

W twierdzeniach Sylowa zakładamy, że G jest skończoną grupą rzędu n , zaś p^k jest najwyższą potęgą liczby pierwszej p dzielącą n . Twierdzenia Sylowa mówią, że G ma podgrupy rzędu p^k , że są one parami sprzężone, a ich liczba dzieli rząd G i przystaje do 1 modulo p .

Tw.(Sylow 1) G ma podgrupę rzędu p^k .

Rozważamy działanie G przez lewe przesunięcia na p^k -elementowych podzbiorach G . Liczba takich podzbiorów nie dzieli się przez p , zatem istnieje orbita – powiedzmy, zbioru U – której rząd nie dzieli się przez p . Wtedy stabilizator U ma rząd podzielny przez p^k ; ale też ma on nie więcej elementów niż U – czyli jego rząd to p^k .

Podgrupa G rzędu p^k to jej p -podgrupa Sylowa. Grupa, której rząd jest potęgą p , to p -grupa.

Tw.(Sylow 2) p -podgrupa G jest zawarta w pewnej p -podgrupie Sylowa. Każde dwie p -podgrupy Sylowa są sprzężone.

Pokażemy, że jeśli $K < G$ i p dzieli rząd K , a H jest p -podgrupą Sylowa G , to dla pewnego $g \in G$ przekrój $gHg^{-1} \cap K$ jest p -podgrupą Sylowa w K .

Rozważamy lewe działanie K na G/H . Pewna orbita $K \cdot gH$ ma rząd niepodzielny przez p . Stabilizator K_{gH} dzieli się więc przez tę samą potęgę p , co i rząd K . Ten stabilizator to $K \cap gHg^{-1}$; jego rząd dzieli także rząd H , czyli jest potęgą p .

Normalizator $N_G(H)$ podgrupy H w grupie G to jej stabilizator przy działaniu G na sobie przez sprzężenia. Jest on równy G jeśli H jest dzielnikiem normalnym, a zawsze zawiera H jako podgrupę.

Tw.(Sylow 3) Liczba p -podgrup Sylowa dzieli rząd G i przystaje do 1 modulo p .

Pierwsza teza wynika z Sylowa 2: p -podgrupy Sylowa stanowią orbitę działania G na sobie przez sprzężenia. Teraz patrzymy, jak na zbiorze p -podgrup Sylowa działa przez sprzężenia jedna z nich (H). Nie może ona stabilizować żadnej innej H' : inaczej obie one byłyby p -podgrupami Sylowa normalizatora H' ; ale ten normalizator normalizuje H' , więc H' i H nie są w nim sprzężone.

Twierdzenia Sylowa dostarczają p -podgrup dla czynników pierwszych p rzędu grupy, a także restrykcji na ich liczbę – czasem pozwalają pokazać jedyność p -podgrupy Sylowa. Dla różnych p podgrupy Sylowa kroją się trywialnie. Aby z tego typu informacji wnioskować o strukturze G , użyjemy lematu.

Lemat. Niech $N, H < G$ kroją się trywialnie. Wtedy

- odwzorowanie wymnożenia składowych $m: N \times H \rightarrow G$ jest różnowartościowe;
- jeśli N jest dzielnikiem normalnym G , to NH – obraz m – jest podgrupą;
- jeśli N i H są normalne w G , to komutują ze sobą i m jest izomorfizmem grupy produktowej $N \times H$ na NH .

Rachunek do b): $nhn'h' = n(hn'h^{-1})hh'$.

Komutowanie w c) widać tak: $nhn^{-1}h^{-1} = (nhn^{-1})h^{-1} = n(hn^{-1}h^{-1})$ plus $N \cap H = \{e\}$.

Przeanalizujemy dokładniej sytuację b): m dostarcza parametryzacji podgrupy NH przez produkt $N \times H$. Jak w tej parametryzacji wygląda działanie grupowe G widać z rachunku: $nh \cdot n'h' = n(hn'h^{-1})hh' = n\iota_h(n') \cdot hh'$. Jeśli więc na produkcie zadać mnożenie wzorem $(n, h) \cdot (n', h') = (n\iota_h(n'), hh')$, to m stanie się izomorfizmem. Inaczej mówiąc, NH jest *produktem półprostym*:

Def. Niech $\varphi: H \rightarrow \text{Aut}(N)$ będzie działaniem grupy H na grupie N przez automorfizmy. *Produktem półprostim* N i H nazywamy grupę $N \rtimes_{\varphi} H = (N \times H, \cdot_{\varphi})$, gdzie $(n, h) \cdot_{\varphi} (n', h') = (n\varphi_h(n'), hh')$.

Przykłady.

0) Jeśli rząd G jest liczbą pierwszą p , to $G \simeq \mathbf{Z}/p$.

1) $|G| = 15$. Wtedy G ma jedyną 3-podgrupę Sylowa i jedyną 5-podgrupę Sylowa; są one normalne w G , zatem G jest ich produktem: $G \simeq \mathbf{Z}/3 \times \mathbf{Z}/5$.

2) $|G| = 21$. Wtedy G ma jedyną 7-podgrupę Sylowa $\mathbf{Z}/7 = \langle x \rangle$, i 1 lub 7 3-podgrup Sylowa $\mathbf{Z}/3 = \langle y \rangle$. W pierwszym przypadku mamy $G \simeq \mathbf{Z}/7 \times \mathbf{Z}/3$; w drugim $G \simeq \mathbf{Z}/7 \rtimes_{\varphi} \mathbf{Z}/3$. Możliwe φ to $\varphi_y(x) = x^2$ i $\varphi_y(x) = x^4$, przy czym nietrywialny automorfizm $\mathbf{Z}/3$ zamienia rolami te dwie możliwości. Są więc dwie grupy rzędu 21.

3) $|G| = 12$.

Jeśli są 4 3-podgrupy Sylowa, to G działa przez sprzężenia na ich zbiorze; dostajemy homomorfizm $G \rightarrow S_4$. G jest generowana przez elementy rzędu 3 (jest ich razem 8), zatem obraz G jest generowany przez 3-cykle i zawarty w A_4 . Jądro rozważanego homomorfizmu to przekrój normalizatorów 3-podgrup Sylowa; ale normalizator takiej podgrupy jest równy niej samej (bo ma ona 4 różne sprzężenia), więc to jądro jest trywialne i $G \simeq A_4$.

Jeśli jest jedna 3-podgrupa Sylowa, to G jest jej produktem przez $\mathbf{Z}/4$ lub $\mathbf{Z}/2 \times \mathbf{Z}/2$, prostym lub półprostym (półprosty w każdym przypadku jest jednoznaczny z dokładnością do izomorfizmu).