Teoremele lui Sylow - o demonstraţie ghidată

lect.dr. Mihai Chiş
Facultatea de Matematică şi Informatică
Universitatea de Vest din Timişoara

Viitori Olimpici ediţia a 10-a, etapa a 4-a, clasa a XII-a

Definiţie 1. Fie $(G,\cdot)$ un grup finit şi p un număr prim. Dacă p^k este cea mai mare putere a lui p care divide ordinul $|G|$ al grupului G, un subgrup de ordin p^k al lui G se numeşte un $p-$subgrup Sylow al lui G. Mulţimea $p-$subgrupurilor Sylow ale lui G se notează $Syl_p(G)$.

I. În problemele 1-18, G este un grup finit de ordin $n = p^a \cdot m$, iar $\mathcal{A} = \{S | S \subseteq G, |S| = p^a\}$ este mulţimea submulţimilor cu p^a elemente ale lui G.

P 1. Arătaţi că $|\mathcal{A}| = C_n^{p^a} = \left(\begin{array}{c} n \\ p^a \end{array}\right)$.

P 2. Funcţia $\alpha : \mathcal{A} \times G \longrightarrow \mathcal{A} : (S, g) \longmapsto S \cdot g$ este o acţiune la dreapta a grupului G pe mulţimea $\mathcal{A}$.

P 3. Fie $\mathcal{R} = \{S_i | i \in I\}$ un sistem de reprezentanţi ai orbitelor acţiunii de mai sus şi $\mathcal{A}_i$ orbita mulţimii S_i. Atunci $|\mathcal{A}| = \sum\limits_{i \in I} |\mathcal{A}_i|$.

P 4. Dacă $U_i = Stab_G(S_i)$, atunci $|\mathcal{A}_i| = [G : U_i]$.

P 5. Deoarece $S_i \cdot U_i = S_i$, rezultă că $S_i = \bigcup\limits_{j=1}^{k_i} g_{ij} \cdot U_i$.

P 6. Deoarece $p^a = |S_i| = k_i \cdot |U_i|$, rezultă că $|U_i| | p^a$,

P 7. Dacă $|U_i| < p^a$, atunci $|\mathcal{A}_i| \equiv 0 \pmod{p \cdot m}$.

P 8. Dacă $|U_i| = p^a$, atunci $|\mathcal{A}_i| = m$.

P 9.

$$|\mathcal{A}| = \left(\begin{array}{c} n \\ p^a \end{array}\right) \equiv \sum_{|\mathcal{A}_i| = m} |\mathcal{A}_i| \pmod{p \cdot m}.$$

P 10. $|\mathcal{A}_i| = m \Longleftrightarrow |U_i| = p^a \Longrightarrow (\exists) g_i \in S_i : S_i = g_i \cdot U_i \Longrightarrow V_i = S_i \cdot g_i^{-1} = g_i \cdot U_i \cdot g_i^{-1} \leq G$; $|V_i| = p^a$, $\mathcal{A}_i = \{V_i \cdot g | g \in G\}$.

P 11. Dacă $V \leq G$, $|V| = p^a$, atunci $\mathcal{S} = \{V \cdot g | g \in G\} \subseteq \mathcal{A}$ este o orbită a acţiunii α, cu $|\mathcal{S}| = m$.

P 12. Dacă $V_i, V_j \leq G$, $|V_i| = |V_j| = p^a$ şi $V_i \neq V_j$, atunci $\mathcal{A}_i \neq \mathcal{A}_j$.

P 13. Notând cu $N(p^a)$ numărul subgrupurilor cu p^a elemente ale grupului G, rezultă că

$$m \cdot n(p^a) = \sum_{|\mathcal{A}_i|=m} |\mathcal{A}_i| \equiv \binom{n}{p^a} \pmod{p \cdot m}.$$

P 14. Dacă G este un grup ciclic, atunci $N(p^a) = 1$, astfel că

$$\binom{n}{p^a} \equiv m \cdot 1 \pmod{p \cdot m}.$$

P 15. În general, rezultă că $m \cdot N(p^a) \equiv m \cdot 1 \pmod{p \cdot m}$, de unde

$$N(p^a) \equiv 1 \pmod{p}.$$

P 16. În particular, $n_p = |Syl_p(G)| \equiv 1 \pmod{p}$.

P 17.

$$Syl_p(G) \neq \emptyset.$$

P 18. $p|\,|G| \Longrightarrow N(p) \geq 1 \Longrightarrow (\exists) g \in G : ord(g) = p$.

II. Fie G un grup finit, cu $|G| = n = p^a \cdot m$, unde p este un număr prim, iar $(m, p) = 1$, $P \in Syl_p(G)$ şi $U \leq G$ cu $|U| = p^b$, $b \leq a$.

P 19. $(\exists) T \subseteq G :$

$$G = \dot{\bigcup_{x \in T}} PxU.$$

P 20. $|PxU| = |P^x \cdot U| = \frac{|P^x| \cdot |U|}{|P^x \cap U|} = |P| \cdot [U : P^x \cap U]$.

P 21. $|G| = |P| \cdot \sum\limits_{x \in T} [U : P^x \cap U]$.

P 22. $\sum\limits_{x \in T} [U : P^x \cap U] = [G : P] \not\equiv 0 \pmod{p}$.

P 23. $(\exists) x \in G : \; [U : P^x \cap U] \not\equiv 0 \pmod{p}$.

P 24. $(\exists) x \in G : \; U = P^x \cap U \leq P^x$.

P 25. $(\forall) P_1, P_2 \in Syl_p(G) (\exists) x \in G : P_1^x = P_2$.

P 26. $(\forall) P \in Syl_p(G) \Longrightarrow Syl_p(G) = \{P^x | \, x \in G\}$.

P 27. $(\forall) P \in Syl_p(G) \Longrightarrow |Syl_p(G)| = [G : N_G(P)]$.

P 28. $n_p = |Syl_p(G)| \mid |G|$, $n_p \equiv 1 \pmod{p}$.