Ορισμός | Έστω $A \subseteq R$ δακτύλιοι, A υποδακτύλιος του R.

Ένα στοιχείο $x \in R$ λέγεται ακέραιο επί του A, αν υπάρχουν $a_{n-1}, a_{n-2}, \dots, a_0 \in A$ με
$\underbrace{x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0}_{\text{μονικό πολυώνυμο}} = 0$.

Παράδειγμα $A = \mathbb{Z}$, $R = \mathbb{Q}$. Οι ρητοί που είναι ακέραιοι επί του $\mathbb{Z}$ θα είναι της μορφής $\frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$, και $(a,b) = 1$.

Έστω $\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \dots + a_1\left(\frac{a}{b}\right) + a_0 = 0$,
όπου $a_{n-1}, a_{n-2}, \dots, a_0 \in \mathbb{Z}$.
Τότε $a^n + a_{n-1}a^{n-1}b + \dots + a_1 a b^{n-1} + a_0 b^n = 0$.
Άρα $a^n = b(-a_{n-1}a^{n-1} - \dots - a_1 a b^{n-2} - a_0 b^{n-1})$
$\Rightarrow b \mid a^n$. Αλλά $(a,b) = 1 \Rightarrow (a^n, b) = 1$.
Από την άλλη, $b \mid a^n \Rightarrow (a^n, b) = |b|$.
Άρα $b = \pm 1 \Rightarrow \frac{a}{b} \in \mathbb{Z}$.

Θεώρημα! Έστω A υποδακτύλιος του R και $x \in R$. Τα επόμενα είναι ισοδύναμα:
1) x ακέραιο επί του A.
2) $A[x]$ είναι πεπερασμένα παραγόμενο A-πρότυπο.
3). Υπάρχει υποδακτύλιος C του R, με $A \subseteq A[x] \subseteq C \subseteq R$ με C πεπερασμένα παραγόμενο A-πρότυπο.
4). Υπάρχει "πιστό" $A[x]$-πρότυπο M, το οποίο είναι πεπερασμένο A-πρότυπο.

Σημείωση! Ένα A-πρότυπο M λέγεται πιστό αν για $a \in A$ με $aM = 0 \Rightarrow a = 0$.

Απόδειξη: 1) $\Rightarrow$ 2) Έστω $x \in R$ ακέραιο επί του A.

Τότε $x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$, όπου $a_0, a_1, \dots, a_{n-1} \in A$. $\Rightarrow$

$$\Rightarrow x^n = -a_{n-1}x^{n-1} - \dots - a_1 x - a_0 \Rightarrow$$

$$\Rightarrow x^n \in Ax^{n-1} + Ax^{n-2} + \dots + A_{\cdot}x + A\cdot 1_A .$$

Άρα $x^{n+1} \in Ax^n + Ax^{n-1} + \dots + Ax^2 + Ax \subseteq$

$$\subseteq A(Ax^{n-1} + Ax^{n-2} + \dots + Ax + 1) +$$
$$+ Ax^{n-1} + \dots + Ax^2 + Ax + A =$$
$$= (A^2 + A)x^{n-1} + (A^2 + A)x^{n-2} + \dots + (A^2 + A)x + A$$
$$= Ax^{n-1} + Ax^{n-2} + \dots + Ax + A .$$

A δακτύλιος

Με επαγωγή $x^r \in Ax^{n-1} + Ax^{n-2} + \dots + Ax + A$ $\forall r \geq n$.

Άρα $A[x] = Ax^{n-1} + \dots + Ax + A$ πεπερασμένα παραγόμενο A-πρότυπο ($x^{n-1}, x^{n-2}, \dots, 1$ γεννήτορες) και φυσικά δακτύλιος και επειδή $A \subseteq R$, $x \in R$ $A \subseteq A[x] \subseteq R$.

2) $\Rightarrow$ 3) Παίρνουμε $C = A[x]$.

3) $\Rightarrow$ 4) Παίρνουμε $M = C$. Το C είναι πιστό $A[x]$-πρότυπο γιατί αν y ανήκει στον υποδακτύλιο $A[x]$ και $yC = 0$, τότε επειδή C δακτύλιος $y \cdot 1 = 0 \Rightarrow y = 0$.

