A.2 ΜΟΔΙΟΙ ΟΡΙΣΜΕΝΟΙ ΥΠΕΡΑΝΩ ΜΕΤΑΘΕΤΙΚΩΝ ΔΑΚΤΥΛΙΩΝ

Η κύρια αλγεβρική δομή που θα μας απασχολήσει είναι αυτή τού *μοδίου* που ορίζεται υπεράνω ενός *μεταθετικού μη τετριμμένου δακτυλίου* (και περιλαμβάνει, ως ειδικές περιπτώσεις, τόσον τη δομή τής αβελιανής ομάδας όσον και τη δομή τού διανυσματικού χώρου).

A.2.1 Ορισμός. Έστω $(R,+,\cdot)$ ένας *μεταθετικός μη τετριμμένος* δακτύλιος και έστω $(M,\boxplus)$ μια (προσθετική) αβελιανή ομάδα με ουδέτερό της στοιχείο το 0_M. Εάν το σύνολο M είναι εφοδιασμένο με μια (εν γένει *εξωτερική*) πράξη[4]

$$R\times M \quad\longrightarrow\quad M,\quad (r,x)\quad\longmapsto\quad r\star x,$$

ούτως ώστε να πληροί τις ακόλουθες ιδιότητες[5]:

(i)	$1_R\star x = x,$	$\forall x\in M,$	
(ii)	$(r+s)\star x = (r\star x)\boxplus(s\star x),$	$\forall x\in M$	και $\forall\,(r,s)\in R\times R,$
(iii)	$r\star(x\boxplus y) = (r\star x)\boxplus(r\star y),$	$\forall (x,y)\in M\times M$	και $\forall r\in R,$
(iv)	$(r\cdot s)\star x = r\star(s\star x)\,,$	$\forall x\in M$	και $\forall\,(r,s)\in R\times R,$

τότε λέμε ότι το M (μαζί με αυτές τις πράξεις "$\boxplus$" και "$\star$") αποτελεί έναν **μόδιο υπεράνω τού** R ή, εν συντομία, έναν R-**μόδιο** (R-module).

A.2.2 Πρόταση. *Έστω $(M,\boxplus,\star)$ ένας R-μόδιος. Εάν για $x\in M$ συμβολίσουμε ως $\backsim x$ το αντίθετό του*[6] *ως προς την "$\boxplus$", τότε ισχύουν τα εξής:*

(i) $0_R\star x = 0_M$, *για κάθε* $x\in M$.

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

(iii) *Για οιαδήποτε* $r\in R^\times$ *και* $x\in M$ *ισχύει* $r\star x = 0_M \iff x = 0_M$.

(iv) $(-1_R)\star x = \backsim x$, *για κάθε* $x\in M$.

(v) $(-r)\star x = r\star(\backsim x) = \backsim (r\star x)$, *για οιαδήποτε* $r\in R$ *και* $x\in M$.

(vi) $r\star(x_1 \backsim x_2) = (r\star x_1)\backsim(r\star x_2)$, *για οιαδήποτε* $r\in R$ *και* $x_1,x_2\in M$.

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν $x\in M$. Κατόπιν εφαρμογής τής ιδιότητας A.2.1 (ii) για $r=s=0_R$ λαμβάνουμε $(0_R\star x)\boxplus(0_R\star x) = (0_R+0_R)\star x = 0_R\star x$. Προσθέτοντας το αντίθετο στοιχείο $\backsim (0_R\star x)$ τού $0_R\star x$ σε αμφότερα τα μέλη συμπεραίνουμε ότι

$$\backsim (0_R\star x)\boxplus((0_R\star x)\boxplus(0_R\star x)) = \backsim (0_R\star x)\boxplus(0_R\star x) = 0_M.$$

[4] Η προκειμένη πράξη καλείται συνήθως **αριθμητικός** ή **βαθμωτός πολλαπλασιασμός**. (Τα στοιχεία τού R είναι τα **αριθμητικά** ή **βαθμωτά μεγέθη** με τα οποία «πολλαπλασιάζουμε» τα στοιχεία τού M μέσω τής "$\star$".)

[5] Οι ιδιότητες (ii) και (iii) είναι γνωστές ως **γενικευμένοι επιμεριστικοί νόμοι** και η (iv) ως **γενικευμένος προσεταιριστικός νόμος**.

[6] Εξ ορισμού, το $\backsim x$ είναι το μοναδικό στοιχείο τής $(M,\boxplus)$ για το οποίο ισχύει $(\backsim x)\boxplus x = 0_M = x\boxplus(\backsim x)$.

Εφαρμόζοντας την προσεταιριστική ιδιότητα τής προσθέσεως τής $(M, \boxplus)$ συμπεραίνουμε τελικώς ότι $0_R \star x = (\backsim (0_R \star x) \boxplus (0_R \star x)) \boxplus (0_R \star x) = 0_M$.
(ii) Λόγω τού (i) έχουμε κατ' αρχάς $0_R \star 0_M = 0_M$. Έστω τώρα τυχόν $r \in R$. Εφαρμόζοντας την ιδιότητα A.2.1 (iv) για $s = 0_R$ λαμβάνουμε

$$r \star 0_M = r \star (0_R \star 0_M) = (r \cdot 0_R) \star 0_M = 0_R \star 0_M = 0_M.$$

(iii) Η συνεπαγωγή "$\Leftarrow$" είναι προφανής λόγω τής (ii). Απομένει να δείξουμε την "$\Rightarrow$". Προς τούτο θεωρούμε $r \in R^\times$ και $x \in M$, τέτοια ώστε $r \star x = 0_M$. Επειδή το r διαθέτει αντίστροφο στοιχείο r^{-1}, από το (ii) και τις ιδιότητες A.2.1 (i) και (iv) συμπεραίνουμε ότι $x = 1_R \star x = (r^{-1} \cdot r) \star x = r^{-1} \star (r \star x) = r^{-1} \star 0_M = 0_M$.
(iv) Έστω τυχόν $x \in M$. Προφανώς, λόγω των ιδιοτήτων A.2.1 (i) και (ii),

$$\begin{aligned} & x \boxplus ((-1_R) \star x) = (1_R \star x) \boxplus ((-1_R) \star x) \\ & = (1_R + (-1_R)) \star x = 0_R \star x = 0_M \Rightarrow (-1_R) \star x = \backsim x. \end{aligned}$$

(v) Θεωρούμε τυχόντα $r \in R$ και $x \in M$. Μέσω τού (i) και τής ιδιότητας A.2.1 (ii) λαμβάνουμε $0_M = 0_R \star x = (r + (-r)) \star x = (r \star x) \boxplus ((-r) \star x)$. Κατ' αναλογίαν, από το (ii) και την ιδιότητα A.2.1 (iii) έπεται ότι

$$0_M = r \star 0_M = r \star (x \boxplus (\backsim x)) = (r \star x) \boxplus (r \star (\backsim x)),$$

οπότε (λόγω τής μοναδικότητας τού ουδετέρου στοιχείου τής ομάδας $(M, \boxplus)$) έχουμε τελικώς $(-r) \star x = r \star (\backsim x) = \backsim (r \star x)$.
(vi) Θεωρούμε τυχόντα στοιχεία $r \in R$ και $x_1, x_2 \in M$. Εφαρμόζοντας την ιδιότητα A.2.1 (iii) λαμβάνουμε

$$\begin{aligned} & r \star x_1 = r \star (x_1 \boxplus 0_M) = r \star ((x_1 \boxplus ((\backsim x_2) \boxplus x_2)) \\ & = (r \star x_1) \boxplus (r \star ((\backsim x_2) \boxplus x_2)) = ((r \star x_1) \boxplus (r \star (\backsim x_2))) \boxplus (r \star x_2) \\ & = (r \star (x_1 \backsim x_2)) \boxplus (r \star x_2), \end{aligned}$$

οπότε (λόγω τού (v))$(r \star x_1) \backsim (r \star x_2) = (r \star x_1) \boxplus ((-r) \star x_2) = r \star (x_1 \backsim x_2)$. □

A.2.3 Σημείωση. (Απλούστευση συμβολισμών) Στον ορισμό A.2.1 και στην πρόταση A.2.2 χρησιμοποιήθηκαν τα σύμβολα " $\boxplus$ " και " $\star$ " για τη σήμανση των πράξεων επί ενός R-μοδίου M και το $\backsim x$ για εκείνην τού αντιθέτου ενός στοιχείου $x \in M$. Ωστόσο, η περαιτέρω διατήρηση ενός τόσο δυσκίνητου συμβολισμού θα ήταν κάτι το πολύ φορτικό. Γι' αυτόν τον λόγο θα μεταβούμε, από εδώ και στο εξής, στον *απλουστευμένο προσθετικό και πολλαπλασιαστικό* συμβολισμό αυτών των πράξεων (διακρίνοντάς τες από εκείνες τού ιδίου τού δακτυλίου R από τα συμφραζόμενα και από τον τρόπο επιλογής των εκάστοτε θεωρούμενων στοιχείων, και παραλείποντας, ως επί το πλείστον, ακόμη και το dot " $\cdot$ "). Έτσι, αντί τού $\backsim x$ θα γράφουμε $-x$ και αντί των (i)-(iv) τού ορισμού A.2.1 θα γράφουμε απλώς

$$\begin{array}{llll} \text{(i)} & 1_R x = x, & \text{(ii)} & (r+s)\,x = rx + sx, \\ \text{(iii)} & r\,(x+y) = rx + ry, & \text{(iv)} & (rs)\,x = r\,(sx)\,. \end{array}$$

Επίσης, όταν $x_1,\ldots,x_k \in M$, $k \in \mathbb{N}$, θα συμβολίζουμε ως $\sum_{i=1}^{k} x_i$ το **άθροισμα** $x_1 + \cdots + x_n$ των $x_1,\ldots,x_n$.

A.2.4 Παραδείγματα. (i) Εάν $(G,+)$ είναι μια προσθετική αβελιανή ομάδα, τότε υπάρχει *ένας και μόνον τρόπος* για να καταστεί αυτή $\mathbb{Z}$-μόδιος[7]: Ως *αριθμητικός* (*βαθμωτός*) *πολλαπλασιασμός* ορίζεται η πράξη

$$\mathbb{Z} \times G \ni (n,g) \longmapsto ng \in G$$

θέτοντας

$$ng := \begin{cases} \underbrace{g + g + \cdots + g}_{n \text{ φορές}}, & \text{όταν } \; n > 0, \\ -((-n)g), & \text{όταν } \; n < 0, \\ 0_G \,, & \text{όταν } \; n = 0, \end{cases}$$

εν είδει «πολλαπλασίου» τού g. Ως εκ τούτου, η έννοια *αβελιανή ομάδα* ταυτίζεται κατ' ουσίαν με την έννοια $\mathbb{Z}$-*μόδιος*.

(ii) Κάθε K-*διανυσματικός χώρος*, ήτοι κάθε διανυσματικός χώρος οριζόμενος υπεράνω ενός *σώματος* K, είναι προφανώς ένας K-μόδιος.

A.2.5 Παραδείγματα. Έστω R ένας μεταθετικός μη τετριμμένος δακτύλιος.

(i) Εκτός από $\mathbb{Z}$-μόδιος (βλ. A.2.4 (i)) ο R μπορεί να ιδωθεί αφ' εαυτού ως R-μόδιος (εάν ως αριθμητικός πολλαπλασιασμός ορισθεί ο πολλαπλασιασμός τού R). Γενικότερα, εάν S είναι ένας μη τετριμμένος υποδακτύλιος τού R, τότε ο R μπορεί (κατ' αναλογίαν) να ιδωθεί ως S-μόδιος.

(ii) Εάν I είναι ένα ιδεώδες τού R, τότε ο πηλικοδακτύλιος R/I καθίσταται R-μόδιος μέσω τού αριθμητικού πολλαπλασιασμού:

$$R \times R/I \ni (r, a + I) \longmapsto ra + I \in R/I.$$

(iii) Εάν $f : R \longrightarrow R'$ είναι ένας ομομορφισμός μεταθετικών δακτυλίων (όπου $1_{R'} \neq 0_{R'}$), τότε ο R'καθίσταται R-μόδιος μέσω τού αριθμητικού πολλαπλασιασμού:

$$R \times R' \ni (r, r') \longmapsto f(r)r' \in R'.$$

(iv) Γενικότερα, εάν $f : R \longrightarrow R'$ είναι ένας ομομορφισμός μεταθετικών δακτυλίων (όπου $1_{R'} \neq 0_{R'}$) και N ένας R'-μόδιος, τότε ο N μπορεί να ιδωθεί *και* ως R-μόδιος με (την ίδια πρόσθεση και) αριθμητικό πολλαπλασιασμό

$$R \times N \ni (r, x) \longmapsto f(r)x \in N.$$

[7] Εν προκειμένω, ως $\mathbb{Z}$ συμβολίζεται ο δακτύλιος των ακεραίων αριθμών ως προς τις *συνήθεις* πράξεις προσθέσεως και πολλαπλασιασμού.

(v) Εάν $m, n \in \mathbb{N}$, τότε η αβελιανή ομάδα $(\mathrm{Mat}_{m\times n}(R), +)$ των $(m \times n)$-πινάκων με εγγραφές ειλημμένες από τον R καθίσταται R-μόδιος μέσω τού αριθμητικού πολλαπλασιασμού:

$$R \times \mathrm{Mat}_{m\times n}(R) \ni (r, (a_{ij})_{1\leq i\leq m, 1\leq j\leq n}) \longmapsto (ra_{ij})_{1\leq i\leq m, 1\leq j\leq n} \in \mathrm{Mat}_{m\times n}(R).$$

(vi) Έστω $n \in \mathbb{N}$. Η αβελιανή ομάδα $(R^n, +)$, όπου

$$R^n := \{ (r_1,..., r_n) | \, r_i \in R, \; \forall i \in \{1,..., n\} \}$$

(με την κατά συντεταγμένες πρόσθεση), καθίσταται R-μόδιος μέσω τού αριθμητικού πολλαπλασιασμού:

$$R \times R^n \ni (r, (r_1,..., r_n)) \longmapsto (rr_1,..., rr_n) \in R^n.$$

(vii) Παρομοίως, εάν $n \in \mathbb{N}$ και M είναι ένας R-μόδιος, τότε το

$$M^n := \{ (x_1,..., x_n) | \, x_i \in M, \; \forall i \in \{1,..., n\} \},$$

μπορεί να ιδωθεί ως R-μόδιος ως προς τις συνήθεις κατά συντεταγμένες πράξεις προσθέσεως και αριθμητικού πολλαπλασιασμού.

(viii) Εάν M είναι ένας R-μόδιος και $\mathcal{X}$ τυχόν μη κενό σύνολο, τότε το σύνολο

$$M^{\mathcal{X}} := \text{ΑΠ}(\mathcal{X}, M) := \{\text{απεικονίσεις } f : \mathcal{X} \longrightarrow M\}$$

καθίσταται R-μόδιος μέσω των πράξεων:

$$\begin{aligned} M^{\mathcal{X}} \times M^{\mathcal{X}} &\ni (f, g) \longmapsto f + g \in M^{\mathcal{X}}, \\ R \times M^{\mathcal{X}} &\ni (r, f) \longmapsto rf \in M^{\mathcal{X}}, \end{aligned}$$

όπου $(f + g)(x) := f(x) + g(x)$, $(rf)(x) := rf(x)$, $\forall x \in \mathcal{X}$ και $\forall r \in R$.

A.2.6 Ορισμός. Ένα μη κενό υποσύνολο U (τού υποκειμένου συνόλου) ενός R-μοδίου M καλείται **υπομόδιος τού** M όταν το U καθίσταται αφ' εαυτού μόδιος ως προς τους περιορισμούς $+|_{U\times U}$ και $\cdot|_{R\times U}$ των πράξεων τής προσθέσεως "+" και τού αριθμητικού πολλαπλασιασμού "·" με τις οποίες είναι εφοδιασμένο το M ή, ισοδυνάμως, όταν για οιαδήποτε $u_1, u_2, u \in U$ και $r \in R$,

$$u_1 - u_2 \in U \;\; \text{και} \;\; ru \in U.$$

A.2.7 Πρόταση. *Ένα μη κενό υποσύνολο U ενός R-μοδίου M είναι υπομόδιος αυτού εάν και μόνον εάν*

$$r_1u_1 + r_2u_2 \in U, \; \forall (r_1, r_2) \in R \times R \;\; \text{και} \;\; \forall (u_1, u_2) \in U \times U. \tag{A.1}$$

ΑΠΟΔΕΙΞΗ. Εάν το U είναι υπομόδιος τού M, τότε για κάθε $(r_1, r_2) \in R \times R$ και κάθε $(u_1, u_2) \in U \times U$ έχουμε

$$\left.\begin{array}{r} r_1 u_1 \in U \\ -r_2 u_2 = (-r_2) u_2 \in U \end{array}\right\} \Rightarrow r_1 u_1 - (-r_2 u_2) = r_1 u_1 + r_2 u_2 \in U.$$

Και αντιστρόφως· εάν ικανοποιείται η συνθήκη (A.1), τότε θέτοντας $r_1 = 1_R$ και $r_2 = -1_R$ συμπεραίνουμε ότι $u_1 - u_2 \in U$, ενώ θέτοντας $r = r_1$, $u = u_1$, $r_2 = 0_R$, συμπεραίνουμε ότι $ru \in U$. Άρα το U είναι όντως ένας υπομόδιος τού M. $\square$

A.2.8 Παραδείγματα. (i) Οι υπομόδιοι μιας αβελιανής ομάδας $(G, +)$ (με τη δομή τού $\mathbb{Z}$-μοδίου, βλ. A.2.4 (i)) είναι ακριβώς οι υποομάδες αυτής.

(ii) Οι υπομόδιοι ενός K-διανυσματικού χώρου (βλ. A.2.4 (ii)) δεν είναι τίποτε άλλο παρά οι γραμμικοί υπόχωροι αυτού.

A.2.9 Παραδείγματα. Έστω R ένας μεταθετικός μη τετριμμένος δακτύλιος.

(i) Εάν ο R θεωρηθεί αφ' εαυτού ως R-μόδιος (βλ. A.2.5 (i)), τότε οι υπομόδιοι αυτού είναι ακριβώς τα ιδεώδη του.

(ii) Εάν M είναι ένας R-μόδιος, τότε τόσον ο ίδιος ο M όσον και τα σύνολα

$$Rx := \{ rx | \, r \in R \}, \;\; x \in M,$$

αποτελούν υπομοδίους τού M. (Ιδιαιτέρως, ο $R0_M = \{0_M\}$ καλείται **τετριμμένος υπομόδιος** τού M.)

(iii) Εάν M είναι ένας R-μόδιος και I ένα ιδεώδες τού R, τότε το

$$IM := \left\{ \sum_{j=1}^{k} r_j x_j \,\middle|\, r_j \in I, \; x_j \in M, \; \forall j \in \{1, ..., k\}, \; k \in \mathbb{N} \right\}$$

αποτελεί έναν υπομόδιο τού M.

(iv) Εάν M είναι ένας R-μόδιος, $\mathcal{X}$ τυχόν μη κενό σύνολο και $f \in M^{\mathcal{X}}$, τότε το σύνολο $\mathrm{supp}(f) := \{ x \in \mathcal{X} | \, f(x) \neq 0_M \}$ καλείται **φορέας** τής f. Είναι άμεσος ο έλεγχος τού ότι το

$$M^{(\mathcal{X})} := \left\{ f \in M^{\mathcal{X}} \,\middle|\, \mathrm{card}(\mathrm{supp}(f)) < \infty \right\}$$

είναι ένας υπομόδιος τού R-μοδίου $M^{\mathcal{X}}$. (Βλ. A.2.5 (viii).) Ειδική περίπτωση αυτού (όταν $M = R$ και $\mathcal{X} = \mathbb{N}_0$) αποτελεί ο *πολυωνυμικός δακτύλιος* $R[\mathsf{X}] = R^{(\mathbb{N}_0)}$ μίας απροσδιορίστου X (με τους συντελεστές των στοιχείων του ειλημμένους από τον R και $\mathsf{X} := (0_R, 1_R, 0_R, 0_R, ...)$).

A.2.10 Πρόταση. *Εάν $(U_\lambda)_{\lambda \in \Lambda}$ είναι μια οικογένεια υπομοδίων ενός R-μοδίου M, τότε η τομή των μελών της $\bigcap_{\lambda \in \Lambda} U_\lambda$ είναι υπομόδιος τού M.*

ΑΠΟΔΕΙΞΗ. Επειδή $0_M \in U_\lambda$ για κάθε $\lambda \in \Lambda$, έχουμε $0_M \in \bigcap_{\lambda\in\Lambda} U_\lambda$, οπότε η τομή αυτή δεν είναι κενή. Για κάθε $(r_1, r_2) \in R \times R$ και κάθε $(u_1, u_2) \in \bigcap_{\lambda\in\Lambda} U_\lambda \times \bigcap_{\lambda\in\Lambda} U_\lambda$,

$$[u_1, u_2 \in U_\lambda,\ \forall \lambda \in \Lambda] \Rightarrow [r_1u_1 + r_2u_2 \in U_\lambda,\ \forall \lambda \in \Lambda] \Rightarrow r_1u_1 + r_2u_2 \in \bigcap_{\lambda\in\Lambda} U_\lambda,$$

οπότε η τομή $\bigcap_{\lambda\in\Lambda} U_\lambda$ αποτελεί όντως έναν υπομόδιο τού M. (Βλ. A.2.7.) □

A.2.11 Ορισμός. Έστω M ένας R-μόδιος και έστω $\mathcal{X} \subseteq M$ τυχόν υποσύνολο (τού κενού μη εξαιρουμένου). Κατά την πρόταση A.2.10 το σύνολο

$$\boxed{\mathrm{Lin}_R(\mathcal{X}) := \bigcap \{U \mid U \text{ υπομόδιος τού } M \text{ με } \mathcal{X} \subseteq U\}}$$

είναι ένας υπομόδιος τού M και καλείται **γραμμική θήκη** ή **γραμμικό περίβλημα τού $\mathcal{X}$ εντός τού M** ή **ο υπομόδιος τού M ο παραγόμενος από το $\mathcal{X}$**. Προφανώς, ο $\mathrm{Lin}_R(\mathcal{X})$ είναι *ο ελάχιστος υπομόδιος τού M* (ως προς τον συνολοθεωρητικό εγκλεισμό) *που περιέχει το $\mathcal{X}$*.

A.2.12 Ορισμός. Έστω M ένας R-μόδιος και έστω $\varnothing \neq \mathcal{X} \subseteq M$. Λέμε ότι ένα στοιχείο $y \in M$ είναι **(R-)γραμμικός συνδυασμός στοιχείων τού $\mathcal{X}$** όταν υπάρχουν (πεπερασμένου πλήθους) στοιχεία $x_1, ..., x_k$ τού $\mathcal{X}$ και $r_1, ..., r_k \in R$, τέτοια ώστε να ισχύει

$$y = r_1x_1 + \cdots + r_kx_k.$$

Συμβολισμός: $\mathrm{L.C.}_R(\mathcal{X}) := \{$όλοι οι γραμμικοί συνδυασμοί στοιχείων τού $\mathcal{X}\}$.

A.2.13 Πρόταση. *Έστω M ένας R-μόδιος και έστω $\mathcal{X} \subseteq M$ τυχόν υποσύνολο. Τότε*

$$\mathrm{Lin}_R(\mathcal{X}) = \begin{cases} \{0_M\}, & \text{όταν } \mathcal{X} = \varnothing, \\ \mathrm{L.C.}_R(\mathcal{X}), & \text{όταν } \mathcal{X} \neq \varnothing. \end{cases}$$

ΑΠΟΔΕΙΞΗ. Όταν $\mathcal{X} = \varnothing$ είναι προφανές ότι ο ελάχιστος υπομόδιος που περιέχει το $\varnothing$ είναι ο τετριμμένος υπομόδιος $\{0_M\}$ τού M. Έστω ότι $\mathcal{X} \neq \varnothing$. Εν τοιαύτη περιπτώσει, εάν $r, r' \in R$ και

$$y = \sum_{j=1}^{k} s_jx_j,\ y' = \sum_{\rho=1}^{l} s'_\rho x'_\rho \in \mathrm{L.C.}_R(\mathcal{X}),$$

όπου $x_1, ..., x_k, x'_1, ..., x'_l \in \mathcal{X}$ και $s_1, ..., s_k, s'_1, ..., s'_l \in R$, τότε

$$ry + r'y' = \sum_{j=1}^{k} (rs_j)x_j + \sum_{\rho=1}^{l} (r's'_\rho)x'_\rho \in \mathrm{L.C.}_R(\mathcal{X}),$$

οπότε το (εξ υποθέσεως μη κενό) σύνολο $\text{L.C.}_R(\mathcal{X})$ είναι υπομόδιος τού M. (Βλ. πρόταση A.2.7.) Επιπροσθέτως, $\mathcal{X} \subseteq \text{L.C.}_R(\mathcal{X})$ (διότι για κάθε στοιχείο $x \in \mathcal{X}$, $1_R x = x \in \text{L.C.}_R(\mathcal{X})$). Επειδή ο $\text{L.C.}_R(\mathcal{X})$ είναι ο ελάχιστος υπομόδιος που περιέχει το $\mathcal{X}$, έχουμε $\text{Lin}_R(\mathcal{X}) \subseteq \text{L.C.}_R(\mathcal{X})$. Απο την άλλη μεριά, είναι πρόδηλο ότι κάθε γραμμικός συνδυασμός στοιχείων τού $\mathcal{X}$ ανήκει σε κάθε υπομόδιο που περιέχει το $\mathcal{X}$, οπότε ισχύει και ο αντίστροφος εγκλεισμός: $\text{L.C.}_R(\mathcal{X}) \subseteq \text{Lin}_R(\mathcal{X})$. □

A.2.14 Ορισμός. Λέμε ότι ένας υπομόδιος U ενός R-μοδίου M **παράγεται από ένα υποσύνολο** $\mathcal{X} \subseteq U$ ή ότι το $\mathcal{X}$ είναι ένα **σύστημα γεννητόρων** ή **παράγον υποσύνολο τού** U όταν $\text{Lin}_R(\mathcal{X}) = U$. Εάν ο ίδιος ο M διαθέτει κάποιο πεπερασμένο σύστημα γεννητόρων, τότε καλείται **πεπερασμένως παραγόμενος**. Εάν ο M είναι δυνατόν να παραχθεί από κάποιο μονοσύνολο $\{x\}$, $x \in M$, τότε λέμε ότι ο M είναι ένας **κυκλικός R-μόδιος**. (Εν τοιαύτη περιπτώσει, $M = Rx$.)

A.2.15 Παραδείγματα. (i) Εάν M είναι ένας R-μόδιος, τότε[8]

$$\{0_M\} = \text{Lin}_R(\varnothing) = \text{Lin}_R(\{0_M\}).$$

(ii) Εάν M είναι ένας R-μόδιος και I ένα ιδεώδες τού R, τότε ο υπομόδιος IM (βλ. A.2.9 (iii)) είναι ο υπομόδιος τού M ο παραγόμενος από το σύνολο $\{rx | \, r \in I, \, x \in M\}$.

A.2.16 Πρόταση. *Εάν* $(U_\lambda)_{\lambda\in\Lambda}$ *είναι μια οικογένεια υπομοδίων ενός* R*-μοδίου* M *με* $\Lambda \neq \varnothing$ *και* $\mathfrak{E}(\Lambda) := \{\Lambda' | \varnothing \neq \Lambda' \subseteq \Lambda : \text{card}(\Lambda') < \infty\}$, *τότε ο υπομόδιος* $\text{Lin}_R(\bigcup_{\lambda\in\Lambda} U_\lambda)$ *τού* M *απαρτίζεται από όλα τα (πεπερασμένα) αθροίσματα τής μορφής*

$$\sum_{\nu\in\Lambda'} x_\nu, \text{ όπου } \Lambda' \in \mathfrak{E}(\Lambda) \text{ και } x_\nu \in U_\nu, \, \forall \nu \in \Lambda'. \tag{A.2}$$

ΑΠΟΔΕΙΞΗ. Κάθε γραμμικός συνδυασμός στοιχείων τής ενώσεως $\bigcup_{\lambda\in\Lambda} U_\lambda$ των μελών τής θεωρούμενης οικογενείας υπομοδίων είναι ακριβώς τής μορφής (A.2). Ως εκ τούτου, ο ισχυρισμός είναι αληθής δυνάμει τής προτάσεως A.2.13. □

A.2.17 Ορισμός. Ο ανωτέρω υπομόδιος $\text{Lin}_R(\bigcup_{\lambda\in\Lambda} U_\lambda)$ καλείται **το άθροισμα** των μελών τής οικογενείας $(U_\lambda)_{\lambda\in\Lambda}$ και συμβολίζεται ως $\sum_{\lambda\in\Lambda} U_\lambda$. Όταν το Λ είναι πεπερασμένο, ας πούμε το $\Lambda = \{1, ..., k\}$ τότε γράφουμε

$$\sum_{j=1}^{k} U_j \text{ ή απλώς } U_1 + \cdots + U_k.$$

[8] Ως εκ τούτου, *και* ο τετριμμένος υπομόδιος τού M θεωρείται ως *πεπερασμένως παραγόμενος*.

A.2.18 Σημείωση. (i) Είναι άμεσος ο έλεγχος τού ότι αυτό το «άθροισμα» έχει τόσον την *προσεταιριστική* όσον και τη *μεταθετική* ιδιότητα, ήτοι ότι

$$\sum_{\lambda\in\Lambda} U_\lambda = \sum_{j\in J}\left(\sum_{\lambda\in\Lambda_j} U_\lambda\right)$$

για κάθε οικογένεια $(\Lambda_j)_{j\in J}$ μη κενών υποσυνόλων τού Λ με $\Lambda = \coprod_{j\in J}\Lambda_j$ και

$$\sum_{\lambda\in\Lambda} U_\lambda = \sum_{\lambda\in\Lambda} U_{\sigma(\lambda)} \text{ για κάθε αμφίρριψη } \ \sigma : \Lambda \longrightarrow \Lambda.$$

(ii) Ιδιαιτέρως, $\sum_{\lambda\in\Lambda} U_\lambda = U_j + \sum_{\lambda\in\Lambda\smallsetminus\{j\}} U_\lambda,\ \forall j\in\Lambda.$

A.2.19 Παρατήρηση. *Εν γένει* $\bigcup_{\lambda\in\Lambda} U_\lambda \subsetneqq \sum_{\lambda\in\Lambda} U_\lambda$ και το $\bigcup_{\lambda\in\Lambda} U_\lambda$ δεν είναι κατ' ανάγκην υπομόδιος τού M. Επί παραδείγματι, εάν $\Lambda = \{1,2\}$, τότε για τους υπόχωρους

$$U_1 := \left\{ (x,0)\in\mathbb{R}^2 \,\middle|\, x\in\mathbb{R}\right\},\ \ U_2 := \left\{ (0,y)\in\mathbb{R}^2 \,\middle|\, y\in\mathbb{R}\right\}$$

τού $\mathbb{R}$-διανυσματικού χώρου $\mathbb{R}^2$ ισχύει $U_1\cup U_2 \subsetneqq U_1+U_2=\mathbb{R}^2$.

A.2.20 Πρόταση. *Εάν U, U', U'' είναι υπομόδιοι ενός R-μοδίου M με $U''\subseteq U$, τότε*

$$U\cap(U'+U'') = (U\cap U') + U''.$$

ΑΠΟΔΕΙΞΗ. Επειδή $U''\subseteq U$, έχουμε $U''+U=U$. Επιπροσθέτως,

$$\left.\begin{array}{r}(U\cap U')+U''\subseteq U+U''\\ (U\cap U')+U''\subseteq U'+U''\end{array}\right\}\Rightarrow (U\cap U')+U''\subseteq (U\cap U')\cap(U'+U''),$$

όπου $(U\cap U')\cap(U'+U'') = U\cap(U'+U'')$. Για την απόδειξη τού αντιστρόφου εγκλεισμού θεωρούμε τυχόν $x\in U\cap(U'+U'')$. Τότε $x\in U$ και $x=y+z$ για κάποια $y\in U'$ και $z\in U''$. Επειδή $U''\subseteq U$, έχουμε $z\in U$, οπότε $y=x-z\in U$ και, κατ' επέκταση, $y\in U\cap U'$, απ' όπου έπεται ότι $x=y+z\in(U\cap U')+U''$. □

A.3 ΟΜΟΜΟΡΦΙΣΜΟΙ R-ΜΟΔΙΩΝ

Ομομορφισμοί μεταξύ R-μοδίων ονομάζονται εκείνες οι απεικονίσεις που είναι συμβατές με τις πράξεις τής προσθέσεως και τού αριθμητικού πολλαπλασιασμού ενός εκάστου.

A.3.1 Ορισμός. Εάν M, N είναι R-μόδιοι, τότε μια απεικόνιση $f : M \longrightarrow N$ καλείται **ομομορφισμός** (**R-μοδίων**) ή **R-γραμμική απεικόνιση** όταν ισχύουν τα ακόλουθα[9]:

[9] Προσοχή! Παρά το γεγονός ότι χρησιμοποιούμε ίδιο συμβολισμό για τις πράξεις επί των M και N, αυτές ενδέχεται να είναι διαφορετικές!

(i) $f(x_1 + x_2) = f(x_1) + f(x_2),\ \forall (x_1, x_2) \in M \times M$.

(ii) $f(rx) = rf(x),\ \forall (r, x) \in R \times M$.

Το σύνολο όλων των ομομορφισμών από τον M στον N συμβολίζεται ως εξής:

$$\boxed{\mathrm{Hom}_R(M,N) := \left\{ f \in N^M \,\middle|\, f \text{ ομομορφισμός } R\text{-μοδίων} \right\}.} \tag{A.3}$$

Ως **πυρήνας** και **εικόνα** ενός $f \in \mathrm{Hom}_R(M,N)$ ορίζονται τα υποσύνολα

$$\boxed{\mathrm{Ker}(f) := f^{-1}(\{0_N\}) = \{x \in M \,|\, f(x) = 0_N\} \subseteq M} \tag{A.4}$$

και

$$\boxed{\mathrm{Im}(f) := f(M) = \{f(x) \,|\, x \in M\} \subseteq N,} \tag{A.5}$$

αντιστοίχως.

A.3.2 Πρόταση. *Για κάθε* $f \in \mathrm{Hom}_R(M,N)$ *ισχύουν τα εξής*:

(i) $f(0_M) = 0_N$.

(ii) $f(-x) = -f(x), \forall x \in M$.

ΑΠΟΔΕΙΞΗ. (i) Δυνάμει των A.2.2 (i) και A.3.1 (ii), $f(0_R \cdot 0_M) = 0_R \cdot f(0_M) = 0_N$.

(ii) Έστω τυχόν $x \in M$. Σύμφωνα με το (i) και το A.3.1 (i),

$$f(x) + f(-x) = f(x + (-x)) = f(0_M) = 0_N,$$

οπότε $f(-x) = -f(x)$. □

A.3.3 Πρόταση. *Δοθέντων δυο R-μοδίων M, N και μιας απεικονίσεως $f \in N^M$, τα ακόλουθα είναι ισοδύναμα*:

(i) $f \in \mathrm{Hom}_R(M,N)$.

(ii) *Για οιαδήποτε* $(x_1, x_2) \in M \times M$ *και* $(r_1, r_2) \in R \times R$ *ισχύει η ισότητα*

$$f(r_1x_1 + r_2x_2) = r_1f(x_1) + r_2f(x_2). \tag{A.6}$$

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν η απεικόνιση f είναι ομομορφισμός, τότε για οιαδήποτε ζεύγη $(x_1, x_2) \in M \times M$ και $(r_1, r_2) \in R \times R$ τα A.3.1 (i) και (ii) δίδουν

$$f(r_1x_1 + r_2x_2) = f(r_1x_1) + f(r_2x_2) = r_1f(x_1) + r_2f(x_2).$$

(ii)⇒(i) Εφαρμόζοντας την (A.6) για $r_1 = r_2 = 1_R$ λαμβάνουμε την ισότητα A.3.1 (i). Εξάλλου, η (A.6) για $x_1 = x$ και $x_2 = 0_M$ δίδει την ισότητα A.3.1 (ii). □

A.3.4 Πρόταση. *Δοθέντων δυο R-μοδίων M, N και ενός πεπερασμένου υποσυνόλου $\{x_1,\ldots,x_k\} \subseteq M$, ισχύει η ακόλουθη ισότητα για οιονδήποτε $f \in \mathrm{Hom}_R(M,N)$ και για οιαδήποτε $r_1,\ldots,r_k \in R$:*

$$f\left(\sum_{i=1}^{k} r_i x_i\right) = \sum_{i=1}^{k} r_i f(x_i). \tag{A.7}$$

Απόδειξη. Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς το πλήθος k των προσθετέων. Για $k = 1$ η (A.7) έπεται άμεσα από το A.3.1 (ii). Για $k = 2$ η (A.7) είναι αληθής, διότι συμπίπτει με την (A.6). Υποθέτοντας ότι για οιονδήποτε φυσικό αριθμό $k \geq 3$ η (A.7) είναι αληθής για $k-1$ προσθετέους, λαμβάνουμε

$$\begin{aligned} f\left(\sum_{i=1}^{k} r_i x_i\right) &= f\left(\sum_{i=1}^{k-1} r_i x_i + r_k x_k\right) \\ &= f\left(\sum_{i=1}^{k-1} r_i x_i\right) + f(r_k x_k) = \sum_{i=1}^{k-1} r_i f(x_i) + r_k f(x_k) = \sum_{i=1}^{k} r_i f(x_i), \end{aligned}$$

όπου η δεύτερη ισότητα έπεται από το A.3.1 (i) και η τρίτη από την επαγωγική μας υπόθεση. Άρα η (A.7) είναι αληθής και για k προσθετέους. □

► **Εικόνες και αντίστροφες εικόνες υπομοδίων μέσω ομομορφισμών**. Οι κύριες ιδιότητες αυτών δίδονται στις προτάσεις A.3.5 και A.3.6.

A.3.5 Πρόταση. *Εάν M, N είναι R-μόδιοι και $f \in \mathrm{Hom}_R(M,N)$, τότε ισχύουν τα εξής:*

(i) *Η αντίστροφη εικόνα $f^{-1}(W)$ οιουδήποτε υπομοδίου W τού N μέσω τού f αποτελεί υπομόδιο τού M.*

(ii) *Ο πυρήνας $\mathrm{Ker}(f)$ τού f* (βλ. (A.4)) *είναι ένας υπομόδιος τού M.*

(iii) *Η εικόνα $f(U) := \{f(u) \,|\, u \in U\}$ οιουδήποτε υπομοδίου U τού M μέσω τού f αποτελεί υπομόδιο τού N.*

(iv) *Η εικόνα $\mathrm{Im}(f)$ τού f* (βλ. (A.5)) *είναι ένας υπομόδιος τού N.*

Απόδειξη. (i) Έστω W τυχών υπομόδιος τού N. Για κάθε ζεύγος $(r,s) \in R \times R$ και για κάθε ζεύγος $(x_1,x_2) \in f^{-1}(W) \times f^{-1}(W)$ έχουμε $f(x_1), f(x_2) \in W$ και

$$f(rx_1 + sx_2) = rf(x_1) + sf(x_2) \in W$$

(λόγω τής προτάσεως A.3.3), οπότε $rx_1 + sx_2 \in f^{-1}(W)$. Αυτό (δυνάμει τής προτάσεως A.2.7) σημαίνει ότι η αντίστροφη εικόνα $f^{-1}(W)$ τού W μέσω τού ομομορφισμού f αποτελεί υπομόδιο τού M.

(ii) Αρκεί να εφαρμοσθεί το (i) στην ειδική περίπτωση όπου $W = \{0_N\}$.

(iii) Έστω U τυχών υπομόδιος τού M. Για κάθε $(r,s) \in R \times R$ και για κάθε $(w_1,w_2) \in f(U) \times f(U)$ υπάρχουν στοιχεία $u_1, u_2 \in U$ με $f(u_1) = w_1$, $f(u_2) = w_2$, και $ru_1 + su_2 \in U$ (διότι το U είναι υπομόδιος τού M, βλ. A.2.7). Επομένως,

$rw_1 + sw_2 = rf(u_1) + sf(u_2) = f(ru_1 + su_2) \in f(U)$ και, ως εκ τούτου, η εικόνα $f(U)$ τού U μέσω τού ομομορφισμού f αποτελεί υπομόδιο τού N (λόγω τής προτάσεως A.3.3).

(iv) Αρκεί να εφαρμοσθεί το (iii) στην ειδική περίπτωση όπου $U = M$. □

A.3.6 Πρόταση. *Έστω U ένας υπομόδιος ενός R-μοδίου M και έστω W ένας υπομόδιος ενός R-μοδίου N. Για κάθε $f \in \mathrm{Hom}_R(M,N)$ ισχύουν τα εξής:*

(i) $f\left(U \cap f^{-1}(W)\right) = f(U) \cap W$.

(ii) $f\left(f^{-1}(W)\right) = \mathrm{Im}(f) \cap W$.

(iii) $f^{-1}(W + f(U)) = f^{-1}(W) + U$.

(iv) $f^{-1}(f(U)) = \mathrm{Ker}(f) + U$.

ΑΠΟΔΕΙΞΗ. (i) Για κάθε $x \in f^{-1}(W)$ έχουμε $f(x) \in W$, οπότε $f\left(f^{-1}(W)\right) \subseteq W$. Επειδή οι σχέσεις εγκλεισμού παραμένουν εν ισχύ κατόπιν εφαρμογής τής απεικονίσεως f, έχουμε

$$\left.\begin{array}{r} f\left(U \cap f^{-1}(W)\right) \subseteq f(U) \\ f\left(U \cap f^{-1}(W)\right) \subseteq f\left(f^{-1}(W)\right) \end{array}\right\} \Longrightarrow f\left(U \cap f^{-1}(W)\right) \subseteq f(U) \cap W.$$

Έστω τώρα τυχόν $w \in f(U) \cap W$. Προφανώς, $w \in W$ και $w = f(u)$ για κάποιο στοιχείο $u \in U$. Επειδή $f(u) \in W$, έχουμε $w \in f\left(U \cap f^{-1}(W)\right)$, οπότε ισχύει και ο αντίστροφος εγκλεισμός $f(U) \cap W \subseteq f\left(U \cap f^{-1}(W)\right)$.

(ii) Αρκεί να εφαρμοσθεί το (i) στην ειδική περίπτωση όπου $U = M$.

(iii) Για κάθε $u \in U$ έχουμε $f(u) \in f(U)$. Κατά συνέπειαν, $U \subseteq f^{-1}(f(U))$. Από το (ii) και από το γεγονός ότι οι σχέσεις εγκλεισμού παραμένουν εν ισχύ κατόπιν θεωρήσεως αντιστρόφων εικόνων προκύπτει ότι

$$\begin{aligned} f^{-1}(W) + U &\subseteq f^{-1}\left(f(f^{-1}(W) + U)\right) \\ &= f^{-1}\left(f(f^{-1}(W)) + f(U)\right) \subseteq f^{-1}(W + f(U)). \end{aligned}$$

Έστω τώρα $y \in f^{-1}(W + f(U))$. Επειδή $f(y) \in W + f(U)$, υπάρχουν $w \in W$ και $u \in U$, τέτοια ώστε να ισχύει $f(y) = w + f(u)$ (βλ. πρόταση A.2.16). Επομένως,

$$f(y + (-u)) = w \in W \Rightarrow y + (-u) \in f^{-1}(\{w\}) \subseteq f^{-1}(W) \Rightarrow y \in f^{-1}(W) + U,$$

οπότε ισχύει και ο αντίστροφος εγκλεισμός $f^{-1}(W + f(U)) \subseteq f^{-1}(W) + U$.

(iv) Αρκεί να εφαρμοσθεί το (iii) στην ειδική περίπτωση όπου $W = \{0_N\}$. □

A.3.7 Πρόταση. *Εάν M, N είναι R-μόδιοι και $f \in \mathrm{Hom}_R(M,N)$, τότε ισχύουν τα εξής:*

(i) *Εάν $\mathcal{E}$ είναι ένα σύστημα γεννητόρων τού M, τότε η εικόνα $f(\mathcal{E})$ αυτού αποτελεί ένα σύστημα γεννητόρων τού R-μοδίου $\mathrm{Im}(f)$.*

(ii) *Εάν $\mathcal{E}'$ είναι ένα σύστημα γεννητόρων τού πυρήνα $\mathrm{Ker}(f)$ τού f και $\mathcal{E}'' \subseteq M$ τέτοιο, ώστε $\mathrm{Lin}_R(f(\mathcal{E}'')) = \mathrm{Im}(f)$, τότε η ένωση $\mathcal{E}' \cup \mathcal{E}''$ αποτελεί ένα σύστημα γεννητόρων τού M.*

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν $x \in M$. Εξ υποθέσεως, υπάρχουν στοιχεία $x_1, ..., x_k$ τού $\mathcal{E}$ και $r_1, ..., r_k \in R$, τέτοια ώστε να ισχύει

$$x = \sum_{j=1}^{k} r_j x_j \Rightarrow f(x) \underset{(\text{A.7})}{=} \sum_{j=1}^{k} r_j \underbrace{f(x_j)}_{\in f(\mathcal{E})} \in \mathrm{Im}(f),$$

οπότε $\mathrm{Im}(f) \subseteq \mathrm{Lin}_R(f(\mathcal{E}))$. Εξάλλου, $f(\mathcal{E}) \subseteq \mathrm{Im}(f) \Rightarrow \mathrm{Lin}_R(f(\mathcal{E})) \subseteq \mathrm{Im}(f)$.
(ii) Έστω τυχόν $x \in M$. Εξ υποθέσεως, υπάρχουν στοιχεία $x_1, ..., x_\rho$ τού $\mathcal{E}''$ και $r_1, ..., r_\rho \in R$, τέτοια ώστε $f(x) = \sum_{j=1}^{\rho} r_j f(x_j)$. Θέτοντας $x' := \sum_{j=1}^{\rho} r_j x_j$ λαμβάνουμε

$$f(x - x') = 0_N \Rightarrow x - x' \in \mathrm{Ker}(f) = \mathrm{Lin}_R(\mathcal{E}'),$$

οπότε υπάρχουν $x_{\rho+1}, ..., x_l \in \mathcal{E}'$ και $r_{\rho+1}, ..., r_l \in R$ με

$$x - x' = \sum_{j=\rho+1}^{l} r_j x_j \Rightarrow x = \sum_{j=1}^{l} r_j x_j,$$

όπου $x_1, ..., x_l \in \mathcal{E}' \cup \mathcal{E}''$. Κατά συνέπειαν, $\mathrm{Lin}_R(\mathcal{E}' \cup \mathcal{E}'') = M$. □

A.3.8 Πόρισμα. *Έστω ότι M, N είναι δυο R-μόδιοι και $f : M \longrightarrow N$ ένας επιμορφισμός. Εάν ο M είναι πεπερασμένως παραγόμενος, τότε και ο N είναι πεπερασμένως παραγόμενος.*

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το (i) τής προτάσεως A.3.7. □

► **Συνθέσεις ομομορφισμών**. Η σύνθεση δυο ομομορφισμών R-μοδίων είναι αφ' εαυτής ομομορφισμός. Η πρόταση A.3.11 περιγράφει λεπτομερώς το πώς σχετίζεται ο πυρήνας και η εικόνα τής συνθέσεως με την εικόνα τού πρώτου εξ αυτών και με τον πυρήνα τού δεύτερου.

