ΦΥΣΙΚΟΙ

(1) Τί είναι οι φυσικοί αριθμοί;

$0 = \emptyset$

$1 = \{\emptyset\} = \{0\}$

$2 = \{\emptyset, \{\emptyset\}\} = \{0,1\}$

$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0,1,2\}$

κτλ.

$\mathbb{N}_0 = \{0,1,2,3,\dots\}$, $\mathbb{N} = \mathbb{N}_0 \setminus \{0\} = \{1,2,3,\dots\}$

(2) Τί "δομή" έχει το $\mathbb{N}$;

→ Δέχεται μια πράξη (πρόσθεση)

$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \ : \ (m,n) \longmapsto m+n$

που έχει τις ιδιότητες:

(Π1) $m+n = n+m \quad \forall\, m,n \in \mathbb{N}$ (μεταθετική)

(Π2) $m+(n+k) = (m+n)+k, \quad \forall\, m,n,k \in \mathbb{N}$ (προσεταιριστική)

(Π3) $m+k = n+k \Leftrightarrow m = n$ (διαγραφή)

→ Δέχεται και μια δεύτερη πράξη (πολλ/σμός)

$\cdot \ \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \ : \ (m,n) \longmapsto m \cdot n$

με τις ιδιότητες:

(Γ1) $m \cdot n = n \cdot m, \quad \forall\, m,n \in \mathbb{N}$

(Γ2) $m \cdot (n \cdot k) = (m \cdot n) \cdot k, \quad \forall\, m,n,k \in \mathbb{N}$

(Γ3) Έχει ουδέτερο στοιχείο; το $1 \in \mathbb{N}$:

$$1 \cdot m = m \cdot 1 = m, \quad \forall m \in \mathbb{N}$$

(Γ4) $m \cdot k = n \cdot k \iff m = n$

Οι δύο πράξεις συνδέονται με την ιδιότητα

$$k \cdot (m+n) = km + kn, \quad \forall\, m, n, k \in \mathbb{N}$$

(επιμεριστική)

→ Δέχεται μια <u>σχέση διάταξης</u>:

$$m \leq n \iff \begin{cases} m = n & \text{ή} \\ \exists\, k \in \mathbb{N}: & m+k = n \end{cases}$$

η οποία είναι συμβατή με τις πράξεις:

$$m+k \leq n+k \iff m \leq n$$

$$mk \leq nk \iff m \leq n$$

<u>Υπενθύμιση</u>: Έστω $(X, \leq)$ διατεταγμένο σύνολο. Λέμε ότι ένα $A \subseteq X$ <u>έχει ελάχιστο στοιχείο</u>, αν $\exists\, a \in A$: $a \leq x$, $\forall x \in A$. Αντίστοιχα, λέμε ότι το $A \subseteq X$ <u>έχει μέγιστο στοιχείο</u>, αν $\exists\, b \in A$: $x \leq b$, $\forall x \in A$.

③ <u>Δεχόμαστε την Αρχή Ελαχίστου</u>:

κάθε $\emptyset \neq S \subseteq \mathbb{N}$ έχει ελάχιστο στοιχείο.

Παρατήρηση: το $\mathbb{N}$ έχει ελάχιστο το 1.

ΘΕΩΡ 1 (Αρχή της Επαγωγής)

$S \subseteq \mathbb{N}$: (i) $1 \in S$

(ii) $k \in S \Rightarrow k+1 \in S$.

Τότε $S = \mathbb{N}$.

Απόδ. Έστω $T = \mathbb{N} \setminus S \neq \emptyset$. Από την Αρχή Ελαχίστου $\exists$ ελάχιστο $a \in T$.

(i): $1 \in S \Rightarrow 1 \notin T$

$\Rightarrow a \neq 1$ και $a > 1$

$\Rightarrow a-1 \in \mathbb{N}$ και $a-1 < a =$ ελάχιστο του T

$\Rightarrow a-1 \notin T \Rightarrow$

$\Rightarrow a-1 \in S \xRightarrow{(ii)}$

$\Rightarrow (a-1)+1 = a \in S$, άτοπο.

Άρα $T = \emptyset$, δηλ. $S = \mathbb{N}$.

ΘΕΩΡ 2 (Μέθοδος της Επαγωγής)

$\Pi(n)$ πρόταση που αφορά στον $n \in \mathbb{N}$. Αν

(i) $\Pi(1)$ αληθής, και

(ii) ισχύει η συνεπαγωγή

$\Pi(k)$ αληθής $\Rightarrow \Pi(k+1)$ αληθής

Τότε $\Pi(n)$ αληθής $\forall n \in \mathbb{N}$.

$\exists$ δύο βασικές παραλλαγές

ΘΕΩΡ 3

$\Pi(n)$ όπως προηγουμένως. Αν:

(i) $\Pi(m)$ αληθής, για κάποιο $m \in \mathbb{N}$, και

(ii) $\Pi(k)$ αληθής $\Rightarrow$ $\Pi(k+1)$ αληθής

Τότε $\Pi(n)$ αληθής, $\forall n \geq m$.