4) $\Rightarrow$ 1) Έστω M πιστό $A[x]$-πρότυπο και πεπερασμένα παραγόμενο επί του A. Τότε $M = Au_1 + Au_2 + \dots + Au_k$, $u_i \in M$. Παίρνουμε $x u_i \in M$. Άρα

$$x u_i = \sum_{j=1}^{k} \gamma_{ij} u_j , \quad \text{όπου } \gamma_{ij} \in A .$$

Ισοδύναμα. $(\delta_{ij}x - \gamma_{ij}) u_j = 0$ $\forall i = 1, \dots, k$.
όπου δ_{ij} τα δέλτα του Kronecker.

Έστω $T(x)$ ο $k\times k$ πίνακας. $(\delta_{ij}x-\gamma_{ij})$

$$T(x)=\begin{pmatrix} x-\gamma_{11} & -\gamma_{12} & \cdots & -\gamma_{1k} \\ -\gamma_{21} & x-\gamma_{22} & \cdots & -\gamma_{2k} \\ \vdots & & & \\ -\gamma_{k1} & -\gamma_{k2} & \cdots & x-\gamma_{kk} \end{pmatrix}$$

Άρα $T(x).\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow$

$$\Rightarrow \operatorname{adj}T(x)\cdot T(x)\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Leftrightarrow$$

$$\Leftrightarrow \det T(x)\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Επειδή $u_1,u_2,\dots,u_k$ γεννήτορες του M, έπεται ότι $\det T(x)\, M=0$. Επειδή M πιστό $A[x]$-πρότυπο $\Rightarrow \det T(x)=0$.

Αλλά $\det T(x)=\begin{vmatrix} x-\gamma_{11} & -\gamma_{12} & \cdots & -\gamma_{1k} \\ -\gamma_{21} & x-\gamma_{22} & \cdots & -\gamma_{2k} \\ \vdots & & & \\ -\gamma_{k1} & -\gamma_{k2} & \cdots & x-\gamma_{kk} \end{vmatrix}=$

μονικό πολυώνυμο βαθμού k του x με συντελεστές αθροίσματα γινομένων των $\gamma_{ij}\in A$.

Άρα $x^k+a_{k-1}x^{k-1}+\dots+a_1x+a_0=0$, όπου τα a_i είναι πολυωνυμικές συναρτήσεις των $\gamma_{ij}\in A$, δηλαδή $a_i\in A$.

Συνεπώς x ακέραιο επί του A.

Πρόταση: Τα ακέραια στοιχεία επί του A του R αποτελούν υποδακτύλιο C του R με $A\subseteq C\subseteq R$.

Απόδειξη: Έστω $x, y \in R$ ακέραια επί του A. (Προφανώς το A ακέραιο επί του εαυτού του γιατί $\forall a \in A$ το a μηδενίζει το μονικό πολυώνυμο ~~του~~ $x-a$)
Τώρα το $A[x]$ είναι πεπερασμένα παραγόμενο A-πρότυπο. Το y είναι ακέραιο επί του A, άρα και επί του $A[x]$, γιατί $A \subseteq A[x]$.
Άρα το $A[x,y] = A[x][y]$ είναι πεπερασμένα παραγόμενο $A[x]$-πρότυπο.

1) $A[x]$ πεπερασμένα παραγόμενο A-πρότυπο, άρα $A[x] = Au_1 + Au_2 + \dots + Au_k$, $u_i \in R$.

2) Το $A[x,y] = A[x][y]$ πεπερασμένα παραγόμενο $A[x]$ πρότυπο.