A.3.9 Πρόταση. *Εάν M, N, L είναι R-μόδιοι, τότε ισχύει η συνεπαγωγή*

$$[f \in \mathrm{Hom}_R(M, N) \text{ και } g \in \mathrm{Hom}_R(N, L)] \Longrightarrow g \circ f \in \mathrm{Hom}_R(M, L).$$

ΑΠΟΔΕΙΞΗ. Για οιαδήποτε $(x_1, x_2) \in M \times M$ και $(r_1, r_2) \in R \times R$ έχουμε

$$\begin{aligned}(g \circ f)(r_1 x_1 + r_2 x_2) &= g(f(r_1 x_1 + r_2 x_2)) = g(r_1 f(x_1) + r_2 f(x_2)) \\ &= r_1 g(f(x_1)) + r_2 g(f(x_2)) = r_1 (g \circ f)(x_1) + r_2 (g \circ f)(x_2),\end{aligned}$$

οπότε $g \circ f \in \mathrm{Hom}_R(M, L)$ λόγω τής προτάσεως A.3.3. □

A.3.10 Πρόταση. *Εάν M, N, L είναι R-μόδιοι, τότε η σύνθεση ομομορφισμών*

$$\mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(N, L) \ni (f, g) \longmapsto g \circ f \in \mathrm{Hom}_R(M, L)$$

έχει τις εξής ιδιότητες:
(i) $g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$, $(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$,
(ii) $g \circ (rf) = r(g \circ f) = (rg) \circ f$,
για οιοδήποτε $r \in R$ και $f, f_1, f_2 \in \mathrm{Hom}_R(M, N)$, $g, g_1, g_2 \in \mathrm{Hom}_R(N, L)$.

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από τους ορισμούς. □

A.3.11 Πρόταση. *Εάν M, N, L είναι R-μόδιοι και*

$$f \in \mathrm{Hom}_R(M,N), \;\; g \in \mathrm{Hom}_R(N,L),$$

τότε

$$\mathrm{Im}\,(f) \cap \mathrm{Ker}\,(g) = f(\mathrm{Ker}\,(g \circ f)) \;\text{ και }\; \mathrm{Im}\,(f) + \mathrm{Ker}\,(g) = g^{-1}\left(\mathrm{Im}(g \circ f)\right).$$

ΑΠΟΔΕΙΞΗ. (i) Έστω τυχόν στοιχείο $y \in \mathrm{Im}\,(f) \cap \mathrm{Ker}(g)$. Εξ ορισμού, υπάρχει κάποιο $x \in M$, τέτοιο ώστε $y = f(x)$. Επειδή $g(y) = 0_L$, έχουμε $(g \circ f)(x) = 0_L$, οπότε $x \in \mathrm{Ker}(g \circ f)$ και $y \in f(\mathrm{Ker}(g \circ f))$. Και αντιστρόφως· εάν $w \in f(\mathrm{Ker}(g \circ f))$, τότε $w \in \mathrm{Im}\,(f)$ και $w = f(u)$ για κάποιο $u \in \mathrm{Ker}(g \circ f)$, οπότε

$$0_L = (g \circ f)(u) = g(f(u)) = g(w) \Rightarrow w \in \mathrm{Ker}\,(g)\,.$$

(ii) Έστω τυχόν στοιχείο $y \in \mathrm{Im}\,(f) + \mathrm{Ker}(g)$. Εξ ορισμού, $y = y_1 + y_2$ για κάποια $y_1 \in \mathrm{Im}\,(f)$ και $y_2 \in \mathrm{Ker}(g)$. Επομένως, $y_1 = f(x)$ για κάποιο στοιχείο $x \in M$ και $g(y_2) = 0_L$, οπότε

$$g(y) = g(y_1 + y_2) = g(y_1) + g(y_2) = g(f(x)) \in \mathrm{Im}(g \circ f) \Rightarrow y \in g^{-1}(\mathrm{Im}(g \circ f)).$$

Και αντιστρόφως· εάν $w \in g^{-1}\left(\mathrm{Im}(g \circ f)\right)$, τότε έχουμε $g(w) \in \mathrm{Im}(g \circ f)$, οπότε $g(w) = g(f(u))$ για κάποιο $u \in M$,

$$g(w - f(u)) = 0_L \Rightarrow w - f(u) \in \mathrm{Ker}\,(g)$$

και $w = f(u) + (w - f(u)) \in \mathrm{Im}\,(f) + \mathrm{Ker}(g)$. □

A.3.12 Ορισμός. Έστω $f : M \longrightarrow N$ ένας ομομορφισμός R-μοδίων. Ο f καλείται

μονομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι ενριπτική,
επιμορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι επιρριπτική,
ισομορφισμός	$\underset{\text{ορσ}}{\Longleftrightarrow}$	η απεικόνιση f είναι αμφιρριπτική,
ενδομορφισμός (τού M**)**	$\underset{\text{ορσ}}{\Longleftrightarrow}$	$M = N$ (με τις ίδιες πράξεις),
αυτομορφισμός (τού M**)**	$\underset{\text{ορσ}}{\Longleftrightarrow}$	$M = N$ και η f είναι ισομορφισμός.

A.3.13 Πρόταση. *Εάν M, N είναι R-μόδιοι και $f \in \mathrm{Hom}_R(M,N)$, τότε τα ακόλουθα είναι ισοδύναμα* :

(i) *Ο f είναι μονομορφισμός.*

(ii) $\mathrm{Ker}(f) = \{0_M\}$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν ο $f : M \longrightarrow N$ είναι μονομορφισμός, τότε για κάθε στοιχείο $x \in \mathrm{Ker}(f)$ έχουμε $f(x) = 0_N = f(0_M) \Rightarrow x = 0_M$, οπότε τελικώς $\mathrm{Ker}(f) = \{0_M\}$.
(ii)⇒(i) Εάν $\mathrm{Ker}(f) = \{0_M\}$ και για δυο στοιχεία $x, x' \in M$ ισχύει $f(x) = f(x')$, τότε

$$\begin{aligned} 0_N &= f(x) + (-f(x')) = f(x) + f(-x') = f(x + (-x')) \\ &\Longrightarrow x - x' = x + (-x') \in \mathrm{Ker}\,(f) = \{0_M\}, \end{aligned}$$

οπότε $x = x'$, απ' όπου έπεται ότι ο $f : M \longrightarrow N$ είναι μονομορφισμός. □

Α.3.14 Παραδείγματα. Έστω R τυχών μεταθετικός μη τετριμμένος δακτύλιος.
(i) Για οιουσδήποτε R-μοδίους M και N η *μηδενική απεικόνιση* $0 \in N^M$,

$$0 : M \longrightarrow N,\ \ x \longmapsto 0(x) := 0_N, \tag{A.8}$$

είναι (προφανώς) ομομορφισμός, **ο μηδενικός ομομορφισμός**.
(ii) Για οιονδήποτε R-μόδιο M η **ταυτοτική απεικόνιση**

$$\mathrm{id}_M : M \longrightarrow M,\ x \longmapsto \mathrm{id}_M(x) := x,$$

είναι ένας *αυτομορφισμός* τού M. Οι **ομοθετικές απεικονίσεις**

$$f_r : M \longrightarrow M,\ r \longmapsto f_r(x) := rx, \tag{A.9}$$

για κάποιο $r \in R$, είναι *ομομορφισμοί*. ($f_{0_R} = 0$, $f_{1_R} = \mathrm{id}_M$.) Επίσης, εάν ο U είναι ένας υπομόδιος τού M, η **συνήθης ένθεση**[10]

$$\mathrm{in}_{U,M} : U \hookrightarrow M,\ x \longmapsto \mathrm{in}_{U,M}(x) := x, \tag{A.10}$$

τού U **στον** M είναι ένας *μονομορφισμός*.
(iii) Εάν M, N είναι R-μόδιοι και $f \in \mathrm{Hom}_R(M, N)$, τότε έχουμε $f = \mathrm{in}_{\mathrm{Im}(f),N} \circ \check{f}$, όπου

$$\check{f} : M \twoheadrightarrow \mathrm{Im}(f),\ x \longmapsto \check{f}(x) := f(x) \tag{A.11}$$

ο επιμορφισμός ο επαγόμενος μέσω τού f.
(iv) Η απεικόνιση

$$f : R^{\mathbb{N}_0} \longrightarrow R^{\mathbb{N}_0},\ \ (a_n)_{n\in\mathbb{N}_0} \longmapsto (b_n)_{n\in\mathbb{N}_0},$$

όπου $b_0 := 0_K$, $b_n := a_{n-1}$, $\forall n \in \mathbb{N}$, είναι μονομορφισμός αλλά *δεν είναι* επιμορφισμός.
(v) Η απεικόνιση

$$f : R^{\mathbb{N}_0} \longrightarrow R^{\mathbb{N}_0},\ \ (a_n)_{n\in\mathbb{N}_0} \longmapsto (c_n)_{n\in\mathbb{N}_0},$$

όπου $c_n := a_{n+1}$, $\forall n \in \mathbb{N}_0$, είναι επιμορφισμός αλλά *δεν είναι* μονομορφισμός.

[10] Αργότερα, αντί τού $\mathrm{in}_{U,M}$ θα χρησιμοποιηθούν και συντομότεροι συμβολισμοί (όπως ι, i, j, ενίοτε και με κάποιους δείκτες, κ.ά.) για τις συνήθεις ενθέσεις υπομοδίων.

Οι προτάσεις A.3.15 και A.3.16 έπονται άμεσα από τις γνωστές ιδιότητες των ενριπτικών, επιρριπτικών και αμφιρριπτικών απεικονίσεων μεταξύ συνόλων.

A.3.15 Πρόταση. *Έστω ότι οι M, N, L είναι R-μόδιοι και*

$$f \in \mathrm{Hom}_R(M,N), \;\; g \in \mathrm{Hom}_R(N,L).$$

Τότε για τον $g \circ f \in \mathrm{Hom}_R(M,L)$ ισχύουν τα ακόλουθα:

(i) *Εάν οι f και g είναι μονομορφισμοί, τότε και ο $g \circ f$ είναι μονομορφισμός.*

(ii) *Εάν οι f και g είναι επιμορφισμοί, τότε και ο $g \circ f$ είναι επιμορφισμός.*

(iii) *Εάν οι f και g είναι ισομορφισμοί, τότε και ο $g \circ f$ είναι ισομορφισμός.*

(iv) *Εάν ο $g \circ f$ είναι μονομορφισμός, τότε ο f είναι μονομορφισμός.*

(v) *Εάν ο $g \circ f$ είναι επιμορφισμός, τότε ο g είναι επιμορφισμός.*

(vi) *Εάν ο $g \circ f$ είναι ισομορφισμός, τότε ο f είναι μονομορφισμός και ο g είναι επιμορφισμός.*

A.3.16 Πρόταση. *Εάν M, N είναι R-μόδιοι και $f \in \mathrm{Hom}_R(M,N)$ ένας ισομορφισμός, τότε και η αντίστροφη απεικόνιση $f^{-1} : N \longrightarrow M$ είναι ισομορφισμός.*

A.3.17 Σημείωση. (i) Λέμε ότι δυο R-μόδιοι M και N είναι (μεταξύ τους) **ισόμορφοι** ή ότι ο M είναι **ισόμορφος με τον** N και σημειώνουμε[11]: $M \cong N$ όταν υπάρχει κάποιος ισομορφισμός[12] $f : M \longrightarrow N$.

(ii) Είναι εύκολος ο έλεγχος (μέσω τού (iii) τής προτάσεως A.3.15 και τής προτάσεως A.3.16) τού ότι η διμελής σχέση "$\cong$" ορίζει μια σχέση ισοδυναμίας επί οιουδήποτε συνόλου απαρτιζομένου από R-μοδίους. Οι κλάσεις ισοδυναμίας ως προς την "$\cong$" ονομάζονται **κλάσεις ισομορφίας**. Δυο R-μόδιοι λογίζονται ως (μοδιοθεωρητικώς) *ταυτιζόμενοι* όταν είναι μεταξύ τους ισόμορφοι, ήτοι όταν ανήκουν στην ίδια κλάση ισομορφίας. Ως εκ τούτου, ο μοδιοθεωρητικός προσδιορισμός μιας οικογενείας R-μοδίων, τα μέλη τής οποίας έχουν μια *ειδική* ιδιότητα, ισοδυναμεί με την *ταξινόμηση* των μελών της *μέχρις ισομορφισμού* [13].

(iii) Ένα *μονοσύνολο* μπορεί να θεωρηθεί κατά έναν και μόνον τρόπο[14] ως μόδιος υπεράνω οιουδήποτε (παγιωμένου) μεταθετικού μη τετριμμένου δακτυλίου R και δυο τέτοια μονοσύνολα είναι μεταξύ τους ισόμορφα (ως R-μόδιοι). Ο *μέχρις ισομορφισμού μονοσημάντως ορισμένος* R-μόδιος με ένα μονοσύνολο ως υποκείμενο

[11] Κατ' αναλογίαν, το σύμβολο $M \ncong N$ θα δηλοί ότι ο M δεν είναι ισόμορφος με τον N.

[12] Ενίοτε, για να τονίσουμε (π.χ., σε μεταθετικά διαγράμματα και αλλού) ότι ένας ομομορφισμός $f : M \longrightarrow N$ είναι *ισομορφισμός*, γράφουμε $f : M \xrightarrow{\cong} N$.

[13] Η φράση «ταξινόμηση μέχρις ισομορφισμού» ή «με ακρίβεια ισομορφισμού» (up to isomorphism) δηλοί τη «διάκριση (R-μοδίων) με μόνο κριτήριο ταυτίσεως τη διαμεσολάβηση κάποιου ισομορφισμού».

[14] Εν τοιαύτη περιπτώσει, εάν $M = \{x\}$, τότε $x + x := x$ και $rx := x$ για κάθε $r \in R$. (Προφανώς, $0_M = x$.)

σύνολό του ονομάζεται **τετριμμένος** R-**μόδιος** και θα συμβολίζεται εφεξής απλώς ως[15] $\{0\}$.

► **«Συμπληρώσεις» τριγώνων**. Ο ταυτόχρονος χειρισμός πολλών συντιθέμενων ομομορφισμών R-μοδίων τοποθετημένων σε (ενίοτε πολύ μεγάλα) διαγράμματα απαιτεί ιδιαίτερη προσοχή. Όπως, επίσης, και η εξεύρεση κατάλληλων συνθηκών, υπό τις οποίες διασφαλίζεται *η ύπαρξη* ή *η κατασκευή* ομομορφισμών που «συμπληρώνουν» κάποια *ελλείποντα βέλη* εντός αυτών. Τέτοιου είδους συνθήκες, όπως θα δούμε στα θεωρήματα A.3.24 και A.3.25, είναι εκ τής φύσεώς τους *αρκούντως περιοριστικές* ακόμη και στην απλούστερη των περιπτώσεων (ήτοι σε εκείνην ενός *τριγώνου*). Ας γυρίσουμε, όμως, προς στιγμήν, κάπως πιο πίσω, *ξεχνώντας* την αλγεβρική δομή τού R-μοδίου κι ας υποθέσουμε ότι διαθέτουμε απλώς τρία μη κενά σύνολα A, B και C. Ευλόγως τίθενται τα εξής ερωτήματα:

• **Ερώτημα 1**: Εάν δοθούν απεικονίσεις f και g (όπως δείχνονται στο κάτωθι αριστερά ευρισκόμενο διάγραμμα) *εκπορευόμενες από το* A (ήτοι έχουσες ως *πεδίο ορισμού τους* το A), πότε υφίσταται απεικόνιση $h : B \longrightarrow C$ η οποία «συμπληρώνει» (ή «κλείνει») το τρίγωνο το καθοριζόμενο από τα A, B και C (όπως δείχνεται στο κάτωθι δεξιά ευρισκόμενο διάγραμμα);

$$\begin{tikzcd} & A \arrow[dl, "f"'] \arrow[dr, "g"] & \\ B & & C \end{tikzcd} \qquad \begin{tikzcd} & A \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[d, phantom, "\circlearrowleft"] & \\ B \arrow[rr, dashed, "h"'] & {} & C \end{tikzcd}$$

• **Ερώτημα 2**: Εάν δοθούν απεικονίσεις f και g (όπως στο κάτωθι αριστερά ευρισκόμενο διάγραμμα) *απολήγουσες στο* A (ήτοι έχουσες ως *πεδίο τιμών τους* το A), πότε υφίσταται απεικόνιση $h : C \longrightarrow B$ η οποία «συμπληρώνει» το τρίγωνο το καθοριζόμενο από τα A, B και C;

$$\begin{tikzcd} & A & \\ B \arrow[ur, "f"] & & C \arrow[ul, "g"'] \end{tikzcd} \qquad \begin{tikzcd} & A \arrow[d, phantom, "\circlearrowleft"] & \\ B \arrow[ur, "f"] & {} & C \arrow[ul, "g"'] \arrow[ll, dashed, "h"] \end{tikzcd}$$

Οι απαντήσεις περιέχονται στις προτάσεις A.3.18 και A.3.19, αντιστοίχως.

A.3.18 Πρόταση. *Εάν A, B, C είναι μη κενά σύνολα και $f : A \longrightarrow B$, $g : A \longrightarrow C$ απεικονίσεις, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

[15] Εν προκειμένω, υφίσταται μια διαφορά μεταξύ τού «τετριμμένου R-μοδίου», όπως εισήχθη εδώ, και τού «τετριμμένου υπομοδίου δοθέντος R-μοδίου», όπως είχε εισαχθεί στο εδάφιο A.2.9 (ii). Ο πρώτος εκφράζει μια *απόλυτη* έννοια (*μέχρις ισομορφισμού*), ενώ ο δεύτερος εκφράζει μια *σχετική* έννοια (παρότι είναι *συνολοθεωρητικώς* μονοσημάντως ορισμένος), αφού είναι -εκ παραλλήλου- απαραίτητη η αναφορά τού R-μοδίου εντός τού οποίου περιέχεται (ως το μονοσύνολο το περιέχον ως στοιχείο του το ουδέτερο στοιχείο τής προσθετικής του ομάδας).

(i) *Υφίσταται μια απεικόνιση* $h : B \longrightarrow C$ *με* $h \circ f = g$.

(ii) $(\forall (x,y) \in A \times A)\ [f(x) = f(y) \Longrightarrow g(x) = g(y)]$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Για οιοδήποτε ζεύγος $(x,y) \in A \times A$ για το οποίο ισχύει $f(x) = f(y)$ έχουμε $g(x) = (h \circ f)(x) = h(f(x)) = h(f(y)) = (h \circ f)(y) = g(y)$.

(ii)⇒(i) Θεωρούμε το σύνολο

$$\mathcal{G} := \{(y,z) \in \mathrm{Im}(f) \times C \,|\, \exists x \in A : y = f(x), z = g(x)\}.$$

Κατ' αρχάς παρατηρούμε ότι $\mathcal{G} \neq \varnothing$, διότι για κάθε $x \in A$ έχουμε $(f(x), g(x)) \in \mathcal{G}$. Για οιοδήποτε $y \in \mathrm{Im}(f)$ υπάρχει *ένα και μόνον* $z \in C$, τέτοιο ώστε να ισχύει $(y,z) \in \mathcal{G}$. (Πράγματι· εάν $y = f(x)$, για κάποιο $x \in A$, τότε θέτουμε $z := g(x)$. Εάν υποθέσουμε ότι $(y,z), (y,z') \in \mathcal{G}$, τότε υπάρχουν $x, x' \in A$ με $y = f(x) = f(x')$ και $z = g(x)$, $z' = g(x')$. Εξ υποθέσεως, $g(x) = g(x')$, οπότε $z = z'$.) Άρα ορίζεται (καλώς) μια απεικόνιση $\beta : \mathrm{Im}(f) \longrightarrow C$, $\beta(f(x)) := g(x), \forall x \in A$, και (μέσω αυτής) η απεικόνιση $h : B \longrightarrow C$,

$$h(y) := \begin{cases} \beta(y), & \text{όταν } y \in \mathrm{Im}(f), \\ \text{κάποιο παγιωμένο } c \in C, & \text{όταν } y \notin \mathrm{Im}(f). \end{cases}$$

Προφανώς, $(h \circ f)(x) = h(f(x)) = \beta(f(x)) = g(x)$ για κάθε $x \in A$. □

A.3.19 Πρόταση. *Εάν* A, B, C *είναι μη κενά σύνολα και* $f : B \longrightarrow A$, $g : C \longrightarrow A$ *απεικονίσεις, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Υφίσταται μια απεικόνιση* $h : C \longrightarrow B$ *με* $f \circ h = g$.

(ii) $\mathrm{Im}(g) \subseteq \mathrm{Im}(f)$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) $g(x) = f(h(x)) \in \mathrm{Im}(g), \forall x \in C$, οπότε $\mathrm{Im}(g) \subseteq \mathrm{Im}(f)$.

(ii)⇒(i) Για κάθε $x \in C$ υπάρχει $y \in B : g(x) = f(y)$, οπότε $f^{-1}(\{g(x)\}) \neq \varnothing$. Αυτό σημαίνει ότι το $\mathcal{E} := \left\{ f^{-1}(\{g(x)\}) \middle| x \in C \right\}$ αποτελεί μια οικογένεια υποσυνόλων τού B, καθένα των οποίων είναι μη κενό. Σύμφωνα με το *αξίωμα τής επιλογής*, $\exists \alpha : \mathcal{E} \longrightarrow \bigcup \mathcal{E} : \alpha(Y) \in Y,\ \forall Y \in \mathcal{E}$. Επομένως,

$$\begin{aligned} [\alpha(Y) \in Y,\ \forall Y \in \mathcal{E}] \quad &\Leftrightarrow \quad [\forall x \in C : \alpha(f^{-1}(\{g(x)\})) \in f^{-1}(\{g(x)\})] \\ &\Leftrightarrow \quad [\forall x \in C : f(\alpha(f^{-1}(\{g(x)\}))) \in \{g(x)\}] \\ &\Leftrightarrow \quad [\forall x \in C : f(\alpha(f^{-1}(\{g(x)\}))) = g(x)] \end{aligned}$$

και (γι' αυτόν τον λόγο) η $h : C \longrightarrow B$, $x \longmapsto h(x) := \alpha(f^{-1}(\{g(x)\}))$ είναι μια *καλώς ορισμένη* απεικόνιση με $(f \circ h)(x) = f(h(x)) = g(x)$ για κάθε $x \in C$. □

A.3.20 Παρατήρηση. Εάν κανείς επαναδιατυπώσει τα ανωτέρω ερωτήματα 1 και 2 αντικαθιστώντας τά σύνολα A, B, C με R-μοδίους M, N, L και υποθέσει (α) ότι οι

f και g είναι *ομομορφισμοί* και (β) ότι οι συνθήκες (ii) των προτάσεων Α.3.18 και Α.3.19 ικανοποιούνται, αξιώνοντας, εκ παραλλήλου, από τις κατασκευαζόμενες απεικονίσεις h να είναι ωσαύτως *ομομορφισμοί*, η απάντηση σε αμφότερα (όπως προδήλως προκύπτει από τα παραδείγματα Α.3.21 και από τα θεωρήματα Α.3.24 και Α.3.25) θα είναι: *Μόνον υπό επιπρόσθετες, ειδικότερες προϋποθέσεις*!

Α.3.21 Παραδείγματα. (i) Έστω $k \in \mathbb{N}$, $k \geq 2$. Εάν $M = N = L = \mathbb{Z}$ ($\mathbb{Z}$ ως $\mathbb{Z}$-μόδιος) και[16] $f := k\mathrm{id}_{\mathbb{Z}}$, $g := \mathrm{id}_{\mathbb{Z}}$, τότε η συνθήκη (ii) τής προτάσεως Α.3.18 ικανοποιείται, οπότε υπάρχει κάποια *απεικόνιση* $h : \mathbb{Z} \longrightarrow \mathbb{Z}$ με $h \circ f = g$.

$$\begin{tikzcd}
& \mathbb{Z} \arrow[dl, "k\,\mathrm{id}_{\mathbb{Z}}"'] \arrow[dr, "\mathrm{id}_{\mathbb{Z}}"] \arrow[d, phantom, "\circlearrowleft"] & \\
\mathbb{Z} \arrow[rr, dashed, "h"'] & & \mathbb{Z}
\end{tikzcd}$$

Επιπροσθέτως, $f, g \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$. Ωστόσο, ο f δεν είναι επιμορφισμός και η h *δεν μπορεί* να είναι ενδομορφισμός τού $\mathbb{Z}$, διότι εάν ήταν θα είχαμε

$$kh(\xi) = h(k\xi) = (h \circ (k\,\mathrm{id}_{\mathbb{Z}}))(\xi) = (h \circ f)(\xi) = g(\xi) = \xi, \ \forall \xi \in \mathbb{Z}.$$

Ειδικότερα, $kh(1) = 1$, πράγμα αδύνατο, διότι θα έπρεπε να ισχύει $h(1) \in \mathbb{Z}$.

(ii) Έστω p ένας πρώτος αριθμός. Μέσω τής υποομάδας $\mathbb{Z}[\frac{1}{p}] := \{ \frac{a}{p^i} \,\big|\, a \in \mathbb{Z}, i \in \mathbb{N}_0 \}$ τής $(\mathbb{Q}, +)$ ορίζουμε την υποομάδα[17]

$$\mathbb{Z}(p^{\infty}) := \mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z} = \left\{ \tfrac{a}{p^i} + \mathbb{Z} \,\middle|\, a \in \mathbb{Z}, i \in \mathbb{N}_0 \right\}$$

τής πηλικοομάδας $(\mathbb{Q}/\mathbb{Z}, +)$. Αυτή καθίσταται κατά τρόπο φυσικό $\mathbb{Z}$-μόδιος[18]. Θέτοντας $M = N = L = \mathbb{Z}(p^{\infty})$, $f(x) := px$, $\forall x \in \mathbb{Z}(p^{\infty})$, και $g := \mathrm{id}_{\mathbb{Z}(p^{\infty})}$, παρατηρούμε ότι $f, g \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}(p^{\infty}), \mathbb{Z}(p^{\infty}))$ και ότι η συνθήκη Α.3.19 (ii) ικανοποιείται, καθώς ισχύει $\frac{a}{p^i} + \mathbb{Z} = p(\frac{a}{p^{i+1}} + \mathbb{Z})$ για κάθε $a \in \mathbb{Z}$ και για κάθε $i \in \mathbb{N}_0$ (οπότε $\mathrm{Im}(g) = \mathrm{Im}(f) = \mathbb{Z}(p^{\infty})$). Άρα υπάρχει κάποια *απεικόνιση* $h : \mathbb{Z}(p^{\infty}) \longrightarrow \mathbb{Z}(p^{\infty})$ με $f \circ h = \mathrm{id}_{\mathbb{Z}(p^{\infty})}$.

$$\begin{tikzcd}
& \mathbb{Z}(p^{\infty}) \arrow[d, phantom, "\circlearrowleft"] & \\
\mathbb{Z}(p^{\infty}) \arrow[ur, "f"] & & \mathbb{Z}(p^{\infty}) \arrow[ul, "\mathrm{id}_{\mathbb{Z}(p^{\infty})}"'] \arrow[ll, dashed, "h"]
\end{tikzcd}$$

[16] Αυτό σημαίνει ότι $f(\xi) := k\xi$ για κάθε $\xi \in \mathbb{Z}$.

[17] Η $(\mathbb{Z}(p^{\infty}), +)$ καλείται, ιδιαιτέρως, p-**σχεδόν κυκλική ομάδα** (διότι είναι μια *μη πεπερασμένως παραγόμενη* ομάδα, κάθε *γνήσια* υποομάδα τής οποίας είναι πεπερασμένη και κυκλική, έχουσα ως τάξη της μια δύναμη τού p.)

[18] Αριθμητικός πολλαπλασιασμός: $\mathbb{Z} \times \mathbb{Z}(p^{\infty}) \ni (\lambda, \frac{a}{p^i} + \mathbb{Z}) \longmapsto \frac{\lambda a}{p^i} + \mathbb{Z} \in \mathbb{Z}(p^{\infty})$.

Ωστόσο, η h *δεν μπορεί* να είναι ενδομορφισμός τού $\mathbb{Z}(p^{\infty})$, διότι εάν ήταν θα είχαμε

$$\begin{aligned} \tfrac{1}{p} + \mathbb{Z} &= f(h(\tfrac{1}{p} + \mathbb{Z})) = ph(\tfrac{1}{p} + \mathbb{Z}) = h(p(\tfrac{1}{p} + \mathbb{Z})) \\ &= h(1 + \mathbb{Z}) = h(0 + \mathbb{Z}) = h(0_{\mathbb{Z}(p^{\infty})}) = 0_{\mathbb{Z}(p^{\infty})} = 0 + \mathbb{Z}, \end{aligned}$$

ήτοι $\frac{1}{p} \in \mathbb{Z}$. (Άτοπο!)

Κατάλληλες *επιπρόσθετες* προϋποθέσεις (υπό τις οποίες οι απεικονίσεις h που συμπληρώνουν τα τρίγωνα καθίστανται ομομορφισμοί, όπως ζητείται στα *αναθεωρημένα* ερωτήματα 1 και 2 τού εδ. A.3.20) μπορούν να εντοπισθούν εάν ανατρέξουμε στα στοιχειώδη λήμματα A.3.22 και A.3.23 τα περιγράφοντα συνθήκες ισοδύναμες τής *επιρριπτικότητας* και, αντιστοίχως, τής *ενριπτικότητας* μιας απεικονίσεως. Η *επιρριπτικότητα* τού ομομορφισμού f (στην πρώτη περίπτωση) και η *ενριπτικότητα* αυτού (στη δεύτερη περίπτωση) είναι δυνατόν να μας οδηγήσουν σε *μοδιοθεωρητικά ανάλογα* των προτάσεων A.3.18 και A.3.19. Και μάλιστα και σε κάτι πιο ισχυρό: Στη *μοναδικότητα* των δημιουργούμενων ομομορφισμών h.

A.3.22 Λήμμα. *Εάν A, B είναι μη κενά σύνολα και $f : A \longrightarrow B$ μια απεικόνιση, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Η f είναι επιρριπτική απεικόνιση.*

(ii) *Υπάρχει κάποια απεικόνιση $\gamma : B \longrightarrow A$, ούτως ώστε να ισχύει $f \circ \gamma = \mathrm{id}_B$.*

(iii) *Η f είναι «εκ δεξιών διαγράψιμη», δηλαδή για οιοδήποτε μη κενό σύνολο C και οιεσδήποτε απεικονίσεις $h_1 : B \longrightarrow C$ και $h_2 : B \longrightarrow C$ ισχύει η συνεπαγωγή*

$$h_1 \circ f = h_2 \circ f \Longrightarrow h_1 = h_2.$$

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν η f είναι επιρριπτική απεικόνιση, τότε για κάθε στοιχείο $y \in B = \mathrm{Im}(f) = f(A)$ επιλέγουμε[19] ένα $x_y \in A$, ούτως ώστε να ισχύει $f(x_y) = y$, και ορίζουμε την απεικόνιση $\gamma : B \longrightarrow A,\ y \longmapsto \gamma(y) := x_y$. Τότε

$$(f \circ \gamma)(y) = f(\gamma(y)) = f(x_y) = y = \mathrm{id}_B(y) \Longrightarrow f \circ \gamma = \mathrm{id}_B.$$

(ii)⇒(iii) Υποθέτουμε ότι υπάρχει κάποια απεικόνιση $\gamma : B \longrightarrow A$, ούτως ώστε να ισχύει $f \circ \gamma = \mathrm{id}_B$. Για οιεσδήποτε απεικονίσεις $h_1 : B \longrightarrow C$ και $h_2 : B \longrightarrow C$ για τις οποίες ισχύει η ισότητα $h_1 \circ f = h_2 \circ f$ λαμβάνουμε

$$\begin{aligned} h_1 \circ f = h_2 \circ f &\Rightarrow (h_1 \circ f) \circ \gamma = (h_2 \circ f) \circ \gamma \\ \Rightarrow h_1 \circ (f \circ \gamma) = h_2 \circ (f \circ \gamma) &\Rightarrow h_1 = h_1 \circ \mathrm{id}_B = h_2 \circ \mathrm{id}_B = h_2. \end{aligned}$$

(iii)⇒(i) Υποθέτουμε ότι η f είναι «εκ δεξιών διαγράψιμη». Εάν το B είναι μονοσύνολο, τότε η f είναι προδήλως επιρριπτική. Εάν το B περιέχει τουλάχιστον δύο στοιχεία y_1, y_2 με $y_1 \neq y_2$, τότε ορίζουμε τις απεικονίσεις

$$h_1(y) := \begin{cases} y, & \text{όταν } y \in \mathrm{Im}(f), \\ y_1, & \text{όταν } y \notin \mathrm{Im}(f), \end{cases} \qquad h_2(y) := \begin{cases} y, & \text{όταν } y \in \mathrm{Im}(f), \\ y_2, & \text{όταν } y \notin \mathrm{Im}(f). \end{cases}$$

[19] Αρκεί να εφαρμοσθεί εκ νέου το *αξίωμα τής επιλογής* (όπως στο (ii)⇒(i) τής προτάσεως A.3.19), αλλά εδώ για την οικογένεια $\mathcal{E} := \{\, f^{-1}(\{y\}) \mid y \in B \}$ (μη κενών) υποσυνόλων τού A.

Προφανώς, $h_1(f(x)) = f(x) = h_2(f(x))$ για κάθε $x \in X$, οπότε

$$h_1 \circ f = h_2 \circ f \Longrightarrow h_1 = h_2.$$

Εάν υπήρχε κάποιο $y \in B \setminus \mathrm{Im}(f)$, τότε θα ίσχυε $h_1(y) = h_2(y) \Rightarrow y_1 = y_2$, ήτοι κάτι που θα αντέκειτο στην υπόθεσή μας. Επομένως, $B = \mathrm{Im}(f)$. □

A.3.23 Λήμμα. *Εάν A, B είναι μη κενά σύνολα και $f : A \longrightarrow B$ μια απεικόνιση, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Η f είναι ενριπτική απεικόνιση.*

(ii) *Υπάρχει κάποια απεικόνιση $\gamma : B \longrightarrow A$, ούτως ώστε να ισχύει $\gamma \circ f = \mathrm{id}_A$.*

(iii) *Η f είναι «εξ αριστερών διαγράψιμη», δηλαδή για οιοδήποτε μη κενό σύνολο C και οιεσδήποτε απεικονίσεις $h_1 : C \longrightarrow A$ και $h_2 : C \longrightarrow A$ ισχύει η συνεπαγωγή*

$$f \circ h_1 = f \circ h_2 \Longrightarrow h_1 = h_2.$$

Απόδειξη. (i)⇒(ii) Εάν η f είναι ενριπτική, τότε για όλα τα $y \in \mathrm{Im}(f) = f(A)$ οι ίνες $f^{-1}(\{y\})$ θα αποτελούνται από ένα και μόνον στοιχείο τού A. Ας συμβολίσουμε λοιπόν για κάθε $y \in \mathrm{Im}(f)$ αυτό το στοιχείο ως x_y. (Για το x_y ισχύει εξ ορισμού $f(x_y) = y$). Αντιθέτως, για κάθε $y \in B \setminus \mathrm{Im}(f)$ έχουμε $f^{-1}(\{y\}) = \varnothing$. Παγιώνουμε εφεξής ένα στοιχείο $x_0 \in A$ (σημειωτέον ότι το A δεν είναι κενό) και ορίζουμε μια απεικόνιση $\gamma : B \longrightarrow A$ ως ακολούθως:

$$\gamma(y) := \begin{cases} x_y, & \text{όταν } y \in \mathrm{Im}(f), \\ x_0, & \text{όταν } y \in B \setminus \mathrm{Im}(f). \end{cases}$$

Τότε για κάθε $x \in A$ λαμβάνουμε $(\gamma \circ f)(x) = \gamma(f(x)) = x_y$, όπου $y := f(x)$, οπότε $f^{-1}(\{y\}) = f^{-1}(\{f(x)\}) = \{x\}$, απ' όπου έπεται ότι $x_y = x = \mathrm{id}_A(x)$, ήτοι $\gamma \circ f = \mathrm{id}_A$.

(ii)⇒(i) Εάν υπάρχει μια απεικόνιση $\gamma : B \longrightarrow A$ με $\gamma \circ f = \mathrm{id}_A$ και εάν τα x_1, x_2 είναι δυο στοιχεία τού A, ούτως ώστε $f(x_1) = f(x_2)$, τότε

$$x_1 = \mathrm{id}_A(x_1) = (\gamma \circ f)(x_1) = \gamma(f(x_1)) = \gamma(f(x_2)) = (\gamma \circ f)(x_2) = \mathrm{id}_A(x_2) = x_2.$$

Άρα η f είναι όντως ενριπτική.

(ii)⇒(iii) Κατά την υπόθεσή μας, $f \circ h_1 = f \circ h_2$. Επομένως,

$$\begin{aligned} \gamma \circ (f \circ h_1) &= \gamma \circ (f \circ h_2) \Rightarrow (\gamma \circ f) \circ h_1 = (\gamma \circ f) \circ h_2 \\ &\Rightarrow \mathrm{id}_A \circ h_1 = \mathrm{id}_A \circ h_1 \Rightarrow h_1 = h_2. \end{aligned}$$

(iii)⇒(ii) Εάν η f είναι «εξ αριστερών διαγράψιμη» και υποθέσουμε ότι δεν είναι ενριπτική, τότε θα υπάρχουν $x, y \in A$, $x \neq y$, με $f(x) = f(y)$. Για οιοδήποτε μη κενό σύνολο C ορίζουμε τις σταθερές απεικονίσεις

$$h_1 : C \longrightarrow A, \ \ c \mapsto h_1(c) := x, \ \ h_2 : C \longrightarrow A, \ \ c \mapsto h_2(c) := y.$$

Παρατηρούμε ότι $h_1 \neq h_2$ αλλά $f \circ h_1 = f \circ h_2$. Άτοπο! Άρα η f είναι κατ' ανάγκην ενριπτική. □

A.3.24 Θεώρημα. *Εάν M, N, L είναι R-μόδιοι, $f : M \longrightarrow N$ ένας επιμορφισμός και $g \in \mathrm{Hom}_R(M, L)$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Υφίσταται ένας και μόνον $h \in \mathrm{Hom}_R(N, L)$ με $h \circ f = g$.*

$$\begin{tikzcd} & M \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[d, phantom, "\circlearrowleft"] & \\ N \arrow[rr, dashed, "h"'] & {} & L \end{tikzcd}$$

(ii) $\mathrm{Ker}(f) \subseteq \mathrm{Ker}(g)$.

Επιπροσθέτως, στην περίπτωση κατά την οποία ικανοποιούνται οι ανωτέρω συνθήκες, ισχύουν τα εξής:

(a) *O h είναι μονομορφισμός* $\Longleftrightarrow \mathrm{Ker}(f) = \mathrm{Ker}(g)$.

(b) *O h είναι επιμορφισμός $\Longleftrightarrow$ ο g είναι επιμορφισμός.*

Απόδειξη. (i)⇒(ii) Έστω τυχόν $x \in \mathrm{Ker}(f)$. Τότε

$$g(x) = h(f(x)) = h(0_N) = 0_L \Longrightarrow x \in \mathrm{Ker}(g),$$

οπότε $\mathrm{Ker}(f) \subseteq \mathrm{Ker}(g)$.

(ii)⇒(i) Υποθέτουμε, αντιστρόφως, ότι $\mathrm{Ker}(f) \subseteq \mathrm{Ker}(g)$. Εάν $(x_1, x_2) \in M \times M$ με $f(x_1) = f(x_2)$, τότε

$$f(x_1 - x_2) = f(x_1) - f(x_2) = 0_N \Rightarrow x_1 - x_2 \in \mathrm{Ker}(f) \subseteq \mathrm{Ker}(g),$$

οπότε $0_N = g(x_1 - x_2) = g(x_1) - g(x_2) \Rightarrow g(x_1) = g(x_2)$. Κατόπιν εφαρμογής τής συνεπαγωγής (ii)⇒(i) τής προτάσεως A.3.18 (με τους M, N, L στη θέση των εκεί παρατεθέντων A, B και C, αντιστοίχως) εξασφαλίζουμε την ύπαρξη μιας απεικονίσεως $h : N \longrightarrow L$ για την οποία ισχύει $h \circ f = g$. Επειδή η απεικόνιση f είναι (εξ υποθέσεως) επιρριπτική, η h (σύμφωνα με τη συνεπαγωγή (i)⇒(iii) τού λήμματος A.3.22) είναι η μοναδική απεικόνιση από τον N στον L που πληροί αυτήν την ιδιότητα. Απομένει λοιπόν να αποδειχθεί ότι $h \in \mathrm{Hom}_R(N, L)$. Προς τούτο θεωρούμε τυχόντα ζεύγη $(y_1, y_2) \in N \times N$ και $(r_1, r_2) \in R \times R$. Λόγω τής επιρριπτικότητας τής απεικονίσεως f υπάρχουν $x_1, x_2 \in M$, τέτοια ώστε να ισχύει $f(x_1) = y_1$ και $f(x_2) = y_2$. Επειδή οι f, g είναι ομομορφισμοί, λαμβάνουμε

$$\begin{aligned} & h\left(r_1 y_1 + r_2 y_2\right) = h\left(r_1 f(x_1) + r_2 f(x_2)\right) = h(f(r_1 x_1 + r_2 x_2)) = (h \circ f)\left(r_1 x_1 + r_2 x_2\right) \\ & = g(r_1 x_1 + r_2 x_2) = r_1 g(x_1) + r_2 g(x_2) = r_1 \left(h \circ f\right)(x_1) + r_2 \left(h \circ f\right)(x_2) \\ & = r_1 h(f(x_1)) + r_2 h(f(x_2)) = r_1 h(y_1) + r_2 h(f(y_2)), \end{aligned}$$

οπότε η h είναι ωσαύτως ομομορφισμός. (Βλ. πρόταση A.3.3.)

Εν συνεχεία, υποθέτοντας ότι ικανοποιούνται οι συνθήκες (i), (ii), θα αποδείξουμε τις αμφίπλευρες συνεπαγωγές (a) και (b).

(a) "⇒" Εξ υποθέσεως, $\mathrm{Ker}(f) \subseteq \mathrm{Ker}(g)$. Έστω τυχόν $x \in \mathrm{Ker}(g)$. Τότε

$$0_L = g(x) = h\left(f(x)\right) \Rightarrow f(x) \in \mathrm{Ker}(h) = \{0_N\},$$

όπου η τελευταία ισότητα οφείλεται στο ότι ο h είναι (εξ υποθέσεως) μονομορφισμός (βλ. πρόταση A.3.13). Επομένως, $x \in \operatorname{Ker}(f)$, και, ως εκ τούτου, ισχύει και ο αντίστροφος εγκλεισμός $\operatorname{Ker}(g) \subseteq \operatorname{Ker}(f)$.

"$\Leftarrow$" Εάν $\operatorname{Ker}(f) = \operatorname{Ker}(g)$ και $y \in \operatorname{Ker}(h)$, τότε (λόγω τής επιρριπτικότητας τής f) $\exists x \in M : y = f(x)$, οπότε

$$0_L = h(y) = h(f(x)) = g(x) \Rightarrow x \in \operatorname{Ker}(g) = \operatorname{Ker}(f) \Rightarrow y = f(x) = 0_N.$$

Άρα $\operatorname{Ker}(h) = \{0_L\}$ και ο h είναι μονομορφισμός. (Βλ. πρόταση A.3.13.)

(b) "$\Rightarrow$" Εάν ο h είναι επιμορφισμός, τότε και ο $g = h \circ f$ είναι επιμορφισμός (ως σύνθεση δύο επιμορφισμών).

"$\Leftarrow$" Εάν $g = h \circ f$ είναι επιμορφισμός και $z \in L$, τότε υπάρχει κάποιο $x \in M$, τέτοιο ώστε να ισχύει $g(x) = z$. Άρα το $f(x)$ απεικονίζεται μέσω τής h στο z και η h είναι επιρριπτική. $\square$

A.3.25 Θεώρημα. *Εάν M, N, L είναι R-μόδιοι, $f : N \longrightarrow M$ ένας μονομορφισμός και $g \in \operatorname{Hom}_R(L, M)$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Υφίσταται ένας και μόνον $h \in \operatorname{Hom}_R(L, N)$ με $f \circ h = g$.*

$$\begin{tikzcd}
 & M \arrow[d, phantom, "\circlearrowright"] & \\
N \arrow[ur, "f"] & {} & L \arrow[ul, "g"'] \arrow[ll, dashed, "h"]
\end{tikzcd}$$

(ii) $\operatorname{Im}(g) \subseteq \operatorname{Im}(f)$.

Επιπροσθέτως, στην περίπτωση κατά την οποία ικανοποιούνται οι ανωτέρω συνθήκες, ισχύουν τα εξής:

(a) *Ο h είναι μονομορφισμός $\Longleftrightarrow$ ο g είναι μονομορφισμός.*

(b) *Ο h είναι επιμορφισμός $\Longleftrightarrow$ $\operatorname{Im}(g) = \operatorname{Im}(f)$.*

ΑΠΟΔΕΙΞΗ. (i)$\Rightarrow$(ii) $g(x) = f(h(x)) \in \operatorname{Im}(g), \forall x \in L$, οπότε $\operatorname{Im}(g) \subseteq \operatorname{Im}(f)$.

