum_{k=1}^{r} \frac{n_i}{\#G}\chi_i(g_k^{-1}) \cdot \frac{\#\overline{g_k}}{n_j}\chi_j(g_k) = \delta_{i,j} \qquad (BA)_{i,j} = \sum_{k=1}^{r} \frac{\#\overline{g_i}}{n_k}\chi_k(g_i) \cdot \frac{n_k}{\#G}\chi_k(g_j^{-1}) = \delta_{i,j}$$

Συνεπώς για την ορθογωνιότητα γραμμών :

$$\delta_{i,j} = \frac{n_i}{n_j \#G} \sum_{k=1}^{r} \#\overline{g_k}\chi_i(g_k^{-1})\chi_j(g_k) = \frac{n_i}{n_j \#G} \sum_{g \in G} \chi_i(g^{-1})\chi_j(g) \Rightarrow$$

$$\sum_{g \in G} \chi_i(g^{-1})\chi_j(g) = \begin{cases} \#G & i = j \\ 0 & i \neq j \end{cases}$$

και για την ορθογωνιότητα στηλών

$$\delta_{i,j} = \sum_{k=1}^{r} \frac{\#\overline{g_i}}{n_k}\chi_k(g_i) \cdot \frac{n_k}{\#G}\chi_k(g_j^{-1}) = \frac{1}{\#C_G(g_i)} \sum_{k=1}^{r} \chi_k(g_i)\chi_k(g_j^{-1}) \Rightarrow$$

$$\sum_{k=1}^{r} \chi_k(g_i)\chi_k(g_j^{-1}) = \begin{cases} \#C_G(g_i) & i = j \\ 0 & i \neq j \end{cases} \iff \sum_{k=1}^{r} \chi_k(g)\chi_k(h^{-1}) = \begin{cases} \#C_G(g) & g \sim h \\ 0 & g \not\sim h \end{cases}$$

□

Παρατήρηση. *Οι (ανάγωγοι) χαρακτήρες διαχωρίζουν τις κλάσεις συζηγίας, δηλαδή* $g \not\sim h$ *αν και μόνο αν υπάρχει κάποιος (ανάγωγος) χαρακτήρας* $\chi : G \to \mathbf{C}$*, τέτοιος ώστε* $\chi(g) \neq \chi(h)$*. Πράγματι, το αντίστροφο είναι προφανές, για το ευθύ : Έστω* $g, h \in G$ *με* $g \not\sim h$*, από την ορθογωνιότητα στηλών γνωρίζω ότι*

$$\sum_{k=1}^{r} \chi_k(g)\overline{\chi_k(h)} = \sum_{k=1}^{r} \chi_k(g)\chi_k(h^{-1}) = 0$$

Έστω, ως προς άτοπο, ότι $\chi(g) = \chi(h)$ *για κάθε χαρακτήρα* $\chi : G \to \mathbf{C}$*, ειδικότερα για τους ανάγωγους χαρακτήρες. Συνεπώς, έχω*

$$\#C_G(g) = \sum_{k=1}^{r} \chi_k(g)\chi_k(g^{-1}) = \sum_{k=1}^{r} \chi_k(g)\overline{\chi_k(g)} = \sum_{k=1}^{r} |\chi_k(g)|^2 = \sum_{k=1}^{r} \chi_k(g)\overline{\chi_k(h)} = 0$$

Το οποίο είναι προφανές άτοπο.

4.2.3 Συναρτήσεις Κλάσεων

Ορισμός 4.2.4. *Θεωρώ το σύνολο των συναρτήσεων κλάσεων της G*

$$c\ell(G) := \{\varphi : G \to \mathbf{C} : \varphi(g) = \varphi(h) \text{ για κάθε } g, h \in G \text{ με } g \sim h\}$$

$$\equiv \{\varphi : \mathcal{C}(G) \to \mathbf{C} : \varphi \text{ απεικόνιση}\}$$

Ο $c\ell(G)$ αποτελεί $\mathbf{C}$-διανυσματικός χώρος και τον εφοδιάζω με ένα εσωτερικό γινόμενο : Για κάθε $\varphi, \psi \in c\ell(G)$ ορίζω

$$\langle \varphi, \psi \rangle := \frac{1}{\#G} \sum_{g \in G} \varphi(g)\overline{\psi(g)}$$

Πόρισμα 4.2.5. *Αν $\chi_1, \ldots, \chi_r \in c\ell(G)$ οι ανάγωγοι χαρακτήρες, τότε ισχύει ότι $\langle \chi_i, \chi_j \rangle = \delta_{i,j}$ για $i, j = 1, 2, \ldots, r$*

Απόδειξη : Από την σχέσεις ορθογωνιότητας γραμμών. □

Πρόταση 4.2.3. *Οι ανάγωγοι χαρακτήρες $\chi_1, \ldots \chi_r \in c\ell(G)$ αποτελούν μια ορθοκανονική βάση του $\mathbf{C}$-διανυσματικού χώρου $c\ell(G)$.*

Απόδειξη: Το σύνολο των ανάγωγων χαρακτήρων αποτελεί γραμμικά ανεξάρτητο σύνολο σαν ορθοκανονικό. Μένει να δείξουμε ότι $\dim_{\mathbf{C}} c\ell(G) = \#\mathcal{C}(G) = r$. Πράγματι, αν σταθεροποιήσουμε αντιπροσώπους $g_1, \ldots, g_r$ των κλάσεων συζηγίας, τα στοιχεία $\delta_1, \ldots, \delta_r \in c\ell(G)$ με

$$\delta_i(h) = \begin{cases} 1 & h \sim g_i \\ 0 & h \not\sim g_i \end{cases}$$

για κάθε $h \in G$, είναι εύκολο να δειχθεί ότι αποτελούν βάση. □

Πόρισμα 4.2.6. *Έστω V ένα $\mathbf{C}G$-πρότυπο με $\dim_{\mathbf{C}} V < \infty$. Το V είναι απλό αν και μόνο αν $\langle \chi_V, \chi_V \rangle = 1$.*

Απόδειξη : Έστω $V_1, \ldots, V_r$ τα απλά $\mathbf{C}G$-πρότυπο, τότε :

($\Rightarrow$) Αν $V \simeq V_i$ για κάποιο $i = 1, 2, \ldots, r$, τότε $\chi_V = \chi_i$ και άρα $\langle \chi_V, \chi_V \rangle = 1$

($\Leftarrow$) Γράφω $V = V_1^{a_1} \oplus V_2^{a_2} \oplus \cdots \oplus V_r^{a_r}$ για κάποια $a_1, \ldots, a_r \in \mathbf{N}$ και έχω ότι $\chi_V = \sum_{i=1}^r a_i \chi_i$, καθώς $\langle \chi_i, \chi_j \rangle = \delta_{i,j}$ είναι εύκολο να δούμε ότι

$$1 = \langle \chi_V, \chi_V \rangle = \sum_{i=1}^r a_i^2$$

Συνεπώς υπάρχει ένα $m \in \{1, 2, \ldots, n\}$ ώστε $a_m = 1$ και $a_i = 0$ για κάθε $i \neq m$, άρα $V \simeq V_m$. □

Πρόταση 4.2.4. *Έστω G πεπερασμένη ομάδα, με απλά $\mathbf{C}G$-πρότυπα $V_1, \ldots, V_r$ με αντίστοιχους χαρακτήρες $\chi_1, \ldots, \chi_r$. Σταθεροποιώ δύο $\mathbf{C}G$-πρότυπα U, W, τότε :*

(i) *$U \simeq W$ αν και μόνο αν $\chi_U(g) = \chi_W(g)$ για κάθε $g \in G$.*

(ii) *Ισχύει $\langle \chi_U, \chi_W \rangle = \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(U, V)$. Συνεπώς, υπάρχουν μη μηδενικές $\mathbf{C}G$-γραμμικές απεικονίσεις $U \to W$ αν και μόνο αν $\langle \chi_U, \chi_W \rangle \neq 0$.*

(iii) *Έστω $\varphi \in c\ell(G)$. Η φ είναι χαρακτήρας αν και μόνο αν $\langle \varphi, \chi_i \rangle \in \mathbf{Z}_{\geq 0}$ για κάθε $i = 1, 2, \ldots, r$*

Απόδειξη : (i) Γνωρίζουμε ότι υπάρχουν θετικοί ακέραιοι $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r$ τέτοιοι ώστε $U \simeq \bigoplus_{i=1}^r V_i^{\alpha_i}$ και $W \simeq \bigoplus_{i=1}^r V_i^{\beta_i}$. Συνεπώς, $\chi_U = \sum_{i=1}^r \alpha_i \chi_i$ και $\chi_W = \sum_{i=1}^r \beta_i \chi_i$. Αν $\chi_U = \chi_W$, τότε για κάθε $j = 1, 2, \dots, r$ είναι $\langle \chi_j, \chi_U \rangle = \langle \chi_j, \chi_W \rangle \iff a_j = b_j$ και άρα $U \simeq W$. Για την αντίστροφη, κατεύθυνση έστω $f : U \to W$ ένας $\mathbf{C}G$-ισομορφισμός, τότε $g|_W = f \circ g|_U \circ f^{-1}$, δηλαδή οι γραμμικές απεικονίσεις $g|_W$ και $g|_U$ είναι όμοιες, έπεται ότι έχουν το ίδιο ίχνος, δηλαδή $\chi_U(g) = \chi_W(g)$

(ii) Έχουμε δείξει στην Πρόταση 4.1.2. ότι $\mathrm{End}_{\mathbf{C}G} V \simeq \mathbf{C}$ για κάθε απλό $\mathbf{C}G$-πρότυπο, ειδικότερα $\dim_{\mathbf{C}} \mathrm{End}_{\mathbf{C}G} V = 1$ για κάθε απλό $\mathbf{C}G$-πρότυπο. Επίσης, από το λήμμα του Schur, για κάθε δύο V, V' μη ισόμορφα απλά $\mathbf{C}G$-πρότυπα είναι $\mathrm{Hom}_{\mathbf{C}G}(V, V') = 0$. Ακόμα, το $\mathrm{Hom}_{\mathbf{C}G}(V_i^{\alpha_i}, V_j^{\beta_j})$ είναι το ευθύ άθροισμα $\alpha_i\beta_j$ το πλήθος αντιτύπων του $\mathrm{Hom}_{\mathbf{C}G}(V_i, V_j)$, Συνεπώς,

$$\mathrm{Hom}_{\mathbf{C}G}(V_i^{\alpha_i}, V_j^{\beta_j}) = \begin{cases} \mathrm{End}_{\mathbf{C}G}(V_i)^{\alpha_i\beta_i} & i = j \\ 0 & i \neq j \end{cases}$$

Τελικά, αν U, W δύο $\mathbf{C}G$-πρότυπα, υπάρχουν μη αρνητικοί ακέραιοι $\alpha_1, \dots, \alpha_r$ και $\beta_1, \dots, \beta_r$, τέτοιοι ώστε $U \simeq \bigoplus_{i=1}^r V_i^{\alpha_i}$ και $W \simeq \bigoplus_{j=1}^r V_j^{\beta_j}$. Υπολογίζω :

$$\mathrm{Hom}_{\mathbf{C}G}(U, W) = \mathrm{Hom}_{\mathbf{C}G}\left(\bigoplus_{i=1}^r V_i^{a_i}, \bigoplus_{j=1}^r V_j^{\beta_j}\right) = \bigoplus_{i,j=1}^r \mathrm{Hom}_{\mathbf{C}G}(V_i^{\alpha_i}, V_j^{\beta_j}) = \bigoplus_{k=1}^r \mathrm{End}_{\mathbf{C}G}(V_k)^{\alpha_k\beta_k}$$

$$\Rightarrow \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(U, W) = \sum_{k=1}^r \dim_{\mathbf{C}} \mathrm{End}_{\mathbf{C}G}(V_k)^{\alpha_k\beta_k} = \sum_{k=1}^r \alpha_\kappa\beta_\kappa \cdot \dim_{\mathbf{C}} \mathrm{End}_{\mathbf{C}G}(V_k) = \sum_{k=1}^r \alpha_\kappa\beta_\kappa$$
$$= \langle \chi_U, \chi_W \rangle$$

(iii) Για το ευθύ : Έστω ότι η $\varphi \in c\ell(G)$ είναι χαρακτήρας, δηλαδή υπάρχει ένα $\mathbf{C}G$-πρότυπο U με $\varphi = \chi_U$. Γνωρίζουμε, ότι υπάρχουν μη αρνητικοί ακέραιοι $\alpha_1, \dots, \alpha_r$ με $U \simeq \bigoplus_{i=1}^r V_i^{\alpha_i}$, συνεπώς $\varphi = \sum_{i=1}^r \alpha_i\chi_i$. Είναι άμεσο ότι $\langle \varphi, \chi_i \rangle = \alpha_i \in \mathbf{Z}_{\geq 0}$. Αντίστροφα, έστω $\varphi \in c\ell(G)$, τέτοια ώστε $\langle \varphi, \chi_i \rangle \in \mathbf{Z}_{\geq 0}$ για κάθε $i = 1, 2, \dots, r$. Θέτω $\alpha_i := \langle \varphi, \chi_i \rangle$ και θεωρώ το $\mathbf{C}G$-πρότυπο $U = \bigoplus_{i=1}^r V_i^{\alpha_i}$, τότε είναι προφανώς $\varphi = \chi_U$. □

Πρόταση 4.2.5. *Έστω U, V δύο $\mathbf{C}G$-πρότυπα, τότε το τανυστικό γινόμενο $U \otimes_{\mathbf{C}} V$ λαμβάνει την δομή $\mathbf{C}G$-προτύπου με την δράση της G να είναι :*

$$g \cdot (u \otimes v) = (gu) \otimes (gv)$$

δηλαδή οι γραμμικές απεικονίσεις $g|_U : U \to U$ και $g|_V : V \to V$, επάγουν την $g|_U \otimes g|_W : U \otimes_{\mathbf{C}} V \to U \otimes_{\mathbf{C}} V$. Συνεπώς, αν $\chi_U, \chi_V : G \to \mathbf{C}$ οι αντίστοιχοι χαρακτήρες, τότε για τον χαρακτήρα του τανυστικού γινομένου, ισχύει

$$\chi_{U \otimes_{\mathbf{C}} V}(g) = \mathrm{tr}(U \otimes_{\mathbf{C}} V \overset{g\otimes g}{\to} U \otimes_{\mathbf{C}} V) = \mathrm{tr}(U \overset{g|_U}{\to} U) \cdot \mathrm{tr}(V \overset{g|_V}{\to} V) = \chi_U(g) \cdot \chi_V(g)$$

Πρόταση 4.2.6. *Έστω ένα μονοδιάστατο $\mathbf{C}G$-πρότυπο U. Τότε ένα $\mathbf{C}G$-πρότυπο V είναι ανάγωγο αν και μόνο αν το $\mathbf{C}G$-πρότυπο $U \otimes_{\mathbf{C}} V$ είναι ανάγωγο*

Απόδειξη : Αφού το U είναι μονοδιάστατο, έχω $|\chi_U(g)| = 1$ για κάθε $g \in G$. Αν θέσω $W = U \otimes_{\mathbf{C}} V$, τότε

$$\langle \chi_W, \chi_W \rangle = \frac{1}{\#G} \sum_{g \in G} |\chi_W(g)|^2 = \frac{1}{\#G} \sum_{g \in G} |\chi_U(g)|^2 \cdot |\chi_V(g)|^2 = \frac{1}{\#G} \sum_{g \in G} |\chi_V(g)|^2 = \langle \chi_V, \chi_V \rangle$$

Συνεπώς, το V είναι ανάγωγο αν και μόνο αν $\langle \chi_V, \chi_V \rangle = 1$ αν και μόνο αν $\langle \chi_W, \chi_W \rangle = 1$ αν και μόνο αν το W είναι ανάγωγο. □

Εφαρμογές. *(i) Θέλω να περιγράψω τον ισομορφισμό* $\mathbf{C}G \xrightarrow{\simeq} \prod_{i=1}^r \mathbf{M}_{n_i}(\mathbf{C})$ *. Αν κάποιος ακολουθήσει την απόδειξη του θεώρηματος Wedderburn-Artin, βλέπουμε ότι για έναν ημιαπλό δακτύλιο* R*, ο ισομορφισμός είναι η εξής σύνθεση*

$$R^{op} \xrightarrow{\simeq} \mathrm{End}_R R \xrightarrow{\simeq} \bigoplus_{i=1}^r \mathrm{End}_R V_i^{n_i} \xrightarrow{\simeq} \bigoplus_{i=1}^r \mathbf{M}_{n_i}(\mathrm{End}_R V_i)$$

$$r \longmapsto (f_r : R \to R) \longmapsto (f_r : V_i^{n_i} \to V_i^{n_i}) \longmapsto (p_k \circ f_r \circ v_\ell : V_i \to V_i)_{\substack{1\le \ell\le n_i \\ 1\le k\le n_i}}$$

όπου f_r *ο (δεξιός) πολλαπλασιασμός με* r*. Συνεπώς, κάθε* $g \in \mathbf{C}G$ *αντιστοιχεί στην* r*-αδα πινάκων, όπου ο* i*-πίνακας είναι ο πίνακας της δράσης του* g *στο αντίστοιχο απλό* $\mathbf{C}G$*-πρότυπο* V_i*. Με λίγα λόγια, ο πίνακας της* i*-ανάγωγης αναπαράστασης. Για παράδειγμα, θεωρώ τον δακτύλιο* $\mathbf{C}S_3$ *και γνωρίζω ότι* $\mathbf{C}S_3 \xrightarrow{\simeq} \mathbf{C}\times\mathbf{C}\times\mathbf{M}_2(\mathbf{C})$*. Τα στοιχεία* $(1\ 2), (1\ 2\ 3) \in S_3$ *παράγουν την ομάδα* S_3 *και μέσω του ισομορφισμού αντιστοιχούν σε*

$$(1\ 2) \longmapsto \left(1, -1, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right) \qquad (1\ 2\ 3) \longmapsto \left(1, 1, \begin{pmatrix} \cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix}\right)$$

Η πρώτη συντεταγμένη αντιστοιχεί στην τετριμμένη αναπαράσταση, η δεύτερη στην πρόσημο και η τρίτη στην δισδιάστατη.

