9/3/20

Το θεώρημα δεν γενικεύεται σε $R[t_1, t_2, \ldots]$.

Αν I ιδεώδες ($I \triangleleft R$) $\Rightarrow$ ορίζεται το $\sqrt{I}$

$\sqrt{I} = \{a \in R : a^n \in I, n \in \mathbb{N}\}$

Το ριζικό του I είναι ιδεώδες του R

(*) αν $\sqrt{I} = I \Rightarrow$ το I καλείται ριζικό ιδεώδες.

Πχ Έστω $R = \mathbb{Z}$, πχ ένα ιδεώδες του είναι το $12\mathbb{Z} = \langle 12 \rangle$

δδο $\sqrt{12\mathbb{Z}} \overset{\subseteq}{\underset{\supseteq}{=}} 6\mathbb{Z}$

· Έστω $x \in \sqrt{12\mathbb{Z}} \Rightarrow \exists n \in \mathbb{N} : x^n \in 12\mathbb{Z} \Rightarrow \exists n \in \mathbb{N} : x^n = 12k, k \in \mathbb{Z}$

$\Rightarrow \exists n \in \mathbb{N} : x^n = \underbrace{2^2 \cdot 3 \cdot k}\in \mathbb{Z} \Rightarrow$ Λόγω της μοναδικότητας της πρωτογενής ανάλυσης, στην πρωτογενή ανάλυση του x υπάρχει τουλ. ένα 2 κ 3

$x = 2 \cdot 3 \cdot \lambda, \lambda \in \mathbb{Z} \Rightarrow x = 6\lambda, \lambda \in \mathbb{Z} \Rightarrow x \in 6\mathbb{Z}$

· Αντίστροφα, έστω $x \in 6\mathbb{Z}$ (άρα $x = 6k$, $k \in \mathbb{Z}$)

Παρατηρώ ότι $\exists n = 2 : x^2 = (6k)^2 = 36k^2 = 12(\ \ ) \Rightarrow \exists n = 2 :$
$x^2 \in 12\mathbb{Z} \Rightarrow x \in \sqrt{12\mathbb{Z}}$

Θυμίζω ότι αν $f \in \mathbb{K}[x_1, \ldots, x_n]$ αυτό καλείται ανάγωγο αν $f = g \cdot h$, $g, h \in \mathbb{K}[x_1, \ldots, x_n] \Rightarrow g, h$ σταθερά.

Αποδεικνύεται ότι κάθε $f \in \mathbb{K}[x_1, \ldots, x_n]$ γράφεται με μοναδικό τρόπο ως $f = \lambda f_1^{a_1} \ldots f_k^{a_k}$, $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ ανάγωγο.

πρωτ ανάλυση

<u>Πρόταση</u>: Αν $f \in K[x_1, \ldots, x_n]$ και έστω $f = \lambda f_1^{a_1} \ldots f_k^{a_k}$, όπου f_i ανάγωγα (και διαφορετικά μεταξύ τους)

Αν $I = \langle f \rangle \Rightarrow \sqrt{I} = \sqrt{\langle \lambda f_1^{a_1} \ldots f_k^{a_k} \rangle} = \langle f_1, \ldots f_k \rangle$

κύριο ιδεώδες

Έστω $\mathbb{K}[x_1, x_2, \dots, x_n]$, $\mathbb{K}$ σώμα, $f_1, \dots, f_k$.
Θεωρώ το σύνολο $\langle f_1, \dots, f_k \rangle = \left\{ \sum a_i f_i \ ,\ a_i \in \mathbb{K} \right\}$
το οποίο παράγεται από τα $f_1, \dots, f_k$.
Αποδεικνύεται ότι το $I = \langle f_1, \dots, f_k \rangle$ είναι ιδεώδες του $\mathbb{K}[x_1, \dots, x_n]$

<u>Ορισμός</u>. Το σύνολο $\{f_1, \dots, f_k\}$ καλείται βάση του I (ή σύνολο γεννητόρων του I.)
Σε αυτή την περίπτωση το I καλείται πεπερασμένα παραγόμενο

<u>Πχ</u> $I = \underbrace{\langle x, y \rangle}_{\text{βάση του } I} \overset{\in \mathbb{K}[x_1, \dots, x_n]}{=} \langle x, x-y, x^{2018} - y^{2020} + \frac{1}{\sqrt{2}} xy, \dots \rangle$

Ελαχιστοτικό σύνολο γεννητόρων (είναι ένα σύνολο γεννητόρων του I, όπου $\nexists$ γν. υποσύνολό του που να παράγει το I)

Περιοχές Μονοσήμαντης Ανάλυσης (Π.Μ.Α)
$\mathbb{Z}$: $10 = 2\cdot 5 = 5 \cdot 2 = (-2)(-5) = (-5)(-2)$
$\mathbb{Z}(\sqrt{-5}) = \{a + \beta\sqrt{-5}\ ,\ a, \beta \in \mathbb{Z}\}$
<u>Πχ</u> $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$
"κακή" περιοχή → δεν έχω μονοσήμαντη ανάλυση στοιχείων.

