22-11-16

$A = \{f: \mathbb{N} \to \mathbb{C} \mid f: \text{συνάρτηση}\}$: σύνολο αριθμητικών συναρτήσεων $\forall f, g \in A : f * g \in A$

$$(f*g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$$

$$\varepsilon \in A, \text{ όπου } \varepsilon(n) = \begin{cases} 1, & n=1 \text{ και τότε: } f*\varepsilon = f = \varepsilon * f, \forall f \in A \\ 0, & n>1 \end{cases}$$

Αν $f \in A$, υπάρχει $g \in A$: $f*g = \varepsilon = g*f$;

Απάντηση: Ναι, αν $f(1) \neq 0$ και αντιστρόφως

Αν $f(1) \neq 0$, τότε η μοναδική συνάρτηση $g \in A$:

$f*g = g*f = \varepsilon$ καλείται ενελικτικά αντίστροφη της f και συμβολίζεται με f^{-1}

$$f^{-1}(n) = \begin{cases} \dfrac{1}{f(1)}, & \text{αν } n=1 \\ -\dfrac{1}{f(1)} \displaystyle\sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \end{cases}$$

$\mathcal{U} = \{f: \mathbb{N} \to \mathbb{C} \mid f(1) \neq 0\}$: σύνολο όλων των ενελικτικά αντιστρέψιμων συναρτήσεων

↳ Παρατήρηση: Αν $f, g \in \mathcal{U}$. Τότε $f^{-1} \in \mathcal{U}$ και $f*g \in \mathcal{U}$

- $f \in \mathcal{U} \Rightarrow f(1) \neq 0 \Rightarrow f^{-1}(1) = \dfrac{1}{f(1)} \neq 0 \Rightarrow f^{-1} \in \mathcal{U}$

$(f*g)(1) = f(1)g(1) \neq 0$, διότι επειδή $f,g \in \mathcal{U}$, έπεται ότι $f(1), g(1) \neq 0$. Άρα $f*g \in \mathcal{U}$

$(\mathcal{U},*)$: αβελιανή ομάδα, $\mathcal{U} \subseteq A$

$\mathcal{U} = \{ f: \mathbb{N} \to \mathbb{C} \mid f(1) \neq 0 \}$ = σύνολο ελικτικά αντιστρεπτών συναρτήσεων

<u>Ορισμός</u>: Αν $f \in A$ τότε η f καλείται πολλαπλασιαστική συνάρτηση $\Leftrightarrow f \neq 0$ και αν $m,n \in \mathbb{N}$ έτσι ώστε $(m,n)=1$, τότε: $f(m \cdot n) = f(m) \cdot f(n)$ ⊛

$\mathcal{M} = \{ f: \mathbb{N} \to \mathbb{C} \mid f$: πολλαπλασιαστική $\}$ = σύνολο πολλαπλασιαστικών συναρτήσεων

Αν $f \in \mathcal{M} \Rightarrow f \neq 0 \Rightarrow \exists\, n \in \mathbb{N}: f(n) \neq 0$. Τότε:

$$0 \neq f(n) = f(n \cdot 1) \underset{(n,1)}{\overset{*}{=}} f(n) f(1) \Rightarrow f(1) = 1.$$

Άρα $f \in \mathcal{U}$ και $f(1) = 1$

<u>Παράδειγμα</u>: 1) Για κάθε $k \in \mathbb{N}$ θεωρούμε τη συνάρτηση

$N^k : \mathbb{N} \to \mathbb{C}$, $N^k(n) = n^k$

Τότε $N^k \in \mathcal{M}$. Πράγματι: $N^k(1) = 1 \neq 0 \Rightarrow N^k \neq 0$ και αν $n,m \in \mathbb{N}: (n,m)=1$, τότε:

$N^k(n \cdot m) = (n \cdot m)^k = n^k m^k = N^k(n) \cdot N^k(m)$

2) $\tau: \mathbb{N} \to \mathbb{C}$, $\tau(n) = \sum_{d|n} 1$: πλήθος θετικών διαιρετών του n

Προφανώς $\tau(1) = 1 \neq 0$

Έστω $n > 1$ και έστω $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$: πρωτογενής ανάλυση του n

