Έστω $\langle R, +, \cdot \rangle$ μεταθετικός δακτύλιος με μονάδα 1_R τότε

$R[[t]] = \left\{ (a_n)_{n\geq 0} \mid \begin{matrix} a_n \in R \\ n\geq 0 \end{matrix} \right\}$

Πρόσθεση: $\forall (a_n)_{n\geq 0}, (b_n)_{n\geq 0} \in R[[t]]: (a_n)_{n\geq 0} + (b_n)_{n\geq 0} = (a_n + b_n)_{n\geq 0}$

Πολλαπλασιασμός: $\forall (a_n)_{n\geq 0}, (b_n)_{n\geq 0} \in R[[t]]: (a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} = (a_n \cdot b_n)$
$= \gamma_n$

όπου $\gamma_n = a_0 \cdot b_n + a_1 b_{n-1} + \dots + a_n b_0 = \sum_{k=0}^{n} a_k b_{n-k}$

Πρόταση: Η τριάδα $\langle R[[t]], +, \cdot \rangle$ είναι ένας μεταθετικός δακτύλιος με μονάδα $1_{R[[t]]} = \{1_R, 0, 0, \dots\}$.

Ο δακτύλιος R καλείται ο δακτύλιος των τυπικών δυναμοσειρών με στοιχεία από τον R

Συμβολισμός: $t := (0, 1_R, 0, 0, \dots)$

$\vdots$

$t^n := (0, 0, 0, \dots, 1, 0, \dots)$, $\forall n \in \mathbb{N}$
(n+1 όροι)

Τότε $t^n = t \cdot t \cdot t \cdot \ldots \cdot t$
$\leftarrow n-0$

Επίσης $\forall r \in R$, $\forall (a_n)_{n\geq 0} : r(a_n)_{n\geq 0} = (ra_n)_{n\geq 0} = (ra_0, ra_1, \ldots, \ldots)$

Άρα $r \cdot (a_n)_{n\geq 0} = (r, 0, 0, \ldots) \cdot (a_0, a_1, a_2, \ldots)$

Έστω τώρα $(a_n)_{n\geq 0} \in R[[t]]$. Τότε $(a_n)_{n\geq 0} = \{a_0, a_1, a_2, \ldots\}$

$= (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + \ldots + (0, 0, \ldots, a_n, 0, \ldots)$

$= a_0(1_R, 0, 0, \ldots) + a_1(0, 1_R, 0, \ldots) + \ldots + a_n(0, 0, \ldots, 1_R, \ldots) + \ldots$

$= a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n + \ldots = \sum_{n=0}^{+\infty} a_n t^n$

Άρα, $\forall (a_n)_{n\geq 0} \in R[[t]] : (a_n)_{n\geq 0} = \sum_{n=0}^{+\infty} a_n t^n$

Ορίζουμε $R[t] = \{(a_n)_{n\geq 0} \in R[[t]] \mid \exists n \in \mathbb{N} : a_k = 0, \forall k > n\}$

$= \left\{ \sum_{n=0}^{+\infty} a_n t^n \in R[[t]] \mid \exists n \in \mathbb{N} : a_k = 0, \forall k > n \right\}$

$= \left\{ \sum_{k=0}^{+\infty} a_k t^k \in R[[t]] \;\middle|\; \begin{matrix} a_k \in R \\ n \in \mathbb{N} \end{matrix} \right\}$

Πρόταση: Το υποσύνολο $R[t]$ είναι ένας υποδακτύλιος του $R[[t]]$.

