Möbiovy inverzní formule podruhé

Jako další aplikaci obecné abstraktní věty o Möbiových inverzních formulích uvedeme speciální případ této věty, který se týká množiny $\mathfrak{N}$ všech kladných celých čísel částečně uspořádané dělitelností. Pro tuto částečně uspořádanou množinu $\mathfrak{N}$ jsme již dříve vypočetli její Möbiovu funkci $\mu_{\mathfrak{N}}$. Zjistili jsme, že pro libovolná kladná celá čísla m, n splňující $m|n$ je hodnota Möbiovy funkce $\mu_{\mathfrak{N}}$ na intervalu $[m, n]$ rovna

$$\mu_{\mathfrak{N}}(m,n) = \begin{cases} 1, & \text{jestliže } m = n, \\ (-1)^t, & \text{jestliže } n/m = q_1 q_2 \dots q_t, \text{ kde} \\ & \quad q_1, q_2, \dots, q_t \text{ jsou vzájemně různá prvočísla,} \\ 0, & \text{jestliže } n/m = r^2 u \text{ pro nějaká kladná celá} \\ & \quad \text{čísla } r, u \text{ splňující } r > 1. \end{cases}$$

V teorii čísel bývá Möbiovou funkcí nazývána číselná funkce, obvykle označovaná symbolem μ, definovaná na množině všech kladných celých čísel předpisem

$$\mu(k) = \begin{cases} 1, & \text{jestliže } k = 1, \\ (-1)^t, & \text{jestliže } k = q_1 q_2 \dots q_t, \text{ kde} \\ & \quad q_1, q_2, \dots, q_t \text{ jsou vzájemně různá prvočísla,} \\ 0, & \text{jestliže } k = r^2 u \text{ pro nějaká kladná celá} \\ & \quad \text{čísla } r, u \text{ splňující } r > 1, \end{cases}$$

a to pro každé kladné celé číslo k. Je pak jasné, že pro libovolná kladná celá čísla m, n splňující $m|n$ máme rovnost

$$\mu_{\mathfrak{N}}(m, n) = \mu(n/m).$$

Odtud pak také pocházejí námi používané termíny Möbiova funkce a Möbiovy inverzní formule v dříve studovaném abstraktním kontextu libovolných lokálně konečných uspořádaných množin.

V částečně uspořádané množině $\mathfrak{N}$ jsou očividně všechny hlavní ideály konečnými podmnožinami. Můžeme tedy na tuto částečně uspořádanou množinu aplikovat obecnou větu o Möbiových inverzních formulích. S přihlédnutím k předchozí poznámce o Möbiových funkcích takto dostáváme následující speciální případ zmíněné věty, který bývá též nazýván větou o Möbiových inverzních formulích.

Věta.

Buď K těleso chrakteristiky 0. Pak pro libovolné dvě funkce $f, g : \mathfrak{N} \to K$ platí rovnosti

$$g(n) = \sum_{d|n} f(d) \quad \text{pro všechna kladná celá čísla } n$$

právě tehdy, když platí rovnosti

$$f(n) = \sum_{d|n} \mu(n/d) g(d) \quad \text{pro všechna kladná celá čísla } n. \qquad \square$$

Jednou z aplikací Möbiových inverzních formulí je snadné odvození vztahu pro Eulerovu funkci. Připomeňme, že Eulerova funkce φ je funkcí na množině všech kladných celých čísel definovanou následovně. Pro každé kladné celé číslo n je $\varphi(n)$ počet všech těch kladných celých čísel, která nepřevyšují hodnotu n a jsou s číslem n nesoudělná.

Lemma.

Pro každé kladné celé číslo n platí

$$\sum_{d|n} \varphi(d) = n.$$

Důkaz.

Označme symbolem A_n množinu všech uspořádaných dvojic (d, c) složených z navzájem nesoudělných kladných celých čísel c, d takových, že $d|n$ a $c \leqslant d$. Označme dále symbolem B_n množinu všech kladných celých čísel e takových, že $e \leqslant n$. Ukážeme, že předpisem

$$(d, c) \mapsto \frac{n}{d} \cdot c$$

je definována bijekce množiny A_n na množinu B_n. Až to budeme mít ověřeno, bude stačit si jenom všimnout, že rovnost uvedená v našem lemmatu říká přesně to, že množiny A_n a B_n mají týž počet prvků.

