Kompozice permutačních grup

Začněme připomenutím několika pojmů z teorie grup. Nechť H a K jsou libovolné grupy. Symbolem $\mathrm{Aut}\, H$ značíme grupu všech automorfismů grupy H. Budeme aplikovat automorfismy grupy H na prvky grupy H zprava. To znamená, že pro libovolný prvek $h \in H$ a pro libovolný automorfismus α grupy H budeme obraz prvku h po aplikaci automorfismu α značit symbolem $h\alpha$. Tomu také bude odpovídat pořadí skládání automorfismů v grupě $\mathrm{Aut}\, H$. Totiž součinem $\alpha \bullet \beta$ dvou automorfismů α a β grupy H budeme rozumět automorfismus grupy H daný pro libovolný prvek $h \in H$ předpisem $h(\alpha \bullet \beta) = (h\alpha)\beta$. Nechť dále $\varphi : K \to \mathrm{Aut}\, H$ je nějaký homomorfismus grupy K do grupy $\mathrm{Aut}\, H$. Pak na množině $K \times H$ definujeme binární operaci $\blacktriangle$ následujícím předpisem. Pro libovolné prvky $h, h' \in H$ a $k, k' \in K$ klademe

$$(k, h) \blacktriangle (k', h') = (k \cdot k',\ h\varphi(k') \cdot h').$$

Přímo lze ověřit, že pak množina $K \times H$ spolu s binární operací $\blacktriangle$ tvoří grupu. Tuto grupu značíme symbolem $K * H$ a nazýváme ji obráceným polopřímým součinem grup H a K určeným homomorfismem φ.

Nechť dále M a N jsou libovolné neprázdné množiny. Předpokládejme, že H je nějaká podgrupa grupy S_M všech permutací množiny M a že K je nějaká podgrupa grupy S_N všech permutací množiny N.

Uvažme dále mocninu H^N grupy H. Jejími prvky jsou všechny soubory prvků $(\sigma_p)_{p\in N}$ grupy H indexované prvky množiny N, takže $\sigma_p \in H$ pro všechna $p \in N$. Tato mocnina H^N je vybavena binární operací násobení definovanou po složkách předpisem

$$(\sigma_p)_{p\in N} \cdot (\sigma'_p)_{p\in N} = (\sigma_p \circ \sigma'_p)_{p\in N}.$$

Spolu s touto operací tvoří mocnina H^N grupu, nazývanou přímá mocnina grupy H. Pro libovolný prvek $\tau \in K$ uvažme zobrazení $\psi(\tau) : H^N \to H^N$ dané předpisem

$$((\sigma_p)_{p\in N})\psi(\tau) = (\sigma_{\tau(p)})_{p\in N}.$$

Přímo lze ověřit, že pak $\psi(\tau)$ je automorfismus mocniny H^N grupy H. Vzniká tak zobrazení $\psi : K \to \mathrm{Aut}\, H^N$ přiřazující každému prvku $\tau \in K$ automorfismus $\psi(\tau)$ grupy H^N. Rovněž přímo lze ověřit, že toto zobrazení ψ je homomorfismus grupy K do grupy $\mathrm{Aut}\, H^N$. Tato situace konečně umožňuje uvažovat o obráceném polopřímém součinu grup $K * H^N$ určeném homomorfismem ψ. Tento obrácený polopřímý součin budeme značit symbolem $K[H]$ a budeme ho nazývat kompozicí permutačních grup H a K. Z teorie grup je tato kompozice $K[H]$ grup H a K známa jako obrácený věnčitý součin (reverse wreath product) permutačních grup H a K.