(ii)$\Rightarrow$(i) Κατά την πρόταση A.3.19 υπάρχει απεικόνιση $h : L \longrightarrow N$, τέτοια ώστε να ισχύει η ισότητα $f \circ h = g$. Επειδή ο f είναι εξ υποθέσεως μονομορφισμός, το λήμμα A.3.23 μας πληροφορεί ότι αυτός είναι «εξ αριστερών διαγράψιμος», πράγμα που σημαίνει ότι η h είναι η μοναδική απεικόνιση με την ιδιότητα $f \circ h = g$. Αρκεί λοιπόν να ελεγχθεί ότι η h είναι *και* ομομορφισμός R-μοδίων. Για τυχόντα ζεύγη $(x_1, x_2) \in L \times L$ και $(r_1, r_2) \in R \times R$ έχουμε

$$\begin{aligned} f(h(r_1x_1 + r_2x_2)) &= g(r_1x_1 + r_2x_2) = r_1g(x_1) + r_2g(x_2) \\ &= r_1f(h(x_1)) + r_2f(h(x_2)) = f(r_1h(x_1) + r_2h(x_2)), \end{aligned}$$

οπότε $h(r_1x_1 + r_2x_2) = r_1h(x_1) + r_2h(x_2)$ (διότι ο f είναι εξ υποθέσεως μονομορφισμός). Επομένως, $h \in \operatorname{Hom}_R(L, N)$. (Βλ. πρόταση A.3.3.)

Εν συνεχεία, υποθέτοντας ότι ικανοποιούνται οι συνθήκες (i), (ii), θα αποδείξουμε τις αμφίπλευρες συνεπαγωγές (a) και (b).

(a) Τούτη έπεται άμεσα από τα (i) και (iv) τής προτάσεως Α.3.15.

(b) "$\Rightarrow$" Εάν ο h είναι επιμορφισμός και $y \in N$, τότε υπάρχει $x \in L$, τέτοιο ώστε να ισχύει $y = h(x)$, οπότε $f(y) = f(h(x)) = g(x) \in \mathrm{Im}(g) \Rightarrow \mathrm{Im}(f) \subseteq \mathrm{Im}(g)$.

"$\Leftarrow$" Έστω $y \in N$. Προφανώς, $f(y) \in \mathrm{Im}(f) = \mathrm{Im}(g)$, οπότε υπάρχει κάποιο $x \in L$, τέτοιο ώστε να ισχύει $f(y) = g(x)$. Επειδή $g(x) = f(h(x))$, λαμβάνουμε $f(y) = f(h(x)) \Rightarrow y = h(x)$ (διότι ο f είναι εξ υποθέσεως μονομορφισμός). Άρα ο h είναι όντως επιμορφισμός. □

Α.3.26 Σημείωση. Σε κατοπινές ενότητες θα συναντήσουμε κατ' επανάληψη το πρόβλημα τής «συμπληρώσεως» ποικίλων διαγραμμάτων R-μοδίων και ομομορφισμών R-μοδίων (και όχι μόνον για τρίγωνα). Ενίοτε, λύοντάς το καθιστούμε τα διαγράμματά μας *μεταθετικά*. (Ένα διάγραμμα μη κενών συνόλων και απεικονίσεων είναι **μεταθετικό διάγραμμα**[20] όταν όλες οι δυνατές συνθέσεις απεικονίσεων από οιοδήποτε δοθέν σύνολο αφετηρίας σε οιοδήποτε σύνολο απολήξεως είναι ίσες μεταξύ τους.)

Α.4 ΠΗΛΙΚΟΜΟΔΙΟΙ ΚΑΙ ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ

Α.4.1 Πρόταση. *Έστω U ένας υπομόδιος ενός R-μοδίου M. Τότε ισχύουν τα εξής:*

(i) *Η διμελής σχέση "$\sim_U$" επί τού M η οριζόμενη ως ακολούθως:*

$$\boxed{x \sim_U y \underset{\text{ορσ}}{\Longleftrightarrow} x - y \in U}$$

αποτελεί σχέση ισοδυναμίας.

(ii) *Συμβολίζουμε το σύνολο των κλάσεων ισοδυναμίας ως προς την "$\sim_U$" ως*

$$\boxed{M/U := \{\, x + U \,|\, x \in M \},}$$

(όπου $x + U := [x]_{\sim_U} := \{\, y \in M \,|\, y \sim_U x \}$). Το M/U καθίσταται R-μόδιος μέσω των πράξεων

$$[x_1]_{\sim_U} + [x_2]_{\sim_U} := [x_1 + x_2]_{\sim_U},\ \forall (x_1, x_2) \in M \times M,$$
$$r[x]_{\sim_U} := [rx]_{\sim_U},\ \forall (r, x) \in R \times M.$$

[20] Όταν δοθέν (συγκεκριμένο) διάγραμμα καλείται (εκ προοιμίου) *μεταθετικό*, τότε εννοείται ότι η μεταθετικότητα τηρείται *παντού*. Όταν η μεταθετικότητα τηρείται μόνον για ορισμένα τμήματα αυτού (αλλά *όχι καθ' ολοκληρίαν*), τότε δίδονται οι απαραίτητες διευκρινίσεις. (Πρβλ., π.χ., λήμμα Β.1.23 και θεώρημα Β.1.25.)

(iii) *Η απεικόνιση*

$$\boxed{\pi_U^M : M \longrightarrow M/U, \;\; x \longmapsto \pi_U^M(x) := x + U,} \tag{A.12}$$

είναι ένας επιμορφισμός έχων ως πυρήνα του τον $\mathrm{Ker}(\pi_U^M) = U$.

ΑΠΟΔΕΙΞΗ. (i) Έστω ότι $x, y, z \in M$. Προφανώς, $x - x = 0_M = 0_U \in U$, οπότε $x \sim_U x$ και η $\sim_U$είναι αυτοπαθής. Εάν $x \sim_U y$, τότε

$$x - y \in U \Rightarrow -(x-y) = y - x \in U \Rightarrow y \sim_U x,$$

οπότε η $\sim_U$είναι συμμετρική. Τέλος, εάν $x \sim_U y$ και $y \sim_U z$, τότε

$$\left.\begin{array}{l} x - y \in U \\ y - z \in U \end{array}\right\} \Rightarrow (x-y) + (y-z) = x - z \in U \Rightarrow x \sim_U z,$$

οπότε η $\sim_U$είναι *και* μεταβατική.

(ii) Ας υποθέσουμε εν πρώτοις ότι $x_1, x_2 \in M$ και ότι το x_1' (και αντιστοίχως, το x_2') ανήκει στην κλάση ισοδυναμίας $[x_1]_{\sim_U}$ (και αντιστοίχως, στην κλάση ισοδυναμίας $[x_2]_{\sim_U}$). Τότε

$$\left.\begin{array}{l} x_1 - x_1' \in U \\ x_2 - x_2' \in U \end{array}\right\} \Rightarrow (x_1 - x_1') + (x_2 - x_2') = (x_1 + x_2) - (x_1' + x_2') \in U,$$

οπότε $[x_1 + x_2]_{\sim_U} = [x_1' + x_2']_{\sim_U}$. Εν συνεχεία, ας θεωρήσουμε τυχόντα $r \in R$ και $x \in M$ κι ας υποθέσουμε ότι το x' ανήκει στην κλάση ισοδυναμίας $[x]_{\sim_U}$. Προφανώς,

$$\left.\begin{array}{r} x - x' \in U \\ r \in R \end{array}\right\} \Rightarrow r(x - x') = rx - rx' \in U \Rightarrow [rx]_{\sim_U} = [rx']_{\sim_U}.$$

Ως εκ τούτου οι “ $+$ ” και “ $\cdot$ ” είναι καλώς ορισμένες πράξεις. Είναι δε άμεσος ο έλεγχος τού ότι τα (i)-(iv) τού ορισμού A.2.1 ικανοποιούνται.

(iii) Για οιαδήποτε ζεύγη $(x_1, x_2) \in M \times M$ και $(r_1, r_2) \in R \times R$ έχουμε

$$\begin{aligned} \pi_U^M(r_1x_1 + r_2x_2) &= (r_1x_1 + r_2x_2) + U = (r_1x_1 + U) + (r_2x_2 + U) \\ &= r_1\,(x_1 + U) + r_2\,(x_2 + U) = r_1\,\pi_U^M(x_1) + r_2\,\pi_U^M(x_2), \end{aligned}$$

οπότε (λόγω τής προτάσεως A.3.3) $\pi_U^M \in \mathrm{Hom}_R(M, M/U)$ με πυρήνα του τον

$$\mathrm{Ker}(\pi_U^M) = \left\{ x \in M \,\middle|\, \pi_U^M(x) = 0_{M/U} \right\} = \{ x \in M \,|\, x + U = U \} = U.$$

Η επιρριπτικότητα τής απεικονίσεως π_U^M είναι προφανής. □

A.4.2 Ορισμός. Ο R-μόδιος M/U καλείται **πηλικομόδιος τού** M **ως προς τον** U και η απεικόνιση (A.12) **φυσικός επιμορφισμός** τού M επί τού M/U ή **επιμορφισμός κλάσεων υπολοίπων** τού M ως προς τον U.

Α.4.3 Πρόταση. *Έστω U ένας υπομόδιος ενός R-μοδίου M. Εάν ο M είναι πεπερασμένως παραγόμενος, τότε και ο πηλικομόδιος M/U είναι πεπερασμένως παραγόμενος.*

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμοσθεί το πόρισμα Α.3.8 για τον (Α.12). □

Α.4.4 Θεώρημα. **(«Θεώρημα αντιστοιχίσεως»)**
Έστω U ένας υπομόδιος ενός R-μοδίου M. Τότε η απεικόνιση

$$\left\{ \begin{array}{c} \text{υπομόδιοι τού } M \\ \text{που περιέχουν τον } U \end{array} \right\} \xrightarrow{\alpha} \{\text{υπομόδιοι τού } M/U\}$$

η οριζόμενη από τον τύπο

$$\boxed{U' \longmapsto \alpha(U') := \pi_U^M(U') = U'/U}$$

είναι μια αμφίρριψη που διατηρεί τους εγκλεισμούς, δηλαδή για οιουσδήποτε υπομόδιους U', U'' τού M ισχύει η συνεπαγωγή

$$U \subseteq U' \subseteq U'' \Longrightarrow \alpha(U') \subseteq \alpha(U'').$$

ΑΠΟΔΕΙΞΗ. Θεωρούμε την απεικόνιση

$$\{\text{υπομόδιοι τού } M/U\} \xrightarrow{\beta} \left\{ \begin{array}{c} \text{υπομόδιοι τού } M \\ \text{που περιέχουν τον } U \end{array} \right\}$$

την οριζόμενη από τον τύπο $W \longmapsto \beta(W) := \left(\pi_U^M\right)^{-1}(W)$. Σημειωτέον ότι η αντίστροφη εικόνα $\left(\pi_U^M\right)^{-1}(W)$ αποτελεί υπομόδιο τού M λόγω τού (i) τής προτάσεως Α.3.5 και

$$\{0_W\} \subseteq W \Rightarrow U = \mathrm{Ker}(\pi_U^M) = \left(\pi_U^M\right)^{-1}(\{0_W\}) \subseteq \left(\pi_U^M\right)^{-1}(W)$$

(βλ. πρόταση Α.4.1). Για κάθε υπομόδιο W τού M/U λαμβάνουμε

$$\alpha(\beta(W)) = \alpha((\pi_U^M)^{-1}(W)) = \pi_U^M((\pi_U^M)^{-1}(W)) = W \cap \mathrm{Im}(\pi_U^M) = W$$

(βλ. Α.3.6 (ii)). Κατά συνέπειαν, $\alpha(\beta(W)) = W$. Από την άλλη μεριά, για κάθε υπομόδιο U' τού M που περιέχει τον U λαμβάνουμε

$$\beta(\alpha(U')) = \beta\left(\pi_U^M(U')\right) = (\pi_U^M)^{-1}\left(\pi_U^M(U')\right) = U' + \mathrm{Ker}(\pi_U^M) = U' + U = U'$$

(βλ. Α.3.6 (iv) και Α.4.1). Κατά συνέπειαν, $\beta(\alpha(U')) = U'$, απ' όπου συνάγεται ότι η απεικόνιση α είναι αμφιρριπτική έχουσα την β ως αντίστροφό της. Τέλος, για οιουσδήποτε υπομόδιους U', U'' τού M, για τους οποίους ισχύει $U \subseteq U' \subseteq U''$, έχουμε $\alpha(U') = U'/U = \pi_U^M(U') \subseteq \pi_U^M(U'') = U''/U = \alpha(U'')$, οπότε η α όντως διατηρεί τους εγκλεισμούς. □

Α.4.5 Πόρισμα. *Έστω U ένας υπομόδιος ενός R-μοδίου M. Τότε κάθε υπομόδιος τού M/U είναι τής μορφής U'/U, όπου U' είναι ένας υπομόδιος τού M περιέχων τον U.*

Εν συνεχεία, δοθέντος ενός υπομοδίου U ενός R-μοδίου M και ενός ομομορφισμού R-μοδίων $g : M \longrightarrow L$, επίκειται να περιγραφούν ικανές και αναγκαίες συνθήκες, ούτως ώστε να υφίσταται ένας «κανονιστικός» ομομορφισμός $h \in \mathrm{Hom}_R(M/U, L)$ με $h \circ \pi_U^M = g$. (Βλ. πρόταση Α.4.6, καθώς και το θεώρημα Α.4.10 στην περίπτωση κατά την οποία ο ίδιος ο L είναι κάποιος πηλικομόδιος.) Γι' αυτό θα απαιτηθεί η εφαρμογή τού θεωρήματος Α.3.24. Κατόπιν τούτου, τα περιώνυμα τρία *θεωρήματα ισομορφισμών* θα έχουν ενταχθεί σε ένα ευρύτερο πλαίσιο εργασίας με ομομορφισμούς R-μοδίων.

Α.4.6 Πρόταση. («Καθολική ιδιότητα πηλικομοδίου») *Έστω U ένας υπομόδιος ενός R-μοδίου M και έστω L τυχών R-μόδιος. Εάν $g \in \mathrm{Hom}_R(M, L)$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Υφίσταται ένας και μόνον $h \in \mathrm{Hom}_R(M/U, L)$ ο οποίος καθιστά το διάγραμμα*

$$\begin{tikzcd} M \arrow[r, "g"] \arrow[d, "\pi_U^M"'] \arrow[dr, phantom, "\circlearrowleft"] & L \\ M/U \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

μεταθετικό, ήτοι ο «κανονιστικός» ομομορφισμός ο οριζόμενος από τον τύπο

$$\boxed{h(x+U) := g(x),\ \forall x \in M.}$$

(ii) $U \subseteq \mathrm{Ker}(g)$.

Επιπροσθέτως, στην περίπτωση κατά την οποία ικανοποιούνται οι ανωτέρω συνθήκες, ισχύουν τα εξής:

(a) *Ο h είναι μονομορφισμός $\Longleftrightarrow U = \mathrm{Ker}(g)$.*

(b) *Ο h είναι επιμορφισμός $\Longleftrightarrow$ ο g είναι επιμορφισμός.*

Απόδειξη. Αρκεί να εφαρμοσθεί το θεώρημα Α.3.24 για τον $N = M/U$, με τον φυσικό επιμορφισμό π_U^M στη θέση τού εκεί παρατεθέντος f. (Σύμφωνα με την πρόταση Α.4.1, $U = \mathrm{Ker}(\pi_U^M)$.) □

Α.4.7 Πρώτο Θεώρημα Ισομορφισμών.
Εάν M, N είναι R-μόδιοι και $f \in \mathrm{Hom}_R(M, N)$, τότε

$$\boxed{M/\mathrm{Ker}(f) \cong \mathrm{Im}\,(f)\,.}$$

Συγκεκριμένα, υπάρχει ένας και μόνον ισομορφισμός R-μοδίων

$$h : M/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}\,(f)$$

ο οποίος καθιστά το διάγραμμα

$$\begin{tikzcd} M \arrow[r, "\check{f}"] \arrow[d, "\pi^M_{\mathrm{Ker}(f)}"'] \arrow[dr, phantom, "\circlearrowleft"] & \mathrm{Im}(f) \\ M/\mathrm{Ker}(f) \arrow[ur, dashed, "h"'] & \end{tikzcd}$$

μεταθετικό, όπου $\check{f}$ ο επιμορφισμός ο επαγόμενος μέσω τού f. (Βλ. (A.11).)

Απόδειξη. Εφαρμόζουμε την πρόταση A.4.6 για τον υπομόδιο $U := \mathrm{Ker}(f)$ τού M και για τον επιμορφισμό $g := \check{f}$. Εν προκειμένω, η συνθήκη (ii) αυτού τού πορίσματος ικανοποιείται, διότι $\mathrm{Ker}(f) = \mathrm{Ker}(\check{f})$. Μάλιστα, ο κατασκευαζόμενος ομομορφισμός h είναι μονομορφισμός. Από την άλλη μεριά, η απεικόνιση h είναι, συν τοις άλλοις, και επιρριπτική, καθόσον για κάθε $y \in \mathrm{Im}(f)$ υπάρχει κάποιο $x \in M$ με $f(x) = y$, οπότε $h(x + \mathrm{Ker}(f)) = y$. □

A.4.8 Παράδειγμα. Εάν $n \in \mathbb{N}$, τότε μέσω τού επιμορφισμού $\mathbb{Z}$-μοδίων

$$\mathbb{Z} \ni a \overset{f}{\longmapsto} [a]_n \in \mathbb{Z}_n$$

επάγεται ισομορφισμός $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ (καθώς $\mathrm{Ker}(f) = n\mathbb{Z}$).

A.4.9 Πόρισμα. *Εάν M, N είναι R-μόδιοι και $f \in \mathrm{Hom}_R(M, N)$, τότε υφίσταται μια αμφίρριψη*

$$\left\{ \begin{array}{c} \text{υπομόδιοι τού } M \\ \text{που περιέχουν τον } \mathrm{Ker}(f) \end{array} \right\} \longleftrightarrow \{\text{υπομόδιοι τού } \mathrm{Im}(f)\}\,.$$

Απόδειξη. Έπεται άμεσα από τα θεωρήματα A.4.4 και A.4.7. □

A.4.10 Θεώρημα. (Μεταφορά ομομορφισμού σε «επίπεδο πηλικομοδίων») *Έστω ότι η $f : M \longrightarrow N$ είναι ένας ομομορφισμός R-μοδίων, U ένας υπομόδιος τού M και W ένας υπομόδιος τού N. Τότε οι εξής συνθήκες είναι ισοδύναμες:*

(i) *Υφίσταται ένας και μόνον $h \in \mathrm{Hom}_R(M/U, N/W)$ ο οποίος καθιστά το διάγραμμα*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi^M_U"'] \arrow[dr, phantom, "\circlearrowleft"] & N \arrow[d, "\pi^N_W"] \\ M/U \arrow[r, dashed, "h"'] & N/W \end{tikzcd}$$

μεταθετικό, ήτοι ο «κανονιστικός» ομομορφισμός ο επαγόμενος από τον f που ορίζεται από τον τύπο

$$\boxed{h(x+U) := f(x) + W,\ \forall x \in M.}$$

(ii) $f(U) \subseteq W$.

Επιπροσθέτως, στην περίπτωση κατά την οποία ικανοποιούνται οι ανωτέρω συνθήκες, ισχύουν τα ακόλουθα:

(a) *Ο h είναι μονομορφισμός* $\Longleftrightarrow U = f^{-1}(W)$.

(b) *Ο h είναι επιμορφισμός* $\Longleftrightarrow \mathrm{Im}(f) + W = N$.

ΑΠΟΔΕΙΞΗ. Εφαρμόζουμε την πρόταση A.4.6 για τον $L := N/W$ και τον ομομορφισμό $g := \pi_W^N \circ f$. Σημειωτέον ότι

$$\mathrm{Ker}(\pi_W^N \circ f) = \{x \in M \,|\, f(x) + W = W\} = \{x \in M \,|\, f(x) \in W\} = f^{-1}(W).$$

Εάν λοιπόν $(U =)\ \mathrm{Ker}(\pi_U^M) \subseteq \mathrm{Ker}(\pi_W^N \circ f)$, τότε $f(U) \subseteq f(f^{-1}(W)) \subseteq W$. Και αντιστρόφως· εάν $f(U) \subseteq W$, τότε $U \subseteq f^{-1}(f(U)) \subseteq f^{-1}(W) = \mathrm{Ker}(\pi_W^N \circ f)$. Άρα η ανωτέρω συνθήκη (ii) ισοδυναμεί, εν προκειμένω, με την A.4.6 (ii). Εν συνεχεία, υποθέτοντας ότι ικανοποιούνται οι συνθήκες (i), (ii), θα αποδείξουμε τις αμφίπλευρες συνεπαγωγές (a) και (b).

(a) Επειδή

$$\begin{aligned}\mathrm{Ker}(h) &= \{x + U \,|\, f(x) + W = W\} = \{x + U \,|\, f(x) \in W\} \\ &= \left\{x + U \,\middle|\, x \in f^{-1}(W)\right\} = f^{-1}(W)/U,\end{aligned}$$

ο h (λόγω τής προτάσεως A.3.13) είναι μονομορφισμός $\Longleftrightarrow U = f^{-1}(W)$.

(b) Επειδή $\mathrm{Im}(h) = \{f(x) + W \,|\, x \in M\}$, ο h είναι επιμορφισμός εάν και μόνον εάν

$$(\forall y \in N)\,(\exists x \in M : y + W = f(x) + W) \Leftrightarrow (\forall y \in N)\,(\exists x \in M : y - f(x) \in W)\,,$$

δηλαδή εάν και μόνον εάν $\mathrm{Im}(f) + W = N$. □

A.4.11 Σημείωση. Ενίοτε, στην περίπτωση όπου είναι γνωστό (από τα δεδομένα ενός *συγκεκριμένου* f και *συγκεκριμένων* U και W) ότι $f(U) \subseteq W$, θα χρησιμοποιείται και ένας ειδικότερος συμβολισμός για τον «κανονιστικό» ομομορφισμό h τού θεωρήματος A.4.10: Αντί τού h θα γράφουμε απλώς $f^{\text{πηλ.}}$ (για να υποδηλούται ρητώς ότι ο εν λόγω ομομορφισμός είναι εκείνος που επάγεται *σε επίπεδο πηλικομοδίων μέσω τού* f).

A.4.12 Δεύτερο Θεώρημα Ισομορφισμών. *Εάν οι U, U' είναι δυο υπομόδιοι ενός R-μοδίου M, τότε*

$$\boxed{U/\left(U \cap U'\right) \cong \left(U + U'\right)/U'.}$$

Συγκεκριμένα, υπάρχει ένας και μόνον ισομορφισμός R-μοδίων

$$h : U/\left(U \cap U'\right) \longrightarrow \left(U + U'\right)/U'$$

ο οποίος καθιστά το διάγραμμα

$$\begin{tikzcd}
U \arrow[rr, "\mathrm{in}_{U,U+U'}"] \arrow[d, "\pi^{U}_{U\cap U'}"'] & & U+U' \arrow[d, "\pi^{U+U'}_{U'}"] \\
U/(U\cap U') \arrow[rr, dashed, "h"'] \arrow[urr, phantom, "\circlearrowleft"] & & (U+U')/U'
\end{tikzcd}$$

μεταθετικό.

Αποδειξη. Επειδή $\mathrm{in}_{U,U+U'}(U \cap U') = U \cap U' \subseteq U'$,

$$\begin{aligned}
&\mathrm{in}^{-1}_{U,U+U'}(U') = \{u \in U \,|\mathrm{in}_{U,U+U'}(u) = u \in U'\} = U \cap U', \\
&\mathrm{Im}(\mathrm{in}_{U,U+U'}) + U' = U + U'.
\end{aligned}$$

ο ισχυρισμός είναι αληθής, προκύπτων άμεσα ύστερα από εφαρμογή τού θεωρήματος Α.4.10 για τους υπομόδιους $U \cap U'$ και U' των U και $U + U'$, αντιστοίχως, και τον ομομορφισμό $f := \mathrm{in}_{U,U+U'}$. □

Α.4.13 Τρίτο Θεώρημα Ισομορφισμών. *Εάν οι U, W είναι δυο υπομόδιοι ενός R-μοδίου M και $W \subseteq U$, τότε*

$$\boxed{M/U \cong \left(M/W\right)/(U/W).}$$

Συγκεκριμένα, υπάρχει ένας και μόνον ισομορφισμός R-μοδίων

$$h : M/U \longrightarrow \left(M/W\right)/(U/W)$$

ο οποίος καθιστά το διάγραμμα

$$\begin{tikzcd}
M \arrow[rr, "\pi^{M}_{W}"] \arrow[d, "\pi^{M}_{U}"'] & & M/W \arrow[d, "\pi^{M/W}_{U/W}"] \\
M/U \arrow[rr, dashed, "h"'] \arrow[urr, phantom, "\circlearrowleft"] & & (M/W)/(U/W)
\end{tikzcd}$$

μεταθετικό.

Αποδειξη. Από το πόρισμα Α.4.5 γνωρίζουμε ότι ο U/W είναι υπομόδιος τού M/W. Επειδή $\pi^{M}_{W}(U) = U/W$,

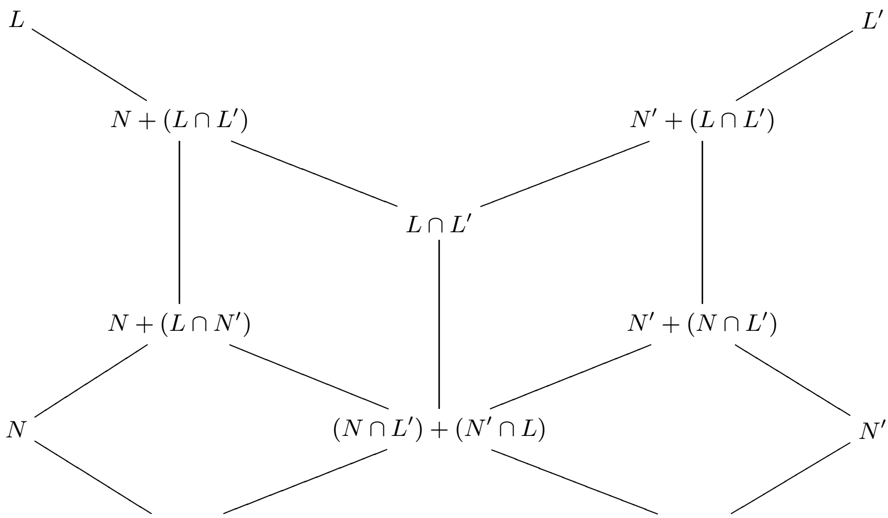
$$
\begin{aligned}
&\left(\pi_W^M\right)^{-1}(U/W) = \left\{x \in M \,\middle|\, \pi_W^M(x) \in U/W\right\} \\
&= \{x \in M \,|\, \exists u \in U : x - u \in W (\subseteq U)\} = U, \\
&U/W \subseteq M/W \Rightarrow \mathrm{Im}(\pi_W^M) + U/W = M/W + U/W = M/W.
\end{aligned}
$$

ο ισχυρισμός είναι αληθής, προκύπτων άμεσα ύστερα από εφαρμογή τού θεωρήματος A.4.10 για τους υπομόδιους U και U/W των M και M/W, αντιστοίχως, και τον ομομορφισμό $f := \pi_W^M$. □

A.4.14 Θεώρημα. («Λήμμα τής πεταλούδας» τού Zassenhaus, 1934) *Έστω M ένας R-μόδιος. Εάν N, L, N', L' είναι υπομόδιοι τού M με $N \subseteq L$ και $N' \subseteq L'$, τότε υφίστανται ισομορφισμοί*

$$
\boxed{
\begin{aligned}
L \cap L'/(N \cap L') + (N' \cap L) &\cong N + (L \cap L')/N + (L \cap N') \\
&\cong N' + (L \cap L')/N' + (N \cap L)
\end{aligned}
}
$$

με τους αντίστοιχους εγκλεισμούς ορατούς μέσω τού ακολούθου εσσιανού διαγράμματος (που ομοιάζει με «πεταλούδα»):



ΑΠΟΔΕΙΞΗ. Επειδή $L \cap N' \subseteq L \cap L'$, έχουμε

$$(L \cap L') + [N + (L \cap N')] = (L \cap L') + N = N + (L \cap L'),$$

οπότε από την πρόταση A.2.20 έπεται ότι

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

Εφαρμόζοντας το δεύτερο θεώρημα ισομορφισμών Α.4.12 για τους $U := L \cap L'$ και $U' := N + (L \cap N')$ λαμβάνουμε

$$\underbrace{L \cap L'}_{=:U} / \underbrace{(N \cap L') + (N' \cap L)}_{=U \cap U'} \cong \underbrace{N + (L \cap L')}_{=U+U'} / \underbrace{N + (L \cap N')}_{=:U'}.$$

Η ύπαρξη τού δευτέρου ισομορφισμού προκύπτει ύστερα από επανάληψη των ιδίων επιχειρημάτων για τα δεδομένα που είναι «συμμετρικά» των ανωτέρω παρατεθέντων ως προς τον «κορμό» (μεσαίο κατακόρυφο ευθύγραμμο τμήμα) τής «πεταλούδας». □

Α.4.15 Ορισμός. Έστω M ένας R-μόδιος. Ένας **πύργος υπομοδίων** του είναι μια πεπερασμένη φθίνουσα αλυσίδα υπομοδίων τής μορφής

$$M =: M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_l \cong \{0\}.$$

Έστω ότι οι

$$\begin{aligned} \Pi_1 : \quad & M =: M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_l \cong \{0\} \\ \Pi_2 : \quad & M =: N_0 \supseteq N_1 \supseteq N_2 \supseteq \cdots \supseteq N_{l'} \cong \{0\} \end{aligned} \tag{A.13}$$

είναι δυο πύργοι υπομοδίων τού M.

(i) Λέμε ότι ο Π_2 αποτελεί μια **εκλέπτυνση τού** Π_1 όταν $l \leq l'$ και όταν (ταυτοχρόνως)

$$\exists j_0, j_1, ... j_l \in \mathbb{N}_0 : j_0 < j_1 < \cdots < j_l \leq l' \text{ με } M_i = N_{j_i}, \forall i \in \{0, 1, ..., l\},$$

ή, με άλλα λόγια, όταν αποκτούμε τον Π_2 από τον Π_1 ύστερα από παρεμβολή $l' - l$ επιπρόσθετων όρων μεταξύ κάποιων εκ των όρων τού Π_1. Ο Π_2 καλείται **γνήσια εκλέπτυνση τού** Π_1 όταν

$$\exists j \in \{1, ..., l'\} : M_i \neq N_j, \ \forall i \in \{0, 1, ..., l\}.$$

(ii) Λέμε ότι οι Π_1 και Π_2 είναι **ισοδύναμοι** όταν $l = l'$ και όταν[21] (ταυτοχρόνως)

$$\exists \sigma \in \mathfrak{S}_l : M_i / M_{i+1} \cong N_{\sigma(i)} / N_{\sigma(i)+1}, \ \forall i \in \{1, ..., l\}.$$

Η χρήση τού λήμματος Α.4.14 τής «πεταλούδας» απλουστεύει την απόδειξη τού ακόλουθου *θεωρήματος των εκλεπτύνσεων* τού O. Schreier.

Α.4.16 Θεώρημα. (O. Schreier, 1928) *Δυο πύργοι υπομοδίων ενός R-μοδίου M διαθέτουν πάντοτε ισοδύναμες εκλεπτύνσεις.*

[21] $\mathfrak{S}_l := \{\sigma : \{1, \ldots, l\} \longrightarrow \{1, \ldots, l\} \,|\, \sigma$ αμφιρριπτική απεικόνιση$\}$.

ΑΠΟΔΕΙΞΗ. Δοθέντων δυο πύργων υπομοδίων (Α.13) ενός R-μοδίου M ορίζουμε για κάθε ζεύγος $(j,k) \in \{1,...,l\} \times \{1,...,l'\}$ τους R-μοδίους

$$M_{j,k} := M_j + (M_{j-1} \cap N_k) \ \text{ και } \ N_{k,j} := N_k + (N_{k-1} \cap M_j).$$

Ας υποθέσουμε, δίχως βλάβη τής γενικότητας, ότι $l' \leq l$. Θέτοντας $M_{j,\rho} := M_{j,l'}$ για κάθε $\rho \in \{l'+1,...,l\}$, λαμβάνουμε τις ακόλουθες φθίνουσες αλυσίδες υπομοδίων τού M:

$$\cdots \supseteq M_{j-1} = M_{j,0} \supseteq M_{j,1} \supseteq \cdots \supseteq M_{j,l'} = \cdots = M_{j,l} = M_j = M_{j+1,0} \cdots$$

$$\cdots \supseteq N_{k-1} = N_{k,0} \supseteq N_{k,1} \supseteq \cdots \supseteq N_{k,l} = N_k = N_{k+1,0} \cdots$$

που αποτελούν εκλεπτύνσεις των Π_1 και Π_2, αντιστοίχως. Εν συνεχεία θεωρούμε τους πηλικομοδίους τούς προκύπτοντες από τους εγκλεισμούς $M_{j,k} \subseteq M_{j,k-1}$ και $N_{k,j} \subseteq N_{k,j-1}$ (και αφορούν σε υπομοδίους εφοδιασμένους με *διαδοχικούς* δείκτες). Εφαρμόζοντας το λήμμα Α.4.14 τής «πεταλούδας» (με τα M_j, M_{j-1}, N_k και N_{k-1} στη θέση των εκεί παρατεθέντων N, L, N' και L', αντιστοίχως) λαμβάνουμε για κάθε ζεύγος $(j,k) \in \{1,...,l\} \times \{1,...,l\}$

$$M_{j,k-1}/M_{j,k} \cong N_{k,j-1}/N_{k,j},$$

οπότε $M_{j,k-1} = M_{j,k} \Leftrightarrow N_{k,j-1} = N_{k,j}$. Εξ αυτού συμπεραίνουμε ότι, κατόπιν παραλείψεως (από τις ανωτέρω αλυσίδες) όλων των υπομοδίων που είναι ίσοι με τους προηγούμενούς τους, προκύπτουν εκλεπτύνσεις Π_1' τού Π_1 και Π_2' τού Π_2 που είναι ισοδύναμες μεταξύ τους. □

Α.4.17 Ορισμός. (i) Λέμε ότι ένας R-μόδιος είναι **απλός** όταν δεν διαθέτει άλλους υπομόδιους πέραν τού τετριμμένου και τού εαυτού του.

(ii) Ένας πύργος υπομοδίων

$$M =: M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_l \cong \{0\}$$

ενός R-μοδίου M καλείται **πύργος των Jordan και Hölder** όταν ο πηλικομόδιος M_i/M_{i+1} είναι απλός για κάθε $i \in \{0,...,l-1\}$.

Λόγω τής αμφιρρίψεως

$$\left\{ \begin{array}{c} \text{υπομόδιοι } U \text{ τού } M \\ \text{με } M_i \supseteq U \supseteq M_{i+1} \end{array} \right\} \longleftrightarrow \{\text{υπομόδιοι τού } M_i/M_{i+1}\},$$

η οποία διατηρεί τους εγκλεισμούς, οι πύργοι των Jordan και Hölder *δεν διαθέτουν γνήσιες εκλεπτύνσεις*. Τούτη η ιδιότητα οδηγεί στο εξής:

Α.4.18 Θεώρημα. *Εάν δυο πύργοι υπομοδίων* (Α.13) *ενός R-μοδίου M είναι πύργοι των Jordan και Hölder, τότε $l = l'$ και οι Π_1, Π_2 είναι κατ' ανάγκην ισοδύναμοι.*

ΑΠΟΔΕΙΞΗ. Κατά το θεώρημα Α.4.16 οι Π_1, Π_2 διαθέτουν ισοδύναμες εκλεπτύνσεις Π_1' και Π_2', αντιστοίχως. Επειδή οι Π_1 και Π_2 είναι εξ υποθέσεως πύργοι των Jordan και Hölder, $\Pi_1 = \Pi_1'$ και $\Pi_2 = \Pi_2'$ (αφού οι μόνες εκλεπτύνσεις τους είναι οι εαυτοί τους). □

Α.4.19 Σημείωση. Το θεώρημα Α.4.18 μας πληροφορεί ότι ο αριθμός των *μη τετριμμένων* υπομοδίων τού M που εμπεριέχονται *σε οιονδήποτε* πύργο των Jordan και Hölder είναι *ανεξάρτητος τής επιλογής τού πύργου*. (Αυτός ο αριθμός είθισται να καλείται **ύψος τού πύργου**.)

Α.5 ΕΥΘΕΑ ΑΘΡΟΙΣΜΑΤΑ ΚΑΙ ΓΙΝΟΜΕΝΑ

Τα *γινόμενα* (products) [υλοποιούμενα μέσω «ευθέων γινομένων»] και τα *συγκινόμενα* (coproducts) [υλοποιούμενα μέσω «ευθέων αθροισμάτων»] R-μοδίων μπορούν να ορισθούν *μέχρις ισομορφισμού* ως λύσεις *καθολικών προβλημάτων* (που αφορούν στην ύπαρξη ομομορφισμών συμπληρώσεως διαγραμμάτων).

Αλλά ας πάρουμε τα πράγματα από την αρχή. Εάν M_1, M_2 είναι δυο R-μόδιοι, τότε το *καρτεσιανό γινόμενο* $M_1 \times M_2$ καθίσταται R-μόδιος μέσω των ακολούθων πράξεων «κατά συντεταγμένες»:

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2), \quad r(x, y) := (rx, ry),$$

για οιαδήποτε $x_1, x_2 \in M_1, y_1, y_2 \in M_2$ και $r \in R$. Ένας ενδιαφέρων χαρακτηρισμός τού R-μοδίου $M_1 \times M_2$ που χρησιμοποιεί τις *προβολές*[22]

$$\mathrm{pr}_1 : M_1 \times M_2 \twoheadrightarrow M_1 \text{ και } \mathrm{pr}_2 : M_1 \times M_2 \twoheadrightarrow M_2$$

επί των M_1 και M_2, αντιστοίχως, έχει ως εξής:

Για κάθε R-μόδιο M και $g_1 \in \mathrm{Hom}_R(M, M_1)$, $g_2 \in \mathrm{Hom}_R(M, M_2)$ υπάρχει *μονοσημάντως ορισμένος* $h \in \mathrm{Hom}_R(M, M_1 \times M_2)$, ούτως ώστε τα κατωτέρω διαγράμματα να είναι μεταθετικά.

$$\begin{tikzcd}
& M_1 & \\
M \arrow[ur, "g_1"] \arrow[rr, dashed, "h"] \arrow[ur, phantom, shift left=6, "\circlearrowleft"] & & M_1 \times M_2 \arrow[ul, "\mathrm{pr}_1"']
\end{tikzcd}
\qquad
\begin{tikzcd}
& M_2 & \\
M \arrow[ur, "g_2"] \arrow[rr, dashed, "h"] \arrow[ur, phantom, shift left=6, "\circlearrowleft"] & & M_1 \times M_2 \arrow[ul, "\mathrm{pr}_2"']
\end{tikzcd}$$

Εδώ, $h(x) := (g_1(x), g_2(x)), \forall x \in M$. Γενίκευση αυτού αποτελεί ο ορισμός Α.5.1.

Α.5.1 Ορισμός. Έστω $(M_j)_{j \in J}$ μια (μη κενή[23]) οικογένεια R-μοδίων. Ένα **γινόμενο** (των μελών) αυτής τής οικογενείας είναι ένα ζεύγος $(P, (f_j)_{j \in J})$ αποτελούμενο από έναν R-μόδιο P και μια οικογένεια ομομορφισμών $f_j \in \mathrm{Hom}_R(P, M_j)$,

[22] $\mathrm{pr}_1(x, y) := x$ και $\mathrm{pr}_2(x, y) := y$ για κάθε $(x, y) \in M_1 \times M_2$.

[23] Από εδώ και στο εξής, όταν γίνεται λόγος για μια οικογένεια R-μοδίων $(M_j)_{j \in J}$ θα υποτίθεται ότι $J \neq \varnothing$ (χωρίς να αναφέρεται ρητώς).

το οποίο ικανοποιεί την εξής *καθολική συνθήκη*:

Για κάθε R-μόδιο M και *για κάθε* οικογένεια ομομορφισμών $g_j \in \mathrm{Hom}_R(M, M_j)$ υπάρχει *μονοσημάντως ορισμένος* $h \in \mathrm{Hom}_R(M, P)$, ούτως ώστε το ακόλουθο διάγραμμα να είναι μεταθετικό.

$$\begin{tikzcd} & M_j & \\ M \arrow[ur, "g_j"] \arrow[rr, dashed, "h"'] & \circlearrowleft & P \arrow[ul, "f_j"'] \end{tikzcd}$$

A.5.2 Λήμμα. *Εάν το $(P, (f_j)_{j\in J})$ είναι ένα γινόμενο μιας οικογενείας R-μοδίων $(M_j)_{j\in J}$, τότε όλοι οι f_j είναι επιμορφισμοί.*

ΑΠΟΔΕΙΞΗ. Εφαρμόζοντας την καθολική συνθήκη τού ορισμού A.5.1 με τον M_j στη θέση τού M και για $g_j := \mathrm{id}_{M_j}$, λαμβάνουμε $f_j \circ h = \mathrm{id}_{M_j}$, απ' όπου έπεται ότι ο ομομορφισμός f_j είναι επιμορφισμός για κάθε $j \in J$. (Βλ. A.3.22 (ii)⇒(i).) □

A.5.3 Θεώρημα. (Μοναδικότητα γινομένου οικογενείας R-μοδίων μέχρις ισομορφισμού) *Εάν $(P, (f_j)_{j\in J})$ είναι ένα γινόμενο μιας οικογενείας R-μοδίων $(M_j)_{j\in J}$, τότε ένα ζεύγος $(P', (f'_j)_{j\in J})$ (όπου P' είναι ένας R-μόδιος και $f'_j \in \mathrm{Hom}_R(P', M_j)$, $\forall j \in J$) είναι ωσαύτως ένα γινόμενο τής $(M_j)_{j\in J}$ εάν και μόνον εάν υπάρχει μονοσημάντως ορισμένος ισομορφισμός $h : P' \xrightarrow{\cong} P$, τέτοιος ώστε να ισχύει η ισότητα*

$$f_j \circ h = f'_j,\ \forall j \in J.$$

ΑΠΟΔΕΙΞΗ. Εξ ορισμού, υπάρχουν μονοσημάντως ορισμένοι $h \in \mathrm{Hom}_R(P', P)$ και $h' \in \mathrm{Hom}_R(P, P')$ που καθιστούν τα διαγράμματα

$$\begin{tikzcd} & M_j & \\ P' \arrow[ur, "f'_j"] \arrow[rr, dashed, "h"'] & \circlearrowleft & P \arrow[ul, "f_j"'] \end{tikzcd} \qquad \begin{tikzcd} & M_j & \\ P \arrow[ur, "f_j"] \arrow[rr, dashed, "h'"'] & \circlearrowleft & P' \arrow[ul, "f'_j"'] \end{tikzcd}$$

μεταθετικά για κάθε $j \in J$. Επειδή $f_j \circ h \circ h' = f'_j \circ h' = f_j$, το διάγραμμα

$$\begin{tikzcd} & M_j & \\ P \arrow[ur, "f_j"] \arrow[rr, dashed, "h\circ h'"'] & \circlearrowleft & P \arrow[ul, "f_j"'] \end{tikzcd}$$

είναι μεταθετικό για κάθε $j \in J$. Από τον ορισμό A.5.1 υπάρχει *ένας και μόνον* ενδομορφισμός τού P που καθιστά το εν λόγω διάγραμμα μεταθετικό για κάθε $j \in J$. Επειδή $f_j \circ \mathrm{id}_P = f_j$, έχουμε κατ' ανάγκην $h \circ h' = \mathrm{id}_P$. Με ανάλογα επιχειρήματα (ύστερα από εναλλαγή των ρόλων των P και P', και των f_j και f'_j) αποδεικνύεται ότι $h' \circ h = \mathrm{id}_{P'}$. Άρα ο h είναι *ισομορφισμός* με $h^{-1} = h'$.