(ii) Θεωρώ πάλι τον ισομορφισμό $\mathbf{C}G \xrightarrow{\simeq} \prod_{i=1}^r \mathbf{M}_{n_i}(\mathbf{C})$*. Πως θα εκφράσω μια τυχαία* r*-αδα* $\sum_{i=1}^r a_i e_i \in Z(\mathbf{C}G)$ *στην μορφή* $\sum_g a_g g$*; Αρκεί να εκφράσω τα στοιχεια της κανονικής βάσης του* $Z(\mathbf{C}G)$*. Για παράδειγμά, θεωρώ τον δακτύλιο* $\mathbf{C}S_3$*, γνωρίζω ότι ο πίνακας χαρακτήρων της* S_3 *είναι*

$\mathcal{C}(G)$	e	$(1\ 2)$	$(1\ 2\ 3)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

και ισχύει η ισότητα $e_i = n_i/\#S_3 \sum_{\sigma\in S_3} \chi_i(\sigma^{-1})\sigma$*. Συνεπώς*

$$e_1 = \frac{1}{6}(e + (1\ 2) + (1\ 3) + (2\ 3) + (1\ 2\ 3) + (1\ 3\ 2))$$

$$e_2 = \frac{1}{6}(e - (1\ 2) - (1\ 3) - (2\ 3) + (1\ 2\ 3) + (1\ 3\ 2))$$

$$e_3 = \frac{2}{6}(2\cdot e - (1\ 2\ 3) - (1\ 3\ 2))$$

(iii) Θεωρώ την συμμετρική ομάδα S_5 *να δρα στα διανύσματα* $e_1, e_2, \ldots, e_5$ *του* $\mathbf{C}^5 = \bigoplus_{i=1}^5 \mathbf{C}e_i$ *και τον αναλλοίωτο υπόχωρο* $U = \langle(1,1,1,1,1)\rangle \subseteq \mathbf{C}^5$*. Τότε το* $\mathbf{C}S_5$*-πρότυπο πηλίκο* $V = \mathbf{C}^5/U$ *είναι απλό. Πράγματι, γράφω* $V = \sum_{i=1}^5 \mathbf{C}\bar{e}_i = \mathbf{C}\bar{e}_1 \oplus \mathbf{C}\bar{e}_2 \oplus \mathbf{C}\bar{e}_3 \oplus \mathbf{C}\bar{e}_4$ *(*$\bar{e}_5 = -\bar{e}_1 - \bar{e}_2 - \bar{e}_3 - \bar{e}_4$*). Υπολογίζω τον χαρακτήρα* $\chi_V : S_5 \to \mathbf{C}$*.*

$\mathcal{C}(S_5)$	1	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2\ 3\ 4)$	$(1\ 2\ 3\ 4\ 5)$	$(1\ 2)(3\ 4)$	$(1\ 2)(3\ 4\ 5)$
#	1	10	20	30	24	15	20
χ_V	4	2	1	0	-1	0	-1
χ_V^2	16	4	1	0	1	0	1

αφού

$$(1\ 2) \longmapsto \begin{pmatrix} 0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}, \quad (1\ 2\ 3) \longmapsto \begin{pmatrix} 0&0&1&0\\1&0&0&0\\0&1&0&0\\0&0&0&1 \end{pmatrix}, \quad (1\ 2\ 3\ 4) \longmapsto \begin{pmatrix} 0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0 \end{pmatrix}$$

$$(1\,2\,3\,4\,5) \longmapsto \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \quad (1\,2)(3\,4) \longmapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (1\,2)(3\,4\,5) \longmapsto \begin{pmatrix} 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Συνεπώς, υπολογίζουμε

$$\langle \chi_V, \chi_V \rangle = \frac{1}{\#S_5} \sum_{\sigma \in S_5} \chi_V(\sigma)\chi_V(\sigma^{-1}) = \frac{1}{120} \sum_{\sigma \in S_5} |\chi_V(\sigma)|^2 =$$

$$= \frac{1}{120}(1 \cdot 16 + 10 \cdot 4 + 20 \cdot 1 + 30 \cdot 0 + 24 \cdot 1 + 15 \cdot 0 + 20 \cdot 1) = 1$$

(vi) *Έστω i, j, k σύμβολα, που διέπονται από τις σχέσεις*

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

$$ij = k, \ jk = i, \ ki = j$$

Εύκολα δείχουμε ότι το σύνολο $\mathcal{Q} = \{1, -1, i, -i, j, -j, k, -k\}$ αποτελεί μη αβελιανή ομάδα τάξης 8. Η ομάδα $\mathcal{Q}$ λέγεται η ομάδα των quaternions. Υπολογίζουμε, τον πίνακα χαρακτήρων της $\mathcal{Q}$: Θεωρώ την αβελιανοποίηση $\mathcal{Q}_{ab}$ και έστω $\mathbf{1}, I, J, K$ τα αντίστοιχα στοιχεία στο πηλίκο. Έχουμε ότι $-K = JI = IJ = K$ και ανάλογα $\mathbf{1} = -\mathbf{1}, I = -I, \ J = -J$. Τελικά, έχω $\mathcal{Q}_{ab} = \{\mathbf{1}, I, J, K\}$ και καθώς υπάρχουν μόνο δύο κλάσεις ισομορφίας αβελιανών ομάδων τάξης 4 και οι $\mathcal{Q}_{ab}$ δεν έχει στοιχείο τάξης 4 είναι $\mathcal{Q}_{ab} \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$. Οι μονοδιάστατες αναπαραστάσεις είναι

$\mathcal{C}(\mathcal{Q})$	1	-1	i	j	k
$\#$	1	1	2	2	2
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1

Παρατηρούμε, ότι λείπει μια 2-διάστατη αναπαράσταση. Η $\mathcal{Q}$ δρα στον $\mathbf{C}^2$ με

$$i \longmapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ j \longmapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \ k \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

όπου ο i μέσα στους πίνακες είναι η φανταστική μονάδα. Το $\mathbf{C}\mathcal{Q}$-πρότυπο $V_5 = \mathbf{C}^2$ είναι ανάγωγο. Πράγματι

$$\langle \chi_5, \chi_5 \rangle = \frac{1}{\#\mathcal{Q}} \sum_{g \in \mathcal{Q}} |\chi_W(g)|^2 = \frac{1 \cdot 2^2 + 1 \cdot (-2)^2 + 2 \cdot 0^2 + 2 \cdot 0^2 + 2 \cdot 0^2}{8} = 1$$

και άρα ο πίνακας χαρακτήρων είναι

$\mathcal{C}(\mathcal{Q})$	1	-1	i	j	k
$\#$	1	1	2	2	2
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

(v) *Χρώσταμε, να συμπληρώσουμε τον πίνακα χαρακτήρων της S_4. Μέχρι τώρα έχουμε δείξει ότι*

$\mathcal{C}(G)$	e	$(1\,2)$	$(1\,2\,3)$	$(1\,2\,3\,4)$	$(1\,2)(3\,4)$
χ_1	1	1	1	1	1
χ_{sign}	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-2	-1

και γνωρίζουμε ότι $\mathbf{C}S_4 \simeq \mathbf{C} \times \mathbf{C} \times \mathbf{M}_2(\mathbf{C}) \times \mathbf{M}_3(\mathbf{C}) \times \mathbf{M}_3(\mathbf{C})$, *δηλαδή λείπει μια 3-διάστατη ανάγωγη αναπαράσταση. Θεωρούμε το τανυστικό γινόμενο* $V^{sign} \otimes_{\mathbf{C}} V_3$, *όπου* V^{sign} *το πρότυπο της αναπαράστασης πρόσημο και* V_3 *το 3-διάστατο ανάγωγο πρότυπο που έχουμε βρει. Αφού το* $\mathbf{C}G$*-πρότυπο* V^{sign} *είναι μονοδιάστατο και το* V_3 *απλό, το τανυστικό γινόμενο είναι επίσης απλό και παρατηρούμε ότι* $\chi_{sign} \otimes \chi_4 = \chi_{sign} \cdot \chi_4 \neq \chi_4$ *και άρα τα πρότυπα δεν είναι ισόμορφα. Τελικά, ο πίνακας χαρακτήρων είναι*

$\mathcal{C}(G)$	e	$(1\,2)$	$(1\,2\,3)$	$(1\,2\,3\,4)$	$(1\,2)(3\,4)$
χ_1	1	1	1	1	1
χ_{sign}	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
$\chi_{sign} \otimes \chi_4$	3	-1	0	2	-1

(iv) *Υπάρχουν μη ισόμορφες ομάδες, με ίδιους πίνακες χαρακτήρων. Έστω η ομάδα* $D_4 = \langle r, s : r^4 = 1, s^2 = 1, srs = r^{-1} \rangle$ *συμμετριών του τετραγώνου. Θεωρούμε το* $\mathbf{C}G$*-πρότυπο* $U = \mathbf{C}^2$ *με τα* r, s *να δρουν*

$$r \longmapsto \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix} \quad s \longmapsto \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{pmatrix}$$

όπου $\vartheta = \pi/2$. *Θα δείξουμε ότι το* $\mathbf{C}G$*-πρότυπο* U *είναι ανάγωγο. Πράγματι, αρκεί* $\langle \chi_U, \chi_U \rangle = 1$. *Με λίγο σκέψη, οι κλάσεις συζηγίας της* D_4 *είναι οι*

$$\mathcal{C}_1 = \{1\} \;\; \mathcal{C}_2 = \{s, sr^2\} \;\; \mathcal{C}_3 = \{sr, sr^3\} \;\; \mathcal{C}_4 = \{r, r^3\} \;\; \mathcal{C}_5 = \{r^2\}$$

και άρα ο πίνακας χαρακτήρων είναι ο εξής

$\mathcal{C}(D_5)$	1	r^2	r	s	sr
#	1	1	2	2	2
χ_U	2	-2	0	0	0
χ_U^2	4	4	0	0	0

άρα

$$\langle \chi_U, \chi_U \rangle = \frac{1}{\#D_4} \sum_{g \in D_5} |\chi_U(g)|^2 = \frac{1 \cdot 4 + 1 \cdot 4 + 2 \cdot 0 + 2 \cdot 0 + 2 \cdot 0}{8} = 1$$

Για τις μονοδιάστατες αναπαραστάσεις, έχουμε ότι $(D_4)_{ab} = \langle R, S : R^2 = S^2 = 1, RS = SR \rangle \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$, *άρα τελικά ο πίνακας χαρακτήρων είναι*

$\mathcal{C}(D_5)$	1	r^2	r	s	sr
#	1	1	2	2	2
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_U	2	-2	0	0	0

παρατηρούμε ότι οι ομάδες $D_4, \mathcal{Q}$ *έχουν τον ίδιο πίνακα χαρακτήρων, αλλά δεν είναι ισόμορφες.*

Πρόταση 4.2.7. *Έστω G πεπερασμένη ομάδα, V ένα $\mathbf{C}G$-πρότυπο με χαρακτήρα $\chi_V : G \to \mathbf{C}$. Ορίζω τον πυρήνα του χαρακτήρα να είναι*

$$\ker \chi_V := \ker(G \xrightarrow{\varrho_V} \mathrm{GL}(V)) = \{g \in G : g = 1_V : V \to V\}$$

Τότε ισχύουν τα εξής :

(*i*) $|\chi_V(g)| \leq \chi_V(1)$ *για κάθε* $g \in G$

(*ii*) $\ker \chi_V = \{g \in G : \chi_V(g) = \chi_V(1)\}$

(*iii*) *Αν* $\vartheta = \sum_{i=1}^{\ell} m_i \chi_i$ *για κάποιος χαρακτήρες* $\chi_1, \dots, \chi_\ell$ *και μη αρνητικούς ακέραιους* $m_1, \dots, m_\ell$, *τότε*

$$\ker \vartheta = \bigcap_{i=1}^{\ell} \ker \chi_i$$

(*iv*) *Αν N μια κανονική υποομάδα της G, τότε υπάρχουν ανάγωγοι χαρακτήρες $\chi_1, \dots, \chi_r$, τέτοιοι ώστε*

$$N = \bigcap_{i=1}^{r} \ker \chi_i$$

Απόδειξη : (*i*) Έστω $g \in G$, αφού η G είναι πεπερασμένη, υπάρχει n τέτοιο ώστε $g^n = 1_V : V \to V$. Αν $m = \chi_V(1) = \dim_{\mathbf{C}} V$, τότε η $g : V \to V$ έχει m ιδιοτιμές $\lambda_1, \dots, \lambda_m \in \mathbf{C}$ οι οποίες ικανοποιούν $\lambda_i^n = 1$ για κάθε $i = 1, 2, \dots, m$, είναι δηλαδή ρίζες της μονάδος. Συνεπώς

$$|\chi_V(g)| = |\lambda_1 + \dots + \lambda_m| \leq |\lambda_1| + \dots + |\lambda_m| = \chi_V(1)$$

(*ii*) Ο εγκλεισμός $\ker \chi_V \subseteq \{g \in G : \chi_V(g) = \chi_V(1)\}$ είναι προφανής. Για τον αντίστροφο, έστω $g \in G$, τέτοιο ώστε $\chi_V(g) = \chi_V(1)$, τότε

$$\chi_V(1) = |\chi_V(1)| = |\chi_V(g)| = |\lambda_1 + \dots + \lambda_m| \leq |\lambda_1| + \dots + |\lambda_m| = \chi_V(1)$$

και άρα υπάρχει ισότητα στην τριγωνική ανισότητα, έπεται ότι οι μιγαδικοί αριθμοί $\lambda_1, \dots, \lambda_m$ είναι συνευθειακοί και αφού ανήκουν στον κύκλο είναι και ίσοι. Ο ενδομορφισμός $g : V \to V$ είναι διαγωνισιμός, καθώς το ελαχιστό πολυώνυμο του διαιρεί το $X^n - 1 \in \mathbf{C}[X]$ και άρα είναι γινόμενο πρωτοβαθμίων. Σαν διαγωνίσιμος, το ευθύ άθροισμα των ιδιοχώρων του είναι ο V και άφου έχει μια μοναδική ιδιοτιμή $\lambda \in \mathbf{C}$, έχουμε ότι $g = \lambda \cdot 1_V : V \to V$. Τέλος, από την ισότητα $\chi_V(g) = \chi_V(1) \Rightarrow \lambda \cdot \dim_{\mathbf{C}} V = \dim_{\mathbf{C}} V \Rightarrow \lambda = 1$, άρα τελικά $g \in \ker \chi_V$.

(*iii*) Ο εγκλεισμός $\bigcap_{i=1}^{\ell} \ker \chi_i \subseteq \ker \vartheta$ είναι προφανής. Για τον αντίστροφο, έστω $g \in \ker \vartheta$ και έστω ως προς άτοπο ότι υπάρχει $j = 1, 2, \dots, \ell$, τέτοιο ώστε $g \notin \ker \chi_j$, ισοδύναμα $|\chi_j(g)| < \chi_j(1)$. Τότε

$$\vartheta(1) = |\vartheta(1)| = |\vartheta(g)| = \left| \sum_{i=1}^{\ell} m_i \chi_i(g) \right| \leq \sum_{i=1}^{\ell} m_i |\chi_i(g)| < \sum_{i=1}^{\ell} m_i \chi_i(1) = \vartheta(1) \ \#$$

Το οποίο είναι άτοπο.

(*iv*) Θεωρώ το κανονικό $\mathbf{C}(G/N)$-πρότυπο $\mathbf{C}(G/N)$, τότε η απεικόνιση πηλίκο $G \xrightarrow{\pi} G/N$ επάγει την δομή $\mathbf{C}G$-προτύπου στο $\mathbf{C}(G/N)$.

$$\mathbf{C}G \xrightarrow{\overline{\pi}} \mathbf{C}(G/N) \xhookrightarrow{\ell_{reg}} \mathrm{End}_{\mathbf{Z}}(\mathbf{C}(G/N), +)$$

$$\textstyle\sum_g \lambda_g g \longmapsto \sum_g \lambda_g (gN) \longmapsto \Big(\alpha \longmapsto \sum_g \lambda_g (gN) \cdot a\Big)$$

Το κανονικό $\mathbf{C}(G/N)$-πρότυπο είναι πιστό, αν $\alpha \in \mathbf{C}(G/N)$ τέτοιο ώστε $\alpha \cdot x = 0$ για κάθε $x \in \mathbf{C}(G/N)$, τότε $\alpha = \alpha \cdot 1 = 0$. Ο χαρακτήρας $\chi : \mathbf{C}G \to \mathbf{C}$ του $\mathbf{C}G$-προτύπου $\mathbf{C}(G/N)$ έχει πύρηνα την κανονική υποομάδα N. Πράγματι, αφού η ℓ_{reg} είναι 1-1, έχω ότι

$$\ker \chi = \ker \ell_{reg} \circ \overline{\pi}\big|_G = \ker \overline{\pi}\big|_G = N$$

και αν θεωρήσω την διάσπαση του στους ανάγωγους χαρακτήρες $\chi = \sum_{i=1}^r n_i \chi_i$, τότε από το (iii) παίρνω

$$N = \ker \chi = \bigcap_{i=1}^{r} \ker \chi_i$$

□

Θεώρημα 4.2.3 (Λήμμα του Burnside). *Έστω G μια πεπερασμένη ομάδα και X ένα σύνολο στο οποίο δρα. Αν N το πλήθος των τροχιών του X, τότε*

$$N = \frac{1}{\#G} \sum_{g \in G} \#\mathrm{Fix}(g)$$

Απόδειξη : Θεωρώ το $\mathbf{C}G$-πρότυπο $V = \bigoplus_{x \in X} \mathbf{C}x$. Έστω, $\mathcal{O}(x_1), \dots, \mathcal{O}(x_N)$ οι τροχιές της δράσης και γνωρίζω ότι ο χαρακτήρας του $\mathbf{C}G$-προτύπου V είναι $\chi_V(g) = \mathrm{Fix}(g)$ για κάθε $g \in G$, άρα

$$\frac{1}{\#G} \sum_{g \in G} \#\mathrm{Fix}(g) = \frac{1}{\#G} \sum_{g \in G} \chi_V(g)\chi_1(g^{-1}) = \langle \chi_V, \chi_1 \rangle = \dim_{\mathbf{C}} \mathrm{Hom}_{\mathbf{C}G}(V, \mathbf{C})$$

όπου $\mathbf{C}$ το τετριμμένο $\mathbf{C}G$-πρότυπο με χαρακτήρα $\chi_1 : G \to \mathbf{C}$. Συνεπώς, αρκεί να υπολογίζω την διάσταση του υπόχωρου $\mathrm{Hom}_{\mathbf{C}G}(V, \mathbf{C})$. Θα δείξω ότι οι $\mathbf{C}G$-γραμμικές απεικονίσεις $\delta_i : V \to \mathbf{C}$ με

$$\delta_i(x) = \begin{cases} 1 & x \in \mathcal{O}(x_i) \\ 0 & x \notin \mathcal{O}(x_i) \end{cases}$$