Grupy H a K byly permutačními grupami, totiž byly podgrupami grup S_M a S_N všech permutací množin M a N. Ukážeme, že i jejich kompozici $K[H]$ lze reprezentovat jako permutační grupu, a to jako podgrupu grupy $S_{N\times M}$ všech permutací množiny $N \times M$. Prvky kompozice $K[H]$, to jest prvky obráceného polopřímého součinu $K * H^N$, jsou tvaru $\big(\tau, (\sigma_p)_{p\in N}\big)$, kde $\tau \in K$ a $\sigma_p \in H$ pro všechna $p \in N$. Ke každému takovému prvku $\big(\tau, (\sigma_p)_{p\in N}\big)$ uvažme zobrazení $\big[\!\big[\tau, (\sigma_p)_{p\in N}\big]\!\big] : N \times M \to N \times M$ dané pro každá $a \in M$ a $q \in N$ předpisem

$$\big[\!\big[\tau, (\sigma_p)_{p\in N}\big]\!\big](q, a) = (\tau(q), \sigma_q(a)).$$

Je snadné nahlédnout, že pak takto definované zobrazení $\big[\!\big[\tau, (\sigma_p)_{p\in N}\big]\!\big]$ je permutací množiny $N \times M$. Navíc zobrazení $\zeta : K[H] \to S_{N\times M}$ dané předpisem

$$\zeta\big(\tau, (\sigma_p)_{p\in N}\big) = \big[\!\big[\tau, (\sigma_p)_{p\in N}\big]\!\big]$$

je prostý homomorfismus grupy $K[H]$ do grupy $S_{N\times M}$. Je snadné ověřit, že toto zobrazení ζ je prosté. Ukážeme, že ζ je homomorfismus grup. K tomu je třeba ukázat, že platí

$$\Big[\!\Big[\big(\tau, (\sigma_p)_{p\in N}\big) \blacktriangle \big(\tau', (\sigma'_p)_{p\in N}\big)\Big]\!\Big] = \big[\!\big[\tau, (\sigma_p)_{p\in N}\big]\!\big] \circ \big[\!\big[\tau', (\sigma'_p)_{p\in N}\big]\!\big].$$

Ale $\big(\tau, (\sigma_p)_{p\in N}\big) \blacktriangle \big(\tau', (\sigma'_p)_{p\in N}\big) = \big(\tau \circ \tau', (\sigma_{\tau'(p)} \circ \sigma'_p)_{p\in N}\big)$. Takže máme ukázat, že platí

$$\big[\!\big[\tau \circ \tau', (\sigma_{\tau'(p)} \circ \sigma'_p)_{p\in N}\big]\!\big] = \big[\!\big[\tau, (\sigma_p)_{p\in N}\big]\!\big] \circ \big[\!\big[\tau', (\sigma'_p)_{p\in N}\big]\!\big].$$

Ověříme, že zobrazení na obou stranách dávají tutéž hodnotu na každé dvojici (q, a), kde $a \in M$ a $q \in N$. Ale skutečně

$$\begin{aligned} [\![\tau \circ \tau', (\sigma_{\tau'(p)} \circ \sigma'_p)_{p \in N}]\!](q, a) &= ((\tau \circ \tau')(q), (\sigma_{\tau'(q)} \circ \sigma'_q)(a)) \\ &= (\tau(\tau'(q)), \sigma_{\tau'(q)}(\sigma'_q(a))), \end{aligned}$$

zatímco

$$\begin{aligned} [\![\tau, (\sigma_p)_{p \in N}]\!]\left([\![\tau', (\sigma'_p)_{p \in N}]\!](q, a)\right) &= [\![\tau, (\sigma_p)_{p \in N}]\!](\tau'(q), \sigma'_q(a)) \\ &= (\tau(\tau'(q)), \sigma_{\tau'(q)}(\sigma'_q(a))). \end{aligned}$$

Celkem je tedy zobrazení $\zeta : K[H] \to S_{N \times M}$ vnořením grupy $K[H]$ do grupy permutací $S_{N \times M}$. Lze tedy kompozici $K[H]$ grup H a K vnímat jako podgrupu grupy $S_{N \times M}$ všech permutací množiny $N \times M$.