Και αντιστρόφως· ας υποθέσουμε ότι η ανωτέρω συνθήκη ικανοποιείται. Επειδή $f_j = f'_j \circ h^{-1}$ για κάθε $j \in J$, έχουμε τη δυνατότητα να χρησιμοποιήσουμε το γεγονός ότι το ζεύγος $(P, (f_j)_{j\in J})$ είναι ένα γινόμενο των μελών τής οικογενείας $(M_j)_{j\in J}$ προκειμένου να κατασκευάσουμε (για οιονδήποτε R-μόδιο M και οιονδήποτε $g_j \in \mathrm{Hom}_R(M, M_j)$) έναν μοναδικό $\theta \in \mathrm{Hom}_R(M, P)$, τέτοιον ώστε το διάγραμμα

$$\begin{tikzcd} & M_j & \\ M \arrow[ur, "g_j"] \arrow[r, dashed, "\theta"'] & P \arrow[u, phantom, "\circlearrowleft"] \arrow[r, "h^{-1}"] & P' \arrow[ul, "f'_j"'] \end{tikzcd}$$

να είναι μεταθετικό για κάθε $j \in J$. Προφανώς, $f'_j \circ (h^{-1} \circ \theta) = g_j$, και για κάθε $\eta \in \mathrm{Hom}_R(M, P')$ για τον οποίο ισχύει $f'_j \circ \eta = g_j$, έχουμε

$$g_j = f'_j \circ \eta = f'_j \circ (h^{-1} \circ h) \circ \eta, \ \forall j \in J,$$

οπότε, λόγω τής μοναδικότητας τής θ, $h \circ \eta = \theta \Rightarrow \eta = h^{-1} \circ \theta$. Τούτο όμως σημαίνει ότι το ζεύγος $(P', (f'_j)_{j\in J})$ είναι όντως ένα γινόμενο των μελών τής οικογενείας $(M_j)_{j\in J}$. □

A.5.4 Ορισμός. Έστω $(M_j)_{j\in J}$ μια οικογένεια R-μοδίων και έστω

$$\prod_{j\in J} M_j := \left\{ \text{απεικονίσεις } \vartheta : J \longrightarrow \bigcup_{j\in J} M_j \,\middle|\, \vartheta(j) \in M_j, \ \forall j \in J \right\}.$$

Συμβολισμός: Αντί τού $\vartheta(j)$ είθισται να γράφουμε x_j και αντί τής ϑ να γράφουμε $(x_j)_{j\in J}$ και να θεωρούμε το $\prod_{j\in J} M_j$ απαρτιζόμενο από εκείνες τις οικογένειες στοιχείων $(x_j)_{j\in J}$ τής ενώσεως $\bigcup_{j\in J} M_j$ για τις οποίες ισχύει $x_j \in M_j, \forall j \in J$. Το $\prod_{j\in J} M_j$, εφοδιασμένο με τις πράξεις

$$(x_j)_{j\in J} + (x'_j)_{j\in J} := (x_j + x'_j)_{j\in J}, \ \ r(x_j)_{j\in J} := (rx_j)_{j\in J},$$

είναι ένας R-μόδιος και καλείται, ιδιαιτέρως, **ευθύ γινόμενο** (των μελών) τής οικογενείας $(M_j)_{j\in J}$. Για κάθε $\lambda \in J$ ορίζουμε ως λ-**οστή φυσική προβολή** τού $\prod_{j\in J} M_j$ επί τού M_λ τον επιμορφισμό

$$\mathrm{pr}_\lambda : \prod_{j\in J} M_j \twoheadrightarrow M_\lambda, \ (x_j)_{j\in J} \longmapsto \mathrm{pr}_\lambda((x_j)_{j\in J}) := x_\lambda,$$

και ως λ-**οστή φυσική ένθεση** τού M_λ εντός τού $\prod_{j\in J} M_j$ τον μονομορφισμό

$$\mathrm{in}_\lambda : M_\lambda \hookrightarrow \prod_{j\in J} M_j, \ x_\lambda \longmapsto \mathrm{in}_\lambda(x_\lambda) := \begin{cases} 0_{M_j}, & \text{όταν } j \neq \lambda, \\ x_\lambda, & \text{όταν } j = \lambda. \end{cases}$$

Α.5.5 Θεώρημα. (Ύπαρξη γινομένου οικογενείας R-μοδίων) *Εάν $(M_j)_{j\in J}$ είναι μια οικογένεια R-μοδίων, τότε το ζεύγος $\left(\prod_{j\in J} M_j, (\mathrm{pr}_j)_{j\in J}\right)$ αποτελεί ένα γινόμενο των μελών τής $(M_j)_{j\in J}$.*

Αποδειξη. Έστω M τυχών R-μόδιος και έστω $(g_j)_{j\in J}$ μια οικογένεια R-μοδίων $g_j : M \longrightarrow M_j$. Ορίζοντας τον ομομορφισμό

$$h : M \longrightarrow \prod_{j\in J} M_j,\ x \longmapsto h(x) := (g_j(x))_{j\in J},$$

παρατηρούμε ότι $\mathrm{pr}_j \circ h = g_j$ για κάθε $j \in J$. Μάλιστα, αυτός είναι ο μόνος ομομορφισμός με αυτήν την ιδιότητα, διότι για κάθε $h' \in \mathrm{Hom}_R(M, \prod_{j\in J} M_j)$ με $\mathrm{pr}_j \circ h' = g_j, \forall j \in J$, έχουμε

$$h(x)_j = g_j(x) = h'(x)_j,\ \forall j \in J \text{ και } \forall x \in M,$$

οπότε $h = h'$ και το ζεύγος $\left(\prod_{j\in J} M_j, (\mathrm{pr}_j)_{j\in J}\right)$ είναι ένα γινόμενο των μελών τής $(M_j)_{j\in J}$. □

Α.5.6 Σημείωση. (i) Είναι άμεσος ο έλεγχος τού ότι το «ευθύ γινόμενο» έχει (μέχρις ισομορφισμού) τόσον την *προσεταιριστική* όσον και τη *μεταθετική* ιδιότητα, ήτοι ότι

$$\prod_{j\in J} M_j \cong \prod_{\lambda\in\Lambda}\left(\prod_{j\in J_\lambda} M_j\right)$$

για κάθε οικογένεια $(J_\lambda)_{\lambda\in\Lambda}$ μη κενών υποσυνόλων τού J με $J = \coprod_{\lambda\in\Lambda} J_\lambda$ και

$$\prod_{j\in J} M_j \cong \prod_{j\in J} M_{\sigma(j)} \text{ για κάθε αμφίρριψη } \sigma : J \longrightarrow J.$$

(ii) Ιδιαιτέρως, $\prod_{j\in J} M_j \cong M_\lambda \times \prod_{j\in J\smallsetminus\{\lambda\}} M_j,\ \forall \lambda \in J.$

Εν συνεχεία, δίδεται ένας ορισμός που είναι «δυϊκός» τού Α.5.1.

Α.5.7 Ορισμός. Έστω $(M_j)_{j\in J}$ μια οικογένεια R-μοδίων. Ένα **συγκινόμενο** (των μελών) αυτής τής οικογενείας είναι ένα ζεύγος $(C, (f_j)_{j\in J})$ αποτελούμενο από έναν R-μόδιο C και μια οικογένεια ομομορφισμών $f_j \in \mathrm{Hom}_R(M_j, C)$, το οποίο ικανοποιεί την εξής *καθολική συνθήκη*:

Για κάθε R-μόδιο M και *για κάθε* οικογένεια ομομορφισμών $g_j \in \mathrm{Hom}_R(M_j, M)$ υπάρχει *μονοσημάντως ορισμένος* $h \in \mathrm{Hom}_R(C, M)$, ούτως ώστε το ακόλουθο διάγραμμα να είναι μεταθετικό.

$$\begin{tikzcd} & M_j \arrow[dl, "f_j"'] \arrow[dr, "g_j"] \arrow[d, phantom, "\circlearrowleft"] & \\ C \arrow[rr, dashed, "h"'] & {} & M \end{tikzcd}$$

A.5.8 Λήμμα. *Εάν το $(C, (f_j)_{j\in J})$ είναι ένα συγκινόμενο μιας οικογενείας R-μοδίων $(M_j)_{j\in J}$, τότε όλοι οι f_j είναι μονομορφισμοί.*

ΑΠΟΔΕΙΞΗ. Ανάλογη εκείνης τού λήμματος A.5.2. □

A.5.9 Θεώρημα. (Μοναδικότητα συγκινομένου οικογενείας μοδίων μέχρις ισομορφισμού) *Εάν $(C, (f_j)_{j\in J})$ είναι ένα συγκινόμενο μιας οικογενείας R-μοδίων $(M_j)_{j\in J}$, τότε ένα ζεύγος $(C', (f'_j)_{j\in J})$ (όπου C' είναι ένας R-μόδιος και $f'_j \in \mathrm{Hom}_R(M_j, C')$, $\forall j \in J$) είναι ωσαύτως ένα συγκινόμενο τής $(M_j)_{j\in J}$ εάν και μόνον εάν υπάρχει μονοσημάντως ορισμένος ισομορφισμός $h : C \xrightarrow{\cong} C'$, τέτοιος ώστε να ισχύει η ισότητα*

$$h \circ f_j = f'_j,\ \forall j \in J.$$

ΑΠΟΔΕΙΞΗ. Ανάλογη εκείνης τού θεωρήματος A.5.3. □

A.5.10 Ορισμός. Έστω $(M_j)_{j\in J}$ μια οικογένεια R-μοδίων και έστω

$$\bigoplus_{j\in J} M_j := \left\{ (x_j)_{j\in J} \;\middle|\; \begin{array}{c} x_j \in M_j,\ \forall j \in J \quad \text{και} \quad x_j \neq 0_{M_j} \\ \text{για πεπερασμένους} \\ \text{το πολύ δείκτες } j \end{array} \right\} \subseteq \prod_{j\in J} M_j.$$

Είναι εύκολο να ελεγχθεί ότι το $\bigoplus_{j\in J} M_j$ είναι ένας υπομόδιος τού ευθέος γινομένου $\prod_{j\in J} M_j$. Ο R-μόδιος $\bigoplus_{j\in J} M_j$ καλείται **εξωτερικό ευθύ άθροισμα** (των μελών) τής οικογενείας $(M_j)_{j\in J}$.

A.5.11 Σημείωση. (i) Στην περίπτωση όπου ο M_j είναι μη τετριμμένος, $\forall j \in J$, το $\bigoplus_{j\in J} M_j$ είναι *γνήσιος* υπομόδιος τού $\prod_{j\in J} M_j$ εάν και μόνον εάν το I είναι *απειροσύνολο*.

(ii) Εάν το σύνολο δεικτών J είναι *πεπερασμένο*, τότε

$$\bigoplus_{j\in J} M_j = \prod_{j\in J} M_j.$$

Στην ειδική περίπτωση όπου $J = \{1,...,n\}$, $n \in \mathbb{N}$, λαμβάνουμε το σύνηθες (καρτεσιανό) γινόμενο $M_1 \times \cdots \times M_n$.

(iii) Εάν $M_j = M$, $\forall j \in J$, το $\bigoplus_{j\in J} M_j$ συμβολίζεται ως $M^{(J)}$ και $\prod_{j\in J} M_j =: M^J$.

(iv) Η εικόνα $\mathrm{in}_\lambda(M_\lambda)$ τού M_λ μέσω τής $\mathrm{in}_\lambda : M_\lambda \hookrightarrow \prod_{j\in J} M_j$ (βλ. A.5.4) είναι ένας υπομόδιος τού $\bigoplus_{j\in J} M_j$ για κάθε $\lambda \in J$.

A.5.12 Θεώρημα. (Ύπαρξη συγκινομένου οικογενείας R-μοδίων) *Εάν $(M_j)_{j\in J}$ είναι μια οικογένεια R-μοδίων, τότε το ζεύγος $\left(\bigoplus_{j\in J} M_j, (\mathrm{in}_j)_{j\in J}\right)$ αποτελεί ένα συγκινόμενο τής $(M_j)_{j\in J}$.*

ΑΠΟΔΕΙΞΗ. Έστω M τυχών R-μόδιος και έστω $(g_j)_{j\in J}$ μια οικογένεια R-μοδίων $g_j : M_j \longrightarrow M$. Ορίζοντας τον ομομορφισμό[24]

$$h : \bigoplus_{j\in J} M_j \longrightarrow M,\ (x_j)_{j\in J} \longmapsto h((x_j)_{j\in J}) := \sum_{j\in J} g_j(x_j),$$

παρατηρούμε ότι $h\circ \mathrm{in}_j = g_j$ για κάθε $j \in J$. Μάλιστα, αυτός είναι ο μόνος ομομορφισμός με αυτήν την ιδιότητα, διότι για κάθε $h' \in \mathrm{Hom}_R(\bigoplus_{j\in J} M_j, M)$ για τον οποίο ισχύει $h'\circ \mathrm{in}_j = g_j, \forall j \in J$, έχουμε

$$h'((x_j)_{j\in J}) = \sum_{j\in J}(h' \circ \mathrm{in}_j)(x_j) = \sum_{j\in J} g_j(x_j) = h((x_j)_{j\in J}),\ \forall (x_j)_{j\in J} \in \bigoplus_{j\in J} M_j,$$

οπότε $h = h'$ και το ζεύγος $\left(\bigoplus_{j\in J} M_j, (\mathrm{in}_j)_{j\in J}\right)$ είναι ένα συγκινόμενο των μελών τής $(M_j)_{j\in J}$. □

Α.5.13 Σημείωση. (i) Είναι άμεσος ο έλεγχος τού ότι το «εξωτερικό ευθύ άθροισμα» έχει (μέχρις ισομορφισμού) τόσον την *προσεταιριστική* όσον και τη *μεταθετική* ιδιότητα, ήτοι ότι

$$\bigoplus_{j\in J} M_j \cong \bigoplus_{\lambda\in\Lambda}\left(\bigoplus_{j\in J_\lambda} M_j\right)$$

για κάθε οικογένεια $(J_\lambda)_{\lambda\in\Lambda}$ μη κενών υποσυνόλων τού J με $J = \coprod_{\lambda\in\Lambda} J_\lambda$ και

$$\bigoplus_{j\in J} M_j \cong \bigoplus_{j\in J} M_{\sigma(j)} \text{ για κάθε αμφίρριψη } \sigma : J \longrightarrow J.$$

(ii) Ιδιαιτέρως, $\bigoplus_{j\in J} M_j \cong M_\lambda \times \bigoplus_{j\in J\smallsetminus\{\lambda\}} M_j,\ \forall \lambda \in J.$

Α.5.14 Θεώρημα. *Εάν η $(U_j)_{j\in J}$ είναι μια οικογένεια υπομοδίων ενός R-μοδίου M με $\mathrm{card}(J) \geq 2$ και $U := \sum_{j\in J} U_j$, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Εάν $\sum_{j\in J} u_j = 0_M$, όπου $u_j \in U_j, \forall j \in J$, με $u_j \neq 0_M$ για πεπερασμένους το πολύ προσθετέους, τότε $u_j = 0_M, \forall j \in J$.*

(ii) *Κάθε $u \in U$ γράφεται ως άθροισμα $u = \sum_{j\in J} u_j$, μονοσημάντως ορισμένων στοιχείων $u_j \in U_j, \forall j \in J$, όπου $u_j \neq 0_M$ για πεπερασμένους το πολύ προσθετέους.*

(iii) *Για κάθε δείκτη $\lambda \in J$ έχουμε $U_\lambda \cap \left(\sum_{j\in J\smallsetminus\{\lambda\}} U_j\right) = \{0_M\}$.*

[24] Η h είναι *καλώς ορισμένη* απεικόνιση, διότι για κάθε $(x_j)_{j\in J} \in \bigoplus_{j\in J} M_j$ έχουμε $x_j \neq 0_{M_j}$ μόνον για πεπερασμένους το πολύ δείκτες j, οπότε το αναγραφόμενο άθροισμα επέχει θέση *συνήθους αθροίσματος* στοιχείων τού M.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Σύμφωνα με την πρόταση A.2.16 κάθε στοιχείο τού U γράφεται ως άθροισμα κάποιων στοιχείων των $U_j, j \in J$, όπου μόνον το πολύ πεπερασμένοι εξ αυτών είναι $\neq 0_M$. Έστω τυχόν $u \in U$. Υποθέτοντας ότι αυτό γράφεται ως

$$u = \sum_{j \in J} u_j = \sum_{j \in J} u'_j,$$

για κάποια $u_j, u'_j \in U_j$, $j \in J$, και κάποια $u_2, u'_2 \in U_2$, όπου μόνον το πολύ πεπερασμένοι εξ αυτών των u_j (και αντιστοίχως, των u'_j) είναι $\neq 0_M$, αρκεί να δείξουμε ότι $u_j = u'_j$, $\forall j \in J$. Επειδή

$$\sum_{j \in J} u_j = \sum_{j \in J} u'_j \Longrightarrow \sum_{j \in J} \left(u_j - u'_j\right) = 0_M,$$

εφαρμόζοντας το (i) για τα στοιχεία $u_j - u'_j$, $j \in J$, λαμβάνουμε

$$\left[u_j - u'_j = 0_M,\ \forall j \in J\right] \Longrightarrow \left[u_j = u'_j,\ \forall j \in J\right].$$

(ii)⇒(iii) Έστω $\lambda \in J$ και έστω τυχόν $u \in U_\lambda \cap \left(\sum_{j \in J \smallsetminus \{\lambda\}} U_j\right) \subseteq U$. Επειδή

$$u = \sum_{j \in J} w_j = \sum_{j \in J} w'_j,$$

όπου

$$w_j := \begin{cases} 0_M, & \text{όταν } j \neq \lambda, \\ u, & \text{όταν } j = \lambda, \end{cases} \quad \text{και} \quad w'_j := \begin{cases} 0_M, & \text{όταν } j \neq \lambda', \\ u, & \text{όταν } j = \lambda', \end{cases}$$

για $\lambda, \lambda' \in J, \lambda \neq \lambda'$, από το (ii) έπεται ότι $u = 0_M \Rightarrow U_\lambda \cap \left(\sum_{j \in J \smallsetminus \{\lambda\}} U_j\right) \subseteq \{0_M\}$.

Από την άλλη μεριά, η τομή $U_\lambda \cap \left(\sum_{j \in J \smallsetminus \{\lambda\}} U_j\right)$ (ούσα, κατά την πρόταση A.2.10, υπομόδιος τού M) οφείλει να περιέχει το 0_M, οπότε

$$U_\lambda \cap \left(\sum_{j \in J \smallsetminus \{\lambda\}} U_j\right) \supseteq \{0_M\}.$$

Άρα τελικώς $U_\lambda \cap \left(\sum_{j \in J \smallsetminus \{\lambda\}} U_j\right) = \{0_M\}$.

(iii)⇒(i) Εάν $\sum_{j \in J} u_j = 0_M$, όπου $u_j \in U_j, \forall j \in J$, με $u_j \neq 0_M$ για πεπερασμένους το πολύ προσθετέους, τότε $u_\lambda = -\sum_{j \in J \smallsetminus \{\lambda\}} u_j \in \sum_{j \in J \smallsetminus \{\lambda\}} U_j,\ \forall \lambda \in J$, οπότε $u_\lambda \in U_\lambda \cap (\sum_{j \in J \smallsetminus \{\lambda\}} U_j)$. Επειδή (εξ υποθέσεως) $U_\lambda \cap (\sum_{j \in J \smallsetminus \{\lambda\}} U_j) = \{0_M\}$, έχουμε $u_\lambda = 0_M, \forall \lambda \in J$. □

Α.5.15 Ορισμός. Έστω $(U_j)_{j\in J}$ μια οικογένεια υπομοδίων ενός R-μοδίου M με $\mathrm{card}(J) \geq 2$ και έστω $U := \sum_{j\in J} U_j$. Εάν ικανοποιείται μία (και, κατ' επέκταση, και οι τρεις) εκ των συνθηκών τού θεωρήματος Α.5.14, τότε λέμε ότι ο U είναι το **εσωτερικό ευθύ άθροισμα** των μελών αυτής τής οικογενείας και γράφουμε (τουλάχιστον προς στιγμήν[25]) $U = \bigoplus\limits_{j\in J}^{\text{εσ.}} U_j$.

Α.5.16 Σημείωση. (i) Εάν υποθεσουμε ότι $(U_j)_{j\in J}$ είναι μια οικογένεια υπομοδίων ενός R-μοδίου M, τότε, εκλαμβάνοντας καθέναν εκ των U_j ως «αυτόνομο» R-μόδιο, σχηματίζουμε το *εξωτερικό* ευθύ άθροισμα $\bigoplus_{j\in J} U_j$ και αποκτούμε (μέσω τού θεωρήματος Α.5.12 και τού ορισμού Α.5.7) τον μοναδικό ομομορφισμό h που καθιστά το ακόλουθο διάγραμμα μεταθετικό:

$$\begin{tikzcd} & U_\lambda \arrow[dl, hook, "\mathrm{in}_\lambda"'] \arrow[dr, hook, "\mathrm{in}_{U_\lambda, M}"] \arrow[d, phantom, "\circlearrowleft"] & \\ \bigoplus_{j\in J} U_j \arrow[rr, dashed, "h"'] & {} & M \end{tikzcd}$$

Ο h είναι *ισομορφισμός* $\Leftrightarrow M = \bigoplus\limits_{j\in J}^{\text{εσ.}} U_j$. Πράγματι· ο h είναι *επιμορφισμός* εάν και μόνον εάν

$$\forall x \in M \;\; \exists (u_j)_{j\in J} \in \bigoplus\nolimits_{j\in J} U_j : x = h((u_j)_{j\in J}) = \sum_{j\in J} u_j,$$

δηλαδή εάν και μόνον εάν $M = \sum\limits_{j\in J} U_i$. Ο h είναι *μονομορφισμός* εάν και μόνον εάν για οιαδήποτε στοιχεία $(u_j)_{j\in J}, (u'_j)_{j\in J} \in \bigoplus_{j\in J} U_j$ ισχύει η συνεπαγωγή

$$\sum_{j\in J} u_j = \sum_{j\in J} u'_j \Longrightarrow [u_j = u'_j, \; \forall j \in J].$$

Άρα ο ισχυρισμός είναι αληθής λόγω τού (ii) τού θεωρήματος Α.5.14.
(ii) Από την άλλη μεριά, εάν $(M_j)_{j\in J}$ είναι τυχούσα οικογένεια R-μοδίων, τότε

$$\bigoplus_{j\in J} M_j = \bigoplus_{j\in J}^{\text{εσ.}} \mathrm{in}_j(M_j).$$

(iii) Επί τη βάσει των προαναφερθέντων, οιοσδήποτε R-μόδιος γραφόμενος ως εσωτερικό ευθύ άθροισμα των μελών μιας οικογενείας υπομοδίων του είναι ισόμορφος με το εξωτερικό ευθύ άθροισμα αυτών (ιδωθέντων ως «αυτονόμων» R-μοδίων) και, αντιστρόφως, το εξωτερικό ευθύ άθροισμα των μελών τυχούσας οικογενείας R-μοδίων είναι ίσο με το εσωτερικό ευθύ άθροισμα υπομοδίων του, καθένας των οποίων είναι ισόμορφος με το αντίστοιχο μέλος της. (Υπ' αυτήν την έννοια, υφίσταται *δομοθεωρητική ταύτιση* μεταξύ *εσωτερικών* και *εξωτερικών* ευθέων αθροισμάτων.) Γι' αυτόν τον λόγο, θα υιοθετηθεί εφεξής το "$\bigoplus$" για την

[25] Βλ. Α.5.16 (iii).

έκφραση *και* των εσωτερικών ευθέων αθροισμάτων και δεν θα γίνεται χρήση καν των επιθέτων *εξωτερικό* και *εσωτερικό*, καθότι θα είναι πάντοτε σαφές από τα συμφραζόμενα το ποιο εξ αυτών θα υπονοείται.

Α.5.17 Πόρισμα. *Εάν U, W είναι υπομόδιοι ενός R-μοδίου M, τότε*

$$M = U \oplus W \Longleftrightarrow [M = U + W \text{ και } U \cap W = \{0_M\}].$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα από το θεώρημα Α.5.14, τον ορισμό Α.5.15 και τα προαναφερθέντα στο εδ. Α.5.16 (iii). □

Α.5.18 Ορισμός. (i) Λέμε ότι δυο υπομόδιοι U, W ενός R-μοδίου M είναι **συμπληρωματικοί** (και ο ένας **συμπλήρωμα** τού άλλου) εντός τού M όταν

$$M = U \oplus W. \tag{A.14}$$

(ii) Ένας υπομόδιος U ενός R-μοδίου M καλείται **ευθύς προσθετέος** τού M όταν υπάρχει κάποιος υπομόδιος W τού M, ούτως ώστε να ισχύει η ισότητα (Α.14).

Α.5.19 Παρατήρηση. (i) Υπάρχουν υπομόδιοι R-μοδίων που *δεν διαθέτουν κανένα* συμπλήρωμα. Π.χ., εάν $k \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$ και εάν υποθέταμε ότι ο υπομόδιος $k\mathbb{Z}$ τού $\mathbb{Z}$-μοδίου $\mathbb{Z}$ διαθέτει κάποιο συμπλήρωμα, αυτό θα έπρεπε (ως ιδεώδες τού δακτυλίου $\mathbb{Z}$) να είναι τής μορφής $l\mathbb{Z}$ για κάποιον $l \in \mathbb{Z}$, οπότε θα είχαμε

$$k\mathbb{Z} \cap l\mathbb{Z} = \text{εκπ}(k, l)\mathbb{Z} = \{0\} \Rightarrow l = 0 \Rightarrow k\mathbb{Z} + 0\mathbb{Z} = k\mathbb{Z} \subsetneqq \mathbb{Z},$$

και θα καταλήγαμε σε άτοπο.

(ii) Υπομόδιοι R-μοδίων ενδέχεται να έχουν *διαφορετικά* συμπληρώματα. Π.χ., θεωρώντας τούς εξής υποχώρους τού $\mathbb{R}$-διανυσματικού χώρου $\mathbb{R}^2$:

$$U_1 := \{(x, 0) | \, x \in \mathbb{R}\}, \; U_2 := \{(0, y) | \, y \in \mathbb{R}\}, \; W := \{(x, x) | \, x \in \mathbb{R}\}$$

και παρατηρώντας ότι κάθε $(x, y) \in \mathbb{R}^2$ μπορεί να εκφρασθεί *μονοσημάντως* ως

$$(x, y) = (x - y, 0) + (y, y) = (0, y - x) + (x, x),$$

διαπιστώνουμε ότι $\mathbb{R}^2 = U_1 \oplus W = U_2 \oplus W$ με $U_1 \neq U_2$.

Ωστόσο, *όλα* τα συμπληρώματα ενός υπομοδίου ενός R-μοδίου οφείλουν να είναι *ισόμορφα*, όπως έπεται από την ακόλουθη πρόταση:

Α.5.20 Πρόταση. *Εάν U, W είναι υπομόδιοι ενός R-μοδίου M με $M = U \oplus W$, τότε $M/W \cong U$.*

ΑΠΟΔΕΙΞΗ. Επειδή $M = U \oplus W$, η απεικόνιση

$$p : M \longrightarrow U,\ x = u + w \longmapsto p(x) := u,$$

είναι επιμορφισμός έχων ως πυρήνα του τον

$$\mathrm{Ker}(p) := \{\, u + w \in M |\, u = 0_M\} \cong W,$$

οπότε το 1ο θεώρημα ισομορφισμών A.4.7 δίδει $M/W \cong U$. □

A.5.21 Πρόταση. *Εάν ένας R-μόδιος M είναι το άθροισμα $M = U + W$ δύο υπομοδίων του U και W, τότε*

$$M/(U \cap W) \cong (M/U) \oplus (M/W).$$

ΑΠΟΔΕΙΞΗ. Είναι άμεσος ο έλεγχος τού ότι η απεικόνιση

$$f : M \longrightarrow (M/U) \oplus (M/W),\ x \longmapsto f(x) := (x + U, x + W),$$

είναι ομομορφισμός, έχων ως πυρήνα του τον

$$\mathrm{Ker}(f) = \{\, x \in M |\, (x + U, x + W) = (U, W)\} = \{\, x \in M |\, x \in U \cap W\} = U \cap W.$$

Για τυχόν $(x+U, y+W) \in (M/U) \oplus (M/W)$, τα x και y γράφονται ως αθροίσματα $x = u_1 + w_1$ και $y = u_2 + w_2$ κάποιων στοιχείων, όπου $u_1, u_2 \in U$ και $w_1, w_2 \in W$. Προφανώς,

$$\begin{aligned} &f(w_1 + u_2) = f(w_1) + f(u_2) = (w_1 + U, 0_M + W) + (0_M + U, u_2 + W) \\ &= (w_1 + U, u_2 + W) = (w_1 + u_1 + U, u_2 + w_2 + W) \\ &= (u_1 + w_1 + U, u_2 + w_2 + W) = (x + U, y + W), \end{aligned}$$

οπότε ο f είναι επιμορφισμός. Υπολείπεται η εφαρμογή τού 1ου θεωρήματος ισομορφισμών A.4.7. □

A.5.22 Παράδειγμα. Εάν $k, l \in \mathbb{N}, k \geq 2, l \geq 2$ και μκδ$(k, l) = 1$, τότε έχουμε $k\mathbb{Z} \cap l\mathbb{Z} = kl\mathbb{Z}$ και $k\mathbb{Z} + l\mathbb{Z} =$ μκδ$(k, l)\mathbb{Z} = \mathbb{Z}$, οπότε

$$\mathbb{Z}_{kl} \cong \mathbb{Z}/kl\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z} \cong \mathbb{Z}_k \oplus \mathbb{Z}_l.$$

A.5.23 Ορισμός. Εάν η $(f_j : M_j \longrightarrow N_j)_{j \in J}$ είναι μια οικογένεια ομομορφισμών R-μοδίων και ορίσουμε **ως ευθύ γινόμενο** των μελών της την απεικόνιση

$$\prod_{j \in J} f_j : \prod_{j \in J} M_j \longrightarrow \prod_{j \in J} N_j,\ \ (x_j)_{j \in J} \longmapsto (f_j(x_j))_{j \in J},$$

και, αντιστοίχως, ως **ευθύ άθροισμα** των μελών της την απεικόνιση

$$\bigoplus_{j \in J} f_j : \bigoplus_{j \in J} M_j \longrightarrow \bigoplus_{j \in J} N_j,\ \ (x_j)_{j \in J} \longmapsto (f_j(x_j))_{j \in J},$$

(όπου εδώ μόνον το πολύ πεπερασμένοι εξ αυτών των x_j είναι διάφορα τού μηδενικού στοιχείου). Αμφότερες οι $\prod_{j\in J} f_j$ και $\bigoplus_{j\in J} f_j$ είναι ομομορφισμοί R-μοδίων με τους υπομοδίους

$$\operatorname{Ker}(\prod_{j\in J} f_j) = \prod_{j\in J} \operatorname{Ker}(f_j), \quad \operatorname{Ker}(\bigoplus_{j\in J} f_j) = \bigoplus_{j\in J} \operatorname{Ker}(f_j) \tag{A.15}$$

ως πυρήνες τους και τους υπομοδίους

$$\operatorname{Im}(\prod_{j\in J} f_j) = \prod_{j\in J} \operatorname{Im}(f_j), \quad \operatorname{Im}(\bigoplus_{j\in J} f_j) = \bigoplus_{j\in J} \operatorname{Im}(f_j) \tag{A.16}$$

ως εικόνες τους.

A.5.24 Πρόταση. *Έστω $(M_j)_{j\in J}$ μια οικογένεια R-μοδίων και έστω N_j ένας υπομόδιος τού M_j, $\forall j \in J$. Τότε μέσω τού ευθέος γινομένου και τού ευθέος αθροίσματος των μελών τής $(\pi^{M_j}_{N_j} : M_j \longrightarrow M_j/N_j)_{j\in J}$ (τής απαρτιζομένης από τους αντιστοίχους φυσικούς επιμορφισμούς) επάγονται ισομορφισμοί R-μοδίων*:

$$(\prod_{j\in J} M_j)/(\prod_{j\in J} N_j) \cong \prod_{j\in J}(M_j/N_j), \quad (\bigoplus_{j\in J} M_j)/(\bigoplus_{j\in J} N_j) \cong \bigoplus_{j\in J}(M_j/N_j).$$

ΑΠΟΔΕΙΞΗ. Επειδή οι $\prod_{j\in J} \pi^{M_j}_{N_j}$ και $\bigoplus_{j\in J} \pi^{M_j}_{N_j}$ είναι επιμορφισμοί και

$$\operatorname{Ker}(\prod_{j\in J} \pi^{M_j}_{N_j}) = \prod_{j\in J} N_j, \quad \operatorname{Ker}(\bigoplus_{j\in J} \pi^{M_j}_{N_j}) = \bigoplus_{j\in J} N_j,$$

αρκεί να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών A.4.7. □

$\boxed{\text{A.6}}$ ΕΛΕΥΘΕΡΟΙ R-ΜΟΔΙΟΙ ΚΑΙ ΒΑΣΕΙΣ

Η κλάση των διανυσματικών χώρων εμπεριέχεται στην (πολύ ευρύτερη) κλάση των *ελευθέρων μοδίων*.

A.6.1 Ορισμός. Έστω $\mathcal{X}$ ένα μη κενό σύνολο. Ορίζουμε ως **ελεύθερο R-μόδιο επί τού** $\mathcal{X}$ κάθε ζεύγος (F, f) αποτελούμενο από έναν R-μόδιο F και μια απεικόνιση $f : \mathcal{X} \longrightarrow F$ που ικανοποιεί την εξής *καθολική συνθήκη*:

Για κάθε R-μόδιο M και *για κάθε* απεικόνιση $g : \mathcal{X} \longrightarrow M$ υπάρχει *μονοσημάντως ορισμένος* $h \in \operatorname{Hom}_R(F, M)$, ούτως ώστε το ακόλουθο διάγραμμα να είναι μεταθετικό.

$$\begin{tikzcd} & \mathcal{X} \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[d, phantom, "\circlearrowleft"] & \\ F \arrow[rr, dashed, "h"'] & & M \end{tikzcd}$$

Α.6.2 Λήμμα. *Εάν (F, f) είναι ένας ελεύθερος R-μόδιος επί ενός μη κενού συνόλου $\mathcal{X}$, τότε η απεικόνιση f είναι ενριπτική και $F = \mathrm{Lin}_R(\mathrm{Im}(f))$.*

ΑΠΟΔΕΙΞΗ. Για να δείξουμε ότι η f είναι ενριπτική, ας υποθέσουμε ότι $x_1, x_2 \in \mathcal{X}$ με $x_1 \neq x_2$. Αρκεί να δείξουμε ότι $f(x_1) \neq f(x_2)$. Προς τούτο θεωρούμε τυχόντα μη τετριμμένο R-μόδιο M (π.χ., τον ίδιον τον R ως R-μόδιο[26]) και τυχούσα απεικόνιση $g : \mathcal{X} \longrightarrow M$, τέτοια ώστε να ισχύει $g(x_1) \neq g(x_2)$. Εάν $h : F \longrightarrow M$ είναι ο μοναδικός ομομορφισμός με $h \circ f = g$, τότε

$$h(f(x_1)) = g(x_1) \neq g(x_2) = h(f(x_2)) \Rightarrow f(x_1) \neq f(x_2).$$

Έστω τώρα $U := \mathrm{Lin}_R(\mathrm{Im}(f))$ ο υπομόδιος τού F ο παραγόμενος από την εικόνα $\mathrm{Im}(f)$ τής απεικονίσεως f. Θεωρούμε το διάγραμμα:

$$\begin{tikzcd}
\mathcal{X} \arrow[r, two heads, "\check{f}"] \arrow[d, "f"'] & \mathrm{Im}(f) \arrow[r, hook, "\iota"] & U \arrow[r, hook, "\iota_U"] & F \\
F \arrow[urr, bend right, "h"] \arrow[urrr, bend right, "\iota_U \circ h"'] & & &
\end{tikzcd}$$

στο οποίο οι $\iota : \mathrm{Im}(f) \hookrightarrow U$ και $\iota_U : U \hookrightarrow F$ είναι οι συνήθεις ενθέσεις, και $\check{f} : \mathcal{X} \twoheadrightarrow \mathrm{Im}(f)$ η επίρριψη η προκύπτουσα ύστερα από περιορισμό τού πεδίου τιμών τής f στην εικόνα της. Εν προκειμένω, επειδή το ζεύγος (F, f) είναι ένας ελεύθερος R-μόδιος επί τού $\mathcal{X}$, ο $h \in \mathrm{Hom}_R(F, U)$ είναι ο μοναδικός ομομορφισμός με την ιδιότητα $h \circ f = \iota \circ \check{f}$. Σημειωτέον ότι $\iota_U \circ h \in \mathrm{Hom}_R(F, F)$ με

$$(\iota_U \circ h) \circ f = \iota_U \circ (h \circ f) = \iota_U \circ \iota \circ \check{f}.$$

Και πάλι, λοιπόν, επειδή το ζεύγος (F, f) είναι ένας ελεύθερος R-μόδιος επί τού $\mathcal{X}$, υφίσταται ένας και μόνον $\theta \in \mathrm{Hom}_R(F, F)$ με την ιδιότητα $\theta \circ f = \iota_U \circ \iota \circ \check{f}$. Προφανώς, $\mathrm{id}_F \circ f = f = \iota_U \circ \iota \circ \check{f} \Rightarrow \theta = \mathrm{id}_F \Rightarrow \iota_U \circ h = \mathrm{id}_F$ (από τη μοναδικότητα τού θ), οπότε η ι_U οφείλει να είναι *και* επιρριπτική (βλ. Α.3.22), πράγμα που σημαίνει ότι $U = F$. □

Α.6.3 Θεώρημα. (Η μοναδικότητα τού (F, f) μέχρις ισομορφισμού) *Εάν (F, f) είναι ένας ελεύθερος R-μόδιος επί ενός μη κενού συνόλου $\mathcal{X}$, τότε ένα ζεύγος (F', f') (όπου F' είναι ένας R-μόδιος και $f' : \mathcal{X} \longrightarrow F'$ μια απεικόνιση) είναι ωσαύτως ένας ελεύθερος R-μόδιος επί τού $\mathcal{X}$ εάν και μόνον εάν υπάρχει ένας μονοσημάντως ορισμένος ισομορφισμός $j : F \xrightarrow{\cong} F'$ με $j \circ f = f'$.*

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι ένα τέτοιο ζεύγος (F', f') είναι ελεύθερος R-μόδιος επί τού $\mathcal{X}$. Τότε υπάρχουν μοναδικοί $j \in \mathrm{Hom}_R(F, F')$ και $j' \in \mathrm{Hom}_R(F', F)$ που

[26] Εξ υποθέσεως, $1_R \neq 0_R$.

καθιστούν τα διαγράμματα

$$\begin{tikzcd} & \mathcal{X} \arrow[dl, "f"'] \arrow[dr, "f'"] \arrow[d, phantom, "\circlearrowleft"] & \\ F \arrow[rr, dashed, "j"'] & & F' \end{tikzcd} \qquad \begin{tikzcd} & \mathcal{X} \arrow[dl, "f'"'] \arrow[dr, "f"] \arrow[d, phantom, "\circlearrowleft"] & \\ F' \arrow[rr, dashed, "j'"'] & & F \end{tikzcd}$$

μεταθετικά. Επειδή $j' \circ j \circ f = j' \circ f' = f$, προκύπτει το μεταθετικό διάγραμμα:

$$\begin{tikzcd} & \mathcal{X} \arrow[dl, "f"'] \arrow[dr, "f"] \arrow[d, phantom, "\circlearrowleft"] & \\ F \arrow[rr, "j' \circ j"'] & & F \end{tikzcd}$$

Επειδή το (F, f) είναι ελεύθερος R-μόδιος επί τού $\mathcal{X}$ και $\mathrm{id}_F \circ f = f$, έχουμε κατ' ανάγκην $j' \circ j = \mathrm{id}_F$. Παρομοίως, ύστερα από εναλλαγή των ρόλων των F και F', δείχνεται ότι $j \circ j' = \mathrm{id}_{F'}$. Ως εκ τούτου, ο j είναι *ισομορφισμός* με $j^{-1} = j'$.

Και αντιστρόφως· εάν υπάρχει μοναδικός ισομορφισμός $j : F \xrightarrow{\cong} F'$ με $j \circ f = f'$, τότε $f = j^{-1} \circ f'$ και για κάθε R-μόδιο M και για κάθε απεικόνιση $g : \mathcal{X} \longrightarrow M$ προκύπτει ένα διάγραμμα

$$\begin{tikzcd} \mathcal{X} \arrow[r, "g"] \arrow[d, "f'"'] \arrow[dr, "f"] & M \\ F' \arrow[r, bend right, "j^{-1}"'] & F \arrow[l, "j"'] \arrow[u, "h"'] \end{tikzcd}$$

όπου $h \in \mathrm{Hom}_R(F, M)$ είναι ο μοναδικός ομομορφισμός με την ιδιότητα

$$h \circ j^{-1} \circ f' = h \circ f = g.$$

Για να αποδειχθεί ότι το ζεύγος (F', f') είναι ελεύθερος R-μόδιος επί τού $\mathcal{X}$ αρκεί να αποδειχθεί ότι για κάθε $\beta \in \mathrm{Hom}_R(F', M)$ με $\beta \circ f' = g$, έχουμε $\beta = h \circ j^{-1}$. Παρατηρούμε ότι $\beta \circ f' = g \Leftrightarrow \beta \circ j \circ f = g$, οπότε, λόγω τής μοναδικότητας τού h, $\beta \circ j = h \Rightarrow \beta = h \circ j^{-1}$. □

A.6.4 Σημείωση. Για την απόδειξη τής *υπάρξεως* ελευθέρου R-μοδίου επί ενός μη κενού συνόλου $\mathcal{X}$ θεωρούμε τον R-μόδιο $R^{(\mathcal{X})}$ (βλ. A.2.9 (iv) και (i)) και ορίζουμε την ενριπτική[27] απεικόνιση

$$\boxed{\begin{gathered} \delta : \mathcal{X} \longrightarrow R^{(\mathcal{X})},\ x \longmapsto \delta_x, \\ \mathcal{X} \ni y \longmapsto \delta_x(y) := \begin{cases} 1_R, & \text{όταν } x = y, \\ 0_R, & \text{όταν } x \neq y, \end{cases} \end{gathered}} \tag{A.17}$$

[27]Εάν $\delta_{x_1} = \delta_{x_2}$, τότε $\delta_{x_1}(y) = \delta_{x_2}(y), \forall y \in \mathcal{X}$, οπότε για $y = x_1 \Rightarrow 1 = \delta_{x_1}(x_1) = \delta_{x_2}(x_1) \Rightarrow x_2 = x_1$.

(Το $\delta_{x,y}$ είναι το σύνηθες **δέλτα τού Kronecker**.)

A.6.5 Θεώρημα. (Ύπαρξη ελευθέρου R-μοδίου επί ενός μη κενού συνόλου $\mathcal{X}$) *Εάν $\mathcal{X}$ είναι ένα μη κενό σύνολο, τότε το ζεύγος $(R^{(\mathcal{X})}, \delta)$ αποτελεί έναν ελεύθερο R-μόδιο επί τού $\mathcal{X}$.*

ΑΠΟΔΕΙΞΗ. Έστω M τυχών R-μόδιος και έστω $g : \mathcal{X} \longrightarrow M$ τυχούσα απεικόνιση. Ορίζουμε μια απεικόνιση $h : R^{(\mathcal{X})} \longrightarrow M$ μέσω τού τύπου[28]

$$h(\theta) := \sum_{x \in \mathcal{X}} \theta(x) g(x), \ \forall \theta \in R^{(\mathcal{X})}. \tag{A.18}$$

Είναι εύκολο να ελεγχθεί ότι $h \in \mathrm{Hom}_R(R^{(\mathcal{X})}, M)$. Επίσης, για κάθε $x \in \mathcal{X}$,

$$(h \circ \delta)(x) = h(\delta_x) = \sum_{y \in \mathcal{X}} \delta_x(y) g(y) = g(x),$$

οπότε $h \circ \delta = g$. Απομένει λοιπόν να αποδειχθεί ότι ο h είναι ο μοναδικός ομομορφισμός με αυτήν την ιδιότητα. Κατ' αρχάς παρατηρούμε ότι για κάθε $\theta \in R^{(\mathcal{X})}$ και για κάθε $y \in \mathcal{X}$ ισχύει

$$\theta(y) = \theta(y) 1_R = \sum_{x \in \mathcal{X}} \theta(x) \delta_x(y) = \left(\sum_{x \in \mathcal{X}} \theta(x) \delta_x \right)(y),$$

οπότε $\theta = \sum_{x \in \mathcal{X}} \theta(x) \delta_x$. Υποθέτοντας τώρα ότι $h' \in \mathrm{Hom}_R(R^{(\mathcal{X})}, M)$ είναι τέτοιος, ώστε $h' \circ \delta = g$, λαμβάνουμε για κάθε $\theta \in R^{(\mathcal{X})}$

$$h'(\theta) = h'\left(\sum_{x \in \mathcal{X}} \theta(x) \delta_x \right) = \sum_{x \in \mathcal{X}} \theta(x) h'(\delta_x) = \sum_{x \in \mathcal{X}} \theta(x) g(x) = h(\theta),$$

απ' όπου έπεται ότι $h' = h$. □

A.6.6 Ορισμός. Λέμε ότι ένας R-μόδιος M είναι **ελεύθερος** όταν ο M είναι *είτε* τετριμμένος *είτε* μη τετριμμένος και (ταυτοχρόνως) υπάρχει κάποιο μη κενό σύνολο $\mathcal{X}$ και ένας ισομορφισμός R-μοδίων $M \xrightarrow{\cong} R^{(\mathcal{X})}$. (Πρβλ. A.6.3 και A.6.5.)

Οι ελεύθεροι R-μόδιοι χαρακτηρίζονται μέσω τής εννοίας τής *βάσεως*, όπως τη γνωρίζουμε από τη Γραμμική Άλγεβρα. (Βλ. θεώρημα A.6.13.)

A.6.7 Ορισμός. Έστω M ένας R-μόδιος.

(i) Λέμε ότι ένα υποσύνολο $\mathcal{X} \subseteq M$ είναι (R-)**γραμμικώς ανεξάρτητο** όταν[29] είτε $\mathcal{X} = \varnothing$ είτε $\mathcal{X} \neq \varnothing$ *και* για οιοδήποτε πεπερασμένο υποσύνολο $\{x_1, ..., x_k\}$ τού $\mathcal{X}$ και $r_1, ..., r_k \in R$ ισχύει η συνεπαγωγή

$$\sum_{j=1}^{k} r_j x_j = 0_M \Rightarrow [r_j = 0_R, \ \forall j \in \{1, ..., k\}].$$

[28] Το εν λόγω άθροισμα είναι *καλώς ορισμένο*, καθότι μόνον πεπερασμένου πλήθους προσθετέοι είναι μη μηδενικοί.

[29] Όταν δεν πληρούται καμία εξ αυτών των συνθηκών, τότε λέμε ότι το $\mathcal{X}$ είναι **γραμμικώς εξαρτημένο.**

(ii) Κάθε γραμμικώς ανεξάρτητο υποσύνολο $\mathcal{X} \subseteq M$ το οποίο αποτελεί σύστημα γεννητόρων τού M (δηλ., $\mathrm{Lin}_R(\mathcal{X}) = M$) καλείται **βάση**[30] τού M.

A.6.8 Παραδείγματα. (i) Έστω M ένας R-μόδιος και έστω $\varnothing \neq \mathcal{X} \subseteq M$. Εάν το $\mathcal{X}$ περιέχει το 0_M, τότε το $\mathcal{X}$ είναι κατ' ανάγκην γραμμικώς εξαρτημένο, διότι για $\{0_M, x_1, ..., x_k\} \subseteq \mathcal{X}$ έχουμε

$$1_R 0_M + 0_R x_1 + \cdots + 0_R x_k = 0_M, \text{ όπου } 1_R \neq 0_R.$$

(ii) Ένα μονοσύνολο $\{r\}$, $r \in R \smallsetminus \{0_R\}$, οιουδήποτε μη τετριμμένου μεταθετικού δακτυλίου R είναι γραμμικώς ανεξάρτητο (με τον R θεωρούμενον ως R-μόδιο) εάν και μόνον εάν το r δεν είναι μηδενοδιαιρέτης εντός τού R.