ΘΕΩΡ 4 (Ισχυρή μορφή της Επαγωγής)

$\Pi(n)$ όπως προηγουμένως. Αν:

(i) $\Pi(1)$ αληθής, και

(ii) $\Pi(1), \Pi(2), \ldots, \Pi(k)$ αληθείς $\Rightarrow$ $\Pi(k+1)$ αληθής

Τότε $\Pi(n)$ αληθής, $\forall n \in \mathbb{N}$.

Παράδειγμα $\quad |S| = n \Rightarrow |\mathcal{P}(S)| = 2^n. \quad (\Pi(n))$

Απόδ $\quad n=1 \Rightarrow S =$ μονοσύνολο $\Rightarrow \mathcal{P}(S) = \{\emptyset, S\} \Rightarrow$

$\Rightarrow |\mathcal{P}(S)| = 2^1$, άρα $\Pi(1)$ ισχύει.

Έστω ότι ισχύει η $\Pi(k)$, για κάποιο $k \in \mathbb{N}$.

ΘΔΟ ισχύει η $\Pi(k+1)$. Θεωρούμε ένα S με $|S| = k+1$,

άρα $S = \{x_1, x_2, \ldots, x_{k+1}\}$. Θέτουμε $T = S \setminus \{x_{k+1}\}$, και

$\mathcal{A} = \{X \subseteq S : x_{k+1} \notin X\}$, $\mathcal{B} = \{X \subseteq S : x_{k+1} \in X\} \Rightarrow$

$= \mathcal{P}(T)$, $|\mathcal{A}| = |\mathcal{P}(T)| = 2^k$ και

$|\mathcal{A}| = |\mathcal{B}|$, ενώ $\mathcal{P}(S) = \mathcal{A} \cup \mathcal{B}$, με $\mathcal{A} \cap \mathcal{B} = \emptyset$

ΑΚΕΡΑΙΟΙ

(1) Στο $\mathbb{N}_0 \times \mathbb{N}_0$ ορίζουμε την <u>σχέση ισοδυναμίας</u>:

$$(m,n) \sim (k,\ell) \Leftrightarrow m+\ell = n+k$$

Έστω $q \in \mathbb{N}$. Ποιά είναι η κλάση ισοδυναμίας του $(q,0) \in \mathbb{N}_0 \times \mathbb{N}_0$; Του $(0,q)$;

$$[(q,0)] = \{(m,n) \in \mathbb{N}_0 \times \mathbb{N}_0 : (q,0) \sim (m,n)\} =$$

$$= \{(m,n) \in \mathbb{N}_0 \times \mathbb{N}_0 : q+n = m+0\} =$$

$$= \{(q,0), (q+1,1), (q+2,2), \dots\}$$

$$[(0,q)] = \{(m,n) \in \mathbb{N}_0 \times \mathbb{N}_0 : (0,q) \sim (m,n)\} =$$

$$= \{(m,n) \in \mathbb{N}_0 \times \mathbb{N}_0 : n = m+q\} =$$

$$= \{(0,q), (1,q+1), (2,q+2), \dots\}$$

Το <u>σύνολο των ακεραίων</u> είναι το σύνολο $\mathbb{Z}$ όλων των κλάσεων ισοδυναμίας.

<u>Συμβολίζουμε:</u>

$$m-n = [(m,n)]$$
$$q = [(q,0)]$$
$$-q = [(0,q)]$$

2 Δομή του $\mathbb{Z}$:

→ Το $\mathbb{Z}$ έχει μια πρόσθεση

$+ : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z} : (a,b) \mapsto a+b$,

με τις ιδιότητες:

(i) $a+b=b+a$, $\forall a,b\in\mathbb{Z}$ (μεταθετική)

(ii) $a+(b+c)=(a+b)+c$, $\forall a,b,c\in\mathbb{Z}$ (προσεταιριστική)

(iii) $\exists$ ουδέτερο στοιχείο, το $0\in\mathbb{Z}$:

$$0+a=a+0=a, \ \forall a\in\mathbb{Z}.$$

(iv) $\forall a\in\mathbb{Z}$ $\exists$ το αντίθετο του a, (συμβ: $-a$) με

$$a+(-a)=(-a)+a=0.$$

→ Το $\mathbb{Z}$ έχει ένα πολλαπλασιασμό

$\cdot\ \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z} : (a,b)\mapsto a\cdot b$

με τις ιδιότητες:

