

**ΑΝΤΙΜΕΤΑΘΕΤΙΚΗ ΑΛΓΕΒΡΑ  
ΕΑΡΙΝΟ ΕΞΑΜΗΝΟ, 2013  
ΣΗΜΕΙΩΣΕΙΣ**

ΧΑΡΑ ΧΑΡΑΛΑΜΠΟΥΣ  
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ, ΑΠΘ

2. ΠΡΩΤΑ ΙΔΕΩΔΗ

Έστω  $R$  αντιμεταθετικός δακτύλιος με μονάδα. Το ιδεώδες  $P$  του  $R$  είναι πρώτο αν και μόνο αν  $R/P$  είναι ακεραία περιοχή. Στην παρούσα ενότητα θα εξετάσουμε ιδιότητες πρώτων ιδεωδών του  $R$ .

**Παραδείγματα 2.1.** Έστω  $R = \mathbb{Z}[x]$ .

- Δεν είναι δύσκολο να δούμε ότι  $x^2 + 1$  είναι ανάγωγο στον  $R$  και ότι  $P = \langle x^2 + 1 \rangle$  είναι πρώτο στον  $R$ . Πράγματι έστω

$$\Phi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[i] \quad x \mapsto i, \quad f(x) \mapsto f(i).$$

Είναι εύκολο να δει κανείς ότι η συνάρτηση  $\Phi$  είναι επιμορφισμός δακτυλίων. Έτσι  $\text{Im } \Phi = \mathbb{Z}[i]$ . Παρατηρούμε επίσης ότι  $x^2 + 1 \in \ker \Phi$ . Θα δείξουμε ότι  $\ker \Phi = \langle x^2 + 1 \rangle$  και επομένως σύμφωνα με το Πρώτο Θεώρημα Ισομορφίας Δακτυλίων έπεται ότι

$$\mathbb{Z}[x]/\langle x^2 + 1 \rangle \cong \mathbb{Z}[i].$$

Έτσι, αφού  $\mathbb{Z}[i] \subset \mathbb{C}$  είναι ακεραία περιοχή, έπεται ότι  $\langle x^2 + 1 \rangle$  είναι πρώτο ιδεώδες του  $\mathbb{Z}[x]$ . Πράγματι έστω  $g(x) \in \ker \Phi$ . Θα δείξουμε ότι  $g(x) = q(x)(x^2 + 1)$ . Ο Ευκλείδιος Αλγόριθμος είναι εφαρμόσιμος, μιας και ο μεγιστοβάθμιος συντελεστής του  $x^2 + 1$  είναι 1. Επομένως  $g(x) = q(x)(x^2 + 1) + r(x)$ , όπου  $q(x), r(x) \in \mathbb{Z}[x]$  και  $\deg(r(x)) < 2$ . Επομένως  $r(x) = ax + b$ , όπου  $a, b \in \mathbb{Z}$ . Αφού  $\Phi(g(x)) = 0$  έπεται ότι  $\Phi(q(x)) \cdot 0 + \Phi(r(x)) = 0 \Rightarrow \Phi(r(x)) = 0$ . Όμως αν  $a, b \neq 0$  τότε  $ai + b \neq 0$ . Άρα  $a, b = 0 \Rightarrow r(x) = 0$  και  $g(x) = q(x)(x^2 + 1)$ . Άρα  $\ker \Phi = \langle x^2 + 1 \rangle$ . Παρατηρούμε ότι το  $\mathbb{Z}[i]$  δεν είναι σώμα, άρα το  $\langle x^2 + 1 \rangle$  δεν είναι μέγιστο ιδεώδες του  $\mathbb{Z}[x]$ .

- Θα δείξουμε ότι το ιδεώδες  $J = \langle x^2 + 1, 5 \rangle$  δεν είναι πρώτο στον δακτύλιο  $\mathbb{Z}[x]$ . Πράγματι  $(x^2 + 1) - 5 = (x - 2)(x + 2) \in J$ . Όμως  $x \pm 2 \notin J$ , όπως μπορεί κανείς εύκολα να αποδείξει. Έπεται ότι  $J$  δεν είναι πρώτο ιδεώδες του  $\mathbb{Z}[x]$ . Θα καταλήξουμε στο ίδιο συμπέρασμα μελετώντας τον δακτύλιο  $\mathbb{Z}[x]/J$ .

Σύμφωνα με το Τρίτο Θεώρημα Ισομορφίας Δακτυλίων έχουμε ότι

$$\mathbb{Z}[x]/J \cong (\mathbb{Z}[x]/\langle x^2 + 1 \rangle)/(\langle x^2 + 1, 5 \rangle/\langle x^2 + 1 \rangle).$$

Προηγουμένως είδαμε ότι

$$\psi : \mathbb{Z}[x]/\langle x^2 + 1 \rangle \cong \mathbb{Z}[i], \quad \text{όπου } f(x) + \langle x^2 + 1 \rangle \mapsto f(i).$$

Παρατηρούμε ότι

$$\psi(\langle x^2 + 1, 5 \rangle / \langle x^2 + 1 \rangle) = \langle 5 \rangle .$$

Άρα

$$\mathbb{Z}[x]/J \cong \mathbb{Z}[i]/\langle 5 \rangle .$$

Αφού  $5 = (2 - i)(2 + i)$ , έπειται ότι  $\mathbb{Z}[i]/\langle 5 \rangle$  και  $\mathbb{Z}[x]/J$  δεν είναι ακεραίες περιοχές.