Άρα $A[x,y] = A[x]v_1 + A[x]v_2 + \dots + A[x]v_\lambda =$

$$= \sum_{j=1}^{\lambda} A[x]v_j = \sum_{j=1}^{\lambda} \sum_{i=1}^{k} Au_i v_j =$$

$$= \sum_{\substack{1 \le j \le \lambda \\ 1 \le i \le k}} A u_i v_j \Rightarrow A[x,y] \text{ πεπερασμένα}$$

παραγόμενο A-πρότυπο και δακτύλιος $\subseteq R$ και περιέχει τον A.
Άρα $A \subseteq A[x,y] \subseteq R$ και κάθε $x \pm y$, xy, 1 κτλ. ανήκουν στο $A[x,y]$. Άρα $x-y$, xy ακέραια επί του A και κάθε πολυωνυμική τους συνάρτηση ακέραια επί του A (γιατί ανήκει στο $A[x,y]$)
Εφόσον το άθροισμα, διαφορά, γινόμενο δύο ακεραίων επί του A στοιχείων του R είναι ακέραιο επί του A, έπεται ότι όλα τα ακέραια στοιχεία του R επί του A αποτελούν υποδακτύλιο του R που περιέχει το A.

Ορισμός: $A \subseteq R$ δακτύλιοι. Ο υποδακτύλιος C του R των ακεραίων επί του A στοιχείων ονομάζεται ακέραια κλειστότητα ή θήκη του A στον R.

Ορισμός: Έστω $A \subseteq R$ δακτύλιοι και κάθε στοιχείο του R είναι ακέραιο επί του A. Τότε ο R λέγεται ακέραιος επί του A.

Πρόταση: Έστω $A \subseteq C \subseteq R$ δακτύλιοι με R ακέραιος επί του C και C ακέραιος επί του A. Τότε R ακέραιος επί του A.

Απόδειξη: Έστω $x \in R$. Εφόσον x ακέραιο επί του C, $x^m + c_{m-1}x^{m-1} + \dots + c_1 x + c_0 = 0$ όπου τα $c_i \in C$.

Εφόσον ~~τα~~ C ακέραιος επί του A, τα c_i είναι ακέραια επί του A.

Άρα, με επαγωγή στο πλήθος των c_i, το $A[c_0, c_1, \dots, c_{m-1}]$ είναι πεπερασμένα παραγόμενο A-πρότυπο. (Ισχύει για δύο και επεκτείνουμε επαγωγικά).

Εφόσον $x^m + c_{m-1}x^{m-1} + \dots + c_1 x + c_0 = 0$, το x είναι ακέραιο επί του $A[c_0, c_1, \dots, c_{m-1}]$, άρα το $A[c_0, c_1, \dots, c_{m-1}][x] = A[c_0, c_1, \dots, c_{m-1}][\boxed{x}]$ πεπερασμένα παραγόμενο $A[c_0, \dots, c_{m-1}]$-πρότυπο.

Επειδή $A[c_0, c_1, \dots, c_{m-1}]$ πεπερασμένα παραγόμενο A-πρότυπο, όπως προηγουμένως το $A[c_0, c_1, \dots, c_{m-1}][x]$ πεπερ. παραγόμενο A-πρότυπο $\Longrightarrow$ x ακέραιο επί του A.

Πόρισμα: Έστω $A \subseteq R$ δακτύλιοι και C η ακέραια κλειστότητα του A στον R. Τότε η C είναι ακέραια κλειστή στον R, δηλαδή αν $x \in R$ ακέραιο επί του C, τότε $x \in C$.

Απόδειξη: Έστω $x \in R$ ακέραιο επί του C. Άρα $C[x]$ ακέραιος επί του C και C ακέραιος επί του A. Άρα $C[x]$ ακέραιος επί του $A \Rightarrow$ $\Rightarrow x$ ακέραιο επί του $A \Rightarrow x \in C$.

Πρόταση: Έστω $A \subseteq R$ δακτύλιοι και R ακέραιος επί του A.

1) Αν J ιδεώδες του R και $I = J \cap A$, τότε R/J ακέραιος επί του A/I.

2) Αν S πολ/κά κλειστό σύνολο ~~και~~ του A, τότε $S^{-1}R$ ακέραιος επί του $S^{-1}A$.

