▸ $\mathbb{Z}_u$: $[\alpha]_u$: αντιστρέψιμο στοιχείο

$[\alpha]_u$: μονάδα $\iff$ μκδ$(\alpha, u) = 1$

$[\alpha]_u$: διαιρέτης του μηδενός $\iff$ μκδ$(\alpha, u) = d$

με $d \neq 1$ & $d \neq u$

▸ Ορισμός $S \subseteq R$ ονομάζεται υποδακτύλιος του δακτυλίου $(R, +, \cdot)$, αν:

(i) Το S είναι δακτύλιος με τις ίδιες πράξεις $(S, +, \cdot)$

▸ Υποδακτύλιος $\Rightarrow$ S υποομάδα της αβελιανής $(R, +)$

- $0 \in S \Rightarrow \boxed{S \neq \emptyset}$
- Αν $\alpha, b \in S \Rightarrow \boxed{\alpha - b \in S}$

(ii) Αν $\alpha, b \in S \Rightarrow \boxed{\alpha \cdot b \in S}$ → κλειστότητα της πράξης του πολλαπλασιασμού

▶ **Ορισμός**: Ένα $S \subseteq R$ είναι υποδακτύλιος, αν:

i) $0 \in S \Rightarrow \boxed{S \neq \emptyset}$

ii) Αν $a, b \in S \Rightarrow a - b \in S$

iii) Αν $a, b \in S \Rightarrow a \cdot b \in S$ & $b \cdot a \in S$

$\boxed{(S,+) \leq (R,+)}$ + κλειστότητα!!!

▶ **Άσκηση**: Βρείτε όλους τους υποδακτύλιους του $(\mathbb{Z},+,\cdot)$

▶ **Λύση**: Έστω S υποδακτύλιος του $\mathbb{Z}$. Τότε:

$\boxed{S \subseteq \mathbb{Z}}$ και S υποομάδα του $\boxed{\mathbb{Z} = \langle 1 \rangle}$

• Όμως, το $\mathbb{Z}$ είναι κυκλική, άρα κάθε υποομάδα του είναι κυκλική.

$\Rightarrow \boxed{S = \langle \nu \rangle}\ \forall \nu \in \mathbb{Z}$

• Θα αποδείξουμε ότι το S είναι υποδακτύλιος του R:

(i) $0 = \nu \cdot 0 \in \langle \nu \rangle \Rightarrow \boxed{S \neq \emptyset}$

(ii) Έστω $a, \beta \in \langle \nu \rangle \Rightarrow a = \nu \cdot k$ & $\beta = \nu \cdot \lambda$

$\Rightarrow a - \beta = \nu(k - \lambda) \in \langle \nu \rangle$

(iii) Πράγματι $a \cdot b \in S \Rightarrow \nu k \cdot \nu \lambda = \nu(k \nu \lambda) \in \langle \nu \rangle$

• Άρα, κάθε υποδακτύλιος S του $(\mathbb{Z},+,\cdot)$, είναι της μορφής: $S = \langle \nu \rangle$, για $\nu \in \mathbb{Z}$

Θεώρημα: Κάθε σώμα είναι ακέραια περιοχή!

▶ **Απόδειξη:**

$$F: \text{σώμα} \longrightarrow \begin{cases} (i)\ F \text{ δακτύλιος με μοναδιαίο στοιχείο} \\ (ii)\ F \text{ δακτύλιος διαιρέσεως} \\ (iii)\ F \text{ αντιμεταθετικός} \end{cases}$$

• Έστω ότι το F έχει διαιρέτες του μηδενός. Θα καταλήξω σε άτοπο!

• Έχουμε, λοιπόν, ότι:

$(\exists\, a\neq 0,\ b\neq 0)$ τ/ω: $\boxed{a\cdot b=0}$

• Όμως: $a\neq 0,\ a\in F \Rightarrow a$: αντιστρέψιμο $\Rightarrow$

$\Rightarrow (\exists\, a^{-1}\in F)$ τ/ω: $\boxed{a^{-1}\cdot a=1}$

~~Άρα~~:

• Άρα: $a\cdot b=0 \Rightarrow a^{-1}\cdot a\cdot b=a^{-1}\cdot 0 \Rightarrow$

$\Rightarrow 1_F\cdot b=0 \Rightarrow \boxed{b=0}$ Άτοπο!!

• Άρα F ακέραια περιοχή!!!

