Βασιλακης Σταυρος

Noetherian και Artinian δακτυλιοι

Πτυχιακη Εργασια

Πανεπιστήμιο Αιγαίου, Τμήμα Μαθηματικών

Σάμος Σεπτεμβρίου 2014

Εισηγητης: Ευστράτιος Πρασίδης

Επιτροπη

Β. Μεταφτσής

Ν. Παπαλεξίου

Στους γονείς μου!

Περιεχόμενα

Εισαγωγή

Οι δακτύλιοι είναι αλγεβρικές δομές που εμφανίζονται με φυσικό τρόπο σε πολλές περιοχές των μαθηματικών (Άλγβερα, Τοπολογία, Θεωρία Αριθμών). Επίσης αβελιανές ομάδες με μια δράση δακτυλίων (modules) είναι φυσικές γενικεύσεις των διανυσματικών χώρων. Η μελέτη των δακτυλίων και της δομής των modules είναι, γενικά, μια φυσική γενίκευση της γραμμμικής άλγεβρας. Η γενίκευση αυτή δεν είναι άμεση και η θεωρία των modules είναι πιο πολύπλοκη και πλούσια από την θεωρία των διανυσματικών χώρων.

Σ′ αυτήν την εργασία αποδεικνύουμε αποτελέσματα που δίνουν την δομή την modules πάνω από δακτύλιους με ειδικές ιδιότητες. Η πρώτη κατηγορία δακτυλίων που θα μελετήσουμε είναι οι δακτύλιοι κυρίων ιδεωδών. Σ′ αυτήν την περίπτωση δίνουμε την πλήρη ταξινόμηση των πεπερασμένα παραγόμενων modules. Το αποτέλεσμα είναι μια γενίκευση της ταξινόμησης των πεπερασμένα παραγόμενων αβελιανών ομάδων.

Οι συνθήκες αλυσίδας ιδεωδών ή modules επίσης επιβάλλουν περιορισμούς στην δομή των δακτυλίων και των modules. Δίνουμε κάποια αποτελέσματα για τους δακτυλίους Noether και τους δακτυλίους Artin. Ιδιότητες των πεπερασμένων παραγόμενων modules πάνω από δακτυλίους Noether δίνονται, οι οποίες γενικεύουν αντίστοιχες ιδότητες της περίπτωσης που ο δακτύλιος είναι κυρίων ιδεωδών. Επίσης αποδεικύουμε το Θεώρημα Βάσης του Hilbert που δίνει τρόπους κατασκευής δακτυλίων Noether. Για τους δακτύλιους Artin δίνουμε το βασικό θεώρημα χαρακτηρισμού τους.

Κεφάλαιο 1

Modules επί μιας περιοχής κύριου ιδεώδους

Σε αυτό το κεφάλαιο θα αναφέρουμε βασικές έννοιες.

1.1 Βασικοί ορισμοί και έννοιες

Ορισμός 1.1.1. *Δακτύλιος είναι ένα μη κενό σύνολο R με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού και πληρεί τα παρακάτω:*

(i) $(R, +)$ *είναι αβελιανή ομάδα*

(ii) $(ab)c = a(bc)$ *για κάθε* $a, b, c \in R$

(iii) $a(b + c) = ab + ac$ *και* $(a + b)c = ac + bc$
Ακόμα εάν :

(iv) $ab = ba$ $\forall$ $a, b \in R$ *τότε ο* R *λέγεται μεταθετικός δακτύλιος*

(v) *Αν ο* R *περιέχει στοιχείο τέτοιο ώστε* $1a = a1 = a$ *για κάθε* $a \in R$ *τότε ο* R *λέμε ότι έχει μονάδα*

Ορισμός 1.1.2. *Έστω* R *και* S *δύο δακτύλιοι. Μία συνάρτηση* $f : R \to S$ *είναι ομομορφισμός δακτυλίων όταν για κάθε* $a, b \in R$*:*

$$f(a + b) = f(a) + f(b) \;\; \text{και} \;\; f(ab) = f(a)f(b)$$

Ορισμός 1.1.3. *Αν* R *δακτύλιος και* $I \subset R$*, τότε* I *ιδεώδες αν* $(I, +)$ *υποομάδα του* $(R, +)$ *και* $ra \in I$, $ar \in I$ *για κάθε* $r \in R$ *και* $a \in I$*.*

Θεώρημα 1.1.4. *Έστω* $\phi : R \to S$ *ένας ομομορφισμός δακτυλίων και* R, S *δύο δακτύλιοι. Τότε*

$$R/ker\phi \cong Im\phi, \;\; r + ker\phi \mapsto \phi(r)$$

είναι ένας ισομορφισμός δακτυλίων.

Θεώρημα 1.1.5 (2ο Θεώρημα Ισομορφισμού)**.** *Έστω* I, J *δύο ιδεώδη ενός δακτυλίου* R*. Τότε υπάρχει ένας ισομορφισμός δακτυλίων* $I/I \cap J \cong (I + J)/J$*.*

Θεώρημα 1.1.6 (3ο Θεώρημα Ισομορφισμού). *Έστω I,J ιδεώδη ενός δακτυλίου R με $I \subseteq J$. Τότε το J/I είναι ένα ιδεώδες του R/I και υπάρχει ένας ισομορφισμός δακτυλίων $(R/I)/(J/I) \cong R/J$.*

Ορισμός 1.1.7. *Έστω X υποσύνολο δακτυλίου R. Έστω $\{A_i : i \in I\}$ η οικογένεια όλων των (αριστερών) ιδεωδών του R που περιέχουν το X.*

(i) *Το ελάχιστο στοιχείο της οικογένειας ονομάζεται το (αριστερό) ιδεώδες που παράγεται από το X και συμβολίζεται με (X). Τα στοιχεία του X λέγονται γεννήτορες του ιδεώδους (X).*

(ii) *Αν $X = \{x_1, \ldots, x_n\}$, τότε το ιδεώδες (X) συμβολίζεται με $(x_1, \ldots, x_n)$ και λέμε ότι είναι πεπερασμένα παραγόμενο.*

(iii) *Ένα ιδεώδες (x) που παράγεται από ένα στοιχείο λέγεται κύριο ιδεώδες.*

(iv) *Ένας δακτύλιος κύριου ιδεώδους είναι ένας δακτύλιος όπου κάθε ιδεώδες είναι κύριο.*

(v) *Ένας δακτύλιος κύριου ιδεώδους ο οποίος είναι ακέραια περιοχή λέγεται περιοχή κύριου ιδεώδους.*

Παρατήρηση 1.1.8 (Ιδιότητες). *Έστω R ένας δακτύλιος, $\alpha \in R$ και $X \subset R$. Τότε:*

(i) *Το κύριο ιδεώδες (α) περιέχει όλα τα στοιχεία της μορφής*
$$r\alpha + s\alpha + n\alpha + \sum_{i=1}^{m} r_i \alpha s_i,$$
όπου $r, s, r_i, s_i \in R$, $m \in \boldsymbol{N} - 0$ και $n \in \boldsymbol{Z}$).

(ii) *Αν R έχει μονάδα, τότε*
$$(\alpha) = \left\{ \sum_{i=1}^{m} r_i \alpha s_i : r_i, s_i \in R, n \in \boldsymbol{N} - 0 \right\}.$$

(iii) *Αν α ανήκει στο κέντρο του R, τότε*
$$(\alpha) = \{r\alpha + n\alpha : r \in R, n \in \boldsymbol{Z}\}.$$

(iv) *$R\alpha = \{r\alpha : r \in R\}$ (αντίστοιχα $\alpha R = \{\alpha r : r \in R\}$) είναι ένα αριστερό (αντ. δεξί) ιδεώδες στο R (που ίσως να μην περιέχει το α). Αν ο R έχει μονάδα, τότε $\alpha \in R\alpha$ και $\alpha \in \alpha R$.*

(v) *Αν ο R έχει μονάδα και a ανήκει στο κέντρο του, τότε $R\alpha = (\alpha) = \alpha R$.*

(vi) *Αν R έχει μονάδα και X ανήκει στο κέντρο του R, τότε το ιδεώδες (X) περιέχει όλα τα πεπερασμένα αθροίσματα*
$$r_1\alpha_1 + ... + r_n\alpha_n (n \in \boldsymbol{N} - 0, r_i \in R, \alpha_i \in X).$$

Ορισμός 1.1.9. *Έστω R δακτύλιος. Ένα (αριστερό) R-module είναι μια προσθετική αβελιανή ομάδα A μαζί με μια συνάρτηση $R \times A \mapsto A((r, a) \mapsto ra)$ τέτοια ώστε $\forall r, s \in R$ και $\forall a, b \in A$:*

(i) $r(a+b) = ra + rb$

(ii) $(r+s)a = ra + sa$

(iii) $R(sa) = (rs)a$
Αν ο R έχει μοναδιαίο στοιχείο 1_R και

(iv) $1_R a = a, \forall a \in A$, *τότε A ονομάζεται μοναδοειδές R-module.*

Ορισμός 1.1.10. *Έστω R ένας δακτύλιος, A ένα R-module και B ένα μη κενό υποσύνολο του A. Τότε το B ονομάζεται ένα submodule του A αν B είναι μια προσθετική υποομάδα του A και $rb \in B$, $\forall r \in R$, $\forall b \in B$.*

Παρατήρηση 1.1.11. *Ένα κυκλικό module που παράγεται από το στοιχείο $a \in R$ ορίζεται ως:*

(i) *Το αριστερό κυκλικό R-module ορίζεται ως Ra.*

(ii) *Το δεξί κυκλικό R-module ορίζεται ως aR.*

(iii) *Το δίπλευρο κυκλικό R-module ορίζεται ως RaR.*

Ορισμός 1.1.12. *Το σύνολο $X \subset F$ του μονοειδούς R-module ονομάζεται βάση του F, αν κάθε στοιχείο του F μπορεί να γραφτεί, μοναδικά, σαν ένας πεπρασμένος γραμμικός συνδυασμός στοιχείων του X.*

Παρατήρηση 1.1.13. *Το σύνολο X είναι βάση τοψ F αν και μόνο αν είναι γραμμικά ανεξάρτητο και παράγει το F. Οι ορισμοί είναι ίδιοι μ΄ αυτούς στους διανυσματικούς χώρους.*

Λήμμα 1.1.14. *Έστω R είναι δακτύλιος με μονάδα και $x \in R$. Τότε το Rx είναι αριστερό module και η συνάρτηση*

$$f : R \to R, \;\; f(r) = rx,$$

είναι επιμορφισμός.

Απόδειξη. Είναι προφανές ότι το Rx είναι αριστερό R-module. Επίσης είναι προφανές ότι ο f είναι ομομορφισμός. Για να δείξουμε ότι ο f είναι επί, έστω $rx \in Rx$. Τότε $f(r) = rx$. □

Θεώρημα 1.1.15. *Έστω R ένας δακτύλιος με μονάδα. Οι παρακάτω συνθήκες σε ένα μοναδοειδές αριστερό R-module F είναι ισοδύναμα:*

(i) *F έχει μια μη κενή βάση*

(ii) *F είναι το ευθύ γινόμενο μιας οικογένειας κυκλικών αριστερών R-modules, το καθένα από τα οποία είναι ισόμορφο με το αριστερό R-module R.*

(iii) *F είναι ένα R-module ισομορφικό με ένα ευθύ άθροισμα από αντίγραφα του αριστερού R-module R*

(iv) *υπάρχει ένα μη κενό σύνολο X και μια συνάρτηση $i : X \to F$ με την παρακάτω ιδιότητα: δεδομένου οποιουδήποτε μοναδοειδούς R-module A και $f : X \to A$, να υπάρχει ένας μοναδικός R-module ομομορφισμός $f' : F \to A$ τέτοιος ώστε $f'i = f$. Δηλαδή, F να είναι ένα ελεύθερο αντικείμενο στην κατηγορία μοναδοειδών R-modules.*

Ένα μοναδοειδές module F σε έναν δακτύλιο R με μονάδα, το οποίο ικανοποιεί το παραπάνω θεώρημα λέγεται ελεύθερο R-module στο σύνολο X.

Απόδειξη. Θα εξετάσουμε την περίπτωση που το X είναι πεπρασμένο. Έστω $X = \{x_1, x_2, \ldots, x_n\}$.
(i) $\Rightarrow$ (ii). Ορίζουμε

$$f : R \to \bigoplus_{i=1}^{n} Rx_i, \quad f(r) = a_1x_1 + \cdots + a_nx_n$$

όπου $r = a_1x_1 + \cdots + a_nx_n$. Επειδή η παράσταση αυτή του r είναι μοναδική, η f είναι καλά ορισμένη. Είναι προφανές ότι η f είναι επιμορφισμός. Η μοναδικότητα της έκφρασης αποδεικνύει ότι είναι 1-1 και συνεπώς είναι ισομορφισμός. Το Λήμμα 1.1.14 δείχνει ότι ο κάθε όρος είναι ισόμορφος με το R.
(ii) $\Rightarrow$ (iii). Προφανές.
(iii) $\Rightarrow$ (iv). Ορίζουμε $i : X \to F$ ως την φυσική εμφύτευση. Έστω

$$g : F \to \oplus_{i=1}^{n} R_i$$

ο ισομορφισμός με αριστερά R-modules ισομορφικά με το R. Τότε εάν έχουμε την f, ορίζουμε, για $g(r) = a_1 + \cdots + a_n x$,

$$f'(r) = a_1 f(x_1) + \cdots + a_n f(x_n).$$

Είναι προφανές ότι η συνάρτηση f' ικανοποιεί τις συνθήκες.
(iv) $\Rightarrow$ (i). Έστω G είναι το ευθύ άθροισμα αντίγραφων του R, ένα για κάθε στοιχείο του X. Τότε το G είναι το ελεύθερο αντικείμενο στα modules. Επειδή το ελεύθερο αντικείμενο είναι μοναδικό, το G είναι ισόμορφο με το F. $\square$

Ορισμός 1.1.16. *Έστω R είναι δακτύλιος με μονάδα. Υποθέτουμε ότι για κάθε ελεύθερο module F κάθε βάση έχει την ίδια πληθικότητα. Τότε λέμε ότι ο R έχει την ιδιότητα της αναλλοίωτης διάστασης και η πληθικότητα κάθε βάσης του F ονομάζεται βαθμός του F (rank(F)).*

Ορισμός 1.1.17. *Ένα ιδεώδες P σε έναν δακτύλιο R λέγεται πρώτο αν $P \neq R$ και για κάθε ιδεώδη $A, B \in R$*

$$AB \subset P \Rightarrow A \subset P \;\text{ ή }\; B \subset P.$$

Ορισμός 1.1.18. *Ένα ιδεώδες M λέγεται μέγιστο σε έναν δακτύλιο R αν $M \neq R$ και για κάθε ιδεώδες N τ.ω $M \subset N \subset R$, είτε $N = M$ είτε $N = R$.*

Ορισμός 1.1.19. *Έστω R ένας αντιμεταθετικός δακτύλιος με μονάδα. Ένα στοιχείο c του R είναι ανάγωγο αν c έιναι μη μηδενικό και μη μοναδιαίο και $c = ab \Rightarrow a$ ή b είναι μια μονάδα .*
Ένα στοιχείο p του R είναι πρώτο αν p είναι μη μηδενικό - μη μοναδιαίο και $p \mid ab \Rightarrow p \mid a$ ή $p \mid b$.

Ορισμός 1.1.20. *Ακριβής διασπαστική ακολουθία είναι μια σύντομη ακριβής ακολουθία η οποία ικανοποιεί τις παρακάτω ισοδυναμίες: Αν R δακτύλιος και $0 \to A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \to 0$ μία σύντομη ακριβής ακολουθία R-module ισομορφισμών τότε:*

(i) *Υπάρχει ένας R-module ομομορφισμός $h : A_2 \to B$ με $gh = 1_{A_2}$*

(ii) *Υπάρχει ένας R-module ομομορφισμός $k : B \to A_1$ με $kf = 1_{A_1}$*

(iii) *Η δοσμένη ακολουθία είναι ισομορφική με το ευθύ άθροισμα σύντομης α-κριβής ακολουθίας $0 \to A_1 \xrightarrow{\iota_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \to 0$, συγκεκριμένα $B \cong A_1 \oplus A_2$.*

Ορισμός 1.1.21. *Έστω $\{N_i \mid i \in I\}$ η οικογένεια κανονικών υποομάδων μιας ομάδας G τέτοια ώστε $G =< \cup_{i\in I} N_i >$ και για κάθε $k \in I$, $N_k \cap < \cup_{i\in I} N_i > = < e >$. Τότε G λέμε ότι είναι το εσωτερικό ευθύ άθροισμα της οικογένειας $\{N_i \mid i \in I\}$.*

Ορισμός 1.1.22. *Ένα (αριστερό) ιδεώδες I του R τέτοιο ώστε $I \neq 0$ και $I \neq R$ λέγεται κατάλληλο (αριστερό) ιδεώδες.*

Θεώρημα 1.1.23. *Έστω F ένα ελεύθερο module σε περιοχή κύριου ιδεώδους R και G ένα submodule του F. Τότε G είναι ένα ελεύθερο R-module και $rankG \leq rankF$.*

Απόδειξη. Έστω $\{x_i \mid i \in I\}$ να είναι μια βάση του F. Τότε $F = \sum_{i\in I} Rx_i$ με κάθε Rx_i ισομορφικό με το R (ως ένα αριστερό R-module). Διαλέγω μια καλή διάταξη $\leq$ του συνόλου I. Για κάθε $i \in I$ συμβολίζω τον άμεσο διάδοχο (Ο άμεσος διάδοχος του $a \in A$ όπου $(A, \leq)$ γραμμικά διατεταγμένο σύνολο είναι το ελάχιστο στοιχείο του συνόλου $\{x \in A \mid a < x\}$) του i με $i+1$. Έστω $J = I \cup \{a\}$, όπου a δεν ανήκει στο I και από ορισμό $i < a$ για κάθε $i \in I$. Τότε J είναι καλά ορισμένο και κάθε στοιχείο του I έχει άμεσο διάδοχο στο J. Για κάθε $j \in J$ ορίζουμε F_j να είναι το submodule του F που παράγεται από το σύνολο $\{x_i \mid i < j\}$. Τα submodules F_j έχουν τις παρακάτω ιδιότητες :