Απόδειξη: • $0_{R[[t]]} = (0,0,\dots,0) \in R[t]$

• $1_{R[[t]]} = (1_R, 0, 0, \dots, 0, \dots) \in R[t]$

• Αν $(a_n)_{n\geq 0}$ και $(b_n)_{n\geq 0} \in R[t] \Rightarrow \exists n \in \mathbb{N}: a_k = 0, \ \forall k > n$
$\exists m \in \mathbb{N}: b_k = 0, \ \forall k > m$

Τότε $(a_n)_{n\geq 0} + (b_n)_{n\geq 0} = (a_n + b_n)_{n\geq 0} \in R[t]$ διότι $a_k + b_k = 0$
για κάθε $k > \max\{n, m\}$

• $(a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} = \left(\sum_{k=0}^{n} a_n b_{n-k} \right)_{n\geq 0} \in R[t]$ διότι
γ_n

$\gamma_k = 0, \ \forall k \geq m+n$

Ο δακτύλιος $R[t]$ καλείται δακτύλιος των πολυωνύμων με συντελεστές από τον δακτύλιο R

Έτσι για παράδειγμα αποκτούμε τους δακτυλίους πολυωνύμων

$Z[t]$, $Q[t]$, $R[t]$, $C[t]$, $Z_n[t]$

Αν $P(t) = \sum_{k=0}^{n} a_k \cdot t^k \in R[t]$ τότε ορίζεται η συνάρτηση

$\varphi: R \to R$ με $\varphi(x) = P(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

Έτσι από ένα πολυώνυμο οδηγηθήκαμε σε μια πολυωνυμική συνάρτηση. Αντίστροφα, κάθε πολυωνυμική συνάρτηση ορίζει ένα πολυώνυμο υπεράνω του R. Αν όμως $|R| = +\infty$ τότε μπορούμε να ταυτίσουμε πολυωνυμικές συναρτήσεις και πολυώνυμα.

Παράδειγμα: (1) $Z[i] = \{a+bi \in \mathbb{C} \mid a, b \in Z\} \subseteq G$

Τότε το $Z[i]$: υποδακτύλιος του $\mathbb{C}$ ο οποίος καλείται υποδακτύλιος των ακεραίων του Gauss.

(2) Για κάθε $X \neq \emptyset$ και για κάθε δακτύλιο R η τριάδα $\langle F(X,R), +, \cdot \rangle$ είναι δακτύλιος όπου $F(X,R) = \{\varphi: X \to R \mid \varphi \text{ απεικόνιση}\}$

Άρα $\langle F([0,1],\mathbb{R}), +, \cdot \rangle$ είναι δακτύλιος και τότε το $\langle C([0,1],\mathbb{R}), +, \cdot \rangle$ είναι υποδακτύλιος του $\langle F([0,1],\mathbb{R}), +, \cdot \rangle$ όπου $C([0,1],\mathbb{R}) = \{\varphi \in F([0,1],\mathbb{R}) : \varphi \text{ συνεχής}\}$

Έστω R_1, R_2 δύο δακτύλιοι τότε θεωρούμε το

$$R_1 \times R_2 = \{(r_1, r_2) \mid r_1 \in R_1 \wedge r_2 \in R_2\}$$

Πρόσθεση: $(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', r_2 + r_2')$

Πολλαπλασιασμός: $(r_1, r_2) \cdot (r_1', r_2') = (r_1 r_1', r_2 r_2')$

Με τις παραπάνω πράξεις το σύνολο $R_1 \times R_2$ είναι δακτύλιος με μονάδα $1_{R_1 \times R_2} = (1_{R_1}, 1_{R_2})$ ο οποίος καλείται ως ο δακτύλιος ευθύ γινόμενο των R_1 και R_2.

Βασικές Ιδιότητες: Έστω R: δακτύλιος και $r, s \in R$. Τότε:

(i) $\forall n, m \geq 1 : r^{n+m} = r^n \cdot r^m$ και $(r^n)^m = r^{mn}$

(ii) Υπό την προϋπόθεση ότι τα r και s μετατίθενται (δηλ. ότι: $rs = sr$)

$$(\forall n \geq 0) : (r+s)^n = \sum_{k=0}^{n} \binom{n}{k} r^{n-k} \cdot s^k$$

(iii) Αν $r_1, r_2, \ldots, r_n \in R$ τότε $s_1, s_2, \ldots, s_m \in R$ τότε (δηλ. ότι:

$$\sum_{i=1}^{n} r_i \cdot \sum_{j=1}^{m} s_j = \sum_{i=1}^{n} \sum_{j=1}^{m} r_i \cdot s_j$$