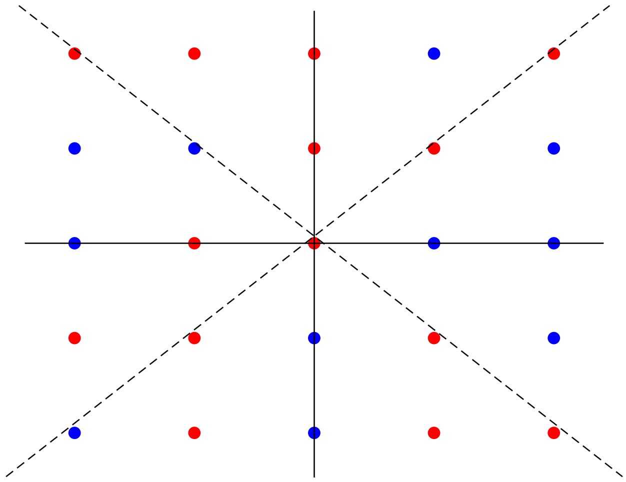
για $i = 1, 2, \dots, N$ αποτελούν βάση. Πράγματι, έστω $f : V \to \mathbf{C}$ μια $\mathbf{C}G$-γραμμική, τότε $f(g \cdot x) = g \cdot f(x) = f(x)$, δηλαδή είναι σταθερή στις τροχιές $f|_{\mathcal{O}(x_i)}(x) = f(x_i)$ για κάθε $i = 1, 2, \dots, N$. Συνεπώς για κάθε $x \in X$ είναι

$$f(x) = \sum_{i=1}^{N} f(x_i) \cdot \delta_i(x)$$

και άρα αφού ισχύει ισότητα στα στοιχεία της βάσης του V, έχουμε ισότητα $\mathbf{C}G$-γραμμικών απεικονίσεων $f = \sum_{i=1}^N f(x_i)\delta_i$ □

Παραδείγματα. (i) *Χρωματίζουμε τα 25 σημεία του τετραγώνου $T = [-2, 2] \times [-2, 2] \subseteq \mathbf{R}^2$ με ακέραιες συντεταγμένες, το καθένα με δύο χρώματα, κόκκινο ή μπλε. Θεωρούμε δύο χρωματισμούς ισοδύναμους αν ο ένας προκύπτει από τον άλλο με στροφή γύρω από το κέντρο του T κατά γωνία που είναι ακέραιο πολλαπλάσιο του $\pi/2$, ή με ορθογώνια ανάκλαση ως προς έναν από τους τέσσερις άξονες συμ-*

μετρίας του T. Πόσες κλάσεις ισοδυναμίας χρωματισμών υπάρχουν;



Η διεδρική ομάδα $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ δρα στο σύνολο X των χρωματισμών του $\mathbf{Z}^2 \cap T$ με στροφή $\pi/2$ και ανάκλαση. Παρατηρούμε, ότι δύο χρωματισμοί ειναι ισοδύναμοι αν και μόνο αν ανήκουν στην ίδια τροχία. Αν N το πλήθος των διαφορετικών χρωματισμών, τότε από λήμμα του Burnside, ξέρω ότι

$$N = \frac{1}{\#D_4} \sum_{g \in D_4} \#\mathit{Fix}(g) = 4,211,744 \text{ χρωματισμοί}$$

όπου $\#\mathit{Fix}(1) = 2^{25}$, $\#\mathit{FIx}(r) = \#\mathit{Fix}(r^3) = 2^7$, $\#\mathit{Fix}(r^2) = 2^{13}$, $\#\mathit{Fix}(s) = \#\mathit{Fix}(sr) = \#\mathit{Fix}(sr^2) = \#\mathit{Fix}(sr^3) = 2^{15}$

(ii) Έστω G μια πεπερασμένη ομάδα και έστω N το πλήθος των κλάσεων συζηγίας. Εύκολα βλέπουμε, ότι $N \leq \#G$. Ο αριθμός N είναι ένας τρόπος μέτρησης το "πόσο κοντά" είναι η G να είναι αβελιανή. Πράγματι, αν επιλέξουμε ομοιόμορφα δύο στοιχεία $g, h \in G$, τότε η πιθανότητα να μετατίθονται είναι ίση με

$$\frac{\#\{(g,h) \in G \times G : gh = hg\}}{\#G \times G} = \frac{1}{(\#G)^2} \sum_{g \in G} \#\{h \in G : gh = hg\} = \frac{\#G \cdot N}{(\#G)^2} = \frac{N}{\#G}$$

4.3 Το θεώρημα του Burnside

4.3.1 Αλγεβρικά στοιχεία.

Ορισμός 4.3.1. *Έστω $R \longrightarrow S$ μια επέκταση δακτυλίων. Ένα στοιχείο S καλείται αλγεβρικό πάνω από τον R, αν υπάρχει ένα μονικό πολύωνυμο $f(X) \in R[X]$ με $f(s) = 0 \in R$.*

Πρόταση 4.3.1. *Έστω $R \longrightarrow S$ μια επέκταση δακτυλίων. Τα επόμενα είναι ισοδύναμα για ένα στοιχείο $s \in S$.*

- (i) *Το s είναι αλγεβρικό πάνω από το R.*
- (ii) *Ο δακτύλιος $R[s] := \{f(s) : f(X) \in R[X]\}$ είναι ένα πεπερασμένα παραγόμενο R-πρότυπο.*
- (iii) *Υπάρχει υποδακτύλιος R' του S, τέτοιος ώστε $R[s] \subseteq R'$ και ο R' είναι ένα πεπερασμένα παραγόμενο R-πρότυπο.*
- (iv) *Υπάρχει ένα πιστό $R[s]$-πρότυπο M που είναι πεπερασμένα παραγόμενο σαν R-πρότυπο.*

Σταθεροποιώντας μια επέκταση $R \hookrightarrow S$, το σύνολο των αλγεβρικών στοιχείων πάνω από το R, το συμβολίζουμε R^{alg}.

Απόδειξη : $(i) \to (ii)$: Είναι προφανές ότι τα στοιχεία $1, s, s^2, \ldots$ παράγουν τον δακτύλιο $R[s]$. Καθώς το στοιχείο s είναι αλγεβρικό πάνω από το R, υπάρχει ένα μονικό πολυώνυμο $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$ (βαθμού $\deg f = n$) ώστε $f(a) = 0$. Σταθεροποιώ έναν $m \geq n+1$ και παρατηρώ ότι

$$s^m = -(a_{n-1}s^{m-1} + \cdots + a_0 s^{m-n})$$

Συνεπώς αν τα στοιχεία $s^{m-n}, \ldots s^{m-1}$ ανήκουν στο R-υποπρότυπο $\sum_{k=1}^n Rs^k$, τότε και το s^m ανήκει. Με επαγωγή, παίρνω το ζητούμενο.

$(ii) \to (iii)$: Προφανές για $R' = R[s]$.

$(iii) \to (iv)$: Το $R[s]$-πρότυπο R' είναι πιστό, καθώς αν $x \in R[s]$ με $x \cdot r = 0$ για κάθε $r \in R'$, αφού $1 \in R'$ έχω $x = x \cdot 1 = 0$.

$(iv) \to (i)$: Το M είναι πεπερασμένο παραγόμενο R-πρότυπο, συνεπώς υπάρχουν $m_1, \ldots, m_n$ με $M = \sum_{i=1}^n Rm_i$. Αφού το M επεκτείνει την δομή του σε ένα $R[s]$-πρότυπο, είναι $sM \subseteq M$[6] και άρα

$$s \cdot m_i = \sum_{j=1}^n a_{i,j} m_j$$

για κάποια $a_{i,j} \in R$. Αν θεωρήσω τον πίνακα $A = (a_{i,j}) \in \mathbf{M}_n(R)$, τότε η προηγούμενη ισότητα γράφεται

$$(A - sI_n) \cdot \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = 0$$

Πολλαπλασιάζοντας αριστερά με τον $adj(A - sI_n)$, παίρνω $\det(A - sI_n) \cdot m_i = 0$ για κάθε $i = 1, 2, \ldots, n$ ισοδύναμα $\det(A - sI_n) \cdot M = 0$. Το $R[s]$-πρότυπο M είναι πιστό και άρα $\det(A - sI_n) = 0$. Το πολυώνυμο $f(X) = \det(A - XI_n)$ είναι μονικό, με συντελεστές από το R και έχει ρίζα το s. ☐

Παρατήρηση. *Έστω $R \hookrightarrow S$ μια επέκταση δακτυλίων. Τότε, $R \subseteq R^{alg}$, αφού για κάθε $r \in R$, το πολυώνυμο $f(X) = X - r$ ανήκει στο $R[X]$, είναι μονικό και έχει ρίζα το $r \in R$.*

Πόρισμα 4.3.1. *Έστω $R \hookrightarrow S$ μια επέκταση δακτυλίων και $s_1, \ldots, s_n \in R^{alg}$. Τότε ο δακτύλιος $R[s_1, \ldots, s_n]$ είναι πεπερασμένα παραγόμενο R-πρότυπο.*

Απόδειξη : Θα χρησιμοποιήσουμε επαγωγή. Για $n = 1$ το έχουμε δείξει για $n > 1$, υποθέτουμε ότι το R-πρότυπο $R[s_1, \ldots, s_{n-1}]$ είναι πεπερασμένα παραγόμενο. Το στοιχείο $s_n \in S$ είναι ακέραιο πάνω από το R και άρα και ακέραιο πάνω από το $R[s_1, \ldots, s_{n-1}]$. Συνεπώς το $R[s_1, \ldots, s_{n-1}]$-πρότυπο $R[s_1, \ldots, s_n] = R[s_1, \ldots, s_{n-1}][s_n]$ είναι πεπερασμένα παραγόμενο και άρα το $R[s_1, \ldots, s_n]$ είναι πεπερασμένα παραγόμενο R-πρότυπο ☐

Παρατήρηση. *Έστω $R \hookrightarrow S \hookrightarrow T$ μια διαδοχική επέκταση δακτυλίων. Αν το S-πρότυπο T και το R-πρότυπο S είναι πεπερασμένα παραγόμενα, τότε και το R-πρότυπο T είναι πεπερασμένα παραγόμενο.*

[6]Ένα $R[s]$-πρότυπο M είναι ακριβώς ένα R-πρότυπο M με $s \cdot M \subseteq M$.

Πράγματι υπάρχουν $t_1, \ldots, t_n \in T$ και $s_1, \ldots, s_m \in S$ με $T = \sum_{i=1}^{n} St_i$ και $S = \sum_{j=1}^{m} Rs_j$, συνεπώς :

$$T = \sum_{i=1}^{n} St_i = \sum_{i,j} Rs_j t_i$$

Στην προηγούμενη πρόταση, εφαρμόσαμε την παρατήρηση αυτή για την διαδοχική επέκταση δακτυλίων

$$R \hookrightarrow R[s_1, \ldots, s_{n-1}] \hookrightarrow R[s_1, \ldots, s_{n-1}, s_n]$$

όπου $s_1, \ldots s_n$ αλγεβρικά πάνω από το R.

Πόρισμα 4.3.2. *Έστω $R \hookrightarrow S$ μια επέκταση δακτυλίων, τότε το σύνολο R^{alg} των ακέραιων στοιχείων πάνω από το R είναι υποδακτύλιος του S.*

Απόδειξη : Έστω $s_1, s_2 \in R^{alg}$, τότε ο δακτύλιος $R' := R[s_1, s_2]$ είναι πεπερασμένα παραγόμενο R-πρότυπο. Ισχύει, ότι $R[s_1 - s_2] \subseteq R'$ και $R[s_1 \cdot s_2] \subseteq R'$. Από την Πρόταση 4.3.1. , ισχύει ότι $s_1 - s_2 \in R^{alg}$ και $s_1 s_2 \in R^{alg}$. □

Ορισμός 4.3.2. *Θεωρώ την επέκταση δακτυλίων $\mathbf{Z} \hookrightarrow \mathbf{C}$. Ένα στοιχείο του $\mathbf{Z}^{alg}$ το ονομάζουμε αλγεβρικό ακέραιο.*

Πρόταση 4.3.2. *Ισχύει ότι $\mathbf{Z}^{alg} \cap \mathbf{Q} = \mathbf{Z}$.*

Απόδειξη : Προφανώς $\mathbf{Z} \subseteq \mathbf{Z}^{alg} \cap \mathbf{Q}$. Για τον αντίστροφο εγκλεισμό, έστω $a/b \in \mathbf{Q}$ με $\gcd(a, b) = 1$ και έστω υπάρχει μονικό πολυώνυμο $f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0 \in \mathbf{Z}[X]$ με $f(a/b) = 0$. Πολλαπλασιάζοντας με b^n παίρνω

$$a^n = -b(c_{n-1}a^{n-1} + \cdots + c_0 b^{n-1})$$

Συνεπώς το b διαιρεί το a^n, άρα $b = +1$ ή -1 δηλαδή $a/b \in \mathbf{Z}$ □

Πρόταση 4.3.3. *Έστω χ ένας χαρακτήρας μια πεπερασμένης ομάδας G. Τότε για κάθε $g \in G$ είναι $\chi(g) \in \mathbf{Z}^{alg}$*

Απόδειξη : Έχουμε δείξει ότι για κάθε $g \in G$, το $\chi(g)$ είναι άθροισμα ριζών την μονάδος. Οι ρίζες μονάδες είναι αλγεβρικοί ακέραιοι, αφού είναι ρίζες του πολυωνύμου $X^n - 1 \in \mathbf{Z}[X]$ για κάποιον n. Το σύνολο των αλγεβρικών ακέραιων είναι δακτύλιος και άρα $\chi(g) \in \mathbf{Z}^{alg}$. □

Παρατήρηση. *Οι μόνοι ρητοί αριθμοί που εμφανίζονται στον πίνακα χαρακτήρων μιας ομάδας G είναι οι ακέραιοι.*

4.3.2 Πως δρουν τα στοιχεία του κέντρου $Z(\mathbf{C}G)$;

Πρόταση 4.3.4. *Έστω V ένα απλό $\mathbf{C}G$-πρότυπο, $\alpha \in Z(\mathbf{C}G)$ και $(v \overset{\varrho_\alpha}{\longmapsto} \alpha \cdot v)$ ο αντίστοιχος ενδομορφισμός. Τότε υπάρχει $\lambda \in \mathbf{C}$, ώστε $\varrho_\alpha = \lambda \cdot 1_V : V \to V$.*

Απόδειξη : Το σώμα $\mathbf{C}$ είναι αλγεβρικά κλειστό, συνεπώς ο ενδομορφισμός $\varrho_a : V \to V$ έχει κάποια ιδιοτιμή $\lambda \in \mathbf{C}$ με αντίστοιχο ιδιόχωρο E_λ. Ο υπόχωρος E_λ είναι στην πραγματικότητα $\mathbf{C}G$-υποπρότυπο. Πράγματι, έστω $v \in E_\lambda$ και $g \in G$, τότε $\varrho_a(gv) = agv = gav = \lambda gv$, δηλαδή $gv \in E_\lambda$. Καθώς το V είναι απλό $\mathbf{C}G$-πρότυπο και ο E_λ μη μηδενικό $\mathbf{C}G$-υποπρότυπο, έπεται ότι $V = E_\lambda$, δηλαδή $\varrho_a = \lambda \cdot 1_V : V \to V$. □

Υπενθύμιση. *Έστω G πεπερασμένη ομάδα και $g_1, \ldots, g_r$ αντιπρόσωποι των κλάσεων συζηγίας της G. Τότε τα στοιχεία $\alpha_i = \sum_{x \in \overline{g}_i} x$ αποτελούν βάση του διανυσματικού χώρου $Z(\mathbf{C}G)$.*

Πρόταση 4.3.5. *Έστω G μια πεπερασμένη ομάδα τάξης n με απλά $\mathbf{C}G$-πρότυπα $V_1, \ldots, V_r$ και αντίστοιχες διαστάσεις $n_i := \dim V_i$. Σταθεροποιώ ένα $g \in G$ και συμβολίζω $\overline{g}$ την κλάση συζηγίας του g. Θεωρώ το στοιχείο $\alpha = \sum_{x \in \overline{g}} x$ και τον αντίστοιχο ενδομορφισμό $\varrho_\alpha : \mathbf{C}G \to \mathbf{C}G$ με $\varrho_\alpha(v) = a \cdot v$ για κάθε $v \in \mathbf{C}G$. Τότε υπάρχει βάση του $\mathbf{C}G$, ώστε ο πίνακας της ϱ_α να είναι ο*

$$\begin{pmatrix} \lambda_1 \cdot I_{n_1^2} & 0 & \cdots & 0 \\ 0 & \lambda_2 \cdot I_{n_2^2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_r \cdot I_{n_r^2} \end{pmatrix}$$

όπου $\lambda_i = \dfrac{\#\overline{g} \cdot \chi_{V_i}(g)}{\chi_{V_i}(1)}$. και το i-block έχε διάσταση n_i^2.

Απόδειξη : Γνωρίζω ότι, $\mathbf{C}G = \bigoplus_{i=1}^r V_i^{n_i}$, συνεπώς αρκεί να καταλάβω τις $\varrho_\alpha|_{V_i} : V_i \to V_i$ για κάθε $i = 1, 2, \ldots, r$. Από την προηγούμενη πρόταση, υπάρχει $\lambda_i \in \mathbf{C}$ τέτοιο ώστε $\varrho_\alpha|_{V_i} = \lambda_i \cdot 1_{V_i} : V_i \to V_i$. Για την τιμή του λ_i :

$$\dim V_i \cdot \lambda_i = \mathrm{tr}(V_i \xrightarrow{\lambda_i \cdot 1_{V_i}} V_i) = \mathrm{tr}(V_i \xrightarrow{\varrho_\alpha|_{V_i}} V_i) = \chi_{V_i}(\alpha) = \#\overline{g} \cdot \chi_{V_i}(g)$$
$$\Rightarrow \lambda_i = \frac{\#\overline{g} \cdot \chi_{V_i}(g)}{\dim V_i} = \frac{\#\overline{g} \cdot \chi_{V_i}(g)}{\chi_{V_i}(1)}$$

□

Πόρισμα 4.3.3. *Έστω χ ένας ανάγωγος χαρακτήρας και $g \in G$. Τότε*

$$\frac{\#\overline{g} \cdot \chi(g)}{\chi(1)} \in \mathbf{Z}^{alg}$$

Απόδειξη : Έστω $\alpha = \sum_{x \in \overline{g}} x$ και $\lambda = \#\overline{g} \cdot \chi(g)/\chi(1)$. Απο την προηγούμενη πρόταση, ο αριθμός λ αποτελεί ιδιοτιμή του ενδομορφισμού $\varrho_\alpha : \mathbf{C}G \to \mathbf{C}G$. Παρατηρούμε ότι ο πίνακας της $\varrho_\alpha : \mathbf{C}G \to \mathbf{C}G$ ως προς την συνήθη βάση $G = \{g_1, \ldots, g_n\}$ έχει ακέραιες εγγραφές, συνεπώς το χαρακτηριστικό του πολυώνυμο $\varphi_{\varrho_\alpha}(X) = \det(\varrho_\alpha - XI_n)$ έχει ακέραιους συντελεστές. Επίσης είναι μονικό και ο λ είναι ρίζα του, δηλαδή $\lambda \in \mathbf{Z}^{alg}$. □

Παραδείγματα. *(i) Έστω G πεπερασμένη ομάδα και V ένα απλό $\mathbf{C}G$-πρότυπο, τότε $\chi_V(1) \mid \#G$. Πράγματι, έστω $g_1, \ldots, g_r$ αντιπρόσωποι των κλάσεων συζηγίας. Γνωρίζω ότι $\#\overline{g}_i \cdot \chi_V(g_i)/\chi_V(1) \in \mathbf{Z}^{alg}$ και $\overline{\chi_V(g)} = \chi_V(g^{-1}) \in \mathbf{Z}^{alg}$ για κάθε $g \in G$. Αφού ο $\mathbf{Z}^{alg}$ είναι δακτύλιος, έχω*

$$\sum_{i=1}^r \frac{\#\overline{g}_i \cdot \chi_V(g_i)\overline{\chi_V(g_i)}}{\chi_V(1)} \in \mathbf{Z}^{alg}$$

και υπολογίζω

$$\sum_{i=1}^r \frac{\#\overline{g}_i \cdot \chi_V(g_i)\overline{\chi_V(g_i)}}{\chi_V(1)} = \frac{1}{\chi_V(1)} \sum_{i=1}^r \#\overline{g}_i \cdot \chi_V(g_i)\overline{\chi_V(g_i)} = \frac{1}{\chi_V(1)} \sum_{g \in G} \chi_V(g)\overline{\chi_V(g)}$$
$$= \frac{\#G \cdot \langle \chi_V, \chi_V \rangle}{\chi_V(1)} = \frac{\#G}{\chi_V(1)}$$

Τελικά παίρνω $\#G/\chi_V(1) \in \mathbf{Z}^{alg} \cap \mathbf{Q} = \mathbf{Z}$, δηλαδή η διάσταση του μιας ανάγωγης αναπαράστασης της G (του απλού $\mathbf{C}G$-προτύπου) διαιρεί την τάξη της ομάδας G.