(i) $j < k \Leftrightarrow F_j \subset F_k$

(ii) $\cup_{j\in J} F_j = F$

(iii) για κάθε $i \in I$, $F_{i+1}/F_i \cong Rx_i \cong R$
Για κάθε $j \in J$ έστω $G_j = G \cap F_j$ και ισχύει ότι :

(iv) $j < k \Rightarrow G_j \subset G_k$

(v) $\cup_{j\in J} G_j = G$

(vi) για κάθε $i \in I$, $G_i = G_{i+1} \cap F_i$

Η ιδιότητα (vi) και η ιδιότητα ότι αν B και C είναι δύο submodules του A επί ενός δακτυλίου R τότε υπάρχει ένας R-module ισομορφισμός με $B/(B \cap C) \cong (B + C)/C$ μας επάγει ότι $G_{i+1}/G_i = G_{i+1}/(G_{i+1} \cap F_i) \cong (G_{i+1} + F_i)/F_i)$. Αλλά $(G_{i+1} + F_i)/F_i$ είναι ένα submodule του F_{i+1}/F_i. Άρα, G_{i+1}/G_i είναι ισομορφικό με ένα submodule του R από την ιδιότητα (iii). Αλλά κάθε submodule του R είναι απαραίτητα ένα ιδεώδες του R και έτσι της μορφής $(c) = Rc$ για κάποιο $c \in R$. Αν $c \neq 0$, τότε ο R-module επιμορφισμός $R \to Rc$ είναι στην πραγματικότητα ένας ισομορφισμός. Έτσι κάθε submodule του R (και έτσι κάθε G_{i+1}/G_i) είναι ελεύθερο βαθμού 0 ή 1. Από 1.1.26 και 1.1.28 η ακολουθία $0 \to G_i \xrightarrow{\subseteq} G_{i+1} \to G_{i+1}/G_i \to 0$ είναι ακριβής διασπαστική για κάθε $i \in I$. Έχουμε ότι G_{i+1} είναι ένα εσωτερικό ευθύ άθροισμα $G_{i+1} = G_i \oplus Rb_i$, όπου

$b_i \in G_{i+1} - G_i$ και $Rb_i \cong R$ αν $G_{i+1} \neq G_i$, και $b_i = 0$ αν $G_{i+1} = G_i$. Έτσι $b_i \in G$ είναι ορισμένο για κάθε $i \in I$. Έστω $B = \{b_i \mid b_i \neq 0\}$. Τότε $\mid B \mid \leq \mid I \mid = rankF$. Για να ολοκληρωθεί η απόδειξη χρειάζεται να δείξουμε ότι το B είναι μια βάση του G. Έστω $u = \sum_j r_j b_j = 0$. Έστω k να είναι ο μεγαλύτερος δείκτης τέτοιος ώστε $r_k \neq 0$. Τότε $u = \sum_{j<k} r_j b_j + r_k b_k \in G_k \oplus Rb_k = G_{k+1}$. Αλλά $u = 0$ συνεπάγεται ότι $r_k = 0$, το οποίο είναι άτοπο. Οπότε $r_j = 0$ για κάθε j. Άρα, B είναι γραμμικά ανεξάρτητο. Έτσι δείχνοντας ότι το B καλύπτει το G καταλήγουμε ότι B είναι μία βάση του G και ολοκληρώνεται η απόδειξη. □

Πόρισμα 1.1.24. *Έστω R μια περιοχή κύριου ιδεώδους. Αν A είναι ένα πεπερασμένα παραγόμενο R-module παραγόμενο από n στοιχεία, τότε κάθε submodule του A παράγεται από m στοιχεία με $m \leq n$.*

Ορισμός 1.1.25. *Ένα module P ενός δακτυλίου R λέγεται προβολικό (projective) εάν δοθέντος οποιουδήποτε διαγράμματος R-module ομομορφισμών έχουμε*

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

Για την απόδειξη του παρακάτω πορίσματος θα χρειαστούμε τα εξής αποτελέσματα (χωρίς απόδειξη) :

Παρατήρηση 1.1.26. *Κάθε ελεύθερο module F επί ενός δακτυλίου R με μονάδα είναι προβολικό.*

Θεώρημα 1.1.27. *Κάθε (μοναδιαίο) module A επί ενός δακτυλίου R (με μονάδα) είναι η ομομορφική εικόνα ενός ελεύθερου R-module F. Αν A είναι πεπερασμένα παραγόμενο, τότε F μπορεί να επιλεγεί ως πεπερασμένα παραγόμενο.*

Απόδειξη. Έστω X να είναι το σύνολο των γεννητόρων του A και F το ελεύθερο R-module του X. Τότε η απεικόνιση $X \to A$ επάγει έναν R-module ομομορφισμό $f : X \to A$ τέτοιο ώστε $X \subset Imf$. Αφού X παράγει το A, πρέπει να έχουμε $Imf = A$. □

Παρατήρηση 1.1.28. *Έστω R δακτύλιος. Οι παρακάτω συνθήκες σε ένα R-module P είναι ισοδύναμες.*

(i) *P προβολικό*

(ii) *κάθε βραχεία ακριβής ακολουθία $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ είναι ακριβής διάσπαση (και έτσι $B \cong A \oplus P$).*

(iii) *υπάρχει ένα ελεύθερο R-module F και ένας R-module K τέτοιος ώστε $F \cong K \oplus P$.*

Πόρισμα 1.1.29. *Ένα μοναδιαίο module A σε μια περιοχή κύριου ιδεώδους είναι ελεύθερο αν και μόνο αν A προβολικό.*

Απόδειξη. ($\Rightarrow$) Θεώρημα 1.1.26.
($\Leftarrow$) Υπάρχει μια βραχεία ακριβής ακολουθία

$$0 \to K \xrightarrow{\subseteq} F \xrightarrow{f} A \to 0$$

με F ελεύθερο, f επιμορφισμός και $K = \ker f$ (Θεώρημα 1.1.27). Αν A είναι προβολικό, τότε $F \cong K \oplus A$ (Θεώρημα 1.1.28). Έτσι, A είναι ισομορφικό με ένα submodule του F, άρα το A είναι ελεύθερο (Θεώρημα 1.1.23). □

1.2 Modules

Για την απόδειξη του επόμενου θεωρήματος θα χρειαστούμε τα εξής:

Θεώρημα 1.2.1. *Έστω R δακτύλιος και A ένα (αριστερό) R-module, X ένα υποσύνολο του A, και $a \in A$. Έστω $Ra = \{ra \mid r \in R\}$. Τότε Ra είναι ένα submodule του A και η απεικόνιση $R \to Ra$ με $r \mapsto ra$ είναι ένας R-module επιμορφισμός.*

Απόδειξη. Υπόδειξη : Αν R έχει μονάδα 1_R και A είναι μοναδιαίο, τότε $n1_R \in R$ για κάθε $n \in Z$ και $na = (n1_R)a$ για κάθε $a \in A$. □

Θεώρημα 1.2.2. *Αν R είναι ένας δακτύλιος και $f : A \to B$ R-module ομομορφισμός και C ένα submodule του $\ker f$, τότε υπάρχει ένας μοναδικός R-module ομομορφισμός $f' : A/C \to B$ τέτοιος ώστε $f'(a + C) = f(a)$ $\forall a \in A$: $Imf' = Imf$ και $\ker f' = \ker f/C$, f' είναι ένας R-module ισομορφισμός αν-ν f είναι ένα R-module επιμορφισμός και $C = \ker f$. Συγκεκριμένα, $A/\ker f \cong Imf$.*

Απόδειξη. Υπόδειξη :1.1.4 και αν $f : G \to H$ είναι ομομορφισμός ομάδων και N κανονική υποομάδα του G που περιέχεται στον πυρήνα της f, τότε υπάρχει ένας μοναδικός ομομορφισμός $f' : G/N \to H$ τέτοιος ώστε $f'(aN) = f(a)$ για κάθε $a \in G$. $Imf = Imf'$ και $\ker f' = (\ker f)/N$. f' είναι ένας ισομορφισμός αν f είναι επιμορφισμός και $N = \ker f$. □

Ορισμός 1.2.3. *Μια ακέραια περιοχή R είναι μια περιοχή μοναδικής παραγοντοποίησης αν:*

(i) *κάθε μη μηδενικό και μη μοναδιαίο στοιχείο a του R μπορεί να γραφεί ως $a = c_1 \cdots c_n$ με $c_1, \ldots, c_n$ ανάγωγα.*

(ii) *Αν $a = c_1 \cdots c_n$ και $a = d_1 \cdots d_m$ (c_i, d_i ανάγωγα), τότε $n = m$ και για κάποια μετάθεση σ του $\{1, 2, \ldots, n$, c_i και $d_{\sigma(i)}$ είναι συνεργάτες, δηλαδή $c_i/d_{\sigma(i)}$ και $d_{\sigma(i)}/c_i$.*

Θεώρημα 1.2.4. *Κάθε περιοχή κύριου ιδεώδους R είναι μια περιοχή μοναδικής παραγοντοποίησης.*

Απόδειξη. Υπόδειξη : Έστω R δακτύλιος. Ένα ευθύ άθροισμα από R-modules $\sum_{i \in I} P_i$ είναι προβολικό αν-ν κάθε P_i είναι προβολικό. □

Θεώρημα 1.2.5. *Έστω a, b και u να είναι στοιχεία ενός αντιμεταθετικού δακτυλίου R με μονάδα.*

(i) *a/b ανν $(b) \subset (a)$,*

(ii) *a και b συνεργάτες αν-ν $(a) = (b)$*

(iii) *u είναι μονάδα αν-ν $u/r, \forall r \in R$*

(iv) *u είναι μια μονάδα αν-ν $(u) = R$*

(v) *Η σχέση 'a είναι συνεργάτης του b' είναι ισοδύναμη σχέση στο R*

(vi) *Αν $a = br, r \in R$ μια μονάδα, τότε a και b είναι συνεργάτες. Αν R είναι ακέραια περιοχή ισχύει και το αντίστροφο.*

Απόδειξη. Από 1.1.8 □

Θεώρημα 1.2.6. *Έστω A ένα αριστερό module σε μια ακέραια περιοχή R και $\forall a \in A$ έστω $O_a = \{r \in R \mid ra = 0\}$*

(i) *O_a είναι ιδεώδες του R $\forall a \in A$*

(ii) *$A_t = \{a \in A \mid O_a \neq 0\}$ είναι submodule του A.*

(iii) *$\forall a \in A$ υπάρχει ισομορφισμός από απιστερά modules*

$$R\ O_a \cong Ra = \{ra \mid r \in R\}$$

Έστω R περιοχή κύριου ιδεώδους και $p \in R$ πρώτος.

(iv) *Αν $p^i a = 0 \Rightarrow O_a = (p^j)$ με $0 \leqslant j \leqslant i$*

(v) *Αν $O_a = (p^i) \Rightarrow p^j a \neq 0, \forall j$ ώστε $0 \leqslant j \leqslant i$*

Απόδειξη. Το (iii) Συνεπάγεται από τα 1.2.1 και 1.2.2 . (iv) Από υπόθεση $O_a = (r)$ για κάποια $r \in R$. Αφού $p^i \in O_a$, r διαιρεί το p^i. Η μοναδική παραγοντοποίηση στο R 1.2.4 συνεπάγει ότι $r = p^i u$ με $0 \leq j \leq i$ και u μια μονάδα. Ως εκ τούτου, $O_a = (r) = (p^i u) = (p^i)$ 1.2.5. (v) Αν $P^i a = 0$, $J < i$, τότε $p^i \in O_a = (p^i)$, όπου p^i/p_j. Άτοπο! από μοναδική παραγοντοποίηση στο R. □

Έστω A ένα module σε μια ακέραια περιοχή. Το ιδεώδες O_a του προηγούμενου θεωρήματος λέγεται κανονικό ιδεώδες του $a \in A$. Το submodule A_t του προηγούμενου θεωρήματος λέγεται submodule στρέψης του A. Το A λέγεται module στρέψης αν $A = A_t$ και είναι ελεύθερο στρέψης αν $A_t = 0$. Κάθε ελεύθερο module είναι ελεύθερη στρέψη, αλλά όχι το ανάποδο. Το ταξικό ιδεώδες του $a \in A$ είναι ένα πρωταρχικό ιδεώδες του R, έστω $O_a = (r)$, και a λέμε οτι έχει τάξη r.

Θεώρημα 1.2.7. *Ένα πεπερασμένα παραγόμενο ελεύθερης στρέψης module A επί μιας περιοχής κύριου ιδεώδους R είναι ελεύθερο.*

Απόδειξη. Υποθέτουμε ότι $A \neq 0$. Έστω X ένα πεπερασμένο σύνολο μη κενών παραγόντων του A. Αν $x \in X$, τότε $rx = 0 (r \in R)$ αν και μόνο αν $r = 0$ αφού A είναι ελεύθερη στρέψη. Συνεπώς, υπάρχει ένα μη κενό υποσύνολο $S = \{x_1, \ldots, x_k\}$ του X που είναι μέγιστο και ικανοποιεί την ιδιότητα:

$$r_1 x_1 + \cdots + r_k x_k = 0 \ \ (r_i \in R) \Rightarrow r_i = 0, \forall i.$$

Το submodule F που παράγεται από το S είναι ένα ελεύθερο R-module με βάση το S. Αν $y \in X - S$, τότε αφού μέγιστη υπάρχουν $r_y, r_1, \ldots, r_k \in R$,όχι όλα μηδέν, τέτοια ώστε $r_y y + r_1 x_1 + \cdots + r_k x_k = 0$. Τότε $r_y y = -\sum_{i=1}^{k} r_i x_i \in F$. Επιπλέον,$r_y \neq 0$ αλλιώς $r_i = 0, \forall i$. Αφού X είναι πεπεράσμενο, υπάρχει ένα μη μηδενικό $r \in R$ τέτοιο ώστε $rX = \{rx \mid x \in X\}$ να περιέχεται στο F. Επομένως, $rA = \{ra \mid a \in A\} \subset F$. Η απεικόνιση $f : A \to A$ όπου $a \mapsto ra$ βλέπουμε εύκολα ότι είναι ένας R-module ομομορφισμός με εικόνα rA. Αφού A είναι ελεύθερης στρέψης $\ker f = 0$, έτσι $A \cong Imf = rA \subset F$. Έτσι, A είναι ελεύθερο από 1.1.23. □

Θεώρημα 1.2.8. *Αν A είναι ένα πεπερασμένα παραγόμενο module επί μιας περιοχής κύριου ιδεώδους R, τότε $A = A_t \oplus F$, όπου F είναι ένα ελεύθερο R-module πεπερασμένης τάξης και $F \cong A/A_t$.*

Απόδειξη. Το πηλίκο module A/A_i είναι ελεύθερης στρέψης αφού για κάθε $r \neq 0$,

$$r(a + A_t) = A_t \Rightarrow ra \in A_t \Rightarrow r_1(ra) = 0$$

για κάποιο $r_1 \neq 0 \Rightarrow a \in A_t$ Επιπλέον, A/A_t είναι πεπερασμένα παραγόμενο αφού είναι και το A. Έτσι, A/A_t είναι ελεύθερο πεπερασμένης τάξης από το προηγούμενο θεώρημα. Συνεπώς, η ακριβής ακολουθία $0 \to A_t \xrightarrow{\subseteq} A \to A/A_t \to 0$ είναι ακριβής διάσπαση και $A \cong A_t \oplus A/A_t$ 1.1.26, 1.1.28. Υπό τον ισομορφισμό $A_t \oplus A/A_t \cong A$ η εικόνα του A_t είναι A_t και η εικόνα του A/A_t είναι ένα submodule F του A, το οποίο είναι αναγκαστικά ελεύθερο πεπερασμένου βαθμού. Ακολουθεί ότι A είναι το εσωτερικό ευθύ άθροισμα $A = A_t \oplus F$. □

Για την απόδειξη του 1.2.11 θα χρειαστούμε τα εξής:
Θυμίζω ότι μέγιστος κοινός διαιρέτης d τότε $d/a, \quad \forall a \in X$ και $c/a, \forall a \in X$ τότε c/d.

Θεώρημα 1.2.9. *Έστω $a_1, \dots, a_n$ να είναι στοιχεία ενός αντιμεταθετικού δακτυλίου R με μονάδα:*

(i) *$d \in R$ είναι ένας μέγιστος κοινός διαίρέτης του $\{a_1, \dots, a_n\}$ τέτοιος ώστε $d = r_1a_1 + \dots + r_na_n$, για κάποιο $r_i \in R$ αν-ν $(d) = (a_1) + \dots + (a_n)$*

(ii) *αν R δακτύλιος κύριου ιδεώδους, τότε ένας μέγιστος κοινός διαιρέτης των $a_1, \dots, a_n$ υπάρχει και καθένας είναι της μορφής $r_1a_1 + \dots + r_na_n (r_i \in R)$*

(iii) *αν R είναι μια περιοχή μοναδικής παραγοντοποίησης, τότε υπάρχει ένας μέγιστος κοινός διαιρέτης των $a_1, \dots, a_n$.*

Απόδειξη. Ιδέα απόδειξης : (i) Χρησιμοποιώντας τον ορισμό του μέγιστου κοινού διαιρέτη και το 1.1.8. Το (ii) βγαίνει από το (i). (iii) Κάθε a_i παραγοντοποιείται ως $a_i = c_1^{m_{i1}} c_2^{m_{i2}} \cdots c_t^{m_{it}}$ με $c_1, \dots, c_t$ διακεκριμένα ανάγωγα στοιχεία και κάθε $m_{ij} \geq 0$. Δείξτε ότι $d = c_1^{k_1} \cdots c_t^{k_t}$ είναι ένας μέγιστος κοινός διαιρέτης των $a_1, \dots, a_n$ όπου $k_j = \min\{m_{1j}, \dots, m_{nj}\}$. □

Θεώρημα 1.2.10. *Έστω R δακτύλιος και $\{A_i \mid i \in I\}$ μια οικογένεια από submodules ενός R-submodule A τέτοια ώστε:*

(i) *A είναι το άθροισμα της οικογένειας $\{A_i \mid i \in I\}$*

(ii) *$\forall k \in I, A_k \cap A'_k = 0$, όπου A'_k είναι το άθροισμα της οικογένειας $\{A_i \mid i \neq k\}$. Τότε υπάρχει ένας ισομορφισμός $A \cong \sum_{i \in I} A_i$.*

Απόδειξη. Υπόδειξη : Έστω $\{N_i \mid i \in I\}$ να είναι μια οικογένεια κανονικών υποομάδων μια ομάδας G τέτοια ώστε $G =< \cup_{i \in I} N_i >$ και για κάθε $k \in I$, $N_k \cap < \cup_{i \neq k} N_i >=< e >$, τότε $G \cong \prod_{i \in I}^{w} N_i$. □

Θεώρημα 1.2.11. *Έστω A ένα module στρέψης επί μιας περιοχής κύριου ιδεώδους R και κάθε πρώτος $p \in R$ ώστε $A(p) = \{a \in A \mid a$ έχει τάξη μια δύναμη του $p\}$*

(i) *$A(p)$ είναι submodule του A, $\forall p \in R$ πρώτο.*

(ii) $A = \sum A(p)$, *όπου το άθροισμα είναι επί των πρώτων* $p \in R$.

