

Grupy rozwiązalne.

Definicja

Niech $(G, \cdot)$ będzie grupą. Wówczas ciąg podgrup grupy G zdefiniowany indukcyjnie wzorami

- ▶ $G^{(0)} = G$,
- ▶ $G^{(i)} = [G^{(i-1)}, G^{(i-1)}]$, dla $i \in \mathbb{N}$

nazywamy **górnym ciągiem centralnym** grupy G , a jego elementy **hipercentralami**;

Uwaga

Niech $(G, \cdot)$ będzie grupą, $(G^{(i)})_{i \in \mathbb{N}}$ jej górnym ciągiem centralnym. Wówczas

1. $G^{(i+1)} \subset G^{(i)}$, $G^{(i)} \triangleleft G$, dla $i \in \mathbb{N}$;
2. $G^{(i)}/G^{(i+1)}$ są abelowe dla $i \in \mathbb{N}$.

Dowód:

(1) Pokażemy, że jeśli $M_1 \triangleleft G$ oraz $M_2 \triangleleft G$, to $[M_1, M_2] \triangleleft G$ i $[M_1, M_2] \subset M_1 \cap M_2$.

Ustalmy w tym celu $M_1 \triangleleft G$ i $M_2 \triangleleft G$.

Pierwsza teza wynika z udowodnionego wcześniej twierdzenia.

Dla dowodu drugiej tezy ustalmy

$[a_1, b_1]^{k_1} \dots [a_n, b_n]^{k_n} \in [M_1, M_2]$, gdzie $a_i \in M_1$, $b_i \in M_2$, dla $i \in \{1, \dots, n\}$.

Wówczas:

$$\begin{aligned} & [a_1, b_1]^{k_1} \dots [a_n, b_n]^{k_n} \\ &= \underbrace{(a_1 b_1 a_1^{-1})}_{\in M_2} \underbrace{(b_1^{-1})}_{\in M_2} \dots \underbrace{(a_n b_n a_n^{-1})}_{\in M_2} \underbrace{(b_n^{-1})}_{\in M_2} \in M_2. \end{aligned}$$

Podobnie $[a_1, b_1]^{k_1} \dots [a_n, b_n]^{k_n} \in M_1$.

Pokażemy, że $G^{(i)} \triangleleft G$, dla $i \in \mathbb{N}$.

Dla $i = 0$ jest to oczywiste, założmy więc, że $G^{(i)} \triangleleft G$.

Wobec tego

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \triangleleft G,$$

co dowodzi tezy na mocy indukcji względem $i \in \mathbb{N}$.

Pokażemy, że $G^{(i+1)} \subset G^{(i)}$, dla $i \in \mathbb{N}$.

Ustalmy $i \in \mathbb{N}$.

Ponieważ $G^{(i)} \triangleleft G$, mamy

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subset G^{(i)} \cap G^{(i)} = G^{(i)}.$$

(2) Pokażemy, że $G^{(i)}/G^{(i+1)}$ są abelowe, dla $i \in \mathbb{N}$.

Ustalmy $i \in \mathbb{N}$.

Ponieważ $G^{(i+1)} \triangleleft G$, więc $G^{(i+1)} \triangleleft G^{(i)}$.

Ponadto $[G^{(i)}, G^{(i)}] < G^{(i+1)}$, więc wobec udowodnionego wcześniej wniosku $G^{(i)}/G^{(i+1)}$ jest abelowa.

Definicja

Niech $(G, \cdot)$ będzie grupą. Wówczas jeżeli $(G^{(i)})_{i \in \mathbb{N}}$ jest jej górnym ciągiem centralnym oraz $G^{(i)} = \{1\}$ dla pewnego $i \in \mathbb{N}$, to G nazywamy **grupą rozwiązalną**, a najmniejszą liczbę $i \in \mathbb{N}$, dla której $G^{(i)} = \{1\}$ **stopniem rozwiązalności**.

Przykłady:

1. Rozważmy grupę $D(3)$. Ciąg

$$D(3) > \{I, O_{120}, O_{240}\} > \{I\}$$

jest górnym ciągiem centralnym i tym samym $D(3)$ jest rozwiązalna.

Definicja

Niech $(G, \cdot)$ będzie grupą. Wówczas skończony ciąg podgrup grupy G , $(G = G_0, G_1, \dots, G_n = \{1\})$, taki, że

- ▶ $G_{i+1} \triangleleft G_i$, dla $i \in \{0, \dots, n-1\}$,

nazywamy **ciągami podnormalnymi** (lub **subnormalnymi**) grupy G . Liczbę n nazywamy **długością ciągu**, a grupy

$$G_i/G_{i+1}, \text{ dla } i \in \{0, \dots, n-1\}$$

faktorami ciągu.

Twierdzenie

Niech $(G, \cdot)$ będzie grupą skończoną. Następujące warunki są równoważne:

1. G jest rozwiązalna,
2. istnieje ciąg $(G = G_0, G_1, \dots, G_n = \{1\})$ podnormalny o faktorach abelowych,
3. istnieje ciąg $(G = G_0, G_1, \dots, G_m = \{1\})$ podnormalny o faktorach cyklicznych.

