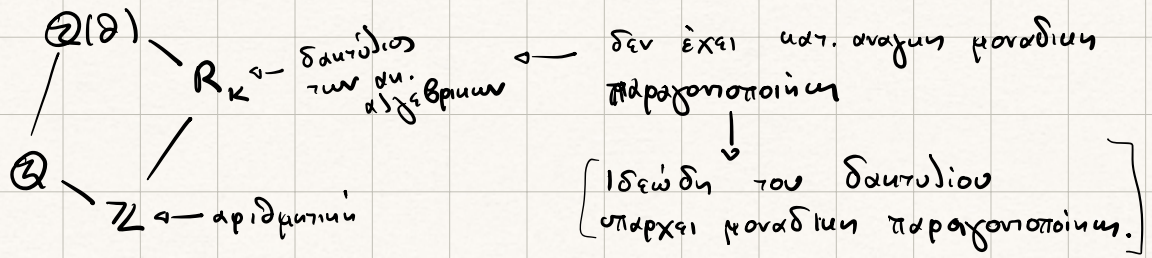


4ο μάθημα Αλγεβρική Θεωρία Αριθμών 1/3/2024



Αναγωγή γενίκευσης της έννοιας του ιδεώδους

↳ ιδεώδη του σώματος

$A \cdot B$ γινόμενο ιδεωδών

$$A \cdot B = B \cdot A$$

$$(A \cdot B) \cdot \Gamma = A \cdot (B \cdot \Gamma)$$

$$R \cdot A = A \cdot R = A$$

οριζήδη

Κάθε στοιχείο να έχει αντιστροφή?

• R Noether (modules της Noether) (δευτερίου $\rightarrow$ συναρτησιακή ανάλυση)

$\mathbb{C}^\infty$ συναρτήσεις $\mathbb{R} \rightarrow \mathbb{R}$
 όχι αναλυτικές δεν είναι της Noether

$$e^{-x^2}$$

A ιδεώδες του R

$$A^* = \{x \in K : xA \subset R\}$$

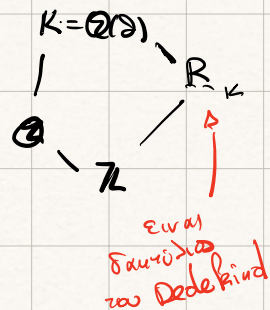
τα υψώματα ιδεωδών του R είναι ιδεώδη του σώματος

R α.κ. απροσκή

$$\xrightarrow{\quad} \text{Quot}(R)$$

Ορισμός R λέγεται δευτερίου του Dedekind αν και μόνο αν κάθε ιδεώδες του $K = \text{Quot}(R)$ είναι απλοσπείσιμο.

Στόχος:



Θεώρημα Αν R δευτερίου του Dedekind τότε ο R είναι δευτερίου της Noether και κάθε πρώτο μη-μηδενικό ιδεώδες του R είναι μέγιστο.

R ένα ιδεώδες λέγεται μέγιστο $M \neq R$

δια υαδε $M \subset A \subset R$ } $A = R$
 A ιδεώδες του R } $A = M$

R ένα ιδεώδες P λέγεται πρώτο

$$a \cdot b \in P \Rightarrow a \in P \text{ ή } b \in P$$

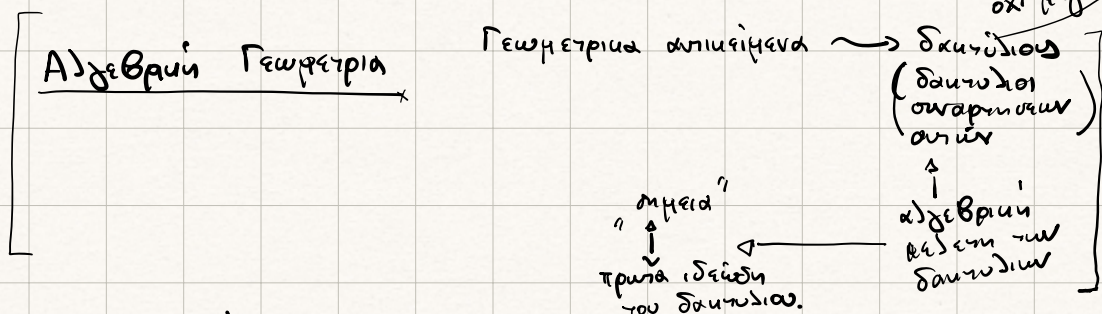
M είναι μέγιστο $\Leftrightarrow R/M$ είναι σώμα $\Downarrow$
 P είναι πρώτο $\Leftrightarrow R/P$ είναι ακ. περιοχή

$\Rightarrow$ υαδε μέγιστο είναι πρώτο.