(ii) Έστω p πρώτος, τότε κάθε ομάδα G τάξης p^2 είναι αβελιανή. Πράγματι, θα δείξω ότι κάθε απλό $\mathbf{C}G$-πρότυπο είναι διάστασης 1. Έστω V ένα απλό $\mathbf{C}G$-πρότυπο διάστασης n, τότε από την προηγούμενη παρατήρηση έχω $n = 1$ ή p ή p^2. Από το θεώρημα Wedderburn-Artin, η τάξη της G είναι το άθροισμα των τετραγωγων των διαστάσεων των απλών $\mathbf{C}G$-προτύπων. Αφού το τετριμμένο $\mathbf{C}G$-πρότυπο είναι απλό, έχω ότι $n^2 + 1 \leq \#G = p^2 \Rightarrow n^2 \leq p^2 - 1 < p^2 \Rightarrow n < p$ και συνεπώς $n = 1$.

4.3.3 Λίγη θεωρία Galois για την επέκταση $\mathbf{Q} \longhookrightarrow \mathbf{Q}(\zeta)$

Ορισμός 4.3.3. *Έστω n φυσικός αριθμός και $\zeta = e^{2\pi i/n}$. Το σύνολο των ριζών του πολυωνύμου $X^n - 1$ αποτελεί κυκλική ομάδα με γεννήτορα το ζ. Τα στοιχεία αυτής της ομάδας $\mathcal{C}_n = \langle \zeta \rangle$ καλούνται n-οστες ρίζες της μονάδος. Η γεννήτορες της κυκλικής ομάδας $\mathcal{C}_n$, δηλαδή τα ζ^k για $\gcd(k,n) = 1$ με $k < n$, ονομάζονται πρωταρχικές n-οστες ρίζες της μονάδος*[7].

Ορισμός 4.3.4. *Έστω $\zeta = e^{2\pi i/n}$ και θεωρώ την επέκταση σωμάτων $\mathbf{Q} \longhookrightarrow \mathbf{Q}(\zeta)$. Ορίζω την ομάδα των $\mathbf{Q}$-αυτομορφισμών να είναι :*

$$\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q}) := \{\sigma : \mathbf{Q}(\zeta) \to \mathbf{Q}(\zeta) : \text{ Ο } \sigma \text{ είναι ισομορφισμός δακτυλίων και } \sigma\big|_{\mathbf{Q}} = 1_{\mathbf{Q}}\}$$

και το σώμα των σταθερών σημείων :

$$\mathrm{FixAut}(\mathbf{Q}(\zeta)/\mathbf{Q}) := \{a \in \mathbf{Q}(\zeta) : \sigma(a) = a \text{ για κάθε } \sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})\}$$

Παρατήρηση. *Καθε $\mathbf{Q}$-αυτομορφισμός είναι $\mathbf{Q}$-γραμμικός και συνεπώς*

$$\sigma(g(\zeta)) = g(\sigma(\zeta))$$

για κάθε $g(X) \in \mathbf{Q}[X]$, δηλαδή κάθε $\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ καθορίζεται πλήρως από την εικόνα της στο ζ.

Λήμμα 4.3.1. *Έστω $\varphi(X)$ μονικό πολυώνυμο με ακέραιους συντελεστές και $\psi(X)$ πολυώνυμο με ρητούς συντελεστές, τέτοιο ώστε $\psi(X) \mid \varphi(X)$. Τότε το $\psi(X)$ έχει ακέραιους συντελεστές*

Απόδειξη : Αφού $\psi(X) \mid \varphi(X)$, κάθε ρίζα του $\psi(X)$ είναι και ρίζα του $\varphi(X)$, δηλαδή κάθε ρίζα του $\psi(X)$ είναι αλγεβρικός ακέραιος. Από τους τύπους Vieta, οι συντελεστές του $\psi(X)$ είναι πράξεις αλγεβρικών ακέραιων, άρα και οι ίδιοι είναι αλγεβρικοί ακέραιοι. Οι ρητοί αλγεβρικοί ακέραιοι είναι ακριβώς οι ακέραιοι. □

Πρόταση 4.3.6. *Θεωρώ τον ομομορφισμό εκτίμησης $ev_\zeta : \mathbf{Q}[X] \to \mathbf{Q}(\zeta)$, ο οποίος είναι επί και έχει πυρήνα $\ker ev_\zeta = (f(X))$ για κάποιο μονικό $f(X) \in \mathbf{Q}[X]$. Το $f(X)$ έχει ακέραιους συντελεστές, είναι ανάγωγο και ισχύει η ισότητα*

$$\dim_{\mathbf{Q}} \mathbf{Q}(\zeta) = \deg f(X)$$

.

Απόδειξη : Έχουμε ότι $f(X) \in \mathbf{Q}[X]$ και $f(X) \mid X^n - 1$ άρα $f(X) \in \mathbf{Z}[X]$ από το προηγούμενο λήμμα. Το $f(X)$ είναι προφανώς ανάγωγο, καθώς το αντίστοιχο πηλίκο είναι σώμα. Για την ισότητα, έστω $\ell := \deg f(X)$, θα δείξω ότι το σύνολο $\{1, \zeta, \ldots, \zeta^{\ell-1}\}$ παράγει το $\mathbf{Q}$-διανυσματικό χώρο $\mathbf{Q}(\zeta)$. Έστω $g(X) \in \mathbf{Q}[X]$, τότε από την ευκλείδια διαίρεση, υπάρχουν $\pi(X), \upsilon(X) \in \mathbf{Q}[X]$ με $g(X) = \pi(X)f(X) + \upsilon(X)$ και $\deg \upsilon(X) < \deg f(X) = \ell$. Συνεπώς

$$g(\zeta) = \pi(\zeta)f(\zeta) + \upsilon(\zeta) = \upsilon(\zeta) \in \mathrm{span}_{\mathbf{Q}}\{1, \zeta, \ldots, \zeta^{\ell-1}\}$$

Τα στοιχεία $1, \zeta, \ldots, \zeta^{\ell-1}$ είναι και γραμμικά ανεξάρτητα. Αν δεν ήταν, θα υπήρχε ένα $h(X) \in \mathbf{Q}[X]$ με $\deg h < \ell$ ώστε $h(\zeta) = 0$, συνεπώς $h(X) \in (f(X)) \iff f(X) \mid h(X) \Rightarrow \ell = \deg f(X) \leq \deg h(X) < \ell$ #. □

[7] Το πλήθος των θετικών ακεραίων $k \leq n$ με $\gcd(k,n) = 1$ είναι ακριβώς $\varphi(n)$, όπου φ η συνάρτηση του Euler. Συνεπώς και το πλήθος των n-οστων πρωταρχικών ριζών της μονάδος είναι $\varphi(n)$

Πρόταση 4.3.7. *Η ομάδα* $\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ *είναι πεπερασμένη και στην πραγματικότητα ισχύει*

$$\#\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q}) = \deg f(X) = \dim_{\mathbf{Q}} \mathbf{Q}(\zeta)$$

Απόδειξη : Πράγματι, έστω $\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$, τότε η σ καθορίζεται πλήρως από την εικόνα της στο ζ. Παρατηρώ, ότι $f(\sigma(\zeta)) = \sigma(f(\zeta)) = \sigma(0) = 0$, δηλαδή το $\sigma(\zeta)$ είναι ρίζα του $f(X)$ για κάθε $\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$, συνεπώς $\#\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q}) \leq \deg f(X)$. Για την αντίστροφη κατεύθυνση, θα δείξω ότι για κάθε άλλη ρίζα $\zeta' \in \mathbf{C}$ του $f(X)$, υπάρχει $\mathbf{Q}$-ισομορφισμός με $\sigma(\zeta) = \zeta'$ και άρα $\#\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q}) \geq \deg f(X)$. Αρχικά, αφού $\zeta^n - 1 = 0$, τότε $f(X) \mid X^n - 1$ και άρα κάθε άλλη ρίζα ζ' του $f(X)$ είναι επίσης ρίζα της μονάδος, έπεται ότι $\mathbf{Q}(\zeta) = \mathbf{Q}(\zeta')$. Σταθεροποίω μια ρίζα $\zeta' \in \mathbf{C}$ του $f(X)$ και θεωρώ την σύνθεση :

$$\begin{tikzcd}
\mathbf{Q}(\zeta) \arrow[r, "(\overline{ev}_{\zeta})^{-1}"] \arrow[rr, bend right, "\sigma"'] & \mathbf{Q}[X]/(f(X)) \arrow[r, "\overline{ev}_{\zeta'}"] & \mathbf{Q}(\zeta') \\
\zeta \arrow[r, mapsto] & X + (f(X)) \arrow[r, mapsto] & \zeta'
\end{tikzcd}$$

Ο σ είναι ισομορφισμός δακτυλίων σαν σύνθεση ισομορφισμών, επεκτείνει την ταυτοτική απεικόνιση $1_{\mathbf{Q}} : \mathbf{Q} \to \mathbf{Q}$, δηλαδή $\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ και $\sigma(\zeta) = \zeta'$. □

Πρόταση 4.3.8. *Θεωρώ την διαδοχική επέκταση σωμάτων*

$$\mathbf{Q} \hookrightarrow \mathrm{FixAut}(\mathbf{Q}(\zeta)/\mathbf{Q}) \hookrightarrow \mathbf{Q}(\zeta)$$

Θέτω $K = \mathrm{FixAut}(\mathbf{Q}(\zeta)/\mathbf{Q})$, *τότε ισχύει* $\dim_K \mathbf{Q}(\zeta) = \#\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ *και άρα* $\mathrm{FixAut}(\mathbf{Q}(\zeta)/\mathbf{Q}) = \mathbf{Q}$.

Απόδειξη : Πράγματι, με την ίδια ακριβώς απόδειξη με το (ii), μπορώ να δείξω ότι $\dim_K \mathbf{Q}(\zeta) = \#\mathrm{Aut}(\mathbf{Q}(\zeta)/K)$, άρα αρκέι να δείξω ότι $\#\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q}) = \#\mathrm{Aut}(\mathbf{Q}(\zeta)/K)$. Η τέλευταια ισότητα είναι προφανής, κάθε K-αυτομορφισμός είναι $\mathbf{Q}$-αυτομορφισμός, αφού $\mathbf{Q} \subseteq K$ και κάθε $\mathbf{Q}$-αυτομορφισμός, από τον ορισμό του K, είναι επίσης K-αυτομορφισμός. □

Λήμμα 4.3.2. *Έστω* $h(X)$ *πολυώνυμο με ακέραιους συντελεστές, τέτοιο ώστε* $h(X) \mid X^n - 1$. *Αν* $\xi \in \mathbf{C}$ *με* $h(\xi) = 0$, *τότε για κάθε πρώτο αριθμό* p *που δεν διαιρεί τον* n *είναι* $h(\xi^p) = 0$

Απόδειξη : Θεωρώ την ποσότητα [8]

$$\Delta = \prod_{i<j} (\zeta^i - \zeta^j)^2 = \pm \prod_{i \neq j} (\zeta^i - \zeta^j) = \pm \prod_{i \neq j} \zeta^i (1 - \zeta^{j-i})$$

$$= \pm \prod_i \zeta^i \prod_{k \neq 0} (1 - \zeta^k) = \pm \prod_i (\zeta^i n) = \pm n^n$$

Έστω, ως προς άτοπο, ότι $h(\xi^p) \neq 0$, τότε $h(X) = (X - \xi_1) \ldots (X - \xi_k)$ για κάποιες $\xi = \xi_1, \ldots, \xi_k \in \mathcal{C}_n$ με $\xi_i \neq \xi^p$ για κάθε i. Συνεπώς, η $0 \neq \overline{h(\xi^p)}$ είναι το γινόμενο των διαφορών, και άρα $h(\xi^p) \mid \Delta$. Από "το όνειρο το πρωτοετή"[9], έχω $\overline{f(\xi^p)} = \overline{f(\xi)}^p = \overline{0} \in \mathbf{Z}_p(\zeta)$ και άρα $p \mid f(\xi^p)$, δηλαδή $p \mid \pm n^n$ #. □

[8] Αν $\varphi(X) = \prod_{k \neq 0} (X - \zeta^k) = (X^n - 1)/(X - 1) = \sum_{i=0}^{n-1} X^i$, άρα $\prod_{k \neq 0} (1 - \zeta^k) = \varphi(1) = n$

[9] Έστω R δακτύλιος χαρακτηριστικής p, τότε για κάθε πολυώνυμο $h(X) \in R[X]$ και $\xi \in R$ είναι $f(\xi^p) = f(\xi)^p$. Στην περίπτωση μας, έχουμε $R = \mathbf{Z}_p(\zeta)$.

Πόρισμα 4.3.4. *Ισχύει ότι* $\#\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q}) = \deg f(X) = \varphi(n)$ *και οι αυτομορφισμοί της ομάδας* $\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ *είναι ακριβώς οι* $\sigma_k : \zeta \longmapsto \zeta^k$ *για κάθε* $k < n$ *με* $\gcd(k, n) = 1$*. Συνεπώς, υπάρχει ισομορφισμός ομάδων*

$$\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q}) \xrightarrow{\simeq} \mathbf{U}(\mathbf{Z}_n)$$

$$(\zeta \overset{\sigma_k}{\longmapsto} \zeta^k) \longmapsto \overline{k}$$

Απόδειξη : Οι $\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ είναι ακριβώς αυτές που μετατίθουν το ζ με τις άλλες ρίζες του $f(X)$. Συνεπώς, αρκεί να δείξουμε ότι οι ρίζες του $f(X)$ είναι ακριβώς οι n-οστές πρωταρχικές ρίζες της μονάδος. Πράγματι, έστω $k < n$ με $\gcd(k, n) = 1$, τότε ο k είναι γινόμενο πρώτων αριθμών που κανένας τους δεν διαιρεί τον n. Από το προηγούμενο λήμμα, έπεται ότι $f(\zeta^k) = 0$. Τώρα, αν ξ μια ρίζα του $f(X)$, τότε υπάρχει $\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ με $\xi = \sigma(\zeta)$ και παρατηρούμε ότι για κάθε $m < n$ είναι $\xi^m = \sigma(\zeta)^m = \sigma(\zeta^m) \neq 1$, δηλαδή η ξ είναι γεννήτορας της $\mathcal{C}_n$. Τέλος η παραπάνω απεικόνιση είναι προφανές ότι είναι αμφιμονοσήμαντη και εύκολα δείχνεται ότι σέβεται την σύνθεση. □

Πόρισμα 4.3.5. *Το μονικό πολυώνυμο* $f(X)$ *που παράγει τον πυρήνα του ομομορφισμούς εκτίμησης* $ev_\zeta : \mathbf{Q}[X] \to \mathbf{Q}(\zeta)$

$$f(X) = \prod_{\gcd(k,n)=1} (X - \zeta^k)$$

καλείται το n*-οστό κυκλωτομικό πολυώνυμο. Το* n*-οστό κυκλωτομικό πολυώνυμο είναι ανάγωγο, είναι βαθμού* $\varphi(n)$ *και έχει ακέραιους συντελεστές.*

Πρόταση 4.3.9. *Τα επόμενα είναι ισοδύναμα για μια πεπερασμένη ομάδα* G*.*

(*i*) $\chi(g) \in \mathbf{Z}$ *για κάθε χαρακτήρα* $\chi : G \to \mathbf{C}$ *και* $g \in G$*.*

(*ii*) $\chi(g) \in \mathbf{Q}$ *για κάθε χαρακτήρα* $\chi : G \to \mathbf{C}$ *και* $g \in G$*.*

(*iii*) *Αν* $g \in G$ *ένα στοιχείο τάξης* n*, τότε* $g \sim g^k$ *για κάθε ακέραιο* $k < n$ *με* $\gcd(k, n) = 1$*.*

Στην περίπτωση αυτή, η ομάδα G *λέγεται ρητή.*

Απόδειξη : (*i*) $\leftrightarrow$ (*ii*) : ΄Αμεσο, καθώς $\chi(g) \in \mathbf{Z}^{alg}$ για κάθε χαρακτήρα $\chi : G \to \mathbf{C}$ και $g \in G$. .

(*ii*) $\to$ (*iii*) : Έστω στοιχείο $g \in G$ τάξης n. Αφού οι χαρακτήρες διαχωρίζουν τις κλάσεις συζηγίας, αρκεί να δείξουμε ότι $\chi(g) = \chi(g^k)$ για κάθε χαρακτήρα $\chi : G \to \mathbf{C}$. Πράγματι, αφού $g^n = 1$, οι ιδιοτιμές της g είναι n-οστές ρίζες της μονάδος και αφού $\chi(g) \in \mathbf{Q} = \mathrm{FixAut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ είναι $\sigma(\chi(g)) = \chi(g)$ για κάθε $\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$. Γνωρίζω, ότι οι $\sigma_k \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ είναι ακριβώς αυτές με $\zeta \overset{\sigma_k}{\longmapsto} \zeta^k$ για κάθε $k < n$ με $\gcd(k, n) = 1$. Συνεπώς,

$$\chi(g) = \lambda_1 + \cdots + \lambda_m \Rightarrow$$

$$\chi(g) = \sigma_k(\chi(g)) = \lambda_1^k + \cdots + \lambda_m^k = \chi(g^k)$$

για κάθε $k < n$ με $\gcd(k, n) = 1$.