(iv) $(\forall n \in \mathbb{Z})\ (\forall r, s \in R) : (n \cdot r) \cdot s = n(rs) = r(ns)$

Ορισμός: Ένα στοιχείο $r \in R$ καλείται αντιστρέψιμο αν
$\exists r' \in R: r \cdot r' = 1_R = r' \cdot r$

$U(R) = \{r \in R \mid r: \text{αντιστρέψιμο}\}$ ← σύνολο των αντιστρέψιμων στοιχείων του R

Πρόταση: Το σύνολο $U(R)$ εφοδιασμένο με την πράξη $\cdot$ του δακτυλίου R είναι ομάδα, η ομάδα των αντιστρέψιμων στοιχείων του R.

Απόδειξη: Αν $r, s \in U(R)$ τότε $\exists r', s' \in R: \begin{cases} r \cdot r' = 1_R = r' \cdot r \\ s \cdot s' = 1_R = s' \cdot s \end{cases}$

Επίσης $(r \cdot s) \cdot (s' \cdot r') = r \cdot \underbrace{s \cdot s'}_{1_R} \cdot r' = r \cdot r' = 1_R$

Όμοια $(s' \cdot r') \cdot (r \cdot s = s' \cdot \underbrace{r' \cdot r}_{1_R} \cdot s = s' \cdot s = 1_R$

Προφανώς, η πράξη $\cdot$ είναι προσεταιριστική επί του $U(R)$ αφού είναι προσεταιριστική επί του R

επιπλέον, $1_R \in U(R)$ και 1_R αντιστρέψιμο ώς την $\cdot$ επί του $U(R)$

$\forall r \in U(R)\ \exists x \in U(R): r \cdot x = 1_R = x \cdot r$ | Αν θέσουμε $x = r'$ τότε $r' \in U(R)$ δείξε $r' \cdot r = 1_R = r \cdot r'$

Από όλα τα παραπάνω το $U(R)$ είναι ομάδα

Παράδειγμα: (1) $U(\mathbb{Z}) = \{-1, 1\}$

(2) $U(\mathbb{Q}) = \mathbb{Q}^*$ (3) $U(\mathbb{R}) = \mathbb{R}^*$ (4) $U(\mathbb{C}) = \mathbb{C}^*$

(5) $U(\mathbb{Z}_n) = \{ [k]_n \in \mathbb{Z}_n \mid (k,n) = 1 \}$

(6) $U(M_n(\mathbb{R})) = \{ A \in M_n(\mathbb{R}) \mid \det A \neq 0 \}$

Ορισμός: Ένας δακτύλιος R καλείται δακτύλιος διαίρεσης αν-ν $U(R) = R^*$, δηλαδή κάθε μη-μηδενικό στοιχείο του αντιστρέψεται.

Ορισμός: Καλούμε σώμα έναν μεταθετικό δακτύλιο διαίρεσης

Παράδειγμα: (1) Ο $\mathbb{Z}$ δεν είναι δακτύλιος διαίρεσης και φυσικά ούτε σώμα. Όμως οι δακτύλιοι $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι σώματα.

(2) Οι δακτύλιοι $M_n(\mathbb{K})$ όπου $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ δεν είναι δακτύλιοι διαίρεσης.

(3) Οι δακτύλιοι πολυωνύμων $R[t]$ δεν είναι ποτέ σώματα.

