Κεφάλαιο 0

Μεταθετικοί Δακτύλιοι, Ιδεώδη

Το κεφάλαιο αυτό έχει προπαρασκευαστικό χαρακτήρα. Θα καθιερώσουμε συμβολισμούς και θα υπενθυμίσουμε ορισμούς και στοιχειώδεις προτάσεις για δακτύλιους και ιδεώδη που είναι γνωστά από το μάθημα Βασική Άλγεβρα. Θα περιοριστούμε στα πλέον απαραίτητα για την ύλη που ακολουθεί.

0.1 Συμβολισμοί

Με $\mathbb{Z} = \{..., -1, 0, 1, ...\}$ και $\mathbb{N} = \{0, 1, ...\}$ συμβολίζουμε το σύνολο των ακεραίων αριθμών και το σύνολο των μη αρνητικών ακεραίων αριθμών αντίστοιχα. Το σύνολο των ρητών αριθμών είναι $\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$, το σύνολο των πραγματικών αριθμών συμβολίζεται με $\mathbb{R}$, ενώ το σύνολο των μιγαδικών αριθμών είναι $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, όπου $i^2 = -1$. Για σύνολα A και B, χρησιμοποιούμε το συμβολισμό $A \subseteq B$ για να δηλώσουμε ότι το A είναι υποσύνολο του B, ενώ ο συμβολισμός $A \underset{\neq}{\subseteq} B$ σημαίνει ότι το A είναι γνήσιο υποσύνολο του B, δηλαδή $A \subseteq B$ και $A \neq B$. Ο πληθικός αριθμός ενός πεπερασμένου συνόλου A συμβολίζεται με $\#A$. Αν $f : A \to B$ είναι συνάρτηση, $C \subseteq A$ και $D \subseteq B$ γράφουμε $f(C) = \{f(c) \mid c \in C\}$ και $f^{-1}(D) = \{a \in A \mid f(a) \in D\}$.

0.2 Δακτύλιοι, Παραδείγματα

Δακτύλιος είναι ένα μη κενό σύνολο R εφοδιασμένο με δύο εσωτερικές πράξεις, πρόσθεση $+ : R \times R \to R$ και πολλαπλασιασμός $\cdot : R \times R \to R$ τέτοιες ώστε: α) το R ως προς την πρόσθεση είναι αβελιανή ομάδα, β) ισχύουν $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2)$

$\cdot r_3$, $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_1 \cdot r_3$, $(r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$ για κάθε $r_1, r_2, r_3 \in R$, και γ) υπάρχει στοιχείο $1_R \in R$ έτσι ώστε $1_R \cdot r = r = r \cdot 1_R$ για κάθε $r \in R$.

Ένας δακτύλιος R καλείται *μεταθετικός* αν ισχύει $r_1 \cdot r_2 = r_2 \cdot r_1$ για κάθε $r_1, r_2 \in R$.

Εφεξής θα γράφουμε $r_1 r_2$ στη θέση του $r_1 \cdot r_2$.

Επειδή στις σημειώσεις αυτές θα ασχοληθούμε αποκλειστικά με μεταθετικούς δακτυλίους, όταν *γράφουμε "δακτύλιο" θα εννοούμε μεταθετικό δακτύλιο*. Έτσι για παράδειγμα η φράση "έστω R δακτύλιος" σημαίνει έστω R μεταθετικός δακτύλιος.

Τα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ με τις συνήθεις πράξεις είναι δακτύλιοι. Το σύνολο των "ακεραίων του Gauss" $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ είναι επίσης δακτύλιος με τις συνήθεις πράξεις. Το σύνολο των κλάσεων υπολοίπων modulo n $(n \in \mathbb{N})$, $\mathbb{Z}_n = \{[0],[1],...,[n-1]\}$, είναι δακτύλιος με πράξεις $[a] + [b] = [a + b]$ και $[a][b] = [ab]$ όπως θυμόσαστε από το μάθημα Βασική Άλγεβρα.

0.2.1 Παράδειγμα (*Τυπικές δυναμοσειρές*) Έστω R ένας δακτύλιος. Θεωρούμε το σύνολο $R^{\mathbb{N}}$ των άπειρων ακολουθιών $(r_i)_{i \in \mathbb{N}} = (r_0, r_1, ..., r_n, ...)$ όπου $r_i \in R$ για κάθε $i \in \mathbb{N}$. Ορίζουμε την πρόσθεση και τον πολλαπλασιασμό

$$(r_i)_{i \in \mathbb{N}} + (s_j)_{j \in \mathbb{N}} = (r_i + s_i)_{i \in \mathbb{N}}$$

$$(r_i)_{i \in \mathbb{N}} (s_j)_{j \in \mathbb{N}} = (t_k)_{k \in \mathbb{N}},$$

όπου

$$t_k = r_0 s_k + r_1 s_{k-1} + \cdots + r_k s_0 = \sum_{i=0}^{k} r_i s_{k-i}$$

για κάθε $k \in \mathbb{N}$. Ως προς αυτές τις πράξεις το $R^{\mathbb{N}}$ είναι δακτύλιος με $1_{R^{\mathbb{N}}} = (1_R, 0_R, ...)$ και $0_{R^{\mathbb{N}}} = (0_R, 0_R, ...)$, όπου 0_R είναι το μηδενικό στοιχείο του R. Συνήθως συμβολίζουμε το στοιχείο $(r_i)_{i \in \mathbb{N}} = (r_0, r_1, ...)$ με

$$\sum_{i=0}^{\infty} r_i x^i = r_0 + r_1 x + \cdots,$$

οπότε οι πράξεις λαμβάνουν τη γνωστή μορφή

$$\sum_{i=0}^{\infty} r_i x^i + \sum_{i=0}^{\infty} s_j x^j = \sum_{i=0}^{\infty} (r_i + s_i) x^i$$

$$\left(\sum_{i=0}^{\infty} r_i x^i\right)\left(\sum_{j=0}^{\infty} s_j x^j\right) = \sum_{k=0}^{\infty} t_k x^k ,$$

όπου $t_k = r_0 s_k + r_1 s_{k-1} + \cdots + r_k s_0$. Με αυτόν το συμβολισμό γράφουμε $R[[x]] = R^{\mathbb{N}}$, και τα στοιχεία του δακτυλίου $R[[x]]$ ονομάζονται *τυπικές δυναμοσειρές*. Το σύνολο των τυπικών δυναμοσειρών $\sum_{i=0}^{\infty} r_i x^i$, όπου όλα τα r_i εκτός από ένα πεπερασμένο πλήθος είναι ίσα με το 0_R είναι το σύνολο $R[x]$ των πολυωνύμων με συντελεστές από το R.

