

3. WYKŁAD 3: p -GRUPY I TWIERDZENIA SYLOWA.

Definicja 3.1. Niech $(G, \cdot)$ będzie grupą. Grupę G nazywamy **p -grupą**, jeżeli $|G| = p^k$ dla pewnej liczby pierwszej p oraz $k \in \mathbb{N}$.

Twierdzenie 3.1. Niech $(G, \cdot)$ będzie p -grupą. Wówczas

$$p \mid |Z(G)|.$$

W szczególności $Z(G)$ jest nietrywialne.

Dowód. Wobec Uwagi 2.5:

$$p^k = |Z(G)| + \sum_{i=1}^l (G : Z(\{x_i\})),$$

gdzie $Orb(x_1), \dots, Orb(x_l)$ są wszystkimi parami rozłącznymi orbitami działania G na zbiór swoich elementów przez automorfizmy wewnętrzne o mocy większej niż 1. Ponadto:

$$p^k = |Z(\{x_i\})| \cdot (G : Z(\{x_i\})), \text{ dla } i \in \{1, \dots, l\},$$

a więc $(G : Z(\{x_i\})) = p^{l_i}$, $i \in \{1, \dots, l\}$ i skoro $(G : Z(\{x_i\})) = |Orb(\{x_i\})| > 1$, to $l_i > 0$, $i \in \{1, \dots, l\}$. Ostatecznie:

$$p^k = |Z(G)| + \sum_{i=1}^l p^{l_i},$$

wobec czego $|Z(G)| = p^m$, dla pewnego $m > 0$. □

Wniosek 3.1. Niech $(G, \cdot)$ będzie grupą rzędu p^2 . Wówczas G jest abelowa.

Dowód. Wobec poprzedniego twierdzenia $p \mid |Z(G)|$ i skoro $Z(G) < G$, to $|Z(G)| \in \{p, p^2\}$. Przypuśćmy, że $|Z(G)| = p$. Wówczas $(G : Z(G)) = |G/Z(G)| = p$. Wobec tego $G/Z(G)$ jest cykliczna, a zatem istnieje element $a \in G$ taki, że:

$$\forall g \in G \exists k \in \mathbb{Z} (gZ(G) = (aZ(G))^k = a^k Z(G)),$$

czyli

$$\forall g \in G \exists k \in \mathbb{Z} (ga^{-k} \in Z(G)),$$

czyli

$$\forall g \in G \exists k \in \mathbb{Z} \exists z \in Z(G) (ga^{-k} = z).$$

Ustalmy $g \in G$ i niech $k \in \mathbb{Z}$ oraz $z \in Z(G)$ będą takie, że

$$g = a^k z.$$

Wówczas

$$ag = aa^k z = a^k az = a^k za = ga,$$

a zatem $a \in Z(G)$, więc $g = a^k z \in Z(G)$, czyli $Z(G) = G$, co jest sprzecznością. □

Definicja 3.2. Niech $(G, \cdot)$ będzie grupą skończoną, niech $H < G$. Jeżeli H jest p -grupą, to H nazywamy **p -podgrupą** grupy G . Jeżeli $|G| = p^k m$, gdzie $p \nmid m$, $k \geq 1$ oraz $|H| = p^k$, to H nazywamy **p -podgrupą Sylowa** grupy G .

Przykład:

- (1) Rozważmy $G = \mathbb{Z}_{12}$ oraz $H_1 = \{0, 6\}$ oraz $H_2 = \{0, 3, 6, 9\}$. Wówczas H_1 jest 2-podgrupą $\mathbb{Z}_{12}$, a H_2 jest 2-podgrupą Sylowa $\mathbb{Z}_{12}$.