<u>Ορισμός</u>. Έστω R μεταθετικός δακτύλιος. Ένα στοιχείο $a \neq 0_R$ καλείται ανάγωγο αν δεν είναι αντιστρέψιμο και οι μοναδικοί του διαιρέτες είναι τα αντιστρέψιμα στοιχεία του R είτε τα συντροφικά στοιχεία του a (τα a, β συντροφικά αν $a|\beta$ και $\beta|a$)

<u>Πχ</u> στο $\mathbb{Z}$ (αντιστ. ± 1)
$a \in \mathbb{Z}$ ανάγωγο $\Leftrightarrow$ δεν είναι ± 1 (μη αντιστρ.) και οι μοναδικοί

διαιρέτες είναι τα ± 1 (αντιστρ. του $\mathbb{Z}$) και $\pm a$ (συντροφικά του)
$\Leftrightarrow$ a πρώτος.

<u>Ορισμός</u>: Μία (ακέραια) περιοχή R καλείται ΠΜΑ αν
1) Κάθε $a \in R$ $\neq 0_R$ είναι είτε αντιστρέψιμο στοιχείο του R
είτε (πεπερασμ) γινόμενο ανάγωγων στοιχείων του R.
2) Η παραπάνω ανάλυση είναι μοναδική ($a = p_1 \dots p_k = q_1 \dots q_\lambda$
$k = \lambda$, με πιθ διατ $p_i = q_i$)
(<u>πχ</u> το $\mathbb{Z}$. <u>πχ</u> όχι το $\mathbb{Z}[\sqrt{-5}]$)
(πρωτ. ανάλυση με μοναδ. τρόπο)

<u>Ισχύει</u>: ΠΚΙ $\subseteq$ ΠΜΑ $\subseteq$ ΑΚ. ΠΕΡΙΟΧΗ.

Έστω $(G, *)$ ομάδα και $H \leq G$
$G/H = \{g * H, g \in G\}$
ομάδα πηλίκο

για να έχει νόημα:
$g * H = H * g$
αρ σύμπλοκα δεξ. σύμπλοκα
αν συμβαίνει αυτό, η H καλείται κανονική υποομάδα της G
$H \trianglelefteq G$.

<u>πχ</u> $G = (\mathbb{Z}, +)$ $3\mathbb{Z}$
$\mathbb{Z}/3\mathbb{Z} = \{a + 3\mathbb{Z}, a \in \mathbb{Z}\}$
- $0 + 3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$
- $1 + 3\mathbb{Z} = \{\dots, -5, -2, 1, 4, 7, \dots\}$
- $2 + 3\mathbb{Z} = \{\dots, -4, -1, 2, 5, 8, \dots\}$

($g_1 + H = g_2 + H \Leftrightarrow g_1 - g_2 \in H$)
$\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$ $\quad g_1 * H = g_2 * H \Leftrightarrow g_1 * g_2^{-1} \in H$

αν $H \trianglelefteq G \Rightarrow$ ορίζεται η ομάδα πηλίκο $G/H = \{g * H, g \in G\}$
ορίζοντας πράξη: $g_1 * H, g_2 * H \Rightarrow (g_1 * H) * (g_2 * H) = (g_1 * g_2) * H$.

<u>πχ</u> $(1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = (1 + 2) + 3\mathbb{Z} = 3 + 3\mathbb{Z} = 0 + 3\mathbb{Z}$

(ο παρανομαστής πρέπει να είναι κανονική υποομάδα του αριθμητή 8)

Δακτύλιοι πηλίκα $(R,+,\cdot)$

Έστω R δακτύλιος και έστω ιδεώδες $I \trianglelefteq R$

Ορίζεται ο δακτύλιος πηλίκο $R/I = \{r+I, \ r \in R\}$

$r_1+I, r_2+I \overset{\text{ορίζεται}}{\Longrightarrow}$ "+" $(r_1+I)+(r_2+I) = (r_1+r_2)+I$

"$\cdot$" $(r_1+I)\cdot(r_2+I) = (r_1 r_2)+I$.