Ένα υποσύνολο S ενός δακτυλίου R ονομάζεται *υποδακτύλιος* του R αν το S είναι δακτύλιος ως προς τις ίδες πράξεις και $1_S = 1_R$. Από το προηγούμενο παράδειγμα, ο $R[x]$ είναι υποδακτύλιος του $R[[x]]$ για κάθε δακτύλιο R.

0.2.2 Πρόταση *Έστω S υποσύνολο του δακτυλίου R. Τότε ο S είναι υποδακτύλιος του R αν και μόνον αν*

(i) $1_R \in S$

(ii) $a, b \in S \Rightarrow a - b \in S$ *και* $ab \in S$.

Απόδειξη. Άσκηση □

Έστω R δακτύλιος. Η τομή (οποιουδήποτε πλήθους) υποδακτυλίων του R είναι υποδακτύλιος του R, πράγμα που προκύπτει άμεσα από την προηγούμενη πρόταση. Αν τώρα A είναι ένα μη κενό υποσύνολο του R, και S υποδακτύλιος του R, με $S[A]$ συμβολίζουμε την τομή όλων των υποδακτυλίων του R που περιέχουν το S και A. Αν το A είναι πεπερασμένο, $A = \{a_1, ..., a_n\}$, ο δακτύλιος $S[A]$ συμβολίζεται και με $S[a_1, ..., a_n]$. Με $S[x_1, ..., x_n]$ συμβολίζουμε το δακτύλιο των πολυωνύμων στις μεταβλητές $x_1, ..., x_n$ επί του S.

0.2.3 Πρόταση *Έστω ένας R δακτύλιος και S ένας υποδακτύλιος του R. Έστω $\{a_1, ..., a_n\} \subseteq R$. Τότε*

$$S[a_1, ..., a_n] = \{f(a_1, ..., a_n) \in R \mid f(x_1, ..., x_n) \in S[x_1, ..., x_n]\} .$$

Απόδειξη. Από την Πρόταση 0.2.2, το σύνολο $\{f(a_1,...,a_n)\in R \mid f(x_1,...,x_n)\in S[x_1,...,x_n]\}$ είναι υποδακτύλιος του *R*. Επιπλέον περιέχει το σύνολο $\{a_1,...,a_n\}$. Άρα από τον ορισμό έχουμε $S[a_1,...,a_n]\subseteq\{f(a_1,...,a_n)\in R \mid f(x_1,...,x_n)\in R[x_1,...,x_n]\}$. Για την άλλη σχέση εγκλεισμού παρατηρούμε ότι ο $\{f(a_1,...,a_n)\in R \mid f(x_1,...,x_n)\in S[x_1,...,x_n]\}$ περιέχεται σε κάθε υποδακτύλιο του *R* που περιέχει το *S* και το $\{a_1,...,a_n\}$. Άρα ισχύει η ισότητα. □

Η προηγούμενη πρόταση εξηγεί το συμβολισμό $\mathbb{Z}[i]$ για τους ακέραιους του Gauss.

0.3 Ομομορφισμοί Δακτυλίων, Ιδεώδη

Έστω *R* και *S* δυο δακτύλιοι και $\varphi: R\to S$ μια απεικόνιση. Η φ καλείται *ομομορφισμός δακτυλίων* αν

(i) $\varphi(r_i + r_2)=\varphi(r_1)+\varphi(r_2)$ για κάθε $r_1, r_2\in R$

(ii) $\varphi(r_1r_2)=\varphi(r_1)\varphi(r_2)$ για κάθε $r_1, r_2\in R$, και

(iii) $\varphi(1_R)=1_S$.

Ένας ομομορφισμός δακτυλίων $\varphi: R\to S$ καλείται *επιμορφισμός* ή *μονομορφισμός* αν η φ ως απεικόνιση είναι αντίστοιχα επί ή $1-1$. *Ισομορφισμός* είναι ομομορφισμός που είναι ταυτόχρονα επιμορφισμός και μονομορφισμός. Αν $\varphi: R\to S$ είναι ένας ισομορφισμός θα λέμε ότι οι δακτύλιοι R και S είναι *ισόμορφοι* και θα συμβολίζουμε αυτό με $R\cong S$. Για παράδειγμα, η απεικόνιση $\varphi:\mathbb{Z}\to\mathbb{Z}_n$, $\varphi(m)=[m]$, είναι επιμορφισμός.

Έστω $\varphi: R\to S$ ένας ομομορφισμός δακτυλίων. Το σύνολο $\ker\varphi=\{r\in R \mid \varphi(r)=0_S\}$ ονομάζεται *πυρήνας* του φ. Η *εικόνα* του φ είναι $\mathrm{Im}\varphi=\{s\in S \mid s=\varphi(r)$ για κάποιο $r\in R\}$. Χρησιμοποιώντας την Πρόταση 0.2.2 εύκολα αποδεικνύεται ότι το $\mathrm{Im}\varphi$ είναι υποδακτύλιος του *S* (άσκηση). Επιπλέον έχουμε:

0.3.1 Πρόταση *Έστω $\varphi: R\to S$ ένας ομομορφισμός δακτυλίων. Τότε*

(i) ο φ είναι μονομορφισμός $\Leftrightarrow \ker\varphi = \{0\}$.

(ii) ο φ είναι επιμορφισμός $\Leftrightarrow \mathrm{Im}\varphi = S$.

Απόδειξη. (i) Έστω φ μονομορφισμός. Αν $r \in \ker\varphi$ τότε $\varphi(r) = 0$ και άρα $\varphi(r) = \varphi(0_R)$. Όμως ο φ είναι μονομορφισμός σημαίνει $r = 0_R$. Αντίστροφα έστω $\ker\varphi = \{0_R\}$. Αν $\varphi(r_1) = \varphi(r_2)$ με $r_1, r_2 \in R$, τότε $\varphi(r_1 - r_2) = 0_S$ και άρα $r_1 - r_2 \in \ker\varphi$. Συνεπώς $r_1 = r_2$.

(ii) Προφανές από τους ορισμούς. □

Έστω R ένας δακτύλιος και I ένα μη κενό υποσύνολο του R. Το I καλείται *ιδεώδες* του R αν i) $a + b \in I$ για κάθε $a, b \in I$ και ii) $ra \in I$ για κάθε $r \in R$ και $a \in I$. Για παράδειγμα, αν $\varphi : R \to S$ είναι ένας ομομορφισμός δακτυλίων, τότε ο πυρήνας $\ker\varphi$ είναι ιδεώδες του R (άσκηση). Ένα ιδεώδες I του R λέγεται *γνήσιο* αν $I \neq R$.