Bude nás dále zajímat cyklový index $Z(K[H])$ kompozice $K[H]$ grup H a K v případě, že množiny M a N jsou konečné, a tedy i permutační grupy H a K jsou konečné. V tom případě předpokládejme, že množina M má m prvků a množina N má n prvků. V takovém případě je pak i kompozice $K[H]$ konečnou grupou, na kterou lze rovněž nahlížet jako na permutační grupu výše popsaným způsobem. Příslušná množina $N \times M$, na níž se permutace odehrávají, pak má mn prvků. Cyklový index $Z(K[H])$ grupy $K[H]$ je pak polynomem v proměných $t_1, t_2, \ldots, t_{mn}$, který vyjádříme pomocí cyklových indexů $Z(H)$ a $Z(K)$ grup H a K následujícím způsobem.

Věta.

Pro cyklový index $Z(K[H])$ grupy $K[H]$ platí rovnost

$$Z(K[H]; t_1, t_2, \dots, t_{mn}) = Z(K; Z(H; t_1, t_2, \dots, t_m),\\ Z(H; t_2, t_4, \dots, t_{2m}), \dots, Z(H; t_n, t_{2n}, \dots, t_{mn})).$$

Výraz vpravo vznikne tak, že do cyklového indexu $Z(K; t_1, t_2, \dots, t_n)$ dosadíme pro každé $\ell = 1, 2, \dots, n$ výraz $Z(H; t_\ell, t_{2\ell}, \dots, t_{m\ell})$ za proměnnou t_ℓ.

Důkaz.

Buď Y libovolná konečná dostatečně velká množina mající η prvků. Je možné si přímo představit, že Y je množina čísel $\{1, 2, \dots, \eta\}$. Připomeňme znovu, že pak pro každé kladné celé číslo k jsme označili symbolem s_k sumu mocnin proměnných $x_1^k + x_2^k + \cdots + x_\eta^k$. Výše uvedenou rovnost cyklových indexů grup dokážeme tak, že ukážeme, že platí rovnost polynomů v proměnných $x_1, x_2, \dots, x_\eta$, která vznikne, když do shora uvedené rovnosti polynomů v proměnných $t_1, t_2, \dots, t_{mn}$ dosadíme pro každý index $k = 1, 2, \dots, mn$ sumu s_k za proměnnou t_k. Z posledního důsledku uvedeného v předchozím paragrafu plyne, že toto skutečně stačí k tomu, abychom ověřili shora uvedenou rovnost cyklových indexů grup.

Chystáme se tedy dokázat, že platí rovnost polynomů

$$Z(K[H]; s_1, s_2, \ldots, s_{mn}) = Z(K; Z(H; s_1, s_2, \ldots, s_m), \\ Z(H; s_2, s_4, \ldots, s_{2m}), \ldots, Z(H; s_n, s_{2n}, \ldots, s_{mn})).$$

Podle Pólyovy věty je polynom $Z(K[H]; s_1, s_2, \ldots, s_{mn})$ stojící nalevo v této rovnosti roven enumerátoru $\gamma(Y^{N \times M}, K[H])$. Potřebujeme tedy ukázat, že také polynom stojící napravo v této rovnosti je roven témuž enumerátoru $\gamma(Y^{N \times M}, K[H])$. Označili jsme symbolem $\mathfrak{M}_{Y^{N \times M}, K[H]}$ množinu všech orbit libovolných zobrazení $N \times M \to Y$ v podgrupě $E^{K[H]}$. Pak podle definice enumerátoru máme pro zmíněný enumerátor rovnost

$$\gamma(Y^{N \times M}, K[H]) = \sum_{\mathcal{O} \in \mathfrak{M}_{Y^{N \times M}, K[H]}} v(\mathcal{O}).$$

Sčítají se zde členy $v(\mathcal{O})$ přes všechny orbity $\mathcal{O} \in \mathfrak{M}_{Y^{N \times M}, K[H]}$. Staráme se tedy dále o orbity libovolných zobrazení $N \times M \to Y$ v podgrupě $E^{K[H]}$. Buď $f : N \times M \to Y$ libovolné takové zobrazení. Pak pro jeho orbitu v podgrupě $E^{K[H]}$, kterou značíme symbolem $fK[H]$, máme vztah

$$\begin{aligned} fK[H] &= \{f \circ \rho : \rho \in K[H]\} \\ &= \left\{f \circ \left[\!\left[\tau, (\sigma_p)_{p \in N}\right]\!\right] : \tau \in K,\, \sigma_p \in H \text{ pro všechna } p \in N\right\}. \end{aligned}$$