Απόδειξη: 1) Εδώ θεωρούμε τον A/I υποδακτύλιο του R/J μέσω της εμφύτευσης $\phi: a+I \mapsto a+J$.
~~Άρα~~ η ϕ καλά ορισμένη $(a+I = a'+I \Leftrightarrow a-a' \in I \subseteq J$ $\Rightarrow a+J = a'+J)$

ϕ: 1-1. Αν $\phi(a+I) = a+J = J \Rightarrow a \in J$ και επειδή $a \in A$, έπεται ότι $a \in A \cap J = I \Rightarrow a+I = I = 0_{A/I}$

Προφανώς ϕ ομομορφισμός.

Άρα όταν γράφουμε $a+J$ με $a \in A$ εννοούμε το $a+I$ και αντίστροφα.

Έστω τώρα $x+J$, όπου $x \in R$, άρα ακέραιο επί του A. Επομένως $x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$, με $a_i \in A$. Συνεπώς $(x+J)^n + (a_{n-1}+J)(x+J)^{n-1} + \dots + (a_1+J)(x+J) + (a_0+J) = 0_{R/J} \equiv 0_{A/I}$

Επειδή $a_i + J \equiv a_i + I$, το $x+J$ είναι ακέραιο επί του A/I, δηλαδή R/J ακέραιος επί του A/I

2) S πολ/κό κλειστό υποσύνολο του A, άρα και του R.

Έστω $\frac{x}{s} \in S^{-1}R$, $s \in S$.

Επειδή x ακέραιο επί του A
$x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$, $a_i \in A$.

~~Άρα~~ $\cancel{\left(\frac{x}{s}\right)^n + \left(\frac{a_{n-1}}{s}\right)\left(\frac{x}{s}\right)^{n-1} + \dots}$

Άρα $\frac{x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0}{s^n} = 0_{S^{-1}R} \Leftrightarrow$

$\Leftrightarrow \left(\frac{x}{s}\right)^n + \left(\frac{a_{n-1}}{s}\right)\left(\frac{x}{s}\right)^{n-1} + \left(\frac{a_{n-2}}{s^2}\right)\left(\frac{x}{s}\right)^{n-2} + \dots +$
$+ \left(\frac{a_1}{s^{n-1}}\right)\left(\frac{x}{s}\right) + \left(\frac{a_0}{s^n}\right) = 0. \Rightarrow \frac{x}{s}$ ακέραιο επί του $S^{-1}A$.

<u>Πρόταση</u>: Έστω $A \subseteq R$ ακέραιες περιοχές και R ακέραιος επί του A.
Τότε ισχύει: A σώμα $\Leftrightarrow$ R σώμα.
<u>Απόδειξη</u> ($\Rightarrow$) Έστω A σώμα και $x \in R \setminus \{0\}$.
Τότε $x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$, $a_i \in A$.
Μπορούμε να υποθέσουμε ότι $a_0 \neq 0$, γιατί αλλιώς
$x^n + a_{n-1}x^{n-1} + \dots + a_1 x = 0 \Leftrightarrow x(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1) = 0 \underset{\substack{R \text{ ακέραια} \\ \text{περιοχή}}}{\Leftrightarrow} x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1 = 0$.

Εφόσον $a_0 \neq 0$ και A σώμα $\exists\, a_0^{-1} \in A$ και άρα
$-(a_0^{-1}x^n + a_0^{-1}a_{n-1}x^{n-1} + \dots + a_0^{-1}a_1 x) = 1 \Leftrightarrow$
$\Leftrightarrow x(-a_0^{-1}x^{n-1} - a_0^{-1}a_{n-1}x^{n-2} - \dots - a_0^{-1}a_1) = 1 \Rightarrow$
$\Rightarrow x$ αντιστρέψιμο. Άρα R σώμα

($\Leftarrow$) Έστω R σώμα. και $a \in A \setminus \{0\}$

Αν $a^{-1} \notin A$, τότε a^{-1} ακέραιο επί του A, άρα
$$a^{-n} + a_{n-1}a^{-n+1} + \dots + a_1 a^{-1} + a_0 = 0, \quad a_i \in A.$$
Πολλαπλασιάζουμε με a^{n-1} και παίρνουμε
$$a^{-1} + a_{n-1} + a_{n-2}a + \dots + a_1 a^{n-2} + a_0 a^{n-1} = 0$$
$$\Leftrightarrow a^{-1} = -(a_{n-1} + a_{n-2}a + \dots + a_1 a^{n-2} + a_0 a^{n-1}) \in A,$$
~~άτοπο~~ Άρα $a^{-1} \in A$ και άρα A σώμα.