⚠ Δεν ισχύει το αντίστροφο!!!

$(\mathbb{Z},+,\cdot)$ ακέραια περιοχή $\Longrightarrow$ όχι σώμα!!!

Αντιστρέψιμα μόνο τα ± 1

$\boxed{\blacktriangleright \text{Θεώρημα}}$ Το $\mathbb{Z}_n$ είναι σώμα $\iff$ n: πρώτος

▸ **Απόδειξη** $(\Leftarrow)$ $n = p$: πρώτος

• Τότε: $\mathbb{Z}_p$ είναι αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο, το:

$$\boxed{[1]_p \text{ και } [1]_p \neq [0]_p}$$

• Έστω: $[\alpha]_p \neq [0]_p \Rightarrow \boxed{\text{μκδ}(\alpha, p) = 1 \text{ ή } p}$.

• Έστω ότι $\text{μκδ}(\alpha, p) = p \Rightarrow p \mid \alpha \Rightarrow \alpha = k \cdot p$

$$\Rightarrow [\alpha]_p = [k \cdot p]_p = [0]_p \quad \text{Άτοπο!!!}$$

• Άρα: $\text{μκδ}(\alpha, p) = 1 \Rightarrow 1 = \lambda\alpha + \mu \cdot p \Rightarrow$

$$\Rightarrow [1]_p = [\lambda\alpha]_p + \cancel{[\mu p]_p}^{0} \Rightarrow \boxed{[\alpha]_p^{-1} = [\lambda]_p}$$

$\Rightarrow \alpha$: αντιστρέψιμο (με μονάδα)

$\Rightarrow \mathbb{Z}_n$: δακτύλιος διαίρεσης, αντιμεταθετικός!!!

$$\Rightarrow \boxed{\mathbb{Z}_n : \text{σώμα}}$$

$(\Rightarrow)$ $\mathbb{Z}_n$: σώμα $\Rightarrow [1]_n \neq [0]_n \Rightarrow \boxed{n \neq 1}$

Ισχυριζόμαστε ότι n: πρώτος, αφού $n \neq 1 \Rightarrow n$: σύνθετος.

$\Rightarrow \boxed{n = k \cdot \lambda}$ και $\begin{cases} 1 < k < n \\ 1 < \lambda < n \end{cases} \Longrightarrow$

$\Longrightarrow [\kappa\lambda]_\mu = [\mu]_\mu = \underline{[0]_\mu}$, όπου

$\begin{cases} [\kappa]_\mu \neq [0]_\mu \\ [\lambda]_\mu \neq [0]_\mu \end{cases} \Longrightarrow [\kappa]_\mu, [\lambda]_\mu$ διαιρέτες του μηδενός.

$\Longrightarrow \mathbb{Z}_\mu$ δεν είναι ακέραια περιοχή!!! Άτοπο!

Άρα $\boxed{\mu : \text{πρώτος}}$

▶ Ορισμός Έστω R και R' δύο δακτύλιοι. Μια απεικόνιση $\varphi : R \longrightarrow R'$ ονομάζεται ομομορφισμός δακτυλίων, αν:

$$\boxed{\varphi(a+b) = \varphi(a) + \varphi(b)}$$

και $\boxed{\varphi(a b) = \varphi(a) \cdot \varphi(b)}$, $\forall a, b \in R$

▶ Ορισμός
- Ένας ομομορφισμός φ ονομάζεται μονομορφισμός, αν είναι 1-1.
- Ένας ομομορφισμός φ ονομάζεται επιμορφισμός, αν η φ είναι επί.
- Ένας ομομορφισμός φ ονομάζεται ισομορφισμός, αν η φ είναι 1-1 & επί.

Δ $\mathbb{Z} \xrightarrow{f} \mathbb{Z}$, με $f(\alpha) = 2\alpha$

• $f(\alpha+b) = 2(\alpha+b) = 2\alpha+2b = f(\alpha)+f(b)$

• $f(\alpha b) = 2\alpha b \neq 2\alpha \cdot 2b = f(\alpha)\cdot f(b)$

→ Άρα η f είναι ομομορφισμός ομάδων, αλλά όχι δακτυλίων!!!

Θεώρημα Έστω $\varphi: R \to R'$ ομομορφισμός δακτυλίων.