Απόδειξη. (*i*) Έστω $a, b \in A(p)$. Αν $O_a = (p^r)$ και $O_b = (p^s)$ έστω $k = \max(r, s)$. Τότε, $p^k(a+b) = 0$, όπου $O_{a+b} = (p^i)$ με $0 \le i \le k$ 1.2.6. Έτσι, $a, b \in A(p)$ συνεπάγεται $a + b \in A(p)$. Με παρόμοιο επιχείρημα δείχνουμε ότι $a \in A(p)$ και $r \in R$ συνεπάγουν $ra \in A(p)$. Έτσι, $A(p)$ είναι submodule. (*ii*) Έστω $0 \neq a \in A$ με $O_a = (r)$. Από 1.2.4 $r = p_1^{n_1} \cdots p_k^{n_k}$ με p διακεκριμένοι πρώτοι στο R και κάθε $n_i > 0$. Για κάθε i, έστω $r_i = p_1^{n_1} \cdots p_{i-1}^{n_i-1} \cdot p_{i+1}^{n_i+1} \cdots p_k^{n_k}$. Τότε $r_1, \ldots, r_k$ είναι σχετικά πρώτοι και υπάρχουν $s_1, \ldots, s_k \in R$ τέτοια ώστε $s_1 r_1 + \cdots + s_k r_k = 1_R$ (1.2.9). Επομένως, $a = 1_R a = s_1 r_1 a + \cdots + s_k r_k a$. Αλλά $p_i^{n_i} s_i r_i a = s_i r a = 0$, όπου $s_i r_i a \in A(p_i)$. Έχουμε αποδείξει ότι τα submodules $A(p)$ (p- πρώτος) παράγουν το module A. Έστω $p \in R$ πρώτος και έστω A_1 να είναι submodule του A που παράγεται από όλα τα $A(q)$ με $q \neq p$. Έστω $a \in A(p) \cap A_1$. Τότε $p^m a = 0$ για κάποιο $m \geq 0$ και $a = a_1 + \cdots + a_t$ με $a_i \in A(q_1)$ για κάποιους πρώτους $q_1, \ldots, q_t$ όλοι διαφορετικοί από το p. Αφού $a_i \in A(q_i)$, υπάρχουν ακέραιοι m_i τέτοιοι ώστε $q_i^{m_i} a_i = 0$, απ΄ όπου $(q_1^{m_1} \cdots q_t^{m_t})a = 0$. Αν $d = q_1^{m_1} \cdots q_t^{m_t}$, τότε p^m και d είναι σχετικά πρώτοι και $rp^m + sd = 1_R$ για κάποια $r, s \in R$. Επομένως, $a = 1_R a = rp^m a + sda = 0$.Έτσι, $A(p) \cap A_1 = 0$ και $A = \sum A(p)$ από 1.2.10. □

Λήμμα 1.2.12. *Έστω A ένα module επί μιας περιοχής κύριου ιδεώδους R τέτοιο ώστε $p^n A = 0$ και $p^{n-1} A \neq 0$ για κάποιον πρώτο $p \in R$ και θετικό ακέραιο n. Έστω $a \in A$ τάξης p^n.*

(i) *Αν $A \neq Ra$, τότε υπάρχει ένα μη μηδενικό $b \in A$ τέτοιο ώστε $Ra \cap Rb = 0$.*

(ii) *Υπάρχει ένα submodule C του A τέτοιο ώστε $A = Ra \oplus C$.*

Απόδειξη. (*i*) Αν $A \neq Ra$, τότε υπάρχει $c \in A - Ra$. Αφού $p^n c \in p_n A = 0$, υπάρχει ένας ελάχιστος θετικός ακέραιος j τέτοιος ώστε $p^j c \in Ra$: όπου p^{i-1} δεν ανήκει στο Ra και $p^i c = r_1 a (r_1 \in R)$. Αφού R είναι περιοχή μοναδικής παραγοντοποίησης $r_1 = rp^k$ για κάποιο $k \geqslant 0$ και $r \in R$ τέτοιο ώστε $p \nmid r$. Επομένως, $0 = p^n c = p^{n-j}(p^j c) = p^{n-j} rp^k a$. Εφόσον $p \nmid r$ και $p^{n-1} \neq 0$, πρέπει να έχουμε $n - j + k \geqslant n$ 1.2.6, όπου $k \geqslant j \geqslant 1$. Άρα, $b = p^{j-1}c - rp^{k-1}a$ είναι καλά ορισμένο στοιχείο του A. Επιπλέον, $b \neq 0$ (αφού $p^{j-1} \notin Ra$) και $pb = p^j c - rp^k a = p^j c - r_1 a = 0$. Αν $Ra \cap Rb \neq 0$, τότε εκεί υπάρχει $s \in R$ τέτοιο ώστε $sb \in Ra$ και $sb \neq 0$. Αφού $sb \neq 0$ και $pb = 0$, p δεν διαιρεί το s. Άρα, s και p^n είναι σχετικά πρώτοι και $sx + p^n y = 1_R$ για κάποια $x, y \in R$ 1.2.9 . Έτσι εφόσον $p^n A = 0$, $b = 1_R b = sxb + p^n yb = x(sb) \in Ra$. Επομένως, $p^{j-1}c = b + rp^{k-1}a \in Ra$. Αν $j - 1 \neq 0$, αυτό αντίκειται στην ελαχτιστότητα του j, και αν $j - 1 = 0$, αυτό αντίκειται στο γεγονός ότι $c \notin Ra$. Τελικά, $Ra \cap Rb = 0$. (*ii*) Αν $A = Ra$, έστω $C = 0$. Αν $A \neq Ra$, τότε έστω $\mathcal{S}$ το σύνολο όλων των submodules B του A τέτοια ώστε $Ra \cap B = 0$. $\mathcal{S}$ είναι μη κενό απ τη στιγμή που από το πρώτο υποερώτημα υπάρχει ένα μη μηδενικό $b \in A$ τέτοιο ώστε $Ra \cap Rb = 0$. Το $\mathcal{S}$ είναι μερικώς διατεταγμένο από συνολοθεωριτική έγκλειση και κάθε αλυσίδα στο $\mathcal{S}$ έχει ένα άνω όριο στο $\mathcal{S}$. Από το λήμμα του Zorn υπάρχει ένα submodule C του A το οποίο είναι μέγιστο στο $\mathcal{S}$. Θεωρώ το πηλίκο module A/C. Προφανώς $p^n(A/C) = 0$ και $p^n(a + C) = 0$. Αφού $Ra \cap C = 0$ και $p^{n-1} \neq 0$, έχουμε $p^{n-1}(a + C) \neq C$, όπου $a + C$ έχει τάξη p^n στο A/C και $p^{n-1}(A/C) \neq 0$. Τώρα εάν A/C δεν είναι το κυκλικό R-module παραγόμενο από το $a + C$ (αυτό είναι, $A/C \neq R(a + C)$), τότε από το πρώτο υποερώτημα υπάρχει $d + C \in A/C$ τέτοιο ώστε $d + C \neq C$ και $R(a + C) \cap R(d + C) = C$. Αφού $Ra \cap C = 0$, παίρνουμε ότι

$Ra \cap (Rd + C) = 0$. Αφού $d \notin C$, $Rd + C$ είναι μέσα στο $\mathcal{S}$ περιέχει κατάλληλα το C, αυτό έρχεται σε αντίθεση με την μεγιστότητα του C. Έτσι, A/C είναι το κυκλικό R-module παραγόμενο από το $a + C$ (το οποίο είναι, $A/C = R(a + C)$). Επομένως, $A = Ra + C$, όπου $A = Ra \oplus C$ από 1.2.10. □

Θεώρημα 1.2.13. *Έστω A ένα πεπερασμένα παραγόμενο module επί μιας περιοχής κύριου ιδεώδους R τέτοιο ώστε κάθε στοιχείο του A έχει τάξη α δύναμη κάποιου πρώτου $p \in R$. Τότε το A είναι το ευθύ άθροισμα κυκλικών R-modules τάξεων $p^{n_1}, ..., p^{n_k}$ αντίστοιχα, όπου $n_1 \geq n_2 \geq .. \geq n_k \geq 1$.*

Απόδειξη. Η απόδειξη γίνεται με επαγωγή στον αριθμό r από γεννήτορες του A,με την περίπτωση $r = 1$ να είναι μηδαμινή. Αν $r > 1$, τότε A παράγεται από τα στοιχεία $a_1, \ldots, a_r$ των οποίων οι τάξεις είναι αντίστοιχα $p^{n_1}, p^{m_2}, p^{m_3}, \ldots, p^{m_r}$. Υποθέτουμε ότι

$$n_1 = \max n_1, m_2, \ldots, m_r.$$

Τότε $p^{n_1}A = 0$ και $p^{n_1-1}A \neq 0$. Από το προηγούμενο λήμμα υπάρχει ένα submodule C του A τέτοιο ώστε $A = Ra_1 \oplus C$. Έστω π να είναι ο κανονικός επιμορφισμός $\pi : A \to C$. Αφού το A παράγεται από τα $a_1, \ldots, a_r$, το C θα πρέπει να παράγεται από τα $\pi(a_1), \ldots, \pi(a_r)$. Αλλά $\pi(a_1) = 0$, ως εκ τούτου το C μπορεί να παράγεται από $r - 1$ ή και λιγότερα στοιχεία. Επομένως, η επαγωγική υπόθεση συνεπάγει ότι το C είναι το ευθύ άθροισμα από κυκλικά R-modules τάξεων $p^{n_2}, p^{n_3}, \ldots, p^{n_k}$ με $n_2 \geq n_3 \geq \cdots \geq n_k \geq 1$ αντίστοιχα. Έτσι το C περιέχει ένα στοιχείο τάξης n_2. Αφού $p^{n_1}A = 0$, έχουμε $p^{n_1}C = 0$, όπου $n_1 \geq n_2$. Αφού Ra_1 είναι ένα κυκλικό R-module τάξης p^{n_1}, A είναι ευθύ άθροισμα από κυκλικά R-modules τάξεων $p^{n_1}, \ldots, p^{n_k}$ αντίστοιχα με $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$. □

Για την απόδειξη του 1.2.16 θα χρειαστούμε τα παρακάτω:

Λήμμα 1.2.14. *Έστω G αβελιανή ομάδα, m ακέραιος και p πρώτος ακέραιος. Τότε η παρακάτω είναι μια υποομάδα της G: Αν $f : G \to H$ ισομορφισμός τότε οι περιορισμοί της f στα G_t και $G(p)$ αντίστοιχα είναι ισομορφισμοί $G_t \cong H_t$ και $G(p) \cong H(p)$. Με $G(p) = \{u \in G : |u| = p^n, n \geq 0\}$ και $G_t = \{u \in G : |u|$ είναι πεπερασμένη$\}$.*

Απόδειξη. Αν $f : G \to H$ είναι ένας ομομορφισμός και $x \in G(p)$ έχει τάξη p^n, τότε $p^n f(x) = f(p^n x) = f(0) = 0$. Άρα $f(x) \in H(p)$. Έτσι $f : G(p) \to H(p)$. Αν f έιναι ένας ισομορφισμός τότε το ίδιο επιχείρημα δείχνει ότι $f^{-1} : H(p) \to G(p)$. Αφού $ff^{-1} = 1_{H(p)}$ και $f^{-1}f = 1_{G(p)}$, $G(p) \cong H(p)$. □

Θεώρημα 1.2.15. *Αν V είναι διανυσματικός χώρος επί ενός δακτυλίου διάσπασης D και X είναι ένα υποσύνολο που καλύπτει το V τότε X περιέχει μία βάση του V.*

Απόδειξη. Διατάξτε μερικώς το σύνολο Σ όλων των γραμμικά ανεξάρτητων υποσυνόλων του X από έγκλειση. Η λήμμα του Zorn επάγει την ύπαρξη ενός μέγιστου γραμμικά ανεξάρτητου συνόλου Y του X. Κάθε στοιχείο του X είναι ένας γραμμικός συνδυασμός από στοιχεία του Y (αλλιώς μπορούμε να κατασκευάσουμε ένα γραμμικά ανεξάρτητο υποσύνολο του X που περιέχει κατάλληλα το Y και έτσι να έρθουμε σε αντίθεση με τη μεγιστότητα). Αφού X καλύπτει το V, θα τον καλύπτει και το Y. Έτσι, Y βάση του V. □

Λήμμα 1.2.16. *Έστω A, B και $A_i, i \in I$ modules επί μιας περιοχής κύριου ιδεώδους R. Έστω $r \in R$ και έστω $p \in R$ πρώτος.*

(i) $rA = \{ra \mid a \in A\}$ *και* $A[r] = \{a \in A \mid ra = 0\}$ *είναι submodules του* A.

(ii) $R/(p)$ *είναι ένα* $field$ *και* $A[p]$ *είναι ένας διανυσματικός χώρος επί του* $R/(p)$.

(iii) $\forall n$ *φυσικό* $\exists R$*-modules ισομορφισμοί*

$$(R/(p^n))[p] \cong R/(p) \ \ \text{και} \ \ p^m(R/(p^n)) \cong R/(p^{n-m}), \ \ 0 \leq m < 1$$

(iv) *Αν* $A \cong \sum_{i \in I} A_i$, *τότε* $rA \cong \sum_{i \in I} rA_i$ *και* $A[r] \cong \sum_{i \in I} A_i[r]$.

(v) *Αν* $f : A \to A$ *είναι ένας R-module ισομορφισμός, τότε* $f : A_t \cong B_t$ *και* $f : A(p) \cong B(p)$

Απόδειξη. (v) Από 1.2.14 (iii) Έχουμε ότι $(R/(p^n))[p]$ παράγεται ως ένα R-module (και έτσι ως ένας διανυσματικός χώρος επί του $R/(p)$) από το απλό μη μηδενικό στοιχείο $p^{n-1} + (p^n)$. Άρα, $(R/(p^n))[p] \cong R/(p)$ από 1.2.15 και 1.1.15. Το submodule του $R/(p^n)$ που παράγεται από το $p^m + (p^n)$ είναι ακριβώς $p^m(R/(p^n))$. Αφού $p^m + (p^n)$ έχει τάξη p^{n-m}, έχουμε $p^m(R/(p^n)) \cong R/(p^{n-m})$ από 1.2.6. □

Για την απόδειξη του 1.2.19 θα χρειαστούμε τα εξής:

Πόρισμα 1.2.17. *Αν* R *δακτύλιος και* A' *είναι ένα submodule του* R*-module* A *και* B' *ένα submodule του* R*-module* B *και* $f : A \to B$ *είναι ένας* R*-module ομομορφισμός τέτοιος ώστε* $f(A') \subset B'$, *τότε* f *επάγει έναν* R*-module ομομορφισμό* $g : A/A' \to B/B'$ *με* $a + A' \mapsto f(a) + B'$. *Η* g *είναι ένας* R*-module ισομορφισμός αν-ν* $Imf + B' = B$ *και* $f^{-1}(B') \subset A'$. *Συγκεκριμένα, αν* f *είναι ένας επιμορφισμός τέτοιος ώστε* $f(A') = B'$ *και* $\ker f \subset A'$, *τότε* g *είναι ένας* R*-module ισομορφισμός.*

Απόδειξη. Υπόδειξη : Αν $f : G \to H$ είναι ένας ομομορφισμός ομάδων, $N \lhd G, M \lhd H$ και $f(N) < M$, τότε f επάγει έναν ομομορφισμό $f' : G/N \to H/M$, με $aN \mapsto f(a)M$. f' είναι ισομορφισμός αν και μόνο αν $Imf \vee M = H$ και $f^{-1}(M) \subset N$. Συγκεκριμένα αν f είναι ένας επιμορφισμός τ.ω. $f(N) = M$ και $\ker f \subset N$, τότε f' είναι ένας ισομορφισμός. □

Παρατήρηση 1.2.18. *Αν* R *δακτύλιος,* $\{A_i \mid i \in I\}$ *μια οικογένεια από* R*-modules,* D *ένα* R*-module, και* $\{\psi_i : A_i \to D \mid i \in I\}$ *μια οικογένεια από* R*-modules ομομορφισμούς, τότε υπάρχει ένας μοναδικός* R*-module ομομορφισμός* $\phi : \sum_{i \in I} A_i \to D$ *τέτοιος ώστε* $\phi_i = \psi_i, \forall i \in I$. *Το* $\sum_{i \in I} A_i$ *καθορίζεται μοναδικά σε ισομορφισμούς από αυτή την ιδιότητα.*

Θεώρημα 1.2.19. *Έστω* R *περιοχή κύριου ιδεώδους. Αν* $r \in R$ *παράγοντες με* $r = p_1^{n_1} \cdots p_k^{n_k}$ *με* $p_1, \ldots, p_k \in R$ *διακεκριμένοι πρώτοι και* $n_i > 0, \forall i$, *τότε υπάρχει ένας* R*-module ισομορφισμός*

$$R/(r) \cong R/(p_1^{n_1}) \oplus ... \oplus R/(p_k^{n_k}).$$

Συνεπώς, κάθε κυκλικό $R-module$ *τάξης* r *είναι ένα ευθύ άθροισμα* k *κυκλικών* R*-modules τάξεων* $p_1^{n_1}, ..., p_k^{n_k}$ *αντίστοιχα.*