Uvedeným předpisem je skutečně definováno zobrazení množiny A_n do množiny B_n. Toto zobrazení je surjektivní, neboť každé kladné celé číslo e splňující $e \leqslant n$ lze psát ve tvaru $e = b \cdot c$, kde b je největší společný dělitel čísel e a n a $c = \frac{e}{b}$. Položíme-li tedy $d = \frac{n}{b}$, pak $b = \frac{n}{d}$ a máme $e = \frac{n}{d} \cdot c$, přičemž jistě $d | n$, $c \leqslant d$ a čísla c, d jsou navzájem nesoudělná. Toto zobrazení je současně prosté, neboť je-li $e = \frac{n}{d} \cdot c$, kde čísla c, d splňují právě zmíněné podmínky, pak poněvadž také $n = \frac{n}{d} \cdot d$ a čísla c, d jsou navzájem nesoudělná, číslo $\frac{n}{d}$ musí být největším společným dělitelem čísel e a n. Je tedy za těchto okolností číslo d číslem e určeno jednoznačně a totéž pak platí také pro číslo c. □

Definujeme-li funkce $f, g : \mathfrak{N} \to K$ předpisy $f(n) = \varphi(n)$ a $g(n) = n$ pro všechna kladná celá čísla n, pak rovnosti uvedené v předchozím lemmatu pro všechna kladná celá čísla n se stanou prvními formulemi uvedenými v předchozí větě o Möbiových inverzních formulích. Podle této věty pak ovšem platí také druhé formule uvedené v této větě. To znamená, že platí rovnosti

$$\varphi(n) = \sum_{d|n} \mu(n/d) \cdot d$$

pro všechna kladná celá čísla n. Nyní jsme připraveni dokázat známý vztah pro Eulerovu funkci φ.

Tvrzení.

Pro každé kladné celé číslo n platí rovnost

$$\varphi(n) = n \cdot \prod_{i=1}^{k} \Big(1 - \frac{1}{p_i}\Big),$$

kde $p_1, p_2, \ldots, p_k$ jsou všechna navzájem různá prvočísla, která dělí n.

Poznámka.

Pro $n = 1$ součin v této formuli napravo zmizí.

Důkaz.

Položíme-li nejprve v poslední formuli uvedené před tímto tvrzením $c = \frac{n}{d}$, přejde tato formule do tvaru

$$\varphi(n) = \sum_{c|n} \mu(c) \cdot \frac{n}{c}.$$

Tato rovnost platí pro všechna kladná celá čísla n. Takové číslo n můžeme psát ve tvaru

$$n = p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot \ldots \cdot p_k^{\varepsilon_k},$$

kde $p_1, p_2, \ldots, p_k$ jsou vzájemně různá prvočísla a $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$ jsou nějaká kladná celá čísla.

Položme dále

$$n^* = p_1 \cdot p_2 \cdot \ldots \cdot p_k.$$

Pak z první formule uvedené výše v tomto důkazu vzhledem k definici Möbiovy funkce μ vyplývá

$$\varphi(n) = \sum_{c \mid n^*} \mu(c) \cdot \frac{n}{c}.$$

Tato rovnost zase platí pro všechna kladná celá čísla n. Rozepíšeme-li tuto rovnost podrobněji, dostaneme

$$\varphi(n) = n - \sum_{i=1}^{k} \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i \cdot p_j} - \sum_{i<j<\ell} \frac{n}{p_i \cdot p_j \cdot p_\ell} + \cdots$$
$$\cdots + (-1)^t \cdot \sum_{i_1 < \cdots < i_t} \frac{n}{p_{i_1} \cdot \ldots \cdot p_{i_t}} + \ldots + (-1)^k \frac{n}{p_1 \cdot \ldots \cdot p_k}.$$

To je ale právě dokazovaný vztah uvedený shora v tomto tvrzení po roznásobení závorek v součinu, který je tam uveden. □