5. Podgrupy normalne i grupy ilorazowe

Niech $\varphi : G \longrightarrow H$ będzie homomorfizmem. Rozpatrzmy zbiór warstw lewostronnych $G/\ker\varphi$ grupy G względem podgrupy $\ker\varphi$. Łatwo zauważyć, że

$$\varphi(x) = \varphi(y) \iff x^{-1}y \in \ker\varphi \iff x\ker\varphi = y\ker\varphi$$

— homomorfizm φ przeprowadza dwa elementy grupy G na ten sam element grupy H wtedy i tylko wtedy, gdy te dwa elementy wyznaczają tę samą warstwę lewostronną. Wynika stąd następujący wniosek:

5.1. Wniosek. *Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem, to*

$$|\operatorname{im}\varphi| = [G : \ker\varphi].$$

Załóżmy teraz, że φ jest *epimorfizmem.* Wówczas $\varphi : G \longrightarrow H$ wyznacza bijekcję $\bar{\varphi} : G/\ker\varphi \longrightarrow H$ (określoną wzorem $\bar{\varphi}(x\ker\varphi) = \varphi(x)$) zbioru $G/\ker\varphi$ i zbioru elementów grupy H. Na zbiorze warstw $G/\ker\varphi$ można więc w naturalny sposób zdefiniować działania, tak by bijekcja $\bar{\varphi}$ stała się izomorfizmem grup. Łatwo sprawdzić, że działania te są określone następującymi wzorami:

$$\begin{aligned}(x\ker\varphi)\cdot(y\ker\varphi) &= xy\ker\varphi,\\ (x\ker\varphi)^{-1} &= x^{-1}\ker\varphi,\end{aligned}$$

a elementem neutralnym jest warstwa $1\ker\varphi$ (czyli po prostu $\ker\varphi$).

Uwaga. Jeżeli założymy tylko tyle, że H jest podgrupą grupy G, to wzór $xH\cdot yH = xyH$ na ogół nie ma sensu, bo warstwa występująca po prawej stronie zależy od wyboru reprezentantów warstw występujących po lewej stronie. Można się o tym przekonać rozpatrując na przykład zbiór warstw $D_6/\{1,\varepsilon\}$.

Zdefiniujemy teraz taką klasę podgrup, dla których powyższy wzór *ma* sens.

5.2. Definicja. *Podgrupę $H \leqslant G$ nazywamy* **podgrupą normalną** *(lub* **dzielnikiem normalnym***), co oznaczamy symbolem $H \trianglelefteq G$, wtedy i tylko wtedy, gdy dla każdego $g \in G$, $gHg^{-1} = \{ghg^{-1} : h \in H\} = H$, czyli dla każdego automorfizmu wewnętrznego ϕ_g grupy G zachodzi równośc $\phi_g(H) = H$.*

5.3. Uwaga. *Warunek $\forall_{g\in G}\ gHg^{-1} = H$, jest równoważny warunkowi $\forall_{g\in G}\ gHg^{-1} \subseteq H$.*

Dowód. Wystarczy przeprowadzić łatwy rachunek. Niech $h \in H$. Wówczas $h = (gg^{-1})h(gg^{-1}) = g(g^{-1}hg)g^{-1} \in gHg^{-1}$, a zatem $H \subseteq gHg^{-1}$ (a zawieranie w drugą stronę jest bezpośrednio zagwarantowane w założeniu). $\square$

5.4. Uwaga. *Warunek $H \trianglelefteq G$ jest równoważny warunkowi $\forall_{g\in G}\ gH = Hg$, czyli równości warstw prawostronnych i lewostronnych.*

Przykłady podgrup normalnych.

5.5. Przykład. $\mathbf{1} \trianglelefteq G$, $G \trianglelefteq G$

5.6. Przykład. Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem, to $\ker\varphi \trianglelefteq G$. Ten, jak się okaże uniwersalny, przykład ma wiele ważnych podprzykładów:

a) $Z(G) \trianglelefteq G$, gdzie $Z(G) = \ker\,\phi$, $\phi : G \longrightarrow Aut(G)$

b) $SO(n) \trianglelefteq O(n)$, gdzie $SO(n) = \ker\, det$, $det : O(n) \longrightarrow \mathbb{Z}_2$. Skonstruujemy najpierw monomorfizm $\Psi : \Sigma_n \longrightarrow GL(n, \mathbb{R})$. Wybieramy bazę uporządkowaną $e_1, \ldots, e_n$ w $\mathbb{R}^n$ i określamy $\Psi(\sigma)$ jako przekształcenie liniowe, które permutuje elementy bazy tak jak każe σ, to jest $\Psi(\sigma)(e_i) = e_{\sigma(i)}$. Wyznacznik macierzy takiego przekształcenia jest równy ± 1. Zatem mamy homomorfizm $det \circ \Psi : \Sigma_n \longrightarrow \{-1, 1\} \leqslant \mathbb{R}^*$

