Μορφισμοί Δακτυλίων

Ορισμός: Έστω $(R, +, \cdot)$ και $(S, \oplus, *)$ δύο προσεταιριστικοί δακτύλιοι με μονάδες 1_R και 1_S, αντίστοιχα. Μια απεικόνιση $f: R \to S$ λέγεται **μορφισμός δακτυλίων** αν (i) $f(x+y) = f(x) \oplus f(y)$, $\forall x, y \in R$.

(ii) $f(xy) = f(x) * f(y)$, $\forall x, y \in R$

(iii) $f(1_R) = 1_S$

▸ Ένας μορφισμός δακτυλίων $f: R \to S$ λέγεται

1. **μονομορφισμός**, αν η f είναι 1-1

2. **επιμορφισμός**, αν η f είναι επί

3. **ισομορφισμός**, αν η f είναι 1-1 και επί.

Ορισμός: Δύο προσεταιριστικοί δακτύλιοι με μονάδες, $(R,+,\cdot)$ και $(S,\oplus,*)$ λέγονται **ισόμορφοι** και γράφουμε $R \cong S$, αν υπάρχει ισομορφισμός δακτυλίων $f: R \to S$.

Πρόταση: Έστω $f: R \to S$ μορφισμός δακτυλίων. Αν $x, y, x_1, \dots, x_n \in R$ τότε

(α) $f(0_R) = 0_S$ (β) $f(x-y) = f(x) - f(y)$

(γ) $f(x_1 + \dots + x_n) = f(x_1) + \dots + f(x_n)$

(δ) $f(x_1 \cdots x_n) = f(x_1) \cdots f(x_n)$, $f(x^n) = (f(x))^n$, $\forall n \in \mathbb{N}_0$

(ε) Αν $x \in U(R)$, τότε $f(x) \in U(S)$ και

$$(f(x))^{-1} = f(x^{-1})$$

(στ) Αν T είναι δακτύλιος και $g: S \to T$ μορφισμός, τότε ο $g \circ f: R \to T$ είναι επίσης μορφισμός δακτυλίων.

(J) Αν $f: R \to S$ είναι ισομορφισμός τότε και η $f^{-1}: S \to R$ είναι ισομορφισμός δακτυλίων.

<u>Απόδειξη</u>: H/W

<u>Πρόταση</u>: Έστω $f: R \to S$ μορφισμός δακτυλίων. Τότε:

(α) $I \underset{\text{υποδακτ.}}{\subseteq} R \implies f(I) \underset{\text{υποδακτ.}}{\subseteq} S$

(β) $U \underset{\text{υποδακτ.}}{\subseteq} S \implies f^{-1}(U) \underset{\text{υποδακτ.}}{\subseteq} R$

<u>Απόδειξη</u>

(α) Έστω I: υποδακτύλιος του R και θα αποδείξουμε ότι $f(I)$: υποδακτύλιος του S. Επειδή $0_R \in I$ και $0_S = f(0_R)$ έπεται $0_S \in f(I)$. Έστω $a, b \in f(I)$. Τότε, υπάρχουν $x, y \in T$ ώστε $f(x) = a$ και $f(y) = b$.

Άρα: $a - b = f(x) - f(y) \xlongequal[\text{μορφ.}]{f:} f(x-y) \in f(T)$

(αφού: $x, y \in T$ και T: υποδακτύλιος του R $\Rightarrow x - y \in T$)

και $ab = f(x) f(y) \xlongequal[\text{μορφ.}]{f:} f(xy) \in f(T)$.

(διότι $x, y \in T$, T: υποδακτ. R $\Rightarrow xy \in T$).

Ώστε, ο $f(T)$ είναι υποδακτύλιος του S.