Ένα ιδεώδες του δακτυλίου R λέγεται *κύριο* αν έχει τη μορφή $I = \{ra \mid r \in R\}$ για κάποιο $a \in I$. Στην περίπτωση αυτή θα γράφουμε $I = (a)$ και θα λέμε ότι το I *παράγεται* από το a.

Έστω A ένα υποσύνολο του δακτυλίου R. Το *ιδεώδες που παράγεται από το A* είναι το ιδεώδες

$$\left\{ \sum_{i=1}^{m} r_i a_i \in R \mid m = 1, 2, \ldots,\ r_i \in R,\ a_i \in A \ \text{ για κάθε } \ i = 1, 2, \ldots, m \right\}$$

και το συμβολίζουμε (A). Αν το A είναι πεπερασμένο $A = \{a_1, \ldots, a_n\}$ χρησιμοποιούμε και το συμβολισμό $(a_1, \ldots, a_n)$ στη θέση του (A).

Έστω I ένα ιδεώδες του δακτυλίου R. Το σύνολο των πλευρικών κλάσεων $R/I = \{r + I \mid r \in R\}$ έχει τη δομή δακτυλίου με τις πράξεις $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$, $(r_1 + I)(r_2 + I) = r_1 r_2 + I$. Πράγματι, το μόνο πράγμα που δεν είναι τελείως προφανές είναι ότι οι προηγούμενες πράξεις είναι καλά ορισμένες: έστω $r_1 + I = r_1' + I$ και $r_2 + I = r_2' + I$. Τότε έχουμε $r_1 - r_1' \in I$ και $r_2 - r_2' \in I$. Για την πρόσθεση παρατηρούμε ότι $(r_1 + r_2) - (r_1' + r_2') = (r_1 - r_1') + (r_2 - r_2') \in I$ και άρα $(r_1 + r_2) + I = (r_1' + r_2') + I$. Για τον πολλαπλασιασμό παρατηρούμε ότι $r_1 r_2 - r_1' r_2' =$

$r_1(r_2 - r_2') + (r_1 - r_1')r_2' \in I$ και άρα $r_1 r_2 + I = r_1' r_2' + I$. Ο R/I καλείται *δακτύλιος πηλίκο*.

Είδαμε ότι σε κάθε μονορφισμό δακτυλίων $\varphi : R \to S$ αντιστοιχεί ο πυρήνας $\ker\varphi$ που είναι ιδεώδες του *R*. Αντίστροφα, έστω *I* ιδεώδες του *R*. Τότε ο ομομορφισμός δακτυλίων $\varphi : R \to R/I$, $f(r) = r + I$ (που καλείται *φυσικός επιμορφισμός*) έχει πυρήνα $\ker\varphi = I$. Έτσι υπάρχει στενή σχέση μεταξύ των εννοιών ομομορφισμός, ιδεώδες και δακτύλιος πηλίκο. Μία άλλη σχέση δίνεται από το παρακάτω αποτέλεσμα.

0.3.2 Θεώρημα (*Το 1ο Θεώρημα Ισομορφισμών Δακτυλίων*) *Έστω* $\varphi : R \to S$ *ένας ομομορφισμός δακτυλίων. Τότε υπάρχει ισομορφισμός δακτυλίων*

$$\overline{\varphi} : R/\ker\varphi \to \mathrm{Im}\,\varphi, \quad \overline{\varphi}(r + \ker\varphi) = \varphi(r).$$

Απόδειξη. Η $\overline{\varphi}$ είναι καλά ορισμένη. Πράγματι, αν $r + \ker\varphi = r' + \ker\varphi$, τότε $r - r' \in \ker\varphi$ και άρα $\varphi(r - r') = 0$. Δηλαδή $\varphi(r) = \varphi(r')$ και κατά συνέπεια $\overline{\varphi}(r + \ker\varphi) = \overline{\varphi}(r' + \ker\varphi)$. Το ότι ο $\overline{\varphi}$ είναι ομομορφισμός δακτυλίων βεβαιώνεται με έναν υπολογισμό ρουτίνας που παραλείπεται. Προφανώς ο $\overline{\varphi}$ είναι επί. Μένει να δείξουμε ότι είναι μονομορφισμός. Από την Πρόταση 0.3.1 (i) αρκεί να δείξουμε ότι $\ker\overline{\varphi} = \{0_{R/\ker\varphi}\}$. Πράγματι, παρατηρούμε ότι $\overline{\varphi}(r + \ker\varphi) = 0_S \Rightarrow \varphi(r) = 0_S \Rightarrow r \in \ker\varphi \Rightarrow r + \ker\varphi = \ker\varphi = 0_{R/\ker\varphi}$.

□

Η επόμενη πρόταση περιγράφει τα ιδεώδη του δακτυλίου πηλίκου R/I και θα χρησιμοποιηθεί συχνά στα παρακάτω.

0.3.3 Πρόταση *Έστω I ένα ιδεώδες του δακτυλίου R. Κάθε ιδεώδες του* R/I *έχει τη μορφή* J/I *όπου J είναι ιδεώδες του R που περιέχει το I.*

Απόδειξη. Σημειώνουμε πρώτα μία γενική παρατήρηση: αν $\varphi : R \to S$ είναι ένας ομομορφισμός δακτυλίων και *K* ένα ιδεώδες του *S*, τότε η αντίστροφη εικόνα $\varphi^{-1}(K) = \{r \in R \mid \varphi(r) \in K\}$ είναι ένα ιδεώδες του *R*. Πράγματι,

$r_1, r_2 \in \varphi^{-1}(K) \Rightarrow \varphi(r_1)$, $\varphi(r_2) \in K \Rightarrow \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) \in K \Rightarrow r_1 + r_2 \in K$, και $a \in R$, $r \in \varphi^{-1}(I) \Rightarrow \varphi(ar) = \varphi(a)\varphi(r) \in K \Rightarrow ar \in \varphi^{-1}(K)$. Εφαρμόζουμε τώρα την προηγούμενη παρατήρηση στον φυσικό επιμορφισμό $f : R \to R/I$. Έστω K ένα ιδεώδες του R/I. Το $f^{-1}(K)$ είναι ιδεώδες του R, που προφανώς περιέχει το I, για το οποίο ισχύει $f^{-1}(K)/I = K$. □

0.4 Κατασκευή Νέων Ιδεωδών από Παλαιά

Από τον ορισμό του ιδεώδους προκύπτει άμεσα ότι η τομή μιας μη κενής οικογένειας ενός δακτυλίου είναι και πάλι ιδεώδες.