Lemat 3.1. Niech p będzie liczbą pierwszą, $m \in \mathbb{N}$, $p \nmid m$, $k \geq 1$. Wówczas:

$$\binom{p^k m}{p^k} \equiv m \pmod{p}.$$

Dowód. Mamy

$$p \mid \binom{p}{i}, \text{ dla } i \in \{1, \dots, p-1\}.$$

Wobec tego

$$(X+1)^p = \sum_{i=0}^p \binom{p}{i} X^i = X^p + 1 + pf(X),$$

dla pewnego $f(X) \in \mathbb{Z}[X]$. Zatem

$$(X+1)^{p^k} = X^{p^k} + 1 + pg(X),$$

dla pewnego $g(X) \in \mathbb{Z}[X]$, a stąd

$$(X+1)^{p^k m} = (X^{p^k} + 1)^m + ph(X) = \sum_{i=0}^m \binom{m}{i} X^{p^k(m-i)} + ph(X),$$

dla pewnego $h(X) \in \mathbb{Z}[X]$. Wobec tego współczynnik przy $X^{p^k(m-1)}$ wielomianu $(X+1)^{p^k m}$ daje przy dzieleniu przez p resztę $\binom{m}{1} = m$. Ponadto

$$(X+1)^{p^k m} = \sum_{i=0}^{p^k m} \binom{p^k m}{i} X^i.$$

Wobec tego współczynnik przy $X^{p^k(m-1)}$ wielomianu $(X+1)^{p^k m}$ równy jest

$$\binom{p^k m}{p^k(m-1)} = \frac{(p^k m)!}{(p^k(m-1))!(p^k m - p^k(m-1))!} = \frac{(p^k m)!}{(p^k)!(p^k m - p^k)!} = \binom{p^k m}{p^k}.$$

□

Twierdzenie 3.2. Niech $(G, \cdot)$ będzie grupą skończoną, niech $p \mid |G|$, gdzie p jest liczbą pierwszą.

- (1) (*I twierdzenie Sylowa*⁷). G zawiera p -podgrupę Sylowa. Ponadto każda p -podgrupa grupy G zawarta jest w pewnej p -podgrupie Sylowa (to znaczy p -podgrupy Sylowa są maksymalne wśród p -podgrup grupy G).
- (2) (*II twierdzenie Sylowa*). Każde dwie p -podgrupy Sylowa są sprzężone.
- (3) (*III twierdzenie Sylowa*). Jeżeli d_p jest liczbą wszystkich p -podgrup Sylowa grupy G , to

$$d_p \mid |G| \text{ oraz } d_p \equiv 1 \pmod{p}.$$

Dowód. Ustalmy grupę skończoną $(G, \cdot)$ i niech $|G| = p^k m$, $p \nmid m$, $k \geq 1$. Zdefiniujemy rodzinę

$$\Omega = \{A \subset G : |A| = p^k\}.$$

Wobec tego $|\Omega| = \binom{p^k m}{p^k}$. Dalej, zdefiniujemy odwzorowanie $\beta : G \times \Omega \rightarrow \Omega$ wzorem

$$\beta(g, A) = gA = \{ga : a \in A\}.$$

Bez trudu sprawdzamy, że β jest działaniem grupy G na zbiorze Ω .

⁷L. Sylow (1832 – 1918) – matematyk norweski, twierdzenie pochodzi z 1872 roku

Pokażemy najpierw, że istnieje $A \in \Omega$ takie, że $p \nmid |Orb(A)|$. Wobec wzoru klas

$$\binom{p^k m}{p^k} = \sum_{i=1}^s |Orb(A_i)|,$$

gdzie $Orb(A_1), \dots, Orb(A_s)$ są wszystkimi parami rozłącznymi orbitami działania β . Wobec lematu:

$$\binom{p^k m}{p^k} \equiv m \pmod{p}.$$

Zatem $\sum_{i=1}^s |Orb(A_i)|$ nie jest podzielne przez p , więc istnieje $A_i \in \Omega$ taki, że

$$p \nmid |Orb(A_i)|.$$

Ustalmy wobec powyższego zbiór $A \in \Omega$ taki, że $p \nmid |Orb(A)|$. Pokażemy, że $Orb(A)$ zawiera dokładnie jedną p -podgrupę Sylowa. Wobec Twierdzenie 2.2:

$$p \nmid |Orb(A)| = (G : Stab(A)) = \frac{|G|}{|Stab(A)|} = \frac{p^k m}{|Stab(A)|}.$$