(i) $\boxed{\varphi(0) = 0'}$ & $\boxed{\varphi(-\alpha) = -\varphi(\alpha)}$

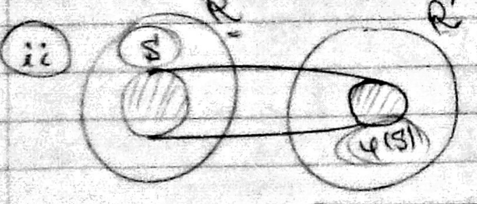
(ii) S υποδακτύλιος του R $\Rightarrow$ $\varphi(S)$ υποδακτύλιος του R'

(iii) S' υποδακτύλιος του R' $\Rightarrow$ $\varphi^{-1}(S')$ υποδακτύλιος του R

Απόδειξη: (i) φ: ομομορφισμός δακτυλίων $\Rightarrow$

$\Rightarrow$ φ: ομομορφισμός ομάδων $\Rightarrow$ $\varphi(0) = 0'$ & $\varphi(-\alpha) = -\varphi(\alpha)$

(ii)



• φ: ομομορφισμός δακτυλίων

$\Rightarrow$ φ: ομομορφισμός ομάδων

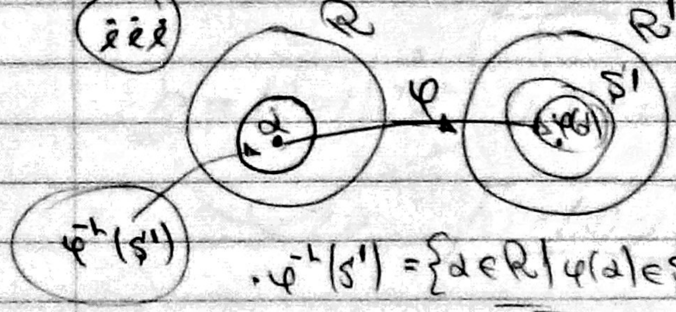
$\Rightarrow S \leq R \Rightarrow \boxed{\varphi(S) \leq R'}$ ($\varphi(S)$: αβελιανή ομάδα, καθώς R': αβελιανή)

• Έστω $x, y \in \varphi(S) \Rightarrow \begin{cases} x = \varphi(\alpha), & \alpha \in S \\ y = \varphi(b), & b \in S \end{cases} \Rightarrow$

Άρα : $x\cdot y = \varphi(a)\cdot\varphi(b) \overset{\varphi:\text{ ομομορφ.}}{=} \varphi(a\cdot b) \in \varphi(S)$

- Συνεπώς : $\left.\begin{cases} \boxed{\varphi(S) \leq R'} \\ \text{Για } x, y \in \varphi(S) \\ \Rightarrow x\cdot y \in \varphi(S) \end{cases}\right\} \Rightarrow \varphi(S)$ υποδακτύλιος του R'

iii)



$\cdot\ \varphi^{-1}(S') = \{a \in R \mid \varphi(a) \in S'\}$

- φ : ομομορφισμός δακτυλίων $\Rightarrow \varphi$: ομομορφισμός ομάδων

$\Rightarrow \boxed{\varphi^{-1}(S') \leq R}$

- Έστω $a, b \in \varphi^{-1}(S') \Rightarrow \left.\begin{matrix} \varphi(a) \in S' \\ \varphi(b) \in S' \end{matrix}\right\} \Rightarrow \varphi(a)\cdot\varphi(b) = \varphi(a\cdot b) \in S'$

$\Longrightarrow \boxed{a\cdot b \in \varphi^{-1}(S')}$

Άρα : $\varphi^{-1}(S')$ υποδακτύλιος του R

▶ Άσκηση: Βρείτε όλους τους ομομορφισμούς δακτυλίων από το $\mathbb{Z} \to \mathbb{Z}$

▶ Λύση: Έστω $\varphi: \mathbb{Z} \to \mathbb{Z}$ ομομορφισμός δακτυλίων!

Τότε: $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) \Rightarrow \varphi(1) = (\varphi(1))^2$

$\mathbb{Z}$: ακέραια περιοχή $\longrightarrow$ $\boxed{\varphi(1)=0}$ ή $\boxed{\varphi(1)=1}$

- $\boxed{\varphi(1)=0} \Rightarrow \varphi(2) = \varphi(1+1) = \varphi(1)+\varphi(1) = \underline{0}$

  Επαγωγικά: $\boxed{\varphi(n)=0}$, $n \in \mathbb{Z}$

- $\boxed{\varphi(1)=1} \Rightarrow \varphi(2) = \varphi(1+1) = \varphi(1)+\varphi(1) = \underline{2}$

  Επαγωγικά: $\boxed{\varphi(n)=n}$, $n \in \mathbb{Z}$

- Άρα, έχουμε **ΜΟΝΟ** δύο ομομορφισμούς δακτυλίων!!!