(iii) Σε κάθε διανυσματικό χώρο V (οριζόμενον υπεράνω ενός σώματος K) κάθε μονοσύνολο $\{x\}$, $x \in V \smallsetminus \{0_V\}$, είναι γραμμικώς ανεξάρτητο, καθόσον από την εξίσωση $\lambda x = 0_V$, $\lambda \in K$, έπεται ότι $\lambda = 0_K$.

(iv) Εάν $q, q' \in \mathbb{Q}$, $q \neq q'$, τότε εντός τού $\mathbb{Z}$-μοδίου $\mathbb{Q}$ το δισύνολο $\{q, q'\}$ είναι πάντοτε γραμμικώς εξαρτημένο. Πράγματι· γράφοντας αυτούς τους ρητούς αριθμούς ως $q = \frac{a}{b}$ και $q' = \frac{a'}{b'}$ για κατάλληλους $a, a' \in \mathbb{Z}$ (με $(a, a') \neq (0, 0)$) και $b, b' \in \mathbb{Z} \smallsetminus \{0\}$, και παρατηρούμε ότι

$$(a'b)q + (-ab')q' = 0, \text{ με τουλάχιστον έναν εκ των συντελεστών } \neq 0.$$

A.6.9 Θεώρημα. *Έστω M ένας R-μόδιος και έστω $\varnothing \neq \mathcal{X} \subseteq M$. Τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Το $\mathcal{X}$ είναι μια βάση τού M.*

(ii) *Κάθε στοιχείο τού M γράφεται κατά τρόπο μονοσήμαντο ως γραμμικός συνδυασμός στοιχείων τού $\mathcal{X}$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εξ ορισμού, κάθε στοιχείο τού M γράφεται ως γραμμικός συνδυασμός στοιχείων τού $\mathcal{X}$. Υποθέτουμε ότι για κάποιο $x \in M$ υφίσταται πεπερασμένο υποσύνολο $\{x_1, ..., x_k\}$ τού $\mathcal{X}$ και $r_1, ..., r_k, s_1, ..., s_k \in R$, ούτως ώστε να ισχύει

$$x = \sum_{j=1}^{k} r_j x_j = \sum_{j=1}^{k} s_j x_j \Rightarrow \sum_{j=1}^{k} (r_j - s_j) x_j = 0_M.$$

Επειδή το $\mathcal{X}$ είναι εξ υποθέσεως γραμμικώς ανεξάρτητο υποσύνολο τού M, έχουμε κατ' ανάγκην $r_j = s_j$ για κάθε $j \in \{1, ..., k\}$.

(ii)⇒(i) Αρκεί να αποδειχθεί ότι το $\mathcal{X}$ είναι ένα γραμμικώς ανεξάρτητο υποσύνολο τού M. Προς τούτο θεωρούμε τυχόν πεπερασμένο υποσύνολο $\{x_1, ..., x_k\}$ τού $\mathcal{X}$. Από κάθε σχέση τής μορφής $\sum_{j=1}^{k} r_j x_j = 0_M$ (με $r_1, ..., r_k \in R$) προκύπτει ότι

$$\sum_{j=1}^{k} r_j x_j = 0_M = \sum_{j=1}^{k} 0_R x_j \Rightarrow [r_j = 0_R, \ \forall j \in \{1, ..., k\}]$$

[30] Προφανώς, το $\varnothing$ αποτελεί βάση τού M εάν και μόνον εάν ο M είναι *τετριμμένος*.

λόγω τής προϋποτεθείσας μοναδικότητας τής παραστάσεως οιουδήποτε στοιχείου τού M ως γραμμικού συνδυασμού στοιχείων τού $\mathcal{X}$. □

Α.6.10 Πρόταση. *Εάν $f : M \xrightarrow{\cong} N$ είναι ένας ισομορφισμός μεταξύ δυο R-μοδίων και $\mathcal{X}$ μια βάση τού M, τότε η εικόνα αυτής $f(\mathcal{X})$ μέσω τού f αποτελεί μια βάση τού N.*

ΑΠΟΔΕΙΞΗ. Επειδή $N = f(M) = f(\mathrm{Lin}_R(\mathcal{X})) = \mathrm{Lin}_R(f(\mathcal{X}))$, η εικόνα $f(\mathcal{X})$ αποτελεί σύστημα γεννητόρων τού N. Εάν $\mathcal{X} = \varnothing$, τότε αμφότεροι οι M, N είναι τετριμμένοι και $f(\varnothing) = \varnothing$. Εάν $\mathcal{X} \neq \varnothing$, τότε για οιοδήποτε πεπερασμένο υποσύνολο $\{f(x_1), ..., f(x_k)\}$ τής εικόνας $f(\mathcal{X})$ και $r_1, ..., r_k \in R$ με

$$\sum_{j=1}^{k} r_j f(x_j) = 0_N \ \left[\Leftrightarrow f(\sum_{j=1}^{k} r_j x_j) = 0_N \Leftrightarrow \sum_{j=1}^{k} r_j x_j \in \mathrm{Ker}(f) \right]$$

έχουμε $\sum_{j=1}^{k} r_j x_j = 0_M$ (διότι $\mathrm{Ker}(f) = \{0_M\}$), οπότε $r_j = 0_R$, $\forall j \in \{1, ..., k\}$, λόγω τού ότι το $\mathcal{X}$ είναι γραμμικώς ανεξάρτητο υποσύνολο τού M. Άρα και η εικόνα $f(\mathcal{X})$ είναι γραμμικώς ανεξάρτητο υποσύνολο τού N. □

Α.6.11 Πρόταση. *Έστω M ένας R-μόδιος και έστω $\mathcal{X} \subseteq M$. Εάν υποτεθεί ότι το $\mathcal{X}$ είναι μια βάση τού M, τότε ισχύουν τα εξής:*

(i) *Το $\mathcal{X}$ είναι ένα ελαχιστικό σύστημα γεννητόρων*[31] *τού M.*

(ii) *Το $\mathcal{X}$ είναι ένα μεγιστικό*[32] *γραμμικώς ανεξάρτητο υποσύνολο τού M.*

ΑΠΟΔΕΙΞΗ. Θα χρησιμοποιήσουμε «εις άτοπον απαγωγή».

(i) Έστω ότι το $\mathcal{X}$ δεν είναι ελαχιστικό σύστημα γεννητόρων τού M. Τότε $\mathcal{X} \neq \varnothing$ και υπάρχει κάποιο $\mathcal{Y} \in \mathfrak{P}(M) : \mathrm{Lin}_R(\mathcal{Y}) = M$ με $\mathcal{Y} \subsetneqq \mathcal{X}$. Έστω $x \in \mathcal{X} \smallsetminus \mathcal{Y}$. Επειδή $x \in M = \mathrm{Lin}_R(\mathcal{Y})$, υπάρχουν $y_1, ..., y_k \in \mathcal{Y}$ ($k \in \mathbb{N}$) και $s_1, ..., s_k \in R$, ούτως ώστε να ισχύει

$$x = \sum_{j=1}^{k} r_j y_j \Rightarrow 1_R x + \sum_{j=1}^{k} (-r_j) y_j = 0_M \ \ (\{x, y_1, ..., y_k\} \subseteq \mathcal{X}).$$

Άρα το $\mathcal{X}$ είναι γραμμικώς εξαρτημένο υποσύνολο τού M. Άτοπο!

(ii) Εάν $\mathcal{X} = \varnothing$, τότε ο ισχυρισμός είναι προδήλως αληθής. Ας υποθέσουμε ότι $\mathcal{X} \neq \varnothing$ και ότι το $\mathcal{X}$ δεν είναι μεγιστικό γραμμικώς ανεξάρτητο υποσύνολο τού M. Τότε υπάρχει κάποιο γραμμικώς ανεξάρτητο $\mathcal{Y} \in \mathfrak{P}(M) : \mathcal{X} \subsetneqq \mathcal{Y}$. Έστω ότι $y \in \mathcal{Y} \smallsetminus \mathcal{X}$. Επειδή (εξ υποθέσεως) $M = \mathrm{Lin}_R(\mathcal{X}) \ni y$, υπάρχουν $x_1, ..., x_k \in \mathcal{X}$ ($k \in \mathbb{N}$) και $s_1, ..., s_k \in R$, ούτως ώστε να ισχύει

$$y = \sum_{j=1}^{k} s_j x_j \Rightarrow 1_R y + \sum_{j=1}^{k} (-s_j) x_j = 0_M \ \ (\{y, x_1, ..., x_k\} \subseteq \mathcal{Y}).$$

[31] Αυτό σημαίνει ότι το υποσύνολο $\mathcal{X} \subseteq M$ αποτελεί ένα ελαχιστικό στοιχείο τού μερικώς διατεταγμένου συνόλου $(\{\mathcal{Z} \in \mathfrak{P}(M) | \mathrm{Lin}_R(\mathcal{Z}) = M\}, \subseteq)$.

[32] *Μεγιστικό* ως προς τη σχέση "$\subseteq$" τού συνολοθεωρητικού εγκλεισμού.

Άρα το $\mathcal{Y}$ είναι γραμμικώς εξαρτημένο υποσύνολο τού M. Άτοπο! □

A.6.12 Λήμμα. *Εάν $\mathcal{X}$ είναι ένα μη κενό σύνολο, τότε η εικόνα* $\mathrm{Im}(\delta)$ *τής* (A.17) *είναι μια βάση τού $R^{(\mathcal{X})}$.*

ΑΠΟΔΕΙΞΗ. Κατά το λήμμα A.6.2 και το θεώρημα A.6.5, $R^{(\mathcal{X})} = \mathrm{Lin}_R(\mathrm{Im}(\delta))$. Εάν $\{\delta_{x_1}, ..., \delta_{x_k}\}$ είναι ένα πεπερασμένο σύνολο τής $\mathrm{Im}(\delta)$ και τα $r_1, ..., r_k \in R$ τέτοια, ώστε να ισχύει $\sum_{j=1}^k r_j \delta_{x_j} = 0_{R^{(\mathcal{X})}}$, τότε

$$0_R = \left(\sum_{j=1}^k r_j \delta_{x_j}\right)(x_\rho) = \sum_{j=1}^k r_j \left(\delta_{x_j}(x_\rho)\right) = r_\rho,\ \forall \rho \in \{1, ..., k\}.$$

Άρα η εικόνα $\mathrm{Im}(\delta)$ είναι *και* γραμμικώς ανεξάρτητο υποσύνολο τού $R^{(\mathcal{X})}$. □

A.6.13 Θεώρημα. *Για έναν R-μόδιο M οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) *Ο M είναι ελεύθερος R-μόδιος.*

(ii) *Ο M διαθέτει τουλάχιστον μία βάση.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν ο M είναι τετριμμένος, τότε αυτός έχει το κενό σύνολο ως (μόνη) βάση του. Εάν ο M δεν είναι τετριμμένος, τότε υφίσταται κάποιο σύνολο $\mathcal{X} \neq \varnothing$, τέτοιο ώστε να ισχύει $M \cong R^{(\mathcal{X})}$ και (σύμφωνα με το λήμμα A.6.12) η εικόνα $\mathrm{Im}(\delta)$ τής (A.17) είναι μια βάση τού $R^{(\mathcal{X})}$. Επομένως η εικόνα αυτής μέσω οιουδήποτε ισομορφισμού μεταξύ τού $R^{(\mathcal{X})}$ και τού M αποτελεί (σύμφωνα με την πρόταση A.6.10) μια βάση τού M.

(ii)⇒(i) Έστω $\mathcal{X}$ μια βάση τού M. Εάν $\mathcal{X} = \varnothing$, τότε είναι ο M (ως τετριμμένος) είναι ελεύθερος. Εάν $\mathcal{X} \neq \varnothing$, τότε (σύμφωνα με το θεώρημα A.6.5) υπάρχει μονοσημάντως ορισμένος $h \in \mathrm{Hom}_R(R^{(\mathcal{X})}, M)$, τέτοιος ώστε να ισχύει $h \circ \delta = \iota$, όπου $\iota : \mathcal{X} \hookrightarrow M$ η συνήθης ένθεση. Επειδή η εικόνα $\mathrm{Im}(h)$ τού h είναι ένας υπομόδιος τού M που περιέχει το $\mathcal{X}$ και $\mathrm{Lin}_R(\mathcal{X}) = M$, η πρόταση A.2.13 μας πληροφορεί ότι $\mathrm{Lin}_R(\mathcal{X}) \subseteq \mathrm{Im}(h) \Rightarrow \mathrm{Im}(h) = M$, οπότε ο h είναι επιμορφισμός. Από την άλλη μεριά, επειδή

$$h(\theta) := \sum_{x \in \mathcal{X}} \theta(x)\iota(x) = \sum_{x \in \mathcal{X}} \theta(x)x,\ \forall \theta \in R^{(\mathcal{X})}$$

(βλ. (A.18)), για κάθε $\theta \in \mathrm{Ker}(h)$ λαμβάνουμε

$$\sum_{x \in \mathcal{X}} \theta(x)x = h(\theta) = 0_M \Rightarrow [\theta(x) = 0_R, \forall x \in \mathcal{X}] \Rightarrow \mathrm{supp}(\theta) = \varnothing \Rightarrow \theta = 0_{R^{(\mathcal{X})}},$$

διότι το $\mathcal{X}$ είναι γραμμικώς ανεξάρτητο. Άρα $\mathrm{Ker}(h) = \{0_{R^{(\mathcal{X})}}\}$ και ο h είναι μονομορφισμός. (Βλ. πρόταση A.3.13.) Τελικώς λοιπόν ο h είναι *ισομορφισμός* και, ως εκ τούτου, ο M είναι ελεύθερος R-μόδιος. □

A.6.14 Πόρισμα. *Εάν M είναι ένας μη τετριμμένος R-μόδιος έχων το $\mathcal{X}$ ως μια βάση του, τότε $M \cong R^{(\mathcal{X})}$.*

Α.6.15 Παραδείγματα. Με τη βοήθεια τής προτάσεως Α.6.11 και τού θεωρήματος Α.6.13 μπορεί κανείς να κατασκευάσει εύκολα *μη ελευθέρους* R-μοδίους.

(i) Εάν $k \in \mathbb{N}$, $k \geq 2$, τότε ο $\mathbb{Z}$-μόδιος $\mathbb{Z}_k$ δεν είναι ελεύθερος. Πράγματι· το μονοσύνολο $\{[1]_k\}$ είναι ελαχιστικό παράγον υποσύνολο τού $\mathbb{Z}_k$ αλλά δεν είναι γραμμικώς ανεξάρτητο, αφού $k[1]_k = [k]_k = [0]_k = 0_{\mathbb{Z}_k}$ (με $k \neq 0$). Ομοίως, και κάθε άλλο μονοσύνολο που παράγει τον $\mathbb{Z}_k$ είναι γραμμικώς εξαρτημένο.

(ii) Παρομοίως αποδεικνύεται ότι *κάθε μη τετριμμένη, πεπερασμένη αβελιανή ομάδα* δεν είναι ελεύθερος $\mathbb{Z}$-μόδιος.

(iii) Εάν $q, q' \in \mathbb{Q}$, $q \neq q'$, τότε (όπως έχουμε εξηγήσει στο εδ. Α.6.8 (iv)) εντός τού $\mathbb{Z}$-μοδίου $\mathbb{Q}$ το δισύνολο $\{q, q'\}$ είναι πάντοτε γραμμικώς εξαρτημένο. Ως εκ τούτου, εάν ο $\mathbb{Z}$-μόδιος $\mathbb{Q}$ διέθετε κάποια βάση, αυτή θα όφειλε να είναι ένα μονοσύνολο $\{q\}$, όπου $q \in \mathbb{Q} \smallsetminus \{0\}$. Όμως $\mathrm{Lin}_{\mathbb{Z}}(\{q\}) = \{\kappa q | \, \kappa \in \mathbb{Z}\} \subsetneqq \mathbb{Q}$. Άρα ο $\mathbb{Z}$-μόδιος $\mathbb{Q}$ δεν είναι ελεύθερος.

(iv) Έστω I ένα μη τετριμμένο ιδεώδες ενός μεταθετικού δακτυλίου R. Το I δεν είναι ελεύθερος R-μόδιος όταν *δεν είναι κύριο* ιδεώδες τού R. Πράγματι· εάν $a, b \in I$ και $a \neq b$, με τουλάχιστον ένα εξ αυτών $\neq 0_R$, τότε

$$(-b)a + ab = 0_R \Rightarrow \text{ το } \{a, b\} \text{ είναι γραμμικώς εξαρτημένο.}$$

Ως εκ τούτου, εάν ο R-μόδιος I διέθετε κάποια βάση, αυτή θα όφειλε να είναι ένα μονοσύνολο $\{x\}$, όπου $x \in I \smallsetminus \{0_R\}$. Όμως

$$\mathrm{Lin}_R(\{x\}) = \{rx | \, r \in R\} = I \Leftrightarrow I = \langle x \rangle \, .$$

Α.6.16 Πόρισμα. *Για έναν μη τετριμμένο R-μόδιο M οι ακόλουθες συνθήκες είναι ισοδύναμες*:

(i) *Ο M είναι ελεύθερος R-μόδιος.*

(ii) *Υπάρχει $\varnothing \neq \mathcal{X} \subseteq M$, τέτοιο ώστε η απεικόνιση $R \ni r \longmapsto rx \in Rx$ να είναι ισομορφισμός για κάθε $x \in \mathcal{X}$ και να ισχύει $M = \bigoplus_{x \in \mathcal{X}} Rx$.*

Απόδειξη. (i)⇒(ii) Κατά το θεώρημα Α.6.13 υπάρχει κάποια βάση $\mathcal{X}$ τού M. Επειδή ο M είναι μη τετριμμένος, $\mathcal{X} \neq \varnothing$. Κάθε στοιχείο τού M γράφεται ως γραμμικός συνδυασμός στοιχείων τού $\mathcal{X}$ (και μάλιστα, σύμφωνα με την πρόταση Α.6.9, κατά τρόπο μονοσήμαντο), οπότε $M = \bigoplus_{x \in \mathcal{X}} Rx$. (Βλ. Α.5.15 και Α.5.16 (iii).) Επίσης, για κάθε $x \in \mathcal{X}$ η απεικόνιση $R \ni r \longmapsto rx \in Rx$ είναι (προφανώς) επιμορφισμός. Η ενριπτικότητά της έπεται άμεσα από το γεγονός ότι το μονοσύνολο $\{x\}$ είναι γραμμικώς ανεξάρτητο.

(ii)⇒(i) $M = \bigoplus_{x \in \mathcal{X}} Rx \Rightarrow M = \mathrm{Lin}_R(\mathcal{X})$. Επειδή η $R \ni r \longmapsto rx \in Rx$ είναι ισομορφισμός, το μονοσύνολο $\{x\}$ είναι γραμμικώς ανεξάρτητο για κάθε $x \in \mathcal{X}$. Έστω $\{x_1, ..., x_k\}$ τυχόν πεπερασμένο υποσύνολο τού $\mathcal{X}$. Εάν $r_1, ..., r_k \in R$ είναι τέτοια, ώστε να ισχύει $\sum_{j=1}^{k} r_j x_j = 0_M$, τότε

$$\left.\begin{array}{r}\sum\limits_{j=1}^{k} \underbrace{r_j x_j}_{\in \mathrm{Lin}_R(\{x_j\})} = 0_M = \underbrace{0_M + \cdots + 0_M}_{k \text{ φορές}} \\ M = \bigoplus\limits_{x \in \mathcal{X}} Rx,\ \forall j \in \{1, ..., \kappa\}\end{array}\right\} \underset{\text{A.5.15, A.5.16 (iii)}}{\Longrightarrow} r_j x_j = 0_M, \forall j \in \{1, ..., k\},$$

οπότε $r_j = 0_R$ (αφού το $\{x_j\}$ είναι γραμμικώς ανεξάρτητο) για κάθε $j \in \{1, ..., k\}$. Άρα το $\mathcal{X}$ είναι (καθ' ολοκληρίαν) γραμμικώς ανεξάρτητο και, κατ' επέκταση, μια βάση τού M. Κατά συνέπειαν, ο M είναι ελεύθερος R-μόδιος (εκ νέου δυνάμει τού θεωρήματος A.6.13). □

A.6.17 Πόρισμα. *Εάν $(M_j)_{j \in J}$ είναι μια οικογένεια ελευθέρων R-μοδίων, τότε και ο R-μόδιος $M := \bigoplus_{j \in J} M_j$ είναι ελεύθερος. Μάλιστα, εάν $\mathcal{X}_j$ είναι μια βάση τού M_j για κάθε $j \in J$, τότε η ένωση $\bigcup_{j \in J} \mathcal{X}_j$ είναι μια βάση τού M.*

ΑΠΟΔΕΙΞΗ. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι ο R-μόδιος M_j είναι μη τετριμμένος για κάθε[33] $j \in J$. Κατά το θεώρημα A.6.13 υπάρχει βάση $\varnothing \neq \mathcal{X}_j \subseteq M_j$ τού M_j και $M_j = \bigoplus_{x \in \mathcal{X}_j} Rx$. Κατά συνέπειαν,

$$M := \bigoplus_{j \in J} M_j = \bigoplus_{j \in J} \Big(\bigoplus_{x \in \mathcal{X}_j} Rx \Big) \underset{\text{A.5.13 (i)}}{\cong} \bigoplus_{x \in \cup_{j \in J} \mathcal{X}_j} Rx,$$

οπότε ο M είναι όντως ελεύθερος έχων την ένωση $\bigcup_{j \in J} \mathcal{X}_j$ ως μια βάση του. □

A.6.18 Σημείωση. Το αντίστροφο τού πορίσματος A.6.17 (όπως θα διαπιστώσουμε μέσω τού παραδείγματος A.6.19) δεν είναι αληθές: Εάν ο $M := \bigoplus_{j \in J} M_j$ είναι ελεύθερος, τότε ο M_j δεν είναι κατ' ανάγκην ελεύθερος *για κάθε* $j \in J$.

A.6.19 Παράδειγμα. Εάν $k, l \in \mathbb{N}, k \geq 2, l \geq 2$ και μκδ$(k, l) = 1$, τότε υφίστανται ισομορφισμοί $\mathbb{Z}_{kl}$-μοδίων[34]

$$\mathbb{Z}_{kl} \cong \mathbb{Z}/kl\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z} \cong \mathbb{Z}_k \oplus \mathbb{Z}_l.$$

(Βλ. εδ. A.5.22.) Ο $\mathbb{Z}_{kl}$-μόδιος $\mathbb{Z}_{kl}$ είναι ελεύθερος. Ωστόσο, οι $\mathbb{Z}_{kl}$-μόδιοι $\mathbb{Z}_k$ και $\mathbb{Z}_l$ *δεν είναι ελεύθεροι*. (Εάν ο -προφανώς, μη τετριμμένος- $\mathbb{Z}_{kl}$-μόδιος $\mathbb{Z}_k$ ήταν ελεύθερος, τότε θα έπρεπε λόγω των πορισμάτων A.6.14 και A.6.16 να υπάρχει βάση αυτού $\mathcal{X} \neq \varnothing$ με $\mathbb{Z}_k \cong \mathbb{Z}_{kl}^{(\mathcal{X})}$, κάτι που θα οδηγούσε σε άτοπο, διότι card$(\mathcal{X})kl > k$. Η ίδια επιχειρηματολογία εφαρμόζεται και για τον $\mathbb{Z}_{kl}$-μόδιο $\mathbb{Z}_l$.)

[33] Εάν *όλοι* οι M_j είναι τετριμμένοι, τότε ο ισχυρισμός είναι προδήλως αληθής. Εάν υπάρχει $\varnothing \neq J' \subsetneqq J$, τέτοιο ώστε οι $M_j, j \in J'$, να είναι μη τετριμμένοι και οι $M_j, j \in J \smallsetminus J'$ να είναι τετριμμένοι, τότε μπορούμε να εργασθούμε με το J' στη θέση τού J.

[34] Οι $\mathbb{Z}_k$ και $\mathbb{Z}_l$ μπορούν να θεωρηθούν (εκτός από $\mathbb{Z}$-μόδιοι) και ως $\mathbb{Z}_{kl}$-μόδιοι μέσω των αριθμητικών πολλαπλασιασμών

$$\mathbb{Z}_{kl} \times \mathbb{Z}_k \ni ([a]_{kl}, [b]_k) \longmapsto [ab]_k \in \mathbb{Z}_k,\ \mathbb{Z}_{kl} \times \mathbb{Z}_l \ni ([a]_{kl}, [b]_l) \longmapsto [ab]_l \in \mathbb{Z}_l.$$

Α.6.20 Θεώρημα. (Θεώρημα «γραμμικής επεκτάσεως») *Εάν M, N είναι R-μόδιοι, με τον M μη τετριμμένο και ελεύθερο και το $\mathcal{X} \subseteq M$ μια βάση αυτού, τότε για οιαδήποτε απεικόνιση $\theta : \mathcal{X} \longrightarrow N$ υφίσταται ακριβώς ένας $f \in \mathrm{Hom}_R(M, N)$ για τον οποίον ισχύει $f|_{\mathcal{X}} = \theta$.*

ΑΠΟΔΕΙΞΗ. Έστω τυχόν $x \in M$. Επειδή το $\mathcal{X}$ είναι εξ υποθέσεως μια βάση τού M, το x γράφεται κατά τρόπο μοναδικό ως γραμμικός συνδυασμός στοιχείων τού $\mathcal{X}$ (βλ. Α.6.9), δηλαδή υπάρχουν μοναδικά στοιχεία $x_1,\ldots,x_n \in \mathcal{X}$ και $r_1,\ldots,r_n \in R$ ($n \in \mathbb{N}$) για τα οποία ισχύει

$$x = \sum_{i=1}^{n} r_i x_i. \tag{A.19}$$

Ως εκ τούτου, θέτοντας

$$\boxed{f(x) := \sum_{i=1}^{n} r_i \theta\,(x_i)}$$

ορίζουμε (καλώς) μια απεικόνιση $f : M \longrightarrow N$. Σημειωτέον ότι για κάθε $x \in \mathcal{X}$ έχουμε $x = 1_R x$, οπότε $f(x) = 1_R \cdot \theta\,(x) = \theta\,(x) \Longrightarrow f|_{\mathcal{X}} = \theta$. Επιπροσθέτως, για οιαδήποτε $r, s \in R$ και οιαδήποτε $x, x' \in M$, γραφόμενα (κατά τρόπο μοναδικό) ως γραμμικοί συνδυασμοί

$$x = \sum_{i=1}^{n} \kappa_i x_i, \ \ x' = \sum_{j=1}^{m} \xi_j x'_j,$$

$x_1,\ldots,x_n, x'_1,\ldots,x'_m \in \mathcal{X}$, $\kappa_1,\ldots,\kappa_n, \xi_1,\ldots,\xi_m \in R$ ($n, m \in \mathbb{N}$), έχουμε

$$\begin{aligned} f(rx + sx') &= f\left(r\left(\sum_{i=1}^{n} \kappa_i x_i\right) + s\left(\sum_{j=1}^{m} \xi_j x'_j\right)\right) \\ &= f\left(\sum_{i=1}^{n} (r\kappa_i)\, x_i + \sum_{j=1}^{m} \left(s\xi_j\right) x'_j\right) = \sum_{i=1}^{n} (r\kappa_i)\, \theta(x_i) + \sum_{j=1}^{m} \left(s\xi_j\right) \theta(x'_j) \\ &= r\left(\sum_{i=1}^{n} \kappa_i \theta(x_i)\right) + s\left(\sum_{j=1}^{m} \xi_j \theta(x'_j)\right) = rf(x) + sf(x'), \end{aligned}$$

οπότε $f \in \mathrm{Hom}_R(M, N)$ (λόγω τής προτάσεως Α.3.3). Απομένει να αποδειχθεί ότι αυτός είναι ο *μοναδικός* ομομορφισμός από τον M στον N, ο περιορισμός τού οποίου επί τής $\mathcal{X}$ ισούται με την θ. Προς τούτο θεωρούμε *τυχόντα* ομομορφισμό $g \in \mathrm{Hom}_R(M, N)$ για τον οποίο ισχύει $g|_{\mathcal{X}} = \theta$. Εάν γράψουμε οιοδήποτε $x \in M$ υπό τη μορφή (Α.19), τότε

$$f(x) = \sum_{i=1}^{n} r_i \theta\,(x_i) = \sum_{i=1}^{n} r_i g\,(x_i) = g\left(\sum_{i=1}^{n} r_i x_i\right) = g(x),$$

όπου η δεύτερη ισότητα οφείλεται στο ότι $f|_{\mathcal{X}} = \theta = g|_{\mathcal{X}}$ και η τρίτη ισότητα προκύπτει από το ότι η g είναι ομομορφισμός. (Βλ. πρόταση Α.3.4.) Επομένως, $f = g$. □

A.6.21 Σημείωση. Ο ομομορφισμός f (ο κατασκευασθείς στο θεώρημα A.6.20), ο οποίος είναι ο μόνος ομομορφισμός από τον M στον N που καθιστά το διάγραμμα

$$\begin{tikzcd} \mathcal{X} \arrow[r, "\theta"] \arrow[d, "\mathrm{in}_{\mathcal{X},M}"'] \arrow[dr, phantom, "\circlearrowleft" near start] & N \\ M \arrow[ur, dashed, "f"'] & \end{tikzcd}$$

μεταθετικό, καλείται, ιδιαιτέρως, (R-)**γραμμική επέκταση** τής θ.

A.6.22 Πόρισμα. *Εάν M, N είναι R-μόδιοι, με τον M μη τετριμμένο και ελεύθερο και το $\mathcal{X} \subseteq M$ μια βάση αυτού, τότε για $f, g \in \mathrm{Hom}_R(M, N)$ ισχύει η συνεπαγωγή*

$$f|_{\mathcal{X}} = g|_{\mathcal{X}} \Longrightarrow f = g.$$

ΑΠΟΔΕΙΞΗ. Έπεται άμεσα ύστερα από εφαρμογή τού θεωρήματος A.6.20 για την $\theta := g|_{\mathcal{X}}$. □

A.6.23 Πόρισμα. *Κάθε R-μόδιος M είναι ισόμορφος με έναν πηλικομόδιο F/W, όπου F είναι ένας ελεύθερος R-μόδιος.*

ΑΠΟΔΕΙΞΗ. Έστω $\mathcal{X}$ ένα σύστημα γεννητόρων τού M. Εάν $\mathcal{X} = \varnothing$, τότε είναι ο ίδιος ο M (ως τετριμμένος) είναι ελεύθερος και ο ισχυρισμός είναι προδήλως αληθής. Εάν $\mathcal{X} \neq \varnothing$, τότε κατά το λήμμα A.6.12 η εικόνα $\mathrm{Im}(\delta)$ τής (A.17) είναι μια βάση τού $R^{(\mathcal{X})}$. Έστω $f \in \mathrm{Hom}_R(R^{(\mathcal{X})}, M)$ η γραμμική επέκταση τής απεικονίσεως

$$\theta : \mathrm{Im}(\delta) \longrightarrow M,\ \delta_x \longmapsto \theta(\delta_x) := x.$$

Αυτή είναι *επι* μορφισμός. Πράγματι· εάν x είναι *τυχόν* στοιχείο τού M, τότε υπάρχει πεπερασμένο υποσύνολο $\{x_1, ..., x_k\}$ τού $\mathcal{X}$ και $r_1, ..., r_k \in R$, ούτως ώστε να ισχύει $x = \sum_{j=1}^{k} r_j x_j$. Επομένως,

$$f(\sum_{j=1}^{k} r_j \delta_{x_j}) = \sum_{j=1}^{k} r_j f(\delta_{x_j}) = \sum_{j=1}^{k} r_j \theta(\delta_{x_j}) = \sum_{j=1}^{k} r_j x_j = x.$$

Σύμφωνα με το θεώρημα A.4.7, έχουμε $R^{(\mathcal{X})}/\mathrm{Ker}(f) \cong M$. Αρκεί λοιπόν να τεθεί $F := R^{(\mathcal{X})}$ και $W := \mathrm{Ker}(f)$. □

► **Παρένθετα δεδομένα από τη Θεωρία των Διανυσματικών Χώρων**. Λόγω τού θεωρήματος A.6.13 η απόδειξη τού ότι *κάθε διανυσματικός χώρος* (ως μόδιος υπεράνω ενός σώματος) *είναι ελεύθερος* αποτελεί άμεσο επακόλουθο τής *υπάρξεως* (τουλάχιστον μιας) *βάσεως*. (Βλ. θεώρημα A.6.25 και πόρισμα A.6.26.) Επιπροσθέτως, για την απόδειξη τής *ισοπληθικότητας* όλων των βάσεων ενός ελευθέρου R-μοδίου (βλ. θεώρημα A.6.38) χρησιμοποιείται ουσιωδώς η *ισοπληθικότητα* όλων των βάσεων ενός διανυσματικού χώρου.

A.6.24 Λήμμα. *Έστω V ένας διανυσματικός χώρος ορισμένος υπεράνω ενός σώματος K και έστω $\mathcal{A} \subseteq V$ ένα γραμμικώς ανεξάρτητο υποσύνολο. Εάν $\mathrm{Lin}_K(\mathcal{A}) \subsetneqq V$, τότε για κάθε $x \in V \smallsetminus \mathrm{Lin}_K(\mathcal{A})$ το σύνολο $\mathcal{A} \cup \{x\}$ είναι γραμμικώς ανεξάρτητο.*

ΑΠΟΔΕΙΞΗ. Εάν $\mathcal{A} = \varnothing$, τότε $\mathrm{Lin}_K(\mathcal{A}) = \{0_V\}$, οπότε το $\{x\}$ είναι γραμμικώς ανεξάρτητο για κάθε $x \in V \smallsetminus \{0_V\}$. Εάν $\mathcal{A} \neq \varnothing$ και

$$\lambda x + \sum_{j=1}^{k} \lambda_j x_j = 0_V,$$

όπου $\{x_1, ..., x_k\} \subseteq \mathcal{A}$ και $\lambda, \lambda_1, ..., \lambda_k \in K$, τότε έχουμε κατ' ανάγκην $\lambda = 0_K$, διότι[35] $x \notin \mathrm{Lin}_K(\mathcal{A})$, οπότε η ανωτέρω ισότητα δίδει

$$\sum_{j=1}^{k} \lambda_j x_j = 0_V \Longrightarrow \lambda_1 = \cdots = \lambda_k = 0_K,$$

καθότι το $\{x_1, ..., x_k\}$ είναι γραμμικώς ανεξάρτητο. Άρα και το σύνολο $\mathcal{A} \cup \{x\}$ είναι γραμμικώς ανεξάρτητο. $\square$

A.6.25 Θεώρημα. *Έστω V ένας διανυσματικός χώρος ορισμένος υπεράνω ενός σώματος K. Εάν το $\mathcal{A} \subseteq V$ είναι ένα γραμμικώς ανεξάρτητο υποσύνολο και το $\mathcal{E}$ ένα παράγον σύνολο τού V (δηλαδή $\mathrm{Lin}_K(\mathcal{E}) = V$), τότε υπάρχει τουλάχιστον μία βάση $\mathcal{X}$ τού V, τέτοια ώστε να ισχύει*

$$\boxed{\mathcal{A} \subseteq \mathcal{X} \subseteq \mathcal{E}.}$$

ΑΠΟΔΕΙΞΗ. Έστω $\mathfrak{Q} := \{\mathcal{C} \subseteq V \mid \mathcal{C} \text{ γραμμικώς ανεξάρτητο} : \mathcal{A} \subseteq \mathcal{C} \subseteq \mathcal{E}\}$. Επειδή $\mathcal{A} \in \mathfrak{Q}$, έχουμε $\mathfrak{Q} \neq \varnothing$. Επιπροσθέτως, το $\mathfrak{Q}$ είναι μερικώς διατεταγμένο σύνολο ως προς τη σχέση τού εγκλεισμού "$\subseteq$".

• *Πρώτος ισχυρισμός*: Κάθε αλυσίδα $\mathfrak{C}$ τού $\mathfrak{Q}$ *διαθέτει άνω φράγμα* (ως προς τη σχέση "$\subseteq$"). Πράγματι· εάν η $\mathfrak{C}$ είναι τυχούσα αλυσίδα τού $\mathfrak{Q}$ και εάν θέσουμε

$$\mathcal{Z} := \bigcup \{\mathcal{C} \mid \mathcal{C} \in \mathfrak{C}\},$$

τότε $\mathcal{C} \subseteq \mathcal{Z}$ για όλα τα $\mathcal{C} \in \mathfrak{C}$, οπότε

$$[\mathcal{A} \subseteq \mathcal{C} \subseteq \mathcal{E},\ \forall \mathcal{C} \in \mathfrak{C}] \Longrightarrow \mathcal{A} \subseteq \mathcal{Z} \subseteq \mathcal{E}. \tag{A.20}$$

[35] Αλλιώς θα είχαμε $x = -\sum_{j=1}^{k} (\lambda^{-1}\lambda_j)\, x_j \in \mathrm{Lin}_K(\mathcal{A})$.

Εάν υποθέσουμε ότι το $\{x_1, ..., x_k\} \subseteq \mathcal{Z}$ είναι ένα πεπερασμένο υποσύνολο τού $\mathcal{Z}$ και λ_1,..., $\lambda_k \in K$, ούτως ώστε να ισχύει

$$\sum_{j=1}^{k} \lambda_j x_j = 0_V \tag{A.21}$$

θα υπάρχουν $\mathcal{C}_1, \mathcal{C}_2, ..., \mathcal{C}_k \in \mathfrak{C}$, τέτοια ώστε $x_j \in \mathcal{C}_j, \forall j \in \{1, ..., k\}$. Η $\mathfrak{C}$ -ούσα αλυσίδα- είναι ένα ολικώς διατεταγμένο σύνολο, πράγμα που σημαίνει ότι τα στοιχεία της θα είναι ανά δύο συγκρίσιμα, οπότε θα υπάρχει κατ' ανάγκην ένα $\mathcal{C} \in \mathfrak{C}$, τέτοιο ώστε $x_j \in \mathcal{C}_j \subseteq \mathcal{C}, \forall j \in \{1, ..., k\}$. Επειδή αυτό το $\mathcal{C}$ είναι γραμμικώς ανεξάρτητο και η (A.21) είναι μια εξίσωση εντός τού $\mathrm{Lin}_K(\mathcal{C})$, λαμβάνουμε $\lambda_1 = \cdots = \lambda_k = 0_K$. Συνεπώς το $\mathcal{Z}$ είναι *γραμμικώς ανεξάρτητο*. Τούτο, συνδυαζόμενο με την (A.20), μας πληροφορεί ότι το $\mathcal{Z}$ ανήκει στην οικογένεια συνόλων $\mathfrak{Q}$, οπότε, από την ίδια του την κατασκευή, το $\mathcal{Z}$ αποτελεί ένα *άνω φράγμα* τής $\mathfrak{Q}$ (ως προς την "$\subseteq$"). Θέτοντας σε εφαρμογή το λήμμα τού Zorn για την $\mathfrak{Q}$, συνάγουμε ότι η $\mathfrak{Q}$ έχει ένα *μεγιστικό στοιχείο*, ας πούμε το $\mathcal{X}$, ως προς την "$\subseteq$".

• *Δεύτερος ισχυρισμός*: Το εν λόγω $\mathcal{X}$ *είναι μια βάση τού* V.

Επειδή $\mathcal{X} \in \mathfrak{Q}$, το $\mathcal{X}$ είναι γραμμικώς ανεξάρτητο. Αρκεί λοιπόν να αποδειχθεί ότι $\mathrm{Lin}_K(\mathcal{X}) = V$. Ας υποθέσουμε ότι $\mathrm{Lin}_K(\mathcal{X}) \subsetneqq V$. Τότε $\mathcal{X} \subsetneqq \mathcal{E}$ και θα υπάρχει κάποιο $x \in \mathcal{E} \setminus \mathrm{Lin}_K(\mathcal{X})$. Όμως, δυνάμει τού λήμματος A.6.24, το $\mathcal{X} \cup \{x\}$ θα είναι γραμμικώς ανεξάρτητο και επειδή $\mathcal{A} \subseteq \mathcal{X} \cup \{x\} \subseteq \mathcal{E}$ θα έχουμε $\mathcal{X} \cup \{x\} \in \mathfrak{Q}$, ήτοι κάτι το οποίο αντίκειται στην προϋποτεθείσα μεγιστικότητα τού $\mathcal{X}$. Άρα τελικώς $\mathrm{Lin}_K(\mathcal{X}) = V$ και το $\mathcal{X}$ είναι μια βάση τού V. □

A.6.26 Πόρισμα. (Ύπαρξη βάσεως) *Κάθε K-διανυσματικός χώρος V διαθέτει τουλάχιστον μία βάση (οπότε είναι ελεύθερος K-μόδιος,* βλ. θεώρημα A.6.13).

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμόσουμε το θεώρημα A.6.25 για $\mathcal{A} := \varnothing$ και $\mathcal{E} := V$. □

A.6.27 Πόρισμα. (Θεώρημα «συμπληρώσεως») *Κάθε γραμμικώς ανεξάρτητο υποσύνολο $\mathcal{A} \subseteq V$ ενός K-διανυσματικού χώρου V μπορεί να συμπληρωθεί καταλλήλως, ούτως ώστε να καταστεί μία βάση αυτού.*

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμόσουμε το θεώρημα A.6.25 για το $\mathcal{A}$ και το $\mathcal{E} := V$. □

A.6.28 Πόρισμα. *Κάθε παράγον σύνολο $\mathcal{E}$ ενός K-διανυσματικού χώρου V εμπεριέχει τουλάχιστον μία βάση τού V.*

ΑΠΟΔΕΙΞΗ. Αρκεί να εφαρμόσουμε το θεώρημα A.6.25 για το $\mathcal{A} := \varnothing$ και το $\mathcal{E}$. □

A.6.29 Σημείωση. Τα πορίσματα A.6.27 και A.6.28 δεν ισχύουν για *τυχόντες ελεύθερους* R-μοδίους. Επί παραδείγματι, το $\mathcal{A} := \{2\}$ ναι μεν είναι ένα γραμμικώς ανεξάρτητο υποσύνολο τού ελευθέρου $\mathbb{Z}$-μοδίου $\mathbb{Z}$ αλλά δεν μπορεί να συμπληρωθεί καταλλήλως, ούτως ώστε να προκύψει μια βάση αυτού. Επίσης, το

$\mathcal{E} := \{2,3\}$ είναι ένα σύστημα γεννητόρων τού ιδίου μοδίου (διότι $3n - 2n = n$ για κάθε $n \in \mathbb{Z}$) αλλά κανένα εκ των μονοσυνόλων $\{2\}, \{3\}$ δεν αποτελεί βάση[36] αυτού (διότι $2\mathbb{Z} \subsetneqq \mathbb{Z}$ και $3\mathbb{Z} \subsetneqq \mathbb{Z}$).

A.6.30 Πόρισμα. *Εάν V είναι ένας K-διανυσματικός χώρος και $\mathcal{X} \subseteq V$, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Το $\mathcal{X}$ είναι μια βάση τού V.*

(ii) *Το $\mathcal{X}$ είναι ένα ελαχιστικό σύστημα γεννητόρων τού V.*

(iii) *Το $\mathcal{X}$ είναι ένα μεγιστικό γραμμικώς ανεξάρτητο υποσύνολο τού V.*

Απόδειξη. Λαμβανομένων υπ' όψιν τού πορίσματος A.6.26 και τού θεωρήματος A.6.13, οι συνεπαγωγές (i)⇒(ii) και (i)⇒(iii) έχουν ήδη αποδειχθεί στην πρόταση A.6.11.

(ii)⇒(i) Το θεώρημα A.6.25 εγγυάται την ύπαρξη μιας βάσεως $\mathcal{Y}$ τού διανυσματικού χώρου V με $\varnothing \subseteq \mathcal{Y} \subseteq \mathcal{X}$. Επειδή $\mathrm{Lin}_K(\mathcal{Y}) = V$ και το $\mathcal{X}$ είναι ένα ελαχιστικό σύστημα γεννητόρων τού V, έχουμε κατ' ανάγκην $\mathcal{Y} = \mathcal{X}$.

(iii)⇒(i) Το πόρισμα A.6.27 εγγυάται την ύπαρξη μιας βάσεως $\mathcal{Y}$ τού V με $\mathcal{Y} \subseteq \mathcal{X}$. Επειδή το $\mathcal{Y}$ είναι γραμμικώς ανεξάρτητο υποσύνολο τού V και το $\mathcal{X}$ ένα μεγιστικό γραμμικώς ανεξάρτητο υποσύνολο τού V, έχουμε κατ' ανάγκην $\mathcal{Y} = \mathcal{X}$. □

A.6.31 Σημείωση. Οι συνεπαγωγές (ii)⇒(i) και (iii)⇒(i) τού πορίσματος A.6.30 δεν ισχύουν για *τυχόντες* R-μοδίους. Επί παραδείγματι, εάν $k \in \mathbb{N}, k \geq 2$, τότε το μονοσύνολο $\{[1]_k\}$ είναι ελαχιστικό παράγον υποσύνολο τού $\mathbb{Z}$-μοδίου $\mathbb{Z}_k$, χωρίς να αποτελεί βάση αυτού. (Βλ. A.6.15 (i).) Επίσης, για κάθε $q \in \mathbb{Q} \smallsetminus \{0\}$ με $q \neq \frac{1}{b}$, όπου $b \in \mathbb{Z} \smallsetminus \{0\}$, το μονοσύνολο $\{q\}$ είναι ένα μεγιστικό γραμμικώς ανεξάρτητο υποσύνολο τού $\mathbb{Z}$-μοδίου $\mathbb{Q}$, χωρίς να αποτελεί βάση αυτού. (Πρβλ. A.6.15 (iii).)

Εν συνεχεία, για την απόδειξη τού ότι όλες οι βάσεις ενός διανυσματικού χώρου είναι ισοπληθείς, προτάσσονται ορισμένα αποτελέσματα από τη Θεωρία Συνόλων.

A.6.32 Θεώρημα. (Schröder & Bernstein) *Εάν A, B είναι δυο σύνολα, τότε ισχύει η συνεπαγωγή*

$$[\mathrm{card}(A) \leq \mathrm{card}(B) \text{ και } \mathrm{card}(B) \leq \mathrm{card}(A)] \Rightarrow \mathrm{card}(A) = \mathrm{card}(B).$$

Απόδειξη. Βλ., π.χ., [43], Κεφ. 22, σελ. 128-132, ή [53], εδ. 16.3, σελ. 246. □

A.6.33 Πρόταση. *Εάν A, B είναι δυο απειροσύνολα, τότε*

$$\mathrm{card}(A \times B) = \sup\{\mathrm{card}(A), \mathrm{card}(B)\}.$$

[36] Το ίδιο το $\{2,3\}$ είναι γραμμικώς εξαρτημένο, καθώς ισχύει $3 \cdot 2 + (-2) \cdot 3 = 0$.