(i) $ab=ba$ $\forall a,b\in\mathbb{Z}$

(ii) $a(bc)=(ab)c$ $\forall a,b,c\in\mathbb{Z}$

(iii) $\exists$ ουδέτερο, το $1\in\mathbb{Z}$:

$$1\cdot a=a\cdot 1=a, \ \forall a\in\mathbb{Z}.$$

(iv) $\forall a\neq 0$ ισχύει ο νόμος της διαγραφής:

$$ax=ay \Rightarrow x=y.$$

→ Οι δύο πράξεις συνδέονται με την επιμεριστική ιδιότητα:

$$a(b+c)=ab+ac, \ \forall a,b,c\in\mathbb{Z}.$$

$\mathbb{Z}^+ =$ μη αρνητικοί ακέραιοι $\equiv \mathbb{N}_0$

$\mathbb{Z}^- = \{-q : q \in \mathbb{N}_0\}$

→ Το $\mathbb{Z}$ δέχεται και <u>διάταξη</u>:

$$a \leq b \iff \exists\, q \in \mathbb{Z}^+ \equiv \mathbb{N}_0 : a + q = b.$$

Η διάταξη των ακεραίων είναι συμβατή με τις πράξεις:

$$a \leq b \iff a + c \leq b + c \quad \forall c \in \mathbb{Z}$$

$$a \leq b \iff ac \leq bc \quad \forall c \in \mathbb{Z}^+,\ c \neq 0.$$

<u>ΠΑΡΑΤΗΡΗΣΕΙΣ</u>

1. Η ύπαρξη του $-c \in \mathbb{Z}$, $\forall c \in \mathbb{Z}$, συνεπάγεται τον <u>νόμο της διαγραφής</u> για την πρόσθεση:

$$a + c = b + c \Rightarrow (a+c) + (-c) = (b+c) + (-c) \Rightarrow$$

$$\Rightarrow a + (c + (-c)) = b + (c + (-c)) \Rightarrow$$

$$\Rightarrow a + 0 = b + 0 \Rightarrow a = b.$$

Επίσης, την λύση των εξισώσεων της μορφής

$$a + x = b$$

Πράγματι, $a + x = b \Rightarrow (-a) + (a + x) = (-a) + b \Rightarrow$

$$\Rightarrow ((-a) + a) + x = b + (-a) \Rightarrow$$

$$\Rightarrow 0 + x = b - a \Rightarrow$$

$$\Rightarrow x = b - a$$

2) Οι εξισώσεις της μορφής $ax=b$ δεν λύνονται πάντα στο $\mathbb{Z}$.

ΟΡΙΣΜΟΣ / Έστω $a,b\in\mathbb{Z}$. Λέμε ότι ο a διαιρεί τον b και γράφουμε $a|b$, αν $\exists\ c\in\mathbb{Z}$ με $ac=b$.

$\boxed{\text{ΘΕΩΡΗΜΑ}}$ (Ταυτότητα της διαίρεσης)

$$\forall b\in\mathbb{Z},\ \forall a\in\mathbb{N}\ \ \exists!\,(q,r)\in\mathbb{Z}\times\mathbb{N}_0:$$
$$b=aq+r,\quad \text{και}\quad 0\leq r<a$$

Απόδ. Θεωρούμε το σύνολο
$$A=\{b-as:\ s\in\mathbb{Z}\}\cap\mathbb{N}_0\subseteq\mathbb{N}_0$$
Είναι $A\neq\emptyset$: αν $b\geq 0\Rightarrow$ για $s=0$: $b-a\cdot 0=b\in A$,
αν $b<0\Rightarrow$ για $s=b$: $b-a\cdot b=\underbrace{b}_{<0}\underbrace{(1-a)}_{\leq 0}\geq 0\Rightarrow$
$\Rightarrow b-ab\in A$.

Από την Αρχή Ελαχίστου, $\exists$ ελάχιστο $r\in A$,
$r=b-aq$, για κάποιο $q\in\mathbb{N}$. Ο.δ.ο. $0\leq r<a$.
Αφού $A\subseteq\mathbb{N}_0$ και $r\in A$, είναι $0\leq r$. Είναι και $r<a$.
Πράγματι, αν $r\geq a$ παίρνουμε

$$r=b-aq\geq a\Rightarrow r-a=b-aq-a\geq 0\Rightarrow$$
$$\Rightarrow r-a=b-a(q+1)\geq 0\Rightarrow$$
$$\Rightarrow r-a<r\ \text{ και }\ r-a\in A\Rightarrow$$
$$\Rightarrow r\ \text{όχι ελάχιστο του } A,\ \text{άτοπο}.$$

Δείχνουμε τώρα ότι το ζεύγος (q,r) είναι <u>μοναδικό</u>:

αν $(q',r') \neq (q,r)$ δύο ζεύγη με τις ζητούμενες ιδιότητες,

τότε $q' \neq q$ ή $r' \neq r$. Όμως: $q' \neq q \iff r' \neq r$ (προφανές).

Έστω $q' > q$. Τότε:

$$q > q' \iff aq > aq' \iff b - aq < b - aq' \iff r < r'.$$

Όμως:

$$\left.\begin{array}{l} a > r \geq 0 \\ a > r' \geq 0 \end{array}\right\} \Rightarrow \left\{\begin{array}{l} 0 \geq -r > -a \\ a > r' \geq 0 \end{array}\right\} \xRightarrow{(+)} a > r' - r$$

$$\Rightarrow a > r' - r = b - aq' - (b - aq) =$$

$$= aq - aq' = a(q - q') \underset{\geq}{>} a, \text{ άτοπο.}$$