(β) Έστω U: υποδακτύλιος του S και θα αποδείξουμε ότι $f^{-1}(U)$: υποδακτύλιος του R. Επειδή $f(0_R) = 0_S \in U$ έπεται $0_R \in f^{-1}(U)$. Έστω $x, y \in f^{-1}(U)$. Τότε $f(x), f(y) \in U$ και εφ' όσον U: υποδακτύλιος του S προκύπτει:

- $f(x-y) = f(x) - f(y) \in U \Rightarrow x - y \in f^{-1}(U)$
- $f(xy) = f(x) f(y) \in U \Rightarrow xy \in f^{-1}(U)$

Ώστε, $f^{-1}(U)$: υποδακτύλιος του R. ∎

Ορισμός: Έστω $f: R \to S$ μορφισμός δακτυλίων.

(1) Το υποσύνολο $Ker(f) = f^{-1}(\{0_S\})$
$= \{r \in R \mid f(r) = 0_S\} \subseteq R$

λέγεται <u>πυρήνας του μορφισμού f.</u>

(2) Το υποσύνολο $f(R) = Im(f) = \{f(x) \in S \mid x \in R\} \subseteq S$

λέγεται <u>εικόνα του μορφισμού f.</u>

Σχόλιο: Σύμφωνα με την προηγούμενη Πρόταση, αν $f: R \to S$ είναι μορφισμός δακτυλίων τότε

(α) $Ker(f) = f^{-1}(\{0_S\})$: υποδακτύλιος του R.
(διότι: $\{0_S\}$: υποδακτύλιος του S)

(β) $Im(f) = f(R)$: υποδακτύλιος του S.
(διότι: R: υποδακτύλιος του R)

Παραδείγματα Μορφισμών Δακτυλίων

(1) Αν R, S είναι δύο δακτύλιοι τότε ο $f: R \to S$ με $f(x) = 0_S, \forall x \in R$ δεν είναι μορφισμός διότι $f(1_R) = 0_S \neq 1_S$. Αν στον ορισμό των μορφισμών δακτυλίων δεν απαιτήσουμε τη συνθήκη $f(1_R) = 1_S$, τότε η παραπάνω απεικόνιση είναι μορφισμός και λέγεται τετριμμένος μορφισμός από τον R στον S. Ωστόσο, εμείς συνεχίζουμε κανονικά με την συνθήκη $f(1_R) = 1_S$.

(2) Για κάθε δακτύλιο R, η ταυτοτική απεικόνιση $Id_R : R \to R$, $Id_R(x) = x$ είναι ισομορφισμός.

(3) Αν T υποδακτύλιος του δακτυλίου R με $1_R \in T$ τότε η απεικόνιση κανονικής έγκλεισης $i: T \to R$, $i(x) = x$ είναι μονομορφισμός.

(4) Για κάθε δακτύλιο R, η απεικόνιση $\varphi: \mathbb{Z} \to R$ με $\varphi(n) = n \cdot 1_R$ είναι μορφισμός:

- $\varphi(n+m) = (n+m) \cdot 1_R = n \cdot 1_R + m \cdot 1_R = \varphi(n) + \varphi(m), \forall n, m \in \mathbb{Z}$
- $\varphi(nm) = (nm) \cdot 1_R = (n 1_R)(m 1_R) = \varphi(n)\varphi(m), \forall n, m \in \mathbb{Z}$
- $\varphi(1) = 1 \cdot 1_R = 1_R$

(5) Έστω $n \in \mathbb{N}$: Η απεικόνιση $\pi: \mathbb{Z} \to \mathbb{Z}_n$ με $\pi(x) = [x]_n$ είναι επιμορφισμός. Πράγματι:

- $\pi(x+y) = [x+y]_n = [x]_n + [y]_n = \pi(x) + \pi(y), \forall x, y \in \mathbb{Z}$
- $\pi(xy) = [xy]_n = [x]_n [y]_n = \pi(x)\pi(y), \forall x, y \in \mathbb{Z}$
- $\pi(1) = [1]_n = 1_{\mathbb{Z}_n}$.

Επίσης, π: επί του $\mathbb{Z}_n$: Έστω $\alpha \in \mathbb{Z}_n$. Τότε $\alpha = [x]_n$ για κάποιο $x \in \mathbb{Z}$ και

$$\pi(x) = [x]_n = \alpha.$$

(6) (sos) Έστω $n, m \in \mathbb{N}$ με $(n,m)=1$.