Zatem $p^k \mid |Stab(A)|$ i w szczególności $|Stab(A)| \geq p^k$. Ponadto z definicji stabilizatora

$$\forall g \in Stab(A) (gA = A),$$

czyli

$$\forall g \in Stab(A) \forall a \in A (ga \in A),$$

czyli

$$\forall a \in A (Stab(A)a \subset A).$$

Wobec tego

$$|Stab(A)| = |Stab(A)a| \leq |A| = p^k, \text{ dla } a \in A.$$

Zatem $|Stab(A)| = p^k$. Ponadto

$$\forall a \in A (Stab(A)a = A),$$

czyli

$$\forall a \in A (a^{-1} Stab(A) a = a^{-1} A).$$

Ustalmy $a \in A$ i zdefiniujmy

$$H = i_{a^{-1}}(Stab(A)) = a^{-1} Stab(A) a.$$

Wówczas $H < G$ i $|H| = |Stab(A)| = p^k$, więc H jest p -podgrupą Sylowa. Ponadto $H = a^{-1} A \in Orb(A)$, więc

$$Orb(H) = Orb(A).$$

Wobec tego

$$Orb(A) = \{gH : g \in G\}$$

i ponieważ jedyną warstwą będącą grupą jest grupa H , więc $Orb(A)$ zawiera dokładnie jedną podgrupę rzędu p^k .

Pokazaliśmy zatem, że G zawiera p -podgrupę Sylowa. Zauważmy, że $|Orb(A)| = m$. Istotnie, mamy:

$$\begin{aligned} |Orb(A)| &= |Orb(H)| = |\{gH : g \in G\}| \\ &= (G : H) = \frac{|G|}{|H|} = \frac{p^k m}{p^k} = m, \end{aligned}$$

gdzie H jest jedyną p -podgrupą Sylowa zawartą w $Orb(A)$.

Niech $Orb(A_1), \dots, Orb(A_t)$ będą wszystkimi parami różnymi orbitami takimi, że $p \nmid |Orb(A_i)|$, $i \in \{1, \dots, t\}$. Pokażemy, że $d_p = t$. Istotnie, nierówność $(\geq)$ jest trywialna, jako że każda z orbit $Orb(A_i)$, $i \in \{1, \dots, t\}$, zawiera dokładnie jedną p -podgrupę Sylowa. Dla dowodu nierówności $(\leq)$ ustalmy p -podgrupę Sylowa $K < G$. Mamy:

$$\begin{aligned} p \nmid m &= \frac{p^k m}{p^k} = \frac{|G|}{|K|} = (G : K) \\ &= |\{gK : g \in G\}| = |Orb(K)|. \end{aligned}$$

Wobec tego istnieje $i \in \{1, \dots, t\}$ takie, że $Orb(K) = Orb(A_i)$. W szczególności $K \in Orb(A_i)$ i ponieważ w $Orb(A_i)$ jest dokładnie jedna p -podgrupa Sylowa, więc $d_p \leq t$.

Dalej, pokażemy, że $d_p \equiv 1 \pmod p$. Niech $Orb(A_1), \dots, Orb(A_t), Orb(A_{t+1}), \dots, Orb(A_s)$ będą wszystkimi parami różnymi orbitami, przy czym

$$\begin{aligned} p \nmid |Orb(A_i)|, & \quad \text{dla } i \in \{1, \dots, t\}, \\ p \mid |Orb(A_i)|, & \quad \text{dla } i \in \{t+1, \dots, s\}. \end{aligned}$$

Wobec wzoru klas:

$$\begin{aligned} \left(\frac{p^k m}{p^k} \right) &= \sum_{i=1}^s |Orb(A_i)| = \sum_{i=1}^t |Orb(A_i)| + \sum_{i=t+1}^s |Orb(A_i)| \\ &= tm + pq, \end{aligned}$$

dla pewnego $q \in \mathbb{N}$. Wobec lematu:

$$\left(\frac{p^k m}{p^k} \right) \equiv m \pmod p,$$

a zatem $tm + pq \equiv m \pmod p$, czyli $tm \equiv m \pmod p$. Wobec tego $p \mid tm - m = m(t-1)$ i skoro $p \nmid m$ i p jest pierwsza, to $p \mid t-1$, a więc