Όμως δεν συμβαίνει το ίδιο για την ένωση. Για παράδειγμα η ένωση $(2) \cup (3)$ των κύριων ιδεωδών (2) και (3) του $\mathbb{Z}$ δεν είναι ιδεώδες (γιατί;). Ένα υποκατάστατο της ένωσης ιδεωδών είναι η πράξη του αθροίσματος ιδεωδών: έστω $(I_\lambda)_{\lambda \in \Lambda}$ μια οικογένεια ιδεωδών του δακτυλίου R. Το *άθροισμα* των I_λ είναι το ιδεώδες του R που παράγεται από το σύνολο $\bigcup_{\lambda \in \Lambda} I_\lambda$, δηλαδή είναι το ιδεώδες

$$\left(\bigcup_{\lambda \in \Lambda} I_\lambda \right) = \left\{ \sum_\lambda r_\lambda c_\lambda \mid r_\lambda \in R,\, c_\lambda \in I_\lambda, \text{ και } r_\lambda = 0 \right.$$

$$\left. \text{εκτός από ένα πεπερασμένο πλήθος } \lambda \right\}.$$

Το συμβολίζουμε με $\sum_{\lambda \in \Lambda} I_\lambda$. Στην ειδική περίπτωση που το Λ είναι πεπερασμένο σύνολο, $\Lambda = \{1,2,...,n\}$ χρησιμοποιούμε συνήθως το συμβολισμό $\sum_{i=1}^{n} I_i$ ή και $I_1 + \cdots + I_n$ και παρατηρούμε ότι ισχύει

$$\sum_{i=1}^{n} I_i = \{c_1 + \cdots + c_n \mid c_i \in I_i \text{ για } i = 1,...,n\}.$$

0.4.1 Παράδειγμα *Έστω $m, n \in \mathbb{N}$. Τότε στο $\mathbb{Z}$ ισχύει $(m) + (n) = (d)$, όπου d είναι ο μέγιστος κοινός διαιρέτης των m και n.*

Απόδειξη. Εφόσον το m είναι πολλαπλάσιο του d, έχουμε $(m) \subseteq (d)$. Όμοια $(n) \subseteq d$. Άρα από τον ορισμό $(m)+(n) \subseteq (d)$. Για την άλλη σχέση εγκλεισμού, γράφουμε το d ως γραμμικό συνδυασμό των m και n (το d είναι ο μέγιστος κοινός διαιρέτης των m και n). Έχουμε $d = mx + ny$, όπου $x, y \in \mathbb{Z}$. Άρα από τον ορισμό $d \in (m)+(n)$, και κατά συνέπεια $(d) \subseteq (m)+(n)$. □

Μια άλλη χρήσιμη πράξη ιδεωδών είναι το γινόμενο. Έστω I και J ιδεώδη του R. Με IJ συμβολίζουμε το ιδεώδες που παράγεται από το σύνολο $\{ab \in R \mid a \in I, b \in J\}$. Αυτό ονομάζεται *γινόμενο* των I και J. Η προσεταιριστικότητα του γινομένου στο R μας επιτρέπει να ορίσουμε κατά τον προφανή τρόπο το γινόμενο πεπερασμένου πλήθους ιδεωδών: Έστω $I_1,...,I_n$ ιδεώδη του R. Τότε ορίζουμε το ιδεώδες $\prod_{i=1}^{n} I_i = I_1 I_2 \cdots I_n$ ως το ιδεώδες του R που παράγεται από το σύνολο $\{a_1 a_2 \cdots a_n \mid a_i \in I_i \text{ για } i = 1,2,...,n\}$. Παρατηρούμε ότι $\prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i$.

Μετά την τομή, το άθροισμα και το γινόμενο ολοκληρώνουμε την "αριθμητική" των ιδεωδών ορίζοντας το ιδεώδες πηλίκο: Έστω I και J ιδεώδη του R. Θέτουμε $(I:J) = \{r \in R \mid rJ \subseteq I\}$. Αυτό είναι ένα ιδεώδες του R για το οποίο ισχύει $I \subseteq (I:J)$. Ονομάζεται *ιδεώδες πηλίκο*. Στην ειδική περίπτωση $I = (0)$, το ιδεώδες πηλίκο $(0:J) = \{r \in R \mid rJ = 0\} = \{r \in R \mid ra = 0 \text{ για κάθε } a \in J\}$ ονομάζεται *μηδενιστής του* J και συμβολίζεται με $\operatorname{Ann} J$.

0.5 Ακέραιες Περιοχές και Σώματα

Ένας δακτύλιος R (μεταθετικός όπως πάντα!) ονομάζεται *ακέραια περιοχή* ή απλώς *περιοχή* αν $0_R \neq 1_R$ και η σχέση $ab = 0$ με $a \in R$ και $b \in R$ ισχύει μόνο αν $a = 0$ ή $b = 0$. Για παράδειγμα οι δακτύλιοι $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Z}_3$ είναι περιοχές, ενώ ο $\mathbb{Z}_4$ δεν είναι.

0.5.1 Πρόταση *Ο δακτύλιος $\mathbb{Z}_n$ είναι περιοχή αν και μόνον αν ο n είναι πρώτος.*

Απόδειξη. Έστω n πρώτος. Αν $[a][b]=[0]$ στο $\mathbb{Z}_n$, τότε το n διαιρεί το γινόμενο ab. Εφόσον ο n είναι πρώτος, θα διαιρεί έναν τουλάχιστον από τους a και b. Άρα $[a]$ ή $[b]=0$, και συνεπώς ο $\mathbb{Z}_n$ είναι περιοχή.

Αντίστροφα, έστω ότι ο $\mathbb{Z}_n$ είναι περιοχή. Τότε αν $n=ab$ $(a,b\in N)$ με $1<a<n$ και $1<b<n$, έχουμε $[0]=[a][b]$ όπου $[a]\neq 0$ και $[b]\neq 0$. Αυτό είναι άτοπο. □

Ένας δακτύλιος R λέγεται *σώμα* αν $0_R\neq 1_R$ και κάθε $a\in R-\{0\}$ είναι αντιστρέψιμο. Προφανώς κάθε σώμα είναι περιοχή.