(*iii*) $\to$ (*ii*) : Αντίστοιχα, με το προηγούμενο, αν $g \sim g^k$ για κάθε $k < n$ με $\gcd(k, n) = 1$, τότε για κάθε χαρακτήρα $\chi : G \to \mathbf{C}$ είναι

$$\lambda_1 + \cdots + \lambda_m = \chi(g) = \chi(g^k) = \lambda_1^k + \cdots + \lambda_m^k \Rightarrow$$

$$\sigma_k(\chi(g)) = \chi(g)$$

για κάθε $\sigma_k \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$, δηλαδή $\chi(g) \in \mathrm{FixAut}(\mathbf{Q}(\zeta)/\mathbf{Q}) = \mathbf{Q}$. □

Παραδείγματα. (*i*) *Η συμμετρική ομάδα* S_n *είναι ρητή, άρα κάθε χαρακτήρας έχει ακέραιες τιμές. Πράγματι, αφού για κάθε* $\tau \in S_n$ *τάξης* $o(\tau) = n$ *είναι* $\tau \sim \tau^k$ *για κάθε* $k < n$ *με* $\gcd(k, n) = 1$*.*

4.3.4 Το $p^a q^b$-Θεώρημα του Burnside

Μια ομάδα G λέγεται επιλύσιμη, αν υπάρχει μια ακολουθία ομάδων

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

ώστε τα πηλίκα G_{i+1}/G_i είναι αβελιανές ομάδες για κάθε $i = 0, 1, 2, \ldots, n-1$. Το $p^a q^b$-θεώρημα του Burnside, λέει ότι κάθε ομάδα G τάξης $p^a q^b$, όπου p, q πρώτοι, είναι επιλύσιμη. Ο βασικός στοχός για να αποδείξουμε το θεώρημα, είναι πρώτα να δείξουμε ότι κάθε τέτοια ομάδα G δεν είναι απλή.

Ορισμός 4.3.5. *Έστω G μια πεπερασμένη ομάδα και V ενα $\mathbf{C}G$-πρότυπο. Ορίζουμε*

$$Z(V) := \{g \in G : g \cdot v = \lambda \cdot v \text{ για κάποιο } \lambda \in \mathbf{C} \text{ και κάθε } v \in V\}$$

Η $Z(V)$ αποτελεί υποομάδα της G και την καλούμε V-κεντρική υποομάδα της G

Παρατήρηση. *(i) Έστω V ένα $\mathbf{C}G$-πρότυπο, τότε η V-κεντρική υποομάδα $Z(V)$ είναι κανονική.*

(ii) Ισχύει ότι $\bigcap\{Z(V) : V \text{ απλό } \mathbf{C}G\text{-πρότυπο}\} = Z(G)$.

Πρόταση 4.3.10. *Έστω G πεπερασμένη και V ένα $\mathbf{C}G$- πρότυπο με χαρακτήρα χ.Αν υπάρχει, $g \in G$ τέτοιο ώστε $\chi(g)/\chi(1)$ να είναι ένας μη μηδενικός αλγεβρικός ακέραιος, τότε $g \in Z(V)$. Ειδικότερα, η G δεν είναι απλή.*

Απόδειξη : Θέτω $n := \chi(1) = \dim_{\mathbf{C}} V$. Έστω $g \in G$ με $\chi(g)/n$ να είναι αλγεβρικός ακέραιος και να έχει ιδιοτιμές $\lambda_1, \ldots, \lambda_n \in \mathbf{C}$. Θα δείξω ότι όλες οι ιδιοτιμές της $g : V \to V$ είναι ίσες. Αν το καταφέρω, τότε θα είναι $g \in Z(V)$, αφού για τον ενδομορφισμο $g : V \to V$ είναι $g^n = 1_V : V \to V$ και άρα είναι διαγωνίσμος[10] στο $\mathbf{C}$, ισοδύναμα το ευθύ άθροισμα των ιδιοχώρων του ισούται με τον V, αλλά έχω μόνο έναν ιδιόχωρο, αυτόν της μοναδικής ιδιοτιμής $\lambda \in \mathbf{C}$ άρα $g = \lambda \cdot 1_V : V \to V$. Έστω, λοιπόν προς άτοπο, ότι υπάρχουν δύο ιδιοτιμές που δεν είναι ίσες, συνεπώς ισχύει ότι

$$|\chi(g)| = |\lambda_1 + \cdots + \lambda_n| < n$$

Θεωρώ την επέκταση σώματων $\mathbf{Q} \hookrightarrow \mathbf{Q}(\zeta)$, όπου $\zeta = e^{2\pi i/n}$. Το σώμα $\mathbf{Q}(\zeta)$ περιέχει κάθε ιδιοτιμή, αφού και αυτές είναι ρίζες της μονάδος. Για κάθε $\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ τα στοιχεία $\sigma(\lambda_1), \ldots, \sigma(\lambda_n)$ είναι ρίζες της μονάδος και δεν είναι όλες ίσες, οπότε

$$|\sigma(\chi(g))| = |\sigma(\lambda_1) + \cdots + \sigma(\lambda_n)| < n$$

και άρα

$$\left| \prod_{\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})} \sigma\left(\frac{\chi(g)}{n}\right) \right| = \prod_{\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})} \left| \frac{\sigma(\chi(g))}{n} \right| < 1$$

Έστω a το παραπάνω γίνομενο μέσα στην απόλυτη τιμή. Ο a είναι γινόμενο αλγεβρικών ακέραιων, συνεπώς είναι αλγεβρικός ακέραιος. Επίσης παρατηρώ ότι για κάθε $\tau \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ είναι

$$\tau(\alpha) = \prod_{\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})} \tau\sigma\left(\frac{\chi(g)}{n}\right) = \prod_{\sigma \in \mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})} \sigma\left(\frac{\chi(g)}{n}\right) = \alpha$$

δηλαδή $\alpha \in \mathrm{FixAut}(\mathbf{Q}(\zeta)/\mathbf{Q})$ και άρα είναι και ρητός. Συνεπώς $\alpha \in \mathbf{Z}^{alg} \cap \mathbf{Q} = \mathbf{Z}$ και $|\alpha| < 1$, δηλαδή τελικά $\alpha = 0$. Έπεται, ότι υπάρχει ένας $\mathbf{Q}$-αυτομορφισμός σ για τον οποίο ισχύει $\sigma(\chi(g)/n) = 0$, δηλαδή $\chi(g) = 0$ #

□

[10] Το ελάχιστο πολυώνυμο $\mu_g(X)$ είναι γινόμενο πρωτοβαθμίων

Πρόταση 4.3.11. *Έστω G μια πεπερασμένη ομάδα και χ ένας ανάγωγος χαρακτήρας. Αν $\gcd(\#\overline{g}, \chi(1)) = 1$, τότε $\chi(g)/\chi(1) \in \mathbf{Z}^{alg}$.*

Απόδειξη : Γνωρίζουμε ότι ο αριθμός $\#\overline{g}\cdot\chi(g)/\chi(1)$ είναι αλγεβρικός ακέραιος. Εφόσον $\gcd(\#\overline{g}, \chi(1)) = 1$, από το λήμμα Bezout υπάρχουν ακέραιοι α, β τέτοιοι ώστε

$$\alpha \cdot \#\overline{g} + \beta\chi(1) = 1 \Rightarrow$$

$$\frac{\chi(g)}{\chi(1)} = \alpha\frac{\#\overline{g}\cdot\chi(g)}{\chi(1)} + \beta\chi(g) \in \mathbf{Z}^{alg}$$

αφού ο $\mathbf{Z}^{alg}$ είναι δακτύλιος. □

Πόρισμα 4.3.6. *Έστω G πεπερασμένη ομάδα και V ένα απλό $\mathbf{C}G$-πρότυπο με χαρακτήρα χ_V. Αν ισχύει ότι $\gcd(\#\overline{g}, \chi_V(1)) = 1$, τότε για κάθε $g \in G$ είναι*

$$\chi_V(g) = 0 \text{ ή } g \in Z(V)$$

Απόδειξη : Αν $\chi_V(g) \neq 0$, τότε από την Πρόταση 4.3.8 ο $\chi_V(g)/\chi_V(1)$ είναι ένας μη μηδενικός αλγεβρικός ακέραιος και άρα από την Πρόταση 4.3.7 είναι $g \in Z(V)$. □

Πρόταση 4.3.12. *Έστω G μια πεπερασμένη ομάδα και έστω ότι υπάρχει $g \in G$, τέτοιο ώστε $\#\overline{g} = p^k$ για κάποιον πρώτο αριθμό p και κάποιον φυσικό k. Τότε, υπάρχει ένα $\mathbf{C}G$-πρότυπο V, τέτοιο ώστε $Z(V) \neq 1$. Ειδικότερα η G δεν είναι απλή.*

Απόδειξη : Έστω $V_1, \ldots, V_r$ τα απλά $\mathbf{C}G$-πρότυπα με αντίστοιχους χαρακτήρες $\chi_1, \ldots, \chi_r$ και θέτω $n_i := \chi_i(1) = \dim_{\mathbf{C}} V_i$. Έστω V_1 να είναι το τετριμμένο $\mathbf{C}G$-πρότυπο. Καθώς $\#\overline{g} \neq 1$, έπεται ότι $1 \notin \overline{g}$ και άρα από τις σχέσεις ορθογωνιότητας γραμμών :

$$0 = \sum_{i=1}^{r} \chi_i(g)\chi_i(1) = \sum_{i=1}^{r} n_i\chi_i(g) = 1 + \sum_{i=2}^{r} n_i\chi_i(g)$$

$$\iff -\frac{1}{p} = \sum_{i=2}^{r} \frac{n_i\chi_i(g)}{p}$$

Από την τελευταία ισότητα, καθώς ο $-1/p$ δεν είναι αλγεβρικός ακέραιος, έπεται ότι υπάρχει ένας $j = 2, 3, \ldots, r$, τέτοιος ώστε ο αριθμός $n_j\chi_j(g)/p$ να μην είναι αλγεβρικός ακέραιος και αφού ο ο $\chi_j(g)$ είναι αλγεβρικός ακέραιος, παίρνουμε ότι ο p δεν διαιρεί τον $n_j = \chi_j(1)$. Συνεπώς, είναι $\gcd(\#\overline{g}, \chi_j(1)) = 1$ και $\chi_j(g) \neq 0$, καθώς $n_j\chi_j(g)/p \notin \mathbf{Z}^{alg}$. Από το Πόρισμα 4.3.4., παίρνουμε το ζητούμενο. □

Θεώρημα 4.3.1 (Burnside). *Έστω G πεπερασμένη ομάδα με $\#G = p^a q^b$ για κάποιους πρώτος p, q και φυσικούς a, b. Τότε η G είναι επιλύσιμη.*

Απόδειξη : Με επαγωγή, μπορώ να υποθέσω ότι κάθε τέτοια ομάδα μικρότερης τάξης είναι επιλύσιμη. Επίσης, μπορώ να υποθέσω ότι $p \neq q$, αφού κάθε p-ομάδα είναι επιλύσιμη και ότι η G δεν είναι αβελιανή, αφού κάθε αβελιανή ομάδα είναι επιλύσιμη. Υπό αυτές τις προϋποθέσεις, θα δείξω ότι η G περιέχει μια μη τετριμμένη κανονική υποομάδα N και άρα από την επαγωγική υπόθεση οι ομάδες N και G/N είναι επιλύσιμες, άρα έπεται ότι και η G είναι επιλύσιμη. Έστω H μια q-Sylow υποομάδα της G, τότε η H, σαν q-υποομάδα, έχει μη τετριμμένο κέντρο. Επιλέγω, ένα $g \in Z(H)$ με $g \neq 1$ και θεωρώ την κεντροποιούσα $\mathcal{C}(g)$. Παρατηρώ ότι $H \subseteq \mathcal{C}(g)$ και άρα

$$\#\overline{g} = \frac{\#G}{\#\mathcal{C}(g)} = p^k$$

για κάποιο $k \leq a$ Αν $k = 0$, τότε $g \in Z(G)$ και άρα η $Z(G)$ είναι μια μη τετριμμένη κανονική υποομαάδα. An $k \geq 1$, από την Πρόταση 4.3.12., υπάρχει ένα $\mathbf{C}G$-πρότυπο V με $Z(V) \neq 1$. Αν $Z(V) \neq G$, τότε τελείωσα, αν $Z(V) = G$, καθώς η G δεν είναι αβελιανή, υπάρχουν στοιχεία $g, h \in G$ με $ghg^{-1}h^{-1} \neq 1$, αλλά καθώς $ghg^{-1}h^{-1} \in Z(V)$ παίρνω ότι το στοιχείο $ghg^{-1}h^{-1}$ ανήκει στο πυρήνα της αναπαράστασης $\varrho : G \to GL(V)$ και άρα στην περίπτωση αυτή, ο πυρήνας $\ker \varrho$ είναι η ζητούμενη μη τετριμμένη κανονική υποομάδα. $\square$

ΚΕΦΑΛΑΙΟ 5

Primitive Δακτύλιοι και Θεώρημα πυκνότητας του Jacobson.

Έστω R ένας δακτύλιος, τότε είναι εύκολο να δειχθεί η εξής ισοδυναμία :

$$\begin{array}{c} R \text{ είναι αριστερά του Artin} \\ + \\ R \text{ είναι απλός} \end{array} \longleftrightarrow \begin{array}{c} R \text{ είναι αριστερά του Artin} \\ + \\ R \text{ έχει ένα πιστό και} \\ \text{απλο } R\text{-πρότυπο } M \end{array}$$

Στο κεφάλαιο αυτό θα αφαιρέσουμε την συνθήκη φθίνουσας άλυσης και θα μελετήσουμε τους δακτύλιους R που έχουν ένα πιστό και απλό R-πρότυπο, αλλά όχι αναγκαστικά του Artin. Τέτοιοι δακτύλιοι καλούνται primitive. Οι primitive δακτύλιοι, παίζουν ανάλογο ρόλο με τους απλούς δακτύλιος, αποτελούν δηλαδή τα δομικά στοιχεία άλλων δακτυλίων.

5.1 Primitive Δακτύλιοι και Primitive Ιδεώδη

Ορισμός 5.1.1. *Έστω R ένας δακτύλιος, M ένα R-πρότυπο και $\ell : R \to \mathrm{End}(M, +)$ ο ομομορφισμός δακτύλιων που δίνει την δομή R-προτύπου στην αβελιανή ομάδα $(M, +)$. Ο πυρήνας του ομομορφισμού*

$$ann_R M = \ker[R \xrightarrow{\ell} \mathrm{End}(M, +)]$$

καλείται ο μηδενιστής του R-προτύπου M. Το R-πρότυπο M καλείται πιστό, αν ο $\ell : R \to \mathrm{End}(M, +)$ είναι μονομορφισμός, δηλαδή $ann_R M = 0$.

Ορισμός 5.1.2. *Αν $I \subseteq R$ ένα αριστερό ιδεώδες και M ένα R-πρότυπο, τότε*

$$IM = \left\{ \sum_{i=1}^{n} r_i m_i : n \in \mathbf{N},\ r_i \in I,\ m_i \in M \right\}$$

είναι ένα R-πρότυπο.

Πρόταση 5.1.1. *Ο R είναι Jacobson ημιαπλός αν και μόνο αν υπάρχει ένα πιστό ημιαπλό R-πρότυπο*

Απόδειξη : $(i) \to (ii)$: Θεωρώ ένα σύνολο αντιπροσώπων όλων των απλών R- προτύπων $(M_\lambda)_\lambda$ και θέτω $M = \bigoplus_\lambda M_\lambda$. Το M είναι ημιαπλό και αν $r \in R$ με $rM = 0$, τότε $rM_\lambda = 0$ για κάθε λ και άρα $r \in ann_R N$ για κάθε απλό R-πρότυπο N. Συνεπώς $r \in J(R) = 0$, οπότε το M είναι και πιστό.

$(ii) \to (i)$: Έστω M ένα πιστό ημιαπλό R-πρότυπο και $r \in J(R)$. Ως ημιαπλό R-πρότυπο, το M είναι το ευθύ άθροισμα απλών R-προτύπων. Καθώς τα στοιχεία του $J(R)$ μηδενίζουν τα απλά R-πρότυπα, είναι $rM = 0$. Συνεπώς $r \in ann_R M = 0$ $\square$

Ορισμός 5.1.3. *Ο δακτύλιος R καλείται αριστερά (δεξιά) primitive αν υπάρχει ένα πιστό απλό αριστερό (δεξί) R-πρότυπο M.*

Ορισμός 5.1.4. *Ένα ιδεώδες $I \subseteq R$ καλείται αριστερά (δεξία) primitive αν ο δακτύλιος πηλίκο R/I είναι αριστερά (δεξία) primitive.*

Πρόταση 5.1.2. *Το ιδεώδες $I \subseteq R$ είναι αριστερά primitive αν και μόνο αν $I = ann_R M$, για κάποιο απλό αριστερό R-πρότυπο M.*

Απόδειξη : $(i) \to (ii)$: Έστω $I \subseteq R$ ένα αριστερά primitive ιδεώδες, ο δακτύλιος R/I είναι αριστερά primitive, δηλαδή υπάρχει ένα πιστό απλό R/I-πρότυπο M. Έστω $\ell : R/I \to \mathrm{End}(M,+)$ ο αντίστοιχος μονομορφισμός. Τότε η σύνθεση :

$$R \xrightarrow{\pi} R/I \xhookrightarrow{\ell} \mathrm{End}(M,+)$$

επάγει την δομή ενός R-προτύπου με πυρήνα $ann_R M = \ker(\ell \circ \pi) = I$.