Απόδειξη. Θα αποδείξουμε ότι αν $s, t \in R$ είναι σχετικά πρώτοι, τότε $R/(st) \cong R/(s) \oplus R/(t)$. Για το πρώτο μέρος του θεωρήματος κάνουμε επαγωγή στον αριθμό διακεκριμένων πρώτων στην ανάλυση των πρώτων παραγόντων του r. Το δεύτερο μέρος είναι άμεση συνέπεια του γεγονότος οτι $R/(c)$ είναι ένα κυκλικό R-module τάξης c για κάθε $c \in R$. Η απεικόνιση $\theta : R \to R$ που στέλνει $x \mapsto tx$ είναι ένας R-module μονομορφισμός που στέλνει το ιδεώδες (s) στο ιδεώδες (st). Από 1.2.17 η θ επάγει έναν R-module ομομορφισμό $R/(s) \to R/(st)$ με $x + (s) \mapsto tx + (st)$. Όμοια υπάρχει ένας ομομορφισμός $R/(t) \to R/(st)$ με $x+(t) \mapsto sx+(st)$. Από την απόδειξη του 1.2.18 η απεικόνιση $\alpha : R/(s) \oplus R/(t) \to R/(st)$ με $(x+(s), y+(t)) \mapsto [tx+sy]+(st)$ είναι ένας καλά ορισμένος R-module ομομορφισμός. Αφού $(s,t) = 1_R$, υπάρχουν $u, v \in R$ τέτοια ώστε $su + tv = 1_R$ (1.2.9). Αν $c \in R$, τότε $c = suc + tvc$, από όπου $\alpha(vc + (s), uc + (t)) = c + (st)$. Έτσι, α είναι ένας επιμορφισμός. Για να δείξουμε ότι α είναι μονομορφισμός πρέπει να δείξουμε ότι

$$\alpha(x + (s), (y) + t) = 0 \Rightarrow x \in (s) \text{ και } y \in (t).$$

Αν $\alpha(x + (s), y + (t)) = 0$, τότε $tx + sy = stb \in (st)$ για κάποιο $b \in R$. Όπου $utx + usy = ustb$. Αλλά $y = 1_R y = (su + tv)y$, όπου $utx + (y - tvy) = ustb$ και $y = ustb - utx + tvy \in (t)$. Ένα παρόμοιο επιχείρημα δείχνει ότι $x \in (s)$. □

Παρατήρηση 1.2.20. *Αν V διανυσματικός χώρος επί ενός δακτυλίου διάσπασης D, τότε δύο οποιεσδήποτε βάσεις του V έχουν τον ίδιο πληθάριθμο.*

Θεώρημα 1.2.21. *Έστω A ένα πεπερασμένα παραγόμενο module επί μιας περιοχής κύριου ιδεώδους R.*

(i) *A είναι το ευθύ άθροισμα ενός ελεύθερου submodule F πεπερασμένου βαθμού και ενός πεπερασμένου αριθμού από κυκλικά modules στρέψης. Οι κυκλικοί παράγοντες στρέψης (αν υπάρχουν) είναι τάξεων $r_1, .., r_t$ όπου $r_1, .., r_t$ είναι (όχι απαραίτητα διακεκριμένα) μη μηδενικά και μη μοναδιαία στοιχεία του R τέτοια ώστε $r_1 / r_2 / ... / r_t$. Ο βαθμός του F και η λίστα των ιδεωδών $(r_1), ..., (r_t)$ καθορίζονται μοναδικά από το A.*

(ii) *A είναι το ευθύ άθροισμα ενός ελεύθερου submodule E πεπερασμένου βαθμού και ενός πεπερασμένου αριθμού από κυκλικά modules στρέψης. Οι κυκλικοί παράγοντες στρέψης (αν υπάρχουν) είναι τάξης $p_1^{s_1}, \ldots, p_k^{s_k}$, όπου $p_1, \ldots, p_k$ είναι (όχι απαραίτητα διακριτοί) πρώτοι στο R και $s_1, \ldots, s_k$ είναι (όχι απαραίτητα διακριτοί) θετικοί ακέραιοι. Ο βαθμός του E και τα ιδεώδη $(p_1^{s_1}), \ldots, (p_k^{s_k})$ καθορίζονται μοναδικά από το A. (εκτός από την τάξη του p_i)*

Απόδειξη. Η ύπαρξη ένος ευθέους αθροίσματος αποσύνθεσης του τύπου που περιγράφεται στο (ii) είναι άμεση συνέπεια των 1.2.8, 1.2.11 και 1.2.13. Έτσι A είναι το ευθύ άθροισμα ενός ελεύθερου module και μιας πεπερασμένης οικογένειας από κυκλικά R-modules, το κάθε ένα από αυτά έχει τάξη μια δύναμη ενός πρώτου. Στην περίπτωση των αβελιανών ομάδων αυτές οι πρώτες δυνάμεις είναι ακριβώς οι στοιχειώδεις διαιρέτες του A. Η μέθοδος υπολογισμού τους διάφορους παράγοντες μιας αβελιανής ομάδας από τους στοιχειώδεις διαιρέτες μπορεί να χρησιμοποιηθεί εδώ για να αποδείξει την ύπαρξη ενός ευθέους αθροίσματος αποσύνθεσης του A στον τύπο που περιγράφεται στο (i). Χρειαζόμαστε να κάνουμε τις παρακάτω τροποποιήσεις. Ο ρόλος του $\mathbf{Z}_{p^n} \cong \mathbf{Z}/(p^n) (p \in \mathbf{Z}$ πρώτος) παίζεται από ένα κυκλικο submodule στρέψης του A τάξης $p^n (p \in R$ πρώτος). Ένα τέτοιο κυκλικό module στρέψης είναι ισομορφικό με το $R/(p^n)$ από το 1.2.6. Η απόδειξη για την μοναδικότητα της αποσύνθεσης στα (i) και (ii) είναι ουσιαστικά η ίδια με την απόδειξη αντίστοιχων γεγονότων για τις αβελιανές ομάδες. Οι ακόλουθες τροποποιήσεις για τον ισχυρισμό είναι απαραίτητες. Πρώτα, η ανάλυση σε πρώτους παράγοντες στο R είναι μοναδική μόνο στον πολλαπλασιασμό με μια μονάδα 1.2.4. Αυτό δεν προκαλεί δυσκολία στο $\mathbf{Z}$ οι μόνες μονάδες είναι τα ± 1 και οι πρώτοι είναι ορισμένοι να είναι θετικοί. Σε μια αυθαίρετη περιοχή κύριου ιδεώδους R, ωστόσο, ένα στοιχείο $a \in R$ μπορεί να έχει τάξη p και τάξη q με p, q διακεκριμένοι πρώτοι. Ωστόσο, αφού $(p) = O_a = (q)$, p και q είναι συνεργάτες 1.2.5, όπου είναι, $q - pu$ με $u \in R$ είναι μια μονάδα. Όπου οι ισχυρισμοί μοναδικότητας στα (i) και (ii) έχουν να κάνουν με ιδεώδη αντί με στοιχεία. Σημειώνω ότι $a \neq 0$ συνεπάγεται ότι $O_a \neq R$ και ότι ένα κυκλικό module Ra είναι ελεύθερο αν και μόνο αν $O_a = (0)$. Έτσι τα στοιχεία r_i στο (i) είναι μη μηδενικά και μη μοναδιαία. Άλλες τροποποιήσεις: όπως παραπάνω αντικαθιστώ κάθε πεπερασμένο κυκλικό παράγοντα $\mathbf{Z}_n \cong \mathbf{Z}/(n)$, $n > 1$, με ένα κυκλικό module στρέψης $R/(r)$ ($r \in R$ μη μηδενικό ,μη μοναδιαίο). Αντικαθιστώ την υποομάδα που παράγεται από το απείρως παραγόμενο παράγοντα $\mathbf{Z}$ με ένα ελεύθερο R-module πεπερασμένου βαθμού. Χρησιμοποιώ τα 1.2.16 και 1.2.19 και το γεγονός ότι το $A[p]$ είναι ένας διανυσματικός χώρος επί του $R/(p)$. Έτσι, ο αριθμός των παραγόντων $R/(p)$ είναι ακριβώς $\dim_{R/(p)} A[p]$, ο οποίος είναι αμετάβλητος από 1.2.20. $\square$

Κεφάλαιο 2

Συνθήκες Αλυσίδας - Noetherian δακτύλιοι και modules

Σ' αυτό το κεφάλαιο θα ορίσουμε τις βασικές συνθήκες αλυσίδας σε δακτύλιους και θα αποδείξουμε τις βασικές ιδιότητές τους.

2.1 Αλυσίδες

Ορισμός 2.1.1. *Ένα module A λέμε ότι ικανοποιεί την συνθήκη αύξουσας αλυσίδας σε submodules (ή ότι είναι Noetherian) εάν για κάθε αλυσίδα $A_1 \subset A_2 \subset A_3 \subset \cdots$ από submodules του A υπάρχει ένας ακέραιος n τέτοιος ώστε $A_i = A_n, \forall i \geq n$. Ένα module B λέμε ότι ικανοποιεί την συνθήκη φθίνουσας αλυσίδας σε submodules (ή ότι είναι Artinian) εάν για κάθε αλυσίδα $B_1 \supset B_2 \supset B_3 \supset \cdots$ από submodules του B υπάρχει ένας ακέραιος m τέτοιος ώστε $B_i = B_m, \forall i \geq m$.*

Ορισμός 2.1.2. *Ένας δακτύλιος R είναι αριστερά (αντ. δεξιά) Noetherian αν ο R ικανοποιεί την συνθήκη αύξουσας αλυσίδας σε αριστερά (αντ. δεξιά) ιδεώδη. Ο R είναι Noetherian αν R είναι και αριστερά και δεξιά Noetherian. Ένας δακτύλιος R είναι αριστερά (αντ. δεξιά) Artinian αν ο R ικανοποιεί την συνθήκη φθίνουσας αλυσίδας στα αριστερά (αντ. δεξιά) ιδεώδη. Ο R λέμε ότι είναι Artinian αν είναι και αριστερά και δεξιά Artinian.*

Ορισμός 2.1.3. *Ένα module A λέμε ότι ικανοποιεί την συνθήκη μεγίστου(αντ. ελαχίστου) στα submodules εάν κάθε μη κενό σύνολο από submodules του A περιέχει ένα μέγιστο (αντ. ελάχιστο) στοιχείο (με σεβασμό στην συνολοθεωριτική έγκλειση).*

Θεώρημα 2.1.4. *Αν Σ σύνολο, $a \in \Sigma$ και $\forall n \in N, f_n : \Sigma \to \Sigma$ συνάρτηση, τότε υπάρχει μοναδική συνάρτηση $\phi : N \to \Sigma$ τέτοια ώστε $\phi(0) = a$ και $\phi(n+1) = f_n(\phi(n)), \ \forall n \in N$.*

Απόδειξη. Ιδέα απόδειξης: Κατασκευάζοντας μια σχέση R επί του $N \times S$ η οποία είναι το γράφημα της συνάρτησης $\phi : N \to S$ με τις επιθυμητές ιδιότητες. Έστω G να είναι το σύνολο όλων των υποσυνόλων Y του $N \times S$ τ.ω.

$$(0, a) \in Y \text{ και } (n, x) \in Y \Rightarrow (n + 1, f_n(x)) \in Y, \ \forall n \in N.$$

Τότε $G \neq \emptyset$ αφού $N \times S \in G$. Έστω $R = \cap_{Y \in G} Y$, τότε $R \in G$. Έστω M να είναι το υποσύνολο του N που αποτελείται από όλα τα $n \in N$ για τα οποία υπάρχει ένα μοναδικό $x_n \in S$ τέτοιο ώστε $(n, x_n) \in R$. Με επαγωγή δείχνουμε ότι $M = N$. Έτσι από το $n \mapsto x_n$ ορίζεται μία συνάρτηση $\phi : N \to S$ με γράφημα R. Αφού $(0, a) \in R$ πρέπει να έχουμε $\phi(0) = a$. Για κάθε $n \in N$, $(n, x_n) = (n, \phi(n)) \in R$ και έτσι $(n+1, f_n(\phi(n)) \in R$ αφού $R \in G$. Αλλά $(n+1, x_{n+1}) \in R$ και η μοναδικότητα του x_{n+1} επάγει ότι $\phi(n+1) = x_{n+1} = f_n(\phi(n))$. □

Θεώρημα 2.1.5. *Ένα module A ικανοποιεί την συνθήκη αύξουσας (αντ. φθίνουσας) αλυσίδας στα submodules αν και μόνο αν το A ικανοποιεί την συνθήκη μεγίστου (αντ. ελαχίστου) στα submodules.*

Απόδειξη. Υποθέτουμε ότι το A ικανοποιεί την συνθήκη ελαχίστου στα submodules και $A_1 \supset A_2 \supset \cdots$ είναι μια αλυσίδα από submodules. Τότε το σύνολο $\{A_i \mid i \geqslant 1\}$ έχει ένα ελάχιστο στοιχείο, έστω το A_n. Επομένως, για $i \geqslant n$ έχουμε $A_n \supset A_i$ από υπόθεση και $A_n \subset A_i$ από ελαχιστότητα, έτσι $A_n = A_i$, για κάθε $i \geqslant n$. Έτσι, το A ικανοποιεί τη συνθήκη φθίνουσας αλυσίδας. Αντίστροφα, υποθέτουμε ότι το A ικανοποιεί τη συνθήκη φθίνουσας αλυσίδας, και S είναι ένα μη κενό σύνολο από submodules του A. Τότε υπάρχει $B_0 \in S$. Αν το S δεν έχει ελάχιστο στοιχείο, τότε για κάθε submodule B στο S υπάρχει τουλάχιστον ένα submodule B' στο S τέτοιο ώστε $B \supsetneqq B'$. Για κάθε B στο S, διαλέγω ένα τέτοιο B' (Αξίωμα της επιλογής). Αυτή η επιλογή ορίζει μία συνάρτηση $f : S \to S$ με $B \mapsto B'$. Από 2.1.4 (με $f = f_n, \forall n$) υπάρχει μία συνάρτηση $\phi : \mathbf{N} \to S$ τέτοια ώστε

$$\phi(0) = B_0 \text{ και } \phi(n+1) = f(\phi(n)) = \phi(n)'.$$

Έτσι εάν το $b_n \in S$ υποδηλώνει το $\phi(n)$, τότε υπάρχει μια ακολουθία $B_0, B_1, \ldots$ τέτοια ώστε $B_0 \supsetneqq B_1 \supsetneqq B_2 \supsetneqq \cdots$. Αυτό έρχεται σε αντίθεση με την συνθήκη φθίνουσας αλυσίδας. Έτσι, το S πρέπει να έχει ένα ελάχιστο στοιχείο, και έτσι το A ικανοποιεί την συνθήκη ελαχίστου. Η απόδειξη για την συνθήκη αύξουσας αλυσίδας και κατάστασης μεγίστου είναι ανάλογη. □

Ορισμός 2.1.6. *Ένα ζευγάρι από module ομομορφισμούς, $A \xrightarrow{f} B \xrightarrow{g} C$, λέγεται ακριβής στο B όταν $Imf = \ker g$. Μια πεπερασμένη ακολουθία από module ομομορφισμούς, $A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \ldots \xrightarrow{f_{n-1}} A_{n-1} \xrightarrow{f_n} A_n$, είναι ακριβής όταν $Imf_i = \ker f_{i+1}$ για $i = 1, 2, \ldots, n-1$.*

Θεώρημα 2.1.7. *Έστω $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ να είναι μια ακριβής ακολουθία από modules. Τότε το B ικανοποιεί την συνθήκη αύξουσας (αντ. φθίνουσας) αλυσίδας σε submodules αν και μόνο αν το A και το C την ικανοποιεί.*

Απόδειξη. Αν το B ικανοποιεί την συνθήκη αύξουσας αλυσίδας, τότε την ικανοποιεί και το submodule $f(A)$. Από ακρίβεια το A είναι ισομορφικό με το $f(A)$, και έτσι A ικανοποιεί την συνθήκη αύξουσας αλυσίδας. Αν $C_1 \subset C_2 \subset \cdots$ είναι μια αλυσίδα από submodules του C, τότε $g^{-1}(C_1) \subset g^{-1}(C_2) \subset \cdots$ είναι μια αλυσίδα από submodules του B. Έτσι, υπάρχει ένα n τέτοιο ώστε $g^{-1}(C_i) = g^{-1}(C_n) \forall i \geqslant n$. Απ' τη στιγμή που g είναι επιμορφισμός από ακρίβεια, ακολουθεί ότι $C_i = C_n, \forall i \geqslant n$. Έτσι, το C ικανοποιεί τη συνθήκη αύξουσας αλυσίδας. Υποθέτω ότι A και C ικανοποιεί τη συνθήκη αύξουσας αλυσίδας και $B_1 \subset B_2 \subset \cdots$ είναι μια αλυσίδα από submodules του B. Για κάθε i έστω

$$A_i = f^{-1}(f(A) \cap B_i) \text{ και } C_i = g(B_i).$$

Έστω $f_i = f \mid A_i$ και $g_i\diamond = g \mid B_i$. Επιβεβαιώστε ότι για κάθε i η παρακάτω ακολουθία είναι ακριβής:

$$0 \to A_i \xrightarrow{f_i} B_i \xrightarrow{g_i C_i} 0.$$

Επιβεβαιώστε ότι $A_1 \subset A_2 \subset \cdots$ και $C_1 \subset C_2 \subset \cdots$. Από υπόθεση υπάρχει ένας ακέραιος n τέτοιος ώστε $A_i = A_n$ και $C_i = C_n$ για όλα τα $i \geqslant n$. Για κάθε $i \geqslant n$ υπάρχει ένα αντιμεταθετικό διάγραμμα με:

$$\begin{tikzcd}
0 \arrow[r] & A_n \arrow[r, "f_n"] \arrow[d, "\alpha"'] & B_n \arrow[r, "g_n"] \arrow[d, "\beta_i"'] & C_n \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & A_i \arrow[r, "f_i"] & B_i \arrow[r, "g_i"] & C_i \arrow[r] & 0
\end{tikzcd}$$

όπου α και γ είναι οι αντίστοιχες μοναδιαίες απεικονίσεις και β_i η απεικόνιση έγκλεισης. Αρα β_i είναι η ταυτοτική απεικόνιση, ως εκ τούτου το B ικανοποιεί την συνθήκη αύξουσας αλυσίδας. Η απόδειξη για τη συνθήκη φθίνουσας αλυσίδας είναι ανάλογη. □