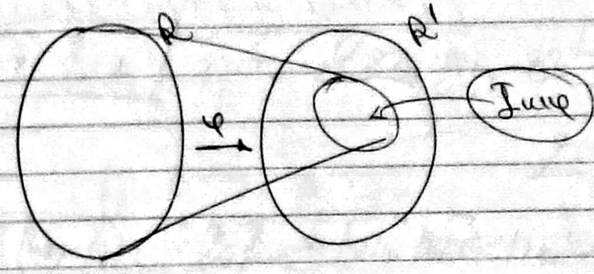
▶ Ορισμός: Ένα στοιχείο $a \in R$ λέγεται ταυτοδύναμο, αν $\boxed{a^2 = a}$.

⚠ Αν $\varphi: R \to R'$ ομομορφισμοί δακτυλίων. Τότε: $\varphi(1)$: ταυτοδύναμο στο R'

▶ **Άσκηση** { Βρείτε όλα τα ταυτοδύναμα στοιχεία του $\mathbb{Z}_{12}$.

▶ **Λύση** $\boxed{[0]_{12}^2=[0]_{12}}$ $\boxed{[1]_{12}^2=[1]_{12}}$

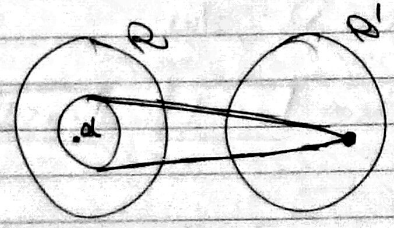
$[2]_{12}^2 \neq [2]_{12}$ ... $\boxed{[4]_{12}^2=[4]_{12}}$ και: $\boxed{[9]_{12}^2=[9]_{12}}$

▶ 

• R υποδακτύλιος του R ⟹ φ(R) υποδακτύλιος του R'

$\varphi(R) = Im\varphi$

• φ: επιμορφισμός, αν και μόνο αν: $Im\varphi=\varphi(R)=R'$

▶ 

• $\varphi^{-1}(\{0\})=\{\alpha\in R / \varphi(\alpha)=0\}=Ker\varphi$.

• $\{0\}$: υποδακτύλιος του R'

• Άρα, $Ker\varphi$ υποδακτύλιος του R

▶ **Θεώρημα** { Ο ομομορφισμός δακτυλίων είναι μονομορφισμός, αν και μόνο αν:

$$\boxed{Ker\varphi=\{0\}}$$

Έστω $\varphi: R \to R'$ ομομορφισμός δακτυλίων και $I = Ker\varphi$. Τότε $I = Ker\varphi$ είναι υποδακτύλιος του R και έχει την παρακάτω ιδιότητα:

SOS

- Αν $\alpha \in I = Ker\varphi$ και $r \in R$, τότε $\boxed{r\alpha \; \& \; \alpha r \in Ker\varphi}$.

$\boxed{\varphi(\alpha) = 0}$

Έχω: $\varphi(\alpha r) = \varphi(\alpha) \cdot \varphi(r) = \boxed{0} = \varphi(r) \cdot \varphi(\alpha) = \varphi(r\alpha)$

$\Rightarrow \boxed{r\alpha \in Ker\varphi \ni \alpha r}$

Ορισμός Ιδεώδες I ενός δακτυλίου R λέγεται ένας υποδακτύλιος I του R, τ/ω:

Αν $\alpha \in I \; \& \; r \in R$, τότε: $\boxed{\alpha r \in I}$ και $\boxed{r\alpha \in I}$.

Παράδειγμα Τα ιδεώδη του $\mathbb{Z}$ είναι της μορφής:

$\langle n \rangle = n\mathbb{Z}$, όπου n: φυσικός.

Ορισμός Δακτύλιος πηλίκο :

$$\boxed{R/I = \{a+I \mid a \in R\}}$$

με πράξεις :

$$\boxed{(a+I)+(b+I) = (a+b)+I}$$

και :

$$\boxed{(a+I)(b+I) = (ab)+I}$$