$(ii) \to (i)$: Αν $I = ann_R M$ για κάποιο απλό R-πρότυπο M, τότε μπορώ να παραγοντοποιήσω τον κανονικό ομομορφισμό $\ell : R \to \mathrm{End}(M,+)$, μέσω της απεικόνισης πηλίκο $\pi : R \to R/I$. Με λίγα λόγια, αφού $I = ann_R M = \ker \ell$, το 1ο θεώρημα ισομορφισμών επάγει έναν μονομορφισμό $\bar{\ell} : R/I \to \mathrm{End}_{\mathbf{Z}} M$, ισοδύναμα ένα πιστό απλό R/I-πρότυπο. □

Παρατήρηση. $J(R) = \bigcap\{ann_R M : M \text{ απλό } R\text{-πρότυπο}\} = \bigcap\{I : I \subseteq R \text{ ιδεώδες αριστερά primitive}\}$

Παραδείγματα. (i) *Δεν καθόλου εύκολο, αλλά είναι αλήθεια ότι υπάρχουν αριστερά primitive δακτύλιοι που δεν είναι δεξιά primitive. Ο G.H. Bergman έδωσε το πρώτο παράδειγμα το 1964 (οταν ήταν ακόμα προπτυχιακός!)*

(ii) *Οι μεταθετικοί primitive δακτύλιοι είναι ακριβώς τα σώματα. Πράγματι, αν ο R είναι ένας μεταθετικός primitive δακτύλιος, θεωρώ έναν απλό πιστό R-πρότυπο M. Είναι $M = R/m$ για κάποιο μεγιστικό ιδεώδες $m \subseteq R$ και άρα $ann_R M = ann_R(R/m) = m$. Συνεπώς $m = 0$ και άρα το $R = R/0 = R/m$ είναι σώμα.*

(iii) *Αν ο R είναι αριστερά primitive, τότε $J(R) = 0$. Πράγματι, αφού ο R είναι αριστερά primitive αν και μόνο αν έχει ένα απλό και πιστό R-πρότυπο, ειδικότερα έχει ένα ημιαπλό και πιστό R-πρότυπο και γνωρίζουμε ότι οι Jacobson ημιαπλοί δακτύλιοι είναι ακριβώς αυτοί που έχουν ένα πιστό και ημιαπλό R-πρότυπο.*

(iv) *Θεωρώ ένα σώμα $\mathbf{F}$ και έναν $\mathbf{F}$-διανυσματικό χώρο V. Τότε ο δακτύλιος $R = \mathrm{End}_{\mathbf{F}} V$ είναι αριστερά primitive. Πράγματι, η αβελιανή ομάδα $(V,+)$ λαμβάνει με φυσιολογικό τρόπο την δομή ένος R-προτύπου $(f \cdot v := f(v))$ το οποίο είναι πιστό, αφού αν $f \in R$ με $f \cdot v = 0$ για κάθε $v \in V$, τότε $f \equiv 0$ και απλό, αφού για κάθε $v \in V/\{0\}$ έχουμε $V = Rv = \{f(v) : f \in R\}$*

(v) *Αν ο R είναι απλός, τότε ο R είναι αριστερά και δεξία primitive. Πράγματι, έστω M ένα απλό R-πρότυπο, τότε η κανονική απεικόνιση $\ell : R \to \mathrm{End}(M,+)$ είναι μονομορφισμός, καθώς ο πυρήνας $\ker \ell \subseteq R$ αποτελεί ιδεώδες. Δηλαδή κάθε απλό R-πρότυπο είναι και πιστό. Το λήμμα του Zorn, εγγυείται μεγιστικά αριστερά και δεξία ιδεώδη και άρα τα αντίστοιχα πηλίκα αποτελούν απλά R-πρότυπα.*

(vi) *Υπάρχουν primitive δακτύλιοι που δεν είναι απλοί. Πράγματι, έστω $\mathbf{F}$ σώμα και V ένας $\mathbf{F}$-διανυσματικός χώρος άπειρης διάστασης. Από το παραπάνω παράδειγμα, ο $R = \mathrm{End}_{\mathbf{F}} V$ είναι αριστερά primitive και ο R δεν είναι απλός. Πράγματι, το σύνολο*

$$I = \{f \in R : \dim_{\mathbf{F}} \mathrm{im} f < \infty\}$$

είναι ένα αμφίπλευρο ιδεώδες του R.

Πρόταση 5.1.3. *Έστω R ένας αριστερά primitive δακτύλιος και $I \subseteq R$ ένα ελαχιστικό αριστερό ιδεώδες. Τότε ισχύουν τα εξής :*

(i) *$I = Re$, όπου $e^2 = e$ και άρα υπάρχει I' με $R = I \oplus I'$*

(ii) *Το R-πρότυπο I είναι πιστό και κάθε απλό και πιστό R-πρότυπο M είναι ισόμορφο με το I.*

(iii) *Υπάρχει ελαχιστικό δεξίο ιδεώδες $J \subseteq R$.*

(iv) *Ο R είναι δεξία primitive.*

Απόδειξη : Έστω M ένα απλό και πιστό R-πρότυπο.

(i) Υπάρχει $a \in I$ με $Ia \neq 0$. Πράγματι έστω ως προς άτοπο ότι $I^2 = 0$, δηλαδή $ab = 0$ για κάθε $a, b \in I$, τότε $0 = 0M = I^2M = I(IM)$, το IM είναι υποπρότυπο του M, αλλά το M είναι απλό και αφού $IM \neq 0$ (M πιστό), ισχύει ότι $IM = M$, οπότε $0 = I(IM) = IM = M$ #. Άρα υπάρχει $a \in I$ με $Ia \neq 0$, αφόυ I ελαχιστικό και $Ia \subseteq I$ είναι $Ia = I$, άρα υπάρχει $e \in I$ με $ea = a$. Παρατηρώ ότι $e^2a = ea = a$,άρα $(e^2 - e)a = 0$. Έστω $\mathfrak{a} = \{x \in I : xa = 0\} \subseteq I$. Το $\mathfrak{a}$ αποτελεί αριστερό ιδεώδες του R, οπότε $\mathfrak{a} = 0$ ή $\mathfrak{a} = I$. Όμως $e \in I \setminus \mathfrak{a}$ και άρα $\mathfrak{a} = 0$, αλλά $e^2 - e \in \mathfrak{a}$ συνεπώς $e^2 = e$. Από την ελαχιστικότητα του I, $I = Re$, είναι εύκολο να δειχθεί ότι $R = Re \oplus R(1 - e)$.

(ii) Έστω $r \in R$ με $rI = 0$. Τότε $0 = 0M = rIM = r(IM) = rM \Rightarrow r \in ann_R M = 0$. Συνεπώς το I είναι ένα πιστό R-πρότυπο. Έστω M' ένα απλό και πιστό R-πρότυπο, είναι $IM' = M' \neq 0$ και άρα υπάρχει $x' \in M'$ με $0 \neq Ix' \subseteq M$. Η απεικόνιση $f : I \to M'$ με $f(r) = rx \in M'$ για κάθε $r \in I$ είναι R-γραμμική και $\text{im} f = Ix' \neq 0$. Από το λήμμα του Schur, αφού έχω δύο απλά πρότυπα και ανάμεσα τους μια μη μηδενική R-γραμμική απεικόνιση, τα απλά πρότυπα είναι ισόμορφα.

(iii) Θεωρώ $a \in I$ με $a \neq 0$. Τότε $I = Ra$, θα δείξω ότι το $J = aR$ είναι ένα ελαχιστικό (δεξί) ιδεώδες, δηλαδή για κάθε $r \in R$ με $ar \neq 0$ είναι $J \stackrel{!}{=} arR$. Για την (!) αρκεί να δείξω ότι $a \in arR$, ισχυρίζομαι ότι υπάρχει $s \in R$ με $arsar \neq 0$. Αν $arsar = 0$ για κάθε $s \in R$, τότε $0 = 0M = (arRar)M = ar(Rar)M = ar((Rar)M) = arM$ #. Συνεπώς, υπάρχει $s \in S$ με $arsar \neq 0$. Θεωρώ την απεικόνιση $g : Ra \to Ra$ με $g(x) = xrsa \in Ra$. Η g είναι προφανώς R-γραμμική και $g(a) = arsa \neq 0$. Από το λήμμα του Schur, είναι ισομορφισμός και άρα ορίζεται η g^{-1}. Υπολογίζω $a = g^{-1}(g(a)) = g^{-1}(arsa) = arsg^{-1}(a) \in arR$.

(iv) Το δεξιό R-πρότυπο J είναι απλό, Θα δείξουμε ότι είναι πιστό. Έστω, ως προς άτοπο, υπάρχει $r \in R \setminus \{0\}$ με $Jr = 0$, δηλαδή $J \cdot Rr$ και άρα $RJRr = 0$. Θεωρώ ένα πιστό απλό R-πρότυπο M και έχω $0 = (RJRr)M = (RJ)(Rr)M = (RJ)M$ άτοπο, καθώς $RJ \neq 0$. □

Πόρισμα 5.1.1. *Τα ακόλουθα είναι ισοδύναμα για τον δακτύλιο R :*

(i) *ο R είναι αριστερά primitive και έχει ένα ελαχιστικό αριστερό ιδεώδες.*

(ii) *ο R είναι δεξία primitive και έχει ένα ελαχιστικό δεξί ιδεώδες.*

Παράδειγμα. (i) *Ο δακτύλιος $R = \text{End}_{\mathbf{F}} V$, όπου $\mathbf{F}$ σώμα και V ένας $\mathbf{F}$-διανυσματικός χώρος είναι δεξία primitive. Πράγματι, αρκεί να δειχθεί ότι έχει ένα ελαχιστικό δεξί ιδεώδες $I \subseteq R$. Θεωρώ έναν διανυσματικό υπόχωρο $U \subseteq V$ και $v \in V \setminus \{0\}$ ώστε $V = U \oplus \mathbf{F}v$. Τότε θα δείξω ότι το*

$$I = \{f \in R : f\big|_U = 0\} \subseteq R$$

είναι ένα ελαχιστικό δεξί ιδεώδες. Πρέπει να δείξω ότι για κάθε $f \in I \setminus \{0\}$ είναι $I = Rf$. Αρχικά παρατηρώ ότι $f(v) \neq 0$, τότε αν $g \in I$, μπορώ να βρω $h : V \to V$ με $h(f(v)) = g(v)$. Τότε είναι $g = h \circ f$, καθώς $g|_U = (h \circ f)|_U = 0$ και $g(v) = (h \circ f)(v)$. Συνεπώς $g \in Rf$.

5.1.1 Ημιευθέα γινόμενα Primitive Δακτυλίων

Ορισμός 5.1.5. *Έστω R ένας δακτύλιος και $\{R_i\}_{i\in I}$ μια οικογένεια δακτυλίων. Λέμε ότι ο R είναι το ημιευθές γινόμενο της οικογένειας $\{R_i\}_{i\in I}$ αν υπάρχει ένας μονομορφισμός δακτυλίων $\alpha : R \to \prod_i R_i$, τέτοιος ώστε για κάθε προβολή $\pi_j : \prod_i R_i \to R_j$, η σύνθεση $\pi_j \circ \alpha : R \to R_j$ να είναι επιμορφισμός δακτυλίων.*

$$\begin{tikzcd} R \arrow[r, hook, "\alpha"] \arrow[rr, bend right, two heads, "\pi_j\circ\alpha"'] & \prod_{i\in I} R_i \arrow[r, two heads, "\pi_j"] & R_j \end{tikzcd}$$

Πρόταση 5.1.4. *Τα επόμενα είναι ισοδύναμα για έναν δακτύλιο R :*

(i) *Ο R είναι Jacobson Ημιαπλός*

(ii) *Ο R είναι το ημιευθές γινόμενο primitive δακτυλίων.*

Απόδειξη : $(i) \to (ii)$: Αφού ο R είναι Jacobson ημιαπλός, υπάρχει μια συλλογή $\{M_i\}_{i\in I}$ απλών R-προτύπων, τέτοια ώστε $\bigcap_i ann_R M_i = 0$. Θέτω $R_i := R/ann_R M_i$ και προφανώς για κάθε $i \in I$, τα M_i είναι απλά και πιστά R_i-πρότυπα, δηλαδή οι δακτύλιοι R_i είναι αριστερά primitive. Παρατηρώ ότι η φυσική απεικόνιση $\alpha : R \to \prod_i R_i$ είναι μονομορφισμός. Πράγματι, αν $r + ann_R M_i = 0$ για κάθε i, τότε $r \in \bigcap_i ann_R M_i = 0$, συνεπώς $r = 0$. Τέλος, για κάθε $j \in I$, η σύνθεση $\pi_j \circ \alpha : R \to R_j$ δεν είναι τίποτα άλλο από την απεικόνιση πηλίκο $R \longrightarrow R/ann_R M_j$ και άρα είναι προφανώς επί.

$(ii) \to (i)$ Έστω ότι ο R είναι το ημιευθές γίνομενο μιας οικογένειας $\{R_i\}_{i\in I}$, όπου κάθε δακτύλιος R_i είναι αριστερά primitive. Για κάθε $i \in I$, υπάρχει ένα πιστό και απλό R_i-πρότυπο M_i. Ο μονομορφισμός $\varphi_i := \pi_i \circ \alpha : R \to \prod_{i\in I} R_i$ επάγει σε κάθε R_i-πρότυπο την δομή ενός R-προτύπου με μηδενιστή :

$$ann_R M_i = \ker[R \overset{\varphi_\iota}{\twoheadrightarrow} R_j \overset{\ell_\iota}{\hookrightarrow} \mathrm{End}_{\mathbf{Z}} M_i] = \ker[R \overset{\varphi_i}{\twoheadrightarrow} R_i]$$

το οποίο είναι και απλό, αφού για κάθε $x \in M \setminus \{0\}$, είναι $R \cdot x = \varphi_i(R)x = R_i x = M$. Τέλος, ισχύει ότι $\bigcap_{j\in I} ann_R M_j = 0$. Πράγματι, αν υπάρχει $x \in \bigcap_{j\in I} ann_R M_j$, τότε $\pi_j \circ \alpha(x) = 0$ για κάθε $j \in I$, ισοδύναμα $\alpha(x) = 0$ και αφου ο $\alpha : R \to \prod_i R_i$ είναι μονομορφισμός, έχουμε $x = 0$. Τα M_j είναι απλά και άρα

$$J(R) = \bigcap_{M \text{ απλό}} ann_R M \subseteq \bigcap_{j\in I} ann_R M_j = 0$$

δηλαδή ο R είναι Jacobson Ημιαπλός. □

Παρατήρηση. *Ένας μεταθετικός δακτύλιος R είναι Jacobson ημιαπλός αν και μόνο αν είναι το ημιευθές γινόμενο σωμάτων. Άμεσο, αφού οι μεταθετικοί primitive δακτύλιοι είναι ακριβώς τα σώματα.*

5.2 Θεώρημα Πυκνότητας του Jacobson

Έστω R ένας δακτύλιος και $X \subseteq R$ ένα αυθαίρετο σύνολο. Ορίζω τον μεταθέτη του συνόλου X

$$X' := \{r \in R : rx = xr \text{ για κάθε } x \in X\}$$

και με την σειρά του, τον διμεταθέτη $X'' := (X')' = \{s \in R : sx' = x's \text{ για κάθε } x' \in X'\}$[1]. Ισχύει προφανώς ότι $X \hookrightarrow X''$ και το ερώτημα που μας ενδιαφέρει είναι : Πόσο χώρο καταλαμβάνει το σύνολο X, μέσα στον διπλό μεταθέτη του; [2] Το Θεώρημα πυκνότητας του Jacobson, απαντάει ένα τέτοιο είδους ερώτημα. Έστω R ένας δακτύλιος, με ένα πιστό και απλό R-πρότυπο M. Έχω την ένθεση $R \hookrightarrow \mathrm{End}_{\mathbf{Z}} M$, θέτω $S = \mathrm{End}_R M$ και θεωρώ τους μεταθέτες

$$R' = \{f \in \mathrm{End}_{\mathbf{Z}} M : f(r \cdot x) = r \cdot f(x) \text{ για κάθε } r \in R\} = \mathrm{End}_R M$$

$$R'' = \{f \in \mathrm{End}_{\mathbf{Z}} M : f(g \cdot x) = g \cdot f(x) \text{ για κάθε } g \in \mathrm{End}_R M\} = \mathrm{End}_S M$$

τότε εφοδιάζοντας το πρότυπο M με την διακριτή τοπολογία, το Θεώρημα πυκνότητας του Jacobson μας λέει ότι ο R είναι πυκνός στον R'' ως προς την αντιστοιχή τοπολογία γινόμενο του M^M.

Πρόταση 5.2.1. *Έστω $\Bbbk$ ένας δακτύλιος και M, N δύο $\Bbbk$-πρότυπα. Εφοδιάζω το N με την διακριτή τοπολογία και το γινόμενο $N^M = \{f : M \to N : f \text{ απεικόνιση}\}$ με την αντίστοιχη τοπολογία γινόμενο, τότε ο υπόχωρος $\mathrm{Hom}_\Bbbk(M, N) = \{f : M \to N : f \text{ είναι } \Bbbk\text{-γραμμική}\} \subseteq N^M$ είναι κλειστός.*

Απόδειξη : Έστω $(f_\lambda)_\lambda$ ένα δίκτυο στο $\mathrm{Hom}_\Bbbk(M, N)$ και $f \in N^M$, ώστε $\lim_\lambda f_\lambda = f$. Θα δείξω ότι f είναι $\Bbbk$-γραμμική, δηλαδή $f(x + y) = f(x) + f(y)$ και $f(rx) = rf(x)$ για κάθε $r \in \Bbbk$ και $x, y \in M$. Ισχύει ότι $\lim_\lambda f_\lambda = f$ αν και μόνο αν $\lim_\lambda f_\lambda(x) = f(x)$ για κάθε $x \in M$. Συνεπώς, σταθεροποιώ $x, y \in M$ και $r \in \Bbbk$. Αφού η τοπολογία του N είναι η διακριτή, κάθε συγκλίνον δίκτυο είναι τελικά σταθερό, άρα υπάρχει $\lambda_1 \in \Lambda$ τέτοιο ώστε για κάθε $\lambda \geq \lambda_1$ $f_\lambda(x) = f_{\lambda_1}(x)$. Αντίστοιχα, υπάρχει $\lambda_2 \in \Lambda$ τέτοιο ώστε $f_\lambda(y) = f_{\lambda_2}(y)$ για κάθε $\lambda \geq \lambda_2$, υπάρχει $\lambda_3 \in \Lambda$ τέτοιο ώστε $f_\lambda(x + y) = f_{\lambda_3}(x + y)$ για κάθε $\lambda \geq \lambda_3$ και υπάρχει $\lambda_4 \in \Lambda$ τέτοιο ώστε $f_\lambda(rx) = f_{\lambda_4}(rx)$ για κάθε $\lambda \geq \lambda_4$. Άρα για κάθε $\lambda \geq \lambda_1, \lambda_2, \lambda_3, \lambda_4$ είναι :

$$f_\lambda(x) = f(x), \;\; f_\lambda(y) = f(y), \;\; f_\lambda(x + y) = f(x + y), \;\; f_\lambda(rx) = f(rx)$$

οπότε $f(x + y) = f_\lambda(x + y) = f_\lambda(x) + f_\lambda(y) = f(x) + f(y)$ και $f(rx) = f_\lambda(rx) = rf_\lambda(x) = rf(x)$ □

Παρατηρήσεις. *(i) Το σύνολο $X \subseteq \mathrm{Hom}_\Bbbk(M, N)$ είναι πυκνό αν και μόνο αν για κάθε $f \in \mathrm{Hom}_\Bbbk(M, N)$, για κάθε $n \in \mathbf{N}$ και για κάθε $m_1, \ldots, m_n \in M$, υπάρχει $g \in X$ ώστε $g(m_i) = f(m_i)$ για κάθε $i = 1, 2, \ldots, n$. Πράγματι το σύνολο $X \subseteq \mathrm{Hom}_\Bbbk(M, N)$ είναι πύκνο αν και μόνο αν τέμνει κάθε ανοιχτό υποσύνολο του $\mathrm{Hom}_\Bbbk(M, N)$ ισοδύναμα τέμνει κάθε στοιχείο της βάσης. Τα στοιχεία της βάσης είναι ακριβώς τα*

$$\{g \in \mathrm{Hom}_\Bbbk(M, N) : g(m_i) = f(m_i) \;\; i = 1, 2, \ldots, n\}$$

όπου $f \in \mathrm{Hom}_\Bbbk(M, N)$ και $m_1, \ldots, m_n \in M$

[1] Η σχέση $(*)'$ είναι μια κλειστή σχέση, με την έννοια του ότι $X' = X'''$ για κάθε σύνολο X. Πράγματι, ισχύει προφανώς ότι $X' \subseteq (X')'' = X'''$. Για την αντίθετη κατεύθυνση, παρατηρώ ότι για τυχαία σύνολα X, Y με $X \subseteq Y$, ισχύει $X' \supseteq Y'$. Συνεπώς, αφού $X \subseteq X''$, παίρνω $X' \supseteq X'''$

[2] Μια παρατήρηση είναι ότι ο διπλός μεταθέτης είναι υποδακτύλιος, οπότε αν το X δεν είναι δακτύλιος δεν έχουμε ελπίδα για ισότητα.