Πόρισμα 2.1.8. *Εάν A είναι ένα submodule του module B, τότε το B ικανοποιεί τη συνθήκη αύξουσας (αντ. φθίνουσας) αλυσίδας αν και μόνο αν το A και το B/A την ικανοποιούν.*

Απόδειξη. Αν εφαρμόσουμε το προηγούμενο θεώρημα για την ακολουθία $0 \to A \xrightarrow{\subset} B \to B/A \to 0$. □

Πόρισμα 2.1.9. *Αν $A_1, \dots, A_n$ είναι modules, τότε το ευθύ άθροισμα $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ ικανοποιεί τη συνθήκη αύξουσας (αντ. φθίνουσας) αλυσίδας στα submodules αν και μόνο αν κάθε A_i την ικανοποιεί.*

Απόδειξη. Με επαγωγή στο n. Αν $n = 2$, από το 2.1.7 για την ακολουθία $0 \to A_1 \xrightarrow{i_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \to 0$. □

Θεώρημα 2.1.10. *Αν R είναι ένας αριστερά Noetherian (αντ. Artinian) δακτύλιος με μονάδα, τότε κάθε πεπερασμένα παραγόμενο μοναδιαίο αριστερό R-module A ικανοποιεί τη συνθήκη αύξουσας (αντ. φθίνουσας) αλυσίδας στα submodules.*

Απόδειξη. Αν A πεπερασμένα παραγόμενο, τότε από 1.1.27 υπάρχει ελεύθερο R-module F με μια πεπερασμένη βάση και ένας επιμορφισμός $\pi : F \to A$. Αφού F είναι ένα ευθύ άθροισμα από πεπερασμένο αριθμό αντίγραφων του R, από 1.1.15, το F είναι αριστερά Noetherian (αντ. Artinian) από το 2.1.9. Έτσι $A \cong F/\ker \pi$ είναι Noetherian(αντ. Artinian) λόγω 2.1.8. □

Θεώρημα 2.1.11. *Ένα module A ικανοποιεί τη συνθήκη αύξουσας αλυσίδας σε submodules αν και μόνο αν κάθε submodule του A είναι πεπερασμένα παραγόμενο. Συγκεκριμένα, ένας αντιμεταθετικός δακτύλιος R είναι Noetherian αν και μόνο αν κάθε ιδεώδες του R είναι πεπερασμένα παραγόμενο.*

Απόδειξη. ($\Rightarrow$) Αν B είναι ένα submodule του A , έστω S να είναι το σύνολο όλων των πεπερασμένα παραγόμενων submodules του B. Αφού το S είναι μη κενο ($0 \in S$), το S έχει ένα μέγιστο στοιχείο C από 2.1.5. Το C είναι πεπερασμένα παραγόμενο από τα $c_1, \dots, c_n$. Για κάθε $b \in B$ έστω D_b να είναι το submodule του B παραγόμενο από τα $b, c_1, \ldots, c_n$. Τότε $D_b \in S$ και $C \subset D_b$. Αφού C μέγιστο, $D_b = C$ για κάθε $b \in B$, ως εκ τούτου $b \in D_b = C$ για κάθε $b \in B$ και $B \subset C$. Αφού $C \subset B$ από κατασκευή, $B = C$ και έτσι το B είναι πεπερασμένα παραγόμενο. ($\Leftarrow$) Δοθέντος μιας αλυσίδας από submodules $A_1 \subset A_2 \subset \cdots$, τότε είναι εύκολο να επιβεβαιώσουμε ότι $\cup_{i \geqslant 1} A_i$ είναι επίσης ένα submodule του A και έτσι είναι πεπερασμένα παραγόμενο, ας πούμε από τα $a_1, a_2, \ldots, a_k$. Αφού κάθε a_i είναι ένα στοιχείο κάποιου A_i, υπάρχει ένας δείκτης n τέτοιος ώστε $a_i \in A_n$ για $i = 1, \ldots, k$. Επομένως, $\cup A_i \subset A_n$, και έτσι $A_i = A_n$ για $i \geqslant n$. □

Ορισμός 2.1.12. (i) *Μία κανονική σειρά για ένα submodule A είναι μια αλυσίδα από submodules: $A = A_0 \supset A_1 \supset \cdots \supset A_n$.*

(ii) *Οι παράγοντες της σειράς είναι τα πηλίκα modules*

$$A_i/A_{i+1} (i = 0, 1, \ldots, n-1)$$

.

(iii) *Το μήκος της σειράς είναι ο αριθμός των κατάλληλων εγκλισμών (= ο αριθμός των τετριμμένων παραγόντων).*

(iv) *Μία επιλέπτυνση κανονικής σειράς $A_0 \supset A_1 \supset \cdots \supset A_n$ είναι μια κανονική σειρά που αποκτιέται εισάγωντας ένα πεπερασμένο αριθμό από προσθετικά submodules ανάμεσα στα δοθέντα.*

(v) *Μια κατάλληλη επιλέπτυνση είναι μια η οποία έχει μήκος μεγαλύτερο από την αυθεντική σειρά.*

(vi) *Δύο κανονικές σειρές λέγονται ισοδύναμες αν υπάρχει μια ένα προς ένα αντιστοιχία μεταξύ των μη τετριμμένων παραγόντων τέτοια ώστε αντίστοιχοι παράγοντες είναι ισομορφικά modules. Έτσι ισοδύναμες σειρές έχουν απαραίτητα το ίδιο μήκος.*

(vii) *Μία σύνθεση σειράς για το A είναι μια κανονική σειρά $A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_n = 0$ τέτοια ώστε κάθε παράγοντας $A_k/A_{k+1} (k = 0, \ldots, n-1)$ είναι ένα μη μηδενικό module χωρίς κατάλληλα submodules.*

Ορισμός 2.1.13. (i) *Μια υποομάδα H μιας ομάδας G τέτοια ώστε $H \neq G, H \neq < e >$ λέγεται κατάλληλη υποομάδα.*

(ii) *Μια ομάδα G λέγεται απλή αν G δεν έχει κάτάλληλες κανονικές υποομάδες.*

(iii) *Μια υποκανονική σειρά μιας ομάδας G είναι μια αλυσίδα από υποομάδες $G = G_0 > G_1 > \cdots > G_n$ τέτοια ώστε G_{i+1} κανονική στην $G_i, 0 \leq i < n$.*

(iv) *Οι παράγοντες της σειράς είναι τα πηλίκα ομάδες G_{i+1}/G_i.*

(v) *Το μήκος της σειράς είναι ο αριθμός των μη-ταυτοτικών παραγόντων.*

(vi) *Μια υποκανονική σειρά τέτοια ώστε $G_i \lhd G, \forall i$ λέγεται κανονική.*

(vii) *Έστω $G = G_0 > G_1 > \cdots > G_n$ μια υποκανονική σειρά. Μία ένα-βήμα βελτίωση της σειράς αυτής είναι μια σειρά της μορφής $G = G_0 > \cdots > G_i > N > G_{i+1} > \cdots > G_n$ ή $G = G_0 > \cdots > G_n > N$, όπου N είναι μια κανονική υποομάδα της G_i και (αν $i < n$) G_{i+1} κανονική στην N.*

(viii) *Μια βελτίωση μιας υποκανονικής σειράς S είναι οποιαδήποτε υποκανονική σειρά που ανακτείται από το S από μια πεπερασμένη ακολουθία με ένα-βήμα βελτιώσεις.*

(ix) *Μια βελτίωση του S λέγεται κατάλληλη αν το μήκος της είναι μεγαλύτερο από το μήκος της S.*

(x) *Μια υποκανονική σειρά $G = G_0 > G_1 > \cdots > G_n =< e >$ είναι μια σύνθεση σειράς αν κάθε παράγοντας G_i/G_{i+1} είναι απλός.*

Παρατήρηση 2.1.14. *Έστω A, A', B, B' να έιναι υποομάδες μιας ομάδας G τέτοια ώστε A' έιναι κανονική στην A και B' κανονική στην B.*

(i) $A'(A \cap B')$ *είναι μια κανονική υποομάδα της* $A'(A \cap B)$

(ii) $B'(A' \cap B)$ *είναι μια κανονική υποομάδα της* $B'(A \cap B$

(iii) $A'(A \cap B)/A'(A \cap B') \cong B'(A \cap B)/B'(A' \cap B)$

Παρατήρηση 2.1.15. *Δύο οποιεσδήποτε υποκανονικές (αντ. κανονικές) σειρές μιας ομάδας G έχουν υποκανονικές (αντ. κανονικές) βελτιώσεις που είναι ισοδύναμες.*

Θεώρημα 2.1.16. *Δύο οποιεσδήποτε συνθέσεις σειρών μιας ομάδας G είναι ισοδύναμες. Άρα κάθε ομάδα που έχει μια σύνθεση σειράς καθορίζει μια μοναδική λίστα από απλές ομάδες.*

Απόδειξη. Αφού οι σύνθεση σειρών είναι υποκανονικές σειρές , δύο οποιεσδήποτε συνθέσεις σειράς έχουν ισοδύναμες βελτιώσεις από 2.1.14. Αλλά κάθε βελτίωση μιας σύνθεσης σειράς S έιναι ισοδύναμη με το S από 2.1.15. Ακολουθεί ότι δύο οποιεσδήποτε συνθέσεις σειράς είναι ισοδύναμες. □

Θεώρημα 2.1.17. *Δύο οποιεσδήποτε κανονικές σείρες ενός module A έχουν επιλεπτύνσεις που είναι ισοδύναμες. Δύο οποιεσδήποτε συνθέσεις σειρών του A είναι ισοδύναμες.*

Απόδειξη. Προκύπτει από τα 2.1.14, 2.1.15 και 2.1.16. □

Για την απόδειξη του 2.1.19 χρειαζόμαστε το εξής αποτέλεσμα:

Θεώρημα 2.1.18. *Αν R δακτύλιος και B submodule ενός R-module A, τότε υπάρχει μια ένα προς ένα αντιστοιχία μεταξύ του συνόλου όλων των submodules του A που περιέχουν το B και το σύνολο όλων των submodules του A/B, που δίνεται από το $C \mapsto C/B$, όπου C είναι ένα submodule του A που περιέχει το B.*

Απόδειξη. Υπόδειξη : Χρησιμοποιούμε τα εξής

(i) Αν $f : G \to H$ είναι ένας επιμορφισμός ομάδων, τότε το $K \mapsto f(K)$ ορίζει μία ένα προς ένα αντιστοιχία μεταξύ του συνόλου $S_f(G)$ όλων των υποομάδων K του G που περιέχει το $\ker f$ και το σύνολο $S(H)$ όλων των υποομάδων του H. Υπό αυτή την αντιστοιχία κανονικές υποομάδες αντιστοιχούν σε κανονικές υποομάδες.

(ii) Αν N είναι μια κανονική υποομάδα μιας ομάδας G, τότε κάθε υποομάδα της G/N είναι της μορφής K/N, όπου K είναι μια υποομάδα της G που περιέχει το N. Επιπλέον, K/N είναι κανονική στη G/N αν-ν K είναι κανονική στη G.

□

Θεώρημα 2.1.19. *Ένα μη μηδενικό module A έχει μια σύνθεση σειρών αν και μόνο αν το A ικανοποιεί την συνθήκη αύξουσας αλυσίδας σε submodules.*

Απόδειξη. ($\Rightarrow$) Έστω ότι το A έχει σύνθεση σειράς S μήκους n. Αν ειτηερ ςηαιν ςονδιτιον φαιλς το ηολδ,ονε ςαν φινδ submodules

$$A = A_0 \supsetneqq A_1 \supsetneqq A_2 \supsetneqq \cdots \supsetneqq A_n \supsetneqq A_{n+1},$$

το οποίο σχηματίζει μια κανονική σειρά T μήκους $n+1$. Από το προηγούμενο θεώρημα S και T έχουν επιλεπτύνσεις που είναι ισοδύναμες. Αυτό είναι άτοπο διότι ισοδύναμες σειρές έχουν ίσο μήκος. Για κάθε επιλέπτυνση σύνθεσης σειράς S έχει το ίδιο μήκος n όπως το S, αλλά κάθε επιλέπτυνση του T έχει απαραίτητα μήκος τουλάχιστον $n+1$. Έτσι, το A ικανοποιεί και τις δύο συνθήκες αλυσίδας. ($\Leftarrow$) Αν B είναι ένα μη μηδενικό submodule του A, έστω $S(B)$ να είναι το σύνολο όλων των submodules C του B τέτοια ώστε $C \neq B$. Έτσι εάν B έχει μη κατάλληλα submodules, $S(B) = 0$. Επίσης ορίζω $S(0) = 0$. Για κάθε B υπάρχει ένα μέγιστο στοιχείο B' του $S(B)$. Έστω S να είναι το σύνολο όλων των submodules του A και ορίζω την απεικόνιση $f : S \to S$ με $f(B) = B'$ (το αξίωμα της επιλογής χρειάζεται για την ταυτόχρονη επιλογή του B'). Από 2.1.4 (με $f = f_n \forall n$) υπάρχει μια συνάρτηση $\phi : \mathbf{N} \to S$ τέτοια ώστε

$$\phi(0) = A \text{ και } \phi(n+1) = f(\phi(n)) = \phi(n)'.$$

Αν με A_i συμβολίζουμε το $\phi(i)$, τότε $A \supset A_1 \supset A_2 \supset \cdots$ είναι μια φθίνουσα αλυσίδα από κατασκευή, όπου για κάποιο n, $A_i = A_n, \ \ \forall i \geqslant n$. Αφού $A_{n+1} = A'_n = f(A_n)$, από ορισμό η f δείχνει ότι $A_{n+1} = A_n$ μόνο αν $A_n = 0 = A_{n+1}$. Έστω m να είναι ο μικρότερος ακέραιος τέτοιος ώστε $A_m = 0$. Τότε $m \leqslant n$ και $A_k \neq 0$ για όλα τα $k < m$. Επιπλέον για κάθε $k < m$, A_{k+1} είναι ένα μέγιστο submodule του A_k τέτοιο ώστε $A_k \supsetneqq A_{k+1}$. Επομένως, κάθε A_k/A_{k+1} είναι μη μηδενικό και έχει μη κατάλληλα submodules από 2.1.19. Άρα, $A \supset A_1 \supset \cdots \supset A_m = 0$ είναι μια σύνθεση σειράς του A. □

Ορισμός 2.1.20. *Έστω A ένας πίνακας επί ενός δακτυλίου R με μονάδα. Κάθε ένα από τα παρακάτω είναι μία στοιχειώδη λειτουργία γραμμής στο A:*

(i) *εναλλαγή δύο γραμμών στον A.*

(ii) *αριστερός πολλαπλασιασμός μιας γραμμής του A με ένα στοιχείο $c \in R$.*

(iii) *για $r \in R$ και $i \neq j$, προσθέτω r-φορές την γραμμή j στην γραμμή i.*

Παρατήρηση 2.1.21. *Έστω A να είναι ένας πίνακας $n \times m$ επί ενός δακτυλίου R με μονάδα και έστω E_n (αντ. E_m) να είναι ο στοιχειώδης πίνακας που αποκτάται εκτελόντας μια στοιχειώδη λειτουργία γραμμής T στο I_n (αντ. I_m). Τότε E_nA (αντ. AE_m) είναι ο πίνακας που αποκτάται από την εκτέλεση της λειτουργίας T στο A.*

Θεώρημα 2.1.22. *Αν D είναι ένας δακτύλιος διαίρεσης, τότε ο δακτύλιος Mat_nD όλων των $n \times n$ πινάκων πάνω στο D είναι και Artinian και Noetherian.*

Απόδειξη. Από 2.1.2 και το παραπάνω θεώρημα επαρκούν για να δείξουμε ότι $R = Mat_n D$ έχει μια σύνθεση σειράς από αριστερά R-modules και μια σύνθεση σειράς από δεξιά R-modules. Για κάθε i έστω $e_i \in R$ να είναι ο πίνακας με 1_D στην θέση (i,i) και 0 οπουδήποτε αλλού. Επιβεβαιώστε ότι $Re_i = \{Ae_i \mid A \in R\}$ είναι ένα αριστερό ιδεώδες (submodule) του R που περιέχει όλους τους πίνακες στο R με στήλη j μηδέν για όλα τα $j \neq i$. Ισχύει ότι Re_i είναι ένα ελάχιστο μη μηδενικό αριστερό ιδεώδες (που είναι, δεν έχει κατάλληλα submodules). Ένας τρόπος να το δείξουμε είναι μέσω στοιχειώδους μετασχηματισμού πινάκων (παραπάνω ορισμός και 2.1.21). Έστω $M_0 = 0$ και για $i \geqslant 1$ έστω $M_i = R(e_1 + e_2 + \cdots + e_i)$. Επιβεβαιώστε ότι κάθε M_i είναι ένα αριστερό ιδεώδες του R και ότι $M_i/M_{i-1} \cong Re_i$, ως εκ τούτου $R = M_n \supset M_{n-1} \supset \cdots \supset M_1 \supset M_0 = 0$ είναι μια σύνθεση σειράς από αριστερά R-modules. Ένα παρόμοιο επιχείρημα με τα δεξιά ιδεώδη $e_iR = \{e_iA \mid A \in R\}$ δείχνει ότι το R έχει σύνθεση σειράς από δεξιά R-modules. □

2.2 Δακτύλιοι και module Noether

Για την απόδειξη του 2.2.2 θα χρειαστούμε το εξής:

Θεώρημα 2.2.1. *Αν R είναι ένας αντιμεταθετικός δακτύλιος με μονάδα και P είναι ένα ιδεώδες το οποίο είναι μέγιστο στο σύνολο όλων των ιδεωδών του R τα οποία δεν είναι πεπερασμένα παραγόμενα, τότε P πρώτο.*