0.5.2 Πρόταση *Κάθε πεπερασμένη περιοχή είναι σώμα.*

Απόδειξη. Έστω R πεπερασμένη περιοχή και $a\in R$ με $a\neq 0$. Θα δείξουμε ότι το a είναι αντιστρέψιμο. Έστω $R=\{a_1,a_2,...,a_n\}$. Θεωρούμε τα στοιχεία $aa_1,aa_2,...,aa_n$. Αυτά είναι διακεκριμένα μεταξύ τους· πράγματι αν $aa_i=aa_j$ τότε $a(a_i-a_j)=0$ και αφού $a\neq 0$ και R είναι περιοχή, έχουμε $a_i=a_j$. Το πλήθος τους είναι n και άρα κάποιο απ' αυτά θα είναι το στοιχείο 1_R, δηλαδή $aa_i=1_R$ για κάποιο i. Άρα το a είναι αντιστρέψιμο. □

0.5.3 Πόρισμα *Ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα αν και μόνον αν ο n είναι πρώτος.*

Απόδειξη. Άμεση από τις Προτάσεις 0.5.1 και 0.5.2. □

0.5.4 Ορισμός *Έστω k σώμα. Μια k-άλγεβρα R είναι ένας δακτύλιος R εφοδιασμένος με μια απεικόνιση $k\times R\ni(a,r)\mapsto a\cdot r\in R$ που ικανοποιεί τις συνθήκες: Το R είναι k-διανυσματικός χώρος και*

$$a\cdot(r_1r_2)=(a\cdot r_1)r_2=r_1(a\cdot r_2)\quad \text{για κάθε}\quad a\in k,\ \ r_1,r_2\in R.$$

Για παράδειγμα, ο δακτύλιος $k[x]$ είναι μια k άλγεβρα.

0.5.5 Ορισμός *Έστω R και S δύο k-άλγεβρες. Μια απεικόνιση $\varphi: R\to S$ ονομάζεται ομομορφισμός (αντίστοιχα, μονομορφισμός, επιμορφισμός, ισομορφισμός) αλγε-*

βρών αν είναι ομομορφισμός (αντίστοιχα, μονομορφισμός, επιμορφισμός, ισομορφισμός) δακτυλίων και επιπλέον ισχύει

$$\varphi(ar) = a\varphi(r)$$

για κάθε $a \in k$ *και* $r \in R$.

Για παράδειγμα, έστω $a \in k$. Η απεικόνιση ("εκτίμηση στο *a*")

$$k[x] \ni f(x) \mapsto f(a) \in k$$

είναι ένας επιμορφισμός *k*-αλγεβρών.

0.6 Πρώτα και Μέγιστα Ιδεώδη

Θυμίζουμε εδώ τα πλέον βασικά περί πρώτων και μέγιστων ιδεωδών.

0.6.1 Ορισμός *Ένα ιδεώδες P του R καλείται πρώτο αν*

(i) $P \neq R$, *και*

(ii) αν $a,b \in R$ *με* $ab \in P$ *τότε* $a \in P$ *ή* $b \in P$.

0.6.2 Πρόταση *Έστω I ιδεώδες του R. Τότε το I είναι πρώτο αν και μόνο αν ο δακτύλιος πηλίκο* R/I *είναι περιοχή.*

Απόδειξη. Έστω *I* πρώτο. Τότε $I \neq R$ και $R/I \neq 0$. Έστω $a,b \in R$ με την ιδιότητα $(a+I)(b+I) = 0_{R/I}$. Τότε $ab + I = I$ και άρα $ab \in I$. Συνεπώς $a \in I$ ή $b \in I$ δηλαδή $a + I = 0_{R/I}$ ή $b + I = 0_{R/I}$.

Αντίστροφα, έστω R/I ακέραια περιοχή. Τότε $R/I \neq 0$ και άρα $I \neq R$. Έστω $a,b \in R$ με $ab \in I$. Τότε $ab + I = 0_{R/I} \Rightarrow (a+I)(b+I) = 0_{R/I} \Rightarrow$ $a + I = 0_{R/I}$ ή $b + I = 0_{R/I} \Rightarrow a \in I$ ή $b \in I$. □

0.6.3 Ορισμός *Ένα ιδεώδες M του R ονομάζεται μέγιστο (ή μεγιστικό) αν*

(i) $M \neq R$, *και*

(ii) δεν υπάρχει ιδεώδες I του R με την ιδιότητα $M \subsetneq I \subsetneq R$.

0.6.4 Πρόταση *Έστω I ένα ιδεώδες του R. Τότε το I είναι μέγιστο αν και μόνο αν ο δακτύλιος πηλίκο* R/I *είναι σώμα.*

Απόδειξη. Έστω ότι το I είναι μέγιστο. Τότε $I \neq R$ και $R/I \neq 0$. Έστω $a+I \in R/I$ με $a+I \neq 0_{R/I}$. Θα δείξουμε ότι το $a+I$ είναι αντιστρέψιμο. Εφόσον $a+I \neq 0_{R/I}$ ισχύει $a \notin I$. Το ιδεώδες $(a)+I$ περιέχει γνήσια το I. Αφού το I είναι μέγιστο έχουμε $(a)+I = R$. Άρα για κάποια $r \in R$ και $b \in I$ ισχύει $ra+b=1$. Συνεπώς $(r+I)(a+I) = ra+I = (1-b)+I = 1+I$ και το $r+I$ είναι αντιστρέψιμο.

Αντίστροφα, έστω ότι ο R/I είναι σώμα. Τότε $R/I \neq 0$ και άρα $I \neq R$. Έστω J ιδεώδες με $I \subsetneq J \subsetneq R$. Θα δείξουμε ότι $J = R$, οπότε το I είναι μέγιστο. Υπάρχει $a \in J$, $a \notin I$. Άρα $a+I \neq 0_{R/I}$ και, αφού το R/I είναι σώμα, $(a+I)(b+I) = 1+I$ για κάποιο $b \in R$. Άρα

$$ab-1 \in I.$$

Εφόσον $I \subseteq J$ και $a \in J$ συμπεραίνουμε ότι $1 \in J$, δηλαδή $J = R$. □

0.6.5 Πόρισμα *Κάθε μέγιστο ιδεώδες είναι πρώτο.*

Απόδειξη. Άμεση από τις Προτάσεις 0.6.4 και 0.6.2. □

Για παράδειγμα, το ιδεώδες (x) του $\mathbb{Z}[x]$ είναι πρώτο, γιατί $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ που είναι περιοχή, και όχι μέγιστο αφού ο $\mathbb{Z}$ δεν είναι σώμα. Το ιδεώδες $(2,x)$ του $\mathbb{Z}[x]$ είναι μέγιστο, αφού $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}_2$ (γιατί;) που είναι σώμα. Στο επόμενο κεφάλαιο θα περιγράψουμε όλα τα πρώτα (και μέγιστα) ιδεώδη του $\mathbb{Z}[x]$ (Πρόταση 1.4.1).

0.7 Σώμα Πηλίκων Ακέραιας Περιοχής

Θυμίζουμε εδώ την κατασκευή του σώματος πηλίκων μιας ακέραιες περιοχής R. Ειδικότερα θα δούμε πως ο R εμφυτεύεται ως υποδακτύλιος σ' ένα σώμα σε αναλογία με την εμφύτευση του $\mathbb{Z}$ στο $\mathbb{Q}$.