(ii) Αν το $\Bbbk$-πρότυπο M είναι πεπερασμένα παραγόμενο, τότε η τοπολογία $\mathrm{Hom}_{\Bbbk}(M,N) \subseteq N^M$ είναι η διακριτή. Πράγματι, θα δείξω ότι για κάθε $f \in \mathrm{Hom}_{\Bbbk}(M,N)$ το μονοσύνολο $\{f\}$ είναι ανοιχτό. Έστω $M = \sum_{i=1}^n \Bbbk m_i$, τότε είναι

$$\mathrm{Hom}_{\Bbbk}(M,N) \cap \{g \in N^M : g(m_i) = f(m_i) \;\; i = 1,2,\ldots,n\}$$

$$= \{g \in \mathrm{Hom}_{\Bbbk}(M,N) : g(m_i) = f(m_i) \;\; i = 1,2,\ldots,n\} = \{f\}$$

Συνεπώς αν $X \subseteq \mathrm{Hom}_{\Bbbk}(M,N)$ ένα πυκνό σύνολο, τότε $X = \mathrm{Hom}_{\Bbbk}(M,N)$.

Παράδειγμα. *Έστω $\mathbf{F}$ σώμα, V ένας απειροδιάστατος $\mathbf{F}$-διανυσματικός χώρος και $R = \mathrm{End}_{\mathbf{F}}V$. Το ιδεώδες*

$$I = \{f \in R : \dim \mathbf{im} f < \infty\}$$

είναι πυκνό. Πράγματι, για κάθε $h : V \to V$ και κάθε πεπερασμένο σύνολο $\{v_1,\ldots,v_n\} \subseteq V$ υπάρχει $f \in I$ με $f(v_i) = h(v_i)$ για κάθε $i = 1,2,\ldots,n$.

Λήμμα 5.2.1. *Έστω V ένα ημιαπλό R-πρότυπο, $\Bbbk = \mathrm{End}_R V$ και $E = \mathrm{End}_{\Bbbk} V$. Τότε το $U \subseteq V$ είναι ένα R-υποπρότυπο αν και μόνο αν το $U \subseteq V$ είναι ένα E-υποπρότυπο.*

Απόδειξη : ($\Rightarrow$) Έστω ότι το $U \subseteq V$ είναι ένα R-υποπρότυπο. Αφού, το V είναι ημιαπλό, υπάρχει R-υποπρότυπο $U' \subseteq V$, τέτοιο ώστε $V = U \oplus U'$. Θεωρώ την R-γραμμική απεικόνιση $p : V \to V$ με $p(u + u') = u$ για κάθε $u \in U$ και $u' \in U'$, άρα $p|_U = 1_U$ και $\mathrm{im}p \subseteq U$. Έστω $t \in E$, παρατηρώ ότι $p \in \mathrm{End}_R V = \Bbbk$ και άρα $t \circ p = t \circ p : V \to V$. Συνεπώς, για κάθε $u \in U$ είναι $t(u) = t(p(u)) = p(t(u)) \in U$.

($\Leftarrow$) Προφανές, αφού υπάρχει ομομορφισμός δακτυλίων $R \to E$. □

Θεώρημα 5.2.1 (Θεώρημα Πυκνότητας του Jacobson). *Έστω R ένας δακτύλιος, V ένα ημιαπλό R-πρότυπο και $\Bbbk = \mathrm{End}_R V$. Τότε ο ομομορφισμός $\varrho : R \to \mathrm{End}_{\Bbbk} V$ με $\varrho(r) = (x \longmapsto rx) \in \mathrm{End}_{\Bbbk} V$ έχει πυκνή εικόνα. Συνεπώς για κάθε $\Bbbk$-γραμμική $f : V \to V$ και κάθε $v_1,\ldots,v_n \in V$, υπάρχει $r \in R$ με $f(v_i) = r \cdot v_i$.*

Απόδειξη : Έστω $f \in \mathrm{End}_{\Bbbk} V$ και $v_1,\ldots,v_n \in V$. Πρέπει να δείξω ότι

$$\mathrm{im}\varrho \cap \{g \in \mathrm{End}_{\Bbbk} V : g(v_i) = f(v_i) \text{ για } i = 1,2,\ldots,n\} \neq \varnothing$$

Θεωρώ το R-πρότυπο $V^n = \{(x_1,\ldots,x_n)^T : x_i \in V,\ i = 1,2,\ldots,n\}$ και παρατηρώ ότι το V^n ένα είναι ημιαπλό R-πρότυπο. Είναι $\mathrm{End}_R V^n = \mathrm{End}_R(\bigoplus_{i=1}^n V) \simeq \mathbf{M}_n(\mathrm{End}_R V) = \mathbf{M}_n(\Bbbk)$. Θεωρώ την απεικόνιση $\varphi : V^n \to V^n$ με

$$\varphi \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} f(x_1) \\ \vdots \\ f(x_n) \end{pmatrix} \text{ για κάθε } \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in V^n$$

Ισχυρίζομαι ότι $\varphi \in \mathrm{End}_{\mathbf{M}_n(\Bbbk)} V^n$. Πράγματι, αν $A = (a_{i,j}) \in \mathbf{M}_n(\Bbbk)$, δηλαδή η $a_{i,j} : V \to V$ είναι R-γραμμική και $f \circ a_{i,j} = a_{i,j} \circ f$ για κάθε i,j. Σταθεροποιώ $(x_1,\ldots,x_n)^T \in V^n$ και υπολογίζω

$$\varphi\left(A \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \right) = \varphi \begin{pmatrix} \sum_j a_{1,j}x_j \\ \sum_j a_{2,j}x_j \\ \vdots \\ \sum_j a_{n,j}x_j \end{pmatrix} = \begin{pmatrix} f(\sum_j a_{1,j}x_j) \\ f(\sum_j a_{2,j}x_j) \\ \vdots \\ f(\sum_j a_{n,j}x_j) \end{pmatrix} = \begin{pmatrix} \sum_j (f \circ a_{1,j})x_j \\ \sum_j (f \circ a_{2,j})x_j \\ \vdots \\ \sum_j (f \circ a_{n,j})x_j \end{pmatrix}$$

$$\stackrel{!}{=} \begin{pmatrix} \sum_j a_{1,j} f(x_j) \\ \sum_j a_{2,j} f(x_j) \\ \vdots \\ \sum_j a_{n,j} f(x_j) \end{pmatrix} = A \cdot \begin{pmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_n) \end{pmatrix} = A \cdot \varphi \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

Από το προηγούμενο λήμμα, για το ημιαπλό R-πρότυπο V^n γνωρίζω ότι κάθε R-υποπρότυπο είναι οπωσδήποτε $\mathrm{End}_{\mathbf{M}_n(\Bbbk)} V^n$-αναλλοίωτο και άρα φ-αναλλοίωτο. Θεωρώ $U = R \cdot (v_1, \ldots, v_n)^T \subseteq V^n$ και έχω ότι $\varphi(U) \subseteq U$. Ειδικότερα, είναι

$$\begin{pmatrix} f(v_1) \\ \vdots \\ f(v_n) \end{pmatrix} = \varphi \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \varphi(U) \subseteq U = R \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Συνεπώς, υπάρχει $r \in R$ με

$$\begin{pmatrix} f(v_1) \\ \vdots \\ f(v_n) \end{pmatrix} = r \cdot \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \iff f(v_i) = r \cdot v_i \text{ για κάθε } i = 1, 2, \ldots, n$$

□

Θεώρημα 5.2.2 (Θεώρημα δομής των αριστερά primitive δακτυλίων). *Έστω R ένας αριστερά primitive δακτύλιος, V ένα απλό και πιστό R-πρότυπο και $\Bbbk = \mathrm{End}_R V$ (ο $\Bbbk$ είναι διαιρετικός δακτύλιος από το λήμμα του Schur), τότε :*

- (i) *ο R είναι ένας πυκνός υποδακτύλιος του $\mathrm{End}_\Bbbk V$*
- (ii) *Αν $\dim_\Bbbk V = n < \infty$, τότε είναι $R = \mathrm{End}_\Bbbk V \simeq \mathbf{M}_n(\Bbbk^{op})$*
- (iii) *Αν $\dim_\Bbbk V = \infty$, τότε για κάθε $n \in \mathbf{N}$, υπάρχει υποδακτύλιος $R_n \subseteq R$, ώστε ο οποίος να επιδέχεται έναν επιμορφισμό $R_n \longrightarrow \mathbf{M}_n(\Bbbk^{op})$.*

Τέλος, είναι $\dim_\Bbbk V < \infty$ αν και μόνο αν ο R είναι του Artin.

Απόδειξη : (i) Δείξαμε ότι ο ομομορφισμός $\varrho : R \to \mathrm{End}_\Bbbk V$ έχει πυκνή εικόνα και και ο ϱ είναι 1-1, αφού το V είναι πιστό.

(ii) Αν $\dim_\Bbbk V < \infty$, τότε $\Bbbk$-πρότυπο V είναι πεπερασμένα παραγόμενο και άρα η τοπολογία στον $\mathrm{End}_\Bbbk V$ είναι η διακριτή. Καθώς ο R είναι πυκνός, έχουμε $R = \mathrm{End}_\Bbbk V = \mathrm{End}_\Bbbk(\Bbbk^n) = \mathbf{M}_n(\mathrm{End}_\Bbbk \Bbbk) \simeq \mathbf{M}_n(\Bbbk^{op})$

(iii) Αν $\dim_\Bbbk V = \infty$, επιλέγω γραμμικά ανεξάρτητα $v_1, v_2, v_3 \ldots$ και θέτω $V_n := \sum_{i=1}^n \Bbbk v_i \subseteq V$. Θεωρώ $R_n = \{r \in R : rV_n \subseteq V_n\}$ και $I_n = \{r \in R : rV_n = 0\} \subseteq R_n$. Παρατηρώ ότι

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq I_{n+1} \supseteq \ldots$$

Ισχύει στην πραγματικότητα $I_{n+1} \subsetneq I_n$ για κάθε n. Πράγματι, υπάρχει μια $\Bbbk$-γραμμική απεικόνιση $f : V \to V$ με $f(v_1) = f(v_2) = \cdots = f(v_n) = 0$ και $f(v_{n+1}) = v_{n+1}$. Λόγω πυκνότητας υπάρχει $r \in R$, τέτοια ώστε $r \cdot v_1 = r \cdot v_2 = \cdots = r \cdot v_n = 0$ και $r \cdot v_{n+1} = v_{n+1}$. Συνεπώς είναι $r \in I_n \setminus I_{n+1}$ και άρα ο R δεν είναι του Artin. Τέλος, παρατηρώ ότι η απεικόνιση $R_n \to \mathrm{End}_\Bbbk V_n$, όπου $r \longmapsto r|_{V_n}$ είναι επί. Πράγματι, αν $h : V_n \to V_n$ είναι μια $\Bbbk$-γραμμική απεικόνιση, τότε υπάρχει μια $\Bbbk$-γραμμική απεικόνιση $h' : V \to V$ με $h'(v) = h(v) \in V_n \subseteq V$ για κάθε $v \in V_n$. Λόγω πυκνότητας, υπάρχει $r \in R$ με $r \cdot v_i = h'(v_i) = h(v_i)$ για $i = 1, 2, \ldots, n$, δηλαδή είναι $r \cdot v_i \in V_n$ για κάθε $i = 1, 2, \ldots, n$

και άρα $r \cdot V_n \subseteq V_n$. Άρα $r \in R_n$ και $r|_{V_n} = h : V_n \to V_n$

Για τον τελευταίο ισχυρισμό, δείξαμε ότι αν $\dim_{\Bbbk} V = \infty$, τότε ο R δεν είναι του Artin. Διαφορετικά, είναι $R \simeq \mathbf{M}_n(\Bbbk^{op})$ και ο R είναι του Artin. □

Πρόταση 5.2.2 (Θεώρημα πυκνότητας του Jacobson). *Έστω R ένας δακτύλιος. Ο R είναι αριστερά primitive αν και μόνο αν υπάρχει διαιρετικός δακτύλιος $\Bbbk$ και $\Bbbk$-πρότυπο V, τέτοια ώστε ο R να είναι πυκνός υποδακτύλιος του δακτυλιού των ενδομορφισμών $\mathrm{End}_{\Bbbk} V$.*

Απόδειξη : Το ευθύ το δείξαμε, για το αντίστροφο : Το $\Bbbk$-πρότυπο V λαμβάνει την δομή ένος πιστού και απλού R-προτύπου. Πράγματι, το V είναι πιστό $\mathrm{End}_{\Bbbk} V$-προτύπο και άρα και πιστό R-πρότυπο. Για την απλότητα, έστω $v \in V \setminus \{0\}$, τότε $Rv = V$. Πράγματι, έστω $w \in V$, τότε υπάρχει μια $\Bbbk$-γραμμική[3] $g : V \to V$ με $g(v) = w$ και άρα από πυκνότητα υπάρχει μια $f \in R$ με $f \cdot v = f(v) = g(v) = w$ □

Ορισμός 5.2.1. *Έστω R υποδακτύλιος ενός δακτυλίου ενδομορφισμών $\mathrm{End}_{\Bbbk} V$, όπου $\Bbbk$ διαιρετικός και V ένα $\Bbbk$-πρότυπο. Ο δακτύλιος R καλείται n-μεταβατικός, αν για κάθε $m \leq n$, για γραμμικά ανεξάρτητα διανύσματα $v_1, \ldots, v_m$ και διανύσματα $w_1, \ldots, w_m$, υπάρχει $f \in R$ με $f(v_i) = w_i$ για κάθε $i = 1, 2, \ldots, m$.*

Παρατηρήσεις. (i) *Το θεώρημα δομής των αριστερά primitive δακτυλίων δίνει μια δεύτερη απόδειξη για το θεώρημα δομής των απλών δακτυλίων του Artin, δηλαδή αν R ένας απλός δακτύλιος του Artin, τότε υπάρχει διαιρετικός δακτύλιος D και φυσικός n, τέτοιοι ώστε $R \simeq \mathbf{M}_n(D)$.*

(ii) *Έστω R υποδακτύλιος ενός δακτυλίου ενδομορφισμών $\mathrm{End}_{\Bbbk} V$, όπου $\Bbbk$ διαιρετικός και V ένα $\Bbbk$-πρότυπο. Αν ο R είναι 1- μεταβατικός, τότε είναι αριστέρα primitive. Υπάρχουν όμως (primitive) δακτύλιοι $R \hookrightarrow \mathrm{End}_{\Bbbk} V$ που είναι 1-μεταβατικοί, αλλά όχι πυκνοί, ειδικότερα $\Bbbk \subsetneq \mathrm{End}_R V$. Πράγματι, έστω V ένας $\mathbf{C}$-διανυσματικός χώρος με $\dim_{\mathbf{C}} V = 2$, σταθεροποιώ μια βάση e_1, e_2 και θεωρώ τον αυτομορφισμό $\xi : V \to V$ με $\xi(e_1) = e_2$ και $\xi(e_2) = e_1$. Έστω η επέκταση δακτυλίων[4]*

$$\mathbf{C}[\xi] \hookrightarrow \mathrm{End}_{\mathbf{C}} V$$

Ο $\mathbf{C}[\xi]$ είναι προφανώς 1-μεταβατικός υποδακτύλιος, αλλά αποκλείεται να είναι πυκνός. Πράγματι, καθώς διαφορετικά, αφού $\dim_{\mathbf{C}} V < \infty$, θα είχα $\mathbf{C}[\xi] = \mathrm{End}_{\mathbf{C}} V$, δηλαδή κάθε $\mathbf{C}$-γραμμική $f : V \to V$ θα γραφόταν σαν $\sum_i a_i \xi^i$, ειδικότερα κάθε κάθε $\mathbf{C}$-γραμμική $f : V \to V$ θα ήταν διαγωνίσιμη, αφού η ξ είναι διαγωνίσιμη. $\#$.

(iii) *Έστω R υποδακτύλιος ενός δακτυλίου ενδομορφισμών $\mathrm{End}_{\Bbbk} V$, όπου $\Bbbk$ διαιρετικός και V ένα $\Bbbk$-πρότυπο. Τότε, τα επόμενα είναι ισοδύναμα :*

(α) Ο R είναι 2-μεταβατικός υποδακτύλιος του $\mathrm{End}_{\Bbbk} V$.

(β) Ο R είναι n-μεταβατικός υποδακτύλιος του $\mathrm{End}_{\Bbbk} V$ για κάθε n.

