Wykład 5.

Konstrukcje grup c.d.

(c) Produkt półprosty grup

Niech $N \triangleleft G$, $H < G$

Lemat 4.7. $NH < G$

D-d ćw. z listy 2.

Tw. 4.8. Zał. że $N \triangleleft G$, $H < G$ oraz

(1) $N \cap H = \{e\}$

(2) $NH = G$.

Wtedy:

(a) W każdej warstwie N w G jest dokładnie jeden element H

(b) Funkcja $f: N \times H \longrightarrow G$ dana wzorem $f(n,h) = n \cdot h$ jest bijekcją.

D-d. (a) • $\underset{\underset{Na}{\parallel}}{aN} \cap H \neq \emptyset$, bo: z (1):

$a = n \cdot h$ dla pewnych $n \in N$, $h \in H$

$\Downarrow$

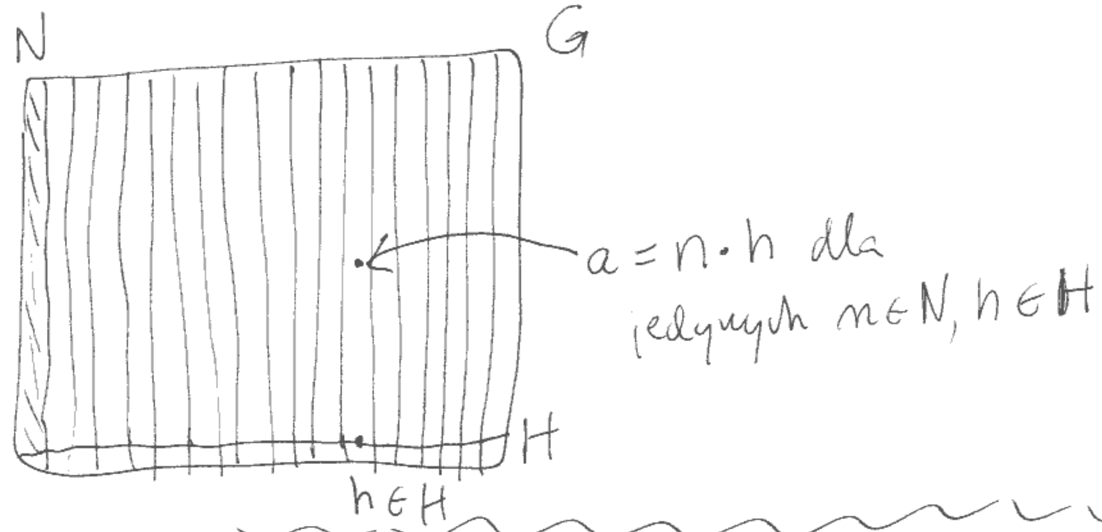
$h = n^{-1} a \in Na = aN$.

• $|aN \cap H| = 1$, bo:

jeśli $an_1 \neq an_2$ są oba w H, to

$e \neq (an_2)^{-1}(an_1) = n_2^{-1} a^{-1} a n_1 = n_2^{-1} n_1 \in H \cap N$ ↯.

(b) wynika z (a)