Ορίζουμε $f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ από τη σχέση $f([x]_{mn}) = ([x]_m, [x]_n)$

<u>Βήμα 1</u>: Η f είναι καλά ορισμένη: Έστω $[x]_{mn} = [y]_{mn}$ και θα αποδείξουμε $f([x]_{mn}) = f([y]_{mn})$.

Επειδή $[x]_{mn} = [y]_{mn}$ έπεται: $mn \mid x-y$.

$$\left.\begin{array}{l} \cdot\ m \mid mn \\ \cdot\ mn \mid x-y \end{array}\right\} \Rightarrow m \mid x-y \Rightarrow [x]_m = [y]_m \quad (i)$$

$$\left.\begin{array}{l} \cdot\ n \mid mn \\ mn \mid x-y \end{array}\right\} \to n \mid x-y \Rightarrow [x]_n = [y]_n \quad (ii)$$

Από (i) και (ii): $([x]_m, [x]_n) = ([y]_m, [y]_n)$

$\Rightarrow f([x]_{mn}) = f([y]_{mn})$, όπως θέλαμε.

<u>Βήμα 2</u>: Η f είναι μορφισμός δακτυλίων:

Πράγματι, για κάθε $[x]_{mn}, [y]_{mn} \in \mathbb{Z}_{mn}$ έχουμε:

- $f([x]_{mn}+[y]_{mn}) = f([x+y]_{mn}) = ([x+y]_m, [x+y]_n)$

$= ([x]_m+[y]_m, [x]_n+[y]_n) =$

$= ([x]_m, [x]_n) + ([y]_m, [y]_n) = f([x]_{mn}) + f([y]_{mn})$

- $f([x]_{mn}\cdot[y]_{mn}) = f([xy]_{mn}) = ([xy]_m, [xy]_n) =$

$= ([x]_m[y]_m, [x]_n[y]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) =$

$= f([x]_{mn}) f([y]_{mn})$

- Τέλος, $f(1_{\mathbb{Z}_{mn}}) = f([1]_{mn}) = ([1]_m, [1]_n)$

$= 1_{\mathbb{Z}_m \times \mathbb{Z}_n}$.

Βήμα 3: Η f είναι 1-1: Έστω $f([x]_{mn}) = f([y]_{mn})$ και θα δείξουμε ότι $[x]_{mn} = [y]_{mn}$. Πράγματι, $f([x]_{mn}) = f([y]_{mn})$

$\Rightarrow ([x]_m, [x]_n) = ([y]_m, [y]_n) \Rightarrow \begin{cases} [x]_m = [y]_m \\ \text{και} \\ [x]_n = [y]_n \end{cases}$

$\Rightarrow m \mid x-y$ και $n \mid x-y$, άρα:

$[m,n] \mid x-y$. Επειδή (ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ)

$mn = [m,n](m,n)$ και $(m,n) = 1$ έπεται:

$mn = [m,n] \Longrightarrow mn \mid x-y \Rightarrow [x]_{mn} = [y]_{mn}$,

όπως θέλαμε.

Βήμα 4: Η f είναι επί: Εφ' όσον f: 1-1

και $|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m||\mathbb{Z}_n| = |\mathbb{Z}_m \times \mathbb{Z}_n|$,

έπεται f: επί.

Ώστε, f: ισομορφισμός δακτυλίων. και

άρα $\boxed{\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n, \quad (m,n) = 1}$

(7) Για $n \in \mathbb{N}$ και R: δακτύλιο, η απεικόνιση

$f: R \longrightarrow \mathbb{M}_n(R)$ με $f(r) = \begin{bmatrix} r & & & 0 \\ & r & & \\ & & \ddots & \\ 0 & & & r \end{bmatrix} := rI_n$

είναι προφανώς μονομορφισμός δακτυλίων.