ειδικότερα, για έναν υποδακτύλιο R του $\mathrm{End}_{\Bbbk} V$, τα επόμενα είναι ισοδύναμα

(α') Για κάθε $g \in \mathrm{End}_{\Bbbk} V$ και $v_1, \ldots, v_n \in V$ υπάρχει $f \in R$ με $f(v_i) = g(v_i)$ για κάθε $i = 1, 2, \ldots, n$ (Ο R είναι πυκνός υποδακτύλιος του $\mathrm{End}_{\Bbbk} V$)

[3] Η θεωρία των προτύπων πάνω από σώματα (διανυσματικών χώρων) είναι σχεδόν ταυτόσιμη με την θεωρία των προτύπων πάνω από διαιρετικούς δακτυλίους. Αν το πιστέψουμε αυτό, άφοβα μπορούμε να πούμε ότι υπάρχει $\Bbbk$-γραμμική $g : V \to V$ με $g(v) = w$. Το μόνο που πρέπει κάποιος να προσέχει είναι η διαφορά ανάμεσα στους $\Bbbk$ και $\Bbbk^{op}$. Αν $\mathbf{F}$ ένα σώμα, τότε $\mathrm{End}_{\mathbf{F}} \mathbf{F}^n \simeq \mathbf{M}_n(\mathbf{F})$, αλλά πιο γενικά αν $\Bbbk$ διαιρετικός η φυσική αριστερή δράση του $\Bbbk$ στον ευατό του δεν είναι εν γένει $\Bbbk$-γραμμική, αλλά $\Bbbk^{op}$-γραμμική και άρα $\mathrm{End}_{\Bbbk} \Bbbk^n \simeq \mathbf{M}_n(\Bbbk^{op})$

[4] $\mathbf{C}[\xi] = \{\sum_{i=1}^n a_i \xi^i : n \in \mathbf{N},\ a_i \in \mathbf{C}\}$

(β') Για κάθε $g \in \mathrm{End}_{\Bbbk} V$ και $v_1, v_2 \in V$ υπάρχει $f \in R$ με $f(v_i) = g(v_i)$ για κάθε $i = 1, 2$

Έστω ότι R είναι 2-μεταβατικός υποδακτύλιος του $\mathrm{End}_{\Bbbk} V$. Καθώς $R \hookrightarrow \mathrm{End}_{\Bbbk} V$, τότε $\Bbbk \hookrightarrow \mathrm{End}_R V$. Έστω, ως προς άτοπο, ότι υπάρχει $f \in \mathrm{End}_R V \setminus \Bbbk$. Αρχικά, $f \neq 0$, καθώς $0 \in \Bbbk$ και αν σταθεροποιήσω $v \in V \setminus \{0\}$, αφού ο $\mathrm{End}_R V$ είναι διαιρετικός, έπεται ότι ο f είναι ισομορφισμός, άρα και $f(v) \neq 0$. Ισχυρίζομαι, ότι τα $v, f(v) \in V$ είναι γραμμικά ανεξάρτητα πάνω από το $\Bbbk$. Πράγματι, καθώς διαφορετικά, θα υπήρχε ένα $\lambda \in \Bbbk$ με $f(v) = \lambda \cdot v \Rightarrow (f - \lambda \cdot 1_V)(v) = 0$, όμως $f - \lambda \cdot 1_V \in \mathrm{End}_R V$ και θα ήταν $f = \lambda \cdot 1_V$, άτοπο. Αφού λοιπόω, τα $v, f(v) \in V$ είναι γραμμικά ανεξάρτητα, από την 2-μεταβατικότητα, υπάρχει $g \in R$ με $g(v) = 0$ και $g(f(v)) \neq 0$, αλλά αφού η f είναι R-γραμμική, έχω $0 = f(0) = f(g(v)) = g(f(v)) \neq 0$ #. Συνεπώς, $\Bbbk = \mathrm{End}_R V$

Παραδείγματα. (i) *Αν ο R είναι αριστερά primitive, τότε το κέντρο $Z(R)$ είναι ακέραια περιοχή. Πράγματι, έστω V το απλό και πιστό R-πρότυπο, τότε έχω τον μονομορφισμό $\varrho : R \hookrightarrow \mathrm{End}_{\mathbf{Z}} V$. Θεωρώ τον περιορισμό $\varrho' := \varrho|_{Z(R)}$ και στην πραγματικότητα είναι $\mathrm{im}\varrho' \subseteq \mathrm{End}_R V$. Όντως, έστω $r \in Z(R), r' \in R$ και $\varrho(r) = f_r = (x \mapsto rx)$, τότε $f_r(r'x) = rr'x = r'rx = r'f_r(x)$. Συνεπώς,*

$$Z(R) \hookrightarrow \mathrm{End}_R V$$

Ο δακτύλιος $\mathrm{End}_R V$ είναι διαιρετικός και άρα ο $Z(R)$ είναι ακέραια περιοχή σαν μεταθετικός υποδακτύλιος διαιρετικού δακτυλίου.

(ii) *Έστω R αριστερά primitive και V ένα απλό και πιστό R-πρότυπο, τότε ο R είναι διαιρετικός αν και μόνο αν για κάθε $r \in R$ και $v \in V$ με $r \cdot v = 0$, ισχύει ότι $r = 0$ ή $v = 0$.
Πράγματι, το ευθύ είναι προφανές, για το αντίστροφο θεωρώ τον διαιρετικό δακτύλιο $\Bbbk = \mathrm{End}_R V$ και γνωρίζουμε ότι ο R είναι πυκνός στον $\mathrm{End}_{\Bbbk} V$. Αρκεί να δείξουμε ότι $\dim_{\Bbbk} V = 1$, καθώς τότε $R \simeq \Bbbk^{op}$. Έστω, λοιπόν προς άτοπο ότι υπάρχουν δύο $\Bbbk$-γραμμικά ανεξάρτητα διανύσματα $v, w \in V$, τότε από πυκνότητα, υπάρχει $r \in R$, τέτοιο ώστε $rv = v$ και $rw = 0$. Από υπόθεση, είναι αναγκαστηκά $r = 0$, αλλά τότε $v = rv = 0$ #.*

(ii) *Έστω ο $\mathbf{Q}$-διανυσματικός χώρος $V = \mathbf{Q}[X]$ και θεωρώ τους $\mathbf{Q}$-ενδομορφισμούς*

$$D : f(X) \longmapsto f'(X)$$

$$I : f(X) \longmapsto \int f(X)\, dX$$

*παραγώγίσης και ολοκλήρωσης αντίστοιχα. Θεωρώ τον δακτύλιο $R = \mathbf{Q}\langle D, I\rangle \subseteq \mathrm{End}_{\mathbf{Q}} V$ που παράγεται από τα στοιχεία $I, D : V \to V$. Τότε το R είναι πυκνός υποδακτύλιος του $\mathrm{End}_{\mathbf{Q}} V$, συνεπώς ο R είναι αριστερά primitive με το V να είναι απλό και πιστό R-πρότυπο.
Είναι εύκολο να δειχθεί ότι ο R είναι 1-μεταβατικός. Από τα προηγούμενα, έχουμε ότι $\mathbf{Q} \hookrightarrow \mathrm{End}_R V$ και άρκει να δείξουμε ότι $\mathrm{End}_R V = \mathbf{Q}$, δηλαδή ότι για κάθε R-γραμμική $f : V \to V$, υπάρχει $q \in \mathbf{Q}$ με $f = q \cdot 1_V : V \to V$. Πράγματι, έστω $f : V \to V$ μια R-γραμμική, τότε $f(1) \in \mathbf{Q}$, καθώς $D(f(1)) = f(D(1)) = f(0) = 0$. Έστω, τώρα $n \geq 0$ φυσικός, τότε υπάρχει $a_n \in \mathbf{Q}$ τέτοιος ώστε για την $\varphi_n = a_n I^n \in R$ να είναι $\varphi_n(1) = X^N \in \mathbf{Q}[X]$. Συνεπώς :*

$$f(X^n) = f(\varphi_n(1)) = \varphi_n(f(1)) = f(1) \cdot \varphi_n(1) = f(1) \cdot X^n$$

άρα $f = q \cdot 1_V : V \to V$, όπου $q = f(1) \in \mathbf{Q}$

(iii) *Έστω* $V = \bigoplus_{i=1}^{\infty} \mathbf{Q}e_i$ *και ορίζω* $R \subseteq \mathrm{End}_{\mathbf{Q}} V$ *ως εξής :*

$$R = \left\{ \begin{pmatrix} A & & & 0 \\ & a & & \\ & & a & \\ 0 & & & \ddots \end{pmatrix} : A \in \mathbf{M}_n(\mathbf{Q}) \text{ για κάποιο } n \text{ και } a \in \mathbf{Z} \right\}$$

$$\equiv \{ f : V \to V : f \text{ είναι } \mathbf{Q}\text{-γραμμική και υπάρχει } a \in \mathbf{Z} \text{ ώστε τελικά } f(e_i) = ae_i \}$$

ο R *είναι πυκνός στον* $\mathrm{End}_{\mathbf{Q}} V$ *και άρα το* R*-πρότυπο* V *είναι απλό. Συνεπώς ο* R *είναι αριστερά primitive και* $Z(R) = \mathbf{Z} \cdot 1_V$.
Ο R *είναι προφανώς 1-μεταβατικός. Όπως και πριν, έχουμε* $\mathbf{Q} \hookrightarrow \mathrm{End}_R V$ *και άρκει να δείξουμε ότι* $\mathrm{End}_R V = \mathbf{Q}$. *Έστω λοιπόν μια* R*-γραμμική απεικόνιση* $f : V \to V$ *και σταθεροποιώ έναν φυσικό* $i \geq 1$. *Για κάθε άλλον φυσικό* $j \neq i$, *έστω* $\alpha_j \in \mathbf{Q}$ *ο συντελεστής του* e_j *στο* $f(e_j)$. *Θεωρώ την στοιχειώδη απεικόνιση* $E_{i,j} \in R$ *και τότε*

$$f(e_i) = (f \circ E_{i,j})(e_j) = (E_{i,j} \circ f)(e_j) = E_{i,j}(f(e_j)) = \alpha_j e_i$$

δηλαδή για κάθε $j \neq i$ *φυσικούς, έχουμε* $f(e_i) = a_j e_i$ *και άρα προφανώς* $a_j = a_{j'}$ *για κάθε* $j, j' \neq i$. *Για τον υπολογισμό του κέντρου* $Z(R)$, *γνωρίζουμε ότι* $Z(R) \hookrightarrow \mathrm{End}_R V = \mathbf{Q} \cdot 1_V$ *και αφού* $Z(R) \subseteq R$, *τότε αναγκαστικά* $Z(R) = \mathbf{Z} \cdot 1_V$.

(iv) *Έστω* $\mathbf{F} \hookrightarrow R$ *μια επέκταση δακτυλίων, όπου* $\mathbf{F}$ *σώμα (=:* $\mathbf{F}$*-άλγεβρα). Θεωρώ τον* $\mathbf{F}$*-διανυσματικό χώρο* $V = \bigoplus_{i \geq 1} Re_i$ *και υποδακτύλιο* $S \subseteq \mathrm{End}_{\mathbf{F}} V$

$$S = \mathbf{F}\langle f_r, g : r \in R \text{ και } \#\mathrm{supp}(g) < +\infty \rangle$$

όπου $f_r : V \to V$ *ο αριστερός πολλαπλασισμός με* $r \in R$ *και* $\mathrm{supp}(g) := \{n \geq 0 : g(e_n) \neq 0\}$ *ο φορέας της γραμμικής απεικόνισης* $g : V \to V$. *Τότε ο* S *είναι primitive και υπάρχει επιμορφισμός* $S \twoheadrightarrow R$. *Συνεπώς, κάθε* $\mathbf{F}$*-άλγεβρα είναι επιμορφική εικόνα primitive* $\mathbf{F}$*-άλγεβρας.*
Όπως και πριν, αρκεί $\mathrm{End}_S V = \mathbf{F}$. *Σταθεροποιώ έναν φυσικό* $i \geq 1$ *και θεωρώ πάλι τις στοιχειώδεις απεικονίσεις* $E_{i,j} : V \to V$ *για κάθε* $j \neq i$, *οι οποίες έχουν πεπερασμένο φορέα, τότε αν* $r_j \in R$ *ο συντελεστής του* e_j *στο* $f(e_j)$, *έχω*

$$f(e_i) = (f \circ E_{i,j})(e_j) = (E_{i,j} \circ f)(e_j) = E_{i,j}(f(e_j)) \overset{!}{=} r_j e_i$$

δηλαδή για κάθε $j \neq i$ *φυσικούς, έχουμε* $f(e_i) = a_j e_i$ *και άρα προφανώς* $r_j = r_{j'}$ *για κάθε* $j, j' \neq i$. *Υπάρχει ένας μοναδικός επιμορφισμός* $\mathbf{F}$*-αλγεβρών* $\Phi : S \twoheadrightarrow R$, *τέτοιος ώστε* $\Phi(f_r) = r$ *και* $\Phi(g) = 0$ *για κάθε* $g : V \to V$ *με πεπερασμένο φορέα.*

(v) *Έστω* R *αριστερά primitive δακτύλιος, τέτοιος ώστε*

$$a(ab - ba) = (ab - ba)a$$

για κάθε $a, b \in R$. *Τότε ο δακτύλιος* R *είναι διαιρετικός. Πράγματι, έστω* V *ένα απλό και πιστό* R*-πρότυπο, θεωρώ τον διαιρετικό δακτύλιο* $\mathfrak{K} = \mathrm{End}_R V$ *και γνωρίζουμε ότι ο* R *είναι πυκνός στον* $\mathrm{End}_{\mathfrak{K}} V$. *Αρκεί να δείξουμε ότι* $\dim_{\mathfrak{K}} V = 1$, *καθώς τότε* $R \simeq \mathfrak{K}^{op}$. *Έστω, ως προς άτοπο, ότι υπάρχουν δύο* $\mathfrak{K}$*-γραμμικά ανεξάρτητα διανύσματα* $v, w \in V$. *Από πυκνότητα, υπάρχουν* $r, s \in R$ *τέτοια ώστε* $rv = v,\ rw = 0$ *και* $sw = v,\ sv = 0$. *Συνεπώς*

$$r(rs - sr) \cdot w = v \quad (rs - sr)r \cdot w = 0$$

δηλαδή $v = 0 \,\#$.

(Μια μεγάλη) Εξέταση στην Μη Μεταθετική Άλγεβρα
$*/*/\sum_{i=1}^{9} i^3$

Πρόβλημα 1ο. (α) Έστω X ένα σύνολο και μια σχέση ισοδυναμίας $\pi : X \twoheadrightarrow X/\sim$ σε αυτό. Θεωρούμε την (μοναδική) γραμμική απεικόνιση $F : \bigoplus_{x \in X} \mathbf{C}x \longrightarrow \bigoplus_{\overline{x} \in X/\sim} \mathbf{C}\overline{x}$ που επεκτείνει την απεικόνιση πηλίκο. Δείξτε ότι $\ker F = \langle x - y : x \sim y \rangle$.
(β) Έστω n ένας φυσικός αριθμός και $X = \{1, 2, \ldots, n\}$. Σταθεροποιώ, έναν φυσικό $k < n$ και θεωρώ το σύνολο $\mathcal{X} \subseteq 2^X$ των υποσυνόλων του X με το πολύ k το πλήθος στοιχεία. Ο $\mathbf{C}$-διανυσματικός χώρος $V = \bigoplus_{A \in \mathcal{X}} \mathbf{C}A$ λαμβάνει την δομή $\mathbf{C}S_n$-προτύπου, επεκτείνοντας γραμμικά την δράση $\sigma \cdot A := \sigma(A) \subseteq X$. Θεωρώ τον υπόχωρο του V

$$W := \{v \in V : \sigma \cdot v = v \text{ για κάθε } \sigma \in S_n\}$$

Να δείξετε ότι $\dim_{\mathbf{C}} W = k$.

Πρόβλημα 2ο. Βρείτε όλες τις πεπερασμένες ομάδες G που έχουν ακριβώς τρεις ανάγωγες αναπαραστάσεις.

Πρόβλημα 3ο. Έστω $R = \mathbf{Z}[X]/((X^2+1)^2) \simeq \mathbf{Z}[x]$, όπου $x \in R$ η κλάση του $X \in \mathbf{Z}[X]$. Θεωρώ τον δακτύλιο $\mathbf{M}_n(R)$ των $n \times n$ πινάκων με εγγραφές από το δακτύλιο R. Βρείτε όλους τους πίνακες $A \in \mathbf{M}_n(R)$, τέτοιοι ώστε για κάθε δύο πίνακες $P, Q \in \mathbf{M}_n(R)$

$$\gcd(X^2+1, d(X)) = 1$$

όπου $d(x) = \det(I + PAQ) \in R$, για κάποιο $d(X) \in \mathbf{Z}[X]$

Πρόβλημα 4ο. Χαρακτηρίστε τις παρακάτω προτάσεις Σώστες ή Λάθος. Δικαιολογήστε τις απαντήσεις σας.

(i) Ο δακτύλιος $\mathbf{M}_3(\mathbf{Z}_9)$ είναι απλός.

(ii) Ο δακτύλιος $\mathbf{Z}_{256} \times \mathbf{M}_6(\mathbf{Q})$ έχει τα ίδια απλά πρότυπα με τον $\mathbf{Z}_2 \times \mathbf{M}_6(\mathbf{Q})$.

(iii) Έστω G μια πεπερασμένη ομάδα και V ένα απλό $\mathbf{C}G$-πρότυπο, τότε $V \hookrightarrow V \otimes_{\mathbf{C}} V$

Πρόβλημα 5ο. (α) Έστω R ένας Jacobson ημιαπλός δακτύλιος, ώστε το $1 + a^2$ να είναι αντιστρέψιμο στοιχείο για κάθε $a \in R$. Δείξτε, ότι τότε ο R είναι το γινόμενο διαιρετικών δακτυλίων.
(β) Έστω S μια ακέραια περιοχή. Δείξτε ότι υπάρχει primitive δακτύλιος R, ώστε $Z(R) \simeq S$.

Πρόβλημα 6ο. (α) Έστω G πεπερασμένη ομάδα και $e = \sum_g e_g g \in \mathbf{C}G$ ένα ταυτοδύναμο στοιχείο. Δείξτε ότι ο αριθμός $\sum_{g \in G} e_g e_{g^{-1}}$ είναι ρητός και επιπλέον είναι ακέραιος αν και μόνο αν είναι ίσος με $1 \in \mathbf{Z}$. (Υπόδειξη : Θεωρήστε τον υπόχωρο $e \cdot \mathbf{C}G \subseteq \mathbf{C}G$.)
(β) Βρείτε όλα τα στοιχεία $e = \sum_g e_g g \in Z(\mathbf{C}S_3)$ που ικανοποιούν $e^3 = e$.
(γ) Έστω $f(X) \in \mathbf{Z}[X]$ ένα πολυώνυμο βαθμού 2025. Πόσα στοιχεία $e \in Z(\mathbf{C}S_3)$ ικανοποιούν $f(e) = 0 \in \mathbf{C}S_3$;

Πρόβλημα 7ο. (α) Έστω R ένας δακτύλιος, τέτοιος ώστε το ριζικό $J(R)$ να είναι μεγιστικό ιδεώδες. Δείξτε ότι για κάθε $x \in R$, είτε το x είναι αντιστρέψιμο, είτε το $1 - x$.
(β) Έστω R ένας δακτύλιος, M ένα R-πρότυπο και $S = \mathrm{End}_R M$ ο δακτύλιος των ενδομορφισμών του M. Δείξτε, ότι αν ο $S/J(S)$ είναι διαιρετικός, τότε για κάθε δύο R-υποπρότυπα $M_1, M_2 \subseteq M$ με $M = M_1 \oplus M_2$ είναι είτε $M_1 = 0$ είτε $M_2 = 0$

Πρόβλημα 8ο Έστω N ένα απλό R-πρότυπο. Ένα R-πρότυπο M καλείται *ομογενές τύπου* N αν είναι το ευθύ άθροισμα απλών R-προτύπων, που το καθένα είναι ισόμορφο με το R-πρότυπο N. Έστω M ένα ομογενές R-πρότυπο τύπου N. Βρείτε, όλα τα υποπρότυπα $M' \subseteq M$, τέτοια ώστε $\varphi(M') \subseteq M'$ για κάθε R-γραμμική απεικόνιση $\varphi : M \to M$.

Διάρκεια Εξέτασης : 3 ώρες.
Καλή επιτυχία !