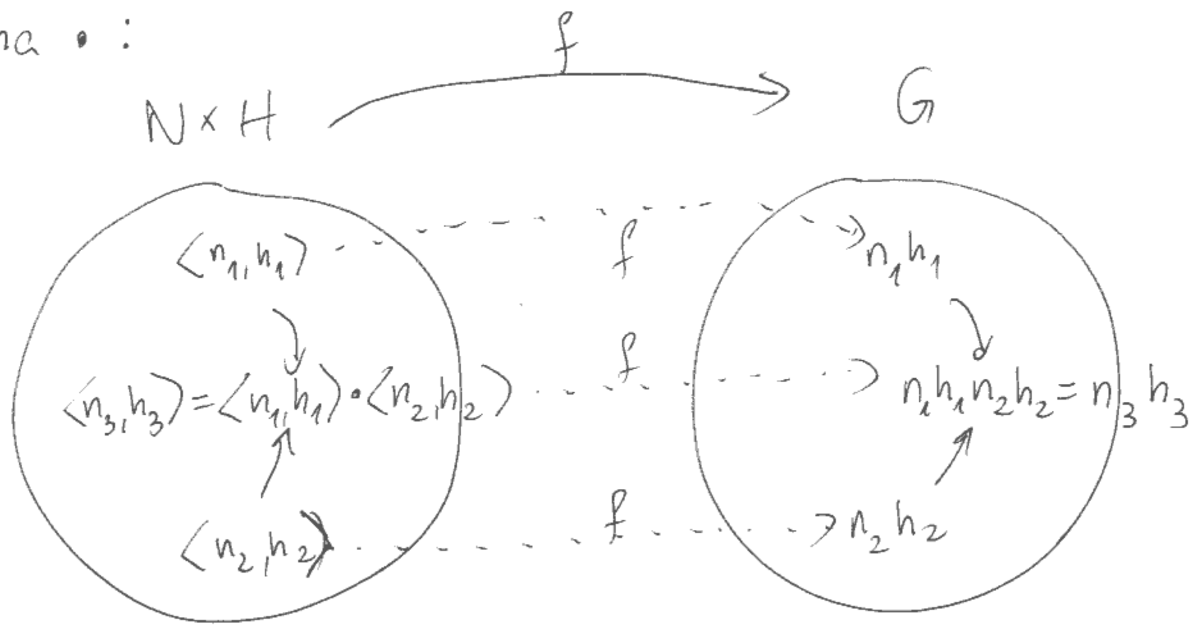


Przy założeniach tw. 4.8:

$$f : N \times H \xrightarrow[\text{na}]{1-1} G$$

Niech $\circ$: działanie w $N \times H$ t.że: $f : (N \times H, \circ) \xrightarrow{\cong} (G, \cdot)$
(jedyne)

Wzór na $\circ$:



Czyli: $\langle n_1, h_1 \rangle \circ \langle n_2, h_2 \rangle =$ jedyne $\langle n_3, h_3 \rangle$ t.że

$$n_1 h_1 n_2 h_2 = n_3 h_3, \qquad n_3 \in N,\ h_3 \in H.$$

Znajdujemy n_3, h_3:

$$n_1 h_1 n_2 h_2 = n_1 \underbrace{h_1 n_2 h_1^{-1}}_{\substack{\| \\ n_2^{h_1} \in N \triangleleft G}} h_1 h_2 = \overbrace{n_1 n_2^{h_1}}^{n_3} \overbrace{h_1 h_2}^{h_3}$$

Więc:

$$\langle n_1, h_1 \rangle \cdot \langle n_2, h_2 \rangle = \langle n_1 j_{h_1}(n_2), h_1 h_2 \rangle$$

$$(N \times H, \cdot) \cong (G, \cdot)$$

- el. neutralny: $\langle e_N, e_H \rangle$
- el. odwrotny do $\langle n, h \rangle$:

$$(nh)^{-1} = h^{-1} n^{-1} = h^{-1} n^{-1} h h^{-1} = j_{h^{-1}}(n^{-1}) \cdot h^{-1}$$

$$\langle n, h \rangle^{-1} = \langle j_{h^{-1}}(n^{-1}), h^{-1} \rangle$$

- Łączność · wynika z ~~i~~ izomorfizmu
  - · można sprawdzić rachunkowo, korzystając z tego że · N, H ~~są~~ grupy
  - · H działa na N przez sprzężenie.

Abstrakcyjnie:

H, N grupy, H działa na N przez automorfizmy, tzn:

$$\varphi : H \xrightarrow[\text{homo}]{} \mathrm{Aut}(N)$$ (a nie tylko $\varphi : H \to \mathrm{Sym}(N)$)

Def. 5.1. Produkt półprosty grup N, H:

$N \rtimes H = (N \times H, \cdot)$, gdzie

$$\langle n_1, h_1 \rangle \cdot \langle n_2, h_2 \rangle = \langle n_1 \varphi_{h_1}(n_2), h_1 h_2 \rangle$$

- łączne, el. neutralny: $\langle e_N, e_H \rangle$
- $\langle n, h \rangle^{-1} = \langle \varphi_{h^{-1}}(n^{-1}), h^{-1} \rangle$

<u>Własności</u>:

$i_N : N \xhookrightarrow[\text{mono}]{} N \rtimes H \qquad i_H : H \xhookrightarrow[\text{mono}]{} N \rtimes H$

$i_N(n) = \langle n, e_H \rangle \qquad i_H(h) = \langle e_N, h \rangle$

Uwaga 5.2. Niech $G = N \rtimes H$, $N^* = i_N[N]$, $H^* = i_H[H]$.
Wtedy $N^* \triangleleft G$, i $H^* < G$ spełniają założenia tw. 4.8

<u>D-d</u> ćw.