(ομοίως $r_1+I = r_2+I \Leftrightarrow r_1-r_2 \in I$)

Μόδια (Module theory) (ή Πρότυπο)

(συμβ $_R M$)

Ορισμός: Έστω R δακτύλιος. Ένα (αριστερό) R-μόδιο ή ένα (αριστερό) μόδιο υπεράνω του R, είναι μία αβελιανή ομάδα M εφοδιασμένη με μία απεικόνιση "$\cdot$" $R\times M \to M$, $(r,m) \mapsto r\cdot m$

όπου, η "$\cdot$" ικανοποιεί τα εξής

1) $(r+s)\cdot m = r\cdot m + s\cdot m \quad , \forall r,s \in R, \ m\in M$
2) $r(sm) = (rs)m \quad , \forall r,s \in R, \ m \in M$
3) $r(m_1+m_2) = rm_1 + rm_2 \quad , \forall r\in R, \ m_1,m_2 \in M$
4) αν ο R έχει και 1_R : $1_R m = m \quad , \forall m \in M$

* αντίστοιχα αν έχω "=" από τα δεξιά τα ίδια στοιχεία $\Rightarrow$ ορίζεται ως M_R (δεξιός R-μόδιος) και το M λέγεται μόδιο

* αν R μεταθετικός, ο διαχωρισμός δεν υφίσταται

Παρατήρηση: Αν ο R είναι σώμα, τότε ο ορισμός του R-μοδίου ταυτίζεται με τον αντίστοιχο του K-διανυσματικού χώρου.

(*) Ο K δ.χ. είναι K-μόδιο (και αντίστροφα)

Πχ (1) οποιαδήποτε αβελιανή ομάδα M είναι ένα $\mathbb{Z}$-μόδιο ορίζοντας $\mathbb{Z}\times M \to M$

$(z,m) \mapsto z\cdot m$

$$\mathbb{Z}m = \begin{cases} \overbrace{m+\dots+m}^{\mathbb{Z} \text{ φορές}}, & \mathbb{Z}>0 \\ 0, & \mathbb{Z}=0 \\ \underbrace{-m+\dots-m}_{-\mathbb{Z} \text{ φορές}}, & \mathbb{Z}<0 \end{cases}$$

$-(-\mathbb{Z}m)$

② Κάθε ιδεώδες $I \triangleleft R$ είναι R-μόδιο $R \times I \to I$ η πράξη του δακτυλίου

$(r, k) \longmapsto r \cdot k$

Πχ $r, s \in R$, $k \in I$

$(r+s)\cdot k = rk + sk$ αφού $I \triangleleft R$

③ Κάθε δακτύλιος R είναι R-μόδιο.

Θεώρημα: Έστω M R-μόδιο. Ισχύουν

1) $0_R \cdot m = m \cdot 0_R = \cancel{0_R}\ 0_M$
2) $r \cdot 0_M = 0_M$
3) $(-r)m = r(-m) = -rm$

$\forall r \in R, m \in M$

Απόδειξη

(1) $0_R \cdot m = (0_R + 0_R)m = 0_R \cdot m + 0_R \cdot m \Rightarrow 0_R \cdot m = 0_M$

Προσοχή! Ισχύει αν M R-μόδιο και $rm = 0_M$ ότι $r = 0_R$ ή $m = 0_M$?

ΟΧΙ Πχ έστω $M = \mathbb{Z}_{12}$ ως $\mathbb{Z}$-μόδιο παρατηρώ ότι

$\underset{\mathbb{Z}}{3} \cdot \underset{M}{\bar{4}_{12}} = \bar{0}_{12}$ και $3 \neq 0_{\mathbb{Z}}$ $\bar{4}_{12} \neq \bar{0}_{12}$

Πχ $\mathbb{Z}_p$ ως $\mathbb{Z}$-μόδιο

$(\mathbb{Z} \times \mathbb{Z}_p) \to \mathbb{Z}_p$

$k \cdot \bar{\lambda}_p \longmapsto (\overline{k\lambda})_p$

$\mathbb{Z} \times \mathbb{Z}_7 \to \mathbb{Z}_7$

$(7, \bar{k}_7) \longmapsto (\overline{7k})_7 = 0$

$7\,\bar{k}_7 = \bar{0}_7$.

αν το $\mathbb{Z}_7$ ως $\mathbb{Z}_7$ μόδιο ισχύει.

αν το $\mathbb{Z}_7$ ως $\mathbb{Z}$ μόδιο δεν ισχύει.