

3ο Μαθημα Αλγεβρική Θεωρία Αριθμών
26/2/2024.

Ιδεώδους Αλγεβρικού σωμάτιος αριθμών.

Ιδεώδη είναι δομές που αναφέρονται σε δακτυλίους
(R, +, ·) Αντιμεταθετικούς με 1

$I \triangleleft R$ είναι μια προσδεμένη υποδομή
 $(I, +) < (R, +)$

για κάθε $r \in R, i \in I \quad r \cdot i \in I$
υπάρχει ένας πολ/μος $R \times I \longrightarrow I$
 $(r, i) \longrightarrow ri$

δίνει στο I την δομή του R-module.

(Μοιάζει με την έννοια
του διανυσματικού χώρου
μόνο που ο πολ/μος
δεν είναι από ένα
σωμά αλλά από
ένα δακτυλίο)

Τα σωμάτια δεν έχουν ιδεώδη
με την υδατική έννοια.

Αν $1 \in I$ τότε το $I = R$ ($\begin{matrix} r \cdot 1 = r \in I \\ \uparrow \quad \uparrow \\ R \quad I \end{matrix}$)

$r \neq 0$ είναι αντιστρέψιμο $r \in I$ $R \subset I \subset R$

τότε $1 \in I$

$\begin{matrix} r^{-1} \cdot r = 1 \\ \uparrow \quad \uparrow \\ R \quad I \end{matrix}$

$\Rightarrow I = R$

$I \triangleleft K$

K σωμά

$I = \{0\}$ είναι ιδεώδες

Αλλά αν υπάρχει $x \neq 0$

με $x \in I$ τότε

το x είναι αντιστρέψιμο

$\Rightarrow I = K$



R ακ. περιοχή (αληθευόμενη δακτυλίω $\neq 1$)
 $\alpha\beta = 0 \Rightarrow \alpha = 0 \vee \beta = 0$

$Quot(R) = K$ σωρα πηλίκων $\mathbb{Z} \rightarrow \mathbb{Q}$,
 κλάση ή καταμεν $\frac{\alpha}{\beta} (\alpha, \beta)$

Ένα υποσύνολο $A \subset K$
 θα λέγεται ιδεώδες του K
 αν και μόνο αν:

- για κάθε $a_1, a_2 \in A$
 $a_1 - a_2 \in A$
- Για κάθε $\lambda \in R$ και $a \in A$
 έχουμε ότι $\lambda a \in A$

(A είναι R -module)

3. $A \neq \langle 0 \rangle = \{0\}$

4. Υπάρχει $\delta \in K, \delta \neq 0$ ώστε $\delta A \subset R$

Παραδείγματα

1) $A \subset R \subset K$

ακέραιο ιδεώδες (και είναι η
 έννοια του
 ιδεώδους όπως
 την γνωρίζαμε
 (μη-μηδενικού))

2) $\frac{1}{3} \mathbb{Z}$

απο είναι ιδεώδες
 του σωρατος

$\delta = 3 \in K$

$A = \frac{1}{3} \mathbb{Z} \not\subset \mathbb{Z}$

$3A \subset \mathbb{Z}$

Τα ιδεώδη που δεν είναι ακέραια θα τα ονομάζουμε
υδατοακέραια

Αν A, B είναι ιδεώδη του K τότε ορίζεται το

γινόμενο των

$$A \cdot B = \left\{ \sum_{i \in I} \alpha_i \beta_i \mid \alpha_i \in A, \beta_i \in B \right\}$$

I πεπερασμένο

↓
 ιδεώδες που παράγεται από όλα
 τα δινομένα (πεπ.π.) από στοιχεία
 $a \in A, b \in B$.

$A \cdot B$ είναι υποακέραιο ιδεώδες.

$$x \in A, B, \quad y \in A \cdot B \quad x+y \in A \cdot B$$

$\swarrow$ πεπ.π. αθροισμα δινομένων $\searrow$ πεπ. αθροισμα δινομένων

$$r \in R \quad r x \in A \cdot B$$

$$x = \sum \alpha_i \beta_i$$

$$rx = \sum (\underbrace{r\alpha_i}_A) \beta_i$$

$$0 \neq x \in A$$

$$0 \neq y \in B$$

$$x \cdot y \neq 0$$

$$\in AB$$

$$\delta_1 A \subset R$$

$$\delta_2 B \subset R$$

$$\delta_1 \delta_2 A \cdot B \subset R$$

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

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

$$\sum (\alpha_i \cdot \beta_i) \cdot \gamma_i$$

$$\sum \alpha_i (\beta_i \cdot \gamma_i)$$

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

το R είναι μοναδιαίο

R είναι ακ. ιδεώδες

$$\underbrace{R \cdot A}_{A \cdot R} \ni \sum \underbrace{r_i}_{\in R} \alpha_i \in A \quad A \subset RA = AR \subset A$$

Το σύνολο των ιδεωδών του R με πράξη
 τον πο/μο είναι αντιμεταθετική υποσυνολο
 με μοναδιαίο.