<u>Πρόταση</u>: Έστω $f: R \to S$ μορφισμός δακτυλίων. Τότε:

(i) f: μονομορφισμός $\Longleftrightarrow$ $Ker(f) = \{0_R\}$

(ii) f: επιμορφισμός $\Longleftrightarrow$ $Im(f) = S$

<u>Απόδειξη</u>

(i) "$\Rightarrow$" Έστω f: μονομορφισμός, δηλαδή η f είναι 1-1, και θα δείξουμε ότι $Ker(f) = \{0_R\}$.

Επειδή $\{0_R\} \subseteq Ker(f)$ [αφού $f(0_R) = 0_S$], αρκεί να δείξουμε ότι $Ker(f) \subseteq \{0_R\}$. Έστω λοιπόν $r \in Ker(f)$. Άρα, $f(r) = 0_S \Rightarrow f(r) = f(0_R)$

$$\xrightarrow[1-1]{f:} r = 0_R \in \{0_R\}.$$

Τελικά, $Ker(f) = \{0_R\}$.

"$\Leftarrow$" Έστω $Ker(f) = \{0_R\}$ και θα δείξουμε ότι f: 1-1. Ας είναι $r, s \in R$ με $f(r) = f(s)$ και θα δείξουμε ότι: $r = s$. Πράγματι,

$$f(r)=f(s) \Rightarrow f(r)-f(s)=0_S \xrightarrow[\text{μορφ.}]{f:} f(r-s)=0_S$$

$$\Rightarrow r-s \in Ker(f)=\{0_R\} \Rightarrow r-s=0_R \Rightarrow r=s,$$

όπως θέλαμε.

(ii) f: επιμορφισμός $\Longleftrightarrow$ f: επί του S $\Longleftrightarrow$ $Im(f)=S$ ∎

<u>Σχόλιο - Ιδέα</u>: Έστω $f: R \to S$ ένας μορφισμός δακτυλίων. Όπως είδαμε, ο πυρήνας $Ker(f)$ της f είναι υποδακτύλιος του R.

Ο $Ker(f)$ έχει μια επιπλέον ιδιότητα:

$$\forall x \in Ker(f),\ \forall r \in R,\quad xr,\ rx \in Ker(f).$$

Πράγματι, για κάθε $x \in Ker(f)$ και $r \in R$ έχουμε:

- $f(xr) \overset{f:}{\underset{\text{μορφ.}}{=\!=}} f(x)f(r) \overset{x \in Ker(f)}{=\!=} 0_R \cdot f(r) = 0_S$
- $f(rx) \overset{f:}{\underset{\text{μορφ.}}{=\!=}} f(r)f(x) \overset{x \in Ker(f)}{=\!=} f(r)\cdot 0_S = 0_S$

άρα, $xr,\ rx \in Ker(f)$.

Από την άλλη, αν $y \in Im(f)$ και $s \in S$ τότε δεν ισχύει απαραίτητα ότι $ys, sy \in Im(f)$.

__Π.χ.__: Έστω R ένας δακτύλιος και ο μορφισμός $f: R \to \mathbb{M}_2(R)$ με $f(r) = \begin{bmatrix} r & 0_R \\ 0_R & r \end{bmatrix}$.

Αν $\begin{bmatrix} r & 0_R \\ 0_R & r \end{bmatrix} \in Im(f)$ και $S = \begin{bmatrix} s_{11} & s_{12} \\ s_{21} & s_{21} \end{bmatrix} \in \mathbb{M}_2(R)$

τότε: $\begin{bmatrix} r & 0_R \\ 0_R & r \end{bmatrix}\begin{bmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{bmatrix} = \begin{bmatrix} rs_{11} & rs_{12} \\ rs_{21} & rs_{22} \end{bmatrix}$ το οποίο, εν γένει, δεν ανήκει στην $Im(f)$.

Για την $Im(f)$ η κατάσταση διορθώνεται αν ο f είναι επιμορφισμός.

Από τα παραπάνω οδηγούμαστε φυσιολογικά στην έννοια του ιδεώδους ενός δακτυλίου.

Ακολουθεί ο ορισμός:

Από εδώ και στο εξής: Έστω $R=(R,+,\cdot)$ ένας προσεταιριστικός δακτύλιος με μονάδα 1_R.