5.7. Definicja. *Permutację nazywamy* **permutacją parzystą,** *jeżeli należy do jądra homomorfizmu* $\det \circ \Psi$*. W przeciwnym przypadku permutację nazywamy* **permutacją nieparzystą.** *Podgrupę permutacji parzystych grupy* Σ_n *oznaczamy symbolem* A_n*.*

Jako jądro pewnego homomorfizmu podgrupa $A_n \leq \Sigma_n$ jest oczywiście normalna w Σ_n. Z twierdzenia o izomorfizmie wynika, że dla $n \geq 2$, $\Sigma_n / A_n \cong \mathbb{Z}_2$.

Ponadto złożenie

✓ dwóch permutacji parzystych jest permutacją parzystą,
✓ dwóch permutacji nieparzystych jest permutacją parzystą,
✓ permutacji parzystej i permutacji nieparzystej jest permutacją nieparzystą.

Zbadamy parzystość cykli. Jest jasne, że cykl długości 2, czyli transpozycja, jest permutacją nieparzystą — wynika to z algorytmu liczenia wyznacznika. Aby ocenić parzystość cyklu dowolnej długości odnotujmy najpierw następujący fakt.

5.8. Stwierdzenie. *Zachodzi równość:*

$$(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_3)(a_1, a_2).$$

□

5.9. Wniosek. *Cykl długości k jest permutacją parzystą jeżeli k jest liczbą nieparzystą, a permutacją nieparzystą jeżeli k jest liczbą parzystą. Jeżeli permutacja jest iloczynem cykli o długościach* $k_1, \ldots, k_s$*, to jest ona parzysta wtedy i tylko wtedy, gdy wśród liczb* $k_1, \ldots, k_s$ *jest parzyście wiele parzystych.* □

5.10. Przykład. Każda podgrupa grupy przemiennej jest normalna. (Ta własność nie charakteryzuje grup przemiennych — mają ją również niektóre grupy nieprzemienne).

5.11. Przykład. $1 \times K \trianglelefteq H \times K$ i $H \times 1 \trianglelefteq H \times K$.

5.12. Stwierdzenie. *Jeżeli* $H \leqslant G$ *i* $[G : H] = 2$*, to* $H \trianglelefteq G$*.*

Dowód. Oczywiście $\forall_{g \in H} \forall_{h \in H}\ ghg^{-1} \in H$. Pozostaje przypadek, gdy $g \notin H$. Przypuśćmy, że $\exists_{h \in H}\ ghg^{-1} \notin H$. Skoro tak, to $ghg^{-1} \in G \setminus H = gH$. Jak widać, elementy g i ghg^{-1} należą do tej samej warstwy (gH) względem podgrupy H. Ale to oznacza, że $g^{-1} \cdot ghg^{-1} \in H$. Po redukcji otrzymujemy $hg^{-1} \in H$, skąd $g \in H$, a to oznacza sprzeczność. □

Przykłady

a) Podgrupa obrotów $J = \{1, \rho, \ldots, \rho^{n-1}\}$ grupy dihedralnej D_{2n} jest dzielnikiem normalnym.

b) W nieprzemiennej grupie Q_8 każda podgrupa jest normalna,

Odnotujmy jeszcze następujące, łatwe do udowodnienia, własności podgrup normalnych:
1) Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem i $N \trianglelefteq H$, to $\varphi^{-1}(N) \trianglelefteq G$
2) Jeżeli $\varphi : G \longrightarrow H$ jest epimorfizmem i $N \trianglelefteq G$, to $\varphi(N) \trianglelefteq H$.
   Jeżeli o przekształceniu φ zakładamy tylko tyle, że jest homomorfizmem, to w każdym razie możemy twierdzić, że $\varphi(N) \trianglelefteq \mathrm{im}\,(\varphi)$.
3) Jeżeli $N_i \trianglelefteq G$ dla $i \in I$ to $\bigcap\limits_{i\in I} N_i \trianglelefteq G$.
4) Jeżeli $N \trianglelefteq G$ i $K \leqslant G$, to $N \cap K \trianglelefteq K$.