Ερώτηση είναι κάποια (η όλα) τα στοιχεία
 αντιμεταθετικά.

Ορισμός R απιμετακρίσιμος με 1

Θα λέγεται δκυτός της Noether αν ισχύει
από τις παρακάτω ισοδύναμες προτάσεις

1. Κάθε κυφούσα ακολουθία ιδεωδων γίνεται σταθερή
2. Κάθε διάφορο του κενού σύνολο ιδεωδων του R
έχει μέγιστο στοιχεία
3. Κάθε ιδεώδες του R είναι πεπερασμένα παραγόμενο

Παράδειγμα $\mathbb{Z}$ είναι δκυτός της Noether.

Κάθε ιδεώδες του είναι κυρίο $I \neq \mathbb{Z}$

$$I = n\mathbb{Z} \quad n \in \mathbb{Z}$$

άρα πεπερασμένα παραγόμενο.

Θα αποδείξουμε τώρα την ισοδυναμία 1, 2, 3

1 $\Rightarrow$ 2 Ω μη κενό σύνολο ιδεωδων του R

$A_0 \in \Omega$ αν δεν είναι μέγιστο

$$A_0 \subsetneq A_1 \subsetneq A_2 \subsetneq A_3 \subsetneq \dots \subsetneq$$

↑
αν ούτε αυτό είναι μέγιστο

↑
έχουμε κατασκευάσει
για δοσμένη κυφούσα
ακολουθία ιδεωδων
του R .

2 $\Rightarrow$ 3

W το σύνολο των πεπερασμένα παραγόμενων
ιδεωδων $W \subset A$

Μη κενό σύνολο $A \neq \{0\} \langle x \rangle \subset A$
 $\{0\} \subset A$

Το σύνολο W έχει ένα μέγιστο στοιχείο M

$M = A$ αν ναι τελειώσαμε

↑
π.α. παραγόμενο.

κν όχι τότε υπάρχει $x \in A, x \notin M$.

$M \neq M + xR$ πεπ. παραγόμενο $\subset A$

άτοπο γιατί το M δεν θα μπορούσε να είναι μέγιστο.

(3) $\Rightarrow$ (1)

$A_0 \subset A, C \dots \subset A_n \subset$

$A = \bigcup_{i=0}^{\infty} A_i$ το οποίο είναι ιδεώδες

$\downarrow$ είναι πεπ. παραγόμενο

(Προσοχή η ένωση ιδεωδων δεν είναι ιδεώδες)

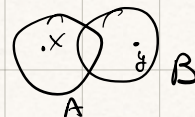
$A = \langle x_1, \dots, x_k \rangle$ α

$x_i \in \bigcup_{j=0}^{\infty} A_j$

αρα υπάρχει ένα

n_0 ώστε $x_1, \dots, x_k \in A_{n_0}$

εμφανώς αν το περιέχεται στο A_{n_0} .



$A_{n_0} = A_{n_0+1} = \dots = A_{n_0+n} = \dots = A$

Πομπία Κάθε δακτύλιος κυρίως ιδεώδες είναι δακτύλιος της Noether.

Ορίσμος R αντιρ. με μονάδα M είναι ένα R -module.

Το M θα λέγεται module της Noether.

κν ισχύει μία από τις παρακάτω ισοδυναμίες προτάσεις

1. Κάθε αλυσίδα αμοιβαία υποmodules του M δίνεται σταθερά.
2. Κάθε διαφορά του κενού ομοιογενούς υποmodules έχει μέγιστο στοιχείο
3. Κάθε υποmodule του M είναι πεπ. παραγόμενο.

- Θεώρημα
- Το ευθύ άθροισμα περιεχόμενων το αλτός modules της Noether είναι module της Noether.
 - Η ομορφισμός εικονα module της Noether είναι module της Noether.