Ορισμός: Ένα μη-κενό υποσύνολο I του R λέγεται ιδεώδες του R αν

(α) $I \leq (R,+)$ και (β) $rx, xr \in I$, $\forall x \in I$ $\forall r \in R$

και γράφουμε τότε $I \trianglelefteq R$.

Σχόλιο: Αν $I \leq (R,+)$ και ισχύει μόνο $rx \in I$, $\forall r \in R$, $\forall x \in I$, τότε το I λέγεται αριστερό ιδεώδες του R. Ανάλογα, αν $I \leq (R,+)$ και ισχύει μόνο $xr \in I$, $\forall x \in I$, $\forall r \in R$, τότε το I λέγεται δεξιό ιδεώδες του R.

Προφανώς, αν ο R είναι μεταθετικός τότε οι έννοιες αριστερό ιδεώδες, δεξιό ιδεώδες και ιδεώδες ταυτίζονται.

Έτσι, ένα μη-κενό υποσύνολο I του R είναι (α) αριστερό ιδεώδες (β) δεξιό ιδεώδες (γ) ιδεώδες

αν για κάθε $r \in R$ και $x, y \in I$ ισχύουν:

1. $0_R \in I$, $x - y \in I$
2. (α) $rx \in I$ (β) $xr \in I$ (γ) $rx, xr \in I$.

Παρατήρηση: I: ιδεώδες $\underset{\not\Leftarrow}{\Rightarrow}$ I: υποδακτύλιος

! Ο R έχει πάντα δύο ιδεώδη: το $\{0\}$: μηδενικό ιδεώδες και τον ίδιο τον R. Ένα ιδεώδες I του R λέγεται γνήσιο αν $I \neq R$. Ο R λέγεται απλός δακτύλιος αν τα μόνα ιδεώδη του είναι ο R και το $\{0\}$. Απ' την άλλη, ένας μη-μεταθετικός δακτύλιος R έχει σχεδόν πάντα, ακόμα και αν είναι απλός, πολύ περισσότερα αριστερά ή δεξιά ιδεώδη. Τα ιδεώδη R και $\{0\}$ λέγονται <u>τετριμμένα ιδεώδη του R</u>. Κάθε άλλο ιδεώδες λέγεται <u>μη-τετριμμένο</u>.

<u>Πρόταση</u>: Έστω I ένα (αριστερό ή δεξιό) ιδεώδες του δακτυλίου R.

(1) $I = R \iff 1_R \in I \iff I \cap U(R) \neq \emptyset$

(2) Αν ο R είναι δακτύλιος διαίρεσης τότε $I = R$ ή $I = \{0\}$.

(3) Κάθε δακτύλιος διαίρεσης, ιδιαίτερα κάθε σώμα, είναι απλός δακτύλιος.

Απόδειξη

(1) $I = R \Rightarrow 1_R \in I$: Προφανές.

$1_R \in I \Rightarrow I \cap U(R) \neq \emptyset$: Πράγματι, αν $1_R \in I$ τότε επειδή ταυτόχρονα $1_R \in U(R)$ θα έχουμε
$$1_R \in I \cap U(R) \Rightarrow I \cap U(R) \neq \emptyset.$$

$I \cap U(R) \neq \emptyset \Rightarrow I = R$: Επειδή $I \subseteq R$ αρκεί να δείξουμε ότι $R \subseteq I$. Έστω λοιπόν $r \in R$. Αφού $I \cap U(R) \neq \emptyset$, επιλέγουμε $x \in I \cap U(R)$, άρα $x \in I$ και $x \in U(R)$, οπότε: $x x^{-1} = 1_R = x^{-1} x$.

Έτσι: $r = 1_R \cdot r = \underset{I}{\underset{\cap}{x}}\, \underset{R}{\underset{\cap}{x^{-1} r}} \in I$ (αν I: αριστερό)

$r = r \cdot 1_R = \underset{R}{\underset{\cap}{r x^{-1}}}\, \underset{I}{\underset{\cap}{x}} \in I$ (αν I: δεξιό)

και ανάλογα, αν I: ιδεώδες. Ώστε $R \subseteq I$, όπως θέλαμε.