__Πρόταση!__ $A \subseteq R$ δακτύλιοι, R ακέραιος επί του A. Έστω Q πρώτο ιδεώδες του R και $P = A \cap Q$. Τότε Q μέγιστο στο $R \Leftrightarrow P$ μέγιστο στο A.

__Απόδειξη!__ P πρώτο ιδεώδες του A. Προφανώς, αν $ab \in P = A \cap Q \subseteq Q \Rightarrow a \in Q$ ή $b \in Q$, δηλαδή $(a, b \in A)$ $a \in Q \cap A = P$ ή $b \in Q \cap A = P$.
Έχουμε δείξει ότι η $\varphi: A/P \hookrightarrow R/Q$ είναι εμφύτευση και ότι ταυτίζουμε το $a+P$ με το $a+Q$. Με βάση αυτή την ταύτιση R/Q ακέραιος επί του A/P και επειδή τα Q, P πρώτα R/Q, A/P ακέραιες περιοχές, έχουμε $A/P \subseteq R/Q$ ακέραιες περιοχές και R/Q ακέραιος επί του A/P. Άρα R/Q σώμα $\Leftrightarrow$

$\Leftrightarrow A/P$ σώμα, ~~δηλαδή~~ Q μέγιστο στο $R \Leftrightarrow$
$\Leftrightarrow P = A \cap Q$ μέγιστο στο A.

Πόρισμα: $A \subseteq R$ δακτύλιοι, R ακέραιος επί του A. Έστω $Q \subseteq Q'$ πρώτα ιδεώδη του R με $Q \cap A = Q' \cap A = P$. Τότε $Q = Q'$.

__Απόδειξη:__ Έστω $S = A \setminus P$ πολλαπλασιαστικά κλειστό γιατί P πρώτο.

Θέτουμε $A_p = S^{-1}A$ και $R_p = S^{-1}R$.

Υπενθυμίζουμε ότι η απεικόνιση $A_p = S^{-1}A \to S^{-1}R = R_p$ με $\frac{a}{s} \mapsto \frac{a}{s}$ είναι εμφύτευση (injection).

Πράγματι αν $\frac{a}{s} = 0_{S^{-1}R}$, τότε $\frac{a}{s} = \frac{0}{1}$ στο R_p $\Rightarrow$ $(a \cdot 1 - 0s)t = 0$, $t \in S \Rightarrow at = 0_R = 0_A$. Αλλά $\frac{a}{s} = \frac{at}{st} = \frac{0}{st} = 0_{A_p}$.

Επομένως μπορούμε να θεωρήσουμε τον A_p υποδακτύλιο του R_p και R_p ακέραιος επί A_p.

Θεωρούμε το (μοναδικό μέγιστο ιδεώδες) $M = \{\frac{a}{s} \mid a \in P, s \in S\}$ του A_p και $N = \{\frac{b}{s} \mid b \in Q, s \in S\}$, $N' = \{\frac{b}{s} \mid b \in Q', s \in S\}$ τις επεκτάσεις των ιδεωδών

Q και Q' στον $R_p = S^{-1}R$. (Το ότι το M είναι μέγιστο στο A_p το δείχνουμε ως εξής: Έστω $\frac{a}{s} \notin M$, $a \in A$, $s \in S$. Άρα $a \notin P$, από τον ορισμό του M. $\Rightarrow a \in A \setminus P = S$, άρα το $\frac{a}{s}$ είναι αντιστρέψιμο στο A_p. $(\frac{a}{s})^{-1} = \frac{s}{a}$ έχει νόημα; γιατί $a \in S$)

Επειδή $Q \subseteq Q' \Rightarrow N \subseteq N'$ και τα N, N' είναι πρώτα στον B_p. Θα το δείξουμε μόνο για το N. Έστω $\frac{a}{s}\frac{b}{s'} \in N = \{\frac{\gamma}{t} \mid \gamma \in Q, t \in S\}$, $t, s, s' \in S$

Τότε $\frac{a}{s}\frac{b}{s'} = \frac{ab}{ss'} = \frac{\gamma}{t} \Rightarrow (tab - \gamma ss')r = 0$.