Přitom pro libovolná $a \in M$ a $q \in N$ máme

$$\big(f \circ [\![\tau, (\sigma_p)_{p\in N}]\!]\big)(q,a) = f\big([\![\tau, (\sigma_p)_{p\in N}]\!](q,a)\big) = f(\tau(q), \sigma_q(a)).$$

Přiřaďme k našemu zobrazení $f : N \times M \to Y$ soubor zobrazení $(f_p)_{p\in N}$, kde pro každé $p \in N$ je $f_p : M \to Y$ zobrazení dané předpisem $f_p(a) = f(p,a)$ pro všechna $a \in M$. Vezměme dále k danému zobrazení f orbity zobrazení f_p v podgrupě E^H pro všechna $p \in N$. Pro tyto orbity, které značíme f_pH, máme vztah

$$f_pH = \{f_p \circ \varsigma : \varsigma \in H\}.$$

Označili jsme symbolem $\mathfrak{M}_{Y^M,H}$ množinu všech orbit libovolných zobrazení $M \to Y$ v podgrupě E^H. Uvažme konečně zobrazení $\widetilde{f} : N \to \mathfrak{M}_{Y^M,H}$ dané pro každé $p \in N$ předpisem $\widetilde{f}(p) = f_pH$. Vezměme k tomuto zobrazení $\widetilde{f}$ jeho orbitu v podgrupě E^K. Tuto orbitu značíme symbolem $\widetilde{f}K$ a máme pro ni vztah

$$\widetilde{f}K = \{\widetilde{f} \circ \tau : \tau \in K\}.$$

Pro množinu všech orbit libovolných zobrazení $N \to \mathfrak{M}_{Y^M,H}$ v podgrupě E^K máme označení $\mathfrak{M}_{\mathfrak{M}^N_{Y^M,H},K}$. Orbita $\widetilde{f}K$ je prvkem této poslední množiny orbit.

Abychom se vyhnuli komplikovanému značení, zavedeme pro množinu orbit $\mathfrak{M}_{Y^M,H}$ krátké označení $\mathfrak{Y}$. Pak orbita $\widetilde{f}K$ je prvkem množiny orbit $\mathfrak{M}_{\mathfrak{Y}^N,K}$.

Ukážeme, že pak existuje vzájemně jednoznačná korespondence

$$\chi : \mathfrak{M}_{Y^{N\times M},K[H]} \to \mathfrak{M}_{\mathfrak{Y}^N,K}$$

definovaná formulí

$$\chi(fK[H]) = \widetilde{f}K$$

pro libovolná zobrazení $f : N \times M \to Y$. Je ovšem třeba zprvu ukázat, že tato definice je korektní.

Nechť tedy $f, g : N \times M \to Y$ jsou dvě zobrazení náležející téže orbitě v podgrupě $E^{K[H]}$, takže $g = f \circ \left[\!\left[\tau, (\sigma_p)_{p\in N}\right]\!\right]$ pro nějaká $\tau \in K$ a $\sigma_p \in H$, kde $p \in N$. Pak pro každé $p \in N$ jsou $f_p, g_p : M \to Y$ zobrazení daná předpisy $f_p(a) = f(p, a)$ a $g_p(a) = g(p, a)$ pro všechna $a \in M$. Ovšem viděli jsme výše, že pak $g_p(a) = g(p, a) = f(\tau(p), \sigma_p(a)) = f_{\tau(p)}(\sigma_p(a))$ pro všechna $a \in M$, takže dostáváme rovnost $g_p = f_{\tau(p)} \circ \sigma_p$ platnou pro všechna $p \in N$. Dále připomeňme, že zobrazení $\widetilde{f}, \widetilde{g} : N \to \mathfrak{M}_{Y^M,H}$ jsou pro každé $p \in N$ dána předpisy $\widetilde{f}(p) = f_pH = \{f_p \circ \varsigma : \varsigma \in H\}$ a $\widetilde{g}(p) = g_pH = \{g_p \circ \varsigma : \varsigma \in H\}$. Kromě toho víme, že $\widetilde{f}K = \{\widetilde{f} \circ \vartheta : \vartheta \in K\}$ a $\widetilde{g}K = \{\widetilde{g} \circ \vartheta : \vartheta \in K\}$.