Όμως : $d|n \Leftrightarrow d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, όπου: $0 \leq \beta_i \leq \alpha_i$, $1 \leq i \leq k$

Δυνατές τιμές για το $\beta_1 : \alpha_1 + 1$
–11– $\beta_2 : \alpha_2 + 1$
–11– $\beta_k : \alpha_k + 1$
$\Rightarrow$

$\Rightarrow$ Δυνατές τιμές για το θετικό διαιρέτη d του n είναι:

$(\alpha_1+1) \cdot (\alpha_2+1) \cdot \ldots \cdot (\alpha_k+1)$

Άρα: $\tau(n) = (\alpha_1+1)(\alpha_2+1) \ldots (\alpha_k+1)$

Έστω $n, m \in \mathbb{N}$ και $(n,m) = 1$. Θα δείξουμε ότι

$\tau(n \cdot m) = \tau(n)\tau(m)$

↳ Αν $\underline{n=1}$, τότε $\tau(n \cdot m) = \tau(1 \cdot m) = \tau(m) = 1 \cdot \tau(m) = \tau(1)\tau(m) =$

$= \tau(n)\tau(m)$

↳ Αν $\underline{m=1}$, ομοίως $\tau(n \cdot m) = \tau(n) \cdot \tau(m)$

Αν $n,m>1$, τότε: $n=p_1^{a_1}\dots p_k^{a_k}$: πρωτογενής ανάλυση του n
$m=q_1^{\beta_1}\dots q_\lambda^{\beta_\lambda}$: —″— m
$(p_i\neq q_j)$: πρώτοι, διότι $(n,m)=1$

Τότε: η πρωτογενής ανάλυση του $nm=p_1^{a_1}\dots p_k^{a_k}q_1^{\beta_1}\dots q_\lambda^{\beta_\lambda}$

$\tau(nm)=\underbrace{(a_1+1)\dots(a_k+1)}_{\tau(n)}\cdot\underbrace{(\beta_1+1)\dots(\beta_\lambda+1)}_{\tau(m)}=\tau(n)\tau(m)$. Άρα, $\tau\in M$

<u>Πχ</u>: $\left.\begin{matrix}\tau(2\cdot4)=\tau(8)=4\\ \tau(2)\cdot\tau(4)=2\cdot3=6\end{matrix}\right\}\neq\ \Rightarrow\tau$: όχι πλήρως πολ/κή

<u>Πρόταση</u>: $\mu\in M$, $\boxed{\nu^{-1}=\mu}$

$$\mu(n)=\begin{cases}1, & n=1\\ 0, & \exists p:\text{πρώτος}: p^2|n\\ (-1)^n, & n=p_1p_2\dots p_k:\text{πρωτ. ανάλυση}\end{cases}$$

<u>Απόδειξη</u>: $\mu(1)=1\neq0\Rightarrow\mu\neq0$

Έστω $n,m\in\mathbb{N}:(n,m)=1$

α) Αν $n=1$, $m\in\mathbb{N}$, τότε: $\mu(n\cdot m)=\mu(1\cdot m)=\mu(m)=1\cdot\mu(m)=\mu(1)\mu(m)=$
$=\mu(\nu)\mu(m)$

β) Ομοίως, αν $m=1$, $n\in\mathbb{N}$, τότε: $\mu(n\cdot m)=\mu(n)\mu(m)$

γ) Έστω $n>1, m>1$ κι έστω $n=p_1^{a_1}\dots p_k^{a_k}$: πρωτ. αναλύσεις των n,m

1) Αν $\exists$ p: πρώτος, $p^2|n$, τότε: $\mu(n)=0\Rightarrow\mu(n)\mu(m)=0$

Όμως προφανώς $p^2|n\cdot m\Rightarrow\mu(n\cdot m)=0\Rightarrow\mu(n\cdot m)=\mu(n)\mu(m)$

2) Αν υπάρχει πρώτος $p : p^2 | m$, τότε ομοίως: $\mu(nm) = \mu(n)\mu(m)$

3) Αν $\nexists$ πρώτος $p : p^2 | n$ και $p^2 | m$, τότε:

$\mu(n) = (-1)^k$ | Αν υπάρχει πρώτος $p : p^2 | n \cdot m$, τότε
$\mu(m) = (-1)^\lambda$ | $p^2 | n$ ή $p^2 | m$: Άτοπο από υπόθεση