Απόδειξη. Έστω $ab \in P$ αλλά a και b δεν ανήκουν στο P. Τότε $P + (a)$ και $P + (b)$ είναι ιδεώδη που περιέχουν το P και έτσι είναι πεπερασμένα παραγόμενα (από μεγιστότητα). Επομένως, $P + (a) = (p_1 + r_1 a, \ldots, p_n + r_n a)$ και $P + (b) = (p'_1 + r'_1 b, \ldots, p'_m + r'_m b)$ για κάποια $p_i, p'_i \in P$ και $r_i, r'_i \in R$. Αν $J = \{r \in R \mid ra \in P\}$, τότε J είναι ένα ιδεώδες. Αφού $ab \in P$, $(p'_i + r'_i b)a = p'_i a + r'_i ab \in P$, $\forall i$, έτσι $P \subsetneq P + (b) \subset J$. Από μεγιστότητα , J είναι πεπερασμένα παραγόμενο, έστω $J = (j_1, \ldots, j_k)$. Αν $x \in P$, τότε $x \in P + (a)$ και έτσι για κάποια $s_i \in R$, $x = \sum_{i=1}^{n} s_i(p_i + r_i a) = \sum_{i=1}^{n} s_i p_i + \sum_{i=1}^{n} s_i r_i a$. Επομένως, $(\sum_i s_i r_i)a = x - \sum_i s_i p_i \in P$, απ' όπου $\sum_i s_i r_i \in J$. Οπότε για κάποια $t_i \in R$, $\sum_{i=1}^{n} s_i r_i = \sum_{i=1}^{k} t_i j_i$ και $x = \sum_{i=1}^{n} s_i p_i + \sum_{i=1}^{k} t_i j_i a$. Επομένως, P είναι παραγόμενο από τα $p_1, \ldots, p_n, j_1 a, \ldots, j_k a$, το οποίο είναι άτοπο. Άρα $a \in P$ ή $b \in P$ και P πρώτο. □

Πρόταση 2.2.2. *Ένας αντιμεταθετικός δακτύλιος R με μονάδα είναι Noetherian αν και μόνο αν κάθε πρώτο ιδεώδες του R είναι πεπερασμένα παραγόμενο.*

Απόδειξη. ($\Leftarrow$) Έστω mS να είναι το σύνολο όλων των ιδεώδων του R τα οποία δεν είναι πεπερασμένα παραγόμενα. Αν το mS είναι μη κενο, τότε χρησιμοποιούμε το λήμμα του Zorn για να βρούμε ένα μέγιστο στοιχείο P του mS. Το P είναι πρώτος από 2.2.1 και έτσι είναι πεπερασμένα παραγόμενο από υπόθεση. Αυτό είναι άτοπο εκτός αν $mS = \emptyset$. Άρα, R είναι Noetherian από 2.1.11. □

Ορισμός 2.2.3. *Αν B είναι ένα module επί ενός αντιμεταθετικού δακτυλίου R, τότε το $I = \{r \in R \mid rb = 0, \forall b \in B\}$ είναι ένα ιδεώδες του R. Το ιδεώδες I λέγεται ο μηδενιστής του B στο R.*

Θεώρημα 2.2.4. *Έστω R δακτύλιος, A ένα R-module, X υποσύνολο του A, $\{B_i \mid i \in I\}$ μια οικογένεια από submodules του A και $a \in A$. Έστω $Ra = \{ra \min r \in R\}$. Το submodule D παραγόμενο από το X είναι $D = RX = \{\sum_{i=1}^{s} r_i a_i \mid s \in N\star; a_i \in X, r_i \in R\}$.*

Απόδειξη. Υπόδειξη: Αν R έχει μονάδα 1_R και A μοναδιαίο, τότε $n1_R \in R$ για κάθε $n \in Z$ και $na = (n1_R)a$ για κάθε $a \in A$. □

Θεώρημα 2.2.5. *Αν $A_1, \ldots, A_n$ ιδεώδη ενός δακτυλίου R, τότε υπάρχει ένας μονομορφισμός δακτυλίων $\theta : R/(A_1 \cap \cdots \cap A_n) \to R/A_1 \times R/A_2 \times \cdots \times R/A_n$. Αν $R^2 + A_i = R \forall i$ και $A_i + A_j = R \forall i \neq j$ τότε θ είναι ισομορφισμός δακτυλίων.*

Απόδειξη. Ο κανονικός επιμορφισμός $\pi_k : R \to R/A_k$ $(k = 1, \ldots, n)$ επάγει έναν ομομορφισμό δακτυλίων $\theta_1 : R \to R/A_1 \times \cdots \times R/A_n$ με $\theta_1(r) = (r + A_1, \ldots, r + A_n)$. Προφανώς $\ker \theta_1 = A_1 \cap \cdots \cap A_n$. Άρα, θ_1 επάγει μονομορφισμό δακτυλίων $\theta : R/(A_1 \cap \cdots \cap A_n) \to R/A_1 \times \cdots \times R/A_n$. Αν $(b_1 + A_1, \ldots, b_n + A_n) \in R/A_1 \times \cdots \times R/A_n$, τότε υπάρχει $b \in R$ τέτοιο ώστε $b \equiv b_i(modA_i)$, $\forall i$. Επομένως $\theta(b + \cap_i A_i) = (b + A_1, \ldots, b + A_n) = (b_1 + A_1, \ldots, b_n + A_n)$, και έτσι θ είναι επιμορφισμός. □

Θεώρημα 2.2.6. *Έστω B ένα ένα πεπερασμένα παραγόμενο module επί ενός αντιμεταθετικού δακτυλίου R με μονάδα και έστω I να είναι ένας μηδενιστής του B στο R. Τότε το B ικανοποιεί τη συνθήκη αύξουσας (αντ. φθίνουσας) αλυσίδας σε submodules αν και μόνο αν R/I είναι ένας Noetherian (αντ. Artinian) δακτύλιος.*

Απόδειξη. Έστω ότι το B παράγεται από τα $b_1, \ldots, b_n$ και υποθέτω ότι το B ικανοποιεί τη συνθήκη αύξουσας αλυσίδας. Τότε $B = Rb_1 + \cdots + Rb_n$ από 2.2.4. Επομένως, $I = I_1 \cap I_2 \cap \cdots \cap I_n$ όπου I_j είναι ο μηδενιστής του submodule Rb_j. Από 2.2.5 υπάρχει μονομορφισμός δακτυλίων $\theta : R/I \to R/I_1 \times \cdots \times R/I_n$. Είναι εύκολο να δούμε ότι θ είναι επίσης ένας R-module μονομορφισμός. Επιβεβαιώστε ότι για κάθε j η απεικόνιση $R/I_j \to Rb_j$ με τύπο $r + I_j \mapsto rb_j$ είναι ένας ισομορφισμός R-modules. Αφού το submodule Rb_j του B αναγκαστικά ικανοποιεί τη συνθήκη αύξουσας αλυσίδας, θα την ικανοποιεί και το R/I_j. Άρα, $R/I_1 \oplus \cdots \oplus R/I_n$ ικανοποιεί τη συνθήκη αύξουσας αλυσίδασσε R-submodules 2.1.9. Επομένως η κάθε submodule $\Im\theta \cong R/I$ ικανοποιεί τη συνθήκη αύξουσας αλυσίδας σε R-submodules. Αλλά κάθε ιδεώδες του δακτυλίου R/I είναι ένα R-submodule του R/I. Άρα, R/I είναι Noetherian. Αντίστροφα, υποθέτω ότι R/I είναι Noetherian. Επιβεβαιώστε ότι B είναι ένα R/I-module με $(r + I)b = rb$ και ότι τα R/I-submodules του B είναι ακριβώς τα R-submodules. Επομένως, το B ικανοποιεί τη συνθήκη αύξουσας αλυσίδας από 2.1.10. □

Παρατήρηση 2.2.7. $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m}) = \sum_{i=1}^{n} \sum_{i=1}^{m} a_i b_j \forall a_i, b_j \in R$.

Παρατήρηση 2.2.8. *Αν R δακτύλιος με μονάδα και X το κέντρο του R (κέντρο του R είναι το σύνολο $C = \{c \in R \mid cr = rc \ \ \forall r \in R\}$, τότε το ιδεώδες (X) περιέχει όλα τα πεπερασμένα αθροίσματα $r_1 a_1 + \cdots + r_n a_n, r_i \in R, a_i \in X$.*

Λήμμα 2.2.9. *Έστω P να είναι ένα πρώτο ιδεώδες σε έναν αντιμεταθετικό δακτύλιο R με μονάδα. Αν C είναι ένα P-πριμαρψ submodule του Noetherian R-module A, τότε υπάρχει ένας θετικός ακέραιος m τέτοιος ώστε $P^m A \subset C$.*

Απόδειξη. Έστω I ο μηδενιστής του A στο R και θεωρώ τον δακτύλιο $\overline{R} = R/I$. Συμβολίζω το ομοσύνολο $r+I \in \overline{R}$ με $\overline{R}$. Προφανώς $I \subset r \in R \mid rA \subset C \subset P$, από όπου $\overline{P} = P/I$ είναι ένα ιδεώδες του $\overline{R}$. Τα A και C είναι το καθένα $\overline{R}$-modules με $\overline{R}a = ra(r \in R, a \in A)$. Ισχυριζόμαστε ότι ένα πρωταρχικό $\overline{R}$-submodule του A. Αν $\overline{R}a \in C$ με $r \in R$ και $a \in A - C$, τότε $ra \in C$. Αφού C είναι ένα πρωταρχικό R-submodule, $r^n A \subset C$ για κάποιο n, όπου $\overline{R}^n A \subset C$ και C είναι $\overline{R}$-πρωταρχικά. Αφού $\overline{R} \in \overline{R} \mid \overline{R}^k A \subset C$για κάποιο$k > 0 = \overline{R} \in \overline{R} \mid r^k A \subset C = \overline{R} \in \overline{R}/midr \in P = \overline{P}$,$\overline{P}$ είναι ένα πρώτο ιδεώδες του $\overline{R}$ και C είναι ένα $\overline{P}$-πρωταρχικό $\overline{R}$-submodule του A. Αφού $\overline{R}$ είναι Noetherian από το προηγούμενο λήμμα, $\overline{P}$ είναι πεπερασμένα παραγόμενο από το 2.1.11. Έστω $\overline{p}_1, \ldots, \overline{p}_s (p_i \in P)$ να είναι οι γεννήτορες του $\overline{P}$. Για κάθε i υπάρχει n_i τέτοιο ώστε $\overline{p}_i^{n_i} A \subset C$. Αν $m = n_1 + \cdots + n_s$, τότε έχουμε από τα 2.2.7 και 2.2.8 ότι $\overline{P}^m A \subset C$. Το γεγονός ότι $\overline{P} = P/I$ και $IA = 0$ συνεπάγει ότι $P^m A \subset C$. □

Ορισμός 2.2.10. *Έστω R να είναι αντιμεταθετικός δακτύλιος με μονάδα και B ένα R-module:*

(i) *Ένα submodule A ($\neq B$) είναι πρωταρχικό αν $r \in R, b \notin A$ και $rb \in A$, τότε $r^n B \subset A$ για κάποιο $n > 0$.*

(ii) *Ένα submodule C του B έχει μια πρωταρχική αποσύνθεση αν $C = A_1 \cap \cdots \cap A_n$ με κάθε A_i ένα P_i-πρωταρχικό submodule του B κάποιο πρώτο ιδεώδες P_i του R. Αν A_i δεν περιέχεται στην $A_1 \cap \cdots \cap A_{i-1} \cap A_{i+1} \cap \cdots \cap A_n$ και αν τα ιδεώδη $P_1, \ldots, P_n$ είναι διακεκριμένα, τότε η πρωταρχική αποσύνθεση λέγεται μειωμένη.*

(iii) *Ένα πρωταρχικό submodule A ενός module B λέγεται P-πρωταρχικό submodule του B αν $P = R$ και $Q_a = \{r \in R \mid r^n B \subset A, n > 0\}$.*

Ορισμός 2.2.11. *Μια πρωταρχική αποσύνθεση ενός ιδεώδους a στον δακτύλιο A είναι μια έκφραση του a ως πεπερασμένη τομή πρωταρχικών ιδεωδών, έστω η $a = \cap_{i=1}^{n} q_i$.*

Θεώρημα 2.2.12. *Έστω R ένας αντιμεταθετικός δακτύλιος με μονάδα και B ένα R-module που ικανοποιεί τη συνθήκη αύξουσας αλυσίδας σε submodules. Τότε κάθε submodule A ($\neq B$) έχει μια μειωμένη πρωταρχική αποσύνθεση. Συγκεκριμένα, κάθε submodule A ($\neq B$) ενός πεπερασμένα παραγόμενου module B επί ενός αντιμεταθετικού Noetherian δακτύλιου R και κάθε ιδεώδες ($\neq R$) του R έχει μια μειωμένη πρωταρχική αποσύνθεση.*

Απόδειξη. Έστω S το σύνολο όλων των submodules του B τα οποία δεν έχουν πρωταρχική αποσύνθεση. Προφανώς, δεν υπάρχουν πρωταρχικά submodule στο S. Πρέπει να δείξουμε ότι S είναι κενό. Αν S είναι μη κενό, τότε S περιέχει ένα μέγιστο στοιχείο C. Αφού C δεν είναι πρωταρχικό, υπάρχει $r \in R$ και $b \in B - C$ τέτοιο ώστε $rb \in C$ αλλά $r^n B \nsubseteq C \ \ \forall n > 0$. Έστω $B_n = \{x \in B \mid r^n x \in C\}$. Τότε κάθε B_n είναι ένα submodule του B και $B_1 \subset B_2 \subset \cdots$. Από υπόθεση υπάρχει $k > 0$ τ.ω $B_i = B_k \ \ \forall i \geq k$. Έστω D το submodule $\{x \in B \mid x = r^k y + c \ \text{ για κάποια } \ y \in B, c \in C\}$. Προφανώς $C \subset B_k \cap D$. Αντίστροφα, αν $x \in B_k \cap D$, τότε $x = r^k y + c$ και $r^k x \in C$, απ' όπου $r^{2k} y = r^k(r^k y) = r^k(x - c) = r^k x - r^k c \in C$. Άρα $y \in B_{2k} = B_k$. Επομένως, $r^k y \in C$ και έτσι $x = r^k y + c \in C$. Άρα $B_k \cap D \subset C$, απ' όπου $B_k \cap D = C$. Τώρα $C \neq B_k \neq B$ και $C \neq D \neq B$ αφού $b \in B_k - C$ και $r^k B \nsubseteq C$. Από τη μεγιστότητα του

C στο S, B_k και D πρέπει να έχουν πρωταρχικές αποσυνθέσεις. Έτσι C έχει μια πρωταρχική αποσύνθεση, το οποίο είναι άτοπο. Άρα, S είναι κενό και κάθε submodule έχει πρωταρχική αποσύνθεση. Επομένως, κάθε submodule έχει μια μειωμένη πρωταρχική αποσύνθεση. $\square$

Θεώρημα 2.2.13. *Έστω R ένας αντιμεταθετικός δακτύλιος με μονάδα, I είναι ένα ιδεώδες του R και A ένα Noetherian R-module. Αν $B = \cap_{n=1}^{\infty} I^n A$, τότε $IB = B$.*

Απόδειξη. Αν $IB = A$, τότε $A = IB \subset B$, από όπου $B = A = IB$. Αν $B \neq A$, τότε από 2.2.12 το IB έχει μία πρωταρχική διάσπαση :

$$IB = A_1 \cap A_2 \cap \cdots \cap A_s,$$

όπου κάθε A_i είναι ένα P_i-πρωταρχικό submodule του A για κάποιο πρώτο ιδεώδες P_i του R. Αφού $IB \subset B$ σε κάθε περίπτωση, χρειαζόμαστε να δείξουμε μόνο ότι $B \subset A_i$ για κάθε i για καταλήξουμε στο ότι $B \subset IB$ και έτσι $B = IB$. Έστω $\imath (1 \leq \imath \leq s)$ δοσμένο. Υποθέτω πρώτα ότι $I \subset P_i$. Από το προηγούμενο λήμμα υπάρχει ένας ακέραιος m τέτοιος ώστε $P_i^m A \subset A_i$, απ' όπου $B = \cap_n I^n A \subset I^m A \subset P_i^m A \subset A_i$. Τώρα υποθέτω ότι $I \not\subseteq P_i$. Τότε υπάρχει $r \in I - P_i$. Αν $B \not\subseteq A_i$, τότε υπάρχει $b \in B - A_i$. Αφού $rb \in IB \subset A_i$, b δεν ανήκει στο A_i και A_i είναι πρωταρχικό, $r^n A \subset A_i$ για κάποιο $n > 0$. Επομένως, $r \in P_i$ αφού A_i είναι ένα P_i-πρωταρχικό submodule. Αυτό έρχεται σε αντίθεση με την επιλογή του $r \in I - P_i$. Άρα, $B \subset A_i$. $\square$

Παρατήρηση 2.2.14. *Σε έναν μη μηδενικό δακτύλιο R με μονάδα υπάρχουν πάντα μέγιστα ιδεώδη. Κάθε ιδεώδες στο R (εκτός του R) περιέχεται σε ένα μέγιστο ιδεώδες.*

Λήμμα 2.2.15. *Αν J είναι ένα ιδεώδες σε έναν αντιμεταθετικό δακτύλιο R με μονάδα, τότε τα παρακάτω είναι ισοδύναμα.*

(i) *το J περιέχεται σε κάθε μέγιστο ιδεώδες του R*

(ii) *$1_R - j$ είναι μια μονάδα για κάθε $j \in J$*

(iii) *Αν A είναι ένα πεπερασμένα παραγόμενο R-module τέτοιο ώστε $JA = A$, τότε $A = 0$*

(iv) *Αν B είναι ένα submodule ενός πεπερασμένα παραγόμενου R-module A τέτοιο ώστε $A = JA + B$, τότε $A = B$.*