Ορισμός: Ένα στοιχείο $r \in R$ καλείται αριστερός διαιρέτης του μηδέν αν-ν: (i) $r \neq 0$ και:
(ii) $\exists\, 0 \neq s \in R : r \cdot s = 0$

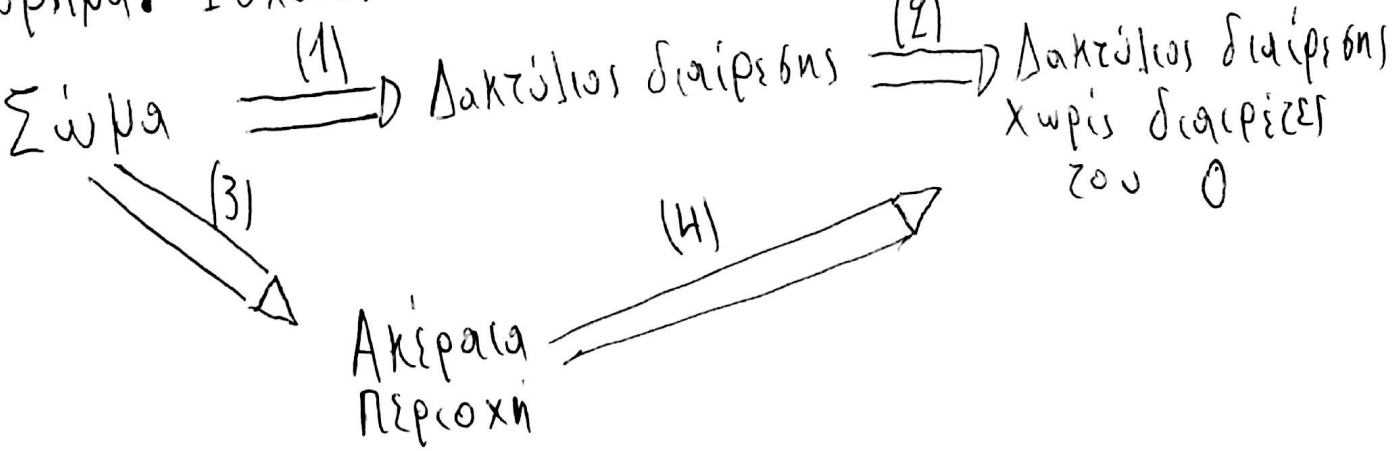
Ορισμός: Ένα στοιχείο $r \in R$ καλείται δεξιός διαιρέτης του μηδέν αν-ν: (i) $r \neq 0$ και (ii) $\exists\, 0 \neq s \in R : s \cdot r = 0$

Ορισμός: Ο δακτύλιος R καλείται δακτύλιος χωρίς διαιρέτες του μηδέν αν δεν υπάρχουν αριστεροί ή δεξιοί διαιρέτες του μηδέν στον R.

Ορισμός: Ακέραια περιοχή καλείται κάθε μεταθετικός δακτύλιος χωρίς διαιρέτες του μηδέν στον R

Παράδειγμα: Στον δακτύλιο $M_2(\mathbb{R})$ εδώ ο πίνακας: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ άρα ο $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ είναι αριστερός διαιρέτης του 0 ενώ ο $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ δεξιός διαιρέτης του 0.

Θεώρημα: Ισχύουν οι παρακάτω συνεπαγωγές



Απόδειξη:

(1) Κάθε σώμα είναι εξ' ορισμού ένας μεταθετικός δακτύλιος διαίρεσης

(4) Κάθε ακέραια περιοχή εξ' ορισμού είναι ένας μεταθετικός δακτύλιος χωρίς διαιρέτες του 0

(2) (Προς άτοπο)

Έστω R: δακτύλιος διαίρεσης και $a \neq 0$ ένας διαιρέτης του 0 στον R τότε $\exists\, 0 \neq b \in R : a \cdot b = 0$. Όμως αφού R δακτύλιος διαίρεσης και $a \neq 0$ με $a \in R \Rightarrow \exists\, a' \in R : a \cdot a' = 1_R$

Τότε $\begin{cases} a'(a \cdot b) = a' \cdot 0 \\ a'(a \cdot b) = (a' \cdot a) \cdot b = 1_R \cdot b = b \end{cases}$ Άρα $a' \cdot 0 = b$ $\Rightarrow b = 0$. (Άτοπο αφού υποθέσαμε $b \neq 0$)

Άρα, δεν υπάρχουν διαιρέτες του μηδέν.