- Το ιδεώδες  $I = \langle x^2 + 1, 3 \rangle$  είναι μέγιστο στον δακτύλιο  $\mathbb{Z}[x]$ . Πράγματι, παρατηρούμε ότι

$$\mathbb{Z}[x]/I \cong (\mathbb{Z}[x]/\langle x^2 + 1 \rangle)/(\langle x^2 + 1, 3 \rangle/\langle x^2 + 1 \rangle) \cong \mathbb{Z}[i]/\langle 3 \rangle .$$

Το  $3$  είναι ανάγωγο στο  $\mathbb{Z}[i]$  και μπορεί να αποδείξει κανείς ότι  $\mathbb{Z}[i]/\langle 3 \rangle$  είναι σώμα.

- Το ιδεώδες  $P = \langle x^2 + 1, p \rangle$  είναι μέγιστο ιδεώδες (και άρα πρώτο) του  $\mathbb{Z}[x]$  αν και μόνο αν το πολυώνυμο  $x^2 + 1$  δεν έχει ρίζα στο  $\mathbb{Z}_p[q]$ . Η απόδειξη επαφίεται στον αναγνώστη.

**Άσκηση 2.2.** Είναι ο δακτύλιος  $\mathbb{Z}[x]$  περιοχή κυρίων ιδεωδών; Ποιά είναι η σχέση των ιδεωδών του  $\mathbb{Z}[x]/J$  και του  $\mathbb{Z}[x]$ ;

Η παρακάτω ακολουθία πρώτων ιδεωδών του  $\mathbb{Z}[x]$

$$0 \subset \langle x^2 + 1 \rangle \subset \langle x^2 + 1, 3 \rangle$$

έχει μήκος  $2$ . Μπορεί να αποδείξει κανείς ότι δεν υπάρχει ακολουθία πρώτων ιδεωδών στο  $\mathbb{Z}[x]$  με μήκος μεγαλύτερο του  $2$ . Έτσι θα δούμε σε επόμενη ενότητα ότι η διάσταση του Krull του  $\mathbb{Z}[x]$  είναι  $2$ .

**Άσκηση 2.3.** Να περιγράψετε όλα τα πρώτα ιδεώδη του  $\mathbb{Z}[x]$ .

Το Λήμμα του Zorn που παραθέτουμε αμέσως μετά είναι ισοδύναμο με το Αξίωμα της Επιλογής.

**Λήμμα του Zorn** Εστω  $A$  ένα μη κενό μερικά διατεταγμένο σύνολο με την ιδιότητα κάθε αλυσίδα στοχείων του  $A$  έχει άνω φράγμα στο  $A$ . Τότε το  $A$  έχει ένα μέγιστο στοιχείο.

Ως εφαρμογή του Λήμματος του Zorn προκύπτει το παρακάτω Θεώρημα:

**Θεώρημα 2.4.** Κάθε αντιμεταθετικός δακτύλιος  $R$  έχει ένα τουλάχιστον μέγιστο ιδεώδες.

Απόδειξη. Έστω  $S$  το σύνολο των γνήσιων ιδεωδών του  $R$ . Το σύνολο  $S$  είναι μη κενό αφού περιέχει το μηδενικό ιδεώδες. Ορίζουμε μία σχέση μερικής διάταξης ' $\leq$ ' στο  $S$ :

$$I \leq J \Leftrightarrow I \subseteq J_2 .$$

Έστω  $L$  μία αλυσίδα στο  $S$ :

$$L : \quad \cdots \leq I_i \leq I_{i+1} \leq \cdots .$$

Το σύνολο  $\bigcup_{J \in L} J$  είναι γνήσιο ιδεώδες του  $R$  και άρα ανήκει στο  $S$ . Είναι επίσης άνω φράγμα του  $L$ . Σύμφωνα με το Λήμμα του Zorn το  $S$  έχει ένα μέγιστο στοιχείο. Το μέγιστο αυτό στοιχείο είναι μέγιστο ιδεώδες του  $R$ .  $\square$

Έστω  $I$  γνήσιο ιδεώδες του  $R$ . Τα ιδεώδη του  $R/I$  βρίσκονται σε μία προς μία αντιστοιχία με τα ιδεώδη του  $R$  που περιέχουν το  $I$ . Τα ιδεώδη του  $R/I$  είναι της μορφής  $J/I$  όπου  $I \subset J$ .

**Πόρισμα 2.5.** Έστω  $I$  γνήσιο ιδεώδες του  $R$ . Υπάρχει τουλάχιστον ένα μέγιστο ιδεώδες του  $R$  που περιέχει το  $I$ .