0.7.1 Πρόταση *Έστω R μια περιοχή. Τότε υπάρχει σώμα k και μονομορφισμός δακτυλίων $\varphi : R \to k$ έτσι ώστε κάθε στοιχείο του k γράφεται στη μορφή $\varphi(r)\varphi(s)^{-1}$ για κάποια $r, s \in R$, $s \neq 0$.*

Απόδειξη. Θέτουμε $S = R - \{0\}$. Στο σύνολο $R \times S$ ορίζουμε μια σχέση ισοδυναμίας

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc .$$

Η κλάση ισοδυναμίας που περιέχει το στοιχείο (a,b) συμβολίζεται $\frac{a}{b}$. Το σύνολο των κλάσεων ισοδυναμίας, έστω k, είναι σώμα με πράξεις

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

(Η επαλήθευση του καλώς ορισμένου των πράξεων και των αξιωμάτων είναι θέμα ρουτίνας και παραλείπεται). Το μηδέν του σώματος αυτού είναι το $\frac{0}{1}$ και το μοναδιαίο στοιχείο είναι το $\frac{1}{1}$. Τέλος η συνάρτηση $\varphi : R \to k$, $\varphi(a) = \frac{a}{1}$ για κάθε $a \in R$, είναι μονομορφισμός δακτυλίων και το τυχαίο $\frac{a}{b} \in k$ γράφεται $\varphi(a)\varphi(b)^{-1}$.

□

Το σώμα που κατασκευάσαμε πιο πάνω ονομάζεται *σώμα πηλίκων* του R. Για παράδειγμα, το σώμα πηλίκων του $\mathbb{Z}$ είναι το $\mathbb{Q}$ και το σώμα πηλίκων του $k[x]$ (k σώμα) είναι το σώμα των ρητών συναρτήσεων

$$k(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x], g(x) \neq 0 \right\}.$$

0.8 Επεκτάσεις Σωμάτων

Αν $E \supseteq F$ είναι σώματα (ως προς τις ίδιες πράξεις) θα λέμε ότι το E είναι *επέκταση* του F. Συμβολικά γράφουμε E / F. Ο *βαθμός* της επέκτασης E / F είναι η διάσταση του E ως F-διανυσματικός χώρος. Συμβολικά $[E : F] = \dim_F E$. Μια επέκταση σωμάτων E / F λέγεται πεπερασμένη αν $[E : F] < \infty$. Ένα στοιχείο

$a \in E$ λέγεται *αλγεβρικό* επί του F αν είναι ρίζα κάποιου μη μηδενικού πολυωνύμου $f(x) \in F[x]$. Για παράδειγμα το $\sqrt{2} \in \mathbb{R}$ είναι αλγεβρικό επί του $\mathbb{Q}$, γιατί είναι ρίζα του $x^2 - 2 \in \mathbb{Q}[x]$. Μια επέκταση E/F λέγεται αλγεβρική αν κάθε $a \in E$ είναι αλγεβρικό επί του F.

0.8.1 Πρόταση *Κάθε πεπερασμένη επέκταση σωμάτων είναι αλγεβρική.*

Απόδειξη. Έστω E/F επέκταση με $[E:F] = n < \infty$. Έστω $a \in E$. Τα στοιχεία

$$1 = a^0, a^1, a^2, ..., a^n$$

είναι γραμμικώς εξαρτημένα επί του F γιατί το πλήθος τους είναι $n+1 > n$. Άρα υπάρχουν $\lambda_0, \lambda_1, ..., \lambda_n \in F$ (όχι όλα μηδέν) με την ιδιότητα

$$\lambda_0 + \lambda_1 a + \cdots + \lambda_n a^n = 0.$$

Αν θέσουμε

$$f(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_n x^n \in F[x]$$

τότε $f(x) \neq 0$ και το a είναι ρίζα του $f(x)$. □

Ένα σώμα F λέγεται *αλγεβρικά κλειστό* αν κάθε μη σταθερό πολυώνυμο $f(x) \in F[x]$ έχει μια τουλάχιστον ρίζα στο F. Συνεπώς ένα σώμα F είναι αλγεβρικά κλειστό αν κάθε μη σταθερό πολυώνυμο $f(x) \in F[x]$ γράφεται ως γινόμενο πρωτοβάθμιων παραγόντων στο $F[x]$.

Αναφέρουμε χωρίς απόδειξη ότι για κάθε σώμα F υπάρχει επέκταση $\overline{F}/F$ όπου το $\overline{F}$ είναι αλγεβρικά κλειστό σώμα. Το $\overline{F}$ είναι μοναδικό (με προσέγγιση ισομορφισμού) και ονομάζεται *αλγεβρική θήκη* του F. Για παράδειγμα η αλγεβρική θήκη του $\mathbb{R}$ είναι το $\mathbb{C}$, πράγμα που έπεται από το Θεμελιώδες Θεώρημα της Άλγεβρας, που παραθέτουμε χωρίς απόδειξη.

0.8.2 Θεμελιώδες Θεώρημα της Άλγεβρας *Το σώμα $\mathbb{C}$ είναι αλγεβρικά κλειστό.*

0.8.3 Θεώρημα *Αν οι επεκτάσεις σωμάτων E/F και K/E είναι πεπερασμένες, τότε η επέκταση K/F είναι πεπερασμένη και*

$$[K:F] = [K:E][E:F].$$

Απόδειξη. Έστω $[E:F]=n$ και $[K:E]=m$. Έστω

$$a_1,...,a_n$$

μια βάση του E ως F-διανυσματικός χώρος και

$$b_1,...,b_m$$

μια βάση του K ως E-διανυσματικός χώρος. Θα δείξουμε ότι το σύνολο

$$X=\{a_ib_j\in K \mid i=1,...,n,\ j=1,...,m\}$$

αποτελεί μία βάση του K ως F-διανυσματικός χώρος.

Έστω $c\in K$. Τότε το c είναι E-γραμμικός συνδυασμός των στοιχείων $b_1,...,b_m$. Επειδή κάθε στοιχείο του E είναι F-γραμμικός συνδυασμός των στοιχείων $a_1,...,a_n$ συμπεραίνουμε ότι το c είναι F-γραμμικός συνδυασμός των στοιχείων a_ib_j. Άρα το X παράγει το K επί του F.