όπου $r \in S$. Άρα $rtab = ryss' \in Q$, γιατί $y \in Q$.
Επειδή ~~[illegible]~~ Αν, $r \in Q$ ή $t \in Q \Rightarrow r \in Q \cap A$ ή $t \in Q \cap A \Rightarrow r \in P$, ή $t \in P$, άτοπο γιατί $r, t \in S = A \setminus P$.
Επομένως Q πρώτο ~~και~~ $r, t \notin Q \Rightarrow ab \in Q \Rightarrow$
$\Rightarrow a \in Q$ ή $b \in Q \Rightarrow \frac{a}{s} \in N$, ή $\frac{b}{s'} \in N$.

Τώρα $M = A_p \cap N = A_p \cap N'$.
Θα το δείξουμε για το N. Έστω $\frac{a}{s} \in N \cap A_p$, όπου $a \in A$, $s \in S$. Τότε $\frac{a}{s} = \frac{b}{s'}$, $b \in Q$, $s' \in S$.
Άρα $(as' - sb)t = 0$ για $t \in S$ $\Rightarrow$
$\Leftrightarrow as't = sbt \underset{b \in Q}{\Rightarrow} as't = stb \in Q$ και $a, s', t \in A$.

Άρα $as't \in Q \cap A = P \underset{s', t \notin P}{\Rightarrow} a \in P \Rightarrow \frac{a}{s} \in M =$
$= \{ \frac{a''}{s''} \mid a'' \in P, s'' \in S \}$.
Τώρα, $P \subseteq Q \subseteq Q' \Rightarrow S^{-1}P \subseteq S^{-1}Q \subseteq S^{-1}Q'$,
δηλαδή $M \subseteq N \subseteq N'$ και $M \subseteq A_p \subseteq R_p$.
Άρα $M = M \cap A_p \subseteq N \cap A_p \subseteq N' \cap A_p$ και τέλος
~~[illegible]~~ $M = N \cap A_p = N' \cap A_p$ μέγιστο στο A_p
Αλλά M μέγιστο στο $A_p \subseteq R_p$ και R_p ακέραιος επί του ~~A_p~~. (Q μέγιστο στο $R \Leftrightarrow P = Q \cap A$ μέγιστο στο A)
Άρα N, N' μέγιστα στο $R_p \Rightarrow N = N'$.
Έστω $\frac{a}{s} \in S^{-1}Q' = N'$, $a \in Q'$. Τότε $\frac{a}{s} = \frac{b}{s'}$, $b \in Q$, $s' \in S$.

Άρα $(as' - bs)t = 0 \Leftrightarrow$ ~~$bst = as't$~~ $as't = bst \in Q$
και ~~[illegible]~~ $s', t \notin S \Rightarrow a \in Q$. Άρα $Q' \subseteq Q \Rightarrow$
$\Rightarrow Q = Q'$.

Από τα προηγούμενα έχουμε δείξει ότι αν $A \subseteq R$ και R ακέραιος επί του A τότε.

1) Αν P πρώτο ιδεώδες του A και $S = A \setminus P$ και τότε $A_p = S^{-1}A \subseteq S^{-1}R = R_p$ και R_p ακέραιος επί του A_p.

2) Αν Q πρώτο ιδεώδες του R με $Q \cap A = P$, ~~τότε~~ $S^{-1}Q = N = \{\frac{a}{s} \mid a \in Q, s \in S\}$, τότε $N \cap A_p = M$, όπου $M = \{\frac{a}{s} \mid a \in P, s \in S\}$ το μοναδικό μέγιστο ιδεώδες του A_p.

<u>Λήμμα:</u> Έστω $A \subseteq R$, R ακέραιος επί του A και P πρώτο ιδεώδες του A. Τότε υπάρχει πρώτο ιδεώδες του Q του R με $Q \cap A = P$.