Dowód:

(1) $\Rightarrow$ (2): oczywiste wobec wcześniejszych uwag i przykładów.

(2) $\Rightarrow$ (3): Pokażemy, że skończona grupa abelowa ma ciąg podnormalny o faktorach cyklicznych.

Jest to oczywiste, gdy $|G| = 1$, zaś w przypadku $|G| = m$ założmy, że dla grup rzędu $|G| < m$ twierdzenie jest prawdziwe.

Pokażemy, że w G istnieje ciąg podnormalny o faktorach cyklicznych.

Ustalmy $a \in G \setminus \{1\}$.

Niech $H = \langle a \rangle$.

Wówczas H jest cykliczna oraz $|G/H| < m$ i oczywiście G/H jest abelowa.

Wobec założenia indukcyjnego

$$(G/H = G'_0, G'_1, \dots, G'_n = \{1\})$$

jest ciągiem podnormalnym o faktorach cyklicznych.

Niech

$$G_i = \kappa^{-1}(G'_i), \text{ dla } i \in \{1, \dots, k\} \text{ oraz } G_{k+1} = \{1\},$$

gdzie $\kappa : G \rightarrow G/H$ jest epimorfizmem kanonicznym.

Wówczas

$$G_{i-1}/G_i = G'_{i-1}/G'_i, \text{ dla } i \in \{1, \dots, k\} \text{ oraz } G_k/G_{k+1} \cong H.$$

Zatem $(G = G_0, G_1, \dots, G_{k+1} = \{1\})$ jest ciągiem podnormalnym o faktorach cyklicznych i na mocy zasady indukcji matematycznej teza została udowodniona.

Niech $(G = G_0, G_1, \dots, G_k = \{1\})$ będzie ustalonym ciągiem podnormalnym o faktorach abelowych.

Grupy G_{i-1}/G_i , $i \in \{1, \dots, k\}$, są skończonymi grupami abelowymi.

Niech

$$G_{i-1}/G_i = G'_{i,0}, G'_{i,1}, \dots, G'_{i,k_i} = \{1\}, \text{ dla } i \in \{1, \dots, k\},$$

będą ciągami podnormalnymi o faktorach cyklicznych.

Niech

$$G_{i,j} = \kappa_i^{-1}(G'_{i,j}), \text{ dla } j \in \{0, \dots, k_i\}, i \in \{1, \dots, k\},$$

gdzie $\kappa_i : G_{i-1} \rightarrow G_{i-1}/G_i$ są epimorfizmami kanonicznymi.

Zatem:

- ▶ $G_{i,0} = G_{i-1}$, $i \in \{1, \dots, k\}$,
- ▶ $G_{i,k_i} = G_i$, $i \in \{1, \dots, k\}$,
- ▶ $G_{i,j} \triangleleft G_{i,j-1}$, dla $j \in \{0, \dots, k_i\}$, $i \in \{1, \dots, k\}$,
- ▶ $G_{i,j-1}/G_{i,j} \cong G'_{i,j-1}/G'_{i,j}$, dla $j \in \{0, \dots, k_i\}$, $i \in \{1, \dots, k\}$.

Zatem $(G = G_{1,0}, G_{1,1}, \dots, G_{1,k_1} = G_2 = G_{2,0}, G_{2,1}, \dots, G_{2,k_2}, \dots, G_{k,0}, \dots, G_k = \{1\})$ jest ciągiem podnormalnym o faktorach cyklicznych.

(3) $\Rightarrow$ (1): Niech $(G = G_0, G_1, \dots, G_k = \{1\})$ będzie ciągiem podnormalnym o faktorach cyklicznych.

Pokażemy, że $G^{(i)} \subset G_i$, dla $i \in \{0, \dots, k\}$.

Jest to oczywiste dla $i = 0$, założmy więc, że dla ustalonego $i > 0$ zachodzi $G^{(i)} \subset G_i$.

Pokażemy, że $G^{(i+1)} \subset G_{i+1}$.

Istotnie:

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subset [G_i, G_i].$$

Ponieważ $G_{i+1} \triangleleft G_i$ oraz G_i/G_{i+1} jest cykliczna, a więc abelowa, więc wobec odpowiedniego wniosku:

$$[G_i, G_i] \subset G_{i+1}.$$

Definicja

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

Niech $(G, \cdot)$ będzie p -grupą. Wówczas G jest rozwiązalna.

Twierdzenie

Niech $(G, \cdot)$ będzie grupą, niech $|G| = pq$, gdzie p i q są liczbami pierwszymi. Wówczas G jest grupą rozwiązalną.

Przykłady:

2. Rozważmy grupę $D(4)$. Mamy

$$|D(4)| = 8 = 2^3,$$

a więc $D(4)$ jest rozwiązalna jako p -grupa.

3. Rozważmy grupę $S(3)$. Mamy

$$|S(3)| = 6 = 2 \cdot 3,$$

a więc $S(3)$ jest rozwiązalna jako grupa rzędu pq .