Wiemy, że jeżeli $K \leq H$ i $H \leq G$ to $K \leq G$. Czy jeżeli $K \trianglelefteq H$ i $H \trianglelefteq G$ to $K \trianglelefteq G$? **5.13. Przykład.** W grupie D_8, $\{1, \epsilon\} \trianglelefteq \{1, \rho^2, \epsilon, \epsilon\rho^2\}, \{1, \rho^2, \epsilon, \epsilon\rho^2\} \trianglelefteq D_8$, ale $\{1, \epsilon\}$ nie jest normalną podgrupą D_8.

5.14. Definicja. *Podgrupę $H \leqslant G$ nazywamy podgrupą* **charakterystyczną***, co oznaczamy symbolem $H \blacktriangleleft G$, wtedy i tylko wtedy, gdy dla każdego automorfizmu $\phi \in AutG$ grupy G zachodzi równość $\phi(H) = H$.*

Przykłady
a) Dla dowolnej grupy G jej centrum $Z(G)$ jest podgrupą charakterystyczną.
b) Dla dowolnej grupy G, $\Phi(G) \blacktriangleleft G$, gdzie $\Phi(G)$ jest częścią wspólną podgrup maksymalnych.
c) Każda podgrupa grupy cyklicznej jest charakterystyczna.

5.15. Stwierdzenie. *Jeżeli $K \blacktriangleleft H$ i $H \trianglelefteq G$ to $K \trianglelefteq G$.*

Dowód jest oczywisty.

Jeżeli $H \trianglelefteq G$, to z taką parą związana jest ważna konstrukcja grupy ilorazowej.

5.16. Definicja. *Niech $H \trianglelefteq G$.* **Grupą ilorazową** *grupy G przez podgrupę normalną H nazywamy zbiór warstw G/H z warstwą $1H$ jako elementem wyróżnionym i z działaniami:*

$$xH \cdot yH = xyH$$
$$(xH)^{-1} = x^{-1}H.$$

Należy sprawdzić, że działanie jest dobrze zdefiniowane, to znaczy nie zależy od wyboru reprezentantów warstw. Niech $xH = x'H$ i $yH = y'H$. Należy pokazać, że $xyH = x'y'H$. Założyliśmy, że $x^{-1}x' \in H$ i $y^{-1}y' \in H$, a chcemy wykazać że $(xy)^{-1}x'y' \in H$. Rozpatrzmy ciąg równości:

$$(xy)^{-1}x'y' = y^{-1}x^{-1}x'y' = y^{-1}x^{-1}x'yy^{-1}y' = \left(y^{-1}(x^{-1}x')y\right)(y^{-1}y').$$

Założyliśmy, że $H \trianglelefteq G$. Zatem $y^{-1}(x^{-1}x')y \in H$. Również $y^{-1}y' \in H$. Wobec tego $(xy)^{-1}x'y' \in H$. Analogicznie sprawdzamy, że działanie jednoargumentowe jest dobrze określone. Fakt, że tak określone działania spełniają aksjomaty grupy jest oczywisty.

Odnotujmy także stwierdzenie:

5.17. Stwierdzenie. *Jeżeli $H \trianglelefteq G$, to odwzorowanie $\pi : G \longrightarrow G/H$, określone wzorem $\pi(g) = gH$ jest epimorfizmem i* $\ker \pi = H$.

Epimomorfizm π nazywamy rzutowaniem grupy G na grupę ilorazową G/H.

5.18. Przykład. Grupa ilorazowa grupy cyklicznej $G = \langle g \rangle$ przez podgrupę H jest grupą cykliczną i oczywiście $G/H = \langle gH \rangle$

Przy pomocy grupy ilorazowej możemy opisać obraz dowolnego homomorfizmu.

5.19. Twierdzenie o homomorfizmie. *Niech $\varphi : G \longrightarrow H$ będzie homomorfizmem, a $\pi : G \longrightarrow G/\ker\varphi$ rzutowaniem. Wówczas istnieje dokładnie jeden monomorfizm $\tilde{\varphi} : G/\ker\varphi \longrightarrow H$, taki że $\tilde{\varphi} \circ \pi = \varphi$. W szczególności $\tilde{\varphi} : G/\ker\varphi \longrightarrow im\,\varphi$ jest izomorfizmem.*

Dowód. Szukanym monomorfizmem jest odwzorowanie ψ, określone wzorem $\psi(g\ker\varphi) = \varphi(g)$. □

Zanotujmy jeszcze przydatny wniosek z powyższego twierdzenia.