Απόδειξη. $(\imath) \Rightarrow (\imath\imath)$ αν $j \in J$ και $1_R - j$ δεν είναι μονάδα, τότε το ιδεώδες $(1_R - j)$ δεν είναι R αυτό κάθε αυτό 1.2.5 και επομένως περιέχεται σε ένα μέγιστο ιδεώδες $M \neq R$ 2.2.14. Αλλά $1_R - j \in M$ και $j \in j \subset M$ συνεπάγουν ότι $1_R \in M$, το οποίο είναι άτοπο. Άρα, $1_R - j$ είναι μια μονάδα. $(\imath) \Rightarrow (\imath\imath)$ Αφού A είναι πεπερασμένα παραγόμενο, θα πρέπει να υπάρχει ένα ελάχιστα παραγόμενο σύνολο $X = \{a_1, \ldots, a_n\}$ του A. Αν $A \neq 0$, τότε $a_1 \neq 0$ από ελαχιστότητα.Αφού $JA = A$, $a_1 = j_1 a_1 + \cdots + j_n a_n (j_i \in J)$, από όπου $1_R a_1 = a_1$ έτσι ώστε $(1_R - j_1) a_1 = 0$ αν $n = 1$ και

$$(1_R - j_1) a_1 = j_2 a_2 + \cdots + j_n a_n \text{αν} n > 1$$

. Αφού $1_R - j_1$ είναι μια μονάδα στο R, $a_1 = (1_R - j_1)^{-1}(1_R - j_1) a_1$. Έτσι αν $n = 1$, τότε $a_1 = 0$ το οποίο είναι άτοπο. Αν $n > 1$, τότε a_1 γράφεται σαν γραμμικός συνδυασμός των $a_2, \ldots, a_n$. Επομενως, $\{a_2, \ldots, a_n\}$ παράγουν το A, το οποίο έρχεται σε αντίθεση με την επιλογή του X. $(\iota\iota\iota) \Rightarrow (\iota)$ Επιβεβαιώστε ότι το χυοτιεντ module A/B είναι τέτοιο ώστε $J(A/B) = A/B$, από όπου $A/B = 0$ και $A = B$ από το $(\iota\iota\iota)$. $(\iota) \Rightarrow (\iota)$ Αν M είναι ένα οποιοδήποτε μέγιστο ιδεώδες, τότε το ιδεώδες $JR + M$ περιέχει το M. Αλλά $JR + M \neq R$ (Αλλιώς $R = M$ από το (ι». Επομένως, $JR + M = M$ από μεγιστότητα. Άρα, $J = JR \subset M$. □

Θεώρημα 2.2.16. *Έστω J ένα ιδεώδες σε έναν αντιμεταθετικό δακτύλιο R με μονάδα. Τότε J περιέχεται σε κάθε μέγιστο ιδεώδες του R αν και μόνο αν για κάθε R-module A ικανοποιείται η συνθήκη αύξουσας αλυσίδας σε submodules, $\cap_{n=1}^{\infty} J^n A = 0$.*

Απόδειξη. ($\Rightarrow$) Αν $B = \cap_n J^n A$, τότε $JB = B$ από 2.2.13. Αφού B είναι πεπερασμένα παραγόμενο 2.1.11, $B = 0$ από 2.2.15. ($\Leftarrow$) Υποθέτουμε ότι $R \neq 0$. Αν M είναι ένα οποιοδήποτε μέγιστο ιδεώδες του R, τότε $M \neq R$ και $A = R/M$ είναι ένα μη μηδενικό R-module το οποίο δεν έχει κατάλληλα submodules. Έτσι A τετριμμένα ικανοποιεί τη συνθήκη αύξουσας αλυσίδας, απ' όπου $\cap_n J^n A = 0$ από υπόθεση. Αφού JA είναι ένα submodule του A, είτε $JA = A$ ή $JA = 0$. Αν $JA = A$, τότε $J^n A = A \forall n$. Επομένως, $\cap_n J^n A = A \neq 0$, το οποίο είναι άτοπο. Έτσι $JA = 0$. Αλλά $0 = JA = J(R/M)$ συνεπάγεται ότι $J \subset JR \subset M$. □

Πόρισμα 2.2.17. *Αν R είναι ένας Noetherian τοπικός δακτύλιος με μέγιστο ιδεώδες M, τότε $\cap_{n=1}^{\infty} M^n = 0$.*

Απόδειξη. Αν $J = M$ και $A = R$, τότε $J^n A = M^n$ από το προηγούμενο θεώρημα. □

Ορισμός 2.2.18. *Ένας τοπικός δακτύλιος είναι ένας δακτύλιος R με ένα μοναδικό μέγιστο ιδεώδες m.*

Θεώρημα 2.2.19. *Αν R τοπικός δακτύλιος, τότε κάθε πεπερασμένα παραγόμενο προβολικό R-module είναι ελεύθερο.*

Απόδειξη. Αν P είναι ένα πεπερασμένα παραγόμενο προβολικό R-module,τότε από πόρισμα υπάρχει ένα ελεύθερο R-module F με μια πεπερασμένη βάση και έναν επιμορφισμό $\pi : F \to P$. Από όλα τα ελεύθερα R-modules F με αυτή την ιδιότητα διαλέγω ένα με μία βάση $\{x_1, \ldots, x_n\}$ η οποία έχει έναν ελάχιστο αριθμό στοιχείων. Αφού π είναι επιμορφισμός $\{\pi(x_1), \ldots, \pi(x_n)\}$ αναγκαστικά παράγουν το P. Πρώτα θα δείξουμε ότι $K = \ker \pi$ περιέχεται στο MF, όπου M είναι το μοναδικό μέγιστο ιδεώδες του R. Αν $K \not\subset MF$, τότε υπάρχει $k \in K$ με k δεν ανήκει στο MF. Τώρα $k = r_1 x_1 + \cdots + r_n x_n$ με $r_i \in R$ μοναδικά καθορισμένο. Αφού k δεν ανήκει στο MF, κάποια από τα r_i,έστω το r_1,δεν είναι στοιχείο του M. Από θεώρημα, το r_1 είναι μονάδα, απ' όπου $x_1 - r_1^{-1} k = -r_1^{-1} r_2 x_2 - \cdots - r_1^{-1} r_n x_n$. Επομένως, αφού $k \in \ker \pi, \pi(x_1) = \pi(x_1 - r_1^{-1} k) = \pi(\sum_{i=2}^{n} -r_1^{-1} r_i x_i) = \sum_{i=2}^{n} -r_1 r_i \pi(x_i)$. Άρα,$\{\pi(x_2), \ldots, \pi(x_n)\}$ παράγει το P. Έτσι εάν F' είναι το ελεύθερο submodule του F με βάση $x_2, \ldots, x_n$ και $\pi' : F' \to P$ ο περιορισμός του π' στο F', τότε π' είναι ένας επιμορφισμός. Αυτό έρχεται σε αντίθεση με την επιλογή του F να έχει μία βάση με ελάχιστο πληθάριθμο. Έτσι $K \subset MF$. Αφού $0 \to K \xrightarrow{\subseteq} F \xrightarrow{\pi} P \to 0$ είναι ακριβής τότε και P είναι προβολικό $K \oplus P \cong F$ από θεώρημα. Υπό τον ισομορφισμό $(k, 0) \mapsto k, \forall k \in K$, απ' όπου F είναι το εσωτερικό ευθύ άθροισμα $F = K \oplus P'$ με $P' \cong P$. Έτσι $F = K + P' \subset MF + P'$. Αν $u \in F$, τότε $u = \sum_i m_i v_i + p_i$ με $m_i \in M, v_i \in F, p_i \in P'$. Επομένως, στο R-module F/P',

$$u + P' = \sum_i m_i v_i + P' = \sum_i m_i(v_i + P') \in M(F/P')$$

, απ' όπου $M(F/P') = F/P'$. Αφού F είναι πεπερασμένα παραγόμενο, θα είναι και το F/P'. Άρα $K \cong F/P'$ από 2.2.15. Έτσι $P \cong P' = F$ και P είναι ελεύθερο. □

Θεώρημα 2.2.20. *Αν R είναι ένας αντιμεταθετικός Noetherian δακτύλιος με μονάδα, τότε το ίδιο είναι και ο $R[x_1, \ldots, x_n]$.*

Απόδειξη. Προφανώς αρκεί να δείξουμε ότι $R[x]$ είναι Noetherian. Από 2.1.11 αρκεί να δείξουμε ότι κάθε ιδεώδες J στο $R[x]$ είναι πεπερασμένα παραγόμενο. Για κάθε $n \geq 0$, έστω I_n να είναι το σύνολο όλων των $r \in R$ τέτοια ώστε $r = 0$ ή r είναι ο μεγιστοβάθμιος συντελεστής ενός πολυωνύμου $f \in J$ βαθμού n. Επιβεβαιώστε ότι κάθε I_n είναι ένα ιδεώδες του R. Αν r είναι ένα μη μηδενικό στοιχείο του I_n και $f \in J$ είναι ένα πολυώνυμο βαθμού n με μεγιστοβάθμιο συντελεστή r, τότε r είναι επίσης ο μεγιστοβάθμιος συντελεστής του xf, το οποίο είναι πολυώνυμο στο J βαθμού $n+1$. Έτσι $I_0 \subset I_1 \subset I_2 \subset \cdots$. Αφού R είναι Noetherian, υπάρχει ένας ακέραιος t τέτοιος ώστε $I_n = I_t, \forall n \geq t$: επιπλέον, από 2.1.11 κάθε $I_n (n \geq 0)$ είναι πεπερασμένα παραγόμενο έστω $I_n = (r_{n1}, r_{n2}, \ldots, r_{ni_n})$. Για κάθε r_{nj} με $0 \leq n \leq t$ και $1 \leq j \leq i_n$, έστω $f_{nj} \in J$ να είναι ένα πολυώνυμο βαθμού n με μεγιστοβάθμιο συντελεστή r_{nj}. Παρατηρήστε ότι $f_{0j} = r_{0j} \in R \subset R[x]$. Θα δείξουμε ότι το ιδεώδες J του $R[x]$ παράγεται από το πεπερασμένο σύνολο των πολυωνύμων $X = \{f \mid 0 \leq n \leq t; 1 \leq j \leq i_n\}$. Προφανώς, $(X) \subset J$. Αντίστροφα, τα πολυώνυμα μηδενικού βαθμού στο J είναι ακριβώς τα στοιχεία του I_0 και έτσι περιέχονται στο (X). Με επαγωγή, υποθέτω ότι (X) περιέχει όλα τα πολυώνυμα του J με βαθμό λιγότερο από k και έστω $g \in J$ να έχει βαθμό k και μεγιστοβάθμιο συντελεστή $r \neq 0$. Αν $k \leq t$, τότε $r \in I_k$ και έτσι $r = s_1 r_{k1} + s_2 r_{k2} + \cdots + s_{i_k} r_{ki_k}$ για κάποια $s_j \in R$. Άρα τα πολυώνυμα $\sum_{j=1}^{i_k} s_j f_{kj} \in (X)$ έχει μεγιστοβάθμιο συντελεστή r και βαθμό k. Επομένως, $g - \sum_j s_j f_{kj}$ έχει βαθμό το πολύ $k-1$. Από επαγωγική υπόθεση $g - \sum_j s_j f_{kj} \in (X)$, απ' όπου $g \in (X)$. Αν $k \geq t$, τότε $r \in I_k = I_t$ και $r = \sum_{j=1}^{i_t} s_j r_{tj} (s_j \in R)$. Επιπλέον $\sum_{j=1}^{i_t} s_j x^{k-t} f_{tj} \in (X)$ έχει μεγιστοβάθμιο συντελεστή r και βαθμό k. Έτσι $g - \sum_j s_j x^{k-t} f_{tj}$ έχει βαθμό το πολύ $k-1$ και βρίσκεται στο (X) από επαγωγική υπόθεση. Επομένως, $g \in (X)$ και ολοκληρώνεται η επαγωγή. Άρα, $J = (X)$. □

Θεώρημα 2.2.21. *Αν R είναι ένας αντιμεταθετικός Noetherian δακτύλιος με μονάδα, τότε είναι και το $R[[x]]$.*

Απόδειξη. Αρκεί από 2.2.2 αρκεί να δείξουμε ότι κάθε πρώτο ιδεώδες P στο $R[[x]]$ είναι πεπερασμένα παραγόμενο. Ορίζω έναν επιμορφισμό δακτυλίων $R[[x]] \to R$ ο οποίος στέλνει κάθε δυναμοσειρά $f = \sum_{i=0}^{\infty} a_i x^i$ στον σταθερό όρο a_0. Έστω $P*$ να είναι η εικόνα του P υπό αυτή την απεικόνιση. Τότε $P*$ είναι πεπερασμένα παραγόμενο ιδεώδες στο R 2.1.11, ας είναι $P* = (r_1, \ldots, r_n)$. Για κάθε r_i διαλέγω

$f_i \in P$ με σταθερό όρο r_i. Αν $x \in P$, ισχυριζόμαστε ότι P παράγεται από τα $r_1, \ldots, r_n, x$. Πρώτα σημειώνουμε ότι αν $f_k = r_k + \sum_{i=1}^{\infty} a_i x^i$, τότε $r_k = f_k - x(\sum_{j=0}^{\infty} a_{j+1} x^j) \in P$. Αν $g = \sum_{i=0}^{\infty} b_i x^i \in P$, τότε $b_0 = s_1 r_1 + \cdots + s_n r_n$ για κάποια $s_i \in R$. Επομένως, $g - \sum_{i=1}^{n} s_i r_i$ έχει μηδενικό σταθερό όρο: ο οποίος είναι $g - \sum_i s_i r_i = x g_1 (g_1 \in R[[x]])$. Άρα, $g = \sum_i s_i r_i + x g_1$ και P παράγεται από τα $r_1, \ldots, r_n, x$. Αν x δεν ανήκει στο P, ισχυριζόμαστε ότι P παράγεται από τα $f_1, \ldots, f_n \in P$. Αν $h = \sum_{i=0}^{\infty} c_i x^i \in P$, τότε $c_0 = t_1 r_1 + \cdots + t_n r_n$ για κάποια $t_i \in R$. Επομένως, $h - \sum_{i=1}^{n} t_i f_i = xh*$ για κάποιο $h* \in R[[x]]$. Αφού x δεν ανήκει στο P και $xh* = h = \sum_i t_i f_i \in P$ και P είναι πρώτο, έχουμε ότι $h* \in P$. Για κάθε $h \in P$, διαλέγω $t_i \in R$ και $h* \in P$ τέτοια ώστε $h = \sum_{i=1}^{m} t_i f_i + xh * (AC)$. Έστω $\lambda : P \to P$ να είναι η απεικόνιση που ορίζεται με $h \mapsto h*$. Έστω g ένα οποιοδήποτε στοιχείο του P. Τότε από 2.1.4 (με $\lambda = f_n, \forall n$) υπάρχει μία συνάρτηση $\phi \mathbf{N} \to P$ τέτοια ώστε

$$\phi(0) = g \ \text{ και } \ \phi(k+1) = \lambda(\phi(k)) = k * .$$

Έστω $\phi(k) = h_k \in R[[x]]$ και συμβόλισε με t_{ki} τα προηγούμενα στοιχεία του R τέτοια ώστε

$$h_k = \sum_{i=1}^{n} t_{ki} f_i + x h_k * = \sum_{i=1}^{n} t_{ki} f_i + x h_{k+1}.$$

Για κάθε $i (1 \leq i \leq n)$ έστω $g_i = \sum_{k=0}^{\infty} t_{ki} x_k \in R[[x]]$. Τότε

$$g_1 f_1 + \cdots + g_n f_n = \sum_{i=1}^{n} (\sum_{k=0}^{\infty} t_{ki} x^k) f_i = \sum_{k=0}^{\infty} (\sum_{i=1}^{n} t_{ki} f_i) x^k = \sum_{k=0}^{\infty} (h_k - x h_{k+1}) x^k.$$

Επομένως, για κάθε $m \geq 0$ ο συντελεστής του x^m στο $g_1 f_1 + \cdots + g_n f_n$ είναι ο ίδιος με τον συντελεστή του x^m στο $\sum_{k=0}^{m} (h_k - x h_{k+1}) x^k$. Αφού

$$\sum_{k=0}^{m} (h_k - x h_{k+1}) x^k = h_0 - x^{m+1} h_{m+1} = g - x^{m+1} h_{m+1},$$

ο συντελεστής του x^m στο $f_1 g_1 + \cdots + f_n g_n$ είναι ακριβώς ο συντελεστής του x^m στο g. Άρα, $g = g_1 f_1 + \cdots + g_n f_n$ και $f_1, \ldots, f_n$ παράγουν το P. $\square$

Κεφάλαιο 3

Artin και Noether δακτύλιοι

3.1 Επιπλέον για Noether δακτυλίους

Θεώρημα 3.1.1. *Υποθέτω ότι M έχει μια σύνθεση σειράς μήκους n. Τότε κάθε σύνθεση σειράς του M έχει μήκος n, και κάθε αλυσίδα του M μπορεί να επεκταθεί σε μια σύνθεση σειράς.*

Απόδειξη. Έστω $\ell(M)$ το ελάχιστο μήκος μιας σύνθεσης σειράς ενός module M. ($\ell(M) = \infty$ αν M δεν έχει σύνθεση σειράς).

(i) $N \subset M \Rightarrow \ell(N) < \ell(M)$. Έστω (M_i) μια σύνθεση σειράς του M ελαχίστου μήκους και θεωρώ τα submodules $N_i = N \cap M_i$ του N. Αφού $N_{i-1}/N_i \subseteq M_{i-1}/M_i$ και το τελευταίο είναι ένα απλό module, έχουμε είτε $N_{i-1}/N_i = M_{i-1}/M_i$, ή αλλιώς $N_{i-1} = N_i$, απ' όπου αφαιρώντας επαναλαμβανόμενους όρους έχουμε μια σύνθεση σειράς του N, τέτοια ώστε $\ell(N) \leq \ell(M)$. Αν $\ell(N) = \ell(M) = n$, τότε $N_{i-1}/N_i = M_{i-1}/M_i$ για κάθε $i = 1, \ldots, n$, έτσι $M_{n-1} = N_{n-1}, M_{n-2} = N_{n-2}, \ldots$ και τελικά $M = N$.

(ii) Κάθε αλυσίδα στο M έχει μήκος $\leq \ell(M)$. Έστω $M = M_0 \supset M_1 \supset \ldots$ μια αλυσίδα μήκους k. Τότε από το (i) έχουμε $\ell(M) > \ell(M_1) > \cdots > \ell(M_k) = 0$, έτσι $\ell(M) \geq k$.

(iii) Έστω οποιαδήποτε σύνθεση σειράς του M. Αν έχει μήκος k, τότε $k \leq \ell(M)$ από το (ii), έτσι $k = \ell(M)$ από ορισμό του $\ell(M)$. Έτσι όλες οι συνθέσεις σειράς έχουν το ίδιο μήκος. Τελικά, έστω οποιαδήποτε αλυσίδα. Αν το μήκος της είναι $\ell(M)$, τότε πρέπει να είναι σύνθεση σειράς. Αν το μήκος της είναι $< \ell(M)$ δεν είναι σύνθεση σειράς, έτσι όχι μέγιστη, και έτσι μπορούμε να προσθέσουμε όρους μέχρι το μήκος να γίνει $\ell(M)$.