Μικρές αλυσίδες ακολουθίες

$$0 \xrightarrow[\varphi_0]{} M_1 \xrightarrow[\varphi_1]{1-1} M \xrightarrow[\varphi_2]{\text{επι}} M_2 \xrightarrow[\varphi_3]{} 0$$

Αλυσίδες: $\text{Im } \varphi_0 = \text{Ker } \varphi_1 \Rightarrow \text{Ker } \varphi_1 = \{0\} \Rightarrow \varphi_1 \text{ 1-1}$

$$M_1 \cong \text{Im } \varphi_1 = \text{Ker } \varphi_2$$

$$\text{Im } \varphi_2 = \text{Ker } \varphi_3 \Rightarrow \text{Im } \varphi_2 = M_2 \Rightarrow \varphi_2 = \text{επι}$$

$$\varphi_3: M_2 \rightarrow 0$$

$$\text{Ker } \varphi_3 = M_2$$

$$\left(\frac{M}{M_1} \right) = \frac{M}{\text{Ker } \varphi_2} \cong \text{Im } \varphi_2 = M_2$$

Λήμμα

$$0 \rightarrow M_1 \xrightarrow[\text{επι}]{1-1} M \xrightarrow[\text{επι}]{\Phi} M_2 \rightarrow 0$$

Μικρή αλυσίδα ακολουθία

Αν M είναι module της Noether το ίδιο είναι και τα M_1, M_2

Αντίστροφα αν τα M_1, M_2 είναι module της Noether το ίδιο είναι και το M .

Αποδ.

Εστω M module της Noether.

Κάθε υποmodule του M είναι υποmodule του M άρα είναι π. περιεχόμενο άρα το M είναι υποmodule της Noether.

Εστω $\{I_n\}_{n \in \mathbb{N}}$ μια αλυσίδα αυξανουσα ακολουθία

τις M_2 .

$$\mathcal{I}'_m = \{ \alpha \in \underline{M} \mid \phi(\alpha) \in \mathcal{I}_m \} = \phi^{-1}(\mathcal{I}_m)$$

υποmodule του $\underline{M}$

$$\mathcal{I}_{m_1} \neq \mathcal{I}_{m_2} \Rightarrow \mathcal{I}'_{m_1} \neq \mathcal{I}'_{m_2}$$

Αρα αν η $\{\mathcal{I}_m\}_{m \in \mathbb{N}}$ είναι άπειρη αυξανουσα ακολουθια του M_2 τότε η

$\{\mathcal{I}'_m\}_{m \in \mathbb{N}}$ είναι άπειρη του M , άτοπο.

αρα M ως Noether $\Rightarrow M_1, M_2$ είναι ως Noether.

Εστω M_1, M_2 ως Noether

$\{\mathcal{I}_m\}_{m \in \mathbb{N}}$ αυξανουσα ακολουθια υπο-module του M

$$\mathcal{J}_m = \phi(\mathcal{I}_m) = \{ a \in M_2 \mid \exists b \in \mathcal{I}_m \text{ such that } \phi(b) = a \}$$

αυξανουσα του M_2 αρα είναι γειυδια σταθερα

$$\mathcal{J}_{n_1} = \mathcal{J}_{n_1+1} = \mathcal{J}_{n_2+2} = \dots$$

$$\{N_m\}_{m \in \mathbb{N}}$$

$$N_m = \mathcal{I}_m \cap M_1 \subset M_1$$

$$N_{n_2} = N_{n_2+1} = N_{n_2+2} = \dots$$

$$l = \max\{n_1, n_2\}$$

$n \geq l$ έχουμε ισοτιμίες και στην ακολουθια $N_m, \mathcal{J}_m$

$$r \geq l \quad \mathcal{I}_r \subset \mathcal{I}_r$$

$$a \in \mathcal{I}_r, \phi(a) \in \mathcal{J}_r = \mathcal{J}_l$$

αρα παρχει $b \in \mathcal{I}_l$

$$\phi(a) = \phi(b) \Rightarrow$$

$$\begin{aligned}
 \phi(\alpha - \beta) &= 0 \Rightarrow \\
 \alpha - \beta &\in \ker \phi = \bigcap_i I_i \\
 \alpha - \beta &\in M, \\
 \alpha &\in I_r \\
 \beta &\in I_1 \quad I_1 \subset I_r \\
 \alpha - \beta &\in I_r \cap M, \\
 \alpha - \beta &\in N_r = M_1 \\
 &\parallel \\
 &M \cap I_1 \\
 \alpha - \beta &\in I_1 \\
 \beta &\in I_1 \Rightarrow \alpha \in I_1 \\
 I_1 &= I_r
 \end{aligned}$$

Η ομορφία είναι module ως Noether είναι module ως Noether.

Για τα εύκολα αθροίσματα

$$\begin{aligned}
 0 &\longrightarrow A \longrightarrow A \oplus B \longrightarrow B \longrightarrow 0 \\
 \alpha &\xrightarrow{1-1} (\alpha, 0) \\
 (\alpha, \beta) &\xrightarrow{\pi_1} \beta \longrightarrow 0 \\
 A \oplus B / A &\cong B.
 \end{aligned}$$

Τα εύκολα αθροίσματα δίνουν μικρές αριθμ. ακολουθίες
αλλά όχι το αντίστροφο.

