Burnsideovo lemma

Buď M konečná neprázdná množina. Buď S_M grupa všech permutací množiny M. Buď H nějaká podgrupa grupy S_M. Označme $\sim_H$ binární relaci na množině M definovanou pro libovolná $a, b \in M$ předpisem

$$a \sim_H b \Longleftrightarrow \text{existuje permutace } \sigma \in H \text{ taková, že } b = \sigma(a).$$

Snadno se ověří, že $\sim_H$ je relace ekvivalence na množině M. Vzniká tak příslušný rozklad $M/{\sim_H}$. Třídy tohoto rozkladu se nazývají orbity v grupě H. Pro libovolný prvek $a \in M$ je třída rozkladu $M/{\sim_H}$ obsahující tento prvek a rovna množině

$$0_H(a) = \{\sigma(a) : \sigma \in H\}$$

a nazývá se orbita prvku a v grupě H. Uvažujme dále pro libovolný prvek $a \in M$ podmnožinu

$$H(a) = \{\sigma \in H : \sigma(a) = a\}$$

grupy H. Pak $H(a)$ je očividně podgrupa grupy H a nazývá se stabilizátor prvku a v grupě H. Uvažujme konečně pro libovolný prvek $a \in M$ zobrazení

$$\psi_a : H \to 0_H(a)$$

dané pro libovolnou permutaci $\sigma \in H$ předpisem

$$\psi_a(\sigma) = \sigma(a).$$

Pak ψ_a je surjektivní zobrazení. Zkoumejme jádro tohoto zobrazení. Pro libovolné dvě permutace $\sigma, \tau \in H$ máme

$$\psi_a(\sigma) = \psi_a(\tau) \iff \sigma(a) = \tau(a) \iff \tau^{-1}(\sigma(a)) = a$$
$$\iff \tau^{-1} \circ \sigma \in H(a) \iff \sigma \circ H(a) = \tau \circ H(a).$$

Poslední rovnost je ovšem rovností tříd levého rozkladu grupy H podle její podgrupy $H(a)$. Dvě permutace $\sigma, \tau \in H$ se tedy zobrazením ψ_a zobrazí na tentýž prvek $\sigma(a) = \tau(a)$ orbity $0_H(a)$ právě tehdy, když tyto permutace σ, τ leží v téže třídě levého rozkladu $H/H(a)$. Indukuje tedy zobrazení ψ_a bijekci

$$\overline{\psi}_a : H/H(a) \to 0_H(a)$$

danou pro libovolnou permutaci $\sigma \in H$ předpisem

$$\overline{\psi}_a(\sigma \circ H(a)) = \sigma(a).$$

Je tedy počet prvků orbity $0_H(a)$ roven počtu tříd levého rozkladu $H/H(a)$ grupy H podle stabilizátoru $H(a)$. Z kurzu algebry víme, že pro počet prvků podgrupy $H(a)$ a pro počet tříd levého rozkladu $H/H(a)$ platí rovnost

$$|H/H(a)| \cdot |H(a)| = |H|.$$

To ale znamená, že máme rovnost

$$|0_H(a)| \cdot |H(a)| = |H|.$$

Z této rovnosti mimo jiné plyne, že pro dva prvky $a, b \in M$ ležící v téže orbitě grupy H, což znamená, že $0_H(a) = 0_H(b)$, platí též rovnost $|H(a)| = |H(b)|$, čili stabilizátory $H(a)$ a $H(b)$ takových prvků jsou podgrupami v H majícími týž počet prvků.

Naší snahou bude určit počet všech orbit v grupě H, to jest počet tříd rozkladu $M/{\sim_H}$. Pro libovolnou permutaci σ množiny M označíme symbolem $j_1(\sigma)$ počet všech cyklů délky 1 v rozkladu permutace σ na součin nezávislých cyklů. Jinými slovy, $j_1(\sigma)$ bude počet všech pevných bodů permutace σ, to jest počet prvků množiny $P_\sigma = \{a \in M : \sigma(a) = a\}$.

Nyní jsme již připraveni formulovat a dokázat následující Burnsideovo lemma, někdy nazývané též Cauchyovo-Frobeniovo lemma:

Věta.

Buď H podgrupa v grupě S_M. Pak pro počet orbit v této grupě H, to jest pro počet tříd rozkladu $M/{\sim_H}$, platí vztah

$$|M/{\sim_H}| = \frac{1}{|H|} \sum_{\sigma \in H} j_1(\sigma).$$

Řečeno slovy, počet orbit v grupě H je roven průměrnému počtu pevných bodů permutací z grupy H.

Důkaz.

Uvedená rovnost je ekvivalentní rovnosti

$$|M/\sim_H| \cdot |H| = \sum_{\sigma \in H} j_1(\sigma),$$

kterou tedy máme dokázat. K tomu účelu uvažme množinu

$$W = \{(\sigma, a) : \sigma \in H,\ a \in M,\ \sigma(a) = a\}.$$

Nyní použijeme následující obrat: budeme počítat velikost množiny W dvěma způsoby. Poprvé bereme jednotlivé permutace $\sigma \in H$ a ke každé z nich zjistíme, kolik je možno vzít prvků $a \in M$ tak, aby vznikla dvojice (σ, a) z W, to jest tak, aby platilo $\sigma(a) = a$. Tímto způsobem dospějeme k zjištění, že

$$|W| = \sum_{\sigma \in H} |P_\sigma| = \sum_{\sigma \in H} j_1(\sigma).$$

Podruhé bereme jednotlivé prvky $a \in M$ a ke každému z nich zjistíme, kolik je možno vzít permutací $\sigma \in H$ tak, aby vznikla dvojice (σ, a) z W, to jest zase tak, aby platilo $\sigma(a) = a$. Tímto způsobem dojdeme k zjištění, že

$$|W| = \sum_{a \in M} |H(a)|.$$

Ovšem víme již, že stabilizátory prvků z téže orbity grupy H mají týž počet prvků. Roztřídíme-li tedy prvky $a \in M$ podle toho, do kterých orbit $\mathcal{O}$ grupy H náležejí, můžeme poslední vyjádření velikosti množiny W přepsat ve tvaru

$$|W| = \sum_{\mathcal{O} \in M/\sim_H} |0_H(u_{\mathcal{O}})| \cdot |H(u_{\mathcal{O}})|,$$

kde $u_{\mathcal{O}}$ je některý (kterýkoliv) prvek orbity $\mathcal{O}$. Pak ovšem $0_H(u_{\mathcal{O}})$ je $\mathcal{O}$. Podle poslední rovnosti odvozené bezprostředně před touto větou jsou ovšem součiny $|0_H(u_{\mathcal{O}})| \cdot |H(u_{\mathcal{O}})|$ rovny hodnotě $|H|$. Dospíváme tak ke zjištění, že

$$|W| = \sum_{\mathcal{O} \in M/\sim_H} |H| = |M/\sim_H| \cdot |H|.$$

Celkem odtud a z předchozího odvození vyplývá, že

$$|M/\sim_H| \cdot |H| = \sum_{\sigma \in H} j_1(\sigma),$$

což bylo třeba dokázat. □