□

Παρατήρηση 3.1.2. *Τα παρακάτω είναι ισοδύναμα:*

(i) *Κάθε αύξουσα ακολουθία $x_1 \leq x_2 \leq \ldots$ στο S είναι σταθερή. (υπάρχει n τέτοιο ώστε $x_n = x_{n+1} = \ldots$).*

(ii) *Κάθε μη κενό υποσύνολο του S έχει ένα μέγιστο στοιχείο.*

Θεώρημα 3.1.3. *Το M έχει σύνθεση σειρών αν και μόνο αν το M ικανοποιεί και τις δύο συνθήκες αλυσίδων.*

Απόδειξη. ($\rightarrow$) Όλες οι αλυσίδες είναι οριοθετιμένου μήκους, έτσι ισχύουν και οι δύο συνθήκες. ($\leftarrow$) Κατασκευάζουμε μια σύνθεση σειρών του M ως εξής. Αφού $M = M_0$ ικανοποιείται η συνθήκη μεγίστου από 3.1.2, και άρα έχει ένα μέγιστο submodule $M_1 \subset M_0$. Παρόμοια, M_1 έχει ένα μέγιστο submodule $M_2 \subset M_1$, και ομοίως συνεχίζουμε. Έτσι έχουμε μια αυστηρώς φθίνουσα αλυσίδα $M_0 \supset M_1 \supset \dots$ η οποία από συνθήκη φθίνουσας αλυσίδας πρέπει να είναι πεπερασμένη και έτσι είναι μια σύνθεση σειρών του M. □

Θεώρημα 3.1.4. *Για k-διανυσματικό χώρο V οι παρακάτω συνθήκες είναι ισοδύναμες:*

(i) *πεπερασμένη διάσταση*

(ii) *πεπερασμένο μήκος*

(iii) *συνθήκη αύξουσας αλυσίδας*

(iv) *συνθήκη φθίνουσας αλυσίδας.*
Επιπλέον, αν ικανοποιούνται αυτές οι συνθήκες έχουμε ότι το μήκος ισούται με την διάσταση.

Απόδειξη. $(i) \rightarrow (ii)$ Προφανές. $(ii) \rightarrow (iii), (iii) \rightarrow (iv)$ από το προηγούμενο θεώρημα. Μένει να δείξουμε ότι $(iii) \rightarrow (i)$ και $(iv) \rightarrow (i)$. Υποθέτουμε ότι δεν έχει πεπερασμένη διάσταση. Τότε υπάρχει μια άπειρη ακολουθία $(x_n)_{n>1}$ από γραμμικώς ανεξάρτητα στοιχεία του V. Έστω U_n (αντ. V_n) να είναι ο διανυσματικός χώρος που καλύπτεται από τα $x_1, \dots, x_n$ (αντ. $x_{n+1}, x_{n+2}, \dots$). Τότε η αλυσίδα $(U_n)_{n\geq 1}$ (αντ. $(V_n)_{n\geq 1}$) είναι άπειρη και αυστηρώς αύξουσα (αντ. αυστηρώς φθίνουσα). □

Χρειαζόμαστε το παρακάτω αποτέλεσμα:

Παρατήρηση 3.1.5. *Έστω $0 \rightarrow M' \xrightarrow{a} M \xrightarrow{b} M'' \rightarrow 0$ μία ακριβής ακολουθία από A-modules. Τότε:*

(i) *M Noetherian αν-ν M' και M'' Noetherian*

(ii) *M Artinian αν-ν M' και M'' Artinian*

Θεώρημα 3.1.6. *Έστω A ένας δακτύλιος στον οποίο το μηδενικό ιδεώδες είναι ένα γινόμενο $m_1 \cdots m_n$ από μέγιστα ιδεώδη. Τότε A είναι Noetherian αν και μόνο αν A Artinian.*

Απόδειξη. Θεωρούμε την αλυσίδα από ιδεώδη $A \supset m_1 \supseteq m_1 m_2 \supseteq \cdots \supseteq m_1 \cdots m_n = 0$. Κάθε παράγοντας $m_1 \cdots m_{i-1}/m_1 \cdots m_i$ είναι διανυσματικός χώρος επί του A/m_i. Έτσι συνθήκη αύξουσας αλυσίδας αν-ν συνθήκη φθίνουσας αλυσίδας για κάθε παράγοντα. Αλλά, συνθήκη αύξουσας αλυσίδας (αντ. συνθήκη φθίνουσας αλυσίδας) για κάθε παράγοντα αν-ν συνθήκη αύξουσας αλυσίδας (αντ. συνθήκη φθίνουσας αλυσίδας) για το A, από επαναλαμβανόμενη εφαρμογή του θεωρήματος 3.1.5. Έτσι συνθήκη αύξουσας αλυσίδας αν-ν συνθήκη φθίνουσας αλυσίδας για το A. □

Ορισμός 3.1.7. *Ένα ιδεώδες a λέγεται ανάγωγο αν $a = b \cap c \Rightarrow (a = bora = c)$*

Λήμμα 3.1.8. *Σε έναν Noetherian δακτύλιο A κάθε ιδεώδες είναι μια πεπερασμένη τομή ανάγωγων ιδεωδών.*

Απόδειξη. Υποθέτουμε το αντίθετο. Τότε το σύνολο από ιδεώδη του A για το οποίο το λήμμα είναι λανθασμένο είναι μη κενό, και έτσι έχει ένα μέγιστο στοιχείο a. Αφού a είναι αναγώγιμο έχουμε $a = b \cap c$ όπου $b \supset a$ και $c \supset a$. Έτσι κάθε ένα από τα b, c είναι μια πεπερασμένη τομή από ανάγωγα ιδεώδη και έτσι και το a. Άτοπο! □

Θεώρημα 3.1.9. *Σε έναν Noetherian δακτύλιο κάθε ανάγωγο ιδεώδες είναι πρωταρχικό.*

Απόδειξη. Αρκεί να δείξουμε ότι αν το μηδενικό ιδεώδες είναι αμείωτο τότε είναι πρωταρχικό. Έστω $xy = 0$ με $y \neq 0$ και έστω η αλυσίδα από ιδεώδη $Ann(x) \subseteq Ann(x^2) \subseteq \ldots$. Από τη συνθήκη αύξουσας αλυσίδας, είναι σταθερή το οποίο σημαίνει ότι $Ann(x^n) = Ann(x^{n+1}) = \ldots$ για κάποιο n. Ακολουθεί ότι $x^n \cap (y) = 0$: αν $a \in (y)$ τότε $ax = 0$ και αν $a \in (x^n)$ τότε $a = bx^n$, έτσι $bx^{n+1} = 0$, απ' όπου έχουμε $b \in Ann(x^{n+1}) = Ann(x^n)$, έτσι $bx^n = 0$ και άρα $a = 0$. Αφού το (0) είναι αμείωτο και $(y) \neq 0$ πρέπει να έχουμε $x^n = 0$ και αυτό σημαίνει ότι (0) είναι πρωταρχικό. □

Θεώρημα 3.1.10. *Σε έναν Noetherian δακτύλιο A κάθε ιδεώδες έχει μία πρωταρχική αποσύνθεση.*

Θεώρημα 3.1.11. *Σε έναν Noetherian δακτύλιο A κάθε ιδεώδες a περιέχει μια δύναμη της ρίζας του.*

Απόδειξη. Έστω τα $x_1, \ldots, x_k$ παράγουν το $r(a) : x_i^{n_i} \in a (1 \leq i \leq k)$. Έστω $m = \sum_{i=1}^{k}(n_i - 1) + 1$. Τότε $r(a)^m$ παράγεται από το γινόμενο $x_1^{r_1} \cdots x_k^{r_k}$ με $\sum_i r_i = m$. Από ορισμό του m πρέπει να έχουμε $r_i \geq n_i$ για τουλάχιστον έναν δείκτη i. Έτσι κάθε μονώνυμο βρίσκεται στο a, και έτσι $r(a)^m \subseteq a$. □

Θεώρημα 3.1.12. *Σε έναν Noetherian δακτύλιο το nilradical είναι μηδενοδύναμο.*

Απόδειξη. Αν πάρουμε για $(a) = 0$ από το προηγούμενο θεώρημα προκύπτει το ζητούμενο. □

3.2 Artin δακτύλιοι

Θεώρημα 3.2.1. *Σε έναν Artinian δακτύλιο A κάθε πρώτο ιδεώδες είναι μέγιστο.*

Απόδειξη. Έστω p ένα πρώτο ιδεώδες του A. Τότε $B = A/p$ είναι μια Artinian ακέραια περιοχή. Έστω $x \in B, x \neq 0$. Από συνθήκη φθίνουσας αλυσίδας έχουμε $(x^n) = (x^{n+1})$ για κάποιο n έτσι $x^n = x^{n+1}y$ για κάποιο $y \in B$. Αφού B είναι ακέραια περιοχή και $x \neq 0$, μπορώ να διαγράψω τα x^n και έτσι $xy = 1$. Έτσι x έχει αντίστροφο στο B, και άρα το B είναι σώμα τέτοιο ώστε p είναι ένα μέγιστο ιδεώδες. □

Ορισμός 3.2.2. *Ένα στοιχείο x (αντ. ένα ιδεώδες I) λέγεται μηδενοδύναμο εάν υπάρχει n τέτοιο ώστε $x^n = 0$ (αντ. $I^n = 0$).*

Ορισμός 3.2.3. *Nilradical ενός αντιμεταθετικού δακτυλίου είναι το ιδεώδες που περιέχει τα μηδενοδύναμα στοιχεία.*

Ορισμός 3.2.4. *Το ριζικό Jacobson ενός δακτυλίου R είναι η τομή των μέγιστων ιδεωδών του R.*

Αφού όλα τα μέγιστα ιδεώδη είναι πρώτα, το nilradical περιέχεται στο ριζικό Jacobson.

Παρατήρηση 3.2.5. *Σε έναν Artinian δακτύλιο το nilradical ισούται με το ριζικό Jacobson.*

Έχουμε την παρακάτω πρόταση χωρίς απόδειξη:

Πρόταση 3.2.6. *Έστω $a_1, \dots, a_n$ ιδεώδη και p ένα πρώτο ιδεώδες που περιέχεται στην τομή $\cap_{i=1}^n a_i$. Τότε $p \supseteq a_i$ για κάποιο i. Αν $p = \cap a_i \Rightarrow p = a_i$*

Θεώρημα 3.2.7. *Ένας Artinian δακτύλιος έχει μόνο έναν πεπερασμένο αριθμό από μέγιστα ιδεώδη.*

Απόδειξη. Θεωρώ το σύνολο όλων των πεπερασμένων τομών $m_1 \cap \cdots \cap m_r$, m_i μέγιστα ιδεώδη. Αυτό το σύνολο έχει ελάχιστο στοιχείο, έστω το $m_1 \cap \cdots \cap m_n$. Έτσι για κάθε μέγιστο ιδεώδες m έχουμε $m \cap m_1 \cap \cdots \cap m_n = m_1 \cap \cdots \cap m_n$ και έτσι $m \supseteq m_1 \cap \cdots \cap m_n$. Από την παραπάνω πρόταση $m \supseteq m_i$ για κάποιο i. Άρα $m = m_i$ αφού m_i μέγιστο. □

Θεώρημα 3.2.8. *Σε έναν Aritinian δακτύλιο το nilradical R είναι μηδενοδύναμο.*

Απόδειξη. Από συνθήκη φθίνουσας αλυσίδας έχουμε $R^k = R^{k+1} = \cdots = a$, για κάποιο $k > 0$. Υποθέτουμε ότι $a \neq 0$, και έστω Σ το σύνολο όλων των ιδεωδών b τέτοια ώστε $ab \neq 0$. Τότε Σ είναι μη κενό αφού $a \in \Sigma$. Έστω c το ελάχιστο στοιχείο του Σ. Τότε υπάρχει $x \in c$ τέτοιο ώστε $xa \neq 0$. Έχουμε $(x) \subseteq c$, και έτσι $(x) = c$ από ελαχιστότητα του c. Αλλά $(xa)a = xa^2 = xa \neq 0$, και $xa \subseteq (x)$, έτσι $(x) = xa$ από ελαχιστότητα. Έτσι $x = xy$ για κάποιο $y \in a$ και άρα $x = xy = xy^2 = \cdots = xy^n = \dots$. Αλλά $y \in a = R^k \supseteq R$, έτσι y είναι μηδενοδύναμο και άρα $x = xy^n = 0$. Αυτό έρχεται σε αντίθεση με την επιλογή του x, και έτσι $a = 0$. □

Ορισμός 3.2.9. *Ορίζουμε ως διάσταση του A και συμβολίζουμε με $\dim A$ να είναι το supremum των μηκών όλων των αλυσίδων από πρώτα ιδεώδη στο A.*

Θεώρημα 3.2.10. *Ένας δακτύλιος A είναι Artinian αν-ν A είναι Noetherian και $\dim A = 0$.*

Απόδειξη. ($\Rightarrow$) Από 3.2.1 έχουμε ότι $\dim A = 0$. Έστω $m_i i = 1, \dots, n$ να είναι διακεκριμένα μέγιστα ιδεώδη του A 3.2.7. Τότε $\prod_{i=1}^n m_i^k \subseteq (\cap_{i=1}^n m_i)^k = R^k = 0$. Έτσι από 3.1.6 A Noetherian. ($\Rightarrow$) Αφού το μηδενικό ιδεώδες έχει πρωταρχική αποσύνθεση 3.1.10, A έχει μόνο έναν πεπερασμένο αριθμό από ελάχιστα πρώτα ιδεώδη, και όλα αυτά είναι μέγιστα αφού $\dim A = 0$. Έτσι $R = \cap_{i=1}^n m_i$, έχουμε $R^k = 0$ από 3.1.12, έτσι $\prod_{i=1}^n m_i^k = 0$ όπως στο προηγούμενο μέρος της απόδειξης. Από 3.1.6 A είναι Artinian. □

Για να αποδείξουμε το Θεμελιώδες Θεώρημα για Artinian δακτυλίους θα χρειαστούμε τα παρακάτω:

Θεώρημα 3.2.11. *Έστω A δακτύλιος και $a_1, \ldots, a_n$ ιδεώδη του A. Ορίζω ομομορφισμό $\phi : A \to \prod_{i=1}^{n}(A/a_i)$ με $\phi(x) = (x + a_1, \ldots, x + a_n)$.*

(i) *Αν a_i, a_j πρώτα μεταξύ τους για $i \neq j$, τότε $\prod a_i = \cap a_i$.*

(ii) *ϕ είναι επί αν-ν a_i, a_j πρώτα μεταξύ τους για $i \neq j$.*

(iii) *ϕ είναι $1:1$ αν-ν $\cap a_i = (0)$.*

Θεώρημα 3.2.12. *Έστω a, b ιδεώδη σε ένα δακτύλιο A τέτοια ώστε $r(a), r(b)$ πρώτα μεταξύ τους. Τότε a, b πρώτα μεταξύ τους. ($r(a) = \{x \in A \mid x^n \in a, n > 0\}$)*

Ορισμός 3.2.13. *Ένα σύνολο Σ από πρώτα ιδεώδη που ανήκουν στο a λέγεται απομονωμένο αν ικανοποιεί την παρακάτω συνθήκη: αν p' είναι ένα πρώτο ιδεώδες που ανήκει στο a και $p' \subseteq p$ για κάποιο $p \in \Sigma$, τότε $p' \in \Sigma$.*

Θεώρημα 3.2.14. *Οι απομονωμένες συνιστώσες (οι οποίες είναι οι πρωταρχικές συνιστώσες q_i που αντιστοιχούν σε ελάχιστα πρώτα ιδεώδη p_i) καθορίζονται μοναδικά από το a.*

Θεώρημα 3.2.15. *Ένας Artinian δακτύλιος A είναι μοναδικώς (μέχρι ισομορφισμών) ένα πεπερασμένο ευθύ γινόμενο από Artinian τοπικούς δακτυλίους.*

Απόδειξη. Έστω $m_i, i = 1, \ldots, n$ να είναι διακριτά μέγιστα ιδεώδη του A. Από την απόδειξη του 3.2.10 έχουμε ότι $\prod_{i=1}^{n} m_i^k = 0$ για κάποιο $k > 0$. Από 3.2.12 τα ιδεώδη m_i^k είναι ανά ζεύγη πρώτα μεταξύ τους, και έτσι $\cap m_i^k = \prod m_i^k$ από 3.2.11. Επομένως από 3.2.11 η φυσική απεικόνιση $A \to \prod_{i=1}^{n}(A/m_i^k)$ είναι ισομορφισμός. Κάθε A/m_i^k είναι ένας Artinian τοπικός δακτύλιος, και άρα A είναι ένα ευθύ γινόμενο από Artinian τοπικούς δακτυλίους. Αντίστροφα, υποθέτω ότι $A \cong \prod_{i=1}^{n} A_i$, όπου τα A_i είναι τοπικοί δακτύλιοι. Τότε για κάθε i έχουμε έναν φυσικό επιμορφισμό (προβολή στον i-οστό παράγοντα) $\phi_i : A \to A_i$. Έστω $a_i = \ker(\phi_i)$. Από 3.2.11 τα a_i είναι ανά ζεύγη πρώτα και $\cap a_i = 0$. Έστω q_i να είναι το μοναδικό πρώτο ιδεώδες του A_i και έστω p_i να είναι η αντίστροφη εικόνα του q_i, δηλαδή $\phi_i^{-1}(q_i)$. Το ιδεώδες p_i είναι πρώτο, και έτσι μέγιστο από 3.2.1. Αφού q_i είναι μηδενοδύναμο, έχουμε ότι a_i είναι p_i-πρωταρχικό και έτσι $\cap a_i = (0)$ είναι μια πρωταρχική απόσύνθεση του μηδενικού ιδεώδους στο A. Αφού τα a_i είναι ανά ζεύγη πρώτα, θα είναι και τα p_i, και άρα είναι απομονωμένα πρώτα ιδεώδη του (0). Έτσι όλες οι πρωταρχικές συνιστώσες a_i είναι απομονωμένες και άρα μοναδικά καθορισμένες από το A 3.2.14. Έτσι οι δακτύλιοι $A_i \cong A/a_i$ καθορίζονται μοναδικά από το A. □

Βιβλιογραφία

[1] Thomas W. Hungerford Algebra (1974)

[2] M. Atiyah Ig. Macdonald introduction to commutative algebra (1969)