(2) Έστω R: δακτύλιος διαιρέσεως. Αν $I = \{0\}$ τότε οκ. Αν $I \neq \{0\}$ τότε

$I \cap U(R) = I \cap R^* = I \setminus \{0\} \neq \emptyset$

Λόγω (1), $I = R$

(3) Συνέπεια του (2)

$\blacksquare$

Συμπέρασμα: Οι δακτύλιοι $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ και $\mathbb{H}$ είναι απλοί δακτύλιοι. Από την άλλη:

Λήμμα: Ο δακτύλιος $\mathbb{Z}$ των ακεραίων δεν είναι απλός δακτύλιος

Απόδειξη: Πράγματι, για κάθε $n \in \mathbb{N}_0$ το $I = n\mathbb{Z}$ είναι ιδεώδες του $\mathbb{Z}$. Έχουμε δεί ότι $I \leq (\mathbb{Z}, +)$ και για κάθε $x \in \mathbb{Z}$ και $nk \in I$ ισχύει: $x(nk) = n(xk) = (nk)x \in I$.

Αντίστροφα, αν I ιδεώδες του $\mathbb{Z}$ τότε επειδή $I \leq (\mathbb{Z}, +)$ έχουμε από θεωρία ομάδων ότι $I = n\mathbb{Z}$ για κάποιο $n \in \mathbb{N}_0$. ∎

Αντίστοιχα, για $n \in \mathbb{N}$, τα ιδεώδη του μεταθετικού δακτυλίου $\mathbb{Z}_n$ είναι τα

$$H_d = \langle d[m]_n \rangle, \text{ όπου } d = (n, m), \ \forall m = 0, 1, \dots, n-1.$$

Διαφοροποίηση Ιδεωδών από Υποδακτυλίους

Έστω ο δακτύλιος $R = \mathbb{M}_2(\mathbb{R})$ και έστω

$$I = \left\{ \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \in \mathbb{M}_2(\mathbb{R}) \;\middle|\; x \in \mathbb{R} \right\} \subseteq \mathbb{M}_2(\mathbb{R}).$$

- Προφανώς, $\mathbb{O} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in I$ και για κάθε

$X = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}, \; Y = \begin{bmatrix} y & 0 \\ 0 & 0 \end{bmatrix} \in I$ έχουμε:

$$X - Y = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} y & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x-y & 0 \\ 0 & 0 \end{bmatrix} \in I$$

$$XY = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} y & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} xy & 0 \\ 0 & 0 \end{bmatrix} \in I.$$

Άρα I: υποδακτύλιος του R με $I_2 \notin I$.

[Θυμήσου ότι το I έχει μονάδα τον πίνακα $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq I_2$]

$\rightarrow$ (ούτε αριστερό, ούτε δεξιό)

Ωστόσο I: όχι ιδεώδες του R διότι:

για το $X = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I$ και $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in R$

έχουμε $AX = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \notin I$, $XA = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \notin I$.

■

! Έστω $R=(R,+,\cdot)$ προσεταιριστικός δακτύλιος με μονάδα 1_R, και έστω $r\in R$. Θέτουμε

$$Rr := \{xr\in R \mid x\in R\}\subseteq R$$

$$rR := \{ry\in R \mid y\in R\}\subseteq R$$

<u>Ισχυρισμός</u>: Το Rr (αντ. rR) είναι το μικρότερο αριστερό ιδεώδες του R (αντ. δεξιό ιδεώδες του R) το οποίο περιέχει το r.

<u>Απόδειξη</u>: Αρχικά, $0_R = 0_R\cdot r\in Rr$ και $r = 1_R\cdot r\in Rr$. Έστω τώρα $xr, yr\in Rr$ και έστω $a\in R$. Τότε:

- $xr - yr = (x-y)r\in Rr$
- $a(xr) = (ax)r\in Rr$

Άρα, το Rr είναι αριστερό ιδεώδες του R.