Απόδειξη. Ο δακτύλιος  $R/I$  έχει ένα τουλάχιστον μέγιστο ιδεώδες, έστω  $\mathfrak{m}/I$ . Το ιδεώδες  $\mathfrak{m}$  είναι μέγιστο στο  $R$ .  $\square$

Θα συμβολίζουμε το σύνολο των πρώτων ιδεωδών του  $R$  με  $\text{Spec}(R)$  ενώ το σύνολο των μεγίστων ιδεωδών του  $R$  με  $\text{maxSpec}(R)$ . Έστω  $P \in \text{Spec}(R)$  και  $S = R \setminus P$ . Τότε  $S$  είναι πολλαπλασιαστικά κλειστό σύνολο.

**Πρόταση 2.6.** Έστω  $U$  πολλαπλασιαστικό κλειστό υποσύνολο του  $R$ . Έστω  $T$  το σύνολο των ιδεωδών του  $R$  που δεν έχουν τίποτα κοινό με το  $U$  και  $Q$  μέγιστο στοιχείο του  $T$ . Τότε  $Q \in \text{Spec}(R)$ .

Απόδειξη. Έστω  $fg \in Q$ . Έστω ότι  $f, g \notin Q$ . Τότε  $Q \not\subseteq \langle f \rangle + Q$  και  $Q \not\subseteq \langle g \rangle + Q$ . Αφού  $Q$  μέγιστο στο  $T$ , έπειτα ότι τα ιδεώδη  $\langle f \rangle + Q$ ,  $\langle g \rangle + Q$  δεν ανήκουν στο  $T$ . Επομένως, η τομή τους με το  $U$  είναι διάφορη του κενού. Άρα υπάρχουν  $a, b \in R$ ,  $q_1, q_2 \in Q$  έτσι ώστε  $af + q_1 \in U$ ,  $bg + q_2 \in U$ . Έπειτα ότι  $h = (af + q_1)(bg + q_2) \in U \cap Q$ , άτοπο.  $\square$

Έστω  $I$  ιδεώδες του  $R$ . Θα χρησιμοποιήσουμε τη παραπάνω πρόταση για να περιγράψουμε τα μηδενοδύναμα στοιχεία του  $R$ , δηλαδή τα στοιχεία του  $\text{rad}(0)$ .

**Θεώρημα 2.7.**  $\text{rad}(0) = \bigcap_{P \in \text{Spec}(R)} P$

Απόδειξη. Έστω  $J = \bigcap_{P \in \text{Spec}(R)} P$ . Θα δείξουμε ότι  $\text{rad}(0) = J$ . Έστω  $f \in \text{rad}(0)$ . Τότε υπάρχει  $m \in \mathbb{N}$ , έτσι ώστε  $f^m = 0$ . Έπειτα ότι αν  $P \in \text{Spec}(R)$  τότε  $f^m \in P$ . Άρα  $f \in P$ ,  $\forall P \in \text{Spec}(R)$  και  $f \in J$ .

Αντίστροφα, έστω  $f \in J$ . Θα δείξουμε ότι αν  $f$  δεν είναι μηδενοδύναμο καταλήγουμε σε άτοπο. Έστω ότι  $f \notin \text{rad}(0)$ . Το σύνολο  $U = \{f^m : m \in \mathbb{N}\}$  είναι πολλαπλασιαστικά κλειστό και δεν περιέχει το 0. Έπειτα ότι το σύνολο των ιδεωδών του  $R$  που δεν έχουν τίποτα κοινό με το  $U$  είναι διάφορο του κενού, (περιέχει το μηδενικό ιδεώδες) και σύμφωνα με το Λήμμα του Zorn έχει μέγιστο στοιχείο, έστω  $Q$ . Σύμφωνα με τη παραπάνω πρόταση  $Q \in \text{Spec}(R)$ , άτοπο.  $\square$

Το παρακάτω τώρα έπειται εφαρμόζοντας το θεώρημα στον δακτύλιο πηλίκο  $R/I$ .

**Θεώρημα 2.8.** Έστω  $I$  ιδεώδες του  $R$ . Τότε

$$\text{rad}(I) = \bigcap_{\substack{P \in \text{Spec}(R) \\ I \subset P}} P$$

Απόδειξη. Στον δακτύλιο  $R/I$  τα μηδενοδύναμα στοιχεία είναι της μορφής  $f + I$  όπου  $f^m \in I$  για κάποιο  $m \in \mathbb{N}$ . Τα πρώτα ιδεώδη του  $R/I$  είναι της μορφής  $P/I$  όπου  $P$  πρώτο ιδεώδες του  $R$  που περιέχει το  $I$ . Σύμφωνα με το προηγούμενο θεώρημα  $f^m \in I$  αν και μόνο αν  $f \in P$  για κάθε πρώτο ιδεώδες  $P$  του  $R$  που περιέχει το  $I$ .  $\square$