ΑΠΟΔΕΙΞΗ. Δίχως βλάβη τής γενικότητας υποθέτουμε ότι $\mathrm{card}(A) \leq \mathrm{card}(B)$. Προφανώς,

$$\mathrm{card}(B) \leq \mathrm{card}(A \times B) \leq \mathrm{card}(B \times B) = \mathrm{card}(B),$$

οπότε $\mathrm{card}(A \times B) = \mathrm{card}(B)$ δυνάμει τού θεωρήματος A.6.32. □

A.6.34 Πρόταση. *Έστω A ένα απειροσύνολο και έστω $(B_j)_{j\in J}$ μια οικογένεια συνόλων με $J \neq \varnothing$, $\mathrm{card}(J) \leq \mathrm{card}(A)$ και $\mathrm{card}(B_j) \leq \mathrm{card}(A)$ για κάθε $j \in J$. Τότε*

$$\mathrm{card}(\textstyle\bigcup_{j\in J} B_j) \leq \mathrm{card}(A). \tag{A.22}$$

ΑΠΟΔΕΙΞΗ. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $B_j \neq \varnothing$ για κάθε $j \in J$. Επειδή $\mathrm{card}(B_j) \leq \mathrm{card}(A)$, υπάρχει μια επίρριψη $g_j : A \longrightarrow B_j$. Η απεικόνιση

$$A \times J \ni (a, j) \longmapsto g_j(a) \in \textstyle\bigcup_{j\in J} B_j$$

είναι ωσαύτως επιρριπτική, οπότε

$$\mathrm{card}(A \times J) \geq \mathrm{card}(\textstyle\bigcup_{j\in J} B_j) \text{ και } \mathrm{card}(A \times J) \leq \mathrm{card}(A)$$

(βλ. A.6.33), απ' όπου έπεται η (A.22). □

A.6.35 Πρόταση. *Έστω M ένας R-μόδιος. Εάν $(x_j)_{j\in J}$ είναι ένα σύστημα γεννητόρων τού M, όπου το σύνολο δεικτών J είναι απειροσύνολο, και $(y_\lambda)_{\lambda\in\Lambda}$ μια βάση αυτού, τότε*

$$\mathrm{card}(J) \geq \mathrm{card}(\Lambda). \tag{A.23}$$

ΑΠΟΔΕΙΞΗ. Για κάθε $j \in J$ το x_j γράφεται (κατά τρόπο μοναδικό) ως γραμμικός συνδυασμός στοιχείων τής οικογενείας $(y_\lambda)_{\lambda\in\Lambda}$. Για να διευκολυνθούμε εργαζόμενοι με *πεπερασμένα* υποσύνολα τού *απειροσυνόλου* δεικτών J (χωρίς να κάνουμε ευρεία χρήση πολλαπλών υποδεικτών) γράφουμε το x_j ως εξής:

$$x_j = \sum_{\lambda\in\Lambda} r_j(\lambda) y_\lambda, \tag{A.24}$$

όπου ο συντελεστής $r_j(\lambda) \in R$ είναι η εικόνα τού λ μέσω μιας (μονοσημάντως ορισμένης) $r_j \in R^{(\Lambda)}$. Προφανώς, το «επίτυπο» άθροισμα (A.24) διαθέτει το πολύ πεπερασμένους προσθετέους που είναι $\neq 0_R$ (οπότε επέχει θέση συνήθους αθροίσματος). Ως εκ τούτου, τα $\Lambda_j := \{\lambda \in \Lambda | \, r_j(\lambda) \neq 0_R\}$ συγκροτούν ένα σύστημα πεπερασμένων υποσυνόλων τού Λ.

Ισχυρισμός: $\Lambda = \bigcup_{j\in J} \Lambda_j$. Εάν υπήρχε $\lambda_\star \in \Lambda$ με $r_j(\lambda_\star) = 0_R$ για κάθε $j \in J$, τότε, επειδή το $(x_j)_{j\in J}$ είναι ένα σύστημα γεννητόρων τού M, θα υπήρχε $b \in R^{(J)}$, ούτως ώστε να ισχύει

$$\left.\begin{array}{r} y_{\lambda_\star} = \sum\limits_{j\in J} b(j)x_j = \sum\limits_{(j,\lambda)\in J\times\Lambda} (b(j)r_j(\lambda))\, y_\lambda \\ (y_\lambda)_{\lambda\in\Lambda} \;\; \text{βάση τού } M \end{array}\right\} \Longrightarrow \left[\sum_{j\in J} b(j)r_j(\lambda_\star) = 1_R \; (\neq 0_R)\right],$$

κάτι που θα αντέκειτο στην υπόθεσή μας (ότι $r_j(\lambda_\star) = 0_R, \forall j \in J$). Άρα ο ισχυρισμός είναι αληθής και εφαρμόζοντας την πρόταση A.6.34 (για $A = J$ και $B_j = \Lambda_j$) λαμβάνουμε την (A.23). □

A.6.36 Θεώρημα. *Όλες οι βάσεις ενός K-διανυσματικού χώρου είναι ισοπληθείς.*

ΑΠΟΔΕΙΞΗ. Έστω V ένας διανυσματικός χώρος ορισμένος υπεράνω ενός σώματος K. Η *ύπαρξη* βάσεων αυτού είναι διασφαλισμένη από το πόρισμα A.6.27. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι ο V δεν είναι τετριμμένος[37]. Υπάρχουν δύο ενδεχόμενα:

Περίπτωση πρώτη: *Ο V διαθέτει μια άπειρη βάση $\mathcal{X} = (x_j)_{j\in J}$*. Ας υποθέσουμε ότι $\mathcal{Y} = (y_\lambda)_{\lambda\in\Lambda}$ είναι μια άλλη βάση τού V. Τότε, επειδή το $\mathcal{X}$ παράγει τον V, από την πρόταση A.6.35

$$\mathrm{card}(\mathcal{X}) = \mathrm{card}(J) \geq \mathrm{card}(\Lambda) = \mathrm{card}(\mathcal{Y}). \tag{A.25}$$

Ισχυρισμός: *Το $\mathcal{Y}$ είναι κατ' ανάγκην απειροσύνολο*. Για την επαλήθευσή του θα εργασθούμε μιμούμενοι τη μέθοδο που ακολουθήσαμε στην απόδειξη τής προτάσεως A.6.35 (αλλά προς την *αντίθετη κατεύθυνση*). Για κάθε $\lambda \in \Lambda$ το y_λ είναι γραμμικός συνδυασμών στοιχείων τής $\mathcal{X}$, οπότε

$$\exists s_\lambda \in K^{(J)} : y_\lambda = \sum_{j\in J} s_\lambda(j) x_j,$$

τα $J_\lambda := \{j \in J |\, s_\lambda(j) \neq 0_K\}$ συγκροτούν ένα σύστημα πεπερασμένων υποσυνόλων τού J και $J = \bigcup_{\lambda\in\Lambda} J_\lambda$. Εάν το $\mathcal{Y}$ ήταν πεπερασμένο, τότε θα είχαμε

$$\mathrm{card}(\mathcal{X}) = \mathrm{card}(J) \leq \sum_{\lambda\in\Lambda} \mathrm{card}(J_\lambda) \leq \underbrace{\mathrm{card}(\Lambda)}_{=\,\mathrm{card}(\mathcal{Y})} \max\{\mathrm{card}(J_\lambda) |\, \lambda \in \Lambda\}$$

με $\mathrm{card}(\mathcal{Y}) < \infty$ και $\mathrm{card}(J_\lambda) < \infty, \forall \lambda \in \Lambda$, και θα οδηγούμεθα σε άτοπο! Άρα *και* το $\mathcal{Y}$ είναι κατ' ανάγκην απειροσύνολο και, ως εκ τούτου, *εάν ένας K-διανυσματικός χώρος διαθέτει μια άπειρη βάση, τότε και κάθε άλλη βάση του είναι άπειρη*. Άπαξ και αποδείξαμε ότι το $\mathcal{Y}$ οφείλει να είναι άπειρο, είμαστε σε θέση να εφαρμόσουμε εκ νέου την πρόταση A.6.35 *αφού προηγουμένως έχουμε εναλλάξει τους ρόλους των $\mathcal{X}$ και $\mathcal{Y}$*. Έτσι λαμβάνουμε

$$\mathrm{card}(\mathcal{Y}) = \mathrm{card}(J) \geq \mathrm{card}(\Lambda) = \mathrm{card}(\mathcal{X}). \tag{A.26}$$

Λόγω τής ισχύος των (A.25) και (A.26) το θεώρημα A.6.32 μας πληροφορεί ότι $\mathrm{card}(\mathcal{X}) = \mathrm{card}(\mathcal{Y})$.

Περίπτωση δεύτερη: *Ο V διαθέτει μια πεπερασμένη βάση $\mathcal{X} = \{x_1, ..., x_k\}$*. Εν τοιαύτη περιπτώσει, και κάθε άλλη βάση τού V οφείλει (κατά τα προαναφερθέντα)

[37]Η μόνη βάση ενός τετριμμένου K-διανυσματικού χώρου είναι το $\varnothing$.

να είναι πεπερασμένη. Κατά τα πορίσματα A.6.26 και A.6.16, $V = \bigoplus_{j=1}^{k} Kx_j$. Επειδή $Kx_j \cong K$, το Kx_j είναι απλός K-μόδιος (βλ. A.4.17 (i)), καθότι το K, όντας σώμα, δεν διαθέτει άλλα ιδεώδη πέραν τού τετριμμένου και τού ιδίου τού K. Επιπροσθέτως, επειδή

$$\left(\bigoplus_{j=1}^{\nu} Kx_j\right) / \left(\bigoplus_{j=1}^{\nu-1} Kx_j\right) \cong \left(\bigoplus_{j=1}^{\nu-1} Kx_j \oplus Kx_\nu\right) / \left(\bigoplus_{j=1}^{\nu-1} Kx_j\right) \underset{\text{A.5.20}}{\cong} Kx_\nu \cong K$$

για κάθε $\nu \in \{2, ..., k\}$, βλέπουμε ότι ο πύργος γραμμικών υποχώρων

$$V = \bigoplus_{j=1}^{k} Kx_j \supsetneqq \bigoplus_{j=1}^{k-1} Kx_j \supsetneqq \cdots \supsetneqq \bigoplus_{j=1}^{3} Kx_j \supsetneqq \bigoplus_{j=1}^{2} Kx_j \supsetneqq Kx_1 \supsetneqq \{0_V\}$$

τού V είναι ένας πύργος των Jordan και Hölder έχων ύψος ίσο με k. (Βλ. A.4.17 (ii).) Λόγω *τού αναλλοιώτου τού ύψους* ενός τέτοιου πύργου (βλ. εδ. A.4.19) *όλες οι βάσεις τού V οφείλουν να έχουν ακριβώς k στοιχεία*[38]. □

A.6.37 Ορισμός. Ο *κοινός* πληθικός αριθμός όλων των βάσεων ενός K-διανυσματικού χώρου V καλείται **διάσταση** αυτού και συμβολίζεται ως $\dim_K(V)$.

A.6.38 Θεώρημα. *Όλες οι βάσεις ενός ελεύθερου R-μοδίου είναι ισοπληθείς.*

ΑΠΟΔΕΙΞΗ. Έστω M ένας ελεύθερος R-μόδιος. Εάν ο M είναι τετριμμένος, τότε το $\varnothing$ είναι η μόνη βάση αυτού. Γι' αυτόν τον λόγο θα υποθέσουμε από εδώ και στο εξής ότι ο M δεν είναι τετριμμένος και θα θεωρήσουμε ένα μεγιστικό ιδεώδες $\mathfrak{m}$ τού R. Ως γνωστόν, ο πηλικοδακτύλιος $R/\mathfrak{m}$ είναι ένα σώμα. (Βλ. ??.) Επίσης, είναι εύκολος ο έλεγχος τού ότι ο πηλικομόδιος $M/\mathfrak{m}M$ είναι *διανυσματικός χώρος* υπεράνω τού $R/\mathfrak{m}$ ως προς τη συνήθη πρόσθεση και τον αριθμητικό πολλαπλασιασμό[39]

$$(R/\mathfrak{m}) \times (M/\mathfrak{m}M) \ni (r + \mathfrak{m}, x + \mathfrak{m}M) \longmapsto rx + \mathfrak{m}M \in M/\mathfrak{m}M.$$

Ας υποθέσουμε ότι το $\mathcal{X} = (x_j)_{j \in J}$ είναι μια βάση τού R-μοδίου M. Κατά το πόρισμα A.6.16 έχουμε

$$M = \bigoplus_{j \in J} Rx_j \Longrightarrow \mathfrak{m}M = \bigoplus_{j \in J} \mathfrak{m}x_j,$$

[38] Εάν θεωρούσαμε μια άλλη βάση $\mathcal{Y} = \{y_1, ..., y_l\}$ τού V, τότε (χρησιμοποιώντας τα ίδια επιχειρήματα) θα καταλήγαμε στο συμπέρασμα ότι $l = k$.

[39] Ο εν λόγω αριθμητικός πολλαπλασιασμός είναι *καλώς ορισμένος*, διότι εάν $r, r' \in R$ και $x, x' \in M$ είναι τέτοια, ώστε να ισχύει $r - r' = a \in \mathfrak{m}$ και $x - x' = a_1 y_1 + \cdots + a_k y_k$ για κάποια $a_1, ..., a_k \in \mathfrak{m}$ και $y_1, ..., y_k \in M$, τότε

$$rx + \mathfrak{m}M = r'x' + \underbrace{ax' + \textstyle\sum_{j=1}^{k}(a + r')a_j y_j}_{\in \mathfrak{m}M} + \mathfrak{m}M = r'x' + \mathfrak{m}M.$$

οπότε

$$\begin{aligned} M/\mathfrak{m}M &\cong \left(\bigoplus_{j\in J} Rx_j\right) / \left(\bigoplus_{j\in J} \mathfrak{m}x_j\right) \\ &\underset{\text{A.5.24}}{\cong} \bigoplus_{j\in J}(Rx_j/\mathfrak{m}x_j) \cong \bigoplus_{j\in J} R/\mathfrak{m} = (R/\mathfrak{m})^{(J)}, \end{aligned}$$

διότι $Rx_j \cong R$ και $\mathfrak{m}x_j \cong \mathfrak{m}$ (ως R-μόδιοι) για κάθε $j \in J$. Κατά συνέπειαν,

$$\dim_{R/\mathfrak{m}}(M/\mathfrak{m}M) = \text{card}(J) = \text{card}(\mathcal{X}).$$

Κατ' αναλογίαν, $\dim_{R/\mathfrak{m}}(M/\mathfrak{m}M) = \text{card}(\mathcal{Y})$ για οιαδήποτε άλλη βάση $\mathcal{Y}$ τού M. Άρα οι βάσεις $\mathcal{X}$ και $\mathcal{Y}$ είναι κατ' ανάγκην ισοπληθείς (δυνάμει τού θεωρήματος A.6.36). □

A.6.39 Ορισμός. Ο *κοινός* πληθικός αριθμός όλων των βάσεων ενός ελεύθερου R-μοδίου M καλείται **βαθμίδα** αυτού και συμβολίζεται ως[40] $\text{rank}_R(M)$.

A.6.40 Παραδείγματα. (i) Για κάθε $n \in \mathbb{N}$ έχουμε $\text{rank}_{\mathbb{Z}}(\mathbb{Z}^n) = n$.
(ii) Προφανώς, $\text{rank}_{\mathbb{Z}}(\mathbb{Z}[\mathsf{X}]) = \aleph_0$.
(iii) Η βαθμίδα τού $\mathbb{Z}$-μοδίου $\mathbb{Z}^{(\mathbb{R})}$ ισούται με τη *δύναμη τού συνεχούς* $\mathfrak{c}$.

A.6.41 Πρόταση. *Για δυο ελεύθερους R-μοδίους M, N ισχύει η αμφίπλευρη συνεπαγωγή*

$$M \cong N \Longleftrightarrow \text{rank}_R(M) = \text{rank}_R(N).$$

ΑΠΟΔΕΙΞΗ. Εάν οι M και N είναι ισόμορφοι, τότε η βαθμίδα τού ενός θα ισούται με τη βαθμίδα τού άλλου δυνάμει τής προτάσεως A.6.10. Και αντιστρόφως· εάν οι βαθμίδες των M, N είναι ίσες με το 0, τότε αμφότεροι οι M, N είναι τετριμμένοι (και, ως εκ τούτου, ισόμορφοι). Εάν υποθέσουμε ότι η κοινή βαθμίδα των M, N είναι $\neq 0$ και $\mathcal{X}$ είναι μια βάση τού M, τότε $M \cong R^{(\mathcal{X})}$ (βλ. πόρισμα A.6.14) και $\text{rank}_R(M) = \text{card}(\mathcal{X})$. Έστω $\mathcal{Y}$ *τυχούσα* βάση τού N. Εξ υποθέσεως,

$$\text{card}(\mathcal{X}) = \text{rank}_R(M) = \text{rank}_R(N) = \text{card}(\mathcal{Y}),$$

οπότε υπάρχει κάποια αμφίρριψη $\theta : \mathcal{X} \longrightarrow \mathcal{Y} \subseteq N$. Είναι εύκολο να δειχθεί ότι η γραμμική επέκταση $f \in \text{Hom}_R(M, N)$ τής θ αποτελεί έναν ισομορφισμό μεταξύ των M και N. □

A.6.42 Πόρισμα. *Για κάθε ελεύθερο R-μόδιο M με* $\text{rank}_R(M) = n \in \mathbb{N}$ *έχουμε* $M \cong R^n$.

A.6.43 Πόρισμα. *Εάν $n_1, n_2 \in \mathbb{N}$, τότε $R^{n_1} \cong R^{n_2} \Longleftrightarrow n_1 = n_2$.*

[40]Προφανώς, $\text{rank}_R(M) = 0$ εάν και μόνον εάν ο M είναι τετριμμένος. Εάν M είναι ένας μη τετριμμένος R-μόδιος έχων το $\mathcal{X}$ ως μια βάση του, τότε $M \cong R^{(\mathcal{X})}$ (βλ. A.6.14) και $\text{rank}_R(M) = \text{card}(\mathcal{X})$.

A.6.44 Πόρισμα. *Εάν $n_1, n_2 \in \mathbb{N}$ και M, N είναι ελεύθεροι R-μόδιοι βαθμίδας n_1 και n_2, αντιστοίχως, τότε ο $M \oplus N$ είναι ελεύθερος βαθμίδας $n_1 + n_2$.*

ΑΠΟΔΕΙΞΗ. Προφανώς, $[M \cong R^{n_1}$ και $N \cong R^{n_2}] \Rightarrow M \oplus N \cong R^{n_1+n_2}$. □

► **Δύο επιπρόσθετα σημαντικά θεωρήματα περί ελευθέρων R-μοδίων**. Η παρούσα ενότητα θα κλείσει με την παράθεση τής αποδείξεως δύο ακόμη θεωρημάτων που αφορούν σε ελεύθερους R-μοδίους. Το πρώτο εξ αυτών (βλ. A.6.46) διασφαλίζει *την ύπαρξη συμπληρώματος*[41] *ενός υπομοδίου U ενός R-μοδίου M υπό την προϋπόθεση ότι ο πηλικομόδιος M/U είναι ελεύθερος*. Το δεύτερο (βλ. A.6.47) μας πληροφορεί ότι *οι υπομόδιοι ελευθέρων R-μοδίων είναι ελεύθεροι όταν ο R είναι* Π.Κ.Ι.

A.6.45 Λήμμα. *Για κάθε επιμορφισμό $f : M \longrightarrow N$ από έναν R-μόδιο M επί ενός ελευθέρου R-μοδίου N*

$$\exists g \in \mathrm{Hom}_R(N, M) : [f \circ g = \mathrm{id}_N \text{ και } M = \mathrm{Ker}(f) \oplus \mathrm{Im}(g)].$$

ΑΠΟΔΕΙΞΗ. Όταν ο N είναι τετριμμένος, ο ισχυρισμός είναι προδήλως αληθής. Ας υποθέσουμε ότι ο N είναι μη τετριμμένος και ότι $\mathcal{X}$ είναι μια βάση αυτού. Κατά το αξίωμα τής επιλογής, για κάθε στοιχείο $x \in \mathcal{X}$ υπάρχει κάποιο $z_x \in M$, τέτοιο ώστε να ισχύει $f(z_x) = x$. Θεωρούμε την απεικόνιση

$$\theta : \mathcal{X} \longrightarrow M, \;\; x \longmapsto \theta(x) := z_x.$$

Δυνάμει τού θεωρήματος A.6.20 υπάρχει ένας (και μόνον) $g \in \mathrm{Hom}_R(N, M)$ με την ιδιότητα $g(x) = \theta(x) := z_x, \; \forall x \in \mathcal{X}$. Προφανώς,

$$[(f \circ g)(x) = f(z_x) = x, \forall x \in \mathcal{X}] \Rightarrow f \circ g|_{\mathcal{X}} = \mathrm{id}_{\mathcal{X}} \underset{\text{A.6.22}}{\Longrightarrow} f \circ g = \mathrm{id}_N.$$

Επομένως ο g είναι *μονομορφισμός* (βλ. A.3.23 (ii)⇒(i)) και ο $\breve{g} : N \longrightarrow \mathrm{Im}(g)$ (που προκύπτει ύστερα από περιορισμό τού πεδίου τιμών τού g στην εικόνα του, βλ. (A.11)) είναι *ισομορφισμός*, έχων τον περιορισμό $f|_{\mathrm{Im}(g)} : \mathrm{Im}(g) \xrightarrow{\cong} N$ τού f επί τής $\mathrm{Im}(g)$ ως αντίστροφό του. Από την ενριπτικότητα αυτού τού περιορισμού έπεται, ιδιαιτέρως, ότι

$$\mathrm{Ker}(f) \cap \mathrm{Im}(g) = \mathrm{Ker}(f|_{\mathrm{Im}(g)}) = \{0_M\}. \tag{A.27}$$

Από την άλλη μεριά, για κάθε $z \in M$ ισχύει

$$z = \underbrace{(z - g(f(z)))}_{\in \mathrm{Ker}(f)} + \underbrace{g(f(z))}_{\in \mathrm{Im}(g)}, \tag{A.28}$$

διότι $f(z - g(f(z))) = f(z) - (f \circ g)(f(z)) = f(z) - \mathrm{id}_N(f(z)) = f(z) - f(z) = 0_N$. Από τις (A.27) και (A.28) συνάγεται ότι $M = \mathrm{Ker}(f) \oplus \mathrm{Im}(g)$. □

[41] Όπως έχει ήδη αναφερθεί στο εδ. A.5.19 (i), υπάρχουν υπομόδιοι R-μοδίων που *δεν διαθέτουν κανένα συμπλήρωμα*.

Α.6.46 Θεώρημα. (Συνθήκη διασφαλίζουσα την ύπαρξη συμπληρώματος) *Έστω U ένας υπομόδιος ενός R-μοδίου M. Εάν ο πηλικομόδιος M/U είναι ελεύθερος, τότε υπάρχει υπομόδιος U' τού M, τέτοιος ώστε να ισχύει $M = U \oplus U'$.*

ΑΠΟΔΕΙΞΗ. Αρκεί η εφαρμογή τού λήμματος Α.6.45 για τους M και $N = M/U$, όπου $f = \pi_U^M$ (διότι $\mathrm{Ker}(\pi_U^M) = U$ με τον π_U^M επιμορφισμό, βλ. Α.4.1 (iii)). $\square$

Α.6.47 Θεώρημα. (Υπομόδιοι ελευθέρων μοδίων υπεράνω Π.Κ.Ι.) *Εάν M είναι ένας ελεύθερος R-μόδιος και ο R είναι Π.Κ.Ι., τότε και κάθε υπομόδιος U τού M είναι ελεύθερος και* $\mathrm{rank}_R(U) \leq \mathrm{rank}_R(M)$.

ΑΠΟΔΕΙΞΗ. Έστω U ένας υπομόδιος τυχόντος ελεύθερου R-μοδίου M.

Περίπτωση πρώτη. Εάν $\mathrm{rank}_R(M) = 0$, τότε ο M είναι τετριμμένος και δεν διαθέτει άλλον υπομόδιο πέραν τού εαυτού του.

Περίπτωση δεύτερη. Υποθέτουμε ότι $\mathrm{rank}_R(M) \neq 0$. Εάν $U = \{0_M\}$, τότε ο U έχει το $\varnothing$ ως βάση του και είναι ελεύθερος έχων βαθμίδα 0. Άρα μπορούμε από τούδε και στο εξής να υποθέσουμε ότι $\{0_M\} \neq U \subseteq M$ και να θεωρήσουμε μια βάση $(x_\lambda)_{\lambda \in \Lambda}$ τού M (με $\mathrm{card}(\Lambda) = \mathrm{rank}_R(M)$). Για κάθε υποσύνολο $J \subseteq \Lambda$ θέτουμε $M_J := \mathrm{Lin}_R((x_j)_{j \in J})$ και $U_J := M_J \cap U$.

Ισχυρισμός πρώτος. Η ακόλουθη οικογένεια τριάδων είναι μη κενή:

$$\mathfrak{N} := \left\{ (J, J', \varphi) \;\middle|\; \begin{array}{c} J' \subseteq J \subseteq \Lambda \text{ και } \varphi : J' \longrightarrow U_J \text{ απεικόνιση τέτοια,} \\ \text{ώστε η } \{\varphi(j) |\, j \in J'\} \text{ να είναι μια βάση τού } U_J \end{array} \right\}.$$

Απόδειξη πρώτου ισχυρισμού. Επειδή $U \neq \{0_M\}$, υπάρχει κάποιο $x \in U \smallsetminus \{0_M\}$. Αυτό γράφεται ως γραμμικός συνδυασμός $x = r_1 x_{j_1} + \cdots + r_\rho x_{j_\rho}$ στοιχείων τής $(x_\lambda)_{\lambda \in \Lambda}$ (με τουλάχιστον έναν εκ των συντελεστών $\neq 0_R$). Επομένως, $x \in U_J$, όπου $J := \{j_1, ..., j_\rho\} \subseteq \Lambda$. Αυτό σημαίνει ότι *υπάρχουν* πεπερασμένα υποσύνολα $J \subseteq \Lambda$ με $U_J \neq \{0_M\}$. Επιλέγουμε ένα εξ αυτών, ας το πούμε $J := \{j_1, ..., j_\nu\}$, ούτως ώστε το πλήθος ν των στοιχείων του να είναι *το ελάχιστο δυνατό* με αυτήν την ιδιότητα, δηλαδή με $U_{\widehat{J}} = \{0_M\}$ για κάθε $\widehat{J} \subsetneqq J \subseteq \Lambda$ (ήτοι για κάθε $\widehat{J}$ με πλήθος στοιχείων $< \nu$). Έστω τυχόν $x \in U_J \smallsetminus \{0_M\}$. Αυτό γράφεται ως

$$x = a_1 x_{j_1} + \cdots + a_\nu x_{j_\nu}, \text{ για κάποια } a_1, ..., a_\nu \in R$$

(με τουλάχιστον ένα εξ αυτών $\neq 0_R$). Έστω τυχών $d \in \mathrm{MK\Delta}_R(a_1, ..., a_\nu)$. Τότε $a_1 = db_1, ..., a_\nu = db_\nu$ για κατάλληλα $b_1, ..., b_\nu \in R$ με[42] $1_R \in \mathrm{MK\Delta}_R(b_1, ..., b_\nu)$. Θέτοντας

$$x' := b_1 x_{j_1} + \cdots + b_\nu x_{j_\nu} \text{ και } I := \{ r \in R |\, rx' \in U \},$$

παρατηρούμε ότι το I είναι ένα ιδεώδες τού R, οπότε $I = Ra$ για κάποιο $a \in R$, καθώς ο R είναι Π.Κ.Ι. Προφανώς,

$$[dx' = x \in U_J \smallsetminus \{0_M\} \text{ και } U_J \subseteq U] \Rightarrow d \in I \Rightarrow I \neq \{0_R\} \Rightarrow a \neq 0_R.$$

[42] Βλ. [87], λήμμα 5.2.28.

Θα δείξουμε ότι $U_J = \mathrm{Lin}_R(\{y\})$, όπου $y := ax'$ (οπότε το $\{y\}$ θα αποτελεί μια βάση τού U_J). Έστω τυχόν $z \in U_J \smallsetminus \{0_M\}$. Αυτό εκφράζεται υπό τη μορφή

$$z = c_1 x_{j_1} + \cdots + c_\nu x_{j_\nu}, \ \text{ για κάποια } \ c_1, ..., c_\nu \in R \smallsetminus \{0_R\}$$

(διότι εάν κάποιο εξ αυτών ήταν $= 0_R$, τότε κάποιος γραμμικός συνδυασμός στοιχείων τής $(x_\lambda)_{\lambda \in \Lambda}$, το πλήθος των οποίων θα ήταν $< \nu$, θα ανήκε στον U, κάτι που θα αντέκειτο στον τρόπο επιλογής τού J). Επειδή

$$\begin{aligned} ab_1 z - c_1 y &= ab_1(c_1 x_{j_1} + \cdots + c_\nu x_{j_\nu}) - c_1 a(b_1 x_{j_1} + \cdots + b_\nu x_{j_\nu}) \\ &= 0_R x_{j_1} + a(b_1 c_2 - c_1 b_2) x_{j_2} + \cdots + a(b_1 c_\nu - c_1 b_\nu) x_{j_\nu} \end{aligned}$$

η διαφορά $ab_1 z - c_1 y \in U_J$ είναι γραμμικός συνδυασμός στοιχείων τής $(x_\lambda)_{\lambda \in \Lambda}$, το πλήθος των οποίων είναι $< \nu$, οπότε ισχύει κατ' ανάγκην

$$\left.\begin{array}{r} 0_R = ab_1 z - c_1 y = a(b_1 z - c_1 x') \\ a \neq 0_R \ \text{ και } R \text{ ακεραία περιοχή} \end{array}\right\} \Rightarrow b_1 z = c_1 x'$$

και (λόγω των ανωτέρω εξισώσεων) $b_1 c_2 = c_1 b_2, ..., b_1 c_\nu = c_1 b_\nu$. Κατά συνέπειαν,

$$\left.\begin{array}{c} b_1 \mid c_1 b_1 \\ b_1 \mid c_1 b_2 \\ \vdots \\ b_1 \mid c_1 b_\nu \end{array}\right\} \Rightarrow b_1 \mid \mathfrak{d}, \ \forall \mathfrak{d} \in \mathrm{MK\Delta}_R(c_1 b_1, ..., c_1 b_\nu),$$

με[43] $\mathrm{MK\Delta}_R(c_1 b_1, ..., c_1 b_\nu) = \{c_1 \delta : \delta \in \mathrm{MK\Delta}_R(b_1, ..., b_\nu)\}$, απ' όπου έπεται (για $\delta = 1_R$) ότι

$$\left.\begin{array}{r} b_1 \mid c_1 \Rightarrow [\exists c_1' \in R : c_1 = b_1 c_1'] \\ 0_R \neq c_1 \Rightarrow b_1 \neq 0_R \ \text{ και } c_1' \neq 0_R \\ R \text{ ακεραία περιοχή} \end{array}\right\} \Rightarrow z = c_1' x'$$

και, κατ' επέκταση, ότι $c_1' \in I$ (αφού $z \in U$). Επομένως, $c_1' = c_1'' a$ για κάποιο $c_1'' \in R \smallsetminus \{0_R\}$ και, ως εκ τούτου,

$$z = c_1' x' = c_1'' a x' = c_1'' y \in \mathrm{Lin}_R(\{y\}).$$

Έχουμε λοιπόν δείξει ότι το $\{y\}$ αποτελεί μια βάση τού U_J. Θέτοντας $J' := \{j_1\}$ και

$$\varphi : J' \longrightarrow U_J, \ \ j_1 \longmapsto \varphi(j_1) := y,$$

παρατηρούμε ότι η (συγκεκριμένη) τριάδα (J, J', φ) ανήκει στην $\mathfrak{N}$.

[43]Βλ. [87], πρόταση 5.2.35 (iv).

Εφαρμογή τού λήμματος τού Zorn. Η οικογένεια $\mathfrak{N} \neq \varnothing$ καθίσταται μερικώς διατεταγμένο σύνολο ως προς την ακόλουθη “$\preceq$”:

$$(J, J', \varphi) \preceq (L, L', \theta) \underset{\text{ορσ}}{\Longleftrightarrow} [J \subseteq L,\ J' \subseteq L' \text{ και } \theta|_{J'} = \varphi].$$

Για κάθε αλυσίδα $(J_\lambda, J'_\lambda, \varphi_\lambda)_{\lambda \in \Lambda}$ τού $(\mathfrak{N}, \preceq)$ η τριάδα $\left(\bigcup_{\lambda \in \Lambda} J_\lambda, \bigcup_{\lambda \in \Lambda} J'_\lambda, \Phi\right)$ με $\Phi|_{J'_\lambda} = \varphi_\lambda$ είναι ένα άνω φράγμα αυτής, οπότε το $(\mathfrak{N}, \preceq)$ είναι επαγωγικώς διατεταγμένο. Δυνάμει τού λήμματος τού Zorn το $(\mathfrak{N}, \preceq)$ διαθέτει κάποιο μεγιστικό στοιχείο $(J_\bullet, J'_\bullet, \varphi_\bullet)$.

Ισχυρισμός δεύτερος. $J_\bullet = \Lambda$.

Απόδειξη δεύτερου ισχυρισμού. Ας υποθέσουμε ότι $J_\bullet \subsetneqq \Lambda$, ας επιλέξουμε ένα $\lambda_\bullet \in \Lambda \smallsetminus J_\bullet$ και ας θέσουμε $L_\bullet := J_\bullet \cup \{\lambda_\bullet\}$. Εάν $U_{J_\bullet} = U_{L_\bullet}$, τότε ισχύει $(J_\bullet, J'_\bullet, \varphi_\bullet) \underset{\neq}{\preceq} (L_\bullet, J'_\bullet, \varphi_\bullet)$, κάτι που αντίκειται στη μεγιστικότητα τής τριάδας $(J_\bullet, J'_\bullet, \varphi_\bullet)$ εντός τής $\mathfrak{N}$. Άρα

$$U_{J_\bullet} \subsetneqq U_{L_\bullet} = (\mathrm{Lin}_R(\{x_{\lambda_\bullet}\}) + M_{J_\bullet}) \cap U$$

και το $Q := \{ r \in R |\, r x_{\lambda_\bullet} + v \in U, \text{ για } v \in M_{J_\bullet}\}$ είναι ένα ιδεώδες τού R. Επειδή $U_{J_\bullet} \subsetneqq U_{L_\bullet}$, έχουμε $Q \neq \{0_R\}$, οπότε $Q = Ra$ για κάποιο $a \in R \smallsetminus \{0_R\}$, καθώς ο R είναι Π.Κ.Ι. Κατά συνέπειαν, υπάρχει κάποιο $w \in M_{J_\bullet}$ με $z := a x_{\lambda_\bullet} + w \in U$. Θέτοντας $L'_\bullet := J'_\bullet \cup \{\lambda_\bullet\}$, ορίζοντας την απεικόνιση

$$\theta_\bullet : L'_\bullet \longrightarrow U_{L_\bullet},\ \ j \longmapsto \theta_\bullet(j) := \begin{cases} \varphi_\bullet(j), & \text{όταν } j \in J'_\bullet, \\ z, & \text{όταν } j = \lambda_\bullet, \end{cases}$$

και λαμβάνοντας υπ' όψιν ότι κάθε $x \in U_{L_\bullet}$ γράφεται ως $x = b x_{\lambda_\bullet} + v$ για κάποια $b \in R$ και $v \in M_{J_\bullet}$, παρατηρούμε ότι

$$b \in Q \Rightarrow [\exists c \in R : b = ac] \Rightarrow x = ac x_{\lambda_\bullet} + v = c(a x_{\lambda_\bullet}) + v = cz + (v - cw)$$

οπότε

$$\left.\begin{array}{r} x - cz = v - cw \in M_{J_\bullet} \cap U =: U_{J_\bullet} \\ \mathrm{Lin}_R(\{\varphi_\bullet(j) |\, j \in J'_\bullet\}) = U_{J_\bullet} \end{array}\right\} \Rightarrow x - cz = s_1 \varphi_\bullet(j_1) + \cdots + s_\kappa \varphi_\bullet(j_\kappa),$$

για κάποιους $s_1, ..., s_\kappa \in R$ και $\{j_1, ..., j_\kappa\} \subseteq J'_\bullet$. Επομένως,

$$x = c\theta_\bullet(\lambda_\bullet) + s_1 \theta_\bullet(j_1) + \cdots + s_\kappa \theta_\bullet(j_\kappa) \Rightarrow \mathrm{Lin}_R(\{\theta_\bullet(j) |\, j \in L'_\bullet\}) = U_{L_\bullet}. \tag{A.29}$$

Από την άλλη μεριά, από κάθε σχέση τής μορφής

$$s_0 \underbrace{\theta_\bullet(\lambda_\bullet)}_{=z} + s_1 \theta_\bullet(j_1) + \cdots + s_\nu \theta_\bullet(j_\nu) = 0_M \tag{A.30}$$

(για κάποιους $s_0, s_1, ..., s_\nu \in R$ και $\{\lambda_\bullet, j_1, ..., j_\nu\} \subseteq L'_\bullet$) προκύπτει ότι

$$a s_0 x_{\lambda_\bullet} = -(s_0 w + s_1 \theta_\bullet(j_1) + \cdots + s_\nu \theta_\bullet(j_\nu)) \Rightarrow a s_0 x_{\lambda_\bullet} \in M_{J_\bullet} \cap \mathrm{Lin}_R(\{x_{\lambda_\bullet}\}) = \{0_M\}.$$

Επειδή η οικογένεια στοιχείων $(x_\lambda)_{\lambda\in\Lambda}$ είναι βάση τού M, έχουμε

$$as_0x_{\lambda_\bullet} = 0_M \Rightarrow as_0 = 0_R \underset{a\neq 0_R}{\Longrightarrow} s_0 = 0_R,$$

οπότε

$$\left.\begin{array}{r} s_1\varphi_\bullet(j_1) + \cdots + s_\nu\varphi_\bullet(j_\nu) = 0_M \\ \text{και το } \{\,\varphi_\bullet(j)|\, j\in J'_\bullet\} \text{ είναι βάση τού } U_{J_\bullet} \end{array}\right\} \Rightarrow s_1 = \cdots = s_\nu = 0_R. \quad \text{(A.31)}$$

Από τις (A.29), (A.30) και (A.31) συνάγεται ότι το $\{\,\theta_\bullet(j)|\, j\in L'_\bullet\}$ αποτελεί μια βάση τού $U_{L_\bullet}$. Αυτό σημαίνει ότι $(J_\bullet, J'_\bullet, \varphi_\bullet) \underset{\neq}{\preceq} (L_\bullet, L'_\bullet, \theta_\bullet)$, κάτι που αντίκειται εκ νέου στη μεγιστικότητα τής τριάδας $(J_\bullet, J'_\bullet, \varphi_\bullet)$ εντός τής $\mathfrak{N}$. Άτοπο!

Αποπεράτωση αποδείξεως. Επειδή $J_\bullet = \Lambda$, έχουμε $M_{J_\bullet} = M$, $U_{J_\bullet} = U$ και το $\{\,\varphi_\bullet(j)|\, j\in J'\}$ αποτελεί μια βάση τού U. Άρα ο U είναι ελεύθερος R-μόδιος και $\mathrm{rank}_R(U) = \mathrm{card}(J') \leq \mathrm{card}(\Lambda) = \mathrm{rank}_R(M)$. □

A.6.48 Παράδειγμα. Το θεώρημα A.6.47 παύει να ισχύει όταν ο R δεν είναι Π.Κ.Ι. Εάν, π.χ., $R = \mathbb{Z}[\sqrt{-5}]$, τότε το ιδεώδες $I := \langle 2, 1+\sqrt{-5}\rangle$ (ως υπομόδιος τού R-μοδίου R) δεν είναι ελεύθερος R-μόδιος[44].

A.6.49 Πόρισμα. *Εάν M είναι ένας πεπερασμένως παραγόμενος R-μόδιος και ο R είναι Π.Κ.Ι., τότε και κάθε υπομόδιος U τού M είναι πεπερασμένως παραγόμενος.*

ΑΠΟΔΕΙΞΗ. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι $M \neq \{0_M\}$ και ότι $M = \mathrm{Lin}_R(x_1,...,x_k)$ με τα $x_1,...,x_k$ σαφώς διακεκριμένα και $\neq 0_M$. Εάν U είναι τυχών υπομόδιος τού M, θα δείξουμε ότι ο U διαθέτει ένα σύνολο γεννητόρων με πληθικό αριθμό $\leq k$. Επειδή $R^{(\{x_1,\ldots,x_k\})} \cong R^k$, υφίσταται ισομορφισμός $M \underset{f}{\xrightarrow{\cong}} R^k/W$, για κάποιον υπομόδιο W τού R^k. (Βλ. απόδειξη τού πορίσματος A.6.23.) Επομένως η εικόνα τού U μέσω αυτού τού ισομορφισμού οφείλει να είναι τής μορφής $f(U) = Z/W$, για κάποιον υπομόδιο Z τού R^k περιέχοντα τον W. (Βλ. θεώρημα A.4.4.) Όμως σύμφωνα με το θεώρημα A.6.47, ο Z (ως υπομόδιος τού *ελευθέρου* R-μοδίου R^k) είναι ελεύθερος και $l := \mathrm{rank}_R(Z) \leq \mathrm{rank}_R(R^k) = k$, οπότε $Z \cong R^l$. (Βλ. A.6.14 και A.6.39.) Εάν $\{\,b_j|\,1\leq j\leq l\}$ είναι μια βάση τού R^l, τότε είναι προφανές ότι $Z/W = \mathrm{Lin}_R(b_1+W,...,b_l+W)$ και ότι ο $U = f^{-1}(Z/W)$ παράγεται από l στοιχεία τού M. □

A.6.50 Παράδειγμα. Το πόρισμα A.6.49 παύει να ισχύει όταν ο R δεν είναι Π.Κ.Ι. Εάν, π.χ., $R = \mathbb{Z}[\mathsf{X}_1, \mathsf{X}_2,..., \mathsf{X}_{m-1}, \mathsf{X}_m,...]$ είναι ο πολυωνυμικός δακτύλιος

$$\mathbb{Z}[\mathsf{X}_1, \mathsf{X}_2,..., \mathsf{X}_{m-1}, \mathsf{X}_m,...] := \bigcup_{n\in\mathbb{N}} \mathbb{Z}[\mathsf{X}_1,..., \mathsf{X}_n],$$

[44] Τούτο έπεται από το ότι το εν λόγω ιδεώδες *δεν είναι κύριο*. (Βλ. A.6.15 (iv) και [87], εδ. 4.2.13.)

άπειρων (αριθμήσιμων, ανεξάρτητων) απροσδιορίστων (με ακεραίους συντελεστές) που προκύπτει ως ένωση των όρων τής ανιούσας ακολουθίας ακεραίων περιοχών

$$\mathbb{Z}[\mathsf{X}_1] \subsetneqq \mathbb{Z}[\mathsf{X}_1, \mathsf{X}_2] \subsetneqq \cdots \subsetneqq \mathbb{Z}[\mathsf{X}_1,\ldots,\mathsf{X}_{n-1}] \subsetneqq \mathbb{Z}[\mathsf{X}_1,\ldots,\mathsf{X}_n] \subsetneqq \cdots,$$

τότε το $\langle\{\,\mathsf{X}_n \mid n \in \mathbb{N}\}\rangle$ δεν είναι πεπερασμένως παραγόμενο ιδεώδες τού R. Ως εκ τούτου, το $\langle\{\,\mathsf{X}_n \mid n \in \mathbb{N}\}\rangle$ αποτελεί έναν μη πεπερασμένως παραγόμενο υπομόδιο τού R-μοδίου R.

A.6.51 Συμβολισμός. Εάν M είναι ένας πεπερασμένως παραγόμενος R-μόδιος, θέτουμε

$$\text{min-g}(M) := \min\{\, n \in \mathbb{N} \mid \exists \text{ σύστημα γεννητόρων } \mathcal{E} \text{ τού } M : \text{card}(\mathcal{E}) = n\}\,.$$

A.6.52 Πόρισμα. *Έστω ότι M, N είναι R-μόδιοι και $f : M \longrightarrow N$ ένας επιμορφισμός. Εάν ο R είναι Π.Κ.Ι. και ο M πεπερασμένως παραγόμενος, τότε τόσον ο N όσον και ο* $\text{Ker}(f)$ *είναι πεπερασμένως παραγόμενοι, και ισχύει*

$$\text{min-g}(N) \leq \text{min-g}(M) \leq \text{min-g}(N) + \text{min-g}(\text{Ker}(f)). \tag{A.32}$$

ΑΠΟΔΕΙΞΗ. Το ότι οι N και $\text{Ker}(f)$ είναι πεπερασμένως παραγόμενοι είναι γνωστό από τα πορίσματα A.3.8 και A.6.49, αντιστοίχως, ενώ οι (A.32) προκύπτουν άμεσα από την πρόταση A.3.7. □

A.7 ΠΕΠΕΡΑΣΜΕΝΩΣ ΠΑΡΑΓΟΜΕΝΟΙ ΜΟΔΙΟΙ ΟΡΙΣΜΕΝΟΙ ΥΠΕΡΑΝΩ Π.Κ.Ι.

Οι *πεπερασμένως παραγόμενοι* μόδιοι, οι οποίοι ορίζονται υπεράνω *περιοχών κυρίων ιδεωδών*, είναι ταξινομήσιμοι *μέχρις ισομορφισμού* με τη βοήθεια *διακριτών αναλλοιώτων*. (Συγκεκριμένα, με τη βοήθεια *τής ελεύθερης βαθμίδας τους, τής τάξεως τού υπομοδίου στρέψεώς τους και των εκθετών των στοιχειωδών διαιρετών τους*.) Το σχετικό *δομικό θεώρημα* (βλ. εδ. A.7.30) είναι λίαν σημαντικό, καθώς γενικεύει *το θεώρημα ταξινομήσεως των πεπερασμένως παραγομένων αβελιανών ομάδων* και υπεισέρχεται σε μια σειρά ενδιαφερουσών εφαρμογών σε πολλούς μαθηματικούς κλάδους, αλλά η απόδειξή του είναι κατά τι μακροσκελής, χωριζόμενη σε αρκετά βήματα.