Άρα $\nexists$ πρώτος $p : p^2 | n \cdot m \Rightarrow \mu(nm) = (-1)^{k+\lambda}$. Άρα $\mu(nm) = (-1)^{k+\lambda} =$
$= (-1)^k (-1)^\lambda = \mu(n)\mu(m)$

↳ Πρόταση: Έστω $f \in M$ και $a_1, a_2, \ldots, a_k$ πρώτοι μεταξύ τους ανά δύο, τότε: $f(a_1 a_2 \ldots a_k) = f(a_1) f(a_2) \ldots f(a_k)$ ⊛

Απόδειξη: Χρησιμοποιώντας (Α.ΜΕ). Για $k=2$, η ⊛ ισχύει απ' τον ορισμό πολ/κής συνάρτησης. Υποθέτουμε ότι η ⊛ ισχύει

Έστω $a_1, a_2, \ldots, a_k, a_{k+1}$: πρώτοι μεταξύ τους ανά δύο: $(a_i, a_j) = 1$
$1 \leq i \neq j \leq k+1$

$f(a_1 a_2 \ldots a_k a_{k+1}) = f[(a_1 a_2 \ldots a_k) a_{k+1}] \overset{(+)}{=} f(a_1 \ldots a_k) f(a_{k+1}) =$
$= f(a_1) f(a_2) \ldots f(a_k) f(a_{k+1})$

(+) Αν $(a_1 a_2 \ldots a_k, a_{k+1}) = d > 1$, τότε $\exists$ πρώτος $p : p | d$

$\Rightarrow p | a_{k+1}$, $p | a_1 \ldots a_k \Rightarrow \begin{cases} p | a_{k+1} \\ \exists i = 1, \ldots, k : p | a_i \end{cases} \Rightarrow p | (a_{k+1}, a_i) = 1$

Άτοπο, άρα $(a_1 \ldots a_k, a_{k+1}) = 1$

↳ Θεώρημα: Αν $n > 1$ με πρωτ. ανάλυση $n = p_1^{a_1} \ldots p_k^{a_k}$

Τότε $\forall f \in M$: $f(n) = f(p_1^{a_1}) f(p_2^{a_2}) \ldots f(p_k^{a_k})$

Απόδειξη: Επειδή $(p_i^{a_i}, p_j^{a_j})=1$, $1\le i\neq j\le k$, το αποτέλεσμα προκύπτει απ' την πρόταση

Πόρισμα: Αν $f,g\in M$, τότε $f=g \Longleftrightarrow \forall p$: πρώτο, $\forall \alpha\in N$

$f(p^\alpha)=g(p^\alpha)$

Απόδειξη: $\forall n>1$ με πρωτογενή ανάλυση $n=p_1^{a_1}\dots p_k^{a_k}$ τότε: $f(n)=f(p_1^{a_1})\dots f(p_k^{a_k})$ "$\Longrightarrow$"

"$\Rightarrow$" Αν $f=g$, τότε προφανώς $f(p^\alpha)=g(p^\alpha)$

$g(n)=g(p^{\alpha_1})\dots g(p_k^{\alpha_k})$ "$\Longleftarrow$" Αντίστροφα

Αν $f(p^\alpha)=g(p^\alpha)$, $\forall$ πρώτο p, $\forall \alpha\in N$

$f(n)=f(p_1^{a_1})\dots f(p_k^{a_k})=g(p_1^{a_1})\dots g(p_k^{a_k})=g(n)$

Τότε: $f(p_i^{a_i})=g(p_i^{a_i})$, $1\le i\le k \Longrightarrow$

• Αν $n=1$: $f(1)=1=g(1)$, συνεπώς

$f(n)=g(n)$, $\forall n\in N \Rightarrow f=g$

Άσκηση : $\sigma\in M$ $\quad \sigma(n)=\sum_{d\mid n} d$

Τότε: $F(n) = F(p_1^{a_1}) \dots F(p_k^{a_k})$ (1)