Έστω

$$\sum_{i,j}\lambda_{ij}a_ib_j=0 \quad (\lambda_{ij}\in F).$$

Γράφοντας

$$\sum_{i,j}\lambda_{ij}a_ib_j=\sum_j\left(\sum_i\lambda_{ij}a_i\right)b_j=0$$

συμπεραίνουμε ότι για κάθε $j=1,...,m$

$$\sum_i\lambda_{ij}a_i=0$$

γιατί τα b_j αποτελούν βάση. Η τελευταία σχέση δίνει $\lambda_{ij}=0$, γιατί τα a_i αποτελούν βάση. Συνεπώς το X είναι γραμμικά ανεξάρτητο επί του F. □

0.9 Θεμελιώδες Θεώρημα Συμμετρικών Πολυωνύμων

Ένα πολυώνυμο $f(x_1,...,x_n)\in R[x_1,...,x_n]$ ονομάζεται *συμμετρικό* αν για κάθε μετάθεση σ των στοιχείων $1,2,...,n$ ισχύει

$$f(x_{\sigma(1)},...,x_{\sigma(n)})=f(x_1,...,x_n).$$

Για παράδειγμα, τα ακόλουθα πολυώνυμα είναι συμμετρικά

$$e_1=x_1+x_2+\cdots+x_n$$

$$e_2=x_1x_2+\cdots+x_1x_n+\cdots+x_{n-1}x_n$$

$$\cdots$$

$$e_n = x_1 x_2 \cdots x_n .$$

Τα e_i ονομάζονται *στοιχειώδη* συμμετρικά πολυώνυμα. Παρατηρούμε ότι αυτά εμφανίζονται ως συντελεστές (με προσέγγιση προσήμου) του πολυωνύμου $(x-x_1)(x-x_2)\cdots(x-x_n) \in R[x_1,...,x_n][x]$ αφού

$$(x-x_1)\cdots(x-x_n) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^n e_n .$$

0.9.1 Θεμελιώδες Θεώρημα Συμμετρικών Πολυωνύμων *Κάθε συμμετρικό πολυώνυμο είναι πολυώνυμο στα στοιχειώδη συμμετρικά πολυώνυμα.*

Δηλαδή αν $f(x_1,...,x_n)$ είναι ένα συμμετρικό πολυώνυμο, τότε ισχύει $f(x_1,...,x_n) = g(e_1,...,e_n)$ για κάποιο $g(x_1,...,x_n) \in R[x_1,...,x_n]$. Για παράδειγμα $x_1^2 + \cdots + x_n^2 = e_1^2 - 2e_2$.

Απόδειξη. Θα δώσουμε μια στοιχειώδη απόδειξη που είναι μάλιστα κατασκευαστική.

Ορίζουμε μια ολική διάταξη στα μονώνυμα $x_1^{a_1} \cdots x_n^{a_n}$

$$x_1^{a_1} \cdots x_n^{a_n} > x_1^{b_1} \cdots x_n^{b_n}$$

αν η πρώτη μη μηδενική διαφορά $a_i - b_i$ είναι θετική. (Η διάταξη αυτή συνήθως καλείται *λεξικογραφική*). Για παράδειγμα $x_1^2 x_2 > x_1 x_2^2 > x_1 x_2$.

Έστω $f(x_1,...,x_n)$ ένα συμμετρικό πολυώνυμο και

$$x_1^{a_1} \cdots x_n^{a_n}$$

το μέγιστο μονώνυμο του $f(x_1,...,x_n)$ ως προς τη λεξικογραφική διάταξη. Επειδή το $f(x_1,...,x_n)$ είναι συμμετρικό θα περιέχει κάθε μονώνυμο που λαμβάνεται από το $x_1^{a_1} \cdots x_n^{a_n}$ με κάποια μετάθεση των $a_1,...,a_n$. Συνεπώς ισχύει

$$a_1 \geq a_2 \geq \cdots \geq a_n .$$

Θεωρούμε τώρα το μέγιστο μονώνυμο που περιέχεται στο πολυώνυμο

$$e_1^{a_1} \cdots e_n^{a_n} .$$

Το μονώνυμο αυτό είναι το

$$x_1^{a_1+\cdots+a_n} x_2^{a_2+\cdots+a_n} \cdots x_n^{a_n} .$$

Συνεπώς το μέγιστο μονώνυμο που περιέχει το πολυώνυμο

$$e_1^{a_1-a_2}e_2^{a_2-a_3}\cdots e_n^{a_n}$$

είναι το

$$x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}.$$

Έστω c ο συντελεστής του $x_1^{a_1}\cdots x_n^{a_n}$ στο $f(x_1,...,x_n)$. Τότε το μέγιστο μονώνυμο του πολυωνύμου

$$f_1 = f(x_1,...,x_n) - ce_1^{a_1-a_2}e_2^{a_2-a_3}\cdots e_n^{a_n}$$

είναι μικρότερο από το $x_1^{a_1}\cdots x_n^{a_n}$. Έχουμε $\deg f_1 \le \deg f(x_1,...,x_n)$ γιατί $\deg e_1^{a_1-a_2}e_2^{a_2-a_3}\cdots e_n^{a_n} = a_1+\cdots+a_n$. Επαναλαμβάνουμε τη διαδικασία στο f_1, κοκ. Όμως το πλήθος των μονωνύμων που είναι μικρότερα του $x_1^{a_1}\cdots x_n^{a_n}$ και έχουν βαθμό $\le \deg f(x_1,...,x_n)$ είναι βέβαια πεπερασμένο. Έτσι, μετά ένα πεπερασμένο πλήθος βήματα, έχουμε $f_k = 0$, δηλαδή το $f(x_1,...,x_n)$ γράφεται ως πολυώνυμο στα $e_1,...,e_n$. □

Για παράδειγμα, έστω $n=3$ και

$$f(x_1,x_2,x_3) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2.$$

Τότε

$$a_1 = 2,\quad a_2 = 1,\quad a_3 = 0,$$

και

$$f_1 = f(x_1,x_2,x_3) - e_1e_2,$$

σύμφωνα με την απόδειξη. Όμως με πράξεις διαπιστώνουμε ότι $f(x_1,x_2,x_3)$ $-e_1e_2 = -3x_1x_2x_3$. Άρα

$$f(x_1,x_2,x_3) = e_1e_2 - 3e_3.$$ □

Ασκήσεις

1*. Ο δακτύλιος R είναι ακέραια περιοχή αν και μόνο αν ο δακτύλιος $R[x]$ είναι ακέραια περιοχή.

2. Το στοιχείο $\sum_{i=0}^{\infty} r_i x^i \in R[[x]]$ είναι αντιστρέψιμο αν και μόνο αν το στοιχείο $r_0 \in R$ είναι αντιστρέψιμο.