<u>Απόδειξη:</u> $\phi : A \to A_p = S^{-1}A / \phi(a) = \frac{a}{1}$.

Επειδή $S^{-1}A = A_p \subseteq R_p = S^{-1}R$ η ϕ επεκτείνεται σε μία (έστω ϕ) $R \to R_p = S^{-1}R$ με $\phi(b) = \frac{b}{1}$ $\forall b \in R$.

~~Έστω $M = \{\frac{a}{s} \mid a \in P, s \in S\}$ μέγιστο ιδεώδες του A_p~~

Έστω N μέγιστο ιδεώδες του R_p. Επειδή R_p ακέραιος επί του A_p, το $M = N \cap A_p$ είναι μέγιστο ιδεώδες του A_p που είναι μοναδικό και είναι το $S^{-1}P = \{\frac{a}{s} \mid a \in P, s \in S\}$

Ποιό είναι το $\phi^{-1}(M) =$; ~~($a \in M \Leftrightarrow \phi(a) = \frac{a}{1} \in M = S^{-1}P \Rightarrow \frac{a}{1} = \frac{a'}{s}$, $a' \in P$ Άρα ... $\Rightarrow ast = a't \in P$ και $s, t \notin P$ Άρα $a \in P$.~~

~~Άρα $\phi^{-1}(M) = P$~~

Έστω $a \in \phi^{-1}(M) \Leftrightarrow \frac{a}{1} \in M = S^{-1}P =$

$= \left\{ \frac{a'}{s'} \middle| a' \in P, s' \in S \right\} \Leftrightarrow \frac{a}{1} = \frac{a'}{s'}, \; a' \in P, \; s' \in S$

$\Leftrightarrow (s'a - a')t = 0 \; (t \in S) \Leftrightarrow s'ta = a't \underset{a' \in P}{\in} P.$

και $s', t \notin P \Rightarrow a \in P$. Άρα $\phi^{-1}(M) = P$

$P = \phi^{-1}(M) = \phi^{-1}(N \cap A_p) = \phi^{-1}(N) \cap \phi^{-1}(A_p) =$
$= \phi^{-1}(N) \cap A \; \left(a \in A \Rightarrow \frac{a}{1} \in A_p \Rightarrow \phi(a) \in A_p \Rightarrow \right.$
$\left. \Rightarrow a \in \phi^{-1}(A_p) \right)$

Το $\phi^{-1}(N)$ είναι πρώτο ιδεώδες του R ~~και περιέχει το~~ ~~B~~. Έστω $bb' \in \phi^{-1}(N)$, $b, b' \in R$.
Τότε $\frac{bb'}{1} \in N \Leftrightarrow \frac{b}{1} \cdot \frac{b'}{1} \in N \underset{N \text{ μέγιστο}}{\Longrightarrow} \frac{b}{1} \in N$ ή

$\frac{b'}{1} \in N \Leftrightarrow b \in \phi^{-1}(N)$ ή $b' \in \phi^{-1}(N)$ άρα πρώτο

Έστω $Q = \phi^{-1}(N)$. Τότε $Q \cap A = P$.

Θεώρημα Ανόδου (Going-up theorem).

Έστω $A \subseteq R$, R ακέραιος επί του A.
Έστω $P_1 \subseteq P_2 \subseteq \dots \subseteq P_n$ αύξουσα ακολουθία πρώτων ιδεωδών του A και $Q_1 \subseteq Q_2 \subseteq \dots \subseteq Q_m$ αύξουσα ακολουθία πρώτων ιδεωδών του R, όπου $1 \leq m < n$, με $Q_i \cap A = P_i \; \forall i = 1, \dots, m$.
Τότε υπάρχουν πρώτα ιδεώδη $Q_{m+1}, \dots, Q_n$ του R με $Q_1 \subseteq \dots \subseteq Q_m \subseteq Q_{m+1} \subseteq \dots \subseteq Q_n$ και $Q_i \cap A = P_i \; \forall i = 1, \dots, n$.