Odvodíme odtud, že $\widetilde{f}K = \widetilde{g}K$. Mějme tedy libovolné zobrazení tvaru $\widetilde{g} \circ \vartheta$, kde $\vartheta \in K$, které náleží orbitě $\widetilde{g}K$. Pak pro každé $p \in N$ platí

$$\begin{aligned}(\widetilde{g} \circ \vartheta)(p) &= \widetilde{g}(\vartheta(p)) = g_{\vartheta(p)}H = \{g_{\vartheta(p)} \circ \varsigma : \varsigma \in H\} \\ &= \{f_{\tau(\vartheta(p))} \circ \sigma_{\vartheta(p)} \circ \varsigma : \varsigma \in H\} = \{f_{\tau(\vartheta(p))} \circ \varsigma : \varsigma \in H\} \\ &= f_{\tau(\vartheta(p))}H = \widetilde{f}(\tau(\vartheta(p))) = (\widetilde{f} \circ \tau \circ \vartheta)(p).\end{aligned}$$

Takže dostáváme rovnost $\widetilde{g} \circ \vartheta = \widetilde{f} \circ \tau \circ \vartheta$. Ovšem $\tau \circ \vartheta \in K$, takže zobrazení $\widetilde{f} \circ \tau \circ \vartheta$ náleží orbitě $\widetilde{f}K$, a tedy i zobrazení $\widetilde{g} \circ \vartheta$ náleží orbitě $\widetilde{f}K$. Dokázali jsme tak inkluzi $\widetilde{g}K \subseteq \widetilde{f}K$. Obrácená inkluze se dokáže analogicky, takže celkem platí rovnost $\widetilde{f}K = \widetilde{g}K$. Je tedy výše uvedená definice korespondence χ korektní.

Ukážeme dále, že korespondence χ je prosté zobrazení. Nechť tedy $f, g : N \times M \to Y$ jsou dvě zobrazení taková, že $\widetilde{f}K = \widetilde{g}K$. To znamená, že $\{\widetilde{f} \circ \vartheta : \vartheta \in K\} = \{\widetilde{g} \circ \vartheta : \vartheta \in K\}$. Zejména tedy existuje $\tau \in K$ takové, že $\widetilde{g} = \widetilde{f} \circ \tau$. Takže pro každé $p \in N$ máme rovnost $\widetilde{g}(p) = \widetilde{f}(\tau(p))$, čili $g_pH = f_{\tau(p)}H$, a tedy $\{g_p \circ \varsigma : \varsigma \in H\} = \{f_{\tau(p)} \circ \varsigma : \varsigma \in H\}$. Zejména tedy pro každé $p \in N$ existuje $\sigma_p \in H$ takové, že $g_p = f_{\tau(p)} \circ \sigma_p$. Odtud pro každé $a \in M$ a pro každé $p \in N$ plyne, že $g(p, a) = g_p(a) = f_{\tau(p)}(\sigma_p(a)) = f(\tau(p), \sigma_p(a))$.

To ale podle našich dřívějších zjištění znamená, že $g = f \circ [[\tau, (\sigma_p)_{p\in N}]]$ pro nalezená $\tau \in K$ a $\sigma_p \in H$, kde $p \in N$. Náležejí tedy obě zobrazení f, g téže orbitě v podgrupě $E^{K[H]}$, takže platí, že $fK[H] = gK[H]$. To dokládá prostotu zobrazení χ.