Υπάρχουν παραδείγματα ιδεωδών που είναι πρώτα αλλά όχι μέγιστα.

$$R = \mathbb{Z}[x] \quad I = xR \quad \text{όλα τα πολυώνυμα που έχουν ρίζα στο 0}$$

$$R/xR = \frac{\mathbb{Z}[x]}{x\mathbb{Z}[x]} \cong \mathbb{Z} \leftarrow \text{είναι ακ. περιοχή αλλά όχι σώμα} \Rightarrow x\mathbb{Z}[x] \text{ πρώτο αλλά όχι μέγιστο}$$



Dedekind πρώτα είναι μέγιστα.

$$\mathbb{Z} \text{ περιοχή κυρίων ιδεωδών} \quad \mathbb{Z}/6\mathbb{Z}$$

$$I = n\mathbb{Z} \quad \begin{matrix} 3 \neq 0 \\ 2 \neq 0 \end{matrix}$$

$\mathbb{Z}/n\mathbb{Z}$ είναι συ. περιοχή αν και μόνο αν n πρώτο.

$n\mathbb{Z}$ είναι πρώτο $\Leftrightarrow n$ είναι πρώτος

$n\mathbb{Z}$ είναι μέγιστο $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ είναι το πεδίο αριθμ $\mathbb{F}_n$ με n το πλ. της στοιχείου

Εάν δακτυλίο $\mathbb{Z}$ δεν θα βρείτε μη-μηδενικά ιδεώδη που να πρώτα και όχι μέγιστα.

$\{0\}$ είναι πρῶτο $\Leftrightarrow \mathbb{Z}$ είναι αμ. περιοχή.

Ορισμός $a \cdot b \in \{0\} \Leftrightarrow a \cdot b = \{0\}$

$$\mathbb{Z} / \{0\} = \mathbb{Z} \quad \text{αμ. περιοχή} \\ \text{δχι, αμ. α}$$

$$\mathbb{Z} / \{0\} = \mathbb{Z}$$

$$a \equiv b \pmod{\{0\}}$$

$$\Leftrightarrow b - a \in \{0\}$$

$$\Leftrightarrow b - a = 0 \Leftrightarrow a = b$$

το $\{0\}$ είναι πρῶτο
αν και μόνο αν ο R
είναι αμ. περιοχή.

Αποδ. Έστω R είναι Dedekind

$A \neq \{0\}$ υπάρχει A^{-1} (ιδεωδές) του $K = \text{Quot}(R)$

$$\underline{A \cdot A^{-1} = R} \quad \text{αρα υπάρχουν } a_i \in A \\ b_i \in A^{-1}$$

$$1 = a_1 b_1 + \dots + a_m b_m$$

Έστω $x \in A$

$$x = \overset{R}{(x b_1)} a_1 + \dots + \overset{R}{(x b_m)} a_m$$

$$\begin{array}{c} \uparrow \\ x \in A \\ x b_i \in R \end{array}$$

$$x b_i \in R$$

Αν υπάρχει το A^{-1}
τότε $A^{-1} = A^* =$

$$\{ \underline{b} \in K : \underline{b} A \subset R \}$$

$$\underline{b_i} \in A^* = A^{-1}$$

$$\underline{A = a_1 R + \dots + a_m R}$$

$$a_1, \dots, a_m \in A$$

$$a_1 R + \dots + a_m R \subseteq A$$

A είναι πεπερασμένα παράγόμενο $\Rightarrow R$ είναι Noether

Λήμμα Έστω P πρῶτο (ιδεωδές) $A, B \nmid P$

$$A \cdot B \subset P \Rightarrow A \subset P \vee B \subset P$$

Αποδ.

Αν γι' αὐτὸ στοιχείο $b \in B$ ἰσχύει $b \in P$ τότε
παράγεται $B \subset P$.

Έστω ότι υπάρχει $b \in B$ με $b \notin P$.

τότε για κάθε $a \in A$ $a \cdot b \in P \xRightarrow{P \text{ πρώτο}} a \in P$
 $a \cdot b \in P \Rightarrow \cancel{b \in P} \Rightarrow$

για κάθε $a \in A \rightarrow a \in P$

$$A \subset P.$$

P πρώτο. Υπάρχει ένα μέγιστο (ιδεώδες) που
 περιέχει το P

$$P \subset N$$

ο δακτύλιος
 μας είναι
 Noether και
 από προκύπτει
 ότι των
 ιδεωδών
 με τα οποία
 είναι αυξαν
 ακολουθία
 ιδεωδών.