$\xrightarrow[\cong]{i_H}$ $\xrightarrow[i_N]{\cong}$ $H^* \curvearrowright N^*$ ($\hat{\varphi}$ sprzężenie w $N \rtimes H$)

$f : (N^* \times H^*, \cdot) \xrightarrow{\cong} (N \rtimes H, \cdot)$

Uwaga 5.3.
W sytuacji jak w tw. 4.8:
$$G \cong N \rtimes H, \text{ gdzie } H \curvearrowright N \text{ przez sprzężenie.}$$

Przykład $\underset{\text{nieabelowa}}{S_3} \not\cong \underset{\text{abelowa}}{\mathbb{Z}_3 \times \mathbb{Z}_2}$, ale:

$$S_3 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2 \qquad \underline{\text{Zad}}\ D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$$

$S_3 \cong D_3$

bo: $S_3 \rhd A_3 = \{id, (1,2,3), (1,3,2)\} \cong \mathbb{Z}_3$, $A_3 = N$

$$S_3 > H = \{id, (1,2)\} \cong \mathbb{Z}_2$$

- H, N spełniają założenia tw. 4.8
- H działa na N przez sprzężenie $\varphi_h(n) = n^h$

$$\varphi_{(1,2)}(n) = n^{-1}$$

$$S_3 \cong N \rtimes H \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2.$$

Trochę teorii: p: l. pierwsza, G: grupa skończona

Def. 5.4. G jest p-grupą, gdy $|G| = p^n$ dla pewnego $n \geq 0$.

Uwaga 5.5. Każda grupa G rzędu p jest cykliczna, $\cong (\mathbb{Z}_p, +_p)$

Tw. 5.6 (Sylov). G : skończona, $|G| = p^n \cdot k$, $p \nmid k$.

Wtedy:

(1) $\exists H < G \; |H| = p^n$ (H nazywamy p-podgrupą Sylova grupy G, ozn. czasem G_p)

(2) Wszystkie p-podgrupy Sylova grupy G są sprzężone, ich liczba $\equiv 1 \pmod p$

(3) Każda p-podgrupa grupy G zawiera się w pewnej p-podgrupie Sylova grupy G.

Lemat 5.7. Niech H : skończona gr. abelowa, $l \in \mathbb{N}^+$, p : ~~l. pierwsza~~ l. pierwsza.

(a) Jeśli $p \mid |H|$, to H ma element rzędu p.

(b) Jeśli $\underbrace{(\forall a \in H)\, a^l = e}_{(*)}$, to $\exists n \; |H| \mid l^n$

D-d (b) Indukcja względem $|H|$. $|H| = 1$: OK.

Krok indukcyjny:

Zał, że $|H| > 1$ i dla grup H_1 rzędu $< |H|$ jest OK.

Niech $a \in H \setminus \{e\}$. Niech $H_1 = \langle a \rangle < H$.

$|H_1| = \operatorname{ord}(a) \mid l$, H/H_1 ma własność $(*)$

$\Downarrow$ zał. ind.

$|H/H_1| \mid l^n$ dla pewnego n.

$\Downarrow$

$|H| = |H_1| \cdot |H/H_1|$ dzieli $l \cdot l^n = l^{n+1}$

(a) Niech $|H| = p^k \cdot l$, $p \nmid l$.

1°. Jeśli istnieje $a \in H$ t. że $ord(a) = p \cdot t$, to $ord(a^t) = p$

Koniec

2°. Jeśli takiego a nie ma, to: $(\forall a \in H)\, a^l = e$

$$\Downarrow (b)$$

$|H| \,|\, l^n$ dla pewnego n

$$\downarrow$$

Sprzeczność.

<u>Lemat 5.8.</u> Zał, że G jest p-grupą, $|G| > 1$. Wtedy

$Z(G) \neq \{e\}$.

<u>D-d.</u> $|G| = p^n$

$G = \{e\} \,\dot\cup\, A_1 \,\dot\cup \ldots \dot\cup\, A_r$: klasy sprzężenia

$|A_i| = [G : C(a_i)]$ dla $a_i \in A_i$ $\qquad C(a_i) = G_{a_i}$ stabilizator a_i

$|A_i| \,\big|\, p^n$. gdy $|A_i| > 1$, to $p \,|\, |A_i|$.