3. Δώστε ένα παράδειγμα ενός υποδακτυλίου του $\mathbb{Q}[x]$ που δεν είναι ιδεώδες του $\mathbb{Q}[x]$.

4. Αποδείξτε ότι το ιδεώδες $(2,x)$ του $\mathbb{Z}[x]$ δεν είναι κύριο.

5. Για τα κύρια ιδεώδη $I=(m)$, $I=(n)$ του $\mathbb{Z}$ ποια είναι τα ιδεώδη $I\cap J$, $I+J$, IJ και $(I:J)$; Η απάντηση να δοθεί συναρτήσει της παραγοντοποίησης των *m* και *n* σε γινόμενα πρώτων αριθμών.

6*. Έστω *I*, *J*, *K* ιδεώδη του *R*, και έστω $(I_\lambda)_{\lambda\in\Lambda}$ μια οικογένεια ιδεωδών του *R*. Αποδείξτε τις παρακάτω σχέσεις.

(i) $\big((I:J):K\big)=(I:JK)=\big((I:K):J\big)$

(ii) $\left(\bigcap_{\lambda\in\Lambda} I_\lambda : K\right)=\bigcap_{\lambda\in\Lambda}(I_\lambda:K)$

(iii) $\left(J:\sum_{\lambda\in\Lambda} I_\lambda\right)=\bigcap_{\lambda\in\Lambda}(J:I_\lambda)$

7. Στον δακτύλιο $\mathbb{Q}[x_1,x_2,x_3,x_4]$ θεωρούμε τα ιδεώδη $I=(x_1,x_2)$ και $J=(x_3,x_4)$. Αποδείξτε ότι $IJ\neq\{fg \mid f\in I,\ g\in J\}$.

8. Έστω *I*, *J*, *K* ιδεώδη του δακτυλίου *R*.

(i) Ισχύει ότι $IJ=I\cap J$;

(ii) Αποδείξτε ότι $I\cap(J+K)\supseteq I\cap J+I\cap K$;

(iii) Αν $I+J=R$ αποδείξετε ότι $IJ=I\cap J$.

9. Είναι ισόμορφοι οι δακτύλιοι $\mathbb{Z}[i]$ και $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$;

10. Έστω $\varphi: R\to S$ ομομορφισμός δακτυλίων όπου το *S* είναι περιοχή. Αποδείξτε ότι το ιδεώδες $\ker\varphi$ είναι πρώτο.

11. Κάθε περιοχή με πεπερασμένο πλήθος ιδεωδών είναι σώμα.

12. Έστω *R* ένας πεπερασμένος δακτύλιος. Τότε κάθε πρώτο ιδεώδες του *R* είναι μέγιστο.

13. Ο δακτύλιος $\mathbb{Z}[x]$ έχει άπειρο πλήθος μέγιστων ιδεωδών.

14*. Σωστό (απαιτείται απόδειξη) ή Λάθος (αρκεί ένα αντιπαράδειγμα). Έστω $\varphi : R \to S$ ένας ομομορφισμός δακτυλίων

(i) I ιδεώδες του $R \Rightarrow \varphi(I)$ ιδεώδες του S.

(ii) I ιδεώδες του R και φ επιμορφισμός $\Rightarrow \varphi(I)$ ιδεώδες του S.

(iii) J ιδεώδες του $S \Rightarrow \varphi^{-1}(J)$ ιδεώδες του R.

(iv) P πρώτο ιδεώδες του R, φ επιμορφισμός $\Rightarrow \varphi(P)$ πρώτο ιδεώδες του S.

(v) P πρώτο ιδεώδες του R, φ επιμορφισμός, $\ker\varphi \subseteq P \Rightarrow \varphi(P)$ πρώτο ιδεώδες του S.

(vi) M μέγιστο ιδεώδες του R, φ επιμορφισμός, $\ker\varphi \subseteq M \Rightarrow \varphi(M)$ μέγιστο ιδεώδες του S.

15. Έστω $I \subseteq J$ ιδεώδη του R. Τότε υπάρχει ισομορφισμός

$$(R/I)/(J/I) \to R/J$$
$$(r+I)+J/I \mapsto r+J$$

(Υπόδειξη: Εφαρμόστε το Θεώρημα 0.3.2).

16*. Έστω $I \subseteq J$ ιδεώδη του R. Τότε

(a) Το ιδεώδες J/I του R/I είναι πρώτο $\Leftrightarrow$ το J είναι πρώτο

(b) Το ιδεώδες J/I του R/I είναι μεγιστο $\Leftrightarrow$ το J είναι μέγιστο.

(Υπόδειξη: Άσκηση 15).

17*. (Ταυτότητα διαίρεσης) Έστω $f, g \in R[x]$. Αν ο μεγιστοβάθμιος συντελεστής του $g(x)$ είναι αντιστρέψιμο στοιχείο του R, τότε υπάρχουν $q, r \in R[x]$ με τις ιδιότητες

(1) $f = qg + r$

(2) $\deg r < \deg q$

Επιπλέον, τα q, r είναι μοναδικά.

(Υπόδειξη: για την ύπαρξη, χρησιμοποιήσετε επαγωγή στο $m = \deg f$. Για το επαγωγικό βήμα, παρατηρήσετε ότι ο βαθμός του $f - a_m b_n^{-1} x^{m-n} g$, όπου $f = a_m x^m + \cdots + a_0$ και $g = b_n x^n + \cdots + b_0$ είναι $< m$).

18*. (Κριτήριο του Eisenstein). Έστω $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ και $p \in \mathbb{Z}$ πρώτος αριθμός. Αν

(i) p διαιρεί τους $a_0, a_1, ..., a_{n-1}$

(ii) p δεν διαιρεί τον a_n

(iii) p^2 δεν διαιρεί τον a_0

τότε το f είναι ανάγωγο πολυώνυμο στο $\mathbb{Z}[x]$.

(Παρατήρηση: ισχύει το ισχυρότερο συμπέρασμα ότι το f είναι ανάγωγο στο $\mathbb{Q}[x]$. Βλέπε Λήμμα 1.3.4 στο επόμενο Κεφάλαιο).

19. Εφαρμόστε το θεμελιώδες θεώρημα των συμμετρικών πολυωνύμων στο πολυώνυμο $x_1^4 + x_2^4 + x_1^3 x_2 + x_1 x_2^3$ $(n = 2)$.

20. Αποδείξτε ότι το $\mathbb{Q}[\sqrt{2}]$ είναι ισόμορφο με το σώμα πηλίκων του $\mathbb{Z}[\sqrt{2}]$.

21. Στην απόδειξη της Πρότασης 0.7.1, που χρησιμοποιήθηκε η υπόθεση ότι το R είναι ακέραια περιοχή;