$$d_p = t \equiv 1 \pmod p.$$

Pokażemy teraz, że każda p -podgrupa zawarta jest w pewnej p -podgrupie Sylowa i że każde dwie p -podgrupy Sylowa są sprzężone. Istotnie, ustalmy p -podgrupę F i niech $|F| = p^l$, $1 \leq l \leq k$. Ustalmy p -podgrupę Sylowa H , $|H| = p^k$. Zdefiniujemy rodzinę

$$X = \{aH \in a \in G\}.$$

Wobec tego $|X| = (G : H) = \frac{|G|}{|H|} = \frac{p^k m}{p^k} = m$. Zdefiniujemy odwzorowanie $\alpha : F \times X \rightarrow X$ wzorem

$$\alpha(f, aH) = (fa)H.$$

Łatwo sprawdzamy, że α jest działaniem grupy F na zbiorze X . Niech $Orb(a_1H), \dots, Orb(a_rH)$ będą wszystkimi parami różnymi orbitami działania α . Wobec Wniosku 2.2:

$$|Orb(a_iH)| = p^{\epsilon_i}, \text{ dla pewnych } \epsilon_i \geq 0, i \in \{1, \dots, r\}.$$

Wobec wzoru klas:

$$m = \sum_{i=1}^r |Orb(a_iH)| = \sum_{i=1}^r p^{\epsilon_i}$$

i skoro $p \nmid m$, to $\sum_{i=1}^r p^{\epsilon_i}$ nie jest podzielne przez p , a więc istnieje $i_0 \in \{1, \dots, r\}$ takie, że $p^{\epsilon_{i_0}} = 1$, czyli

$$|Orb(a_{i_0}H)| = 1.$$

Wobec tego $Orb(a_{i_0}H) = \{a_{i_0}H\}$, czyli z definicji orbity

$$\forall f \in F(fa_{i_0}H = a_{i_0}H),$$

czyli

$$\forall f \in F(a_{i_0}^{-1}fa_{i_0}H = H),$$

czyli

$$\forall f \in F(a_{i_0}^{-1}fa_{i_0} \in H),$$

czyli

$$\forall f \in F(f \in a_{i_0}Ha_{i_0}^{-1}),$$

czyli

$$F \subset a_{i_0}Ha_{i_0}^{-1} = i_{a_{i_0}}(H).$$

Ponadto, skoro H jest p -podgrupą Sylowa oraz $i_{a_{i_0}}$ jest izomorfizmem, więc $i_{a_{i_0}}(H)$ jest p -podgrupą Sylowa. W szczególności, jeżeli G jest p -podgrupą Sylowa, to $F \subset i_{a_{i_0}}(H)$ i skoro $|F| = |H| = |i_{a_{i_0}}(H)|$, to $F = i_{a_{i_0}}(H)$.

Na koniec, pokażemy, że $d_p \mid |G|$. Zdefiniujmy rodzinę

$$Y = \{H : H \text{ jest } p\text{-podgrupą Sylowa}\}.$$

W szczególności $|Y| = d_p$. Zdefiniujmy odwzorowanie $\gamma : InnG \times Y \rightarrow Y$ wzorem

$$\gamma(i_a, H) = i_a(H).$$

γ , jak łatwo się przekonać, jest działaniem grupy $InnG$ na zbiorze Y . Ponadto, ponieważ każde dwie p -podgrupy Sylowa są sprzężone, działanie to jest przechodnie, a więc

$$\forall H \in Y(Orb(H) = Y).$$

Ustalmy $H \in Y$. Wobec wzoru klas

$$d_p = |Orb(H)|.$$

Dalej, wobec Wniosku 2.2:

$$d_p = |Orb(H)| \mid |InnG|,$$

i wobec Uwagi 1.4:

$$d_p \mid |InnG| = |G/Z(G)| = \frac{|G|}{|Z(G)|}.$$

Zatem, w szczególności, $d_p \mid |G|$. □

Przykłady:

(2) Rozważmy grupę G rzędu 15. Wówczas

$$d_3 \equiv 1 \pmod{3} \text{ oraz } d_3 \mid 15, \text{ a więc } d_3 = 1,$$

$$d_5 \equiv 1 \pmod{5} \text{ oraz } d_5 \mid 15, \text{ a więc } d_5 = 1.$$

Zatem w G istnieją dokładnie jedna 3-podgrupa Sylowa (rzędu 3) i dokładnie jedna 5-podgrupa Sylowa (rzędu 5).