A.7.1 Ορισμός. Έστω M ένας R-μόδιος, όπου R μια ακεραία περιοχή. Ένα στοιχείο $x \in M$ καλείται **στοιχείο στρέψεως** όταν υπάρχει κάποιο $r \in R \smallsetminus \{0_R\}$, τέτοιο ώστε να ισχύει $rx = 0_M$. Τα στοιχεία στρέψεως τού M συνιστούν έναν υπομόδιο[45]

[45] Εάν υποθέσουμε ότι $s_1, s_2 \in R$ και $x, y \in \text{tors}(M)$, τότε υπάρχουν στοιχεία $r_1, r_2 \in R \smallsetminus \{0_R\}$, τέτοια ώστε να ισχύει $r_1 x = 0_M = r_2 x$. Επειδή ο δοθείς δακτύλιος R είναι ακεραία περιοχή, έχουμε $r_1 r_2 \in R \smallsetminus \{0_R\}$ και $r_1 r_2(s_1 x + s_2 y) = 0_M \Rightarrow s_1 x + s_2 y \in \text{tors}(M)$ και το $\text{tors}(M)$ αποτελεί υπομόδιο τού M. (Βλ. πρόταση A.2.7.)

$\mathrm{tors}(M)$ τού M. Ο $\mathrm{tors}(M)$ καλείται[46] **υπομόδιος στρέψεως τού** M. Λέμε ότι ο M είναι R-**μόδιος στρέψεως** όταν $\mathrm{tors}(M) = M$. Κατ' αναλογίαν, λέμε ότι ο M είναι R-**μόδιος χωρίς στρέψη** (ή ότι ο M **δεν διαθέτει στρέψη** ή ότι **στερείται στρέψεως**) όταν $\mathrm{tors}(M) = \{0_M\}$.

Α.7.2 Παράδειγμα. Έστω $(G, +)$ μια μη τετριμμένη αβελιανή ομάδα (θεωρούμενη ως $\mathbb{Z}$-μόδιος, βλ. Α.2.4 (i)). Τα στοιχεία στρέψεως αυτής είναι ακριβώς εκείνα τα στοιχεία, η (ομαδοθεωρητική) τάξη των οποίων είναι *πεπερασμένη*.

Α.7.3 Λήμμα. *Εάν M είναι ένας R-μόδιος, όπου R ακεραία περιοχή, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) *Ο M δεν διαθέτει στρέψη.*

(ii) *Τα μονοσύνολα $\{x\}$ είναι γραμμικώς ανεξάρτητα για κάθε $x \in M \smallsetminus \{0_M\}$.*

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Εάν $\mathrm{tors}(M) = \{0_M\}$ και $x \in M \smallsetminus \{0_M\} = M \smallsetminus \mathrm{tors}(M)$, τότε για κάθε $r \in R$ με $rx = 0_M$ έχουμε $r = 0_R$ (διότι αλλιώς το x θα ήταν στοιχείο στρέψεως τού M), οπότε το μονοσύνολο $\{x\}$ είναι γραμμικώς ανεξάρτητο.

(ii)⇒(i) Εάν υπήρχε κάποιο $x \in \mathrm{tors}(M)$ με $x \neq 0_M$, τότε θα υπήρχε κάποιο $r \in R \smallsetminus \{0_R\}$, τέτοιο ώστε να ισχύει $rx = 0_M$, απ' όπου θα έπετο ότι το $\{x\}$ είναι γραμμικώς εξαρτημένο. □

Α.7.4 Πρόταση. *Εάν R είναι μια Π.Κ.Ι., τότε κάθε πεπερασμένως παραγόμενος R-μόδιος M χωρίς στρέψη είναι ελεύθερος.*

ΑΠΟΔΕΙΞΗ. Έστω $\{x_1, ..., x_k\}$ ένα σύστημα γεννητόρων ενός τέτοιου R-μοδίου M. Δίχως βλάβη τής γενικότητας μπορούμε να υποθέσουμε ότι[47] $x_j \neq 0_M$ για κάθε $j \in \{1, ..., k\}$. Επειδή ο M δεν διαθέτει στρέψη, κάθε μονοσύνολο $\{x_j\}$, $j \in \{1, ..., k\}$, είναι γραμμικώς ανεξάρτητο. (Βλ. λήμμα Α.7.3.) Από όλα τα γραμμικώς ανεξάρτητα υποσύνολα τού $\{x_1, ..., x_k\}$ επιλέγουμε ένα με το *μέγιστο δυνατό πλήθος στοιχείων*. Δίχως βλάβη τής γενικότητας (ενδεχομένως έπειτα από κάποια αναδιάταξη δεικτών) μπορούμε να υποθέσουμε ότι αυτό είναι το $\{x_1, ..., x_l\}$, όπου $l \in \{1, ..., k\}$. Εάν $l = k$, τότε το $\{x_1, ..., x_k\}$ είναι μια βάση τού M, οπότε ο M είναι ελεύθερος. Εάν $l \in \{1, ..., k-1\}$, τότε όλα τα σύνολα $\{x_1, ..., x_l\} \cup \{x_j\}$, $l < j \leq k$, είναι (εξ υποθέσεως) γραμμικώς εξαρτημένα. Κατά συνέπειαν,

$$\exists (r_{1,j}, ..., r_{l,j}) \in R^l \text{ και } \exists r_j \in R \smallsetminus \{0_R\} : r_j x_j = \sum_{i=1}^{l} r_{i,j} x_i, \ \forall j \in \{l+1, ..., k\}.$$

Θέτοντας[48] $r := r_{l+1} r_{l+2} \cdots r_k \in R \smallsetminus \{0_R\}$ λαμβάνουμε για κάθε $j \in \{l+1, ..., k\}$

$$r x_j \in R x_1 \oplus R x_2 \oplus \cdots \oplus R x_l =: N.$$

[46]Το σύμβολο $\mathrm{tors}(M)$ προκύπτει από τον όρο torsion (= στρέψη).

[47]Εάν κάποιο εξ αυτών είναι $= 0_M$, τότε μπορεί να παραλειφθεί. Εάν $k = 1$ και $x_1 = 0_M$, τότε ο M είναι τετριμμένος, οπότε ο ισχυρισμός είναι προδήλως αληθής.

[48]Το ότι $r \neq 0_R$ οφείλεται στο ότι ο δακτύλιος R είναι *ακεραία περιοχή*.

Προφανώς, $rx_j \in N$ *και* για κάθε $j \in \{1, ..., l\}$. Αυτό σημαίνει ότι

$$[rx \in N, \; \forall x \in M] \Rightarrow \{rx | \, x \in M\} =: rM \subseteq N.$$

Το rM είναι ελεύθερος R-μόδιος ως υπομόδιος τού ελευθέρου R-μοδίου N. (Βλ. θεώρημα A.6.47.) Επειδή ο M δεν διαθέτει στρέψη και $r \neq 0_R$, η απεικόνιση $M \ni x \mapsto rx \in rM$ είναι ισομορφισμός. Άρα ο $M \cong rM$ είναι (και σε αυτήν την περίπτωση) ελεύθερος R-μόδιος. □

A.7.5 Λήμμα. *Εάν M είναι ένας R-μόδιος, όπου R ακεραία περιοχή, τότε ο πηλικομόδιος $M/\mathrm{tors}(M)$ δεν διαθέτει στρέψη.*

ΑΠΟΔΕΙΞΗ. Θέτοντας $U := \mathrm{tors}(M)$ και υποθέτοντας ότι $x + U \in \mathrm{tors}(M/U)$, όπου $x \in M$, υπάρχει $r \in R \smallsetminus \{0_R\}$, τέτοιο ώστε να ισχύει

$$rx + U = r(x + U) = 0_{M/U} = U \Rightarrow rx \in U.$$

Κατά συνέπειαν, $\exists s \in R \smallsetminus \{0_R\} : s(rx) = (sr)x = 0_M$ με $sr \neq 0_R$ (διότι ο δακτύλιος R είναι ακεραία περιοχή). Αυτό σημαίνει ότι $x \in U$, απ' όπου έπεται ότι $x + U = U = 0_{M/U}$ και, κατ' επέκταση, ότι $\mathrm{tors}(M/U) = \{0_{M/U}\}$. □

A.7.6 Θεώρημα. *Εάν R είναι μια Π.Κ.Ι., τότε κάθε πεπερασμένως παραγόμενος R-μόδιος M γράφεται ως ευθύ άθροισμα*

$$\boxed{M = \mathrm{tors}\,(M) \oplus \mathrm{frp}(M),}$$

όπου[49] $\mathrm{frp}(M) \cong M/\mathrm{tors}(M)$ *είναι ένας ελεύθερος υπομόδιος τού M (το λεγόμενο **ελεύθερο μέρος** τού M).*

ΑΠΟΔΕΙΞΗ. Εάν $\{x_1, ..., x_k\}$ είναι ένα σύστημα γεννητόρων ενός τέτοιου R-μοδίου M, τότε το $\{x_1 + \mathrm{tors}(M), ..., x_k + \mathrm{tors}(M)\}$ αποτελεί ένα σύστημα γεννητόρων τού $M/\mathrm{tors}(M)$. Επομένως ο πηλικομόδιος $M/\mathrm{tors}(M)$ είναι πεπερασμένως παραγόμενος και ταυτοχρόνως (σύμφωνα με το λήμμα A.7.5) χωρίς στρέψη. Εξ αυτού προκύπτει ότι ο $M/\mathrm{tors}(M)$ είναι ελεύθερος. (Βλ. πρόταση A.7.4.) Από την άλλη μεριά, υπάρχει υπομόδιος $\mathrm{frp}(M)$ τού M, τέτοιος ώστε $M = \mathrm{tors}(M) \oplus \mathrm{frp}(M)$. (Βλ. θεώρημα A.6.46.) Ο $\mathrm{frp}(M)$ είναι ελεύθερος R-μόδιος δυνάμει τού θεωρήματος A.6.47. Τέλος, ο ισομορφισμός $\mathrm{frp}(M) \cong M/\mathrm{tors}(M)$ προκύπτει από την πρόταση A.5.20. □

A.7.7 Ορισμός. Εάν R είναι μια Π.Κ.Ι. και M ένας πεπερασμένως παραγόμενος R-μόδιος, τότε ορίζουμε ως **ελεύθερη βαθμίδα** τού M

$$\boxed{\text{fr-rank}_R(M) := \mathrm{rank}_R(\mathrm{frp}\,(M))} \tag{A.33}$$

τη βαθμίδα τού ελεύθερου μέρους του.

[49] Επελέχθη το σύμβολο "$\mathrm{frp}(M)$" για να θυμίζει το free part of M.

Α.7.8 Λήμμα. *Εάν $f : M \longrightarrow N$ είναι ένας ομομορφισμός R-μοδίων, τότε ισχύει ο εγκλεισμός $f(\text{tors}(M)) \subseteq \text{tors}(N)$ και, ως εκ τούτου, ορίζεται καλώς ο «κανονιστικός» ομομορφισμός*

$$f^{\pi\eta\lambda.} : M/\text{tors}(M) \longrightarrow N/\text{tors}(N)$$
$$x + \text{tors}(M) \longmapsto f^{\pi\eta\lambda.}(x + \text{tors}(M)) := f(x) + \text{tors}(N),$$

ο οποίος καθιστά το διάγραμμα

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\pi^{M}_{\text{tors}(M)}"'] \arrow[dr, phantom, "\circlearrowleft"] & N \arrow[d, "\pi^{N}_{\text{tors}(N)}"] \\ M/\text{tors}(M) \arrow[r, dashed, "f^{\pi\eta\lambda.}"'] & N/\text{tors}(N) \end{tikzcd}$$

μεταθετικό. Επιπροσθέτως, ισχύουν τα ακόλουθα:

(a) *Ο $f^{\pi\eta\lambda.}$ είναι μονομορφισμός* $\Longleftrightarrow \text{tors}(M) = f^{-1}(\text{tors}(N))$.

(b) *Ο $f^{\pi\eta\lambda.}$ είναι επιμορφισμός* $\Longleftrightarrow \text{Im}(f) + \text{tors}(N) = N$.

Αποδειξη. Εάν $x \in M$ με $rx = 0_M$ για κάποιο $r \in R \smallsetminus \{0_R\}$, τότε έχουμε

$$rf(x) = f(rx) = f(0_M) = 0_N \Rightarrow f(x) \in \text{tors}(N).$$

Επομένως, $f(\text{tors}(M)) \subseteq \text{tors}(N)$. Οι λοιποί ισχυρισμοί (λαμβανομένης υπ' όψιν τής σημειώσεως Α.4.11) είναι αληθείς δυνάμει τού θεωρήματος Α.4.10. □

Α.7.9 Θεώρημα. *Εάν R είναι μια Π.Κ.Ι. και M, N πεπερασμένως παραγόμενοι R-μόδιοι, τότε οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) $M \cong N$.

(ii) $\text{tors}(M) \cong \text{tors}(N)$ *και* $\text{frp}(M) \cong \text{frp}(N)$.

Αποδειξη. (i)$\Rightarrow$(ii) Έστω $f : M \xrightarrow{\cong} N$ ένας ισομορφισμός. Εφαρμόζοντας το λήμμα Α.7.8 τόσον για τον f όσον και για τον f^{-1} λαμβάνουμε

$$\left.\begin{array}{l} f(\text{tors}(M)) \subseteq \text{tors}(N) \\ f^{-1}(\text{tors}(N)) \subseteq \text{tors}(M) \end{array}\right\} \Rightarrow f(\text{tors}(M)) = \text{tors}(N), \tag{A.34}$$

οπότε η $f|_{\text{tors}(M)} : \text{tors}(M) \longrightarrow \text{tors}(N)$ είναι ισομορφισμός με τον $f^{-1}|_{\text{tors}(N)}$ ως αντίστροφό του. Επίσης, λόγω τής ισότητας (Α.34) πληρούται η συνθήκη (a) τού λήμματος Α.7.8 για τον $f^{\pi\eta\lambda.}$. Επειδή δε $\text{Im}(f) = N$, πληρούται *και* η συνθήκη (b) τού λήμματος Α.7.8 για τον $f^{\pi\eta\lambda.}$. Άρα ο $f^{\pi\eta\lambda.}$ είναι ισομορφισμός και ο ισχυρισμός είναι αληθής, διότι (βάσει των αποδειχθέντων στο θεώρημα Α.7.6)

$$\text{frp}(M) \cong M/\text{tors}\,(M) \;\; \text{και} \;\; \text{frp}(N) \cong N/\text{tors}\,(N)\,.$$

(ii)⇒(i) Κατά το θεώρημα A.7.6,

$$M \cong \text{tors}\,(M) \oplus \text{frp}\,(M) \quad \text{και} \quad N \cong \text{tors}\,(N) \oplus \text{frp}\,(N)\,.$$

Εάν $f_1 : \text{tors}(M) \xrightarrow{\cong} \text{tors}(N)$ και $f_2 : \text{frp}(M) \xrightarrow{\cong} \text{frp}(N)$ είναι ισομορφισμοί, τότε ο $f_1 \oplus f_2 : M \longrightarrow N$ είναι ωσαύτως ισομορφισμός. □

► **Μόδιοι στρέψεως υπεράνω Π.Κ.Ι.** Επειδή (κατά την πρόταση A.6.41 και τον ορισμό (A.33)) ισχύει

$$\text{frp}\,(M) \cong \text{frp}\,(N) \Leftrightarrow \text{fr-rank}_R(M) = \text{fr-rank}_R(N), \tag{A.35}$$

για να καταλήξουμε σε ένα όμορφο θεώρημα ταξινομήσεως των πεπερασμένως παραγομένων μοδίων υπεράνω Π.Κ.Ι. *μέχρις ισομορφισμού* αρκεί να εστιάσουμε την προσοχή μας στο πότε δυο πεπερασμένως παραγόμενοι μόδιοι *στρέψεως* (υπεράνω Π.Κ.Ι.) είναι ισόμορφοι.

A.7.10 Ορισμός. Έστω M ένας R-μόδιος και έστω $x \in M$. Το σύνολο

$$\boxed{\text{Ann}_R(x) := \{r \in R \,|\, rx = 0_M\,\}}$$

ονομάζεται **μηδενιστής τού στοιχείου** x. Σημειωτέον ότι

$$\text{tors}\,(M) = \{x \in M \,|\, \text{Ann}_R(x) \neq \{0_R\}\,\}\,.$$

Εάν U είναι ένας υπομόδιος τού M, τότε το σύνολο

$$\boxed{\text{Ann}_R(U) := \{r \in R \,|\, ru = 0_M,\ \forall u \in U\,\}}$$

ονομάζεται **μηδενιστής τού υπομοδίου** U.

A.7.11 Πρόταση. *Έστω M ένας R-μόδιος και έστω $x \in M$. Τότε ισχύουν τα εξής:*
(i) *Το* $\text{Ann}_R(x)$ *είναι ένα ιδεώδες τού R (και κατ' επέκταση υπομόδιος τού R-μοδίου R) και υφίσταται ένας ισομορφισμός R-μοδίων:*

$$R/\text{Ann}_R(x) \cong Rx. \tag{A.36}$$

(ii) *Εάν U είναι ένας υπομόδιος τού M, τότε το* $\text{Ann}_R(U)$ *είναι ένα ιδεώδες τού R (και κατ' επέκταση υπομόδιος τού R-μοδίου R).*
(iii) *Εάν ο M είναι πεπερασμένως παραγόμενος και $\{x_1, ..., x_k\}$ τυχόν σύστημα γεννητόρων αυτού, τότε*

$$\text{Ann}_R(M) = \bigcap_{j=1}^{k} \text{Ann}_R(x_j).$$

ΑΠΟΔΕΙΞΗ. (i) Εάν $a_1, a_2, a \in \mathrm{Ann}_R(x)$ και $r \in R$, τότε

$$(a_1 - a_2)x = a_1x - a_2x = 0_M - 0_M = 0_M \Rightarrow a_1 - a_2 \in \mathrm{Ann}_R(x),$$
$$(ra)x = r(ax) = r0_M = 0_M \Rightarrow ra \in \mathrm{Ann}_R(x).$$

Επιπροσθέτως, ο επιμορφισμός R-μοδίων $R \ni r \longmapsto rx \in Rx$ έχει ως πυρήνα του τον μηδενιστή τού x, οπότε ο (Α.36) προκύπτει από το 1ο θεώρημα ισομορφισμών Α.4.7.

(ii) Εάν $a_1, a_2, a \in \mathrm{Ann}_R(U)$ και $r \in R$, τότε για κάθε $u \in U$ έχουμε

$$(a_1 - a_2)u = a_1u - a_2u = 0_M - 0_M = 0_M \Rightarrow a_1 - a_2 \in \mathrm{Ann}_R(U),$$
$$(ra)u = r(au) = r0_M = 0_M \Rightarrow ra \in \mathrm{Ann}_R(U).$$

(iii) Εξ ορισμού, $\mathrm{Ann}_R(M) \subseteq \mathrm{Ann}_R(x_j)$ για κάθε $j \in \{1, ..., k\}$, απ' όπου έπεται ότι $\mathrm{Ann}_R(M) \subseteq \bigcap_{j=1}^{k} \mathrm{Ann}_R(x_j)$. Και αντιστρόφως· εάν $r \in \bigcap_{j=1}^{k} \mathrm{Ann}_R(x_j)$ και $x \in M$, τότε υπάρχουν $r_1, ..., r_k \in R$, τέτοια ώστε

$$x = \sum_{j=1}^{k} r_j x_j \Rightarrow rx = r\left(\sum_{j=1}^{k} r_j x_j\right) = \sum_{j=1}^{k} r_j(rx_j) = \sum_{j=1}^{k} r_j 0_M = 0_M,$$

απ' όπου έπεται ότι $x \in \mathrm{Ann}_R(M)$, οπότε $\bigcap_{j=1}^{k} \mathrm{Ann}_R(x_j) \subseteq \mathrm{Ann}_R(M)$. □

Α.7.12 Ορισμός. Έστω R μια Π.Κ.Ι. και έστω M ένας R-μόδιος.

(i) Για κάθε $s \in R$ ορίζουμε τον υπομόδιο τού M

$$\boxed{M[s] := \{x \in M \,|\, sx = 0_M\}}$$

τον απαρτιζόμενο από εκείνα τα στοιχεία τού M τα οποία μηδενίζονται πολλαπλασιαζόμενα με το s. Εάν $s, s' \in R$ και $s \mid s'$, τότε είναι πρόδηλο ότι $M[s] \subseteq M[s']$. Ιδιαιτέρως, για κάθε $s \in R$ και κάθε $n \in \mathbb{N}$ έχουμε

$$M[s] \subseteq M[s^2] \subseteq M[s^3] \subseteq \cdots \subseteq M[s^n] \subseteq M[s^{n+1}] \subseteq \cdots \tag{A.37}$$

(ii) Εάν $s \in R$, τότε λόγω τής (Α.37) ορίζεται ο υπομόδιος

$$\boxed{M(s) := \bigcup_{n \in \mathbb{N}} M[s^n] = \{x \in M \,|\, s^n x = 0_M \text{ για κάποιον } n \in \mathbb{N}\}}$$

τού M που καλείται s-**συνιστώσα τού** M.

(iii) Εάν το p είναι ένα πρώτο στοιχείο τής R (βλ. ??), τότε ο $M(p)$ ονομάζεται p-**πρωτεύουσα συνιστώσα τού** M.

(iv) Εάν το p είναι ένα πρώτο στοιχείο τής R, τότε ο M καλείται p-**πρωτεύων** (ή p-**περιοδικός**) όταν $M = M(p)$, ήτοι όταν ισούται με την p-πρωτεύουσα συνιστώσα του.

A.7.13 Παρατήρηση. $U(s) = M(s) \cap U$, $\forall s \in R$, για κάθε υπομόδιο U τού M.

A.7.14 Πρόταση. *Εάν R είναι μια Π.Κ.Ι. και M ένας R-μόδιος, τότε*

$$\operatorname{tors}(M) = \{0_M\} \Longleftrightarrow (M[s] = \{0_M\},\ \forall s \in R\smallsetminus\{0_R\}).$$

ΑΠΟΔΕΙΞΗ. "$\Rightarrow$" Έστω ότι υπάρχει $s \in R\smallsetminus\{0_R\}$ με $M[s] \neq \{0_M\}$. Τότε υπάρχει κάποιο $x \in M[s]\smallsetminus\{0_M\}$. Γι' αυτό το στοιχείο ισχύει η ισότητα $sx = 0_M$, οπότε έχουμε $x \in \operatorname{tors}(M)\smallsetminus\{0_M\}$, απ' όπου έπεται ότι $\operatorname{tors}(M) \neq \{0_M\}$.

"$\Leftarrow$" Έστω ότι $\operatorname{tors}(M) \neq \{0_M\}$. Τότε υπάρχει $x \in \operatorname{tors}(M)\smallsetminus\{0_M\}$, οπότε υπάρχει κάποιο στοιχείο $s \in R\smallsetminus\{0_R\}$ με $sx = 0_M$. Εξ αυτού έπεται ότι $x \in M[s]\smallsetminus\{0_M\}$, ήτοι ότι $M[s] \neq \{0_M\}$. □

A.7.15 Πρόταση. *Εάν R είναι μια Π.Κ.Ι., $k \in \mathbb{N}$, $k \geq 2$, τα $a_1, a_2, ..., a_k \in R$ ανά δύο "σχετικώς πρώτα" (δηλαδή $1_R \in \mathrm{MK\Delta}_R(a_i, a_j)$ για $i, j \in \{1, ..., k\}$ με $i \neq j$) και M ένας R-μόδιος, τότε*

$$M\left[a_1 a_2 \cdots a_k\right] = \bigoplus_{j=1}^{k} M[a_j].$$

ΑΠΟΔΕΙΞΗ. Χρησιμοποιούμε μαθηματική επαγωγή ως προς τον k. Εάν $k = 2$, τότε $\exists (b_1, b_2) \in R \times R : 1_R = a_1 b_1 + a_2 b_2$, οπότε για κάθε $x \in M\left[a_1 a_2\right]$ έχουμε

$$x = a_1 b_1 x + a_2 b_2 x = a_2 b_2 x + a_1 b_1 x,$$

απ' όπου έπεται ότι $a_1 b_1 x \in M\left[a_2\right]$ (διότι $a_2(a_1 b_1 x) = b_1(a_1 a_2 x) = b_1 0_M = 0_M$) και (κατ' αναλογίαν) $a_2 b_2 x \in M\left[a_1\right]$. Κατά συνέπειαν,

$$\left.\begin{array}{c} M\left[a_1 a_2\right] \subseteq M\left[a_1\right] + M\left[a_2\right] \\ M\left[a_1\right] \subseteq M\left[a_1 a_2\right],\ M\left[a_2\right] \subseteq M\left[a_1 a_2\right] \end{array}\right\} \Rightarrow M\left[a_1 a_2\right] = M\left[a_1\right] + M\left[a_2\right].$$

Από την άλλη μεριά, για κάθε $y \in M\left[a_1\right] \cap M\left[a_2\right]$ έχουμε

$$y = a_1 b_1 y + a_2 b_2 y = b_1(a_1 y) + b_2(a_2 y) = b_1 0_M + b_2 0_M = 0_M,$$

οπότε

$$\left.\begin{array}{r} M\left[a_1 a_2\right] = M\left[a_1\right] + M\left[a_2\right] \\ M\left[a_1\right] \cap M\left[a_2\right] = \{0_M\} \end{array}\right\} \underset{\text{A.5.17}}{\Longrightarrow} M\left[a_1 a_2\right] = M\left[a_1\right] \oplus M\left[a_2\right].$$

Εάν υποθέσουμε ότι $k \geq 3$ και ότι ο ισχυρισμός είναι αληθής για *οιαδήποτε* $k-1$ ανά δύο σχετικώς πρώτα στοιχεία τής R, τότε

$$M = M\left[a_1 a_2 \cdots a_{k-1}\right] \oplus M\left[a_k\right] = (\bigoplus_{j=1}^{k-1} M[a_j]) \oplus M\left[a_k\right] = \bigoplus_{j=1}^{k} M[a_j],$$

λόγω τής επαγωγικής υποθέσεώς μας (διότι τα $a_1 \cdots a_{k-1}$ και a_k είναι σχετικώς πρώτα). □

Α.7.16 Πόρισμα. *Εάν R είναι μια Π.Κ.Ι., $r \in R$ και $r \underset{\text{συν.}}{\sim} p_1^{\nu_1} p_2^{\nu_2} ... p_t^{\nu_t}$ είναι η παράσταση τού r ως γινομένου (κατάλληλων θετικών ακεραίων δυνάμεων) πρώτων στοιχείων $p_1, p_2, ..., p_t$ τής R (που είναι ανά δύο μη συντροφικά όταν $t \geq 2$), τότε για κάθε $j \in \{1, ..., t\}$ ισχύει η ισότητα*

$$M[r](p_j) = M[p_j^{\nu_j}] \; (:= \left\{ x \in M \left| p_j^{\nu_j} x = 0_M \right. \right\}).$$

ΑΠΟΔΕΙΞΗ. *Περίπτωση πρώτη.* Εάν $t = 1$, τότε[50] $M[r] = M[p_1^{\nu_1}]$ και

$$M[r](p_1) = M[r] \cap M(p_1) = M[p_1^{\nu_1}] \cap M(p_1) = M[p_1^{\nu_1}],$$

διότι είναι προφανές ότι $M[p_1^{\nu_1}] \subseteq M(p_1)$.

Περίπτωση δεύτερη. Εάν $t \geq 2$, τότε για κάθε $j \in \{1, ..., t\}$ τα $p_j^{\nu_j}$ και $\prod\limits_{i \in \{1,...,t\} \smallsetminus \{j\}} p_i^{\nu_i}$ είναι σχετικώς πρώτα, οπότε η πρόταση Α.7.15 μας πληροφορεί ότι

$$M[r] = M[p_j^{\nu_j}] \oplus M[\textstyle\prod_{i \in \{1,...,t\} \smallsetminus \{j\}} p_i^{\nu_i}].$$

Επειδή $M[p_j^{\nu_j}] \subseteq M(p_j), \forall j \in \{1, ..., t\}$, έχουμε

$$\begin{aligned} M[r](p_j) &= M[r] \cap M(p_j) \\ &= \left(M[p_j^{\nu_j}] \oplus M[\textstyle\prod_{i \in \{1,...,t\} \smallsetminus \{j\}} p_i^{\nu_i}] \right) \cap M(p_j) \\ &\underset{\text{Α.2.20}}{=} \left(M(p_j) \cap M[\textstyle\prod_{i \in \{1,...,t\} \smallsetminus \{j\}} p_i^{\nu_i}] \right) + M[p_j^{\nu_j}]. \end{aligned}$$

Αρκεί λοιπόν να αποδειχθεί ότι

$$M(p_j) \cap M[\textstyle\prod_{i \in \{1,...,t\} \smallsetminus \{j\}} p_i^{\nu_i}] = \{0_M\}. \tag{Α.38}$$

Επειδή *για κάθε* $n \in \mathbb{N}$ ισχύει[51]

$$\begin{aligned} & 1_R \in \text{ΜΚΔ}_R(p_j, \prod_{i \in \{1,...,t\} \smallsetminus \{j\}} p_i^{\nu_i}) \Longrightarrow 1_R \in \text{ΜΚΔ}_R(p_j^n, \prod_{i \in \{1,...,t\} \smallsetminus \{j\}} p_i^{\nu_i}) \\ & \Longrightarrow \exists (a, b) \in R \times R : 1_R = a p_j^n + b \left(\textstyle\prod_{i \in \{1,...,t\} \smallsetminus \{j\}} p_i^{\nu_i} \right), \end{aligned}$$

υπάρχει *για κάθε* $y \in M(p_j) \cap M[\prod_{i \in \{1,...,t\} \smallsetminus \{j\}} p_i^{\nu_i}]$ *αρκούντως μεγάλος* $n_\bullet \in \mathbb{N}$ με

$$y = a \left(p_j^{n_\bullet} y \right) + b \left(\textstyle\prod_{i \in \{1,...,t\} \smallsetminus \{j\}} p_i^{\nu_i} \right) y = a 0_M + b 0_M = 0_M,$$

οπότε η ισότητα (Α.38) είναι όντως αληθής. □

---

[50] Προφανώς, $p_1^{\nu_1} \mid r \Rightarrow M[p_1^{\nu_1}] \subseteq M[r]$. Και αντιστρόφως· επειδή $r = u p_1^{\nu_1}$ για κάποιο $u \in R^\times$, εάν $x \in M[r]$, τότε από την $\left(u p_1^{\nu_1} \right) x = 0_M$ έπεται ότι $p_1^{\nu_1} x = 0_M$, ήτοι ότι $x \in M[p_1^{\nu_1}]$.

[51] Πρβλ. [87], πόρισμα 5.2.17.

Α.7.17 Θεώρημα. («Θεώρημα πρωτεύουσας αποσυνθέσεως») *Έστω R μια Π.Κ.Ι. και έστω M ένας μη τετριμμένος πεπερασμένως παραγόμενος R-μόδιος στρέψεως. Τότε ισχύουν τα εξής:*

(i) *Ο μηδενιστής τού M είναι ένα μη τετριμμένο, γνήσιο και κύριο ιδεώδες $\mathrm{Ann}_R(M) = \langle r \rangle$ τής R, όπου το $r \in R \smallsetminus (R^\times \cup \{0_R\})$ (για τον δοθέντα M) είναι μονοσημάντως ορισμένο μέχρις συντροφικότητας.*

(ii) *Εάν $r \underset{\text{συν.}}{\sim} p_1^{\nu_1} p_2^{\nu_2} ... p_t^{\nu_t}$ είναι η παράσταση τού r ως γινομένου (κατάλληλων θετικών ακεραίων δυνάμεων) πρώτων στοιχείων $p_1, p_2, ..., p_t$ τής R (που είναι ανά δύο μη συντροφικά όταν $t \geq 2$), τότε $M(p_j) \neq \{0_M\}$ για κάθε $j \in \{1, ..., t\}$ και*

$$\boxed{M = M(p_1) \oplus M(p_2) \oplus \cdots \oplus M(p_t),} \tag{A.39}$$

όπου η εν λόγω αποσύνθεση τού M στα ευθέα αθροίσματα των πρωτευουσών συνιστωσών του είναι μοναδική.

ΑΠΟΔΕΙΞΗ. (i) Θεωρούμε τον μηδενιστή $\mathrm{Ann}_R(M)$ τού M. Σύμφωνα με το (ii) τής προτάσεως Α.7.11 ο $\mathrm{Ann}_R(M)$ αποτελεί ένα *ιδεώδες* τής R. Το ιδεώδες αυτό είναι αφ' ενός μεν *γνήσιο*, διότι ο M είναι μη τετριμμένος, αφ' ετέρου δε *μη τετριμμένο*, διότι εάν $\{x_1, ..., x_n\}$ είναι τυχόν σύστημα γεννητόρων τού M, υπάρχει $r_j \in R \smallsetminus \{0_R\}$ με $r_j x_j = 0_M$ για κάθε $j \in \{1, ..., n\}$, οπότε

$$0_R \neq \prod_{j=1}^{n} r_j \in \mathrm{Ann}_R(M).$$

Έστω τώρα $\{x_1, ..., x_k\}$ ένα σύστημα γεννητόρων τού M με το *ελάχιστο δυνατό πλήθος στοιχείων*[52]. Επειδή ο M είναι R-μόδιος στρέψεως, υπάρχει $r_j \in R \smallsetminus \{0_R\}$ με $r_j x_j = 0_M$ για κάθε $j \in \{1, ..., k\}$, οπότε

$$[\mathrm{Ann}_R(x_j) \neq \{0_R\},\ \forall j \in \{1, ..., k\}] \text{ και } \mathrm{Ann}_R(M) = \bigcap_{j=1}^{k} \mathrm{Ann}_R(x_j).$$

(Βλ. Α.7.11 (iii).) Επειδή ο δακτύλιος αναφοράς R είναι εξ υποθέσεως Π.Κ.Ι., υπάρχει ένα (μέχρις συντροφικότητας μονοσημάντως ορισμένο[53]) $s_j \in R \smallsetminus \{0_R\}$ με $\mathrm{Ann}_R(x_j) = \langle s_j \rangle$ για κάθε $j \in \{1, ..., k\}$. Κατά συνέπειαν,

$$\mathrm{Ann}_R(M) = \bigcap_{j=1}^{k} \mathrm{Ann}_R(x_j) = \bigcap_{j=1}^{k} \langle s_j \rangle = \langle r \rangle$$

για κάποιο[54] $r \in \text{ΕΚΠ}_R(s_1, ..., s_k)$. Το[55] $r \in R \smallsetminus (R^\times \cup \{0_R\})$ είναι ωσαύτως μονοσημάντως ορισμένο μέχρις συντροφικότητας.

[52] Αυτό σημαίνει, ιδιαιτέρως, ότι $x_j \neq 0_M$ για κάθε $j \in \{1, ..., k\}$.

[53] Βλ. [87], πρόταση 5.2.4 (ii).

[54] Βλ. [87], θεώρημα 5.2.24.

[55] Για το ότι $r \neq 0_R$, βλ. [87], πόρισμα 5.2.26. Επίσης, το ότι $r \notin R^\times$ είναι άμεσο επακολούθημα τού γνησίου εγκλεισμού $\mathrm{Ann}_R(M) \subsetneqq R$.

(ii) Επειδή (βάσει των προαναφερθέντων στο (i)) $M = M[r]$, έχουμε (δυνάμει τής προτάσεως Α.7.15 και τού πορίσματος Α.7.16)

$$M = M[r] = M[p_1^{\nu_1} p_2^{\nu_2} ... p_t^{\nu_t}] = \bigoplus_{j=1}^{t} M[p_j^{\nu_j}] = \bigoplus_{j=1}^{t} M(p_j).$$

Εάν $t = 1$, τότε $M(p_1) = M \neq \{0_M\}$. Έστω ότι $t \geq 2$. Εάν υπήρχε κάποιος δείκτης $j_\bullet \in \{1, ..., t\}$ με $M(p_{j_\bullet}) = \{0_M\}$, τότε θα είχαμε

$$M = \bigoplus_{i \in \{1,...,t\} \smallsetminus \{j_\bullet\}} M(p_i) = \bigoplus_{i \in \{1,...,t\} \smallsetminus \{j_\bullet\}} M[p_i^{\nu_i}] = M[\textstyle\prod_{i \in \{1,...,t\} \smallsetminus \{j_\bullet\}} p_i^{\nu_i}],$$

απ' όπου θα έπετο ότι

$$\prod_{i \in \{1,...,t\} \smallsetminus \{j_\bullet\}} p_i^{\nu_i} \in \mathrm{Ann}_R(M) = \langle r \rangle \Rightarrow r \mid \prod_{i \in \{1,...,t\} \smallsetminus \{j_\bullet\}} p_i^{\nu_i}$$

και, κατ' επέκταση, ότι $p_{j_\bullet} \mid \prod_{i \in \{1,...,t\} \smallsetminus \{j_\bullet\}} p_i^{\nu_i}$ (αφού $p_{j_\bullet} \mid r$). Άτοπο! Άρα $M(p_j) \neq \{0_M\}$ για κάθε $j \in \{1, ..., t\}$. Τέλος, σε ό,τι αφορά στη *μοναδικότητα* τής ανωτέρω αποσυνθέσεως, θεωρούμε *τυχόν* πρώτο στοιχείο q τής R με $M(q) \neq \{0_M\}$ καθώς και *τυχόν* $x \in M(q) \smallsetminus \{0_M\}$. Επειδή ο δακτύλιος αναφοράς R είναι εξ υποθέσεως Π.Κ.Ι., υπάρχει ένα[56] (μέχρις συντροφικότητας μονοσημάντως ορισμένο[57]) $d \in R \smallsetminus (R^\times \cup \{0_R\})$ με $\mathrm{Ann}_R(x) = \langle d \rangle$. Το ιδεώδες $\langle d \rangle$ περιέχει τόσον το r όσον και το q^n για κάποιον κατάλληλο $n \in \mathbb{N}$. Επειδή $d \mid q^n$, υπάρχει $m \in \mathbb{N}$, $1 \leq m \leq n$, τέτοιο ώστε να ισχύει $d = q^m$. Επιπροσθέτως, επειδή το q είναι πρώτο στοιχείο τής R, έχουμε $q^m = d \mid r \Rightarrow q \mid r$ και $q \underset{\text{συν.}}{\sim} p_j$ για κάποιο $j \in \{1, ..., t\}$. Εξ αυτού συνάγεται ότι $M(q) = M(p_j)$. □

Α.7.18 Ορισμός. Έστω R μια Π.Κ.Ι. και έστω M ένας μη τετριμμένος πεπερασμένως παραγόμενος R-μόδιος στρέψεως.

(i) Έστω $r \in R \smallsetminus (R^\times \cup \{0_R\})$ το μέχρις συντροφικότητας μονοσημάντως ορισμένο για το οποίο (σύμφωνα με το (i) τού θεωρήματος Α.7.17) ισχύει $\mathrm{Ann}_R(M) = \langle r \rangle$. Η κλάση ισοδυναμίας τού r ως προς την "$\underset{\text{συν.}}{\sim}$" καλείται **τάξη**[58] **τού** M και συμβολίζεται ως $\mathrm{ord}(M)$. Είθισται να γράφουμε (για λόγους συντομίας) $\mathrm{ord}(M) = r$ (υπονοώντας, ωστόσο, ότι "$r \in \mathrm{ord}(M)$").

(ii) Έστω $x \in M \smallsetminus \{0_M\}$ και έστω $s \in R \smallsetminus \{0_R\}$ το μέχρις συντροφικότητας μονοσημάντως ορισμένο στοιχείο, για το οποίο ισχύει $\mathrm{Ann}_R(x) = \langle s \rangle$. Η κλάση ισοδυναμίας τού s ως προς την "$\underset{\text{συν.}}{\sim}$" καλείται **τάξη τού** x και συμβολίζεται ως $\mathrm{ord}(x)$. Είθισται (και σε αυτήν την περίπτωση, για λόγους συντομίας) να γράφουμε απλώς $\mathrm{ord}(x) = s$. Εξ ορισμού, $\mathrm{Ann}_R(M) \subseteq \mathrm{Ann}_R(x)$, οπότε

$$\langle r \rangle \subseteq \langle s \rangle \Rightarrow s \mid r. \tag{Α.40}$$

[56]Εάν ίσχυε $d \in R^\times$, τότε θα είχαμε (λόγω τού (Α.36)) $\mathrm{Ann}_R(x) = R \Rightarrow x = 0_M$ (ήτοι κάτι εξ υποθέσεως αποκλεισθέν).

[57]Βλ. [87], πρόταση 5.2.4 (ii).

[58]Ορισμένοι συγγραφείς αντί τού όρου *τάξη* χρησιμοποιούν τον όρο *εκθέτης* (τού M). Πρβλ. Α.7.19 (i).

Α.7.19 Παραδείγματα. (i) Έστω $(G,+)$ μια μη τετριμμένη αβελιανή ομάδα (θεωρούμενη ως $\mathbb{Z}$-μόδιος, βλ. Α.2.4 (i)). Είναι γνωστό (από τη Θεωρία Ομάδων) ότι η G είναι πεπερασμένως παραγόμενη ομάδα στρέψεως εάν και μόνον εάν είναι *πεπερασμένη ομάδα*. Υποθέτοντας, λοιπόν, ότι $|G| < \infty$ και θεωρώντας ένα στοιχείο $x \in G \smallsetminus \{0_G\}$ παρατηρούμε ότι ο μηδενιστής αυτού $\mathrm{Ann}_{\mathbb{Z}}(x)$, όντας ένα (κατ' ανάγκην κύριο) ιδεώδες τής Π.Κ.Ι. $\mathbb{Z}$, οφείλει να ισούται με $\langle n \rangle = n\mathbb{Z}$ για κάποιον $n \in \mathbb{Z} \smallsetminus \{0\}$. Επειδή $\langle n \rangle = \langle -n \rangle$, ο θετικός ακέραιος $|n| = \min\{ l \in \mathbb{N} |\, l \in n\mathbb{Z}\}$ είναι ο *μοναδικός θετικός γεννήτορας* τού ιδεώδους $n\mathbb{Z}$. (Σημειωτέον ότι $\mathbb{Z}^{\times} = \{\pm 1\}$, οπότε οι n και $-n$ είναι οι μοναδικοί γεννήτορες τού $n\mathbb{Z}$.) Εν προκειμένω, ο (Α.36) δίδει

$$\mathbb{Z}x \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\,|n|\,\mathbb{Z} \cong \mathbb{Z}_{|n|}.$$

Ως εκ τούτου, ο $|n| = |\mathbb{Z}x|$ ισούται με την *ομαδοθεωρητική τάξη* τού στοιχείου x (και μπορεί να εκληφθεί ως *ο πλέον βολικός εκπρόσωπος* τής $\mathrm{ord}(x)$, όπως αυτή ορίζεται στο γενικότερο πλαίσιο τού εδ. Α.7.18 (ii)). Επιπροσθέτως, ο *ομαδοθεωρητικός εκθέτης*[59] $\exp(G)$*τής ίδιας τής* G ισούται με το ελάχιστο κοινό πολλαπλάσιο των ομαδοθεωρητικών τάξεων των στοιχείων της (και μπορεί να εκληφθεί ως *ο πλέον βολικός εκπρόσωπος* τής *μοδιοθεωρητικής τάξεως* $\mathrm{ord}(G)$, όπως αυτή ορίζεται στο εδ. Α.7.18 (i)).

(ii) ??????

Α.7.20 Πόρισμα. *Εάν R είναι μια Π.Κ.Ι. και M ένας μη τετριμμένος και πεπερασμένως παραγόμενος R-μόδιος στρέψεως, τότε ισχύουν τα ακόλουθα*:

(i) *Οι πρωτεύουσες συνιστώσες τού M είναι μονοσημάντως ορισμένες μέσω τής τάξεως* $\mathrm{ord}(M) = r \in R \smallsetminus (R^{\times} \cup \{0_R\})$ *τού M.*

(ii) *Εάν $r \underset{\text{συν.}}{\sim} p_1^{\nu_1} p_2^{\nu_2} ... p_t^{\nu_t}$ είναι η παράσταση τής τάξεως* $\mathrm{ord}(M) = r$ *ως γινομένου (κατάλληλων θετικών ακεραίων δυνάμεων) πρώτων στοιχείων $p_1, p_2, ..., p_t$ τής R (που είναι ανά δύο μη συντροφικά όταν $t \geq 2$), τότε η πρωτεύουσα συνιστώσα $M(p_j)$ έχει ως τάξη της το $p_j^{\nu_j}$ για κάθε $j \in \{1, ..., t\}$.*

ΑΠΟΔΕΙΞΗ. (i) Έπεται από τον ορισμό Α.7.18 (i), το θεώρημα Α.7.17 και το γεγονός ότι κάθε Π.Κ.Ι. είναι Π.Μ.Π.

(ii) Τούτο έπεται από τον ορισμό Α.7.12 (ii), το (iii) τής προτάσεως Α.7.11 και το θεώρημα Α.7.17. □

Α.7.21 Λήμμα. *Εάν R είναι μια Π.Κ.Ι., M, N δυο R-μόδιοι και $f \in \mathrm{Hom}_R(M,N)$, τότε $f(M(p)) \subseteq N(p)$ για κάθε πρώτο στοιχείο p τής R. Επιπροσθέτως, στην περίπτωση όπου ο f είναι ισομορφισμός, $f(M(p)) = N(p)$.*

[59] $\exp(G) := \min\{ l \in \mathbb{N} |\, lx = 0_G, \forall x \in G\}$.