(3) Όμοια με (2)

Παρατήρηση: (i) Η (3) δεν ανταποδείχνεται, αφού $\mathbb{Z}$ είναι ακέραια περιοχή αλλά όχι σώμα, αφού $U(\mathbb{Z}) = \{-1, 1\}$

(ii) Η (1) δεν ανταποδείχνεται, ο δακτύλιος των τετραγώνων του Hamilton $\mathbb{H}$ είναι δακτύλιος διαίρεσης αλλά όχι σώμα

Θεώρημα: Κάθε δακτύλιος R χωρίς διαιρέτες του μηδέν με πεπερασμένο πλήθος στοιχείων είναι δακτύλιος διαίρεσης

Απόδειξη: Έστω $a \in R$ και $a \neq 0$. Θα δείξω ότι $a \in U(R)$

Ορίζουμε την απεικόνιση $\varphi_a: R \to R$, $\varphi_a(x) = a \cdot x$

Η απεικόνιση φ_a είναι 1-1. Έστω ότι $\varphi_a(x) = \varphi_a(y)$

$\Rightarrow ax = ay \Rightarrow ax - ay = 0 \Rightarrow a(x-y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$

($a(x-y)=0$: αφού δεν υπάρχουν διαιρέτες του 0)

Επειδή, $|R| < +\infty$ και $\varphi_a: R \to R$ είναι 1-1 έπεται ότι φ_a: επί

Επειδή, η φ_a: επί $\Rightarrow \exists b \in R : \varphi_a(b) = 1_R \Rightarrow a \cdot b = 1_R$

Τότε $a(ba - 1_R) = a(ba) - a = (ab)a - a = 1_R \cdot a - a$
$= a - a = 0$.

Άρα, $a(ba - 1_R) = 0$. Όμως αφού $a \neq 0$ και ο R δεν έχει διαιρέτες του μηδέν $\Rightarrow ba - 1_R = 0 \Rightarrow ba = 1_R$

$\Rightarrow a \in U(R)$

Πόρισμα: Κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.

Πρόταση: Για κάθε $n \in \mathbb{N}$ τα παρακάτω είναι ισοδύναμα:

(1) $\mathbb{Z}_n$: σώμα

(2) $\mathbb{Z}_n$: ακέραια περιοχή

(3) n: πρώτος

Απόδειξη:

(1) $\Leftrightarrow$ (2): Προφανές από προηγούμενο θεώρημα και πόρισμα.

(1) $\Leftrightarrow$ (3): $\mathbb{Z}_n$: σώμα $\Leftrightarrow$ $U(\mathbb{Z}_n) = \mathbb{Z}_n^*$

Τότε $\varphi(n) = |U(\mathbb{Z}_n)| = |\mathbb{Z}_n^*| = n-1 \Leftrightarrow \varphi(n) = n-1$

$\Leftrightarrow$ n: πρώτος

Θεώρημα (Wedderburn 1905): Κάθε πεπερασμένος δακτύλιος διαίρεσης είναι μεταθετικός και άρα είναι σώμα.

$$H = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \in M_2(\mathbb{C}) \;\middle|\; z, w \in \mathbb{C} \right\} \leq M_2(\mathbb{C})$$

Το σύνολο H είναι έναν υποδακτύλιος του $M_2(\mathbb{C})$ δεν είναι μεταθετικός δακτύλιος διότι π.χ

$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in H$. Όμως $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$

Αν $A=\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \in H$ και $A \neq 0 \Rightarrow (z,w) \neq (0,0)$

Άρα $|A| = z\cdot\bar{z} + w\cdot\bar{w} = |z|^2 + |w|^2 \neq 0$

Άρα, ο A αντιστρέψιμος με $A^{-1} = \frac{1}{|z|^2+|w|^2}\begin{pmatrix} \bar{z} & -w \\ \bar{w} & z \end{pmatrix} \in H$

Επομένως, δείξαμε ότι το A είναι αντιστρέψιμο στοιχείο του H, άρα ο H είναι δακτύλιος διαίρεσης ο οποίος δεν είναι μεταθετικός.