(3) Rozważmy grupę G rzędu 12. Wówczas

$$d_2 \equiv 1 \pmod{2} \text{ oraz } d_2 \mid 12, \text{ a więc } d_2 \in \{1, 3\},$$

$$d_3 \equiv 1 \pmod{3} \text{ oraz } d_3 \mid 12, \text{ a więc } d_3 \in \{1, 4\}.$$

Zatem w G istnieje dokładnie jedna 2-podgrupa Sylowa (rzędu 4) lub istnieją 3 2-podgrupy Sylowa (rzędu 4). Podobnie, w G istnieje dokładnie jedna 3-podgrupa Sylowa rzędu 3, lub 4 3-podgrupy Sylowa rzędu 3.

Wniosek 3.2 (twierdzenie Cauchy'ego). *Niech $(G, \cdot)$ będzie grupą skończoną, niech $p \mid |G|$, gdzie p jest liczbą pierwszą. Wówczas G zawiera element rzędu p .*

Dowód. Ustalmy grupę skończoną $(G, \cdot)$ i niech $|G| = p^k m$, $p \nmid m$, $k \geq 1$. Wobec twierdzenia Sylowa istnieje $H < G$ taka, że $|H| = p^k$. Ustalmy $a \in H$. Wówczas $r(a) \mid p^k$. Jeżeli $r(a) = p$, to a jest szukanym elementem. Jeżeli $r(a) = p^l$, $1 < l \leq k$, to $r(a^{p^{l-1}}) = p$ i $a^{p^{l-1}}$ jest szukanym elementem. $\square$

Wniosek 3.3. *Niech $(G, \cdot)$ będzie grupą skończoną, niech $p \mid |G|$, gdzie p jest liczbą pierwszą. Niech $H < G$ będzie p -podgrupą Sylowa. Wówczas*

$$H \triangleleft G \text{ wtedy i tylko wtedy, gdy } d_p = 1.$$

Dowód. $(\Rightarrow)$: Ustalmy p -podgrupę Sylowa F . Wobec twierdzenia Sylowa

$$\exists a \in G(F = i_a(H)).$$

Ponieważ $H \triangleleft G$, więc $i_a(H) = H$ dla $a \in G$, więc $H = F$ i $d_p = 1$.

$(\Leftarrow)$: Implikacja ta jest oczywista. $\square$

Przykłady:

(4) Roważmy ponownie grupę G rzędu 15. Wówczas, ponieważ $d_3 = 1$ i $d_5 = 1$:

jeśli $H < G$ i $|H| = 5$, to $H \triangleleft G$,

jeśli $F < G$ i $|F| = 3$, to $F \triangleleft G$.

Ponadto

$$\forall a \in G(r(a) \in \{1, 3, 5, 15\}),$$

a więc

jeśli $r(a) = 3$ to $|\langle a \rangle| = 3$, a więc $\langle a \rangle = H$,

jeśli $r(a) = 5$ to $|\langle a \rangle| = 5$, a więc $\langle a \rangle = F$.

Dalej:

$$|H \cup F| = 2 + 4 + 1 = 7,$$

więc w G jest 8 elementów rzędu 15.

Wniosek 3.4. *Niech $(G, \cdot)$ będzie grupą skończoną, niech $|G| = pq$, gdzie p i q są liczbami pierwszymi, $p > q$. Wówczas istnieje $H \triangleleft G$ i $|H| = p$.*

Dowód. Wobec twierdzenia Sylowa istnieje p -podgrupa Sylowa H rzędu p . Ponadto

$$d_p \equiv 1 \pmod{p} \text{ oraz } d_p \mid pq.$$

Zatem $d_p = 1$ i H jest normalna. $\square$