5.20. Wniosek. *Niech $\varphi : G \longrightarrow H$ będzie epimorfizmem i niech $K \trianglelefteq H$. Wówczas*

$$G/\varphi^{-1}(K) \cong H/K.$$

Dowód. Złożenie $G \xrightarrow{\varphi} H \xrightarrow{\pi_K} H/K$ (gdzie $\pi_K : H \longrightarrow H/K$ jest rzutowaniem) jest epimorfizmem, a jego jądrem jest $\varphi^{-1}(K)$. □

Twierdzenie o izomorfizmie leży u podstaw ważnego sposobu przedstawienia grupy. Niech $G =< A >$ i niech $F(A)$ będzie grupą słów o alfabecie A. Mamy naturalny epimorfizm $\varphi: F(A) \to G$. Zgodnie z twierdzeniem o izomorfizmie indukuje on izomorfizm $\tilde{\varphi} : F(A)/\ker\varphi \to G$. Niech $R \subset \ker\varphi$ będzie zbiorem generatorów $\ker\varphi$ **jako podgrupy normalnej**. Wówczas przedstawienie $G = \{A \mid R\}$ nazywamy przedstawieniem grupy przy pomocy generatorów i relacji.

5.21. Przykład. Niech $G = \mathbb{Z}_n$ i niech ρ będzie generatorem G. Wówczas $F(\rho) \cong \mathbb{Z}$, generatorem jądra jest ρ^n i piszemy $\mathbb{Z}_n = \{\rho \mid \rho^n\}$ lub stosowany jest też zapis $\mathbb{Z}_n = \{\rho \mid \rho^n = 1\}$

5.22. Przykład. Niech $G = \mathbb{Z} \times \mathbb{Z}$ (w zapisie addytywnym) i niech $a = (1, 0)$, $b = (0, 1)$. Mamy $F(\{a, b\}) \to \mathbb{Z} \times \mathbb{Z}$ i przedstawienie $\mathbb{Z} \times \mathbb{Z} = \{a, b \mid aba^{-1}b^{-1} = 1\}$.

5.23. Przykład. Niech $G = D_{2n} =< \rho, \epsilon >$. Przedstawienie w postaci generatorów i relacji grupy dihedralnej : $D_{2n} = \{\rho, \epsilon \mid \rho^n = 1, \epsilon^2 = 1, \epsilon\rho\epsilon\rho = 1\}$ lub równoważnie $D_{2n} = \{\rho, \epsilon \mid \rho^n = 1, \epsilon^2 = 1, \epsilon\rho\epsilon = \rho^{n-1}\}$.

Przedstawienie grupy w postaci generatorów i relacji nie jest jednoznaczne - zależy tak od wyboru generatorów grupy, jak i generatorów jądra . Rozstrzygnięcie, czy dwie grupy przedstawione przy pomocy generatorów i relacji są izomorficzne nie jest zadaniem łatwym, podobnie jak rozstrzygnięcie czy dane słowo jest elementem trywialnym.

Wróćmy do rozważania homomorfizmów. Na początek niech $\varphi : G \longrightarrow A$ będzie homomorfizmem i niech A będzie przemienna. Wówczas $\forall_{x,y \in G}\ x^{-1}y^{-1}xy \in \ker\varphi$. Element $x^{-1}y^{-1}xy$ nazywamy **komutatorem** elementów x i y i oznaczamy symbolem $[x, y]$. **Komutantem** grupy G nazywamy podgrupę

$$[G, G] = \langle \{[x, y] :\ x, y \in G\} \rangle.$$

5.24. Stwierdzenie. *Komutant jest podgrupą charakterystyczną.*

Dowód. Niech $\phi : G \to G$ będzie dowolnym automorfizmem grupy G. Wówczas $\phi([x,y]) = [\phi(x), \phi(y)]$. Wobec tego $\phi([G,G]) = [G,G]$. $\square$

Jest jasne, że grupa ilorazowa $G/[G,G]$ jest przemienna i że wśród podgrup normalnych grupy G podgrupa $[G,G]$ jest najmniejszą taką, że grupa ilorazowa jest przemienna. Grupę $G/[G,G]$ nazywamy **abelianizacją grupy** G. Jest to największa przemienna grupa ilorazowa grupy G. Precyzyjnie wyraża to następujące twierdzenie.