$|G| = \underset{|\{e\}|}{1} + \sum_{i=1}^{r} |A_i|$. p dzieli prawą stronę, więc

$p \nmid |A_i|$ dla pewnego i

$$\Downarrow$$

$|A_i| = 1 \iff A_i \subseteq Z(G)$.

D-d tw. Sylowa 5.6(1): $|G| = p^n \cdot k$, $p \nmid k$

$$\exists\, H \leq G \quad |H| = p^n.$$

Indukcja względem $|G|$.

(a) $|G| = 1$: OK.

(b) krok indukcyjny: $|G| > 1$

1°. $\exists\, H \lneq G$ $p^n \mid |H|$. Z zał. ind. dla H:

istnieje $H_1 < H$, $|H_1| = p^n$ OK.

$$H_1 \leq G$$

2°. $\neg \exists\, H \lneq G$ $p^n \mid |H|$.

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

bo: $x \in Z(G) \iff |x^G| = 1$

$$G = Z(G) \,\dot\cup\, \underbrace{A_1 \dot\cup \ldots \dot\cup A_r}_{\text{klasy sprzężenia mocy } > 1.}$$

$$A_i = a_i^G$$

$$|A_i| \cdot |C(a_i)| = |G|$$

$p \mid |A_i| \Leftarrow p^n \nmid |C(a_i)|$ (z 2°), $p^n \mid |G|$

$$|G| = |Z(G)| + \sum_{i=1}^{r} |A_i|$$

$p \mid |G| \Rightarrow p \mid |Z(G)| \Leftarrow p \mid \sum_{i=1}^{r} |A_i|$

- z lematu 5.7 istnieje $a \in Z(G)$ $\operatorname{ord}(a) = p$.

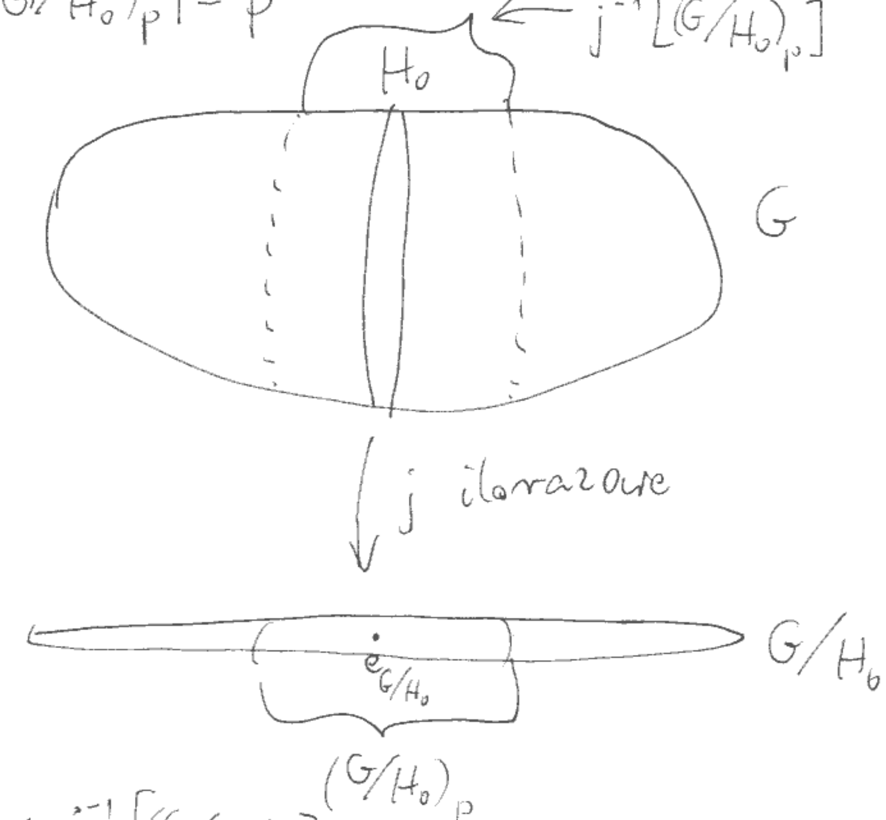
Niech $H_0 = \langle a \rangle$. $H_0 \subseteq Z(G)$, więc $H_0 \triangleleft G$.