Ukážeme nakonec, že korespondence χ je surjektivní zobrazení. Nechť tedy $\mathcal{Q}$ je libovolná orbita v množině $\mathfrak{M}_{\mathfrak{Y}^N,K}$. Tato orbita se skládá z nějakých zobrazení $N \to \mathfrak{M}_{Y^M,H}$. Zvolme libovolné zobrazení $h : N \to \mathfrak{M}_{Y^M,H}$ z této orbity $\mathcal{Q}$. Pro každé $p \in N$ je $h(p)$ nějaká orbita v množině $\mathfrak{M}_{Y^M,H}$. Tato orbita se zase skládá z nějakých zobrazení $M \to Y$. Zvolme pro každé $p \in N$ nějaké zobrazení $f_p : M \to Y$ z orbity $h(p)$. Definujme konečně zobrazení $f : N \times M \to Y$ pro každá $a \in M$ a $p \in N$ předpisem $f(p, a) = f_p(a)$. Ukážeme, že pak platí $\widetilde{f}K = \mathcal{Q}$. K tomu stačí ukázat, že $\widetilde{f} \in \mathcal{Q}$. My ukážeme, že ve skutečnosti platí rovnost $\widetilde{f} = h$, kde h je odpočátku zvolené zobrazení z orbity $\mathcal{Q}$. Ale pro každé $p \in N$ máme $\widetilde{f}(p) = f_pH = h(p)$, neboť f_p je zobrazení z orbity $h(p)$. Takže skutečně máme rovnost $\widetilde{f} = h$. To potvrzuje surjektivitu zobrazení χ.

Buď nyní $\mathcal{O}$ libovolná orbita v množině $\mathfrak{M}_{Y^{N\times M},K[H]}$. Tato orbita je tvaru $fK[H]$ pro nějaké zobrazení $f : N \times M \to Y$. Člen $v(\mathcal{O})$ je určen jako člen $v(f)$, a tento poslední člen je definován jako součin proměnných

$$v(f) = \prod_{a \in M,\, p \in N} x_{f(p,a)}.$$

Rozepišme tento součin ve tvaru

$$v(f) = \prod_{p \in N} \Big(\prod_{a \in M} x_{f(p,a)} \Big).$$

Zavedeme-li stejně jako výše zobrazení $f_p : M \to Y$ pro všechna $p \in N$ předpisem $f_p(a) = f(p, a)$ pro všechna $a \in M$, můžeme poslední součin ještě přepsat ve tvaru

$$v(f) = \prod_{p \in N} \Big(\prod_{a \in M} x_{f_p(a)} \Big).$$

Vnitřní součin v závorkách lze ale nyní vnímat jako člen $v(f_p)$, a to je člen $v(f_p H)$, kde $f_p H$ je orbita zobrazení f_p v podgrupě E^H. To je ale orbita v množině $\mathfrak{M}_{Y^M,H}$. Dostáváme tak vyjádření

$$v(f) = \prod_{p \in N} v(f_p).$$

Podle našeho dřívějšího zjištění máme vzájemně jednoznačnou korespondenci $\chi : \mathfrak{M}_{Y^{N \times M},K[H]} \to \mathfrak{M}_{\mathfrak{Y}^N,K}$ danou formulí $\chi(fK[H]) = \widetilde{f} K$.

Naší shora vybrané orbitě $\mathcal{O}$ z množiny $\mathfrak{M}_{Y^{N\times M},K[H]}$ tak odpovídá orbita $\chi(\mathcal{O})$ z množiny $\mathfrak{M}_{\mathfrak{Y}^N,K}$. Naše původní orbita $\mathcal{O}$ byla tvaru $fK[H]$ pro nějaké zobrazení f, naše nynější orbita $\chi(\mathcal{O})$ je tvaru $\widetilde{f}K$ pro totéž zobrazení f. Připomeňme, že zobrazení $\widetilde{f} : N \to \mathfrak{M}_{Y^M,H}$ je dáno pro každé $p \in N$ předpisem $\widetilde{f}(p) = f_p H$. Přiřaďme nyní každé orbitě $\mathcal{R}$ v množině $\mathfrak{M}_{Y^M,H}$ nějakou novou proměnnou $\overline{x}_{\mathcal{R}}$. Pak bychom mohli uvažovat pro zobrazení $\widetilde{f}$ o členu

$$\overline{v}(\widetilde{f}) = \prod_{p\in N} \overline{x}_{\widetilde{f}(p)}.$$