5.25. Twierdzenie. *Dla każdego homomorfizmu $\varphi : G \longrightarrow A$, gdzie A jest grupą przemienną, istnieje dokładnie jeden homomorfizm $\psi : G/[G,G] \longrightarrow A$, taki że $\psi \circ \pi = \varphi$ ($\pi : G \longrightarrow G/[G,G]$ jest rzutowaniem).*

Spróbujmy teraz znaleźć wszystkie homomorfizmy $G \longrightarrow H$, dla danych grup G i H lub przynajmniej obliczyć ile ich jest.
Umiemy to zadanie rozwiązać, gdy $G = \langle g \rangle$ jest grupą cykliczną — homomorfizm $\varphi : \langle g \rangle \longrightarrow H$ jest jednoznacznie wyznaczony przez wskazanie elementu $\varphi(g)$, takiego że $o(\varphi(g)) \mid o(g)$. Homomorfizmów jest więc dokładnie tyle ile elementów $h \in H$, takich że $o(h) \mid o(g)$.

W przypadku dowolnej grupy G zaczniemy od zbadania liczby epimorfizmów $G \longrightarrow K$ dla ustalonego K. Po pierwsze trzeba znaleźć wszystkich kandydatów na jądro takiego epimorfizmu, czyli wszystkie normalne podgrupy $N \trianglelefteq G$, takie że $G/N \cong K$. Nie ma tu żadnego algorytmu. Dwa epimorfizmy ϕ, ψ o tym samym jądrze N różnią się o automorfizm $\tilde{\phi}(\tilde{\psi})^{-1}$ grupy K — mamy bowiem $\phi = \tilde{\phi}\pi_N = \tilde{\phi}(\tilde{\psi})^{-1}\tilde{\psi}\pi_N = \tilde{\phi}(\tilde{\psi})^{-1}\psi$. Zatem liczba epimorfizmów $G \longrightarrow K$ jest równa $n_K \cdot |Aut(K)|$, gdzie n_K jest liczbą normalnych podgrup G, takich że grupa ilorazowa jest izomorficzna z K. Zanotujmy jeszcze, że $|Aut(\mathbb{Z}_n)| = \varphi(n)$.

5.26. Przykład. Niech $H \leqslant G$ będzie dowolną podgrupą. Rozpatrzymy znany nam homomorfizm $\phi : G \longrightarrow \Sigma_{G/H}$ zadany wzorem $\phi_g(xH) = gxH$, opisujący działanie G na zbiorze warstw G/H. Wówczas $\ker \phi = \bigcap_{g \in G} gHg^{-1} \leqslant H$ jest podgrupą normalną grupy G — jest to *największa ze względu na zawieranie podgrupa normalna grupy G, spośród tych, które są zawarte w H* nazywamy ją **rdzeniem** podgrupy H. Oczywiście jeżeli $H \trianglelefteq G$, to $H = \ker \phi$.

Informacja, że otrzymana podgrupa jest jądrem homomorfizmu ϕ jest użyteczna w dowodzie następującego wniosku.

5.27. Wniosek. *Niech H będzie podgrupą indeksu n w grupie skończonej G. Wówczas istnieje podgrupa normalna $N \trianglelefteq G$, $N \leq H$, taka że $n \big| [G:N]$ i $[G:N] \big| n!$ (tzn. indeks N w G jest wielokrotnością n, a dzielnikiem $n!$).*

Dowód. Szukaną grupą jest właśnie grupa $N = \ker \varphi$ opisana w przykładzie 5.26. Podzielność $n \big| [G:N]$ jest oczywista — indeks mniejszej podgrupy jest wielokrotnością indeksu większej podgrupy. Natomiast podzielność $[G:N] \big| n!$ wynika z faktu, że $|\operatorname{im} \varphi| = [G : \ker \phi] = [G:N]$ (Wniosek 5.1), z drugiej zaś strony $|\operatorname{im} \phi| \, \big| \, |\Sigma_{G/H}|$ (Twierdzenie Lagrange'a). $\square$

5.28. Przykład. Niech $H \leqslant G$. Zdefiniujmy podgrupę

$$N_G(H) = \{g \in G\colon\ gHg^{-1} = H\}.$$

Oczywiście $H \leqslant N_G(H) \leqslant G$ i $H \trianglelefteq N_G(H)$. Zauważmy, że $N_G(H)$ jest *największą taką podgrupą grupy G zawierającą H, w której H jest normalna.* Jest jasne, że jeżeli $H \trianglelefteq G$, to $N_G(H) = G$. Podgrupę $N_G(H)$ nazywamy **normalizatorem** H w G.