ΑΠΟΔΕΙΞΗ. Εάν $x \in M(p)$, τότε $p^n x = 0_M$ για κάποιον $n \in \mathbb{N}$, οπότε

$$p^n f(x) = f(p^n x) = f(0_M) = 0_N \Rightarrow f(x) \in N(p).$$

Στην περίπτωση όπου ο f είναι ισομορφισμός, έχουμε

$$\left.\begin{array}{l} f(M(p)) \subseteq N(p) \\ f^{-1}(N(p)) \subseteq M(p) \end{array}\right\} \Rightarrow f(M(p)) = N(p),$$

οπότε ο $f|_{M(p)} : M(p) \longrightarrow N(p)$ είναι ισομορφισμός με τον $f^{-1}|_{N(p)}$ ως αντίστροφό του. $\square$

Α.7.22 Πρόταση. *Έστω R μια Π.Κ.Ι. Εάν M, N είναι δυο μη τετριμμένοι και πεπερασμένως παραγόμενοι R-μόδιοι στρέψεως, τότε*

$$M \cong N \Longleftrightarrow [M(p) \cong N(p) \text{ για κάθε πρώτο στοιχείο } p \text{ τής } R].$$

ΑΠΟΔΕΙΞΗ. Η συνεπαγωγή “$\Rightarrow$” έπεται άμεσα από το προηγηθέν λήμμα Α.7.21. Για την “$\Leftarrow$” υποθέτουμε ότι υπάρχουν ισομορφισμοί $f_{(p)} : M(p) \xrightarrow{\cong} N(p)$ για κάθε πρώτο στοιχείο $p \in R$. Έστω ότι $M = M(p_1) \oplus M(p_2) \oplus \cdots \oplus M(p_t)$ είναι η μοναδική αποσύνθεση (Α.39) τού M στα ευθέα αθροίσματα των πρωτευουσών συνιστωσών του. Τότε $M(p) = \{0_M\}$ για κάθε πρώτο στοιχείο $p \in R \smallsetminus \{p_1, ..., p_t\}$. Κατά συνέπειαν,

$$M = \bigoplus_{j=1}^{t} M(p_j) \cong \bigoplus_{p \text{ πρώτο στοιχείο}} M(p),$$

Κατ' αναλογίαν, $N \cong \bigoplus_{p \text{ πρώτο στοιχείο}} N(p)$, οπότε

$$M \cong \bigoplus_{p \text{ πρώτο στοιχείο}} M(p) \xrightarrow[f]{\cong} \bigoplus_{p \text{ πρώτο στοιχείο}} N(p) \cong N,$$

όπου $f((x_p)_{p \text{ πρώτο στοιχείο}}) := (f_{(p)}(x_p))_{p \text{ πρώτο στοιχείο}}$. $\square$

Α.7.23 Πόρισμα. *Έστω R μια Π.Κ.Ι. Εάν M, N είναι δυο μη τετριμμένοι και πεπερασμένως παραγόμενοι R-μόδιοι στρέψεως και*

$$M = M(p_1) \oplus M(p_2) \oplus \cdots \oplus M(p_t), \; N = N(q_1) \oplus N(q_2) \oplus \cdots \oplus N(q_{t'})$$

οι μοναδικές αποσυνθέσεις τους (Α.39) *στα ευθέα αθροίσματα των πρωτευουσών συνιστωσών τους, τότε*[60]

$$M \cong N \Longleftrightarrow [t = t' \text{ και } \exists \sigma \in \mathfrak{S}_t : M(p_j) \cong N(q_{\sigma(j)}) = N(p_j), \; \forall j \in \{1, ..., t\}].$$

[60] Το $\mathfrak{S}_t$ συμβολίζει το σύνολο των αμφιρρίψεων $\sigma : \{1, ..., t\} \longrightarrow \{1, ..., t\}$.

► **p-πρωτεύοντες μόδιοι υπεράνω Π.Κ.Ι.** Λόγω τού θεωρήματος Α.7.17 και των πορισμάτων Α.7.20 και Α.7.23 είναι αρκετό, από τούδε και στο εξής, να επικεντρωθούμε στη μελέτη των μη τετριμμένων, *πεπερασμένως παραγομένων p-πρωτευόντων* μοδίων που ορίζονται υπεράνω Π.Κ.Ι. (Βλ. Α.7.12 (iv).)

Α.7.24 Λήμμα. *Ας υποθέσουμε ότι p είναι ένα πρώτο στοιχείο μιας Π.Κ.Ι. R και M ένας μη τετριμμένος, πεπερασμένως παραγόμενος, p-πρωτεύων R-μόδιος τάξεως* $\mathrm{ord}(M) = p^{\nu}$, $\nu \in \mathbb{N}$. *Τότε υπάρχει ένα $x \in M \smallsetminus \{0_M\}$ τάξεως* $\mathrm{ord}(x) = p^{\nu}$ *και ένας υπομόδιος U τού M, ούτως ώστε να ισχύουν τα ακόλουθα:*

(i) $M = U \oplus Rx$, *όπου* $Rx \cong R/\langle p^{\nu}\rangle$.

(ii) *Ο U παράγεται από ένα σύνολο, ο πληθικός αριθμός τού οποίου είναι μικρότερος τού πληθικού αριθμού οιουδήποτε συστήματος γεννητόρων τού M.*

ΑΠΟΔΕΙΞΗ. Έστω $\mathcal{X} = \{x_1, ..., x_k\}$ ένα σύστημα γεννητόρων τού $M = M(p)$ με το *ελάχιστο δυνατό πλήθος στοιχείων*[61]. Επειδή $\mathrm{ord}(M) = p^{\nu}$, $\nu \in \mathbb{N}$, έχουμε $\mathrm{ord}(x_j) = p^{e_j}$, $e_j \in \mathbb{N}$, όπου $e_j \leq \nu$ για κάθε $j \in \{1, ..., k\}$. (Βλ. (Α.40).) Κάθε στοιχείο τού M γράφεται ως γραμμικός συνδυασμός $\sum_{j=1}^{k} r_j x_j$ των στοιχείων τού $\mathcal{X}$ (για κατάλληλα $r_1, ..., r_k \in R$). Ως εκ τούτου, υπάρχει τουλάχιστον ένας δείκτης $j_\bullet \in \{1, ..., k\}$ με[62] $\mathrm{ord}(x_{j_\bullet}) = p^{\nu}$. Αρκεί να θέσουμε $x := x_{j_\bullet}$.

(i) Θεωρούμε την οικογένεια υπομοδίων

$$\mathfrak{W} := \{W \,|W \text{ υπομόδιος τού } M : W \cap Rx = \{0_M\}\}.$$

Επειδή η $\mathfrak{W}$ περιέχει τον τετριμμένο υπομόδιο $\{0_M\}$ τού M, έχουμε $\mathfrak{W} \neq \varnothing$. Η $\mathfrak{W}$ καθίσταται μερικώς διατεταγμένο σύνολο ως προς τον συνήθη (συνολοθεωρητικό) εγκλεισμό. Για κάθε αλυσίδα $(W_\lambda)_{\lambda \in \Lambda}$ τού $(\mathfrak{W}, \subseteq)$ έχουμε[63]

$$\textstyle\bigcup_{\lambda \in \Lambda} W_\lambda = \sum_{\lambda \in \Lambda} W_\lambda$$

(όπου $\sum_{\lambda \in \Lambda} W_\lambda$ είναι ένας υπομόδιος τού M) και

$$\left(\textstyle\bigcup_{\lambda \in \Lambda} W_\lambda\right) \cap Rx = \textstyle\bigcup_{\lambda \in \Lambda} (W_\lambda \cap Rx) = \{0_M\},$$

οπότε $\bigcup_{\lambda \in \Lambda} W_\lambda \in \mathfrak{W}$ και η εν λόγω ένωση είναι ένα άνω φράγμα τής $(W_\lambda)_{\lambda \in \Lambda}$. Κατά συνέπειαν, το $(\mathfrak{W}, \subseteq)$ είναι επαγωγικώς διατεταγμένο και (σύμφωνα με το λήμμα τού Zorn) υφίσταται ένας υπομόδιος τού M, ας τον πούμε U, ο οποίος είναι

[61] Αυτό σημαίνει, ιδιαιτέρως, ότι $x_j \neq 0_M$ για κάθε $j \in \{1, ..., k\}$.

[62] Αλλιώς, $p^{\nu} \notin \text{ΕΚΠ}_R(p^{e_1}, ..., p^{e_k})$. Βλ. απόδειξη τού (i) τού θεωρήματος Α.7.17 και [87], θεώρημα 5.6.13.

[63] Εξ ορισμού, $\bigcup\limits_{\lambda \in \Lambda} W_\lambda \subseteq \sum\limits_{\lambda \in \Lambda} W_\lambda$. Κάθε στοιχείο τού $\sum\limits_{\lambda \in \Lambda} W_\lambda$ γράφεται υπό τη μορφή $w_{\lambda_1} + \cdots + w_{\lambda_n}$, όπου $n \in \mathbb{N}$ και $\{\lambda_1, ..., \lambda_n\} \subseteq \Lambda$. (Βλ. Α.2.16 και Α.2.17.) Επειδή η αλυσίδα $(W_\lambda)_{\lambda \in \Lambda}$ είναι εξ ορισμού ένα *ολικώς* διατεταγμένο υποσύνολο τού $\mathfrak{W}$, υπάρχει κάποιος δείκτης $\rho \in \{1, ..., n\} : W_{\lambda_j} \subseteq W_{\lambda_\rho}, \forall\, j \in \{1, ..., n\}$. Επομένως, $w_{\lambda_1} + \cdots + w_{\lambda_n} \in W_{\lambda_\rho} \subseteq \bigcup\limits_{\lambda \in \Lambda} W_\lambda$ και ισχύει και ο αντίστροφος εγκλεισμός $\sum\limits_{\lambda \in \Lambda} W_\lambda \subseteq \bigcup\limits_{\lambda \in \Lambda} W_\lambda$.

μεγιστικός (ως προς τον συνήθη συνολοθεωρητικό εγκλεισμό) εντός τής $\mathfrak{W}$. Θα δείξουμε ότι $M = M'$, όπου

$$M' := U \oplus Rx.$$

Προς τούτο θα χρησιμοποιήσουμε «εις άτοπον απαγωγή». Ας υποθέσουμε ότι $M' \subsetneqq M$. Τότε υπάρχει κάποιο στοιχείο $z \in M \smallsetminus M'$. Επειδή $p^\nu z = 0_M \in M'$, μπορούμε να ορίσουμε τον

$$\xi := \min\left\{n \in \mathbb{N} \,\middle|\, p^{n+1}z \in M' \text{ και } p^n z \notin M'\right\}.$$

Θέτοντας $y := p^\xi z$ παρατηρούμε ότι $y \in M \smallsetminus M'$ και $py \in M'$. Γι' αυτόν τον λόγο

$$\exists!(u,r) \in U \times R : py = u + rx.$$

Επειδή $p^\nu = \mathrm{ord}(M)$, έχουμε $0_M = p^\nu y = p^{\nu-1}(py) = p^{\nu-1}u + (p^{\nu-1}r)x$, οπότε

$$\left(p^{\nu-1}r\right)x = -p^{\nu-1}u \in U \cap Rx = \{0_M\} \Rightarrow p^{\nu-1}r \in \mathrm{Ann}_R(x) = \langle p^\nu \rangle,$$

απ' όπου προκύπτει ότι $p^{\nu-1}r = p^\nu r' \Rightarrow r = pr'$ για κάποιο $r' \in R$. Θέτοντας $v := y - r'x$ λαμβάνουμε

$$pv = p(y - r'x) = py - pr'x = rx + u - rx = u. \tag{A.41}$$

Όμως $y \notin M' \Rightarrow v \notin M'$ (διότι $r'x \in M'$) και, ως εκ τούτου, $v \notin U$. Αυτό σημαίνει ότι[64] $(U + Rv) \cap Rx \neq \{0_M\}$, οπότε υπάρχουν $u' \in U$ και $s, s' \in R$ με

$$0_M \neq sx = u' + s'v \in (U + Rv) \cap Rx. \tag{A.42}$$

Επομένως, $s'v = -u' + sx \in U \oplus Rx =: M'$. Εάν το p δεν διαιρούσε το s', θα είχαμε

$$\begin{aligned} & 1_R \in \mathrm{MK\Delta}_R(p, s') \Rightarrow [\exists (a,b) \in R \times R : ap + bs' = 1_R] \\ & \Rightarrow v = 1_R v = a\,(pv) + b\,(s'v) \underset{\text{(A.41)}}{=} au + b\,(s'v) \in U + M' = M', \end{aligned}$$

κάτι που θα αντέκειτο στο ότι $v \notin M'$. Κατά συνέπειαν, $s' = s''p$ για κάποιο $s'' \in R$. Από τις (A.41) και (A.42) λαμβάνουμε

$$0_M \neq sx = u' + s'v = u' + s''(pv) = u' + s''u \in U \cap Rx = \{0_M\}.$$

Άτοπο! Άρα $M = M'$. Τέλος, ο ισομορφισμός $Rx \cong R/\langle p^\nu \rangle$ έπεται από τον (A.36), καθώς $\mathrm{Ann}_R(x) = \langle p^\nu \rangle$.

(ii) Επειδή $x := x_{j_\bullet}$, ο M/Rx παράγεται από τα $k-1$ στοιχεία[65] $x_\rho + Rx$, $\rho \in \{1, ..., k\} \smallsetminus \{j_\bullet\}$. Κατά την πρόταση A.5.20, $U \cong M/Rx$. Άρα ο υπομόδιος U παράγεται από ένα σύνολο με πληθικό αριθμό[66] $k - 1 < k$. □

[64] Εάν ίσχυε $(U + Rv) \cap Rx = \{0_M\}$, τότε θα είχαμε $U + Rv \in \mathfrak{W}$ με $U \subsetneqq U + Rv$, κάτι που θα αντέκειτο στη μεγιστικότητα τού U.

[65] Εφαρμόζοντας το (i) τής προτάσεως A.3.7 και το πόρισμα για τον φυσικό επιμορφισμό $\pi^M_{Rx} : M \longrightarrow M/Rx$ λαμβάνουμε $M/Rx = \mathrm{Lin}_R(x_1 + Rx, ..., x_k + Rx)$. Επειδή $x_{j_\bullet} = x \in Rx$, ο γεννήτορας $x_{j_\bullet} + Rx$ μπορεί να αφαιρεθεί.

[66] Αυτό το σύνολο είναι το κενό (και ο U τετριμμένος) όταν $k = 1$.

A.7.25 Λήμμα. *Εάν R είναι μια ακεραία περιοχή και $a \in R \setminus \{0_R\}, b \in R$, τότε υφίσταται ισομορφισμός R-μοδίων*

$$\boxed{Ra/R(ab) \cong R/Rb.} \tag{A.43}$$

ΑΠΟΔΕΙΞΗ. Η επιρριπτική απεικόνιση

$$f : R \longrightarrow Ra/R(ab),\ r \longmapsto f(r) := ra + R(ab),$$

είναι επιμορφισμός R-μοδίων, διότι

$$\begin{aligned} f(s_1r_1 + s_2r_2) &= (s_1r_1 + s_2r_2)a + R(ab) \\ = s_1(r_1a + R(ab)) + s_2(r_2a + R(ab)) &= s_1f(r_1) + s_2f(r_2), \end{aligned}$$

για οιαδήποτε $s_1, s_2, r_1, r_2 \in R$ (βλ. πρόταση A.3.3), ο δε πυρήνας αυτού είναι ο

$$\begin{aligned} \mathrm{Ker}(f) &= \{r \in R \,|\, \exists c \in R : ra = cab\} \\ &= \{r \in R \,|\, \exists c \in R : r = cb\} = \langle b \rangle = Rb, \end{aligned}$$

καθόσον ο δακτύλιος R είναι ακεραία περιοχή και $a \neq 0_R$. Αρκεί λοιπόν να εφαρμοσθεί το 1ο θεώρημα ισομορφισμών A.4.7. □

A.7.26 Λήμμα. *Έστω p ένα πρώτο στοιχείο μιας Π.Κ.Ι. R και έστω M ένας μη τετριμμένος, πεπερασμένως παραγόμενος, p-πρωτεύων R-μόδιος. Τότε ισχύουν τα εξής:*

(i) *Ο πηλικοδακτύλιος $R/\langle p \rangle$ είναι ένα σώμα.*

(ii) *Ο υπομόδιος $M[p]$ τού M αποτελεί έναν $(R/\langle p \rangle)$-διανυσματικό χώρο διαστάσεως $\dim_{R/\langle p \rangle}(M[p]) = k$, όπου k είναι ο ελάχιστος εκ των πληθικών αριθμών όλων των πεπερασμένων συστημάτων γεννητόρων τού M.*

ΑΠΟΔΕΙΞΗ. (i) Το $\langle p \rangle$ ως πρώτο ιδεώδες μιας Π.Κ.Ι. είναι και μεγιστικό ιδεώδες[67]. Επομένως ο πηλικοδακτύλιος $R/\langle p \rangle$ είναι ένα σώμα. (Βλ. ??.)

(ii) Προφανώς, $\mathrm{ord}(M) = p^{\nu}$ για κάποιον $\nu \in \mathbb{N}$. Ο υπομόδιος $M[p]$ τού R-μοδίου $M = M(p)$, εφοδιαζόμενος με τον αριθμητικό πολλαπλασιασμό[68]

$$R/\langle p \rangle \times M[p] \ni (r + \langle p \rangle, x) \longmapsto rx \in M[p],$$

καθίσταται διανυσματικός χώρος υπεράνω τού σώματος $R/\langle p \rangle$. Έστω $\{x_1, ..., x_k\}$ ένα σύστημα γεννητόρων τού M με το *ελάχιστο δυνατό πλήθος στοιχείων* (ήτοι με

[67] Βλ. [87], πρόταση 4.2.15.

[68] Αυτός είναι *καλώς ορισμένος*, διότι εάν $r, r' \in R$ είναι τέτοια, ώστε να ισχύει $r + \langle p \rangle = r' + \langle p \rangle$ ή, ισοδυνάμως, $r - r' = sp$ για κάποιο $s \in R$, τότε για κάθε $x \in M[p]$ λαμβάνουμε

$$rx - r'x = (r - r')\,x = s(px) = s0_M = 0_M \Rightarrow rx = r'x.$$

min-g$(M) = k$, βλ. A.6.51). Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον k. Εάν $k = 1$, τότε ο ισχυρισμός είναι αληθής, καθώς $M = Rx_1 \cong R/\langle p^\nu \rangle$, ord$(x_1) = p^\nu$ και[69]

$$M[p] \cong (R/\langle p^\nu \rangle)[p] \cong Rp^{\nu-1}/Rp^\nu = Rp^{\nu-1}/R(p^{\nu-1}p) \underset{\text{(A.43)}}{\cong} R/pR = R/\langle p \rangle,$$

οπότε $\dim_{R/\langle p \rangle}(M[p]) = 1$. Εάν υποθέσουμε ότι $k \geq 2$ και ότι αυτός είναι αληθής και για όλους τους R-μοδίους αυτού τού είδους που διαθέτουν συστήματα γεννητόρων με ελάχιστο δυνατό πλήθος στοιχείων $< k$, τότε (σύμφωνα με τα προαναφερθέντα στην απόδειξη τού (i) τού λήμματος A.7.24) υπάρχει κάποιο $x \in \{x_1, ..., x_k\}$ τάξεως ord$(x) = p^\nu$, καθώς και ένας υπομόδιος U τού M με $M = U \oplus Rx$, όπου $Rx \cong R/\langle p^\nu \rangle$. Ο U είναι μη τετριμμένος (αφού $k \geq 2$) και (ως υπομόδιος τού M) p-πρωτεύων και πεπερασμένως παραγόμενος (κατά το πόρισμα A.6.49). Επιπροσθέτως, σύμφωνα με τα προαναφερθέντα στην απόδειξη τού A.7.24 (ii), ο U παράγεται από ένα σύνολο, ο πληθικός αριθμός τού οποίου είναι $k - 1 < k$.

Ισχυρισμός. Δεν υφίσταται σύστημα γεννητόρων τού U με πληθικό αριθμό $< k-1$. Πράγματι· επειδή (κατά την πρόταση A.5.20) υφίσταται ισομορφισμός $M/Rx \cong U$, εάν ίσχυε min-g$(U) < k - 1$, τότε εφαρμόζοντας το πόρισμα A.6.52 για τον φυσικό επιμορφισμό $\pi^M_{Rx} : M \longrightarrow M/Rx$ (όπου $\mathrm{Ker}(\pi^M_{Rx}) = Rx$) θα καταλήγαμε σε άτοπο:

$$k = \text{min-g}(M) \leq \text{min-g}(U) + \text{min-g}(Rx) < (k-1) + 1 = k.$$

Επομένως, min-g$(U) = k - 1$. Ο $U[p]$ αποτελεί γραμμικό υπόχωρο τού $(R/\langle p \rangle)$-διανυσματικού χώρου $M[p]$ και από την επαγωγική μας υπόθεση λαμβάνουμε

$$\dim_{R/\langle p \rangle}(U[p]) = \text{min-g}(U) = k - 1.$$

Αποπεράτωση αποδείξεως. Είναι άμεσος ο έλεγχος τού ότι

$$M[p] = U[p] \oplus (Rx)[p],$$

όπου $(Rx)[p] \cong (R/\langle p^\nu \rangle)[p] \cong R/\langle p \rangle$. Κατά συνέπειαν,

$$\dim_{R/\langle p \rangle}(M[p]) = \dim_{R/\langle p \rangle}(U[p]) + \dim_{R/\langle p \rangle}((Rx)[p]) = (k-1) + 1 = k,$$

απ' όπου έπεται το ζητούμενο. □

A.7.27 Θεώρημα. *Ας υποθέσουμε ότι p είναι ένα πρώτο στοιχείο μιας Π.Κ.Ι. R και M ένας μη τετριμμένος, πεπερασμένως παραγόμενος, p-πρωτεύων R-μόδιος τάξεως* ord$(M) = p^\nu$, $\nu \in \mathbb{N}$. *Τότε ισχύουν τα εξής:*

(i) *Ο M είναι το ευθύ άθροισμα*

$$\boxed{M = M_1 \oplus M_2 \oplus \cdots \oplus M_k,} \tag{A.44}$$

[69]Η απεικόνιση $Rp^{\nu-1} \ni rp^{\nu-1} \longmapsto rp^{\nu-1} + \langle p^\nu \rangle \in (R/\langle p^\nu \rangle)[p]$ είναι επιμορφισμός R-μοδίων έχων ως πυρήνα του το Rp^ν.

κυκλικών p-πρωτευόντων υπομοδίων M_j, $j \in \{1, ..., k\}$, όπου $k = \dim_{R/\langle p\rangle}(M[p])$.
(ii) *$M_j \cong R/\left\langle p^{\ell_j}\right\rangle$, όπου ο $\ell_j \in \mathbb{N}$ είναι μονοσημάντως ορισμένος μέσω τής τάξεως $\operatorname{ord}(M_j)$ για κάθε $j \in \{1, ..., k\}$, και $1 \leq \ell_1 \leq \ell_2 \leq \cdots \leq \ell_k = \nu$.*
(iii) *Η αποσύνθεση (A.44) είναι μονοσημάντως ορισμένη υπό την εξής έννοια: Εάν*

$$M = M_1' \oplus M_2' \oplus \cdots \oplus M_{k'}'$$

είναι μια άλλη ομοειδής αποσύνθεση τού M με $M_i' \cong R/\left\langle p^{\ell_i'}\right\rangle$, $\forall i \in \{1, ..., k'\}$, και

$$1 \leq \ell_1' \leq \ell_2' \leq \cdots \leq \ell_{k'}' = \nu,$$

και εάν θέσουμε για κάθε[70] *$\rho \in \mathbb{N}$, $\mathfrak{d}_\rho(M) := \operatorname{card}(\{ j \in \{1, ..., k\} | \, \ell_j = \rho\})$ και*

$$\mathfrak{d}_\rho'(M) := \operatorname{card}\left(\{ i \in \{1, ..., k'\} | \, \ell_i' = \rho\}\right),$$

τότε $k = k'$, $\ell_j = \ell_j'$, $\forall j \in \{1, ..., k\}$, και

$$\mathfrak{d}_\rho(M) = \mathfrak{d}_\rho'(M), \ \forall \rho \in \{1, ..., \nu\}. \tag{A.45}$$

ΑΠΟΔΕΙΞΗ. (i)-(ii) Έστω $\{x_1, ..., x_k\}$ ένα σύστημα γεννητόρων τού M με το *ελάχιστο δυνατό πλήθος στοιχείων*. Γνωρίζουμε ότι $k = \dim_{R/\langle p\rangle}(M[p])$ (από το λήμμα A.7.26). Θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον k. Όταν $k = 1$ ο ισχυρισμός είναι προδήλως αληθής. Εάν υποθέσουμε ότι $k \geq 2$ και ότι αυτός είναι αληθής και για όλους τους R-μοδίους αυτού τού είδους που διαθέτουν συστήματα γεννητόρων με ελάχιστο δυνατό πλήθος στοιχείων $< k$, τότε (σύμφωνα με τα προαναφερθέντα στην απόδειξη τού (i) τού λήμματος A.7.24) υπάρχει κάποιο $x \in \{x_1, ..., x_k\}$ τάξεως $\operatorname{ord}(x) = \operatorname{ord}(M) = p^\nu$, καθώς και ένας υπομόδιος U τού M με $M = U \oplus Rx$, όπου $Rx \cong R/\langle p^\nu\rangle$. Δίχως βλάβη τής γενικότητας μπορούμε (ενδεχομένως ύστερα από κάποια αναδιάταξη δεικτών) να υποθέσουμε ότι $x = x_k$. Επιπροσθέτως, θέτουμε $\ell_k := \nu$. Σύμφωνα με τα προαναφερθέντα στην απόδειξη τού λήμματος A.7.26, ο U είναι μη τετριμμένος, πεπερασμένως παραγόμενος και p-πρωτεύων με $\dim_{R/\langle p\rangle}(U[p]) = \text{min-g}(U) = k - 1$. Βάσει τής επαγωγικής μας υποθέσεως,

$$U = M_1 \oplus M_2 \oplus \cdots \oplus M_{k-1},$$

όπου ο $M_j \cong R/\left\langle p^{\ell_j}\right\rangle$ είναι κυκλικός υπομόδιος τού U και ο $\ell_j \in \mathbb{N}$ είναι μονοσημάντως ορισμένος μέσω τής τάξεως $\operatorname{ord}(M_j) = p^{\ell_j}$ για κάθε $j \in \{1, ..., k-1\}$, και $1 \leq \ell_1 \leq \cdots \leq \ell_{k-1}$ με $\operatorname{ord}(U) = \operatorname{ord}(M/Rx_k) = p^{\ell_{k-1}}$. Επειδή ο U είναι υπομόδιος τού M, έχουμε $\operatorname{ord}(U) \; |\operatorname{ord}(M)$, οπότε $\ell_{k-1} \leq \ell_k$, και καταλήγουμε στην (A.44) θέτοντας $M_k := Rx_k$.

[70] Προφανώς, $\mathfrak{d}_\rho(M) = \mathfrak{d}_\rho'(M) = 0$ όταν $\rho > \nu$.

(iii) Προφανώς, $k = \dim_{R/\langle p\rangle}(M[p]) = k'$, καθώς αυτός ο αριθμός είναι μοναδικός, εξαρτώμενος μόνον από τον ίδιον τον M:

$$k = \sum_{\rho=1}^{\nu} \mathfrak{d}_\rho(M) = \sum_{\rho=1}^{\nu} \mathfrak{d}'_\rho(M) = k'. \tag{A.46}$$

Εν συνεχεία, για την επαλήθευση των λοιπών ισχυρισμών θα χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον ν. Όταν $\nu = 1$ έχουμε

$$\ell_1 = \ell_2 = \cdots = \ell_k = 1 = \ell'_1 = \ell'_2 = \cdots = \ell'_k \text{ και } \mathfrak{d}_1(M) = k = \mathfrak{d}'_1(M).$$

Ας υποθέσουμε τώρα ότι $\nu \geq 2$. Θεωρώντας τόν $pM := \{p\,x |\, x \in M\}$ στη θέση τού M λαμβάνουμε τις αποσυνθέσεις

$$pM = pM_1 \oplus pM_2 \oplus \cdots \oplus pM_k = pM'_1 \oplus pM'_2 \oplus \cdots \oplus pM'_k.$$

Προφανώς,

$$\begin{aligned} pM &\cong Rp/Rp^{\ell_1} \oplus Rp/Rp^{\ell_2} \oplus \cdots \oplus Rp/Rp^{\ell_k} \\ &\underset{\text{(A.43)}}{\cong} R/Rp^{\ell_1-1} \oplus R/Rp^{\ell_2-1} \oplus \cdots \oplus R/Rp^{\ell_k-1} \end{aligned}$$

με τους πρώτους $\mathfrak{d}_1(M)$ ευθείς προσθετέους τετριμμένους (καθώς εξ υποθέσεως ισχύει $\ell_1 = \ell_2 = \cdots = \ell_{\mathfrak{d}_1(M)} = 1$),

$$pM \cong R/Rp^{\ell_{\mathfrak{d}_1(M)+1}-1} \oplus R/Rp^{\ell_{\mathfrak{d}_1(M)+2}-1} \oplus \cdots \oplus R/Rp^{\ell_k-1}$$

και $1 \leq \ell_{\mathfrak{d}_1(M)+1} - 1 \leq \ell_{\mathfrak{d}_1(M)+2} - 1 \leq \cdots \leq \ell_k - 1 = \nu - 1$. Κατ' αναλογίαν,

$$pM \cong R/Rp^{\ell'_{\mathfrak{d}'_1(M)+1}-1} \oplus R/Rp^{\ell'_{\mathfrak{d}'_1(M)+2}-1} \oplus \cdots \oplus R/Rp^{\ell'_k-1},$$

όπου $1 \leq \ell'_{\mathfrak{d}'_1(M)+1} - 1 \leq \ell'_{\mathfrak{d}'_1(M)+2} - 1 \leq \cdots \leq \ell'_k - 1 = \nu - 1$. Επειδή ο τελευταίος αριθμός είναι $< \nu$, μπορούμε να εφαρμόσουμε την επαγωγική μας υπόθεση για τον pM και να λάβουμε

$$k - \mathfrak{d}_1(M) = \dim_{R/\langle p\rangle}(pM[p]) = k - \mathfrak{d}'_1(M) \Rightarrow \mathfrak{d}_1(M) = \mathfrak{d}'_1(M) \tag{A.47}$$

και $\ell_j - 1 = \ell'_j - 1 \Rightarrow \ell_j = \ell'_j$ για κάθε[71] $j \in \{\mathfrak{d}_1(M)+1, ..., k\}$. Οι (A.46) και (A.47) δίδουν

$$\sum_{\rho=2}^{\nu} \mathfrak{d}_\rho(M) = \sum_{\rho=2}^{\nu} \mathfrak{d}'_\rho(M). \tag{A.48}$$

[71]Επειδή $\mathfrak{d}_1(M) = \mathfrak{d}'_1(M)$, έχουμε ήδη εξ αρχής $\ell_j = \ell'_j = 1,\ \forall j \in \{1, ..., \mathfrak{d}_1(M)\}$.

Κατόπιν επαναλήψεως αυτής τής διαδικασίας (με τον p^2M στη θέση τού pM, τον p^3M στη θέση τού p^2M κ.ο.κ) καταλήγουμε στις ισότητες

$$\left\{ \begin{array}{c} \sum\limits_{\rho=3}^{\nu} \mathfrak{d}_\rho(M) = \sum\limits_{\rho=3}^{\nu} \mathfrak{d}'_\rho(M), \\ \vdots \\ \mathfrak{d}_{\nu-1}(M) + \mathfrak{d}_\nu(M) = \mathfrak{d}'_{\nu-1}(M) + \mathfrak{d}'_\nu(M), \\ \mathfrak{d}_\nu(M) = \mathfrak{d}'_\nu(M). \end{array} \right\} \tag{A.49}$$

Η (A.45) προκύπτει άμεσα από τις (A.46), (A.48) και (A.49). □

A.7.28 Ορισμός. Ένας M όπως στο θεώρημα A.7.27 ονομάζεται p-**πρωτεύων** R-**μόδιος τύπου** $(\ell_1, \ell_2, ..., \ell_k)$. Οι μονοσημάντως ορισμένοι ευθείς προσθετέοι στην (A.44) καλούνται **στοιχειώδεις κυκλικοί προσθετέοι**, οι δε τάξεις αυτών $p^{\ell_1}, p^{\ell_2}, ..., p^{\ell_k}$ **στοιχειώδεις διαιρέτες τού** M. Η γνώση των στοιχειωδών διαιρετών (ή, ισοδυνάμως, των εκθετών τού p που συγκροτούν τον τύπο του) επαρκεί για τον *μέχρις ισομορφισμού* χαρακτηρισμό τού M.

A.7.29 Πρόταση. *Έστω p ένα πρώτο στοιχείο μιας Π.Κ.Ι. R. Για δυο μη τετριμμένους, πεπερασμένως παραγομένους, p-πρωτεύοντες R-μοδίους M, N οι ακόλουθες συνθήκες είναι ισοδύναμες:*

(i) $M \cong N$.

(ii) *Οι M και N διαθέτουν τους ίδιους στοιχειώδεις διαιρέτες $p^{\ell_1}, p^{\ell_2}, ..., p^{\ell_k}$.*

Αποδειξη. (i)⇒(ii) Εάν $M \cong N$, τότε οι $M[p], N[p]$ είναι ισόμορφοι ως διανυσματικοί χώροι υπεράνω τού σώματος $R/\langle p \rangle$, οπότε

$$\dim_{R/\langle p \rangle}(M[p]) = k = \dim_{R/\langle p \rangle}(N[p]),$$

όπου k είναι ο αριθμός των στοιχειωδών διαιρετών τού M και, κατ' επέκταση, και τού N. Επειδή $M \cong N$, οι τάξεις των M και N (σύμφωνα με το πόρισμα A.7.23 και το (i) τού πορίσματος A.7.20) είναι ίσες, ας πούμε $\mathrm{ord}(M) = p^\nu = \mathrm{ord}(N)$, για κάποιον $\nu \in \mathbb{N}$. Αυτό σημαίνει ότι οι τελευταίοι τους στοιχειώδεις διαιρέτες είναι ίσοι. Αρκεί λοιπόν να χρησιμοποιήσουμε μαθηματική επαγωγή ως προς τον k. Εάν $k = 1$, τότε οι M, N είναι κυκλικοί και ο ισχυρισμός είναι προδήλως αληθής. Εάν υποθέσουμε ότι $k \geq 2$ και ότι αυτός είναι αληθής και για όλους τους R-μοδίους αυτού τού είδους με αριθμό στοιχειωδών διαιρετών $< k$, τότε (σύμφωνα με τα προαναφερθέντα στην απόδειξη τού (i) τού λήμματος A.7.24) υπάρχουν κάποια $x \in M$ και $y \in N$ με

$$\mathrm{ord}(x) = \mathrm{ord}(M) = p^\nu = \mathrm{ord}(N) = \mathrm{ord}(y),$$

καθώς και υπομόδιοι U και W των M και N, αντιστοίχως, τέτοιοι ώστε

$$M = U \oplus Rx \;\text{ και }\; N = W \oplus Ry, \;\text{ όπου }\; Rx \cong R/\langle p^\nu \rangle \cong Ry.$$

Επειδή $M \cong N \Rightarrow M/Rx \cong N/Ry \underset{\text{A.5.20}}{\Longrightarrow} U \cong W$ και (βάσει των προαναφερθέντων στο λήμμα Α.7.26 και στο (i) τού θεωρήματος Α.7.27) ισχύουν οι ισότητες

$$\dim_{R/\langle p\rangle}(U[p]) = \text{min-g}(U) = k-1 = \text{min-g}(W) = \dim_{R/\langle p\rangle}(W[p]),$$

από την επαγωγική μας υπόθεση έπεται ότι οι U και W διαθέτουν τους ίδιους στοιχειώδεις διαιρέτες $p^{\ell_1}, p^{\ell_2}, ..., p^{\ell_{k-1}}$. Κατά συνέπειαν, και οι M και N διαθέτουν τους ίδιους στοιχειώδεις διαιρέτες $p^{\ell_1}, p^{\ell_2}, ..., p^{\ell_{k-1}}, p^{\ell_k}$, όπου $\ell_k = \nu$.

(ii)⇒(i) Εν τοιαύτη περιπτώσει, $M \cong \bigoplus_{j=1}^{k} R/\left\langle p^{\ell_j}\right\rangle \cong N$ επί τη βάσει τού θεωρήματος Α.7.27. □

Α.7.30 Θεώρημα. («Δομικό θεώρημα» περί των πεπ. παρ. μοδίων υπεράνω Π.Κ.Ι.) *Εάν R είναι μια Π.Κ.Ι. και M ένας πεπερασμένως παραγόμενος R-μόδιος, τότε ισχύουν τα εξής:*

(i) $M = \text{tors}(M) \oplus \text{frp}(M)$.

(ii) *Εάν ο υπομόδιος στρέψεως* $\text{tors}\,(M)$ *τού M δεν είναι τετριμμένος, τότε διαθέτει μια ευθεία αποσύνθεση*

$$\boxed{\text{tors}\,(M) = \text{tors}\,(M)\,(p_1) \oplus \cdots \oplus \text{tors}\,(M)\,(p_t)}$$

στις πρωτεύουσες συνιστώσες του (μοναδική, μέχρις αναδιατάξεως αυτών) και

$$\exists \nu_j \in \mathbb{N} : \text{ord}(\text{tors}\,(M)\,(p_j)) = p_j^{\nu_j},\ \forall j \in \{1, ..., t\}.$$

(iii) *Εάν* $\text{tors}\,(M) \neq \{0_M\}$, *τότε κάθε πρωτεύουσα συνιστώσα* $\text{tors}\,(M)\,(p_j)$ *τού* $\text{tors}\,(M)$ *διαθέτει μια (μέχρις ισομορφισμού μονοσημάντως ορισμένη) αποσύνθεση σε ευθέα αθροίσματα κυκλικών υπομοδίων:*

$$\boxed{\text{tors}\,(M)\,(p_j) \cong \left(R/\left\langle p_j^{\ell_{j,1}}\right\rangle\right) \oplus \left(R/\left\langle p_j^{\ell_{j,2}}\right\rangle\right) \oplus \cdots \oplus \left(R/\left\langle p_j^{\ell_{j,k_j}}\right\rangle\right),}$$

$$\text{με}\quad 1 \leq \ell_{j,1} \leq \ell_{j,2} \leq \cdots \leq \ell_{j,k_j} = \nu_j,\ \forall j \in \{1, ..., t\}.$$

(iv) *Ο M είναι μονοσημάντως ορισμένος μέχρις ισομορφισμού μέσω των ακολούθων «αναλλοιώτων» του*[72]:

- τής ελεύθερης βαθμίδας $\text{fr-rank}_R(M) \in \mathbb{N}_0$,
- τής τάξεως $\text{ord}(\text{tors}\,(M)) = p_1^{\nu_1} p_2^{\nu_2} \cdots p_t^{\nu_t}$,
- των εκθετών $\ell_{j,1}, \ell_{j,2}, ..., \ell_{j,k_j}$, $\forall j \in \{1, ..., t\}$.

[72]Εδώ αναφερόμαστε στη γενική περίπτωση (όπου $\text{tors}(M) \neq \{0_M\}$). Όταν ο M δεν διαθέτει στρέψη, τότε είναι ελεύθερος, οπότε αρκεί μόνον η γνώση τής βαθμίδας του για τη μέχρις ισομορφισμού ταξινόμησή του.

ΑΠΟΔΕΙΞΗ. (i) Βλ. θεώρημα A.7.6.

(ii) Αρκεί να εφαρμοσθεί το θεώρημα A.7.17 για τον $\mathrm{tors}(M)$.

(iii) Τούτο έπεται από το θεώρημα A.7.27 (εφαρμοζόμενο για καθεμιά εκ των πρωτευουσών συνιστωσών τού υπομοδίου στρέψεως τού M).

(iv) Βλ. (A.35), το θεώρημα A.7.9, τα πορίσματα A.7.20 και A.7.23, και την πρόταση A.7.29. □

A.7.31 Συμβολισμός. Έστω $n \in \mathbb{N}$. Για κάθε $k \in \{1,...,n\}$ συμβολίζουμε ως

$$\Pi_k\,(n) := \left\{(\ell_1,\ell_2,...,\ell_k) \in \mathbb{N}^k \mid \ell_1 \leq \ell_2 \leq \cdots \leq \ell_k,\ \text{με}\ \ell_1 + \cdots + \ell_k = n\right\}$$

το σύνολο *όλων των διαμερίσεων τού* n (ως προς την πρόσθεση τού $\mathbb{N}$) *σε* k *φυσικούς αριθμούς*. (Προφανώς, $\Pi_1\,(n) = \{n\}$ και $\Pi_n\,(n) = \{(1,1,...,1)\}$.) Επίσης, συμβολίζουμε ως $\Pi\,(n) := \bigcup_{k=1}^{n} \Pi_k\,(n)$ το σύνολο *όλων των δυνατών διαμερίσεων* τού ν και θέτουμε

$$\varpi\,(n) := \mathrm{card}(\Pi\,(n)).$$

A.7.32 Θεώρημα. (Ταξινόμηση πεπερασμένως παραγομένων αβελιανών ομάδων) *Έστω $(G,+)$ μια μη τετριμμένη, μη ελεύθερη*[73]*, πεπερασμένως παραγόμενη αβελιανή ομάδα.*

(i) *Εάν*

$$\exp(\mathrm{tors}\,(G)) := \min\{\, l \in \mathbb{N} |\, lx = 0_G, \forall x \in \mathrm{tors}\,(G)\} = p_1^{\nu_1} p_2^{\nu_2}\ \cdots\ p_t^{\nu_t}$$

($t \in \mathbb{N},\ \nu_1,...,\nu_t \in \mathbb{N}$) *είναι η κανονική παράσταση τού ομαδοθεωρητικού εκθέτη τής υποομάδας* $\mathrm{tors}\,(G)$ *ως γινομένου (κατάλληλων δυνάμεων) πρώτων αριθμών* $p_1,...,p_t$ *με* $p_1 < \cdots < p_t$,

$$|\mathrm{tors}\,(G)| = p_1^{n_1} p_2^{n_2}\ \cdots\ p_t^{n_t}$$

η αντίστοιχη παράσταση τής τάξεως τής $\mathrm{tors}\,(G)$ *(όπου* $1 \leq \nu_j \leq n_j$*) και* $G\,(p_j)$ *η υποομάδα τής* G *η απαρτιζόμενη εκείνα τα στοιχεία τής* G, *η ομαδοθεωρητική τάξη των οποίων ανήκει στο σύνολο* $\{p_j^i\ |i \in \{0,1,...,n_j\}\}$ *για κάθε* $j \in \{1,...,t\}$, *τότε*

$$\boxed{G \cong \left(\bigoplus_{j=1}^{t} G\,(p_j)\right) \oplus \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{\text{fr-rank}_{\mathbb{Z}}(G)\ \text{φορές}},}$$

όπου $\exp(G\,(p_j)) = p_j^{\nu_j}$ *και* $|G\,(p_j)| = p_j^{n_j},\ \forall j \in \{1,...,t\}$.

[73] Εάν η $(G,+)$ είναι ελεύθερη και πεπερασμένως παραγόμενη, τότε $G \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{\mathrm{rank}_{\mathbb{Z}}(G)\ \text{φορές}}$.

(ii) *Για κάθε* $j \in \{1,...,t\}$

$$\exists k_j \in \{1,...,n_j\} \ \ \textit{και} \ \ \exists(\ell_{j,1},\ell_{j,2},...,\ell_{j,k_j}) \in \Pi_{k_j}(n_j)$$

με $\ell_{j,k_j} = \nu_j$, *ούτως ώστε να υφίστανται ισομορφισμοί*

$$\boxed{G(p_j) \cong \mathbb{Z}_{p_j^{\ell_{j,1}}} \oplus \mathbb{Z}_{p_j^{\ell_{j,2}}} \oplus \cdots \oplus \mathbb{Z}_{p_j^{\ell_{j,k_j}}}.}$$

(iii) *Η* G *είναι μονοσημάντως ορισμένη μέχρις ισομορφισμού μέσω των «αναλλοιώτων» της*: fr-rank$_{\mathbb{Z}}(G)$, $|\mathrm{tors}(G)|$ *και* $(\ell_{j,1},\ell_{j,2},...,\ell_{j,k_j})$ *για κάθε* $j \in \{1,...,t\}$.

ΑΠΟΔΕΙΞΗ. Θεωρούμε την G ως $\mathbb{Z}$-μόδιο (βλ. Α.2.4 (i)) και λαμβάνουμε υπ' όψιν τις συμβάσεις τού εδ. Α.7.19 (i) για την tors(G). Είναι άμεσος ο έλεγχος τού ότι

$$\begin{aligned} G(p_j) = \mathrm{tors}(G)(p_j) &\cong \mathbb{Z}/p_j^{\ell_{j,1}}\mathbb{Z} \oplus \mathbb{Z}/p_j^{\ell_{j,2}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_j^{\ell_{j,k_j}}\mathbb{Z} \\ &\cong \mathbb{Z}_{p_j^{\ell_{j,1}}} \oplus \mathbb{Z}_{p_j^{\ell_{j,2}}} \oplus \cdots \oplus \mathbb{Z}_{p_j^{\ell_{j,k_j}}} \end{aligned}$$

όπου $1 \leq \ell_{j,1} \leq \ell_{j,2} \leq \cdots \leq \ell_{j,k_j} = \nu_j$, $k_j = \dim_{\mathbb{Z}_{p_j}}(\mathrm{tors}(G)[p_j])$, για κάθε $j \in \{1,...,t\}$ (με τον πρώτον εκ των ανωτέρω ισομορφισμών οφειλόμενον στα (i) και (ii) τού θεωρήματος Α.7.27). Επειδή

$$|G(p_j)| = p_j^{n_j} = p^{\ell_{j,1}+\ell_{j,2}+\cdots+\ell_{j,k_j}} = \left|\bigoplus\nolimits_{j=1}^{t} G(p_j)\right|,$$

λαμβάνουμε $1 \leq k_j \leq n_j = \ell_{j,1} + \ell_{j,2} + \cdots + \ell_{j,k_j}$ για κάθε $j \in \{1,...,t\}$. Για επαλήθευση των λοιπών ισχυρισμών βλ. θεώρημα Α.7.30. $\square$

Α.7.33 Πόρισμα. *Το πλήθος των ανά ζεύγη μη ισομόρφων πεπερασμένων αβελιανών ομάδων τάξεως* $p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t}$ $(t \in \mathbb{N},\ n_1,...,n_t \in \mathbb{N})$, *όπου οι* $p_1,...,p_t$ *είναι πρώτοι αριθμοί με* $p_1 < \cdots < p_t$, *ισούται με*

$$\prod_{j=1}^{t} \varpi(n_j).$$