Έστω τώρα I αριστερό ιδεώδες του R με $r\in I$ και θα αποδείξουμε ότι $Rr\subseteq I$.

Έστω $xr \in Rr$. Επειδή $x \in R$, $r \in I$ και I: αριστερό ιδεώδες του R προκύπτει $xr \in I$. ∎

Το $RrR = \left\{ \sum_{i=1}^{n} x_i r y_i \in R \mid x_i, y_i \in R,\ i=1,\dots,n,\ n \in \mathbb{N} \right\}$

είναι το μικρότερο ιδεώδες του R που περιέχει το r.

<u>Παρατήρηση</u>: Αν ο R είναι μεταθετικός τότε: $\forall r \in R$: $Rr = rR = RrR$ και θα γράφουμε τότε $Rr = \langle r \rangle \trianglelefteq R$.

<u>Ορισμός</u>: Αν $r \in R$ τότε:

(i) το Rr λέγεται το <u>αριστερό ιδεώδες του R που παράγεται από το r</u>.

(ii) το rR λέγεται το <u>δεξιό ιδεώδες του R που παράγεται από το r</u>.

(iii) το RrR λέγεται το <u>ιδεώδες του R που παράγεται από το r</u>.

Πρόταση: Η τομή μιας οικογένειας (αριστερών, αντίστοιχα δεξιών) ιδεωδών ενός δακτυλίου R είναι (αριστερό, αντίστοιχα δεξιό) ιδεώδες του R.

Απόδειξη: H/W

Ορισμός: Ένα ιδεώδες I ενός δακτυλίου R λέγεται κύριο ιδεώδες, αν υπάρχει $r \in R$ ώστε $I = \langle r \rangle = RrR$.

- Ανάλογα, το I λέγεται αριστερό (δεξιό) κύριο ιδεώδες αν $I = Rr$ (rR) για κάποιο $r \in R$.

Πρόταση: Για ένα δακτύλιο R τα ακόλουθα ισοδυναμούν:

(1) R: δακτύλιος διαίρεσης

(2) Τα μόνα αριστερά (ή δεξιά) ιδεώδη του R είναι τα $\{0_R\}$ και R.

<u>Απόδειξη</u>: (1) $\Rightarrow$ (2) Έχει αποδειχθεί.

(2) $\Rightarrow$ (1) Υποθέτουμε ότι ο R έχει ως μοναδικά αριστερά ιδεώδη τα $\{0_R\}$ και R. Θα αποδείξουμε ότι ο R είναι δακτύλιος διαίρεσης, δηλαδή ότι κάθε μη-μηδενικό στοιχείο του αντιστρέφεται. Πράγματι, έστω $r \in R$, $r \neq 0_R$. Τότε το $I = Rr$ είναι αριστερό ιδεώδες του R. Λόγω υπόθεσης, $Rr = \{0_R\}$ ή $Rr = R$. Επειδή $r \in Rr$ και $r \neq 0_R$, έπεται $Rr \neq \{0_R\}$ και έτσι $Rr = R$. Άρα, $1_R \in R \Rightarrow 1_R \in Rr \Rightarrow$
$\Rightarrow \exists\, s \in R : sr = 1_R$. Προφανώς $s \neq 0_R$ διότι διαφορετικά θα είχαμε $0_R = 1_R$, άτοπο.
Θεωρούμε τώρα το κύριο αριστερό ιδεώδες $J = Rs$ και επειδή $s \neq 0_R$, όπως πριν, $J \neq \{0_R\}$. Λόγω υπόθεσης, $J = Rs = R$.

$1_R \in R \Rightarrow 1_R \in Rs \Rightarrow \exists t \in R : 1_R = ts.$

Τότε: $t = t \cdot 1_R = t \cdot (sr) = (ts)r = 1_R \cdot r = r$

και συνεπώς: $rs = 1_R = sr$, που σημαίνει

ότι r: αντιστρέψιμο, όπως θέλαμε. ∎

<u>Πρόταση</u>: (Χωρίς απόδειξη) Έστω R ένας δακτύλιος διαίρεσης και έστω $n \in \mathbb{N}$. Τότε ο $\mathbb{M}_n(R)$ είναι απλός δακτύλιος, δηλαδή τα μόνα τα ιδεώδη είναι τα $\{0\}$ και $\mathbb{M}_n(R)$.