Jeżeli rozpatrzymy działanie grupy G na zbiorze jej podgrup, zadane przez automorfizmy wewnętrzne, to $N_G(H)$ jest grupą izotropii podgrupy H, a punktami stałymi tego działania są podgrupy normalne.

Grupy proste

Grupy, które mają mało podgrup normalnych są z pewnych względów szczególnie interesujące. Wobec tego odnotujmy w tym miejscu następującą definicję.

5.29. Definicja. *Niech G będzie nietrywialną grupą. Jeżeli jedynymi podgrupami normalnymi grupy G są G i podgrupa trywialna, to mówimy, że grupa G jest* **grupą prostą**.

Oczywistym przykładem grupy prostej jest dowolna grupa $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą. Grupy $\mathbb{Z}_p$ są jedynymi przemiennymi grupami prostymi. Grupy A_n (dla $n \geq 5$) również są proste (to już jest mniej oczywiste; pokażemy to dla $n = 5$). Grupy proste są jakby "nierozkładalnymi cegiełkami, z których zbudowane są inne grupy". Skończone grupy proste zostały sklasyfikowane. Dowód twierdzenia o klasyfikacji grup prostych był jednym z największych przedsięwzięć w historii matematyki i został zakończony w kwietniu 1981 roku. Jednym z najważniejszych jego kroków było twierdzenie Feita i Thompsona, z którego wynika, że rząd skończonej nieabelowej grupy prostej jest liczbą parzystą. Dowód tego twierdzenia, opublikowany w 1963 roku w pracy *Solvability of groups of odd order,* zajmuje 225 stron.

Na zakończenie tego rozdziału udowodnimy, że A_5 jest grupą prostą.

Przypomnijmy, że w dowolnej grupie G moc klasy sprzężoności elementu x jest równa $[G : C_G(x)]$. Zauważmy, że jeżeli dla permutacji $\sigma \in A_n$ jeżeli istnieje permutacja nieparzysta $\tau \in C_{\Sigma_n}$, to klasa sprzężoności σ w A_n jest tożsama z klasą sprzężoności σ w Σ_n. W przeciwnym przypadku klasa sprzężoności σ w Σ_n rozpada się na dwie równoliczne klasy sprzężoności σ w A_n.

Zaczniemy od policzenia ile jest klas sprzężoności elementów A_5 i ile elementów liczy każda klasa. W poniższej tabeli przedstawiamy możliwe typy rozkładów na cykle, rzędy centralizatorów, moce klas sprzężoności elementów każdego typu ($conj(x)$), liczby elementów o ustalonym typie rozkładu ($sim(x)$) i liczby klas sprzężoności elementów o danym typie rozkładu.

Tabela

rozkład na cykle	$\lvert C_{A_5}(x)\rvert$	$conj(x)$	$sim(x)$	liczba klas sprzężoności
(.)(.)(.)(.)(.)	60	1	1	1
(..)(..)(.)	4	15	15	1
(...)(.)(.)	3	20	20	1
(.....)	5	12	24	2

5.30. Twierdzenie. *Grupa A_5 jest prosta.*

Dowód. Podgrupa normalna (w każdej grupie) jest zawsze sumą mnogościową pewnych klas sprzężoności — bo jeżeli pewien element należy do tej podgrupy normalnej, to już cała jego klasa sprzężoności musi być w niej zawarta. Zatem rząd podgrupy normalnej musi się dać wyrazić jako suma liczebności pewnych klas sprzężoności. W przypadku podgrupy normalnej N grupy A_5 dochodzimy do wniosku, że $|N| = 1 + b \cdot 15 + c \cdot 20 + d \cdot 12$, przy czym współczynniki b i c mogą przyjmować wartości 0 lub 1, a współczynnik d być może również 2 (bo są dwie klasy sprzężoności cykli długości 5 w grupie A_5 i być może obie są zawarte w N). Z twierdzenia Lagrange'a wiemy, że $|N| \,\big|\, 60$. Łatwo sprawdzić, że jedynymi dzielnikami liczby 60, dającymi się przedstawić w żądany sposób są 1 i 60. Zatem w A_5 nie ma podgrup normalnych innych niż sama grupa A_5 i jej podgrupa trywialna.
$\square$