$\forall\, p$: πρώτο, $\forall\, \alpha \in \mathbb{N}$: $F(p^\alpha) = \sum_{d \mid p^\alpha} (\mu f)(d) =$

$$= \sum_{d \mid p^\alpha} \mu(d) f(d) = \mu(1)f(1) + \mu(p)f(p) + \mu(p^2)f(p^2) + \dots + \mu(p^\alpha)f(p^\alpha) = 1 - f(p)$$

$\Rightarrow F(p^\alpha) = 1 - f(p)$

Απ' τις (1), (2) έπεται ότι $\Rightarrow F(n) = [(1-f(p_1)) \dots (1-f(p_k))]$

$\hookrightarrow = \sum_{d \mid n} \mu(d) f(d)$

Εφαρμογή: (1) Θέτοντας $f = T$, θα έχουμε $T \in M$

$$\sum_{d \mid n} \mu(d) T(d) = \begin{cases} 1, & n = 1 \\ (1 - T(p_1)) \dots (1 - T(p_k)), & \text{αν } n = p_1^{a_1} \dots p_k^{a_k} \end{cases}$$

Άρα, $\forall\, n > 1$: $\sum_{d \mid n} \mu(d) T(d) = \underbrace{(1-2) \dots (1-2)}_{k \text{ φορές}} = (-1)^k$

(2) Θέτοντας $f = \sigma$, θα έχουμε

$$\sum_{d \mid n} \mu(d) \sigma(d) = \begin{cases} 1, & n = 1 \\ (1 - \sigma(p_1)) \dots (1 - \sigma(p_k)), & \text{αν } n = p_1^{a_1} \dots p_k^{a_k} \end{cases}$$

Όμως $\forall p$: πρώτος : $\sigma(p) = 1 + p$ και άρα

$$\forall n > 1 : \sum_{d|n} \mu(d)\sigma(d) = (1-(1+p_1))\dots(1-(1+p_k))$$

$$= (-p_1)\dots(-p_k) = (-1)^k p_1 \dots p_k$$

Θεώρημα: Τύπος αντιστροφής του Möbius

Έστω $f, g \in \mathcal{A}$

Τότε: $\forall n \geq 1$, $g(n) = \sum_{d|n} f(d) \iff$

$$\iff f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right), \ \forall n \geq 1$$

Απόδειξη: 1) $\forall n \geq 1 : g(n) = \sum_{d|n} f(d) =$

$$= \sum_{d|n} f(d) v\left(\frac{n}{d}\right) = (f * v)(n) \Rightarrow g = f * v$$

2) $\forall n \geq 1 : f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = (\mu * g)(n) \Rightarrow$

$$\Rightarrow f = \mu * g$$

Άρα αρκεί νδο: $g = f * v \iff f = \mu * g$

"$\Rightarrow$" Έστω ότι: $g = f * \nu \xrightarrow{*\nu^{-1}}$

$\Rightarrow g * \nu^{-1} = (f * \nu) * \nu^{-1} \Rightarrow g * \mu = f * (\nu * \nu^{-1}) = f * \varepsilon = f \Rightarrow$

$\Rightarrow f = g * \mu = \mu * g$

"$\Leftarrow$" Έστω ότι $f = \mu * g \Rightarrow f * \nu = \mu * g * \nu$

$\Rightarrow f * \nu = \nu * (\mu * g) \Rightarrow f * \nu = (\nu * \mu) * g \Rightarrow f * \nu = \varepsilon * g = g$

$\Rightarrow g = \nu * f = f * \nu$

↳ Εφαρμογή: Αν $f \in A$ και $F(n) = \sum_{d|n} f(d)$

Τότε: $f \in M \Leftrightarrow F \in M$

"$\Rightarrow$" Αν $f \in M$ τότε $F \in M$ (έχει αποδειχθεί)

"$\Leftarrow$" Έστω ότι $F \in M$

Απ' την αντιστροφή του Mobius $\Rightarrow$

$\Rightarrow f = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) \Rightarrow f = \mu * F \in M$

διότι $\mu \in M$, $F \in M$

Πρόταση: $f \in M \Leftrightarrow f^{-1} \in M$

$M \subseteq U \subseteq A$ $f, g \in M \Rightarrow f * g \in M$ | U: αβελιανή ομάδα

$f \in M \Rightarrow f^{-1} \in M$ | M: κανονική υποομάδα