Tento člen $\overline{v}(\widetilde{f})$ by bylo možno vzít jako člen $\overline{v}(\chi(\mathcal{O}))$. Tím by však byl definován člen $\overline{v}(\mathcal{Q})$ pro každou orbitu $\mathcal{Q} \in \mathfrak{M}_{\mathfrak{Y}^N,K}$. Dále bychom mohli zavést enumerátor

$$\overline{\gamma}(\mathfrak{Y}^N, K) = \sum_{\mathcal{Q}\in\mathfrak{M}_{\mathfrak{Y}^N,K}} \overline{v}(\mathcal{Q}).$$

Pro tento enumerátor bychom pak ovšem měli rovnost

$$\overline{\gamma}(\mathfrak{Y}^N, K) = \sum_{\mathcal{O}\in\mathfrak{M}_{Y^{N\times M},K[H]}} \overline{v}(\chi(\mathcal{O})).$$

Podle Pólyovy věty pro tento enumerátor platí rovnost

$$\overline{\gamma}(\mathfrak{Y}^N, K) = Z(K; \overline{s}_1, \overline{s}_2, \ldots, \overline{s}_n),$$

kde pro každé $\ell = 1, 2, \ldots, n$ je $\overline{s}_\ell = \sum_{\mathcal{R} \in \mathfrak{M}_{Y^M,H}} \overline{x}_{\mathcal{R}}^\ell$. Porovnejme nyní mezi sebou enumerátory $\gamma(Y^{N\times M}, K[H])$ ve vyjádření uvedeném zkraje tohoto důkazu a $\overline{\gamma}(\mathfrak{Y}^N, K)$ ve vyjádření uvedeném v předminulé formuli. V obou případech se sčítá přes všechny orbity $\mathcal{O} \in \mathfrak{M}_{Y^{N\times M}, K[H]}$. V prvním případě se sčítají členy $v(\mathcal{O})$, ve druhém případě se sčítají členy $\overline{v}(\chi(\mathcal{O}))$. Je-li orbita $\mathcal{O}$ tvaru $fK[H]$ pro nějaké zobrazení f, pak orbita $\chi(\mathcal{O})$ je tvaru $\widetilde{f}K$ pro totéž zobrazení f. Příslušný člen $v(\mathcal{O})$ je pak roven členu $v(fK[H])$, to jest členu $v(f)$, kdežto člen $\overline{v}(\chi(\mathcal{O}))$ je pak roven členu $\overline{v}(\widetilde{f}K)$, to jest členu $\overline{v}(\widetilde{f})$. Konečně porovnejme nyní mezi sebou tyto členy $v(f)$ a $\overline{v}(\widetilde{f})$ ve vyjádřeních uvedených výše v tomto důkazu:

$$v(f) = \prod_{p \in N} v(f_p) \qquad \text{a} \qquad \overline{v}(\widetilde{f}) = \prod_{p \in N} \overline{x}_{\widetilde{f}(p)}.$$

Vidíme, že člen $v(f)$ vznikne dosazením členů $v(f_p)$ za proměnné $\overline{x}_{\widetilde{f}(p)}$ do člene $\overline{v}(\widetilde{f})$ pro všechna $p \in N$. Je třeba zde ovšem připomenout, že $v(f_p) = v(f_p H)$ a $\widetilde{f}(p) = f_p H$, kde $f_p H$ je orbita zobrazení f_p v podgrupě E^H, tedy orbita v množině $\mathfrak{M}_{Y^M,H}$. Navíc odtud vyplývá následující závěr.