$|G/H_0| \cdot \underset{p}{\underset{\shortparallel}{|H_0|}} = |G|$, więc

$|G/H_0| = |G|/_p < |G|$. Z zał. ind istnieje gpa

$(G/H_0)_p < G/H_0$.

tzn: $|(G/H_0)_p| = p^{n-1}$



Niech $G_p = j^{-1}[(G/H_0)_p] < G$.

$|G_p| = p^{n-1} \cdot p = p^n$.

Lemat 5.9.

Zał., że G_p : p-podgrupa Sylova grupy G,

$H < G$ p-podgrupa, $H \subseteq N(G_p)$.

<u>Wtedy</u> $H \subseteq G_p$.

Def. 5.9' Dla $H < G$ niech $N(H) = \{g \in G : gHg^{-1} = H\}$

normalizator podgrupy H w grupie G

Ćw. $H \triangleleft N(G) < G$ ćwiczenie.

<u>D-d.</u> $G_p \triangleleft N(G_p)$, $H < N(G_p) \Rightarrow G_p \cdot N < N(G_p)$

i $G_p \triangleleft G_p \cdot N$.

$G_p \cdot H / G_p \cong H / G_p \cap H \leftarrow$ p-grupa

<u>stąd</u>: $G_p \cdot H$ p-grupa. Z maksymalności G_p:

$G_p \cdot H = G_p$, więc $H \subseteq G_p$.

<u>D-d</u> tw. Sylova 5.6 (2), (3)

Niech G_p : pewna p-podgrupa S. grupy G.

Niech $\mathcal{G}_p = \{G_p^1, \dots, G_p^m\}$: wszystkie p-podgrupy S. w G sprzężone z G_p.

$G_p^1 = G_p$

$G_p \curvearrowright \mathcal{G}_p$ działa na $\mathcal{G}_p$ przez sprzężenie, $O(G_p) = \{G_p^1\}$.

- $i > 1 \Rightarrow |O(G_p^i)| > 1$

(bo: jeśli $O(G_p^i) = \{G_p^i\}$, to $G_p \subseteq N(G_p^i)$
$\Downarrow 5.9$
$G_p \subseteq G_p^i$
$\Downarrow$ maksymalności G_p
$G_p = G_p^i$ $\lightning$.)

z $|O(G_p^i)| > 1$ wynika

- $p \mid |O(G_p^i)|$ (jak poprzednio)

$G_p \curvearrowright \mathcal{G}_p$, $|O(G_p^i)| \mid |G_p| = p^n$.
$\mathcal{G}_p \ni G_p^i$

$\mathcal{G}_p = \{G_p^i\} \dot\cup \underbrace{A_1 \dot\cup \ldots \dot\cup A_r}_{\text{orbity mocy} > 1}$: orbity

$p \mid$

stąd: $m = |\mathcal{G}_p| \equiv 1 \pmod p$. (część 5.6(2))

- Niech $H < G$ dowolna p-podgrupa grupy G.

$H \curvearrowright \mathcal{G}_p$ przez sprzężenie

orbity tego działania: moc 1 lub moc p
(bo te moce dzielą $|H|$).

<u>Stąd</u> $\underbrace{\text{pewna z tych orbit}}_{\{G_p^i\}}$ ma moc 1 (bo: $|\mathcal{G}_p| \equiv 1 \pmod p$)

Tzn: $(G_p^i)^H = G_p^i \Longrightarrow H \subseteq N(G_p^i) \overset{5.9}{\Longrightarrow} H \subseteq G_p^i$, co daje 5.6(3)

AII.5 (12

Uwaga: Jeśli H: p-podgrupa S. grupy G, to $H = G_p^i$, czyli $H \sim G_p$, co ~~#~~ daje 5.6(2).

Wn. 5.10 (tw. Cauchy'ego)

G skończona, $p \mid |G| \Rightarrow$ istnieje $a \in G$ $\mathrm{ord}(a) = p$.

D-d Niech G_p: p-podgrupa S. grupy G.

Z lematu 5.8: $Z(G_p) \neq \{e\}$.

Z lematu 5.7: $\exists \overset{\Psi}{a}$ $\mathrm{ord}(a) = p$.