$\mathbb{Z}$ -module $\longleftrightarrow$ αβελιανός ομαδικός

$$\begin{aligned}
 0 &\longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{\text{mod } 2} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0 \\
 \alpha &\longmapsto 2\alpha \\
 \text{μικρή αριθμ. ακολουθία}
 \end{aligned}$$

$$\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Έστω διανυσματικός χώρος V με βάση B και C άλλη βάση.
 Η αντιστοιχία T_B^C που δίνει τον πίνακα μετασχηματισμού T_B^C είναι $T_B^C = I$.

$$0 \rightarrow M_1 \xrightarrow{f} M_2$$

A ιδεώδες του R $K = \text{Quot}(R)$

$$A^* = \{x \in K \mid xA \subset R\} \quad \text{αναστροφes του } A$$

$$R = \mathbb{Z} \quad K = \mathbb{Q} \quad A = 3\mathbb{Z} \quad \frac{1}{3} \in K \quad \frac{1}{3} \cdot 3\mathbb{Z} \subset \mathbb{Z}$$

$$A^* = \frac{1}{3}\mathbb{Z}$$

$$(A^*)^* = \frac{1}{\frac{1}{3}}\mathbb{Z} = 3\mathbb{Z}$$

$$3\mathbb{Z} \cdot \left(\frac{1}{3}\mathbb{Z}\right) = \mathbb{Z}$$

$A \quad A^*$

A^* είναι R -module. $A^* \neq \emptyset$.

$$\lambda_1 A \subset R$$

$$\lambda_2 A \subset R$$

$$(\lambda_1 + \lambda_2)A \subset R$$

$$\lambda_1 A \subset R$$

$$\lambda_1 \in A^*$$

$$(r\lambda_1)A \subset R$$

$$(r\lambda_1) \in A^*$$

$$A_1 \subset A_2$$

$$\text{τότε } A_2^* \subset A_1^*$$

$$\lambda \in A_2^* \stackrel{\text{op}}{\iff} \lambda A_2 \subset R$$

$$\lambda \bigcup A_1 \subset R \Rightarrow \lambda \in A_1^*$$

$$\underbrace{A^* A}_{\lambda} \subset R$$

$$\lambda a \in R$$

} εν χυθεί η ιδιότητα
έν ρυθεί.

As υποθέσουμε ότι ένα A των ιδεωδων έχει αντιστροφή
δηλαδή υπάρχει ιδεώδες που R

$$\bar{A}^{-1} A = R$$

$$\text{Αν } x \in A^{-1} \quad xa \in R \text{ για κάθε } a \in A.$$

$$A^{-1} \subset A^*$$

$$A A^* \subset R$$

$$A^{-1} (A A^*) \subset A^{-1} R = A^{-1}$$

$$(A^{-1} A) A^*$$

$$R A^*$$

$$\parallel A^*$$

$$A^* = A^{-1}$$

Δηλαδή αν ένα ιδεώδες αντιστρέφεται αυτό είναι το $A^{-1} = A^*$.

Λήμμα Κάθε κύριο ιδεώδες του R είναι
αντιστρέψιμο.

$$H = \{ aR \mid a \in R \setminus \{0\} \}$$

είναι πολλαπλή ομάδα

κύρια αντιστρέψιμο
ιδεώδες

$$\langle a \rangle = aR$$

$$a \in K \setminus \{0\}$$

$$3\mathbb{Z}, \frac{1}{3}\mathbb{Z}$$

$$a^{-1} \in K \setminus \{0\} \quad R \text{ απρ.α.}$$

$$aR \cdot a^{-1}R = R$$

$$I = \{ A : A = \text{προϊόντος ιδεωδών του } R \}$$

$$I \supset I' = \{ A \in I, A^{-1} \in I \mid AA^{-1} = R \}$$

πολύ/μη σφύδα.

$$A_1 \text{ αντιστρέφεται}, A_2 \text{ αντιστρέφεται}$$

$$(A_2^{-1} A_1^{-1}) A_1 A_2 \text{ αντιστρέφεται}$$

$$\left[\begin{array}{l} \text{Ορισμός} \quad R \text{ απ. περιοχή} \quad \Theta \alpha \text{ λέγεται} \\ \text{δακτύλιος του Dedekind αν κάθε ιδεώδες του} \\ R = \text{Quot}(R) \text{ είναι αντιστρέψιμο} \end{array} \right]$$

Θα δείξουμε στην ανέναντα τα παρακάτω:

— Κάθε ιδεώδες του R γραφεται με μονοσημαντικό τρόπο ως γινόμενο πρώτων ιδεωδών.

— R ο δακτύλιος των ακέραιων ^{αλγεβρικών} ενός συμπητος ^{αριθμών} είναι δακτύλιος του Dedekind.