Απόδειξη. Ανάγεται στην περίπτωση που

$P_1 \subseteq P_2$ πρώτα ιδεώδη του A, Q_1 πρώτο ιδεώδες του R με $Q_1 \cap A = P_1$. Πάμε να βρούμε το Q_2 με $Q_2 \supseteq Q_1$ και $Q_2 \cap A = P_2$.

Εφόσον R ακέραιος επί του A και $Q_1 \cap A = P_1$, τότε $R/Q_1 = \overline{R}$ ακέραιος επί του $A/P_1 = \overline{A}$

Το $P_2/P_1 = \overline{P_2}$ είναι πρώτο ιδεώδες του $A/P_1 = \overline{A}$ και άρα

υπάρχει πρώτο ιδεώδες $\overline{Q_2}$ του $R/Q_1 = \overline{R}$ με $\overline{Q_2} \cap \overline{A} = \overline{P_2}$. Το $\overline{Q_2}$ είναι της μορφής Q_2/Q_1, όπου Q_2 πρώτο ιδεώδες του R.

Η $\overline{A} \xrightarrow{\phi} \overline{R}$ / $A/P_1 \xrightarrow{\phi} R/Q_1$ είναι εμφύτευση ($P_1 = Q_1 \cap A$). Άρα η $P_2/P_1 \to Q_2/Q_1$ είναι εμφύτευση και $Q_2 \cap A = P_2$.
(περιορισμός της ϕ.)

Εναλλακτικά $\overline{Q_2} \cap \overline{A} = \overline{P_2}$, άρα ~~εμφύτευση φ πάει το~~ ~~A/P_1 στο Q_2/Q_1~~ και το ~~P_2/P_1 στο~~

εμφαίνει ότι η εικόνα μέσω της ϕ του P_2 ισούται με την τομή της εικόνας του A και της εικόνας του Q_2.
Η εικόνα του P_2 μέσω της ϕ είναι $(P_2+Q_1)/Q_1$
Η εικόνα του $\overline{A} = A/P_1$ είναι ο $(A+Q_1)/Q_1$
και το $\overline{Q_2}$ είναι το Q_2/Q_1.

Άρα $Q_2/Q_1 \cap A+Q_1/Q_1 = P_2+Q_1/Q_1 \Rightarrow$

~~$Q_2 \cap (A+Q_1) = Q_2$~~

Αρκεί.

~~Το ... κάθε προφανώς. Αν $a\in A$, $x\in Q_1$ μ.ε. $(a+x)+Q_1 = y+Q_1$, $y\in Q_2/Q_1$ $\Leftrightarrow$ $a+Q_1 = y+Q_1$~~

~~$a-y\in Q_1 \subseteq Q_2 \Rightarrow a\in Q_2$.~~

~~Άρα $Q_2\cap (A+Q_1) = Q_2$ και~~

Επομένως αν $x\in Q_2$, $a\in A$, $y\in Q_1$ μ.ε.

$x+Q_1 = a+y+Q_1 \underset{y\in Q_1}{\Rightarrow} x+Q_1 = a+Q_1 \Leftrightarrow$

$\Leftrightarrow x-a\in Q_1 \subseteq Q_2$ και $x\in Q_2 \Rightarrow a\in Q_2$.

Άρα $Q_2/Q_1 \cap A+Q_1/Q_1 = Q_2/Q_1 = P_2+Q_1/Q_1 \Leftrightarrow$

$\Leftrightarrow P_2+Q_1 = Q_2$. Αν

Αν $x\in Q_2\cap A$, τότε εφόσον $Q_2 = P_2+Q_1$ $\exists\, y\in P_2$, $z\in Q_1$ μ.ε. $x = y+z \Rightarrow \underbrace{x}_{\in A}-\underbrace{y}_{\in A}\in A \Leftrightarrow z\in A \Leftrightarrow z\in A\cap Q_1 = P_1$

Άρα $Q_2\cap A \subseteq P_1+P_2 \underset{P_1\subseteq P_2}{=} P_2$

$P_2 \subseteq P_2+Q_1 = Q_2 \Rightarrow P_2 = P_2\cap A \subseteq Q_2\cap A$.