$$P \neq I \neq R$$

$$P \subset N$$

$$PN^{-1} \subset NN^{-1} = R$$

$\Rightarrow PN^{-1}$ είναι ιδεώδες (ιδεώδες) του R

$$(PN^{-1})N = P \quad P \text{ πρώτο}$$

συνεπώς $PN^{-1} \subset P$ ή $\underline{N \subset P \subset N} \Rightarrow \underline{P = N}$

$$PN^{-1} \subset P \Rightarrow \underline{N^{-1}} \subset P^{-1}PN^{-1} \subset P^{-1} \cdot P = R$$

$$R \subset N^{-1} \subset R \quad \text{Αν για κάθε } x \in R \quad xR \subset R$$

$$N^{-1} = R \Rightarrow N = \underline{R} \quad R^{-1} = \underline{R}$$

αυτό, τα μέγιστα
 ιδεώδη είναι
 γνήσια.

Θεώρημα Η ακ. περιοχή R είναι δακτύλιος Dedekind

1. R είναι Noether

2. Κάθε μη μηδενικό πρώτο του R είναι μέγιστο

3. Ο R είναι ακ. κλειστός

$$R \text{ --- } R = \text{Quot}(R) \text{ --- } L$$

Ένα $x \in R(L)$ θα λέγεται R -ακέραιο αν υπάρχουν

$$a_i \in R$$

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$$

Θεώρημα $R \subset L$ ο-συστ

Τα παραπάνω είναι ισοδύναμα.

1. Το x είναι R -ακέραιο
2. Ο δακτύλιος $R[x]$ είναι πεπερασμένο παράγωγο R -module
3. Υπάρχει ένα πεπερασμένο παράγωγο R -module $M \subset L$ ώστε $xM \subset M$

1 $\Rightarrow$ 2

Πράγματι αν ο x είναι R ακέραιος

$$R[x] = \langle 1, x, \dots, x^{n-1} \rangle$$

$R[x]$ είναι περ.
παράγωγο
δακτύλιος
κ)α δεν είναι
περ. παράγωγο
 R -modules

$$x^n = -(\alpha_{n-1}x^{n-1} + \dots + \alpha_1x + \alpha_0)$$

$$\forall k \in \mathbb{N} \quad x^{n+k} = -x^k (\dots)$$

Διαιρείται με ακέραιο και υπόλοιπο
 $R[x]$ k αμφι
 θα πρέπει ομεγενοβοδω $R[x]$
 σιντελεις να
 είναι αυτοπερ.γος.

2 $\Rightarrow$ 3 (2) $R[x]$ είναι περ. παράγωγο R -module

(3) υπάρχει περ. παράγωγο R -module $M \subset L$ ώστε $xM \subset M$

$$M = R[x]$$

$$x R[x] \subset R[x]$$

3 $\Rightarrow$ 1

M περ. παράγωγο R -module

$$M = R z_1 + R z_2 + \dots + R z_r \quad z_i \in L$$

$$xM \subset M$$

$$xz_i \in M \quad \text{για καθε } i=1,2,\dots,r$$

$$x \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} = A \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix}$$

$$xz_i = \sum_{j=1}^r a_{ij} z_j$$

⏟

$$\underbrace{(xI_d - A)}_B \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} = 0$$

$$B \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} = 0$$

$$\underbrace{\text{adj}(B)}_{\det B} B \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} = \text{adj} B \cdot 0 = 0$$

$$\underbrace{(z_1, \dots, z_r)}_{\neq (0, \dots, 0)}$$

$$\det B$$

$$M \neq 0$$

ΕΧΕΙ τολάχιστον
ένα μη-μηδενικό
συντελεστή

$$\det B = 0$$

$$\det(xI_r - A) = \underbrace{x^r + \underbrace{a_1}_{\lambda_1} x^{r-1} + \dots + \underbrace{a_r}_{\lambda_r}}_{\lambda_i \in R} = 0$$

⏟

$R[x]$ μονία που την
ικανοποιεί το x

και το x είναι αλγεβρικό.

Σταθμισμα Αν $x_1, \dots, x_m \in L$ είναι R -αλγεβρικά

τοτε $R[x_1, \dots, x_m]$ είναι πεπ. παράγωγο

R -σποmodule του L .