! Όπως είδαμε, η τομή ιδεωδών είναι ιδεώδες. Η ένωση ιδεωδών ωστόσο δεν είναι πάντα ιδεώδες.

Πώς "διορθώνεται" αυτό;

Πρόταση: Έστω R ένας δακτύλιος και I, J δύο (αριστερά, δεξιά) ιδεώδη του R. Τότε το $I+J := \{ x+y \in R \mid x \in I, y \in J \}$ είναι (αριστερό, δεξιό) ιδεώδες του R και μάλιστα είναι το μικρότερο ιδεώδες του R που περιέχει το $I \cup J$.

Απόδειξη: $0_R = 0_R + 0_R \in I+J$ διότι $0_R \in I$ και $0_R \in J$, αφού I, J: ιδεώδη του R.

Έστω τώρα $u, v \in I+J$ και $r \in R$ και θα δείξουμε ότι: $u-v \in I+J$ και $ru, ur \in I+J$.

- $u \in I+J \Rightarrow \exists x_1 \in I, \exists y_1 \in J : u = x_1 + y_1$
- $v \in I+J \Rightarrow \exists x_2 \in I, \exists y_2 \in J : v = x_2 + y_2$

Τότε: $u - v = x_1 + y_1 - x_2 - y_2 = (x_1 - x_2) + (y_1 - y_2)$

με $x_1 - x_2 \in I$ (διότι $x_1, x_2 \in I$ και $I \leq (R,+)$)

$y_1 - y_2 \in J$ (διότι $y_1, y_2 \in J$ και $J \leq (R,+)$)

άρα $u - v \in I+J$.

· $ru = r(x_1+y_1) = rx_1 + ry_1$ με $rx_1 \in I$ (αφού $r \in R$, $x_1 \in I$ και I: ιδεώδες του R) και $ry_1 \in J$ (διότι $r \in R$, $y_1 \in J$ και J: ιδεώδες του R). Ώστε $ru \in J+J$.

Ανάλογα, $ur = x_1 r + y_1 r \in I+J$.

Επομένως, το $I+J$ είναι ιδεώδες του R. Έστω $z \in I \cup J$. Τότε $z \in I$ ή $z \in J$.

· Αν $z \in I$ τότε: $z = \underset{\underset{I}{\cap}}{z} + \underset{\underset{J}{\cap}}{0_R} \in I+J$

· Αν $z \in J$ τότε $z = \underset{\underset{I}{\cap}}{0_R} + \underset{\underset{J}{\cap}}{z} \in I+J$

Σε κάθε περίπτωση, $z \in I+J$ και άρα $I \cup J \subseteq I+J$. Έστω τέλος ένα ιδεώδες K του R με $I \cup J \subseteq K$ και θα αποδείξουμε ότι $I+J \subseteq K$. Πράγματι, έστω $u \in I+J$. Τότε $u = x+y$ με $x \in J$ και $y \in J$.

• $x \in I \Rightarrow x \in I \cup J \Rightarrow x \in K$.

• $y \in J \Rightarrow y \in I \cup J \Rightarrow y \in K$

Άρα: $\left.\begin{array}{l} x, y \in K \\ K \leq (R,+) \end{array}\right\} \Rightarrow x+y \in K \Rightarrow u \in K$.

Επομένως, $I+J \subseteq K$, όπως θέλαμε. ∎

<u>**Ορισμός**</u>: Το $I+J$ λέγεται <u>άθροισμα των ιδεωδών I και J</u>. Αν επιπλέον $I \cap J = \{0_R\}$

τότε γράφουμε $I \oplus J$

↑ ευθύ άθροισμα των ιδεωδών I και J.