Poslední pozorování ohledně dosazování lze přeformulovat následovně. Člen $v(f)$ vznikne dosazením členů $v(\mathcal{R})$ za proměnné $\overline{x}_{\mathcal{R}}$ do člene $\overline{v}(\widetilde{f})$ pro všechny orbity $\mathcal{R} \in \mathfrak{M}_{Y^M,H}$. Provedeme-li toto dosazení ve všech sčítancích enumerátoru $\overline{\gamma}(\mathfrak{Y}^N, K)$, dospějeme nakonec k závěru, že enumerátor $\gamma(Y^{N\times M}, K[H])$ vznikne dosazením členů $v(\mathcal{R})$ za proměnné $\overline{x}_{\mathcal{R}}$ do enumerátoru $\overline{\gamma}(\mathfrak{Y}^N, K)$ pro všechny orbity $\mathcal{R} \in \mathfrak{M}_{Y^M,H}$. Vraťme se nyní k výše uvedenému vztahu vyjadřujícímu enumerátor $\overline{\gamma}(\mathfrak{Y}^N, K)$ prostřednictvím cyklového indexu $Z(K)$ grupy K a prostřednictvím sum mocnin proměnných $\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_n$. Dosadíme-li pro dané $\ell = 1, 2, \ldots, n$ členy $v(\mathcal{R})$ za proměnné $\overline{x}_{\mathcal{R}}$ do polynomu $\overline{s}_\ell$ pro všechny orbity $\mathcal{R} \in \mathfrak{M}_{Y^M,H}$, přejde tak polynom $\overline{s}_\ell$ v sumu $\sum_{\mathcal{R}\in\mathfrak{M}_{Y^M,H}} v^\ell(\mathcal{R})$. Pro $\ell = 1$ se jedná o sumu $\sum_{\mathcal{R}\in\mathfrak{M}_{Y^M,H}} v(\mathcal{R})$. To je ale podle definice enumerátoru právě enumerátor $\gamma(Y^M, H)$. Pro něj podle Pólyovy věty máme rovnost

$$\gamma(Y^M, H) = Z(H; s_1, s_2, \ldots, s_m).$$

Pro obecné $\ell = 1, 2, \ldots, n$ pak vznikne suma $\sum_{\mathcal{R}\in\mathfrak{M}_{Y^M,H}} v^\ell(\mathcal{R})$ ze sumy $\sum_{\mathcal{R}\in\mathfrak{M}_{Y^M,H}} v(\mathcal{R})$ dosazením mocnin proměnných $x_1^\ell, x_2^\ell, \ldots, x_\eta^\ell$ za proměnné $x_1, x_2, \ldots, x_\eta$. To znamená, že suma $\sum_{\mathcal{R}\in\mathfrak{M}_{Y^M,H}} v^\ell(\mathcal{R})$ vznikne takovýmto dosazením z enumerátoru $\gamma(Y^M, H)$.

Vzhledem k předchozímu vyjádření enumerátoru $\gamma(Y^M, H)$ to pak má za následek, že dotyčná suma je rovna polynomu

$$Z(H; s_\ell, s_{2\ell}, \ldots, s_{m\ell}).$$

Celkem to znamená, že enumerátor $\gamma(Y^{N\times M}, K[H])$ vznikne nahrazením polynomů $\bar{s}_1, \bar{s}_2, \ldots, \bar{s}_n$ v enumerátoru $\overline{\gamma}(\mathfrak{Y}^N, K)$ postupně polynomy $Z(H; s_1, s_2, \ldots, s_m)$, $Z(H; s_2, s_4, \ldots, s_{2m})$, $\ldots$, $Z(H; s_n, s_{2n}, \ldots, s_{mn})$. Vzhledem k výše uvedené podobě enumerátoru $\overline{\gamma}(\mathfrak{Y}^N, K)$ to ale říká, že enumerátor $\gamma(Y^{N\times M}, K[H])$ vznikne dosazením polynomů $Z(H; s_1, s_2, \ldots, s_m)$, $Z(H; s_2, s_4, \ldots, s_{2m})$, $\ldots$, $Z(H; s_n, s_{2n}, \ldots, s_{mn})$ za proměnné $t_1, t_2, \ldots, t_n$ do polynomu $Z(K; t_1, t_2, \ldots, t_n)$. To je ale ta skutečnost, kterou bylo potřeba dokázat. $\square$