Το σύνολο των R αλ. στοιχείων του L είναι
δαυτοδίο

Πράγματι, αν $a, b \in L$ είναι R -αλγεβρικά τοτε παρχον

πεπ. παράγωγα R -modules M, N

$$aM \subset M \quad bN \subset N$$

$$\frac{(\alpha - b) MN \subset MN}{\alpha - b \text{ είναι αλγεβρικό}}$$

$$\frac{\alpha MN \subset MN}{b MN = M b N \subset MN}$$

$$ab \cdot N \subset MN \Rightarrow ab \text{ είναι αλγεβρικό}$$

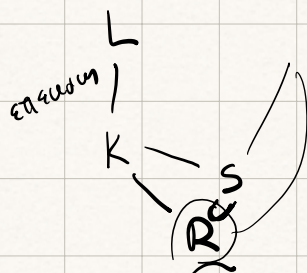
Ορισμός

Ο δακτύλιος $R' = \{x \in L \mid x \text{ να είναι } R\text{-αλγεβρικό}\}$

λεγεται η αλγεβρική θύλη του R στο L

Αν $R' = R$ τότε ο δακτύλιος
λεγεται αλγεβρική υψίλινος στο L
 $L = K = \text{Quot}(R)$

ο R λεγεται αλ. υψίλινος.



Αν S είναι η αλ. θύλη του R τον K

οι αλ. θύλη του S στο L ταυτίζονται.
αλ. θύλη του R στο L

Απόδειξη $x \in L$ που να είναι S -αλγεβρ. συνεπώς

υπάρχουν $a_0, \dots, a_{n-1} \in S$

$$x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$$

$R_1 = R[a_0, \dots, a_{n-1}]$ είναι περ.
παράγωγο
 R -module.

Αρα και το $R_1[x]$ είναι περ. παράγωγο
 R_1 module αλλά και
 R -module.

$$x \in R_1[x] \in R_1[x]$$

$\Rightarrow x$ είναι R -αλγεβρικό.

Προτάση Η αλγεβρική θύλη S του R στο L $R \subset L$
είναι αλ. υψίλινος

Απόδειξη $L = K$

R είναι δακτύλιος του Dedekind $\Rightarrow$ 1. R είναι Noether
2. Πρώτος $\Rightarrow$ Πρώτος
?
 $P \neq 0$

3. R είναι
ακ. υδατος.

Έστω $x \in K = \text{Quot}(R)$ x είναι R -αξία.

Τότε το $R[x]$ είναι πεπερασμένο παράγωγο.

$$R[x] = a_1 R + \dots + a_n R \quad a_i \in R$$

Διαιρούμε $b \neq 0$ ώστε $b a_i \in R$

$$b R[x] \subset R \quad b R[x] = (b a_1) R + \dots + (b a_n) R$$

Ανάλυση το $R[x]$ είναι υδατικό ιδεώδες του K .

Το $R[x]$ δαυτικό (υδατικό) του K

$R[x] \neq 0$
να είναι R -mod.
να υπάρχει
σε K δα CR

$$R[x]^2 = R[x]$$

$$R[x] = R[x]^2 \cdot R[x]^{-1} = R[x] \cdot R[x]^{-1} = R$$

$\Rightarrow x \in R \Rightarrow R$ είναι ακ. υδατος.

Dedekind $\Rightarrow (1), (2), (3)$

(1), (2), (3) $\Rightarrow$ Dedekind.

Λήμμα R Noether A είναι μη-μηδενικό ιδεώδες του R $A \neq R$

τότε υπάρχουν πρώτα ιδεώδη

$P_1, \dots, P_r$ ώστε

$$P_1 P_2 \dots P_r \subset A \subset P_1 \cap \dots \cap P_r$$

Απόδ

$$\mathcal{A} = \left\{ A \triangleleft R, A \neq 0, \text{ δα η οποία το λήμμα δεν ισχύει} \right\}$$

Έστω $\mathcal{A} \neq \emptyset$ R είναι Noether $\Rightarrow \mathcal{A}$ έχει μέγιστο στοιχείο M_0

Το M_0 δεν είναι άραιο $P \subset M_0 \subset P = M_0$
 γιατί τότε $M_0 \notin \mathcal{A}$.

Ενδεώς υπάρχουν $a, b \in M_0$ με $a \cdot b \in M_0$

$$M_0 \not\subseteq A \equiv M_0 + (a)R \quad a, b \notin M_0$$

$$M_0 \not\subseteq B \equiv M_0 + (b)R$$

Άρα το M_0 είναι μέγιστο του $\mathcal{A}$.

Οτι για τα A, B ισχύει η σχέση του Λήμματος

$$P_1, \dots, P_r \subset A \subset P_1 \cap \dots \cap P_r$$

$$Q_1, \dots, Q_s \subset B \subset Q_1 \cap \dots \cap Q_s$$

$$P_1, \dots, P_r, Q_1, \dots, Q_s \subset M_0 = A \cdot B \subset P_1 \cap \dots \cap P_r \cap Q_1 \cap \dots \cap Q_s$$

άρα $M_0 \notin \mathcal{A}$ άρα.