Twierdzenie (Burnside'a)

¹ Niech $(G, \cdot)$ będzie grupą, niech $|G| = p^a q^b$, gdzie p i q są liczbami pierwszymi oraz $a, b \in \mathbb{N}$. Wówczas G jest grupą rozwiązalną.

¹Twierdzenie pochodzi z 1911 roku, zwiemy je też “ $p^a q^b$ -theorem”.

Twierdzenie (Feit'a-Thompsona)

² Niech $(G, \cdot)$ będzie grupą, niech $|G| = 2k + 1$, gdzie $k \in \mathbb{N}$.
Wówczas G jest grupą rozwiązalną.

²Twierdzenie pochodzi z 1963 roku, jego oryginalny dowód zajmuje 254 strony: W. Feit, J. Thompson, *Solvability of groups of odd order*, Pacific J. of Math. 13 (1963), 775-1029.

Iliczyny (sumy) proste
wewnętrzne i zewnętrzne.

Uwaga

Niech $(G, \cdot)$ będzie grupą, $H_1, H_2 < G$. Następujące warunki są równoważne:

1. $G = H_1 H_2$ oraz $H_1 \cap H_2 = \{1\}$,
2. każdy element $g \in G$ ma jednoznaczne przedstawienie w postaci

$$g = h_1 h_2,$$

gdzie $h_1 \in H_1$ oraz $h_2 \in H_2$.

Dowód.

(1) $\Rightarrow$ (2): Załóżmy, że $G = H_1 H_2$ oraz $H_1 \cap H_2 = \{1\}$.

Załóżmy, że dla pewnych $h_1, h'_1 \in H_1$ oraz $h_2, h'_2 \in H_2$ zachodzi $h_1 h_2 = h'_1 h'_2$.

Wówczas $(h'_1)^{-1} h_1 = h'_2 h_2^{-1} \in H_1 \cap H_2 = \{1\}$, więc $h_1 = h'_1$ oraz $h_2 = h'_2$.

(2) $\Rightarrow$ (1): Załóżmy, że każdy element $g \in G$ ma jednoznaczne przedstawienie postaci $g = h_1 h_2$, gdzie $h_1 \in H_1$, $h_2 \in H_2$.

Wówczas oczywiście $G = H_1 H_2$.

Załóżmy, że $g \in H_1 \cap H_2$.

Wówczas $g = g \cdot 1 = 1 \cdot g$.

Zatem $g = 1$.



Oznaczenie:

Gdy $(G, +)$ zapisana jest w notacji addytywnej, piszemy $H_1 + H_2$ zamiast $H_1 H_2$.

Definicja

Niech $(G, \cdot)$ będzie grupą, $H_1, H_2 < G$.

1. G jest słabym iloczynem (sumą) wewnętrznym podgrup H_1 i H_2 , gdy spełnia jeden (a więc wszystkie) warunki Uwagi 0.2.
2. G jest słabym iloczynem (sumą) półprostym wewnętrznym podgrup H_1 i H_2 , gdy jest słabym iloczynem (sumą) wewnętrznym oraz $H_1 \triangleleft G$ lub $H_2 \triangleleft G$.
3. G jest słabym iloczynem (sumą) prostym wewnętrznym podgrup H_1 i H_2 , gdy jest słabym iloczynem (sumą) wewnętrznym oraz $H_1 \triangleleft G$ i $H_2 \triangleleft G$.

Przykłady:

1. Rozważmy grupę $D(n)$. Niech $Obr(n)$ oznacza grupę obrotów, a $Odb(n)$ dowolną dwuelementową grupę generowaną przez odbicie. Wówczas

$$D(n) = Obr(n) \cdot Odb(n)$$

jest słabym iloczynem półprostym wewnętrznym, ale nie jest słabym iloczynem prostym wewnętrznym.

2. Rozważmy grupę abelową $(A, \cdot)$. Każda podgrupa grupy abelowej jest normalna, a więc

A jest słabym iloczynem wewnętrznym

$$\Leftrightarrow$$

A jest słabym iloczynem półprostym wewnętrznym

$$\Leftrightarrow$$

A jest słabym iloczynem prostym wewnętrznym.

Uwaga

Niech $(G, \cdot)$ będzie grupą, $H_1, H_2 < G$. Następujące warunki są równoważne:

1. odwzorowanie $\phi : H_1 \times H_2 \rightarrow G$ dane wzorem $\phi(h_1, h_2) = h_1 h_2$ jest izomorfizmem;
2. $G = H_1 H_2$, $H_1 \cap H_2 = \{1\}$ oraz $\forall h_1 \in H_1 \forall h_2 \in H_2 (h_1 h_2 = h_2 h_1)$;
3. G jest słabym iloczynem prostym wewnętrznym podgrup H_1 i H_2 .

Dowód:

(1) $\Rightarrow$ (2) : Ponieważ ϕ jest izomorfizmem, więc jest surjekcją, a zatem $G = H_1 H_2$.

Ustalmy $h_1 \in H_1$, $h_2 \in H_2$.

Wówczas:

$$h_1 h_2 = \phi(h_1, h_2) = ((\phi(h_1, h_2))^{-1})^{-1} = (\phi(h_1^{-1}, h_2^{-1}))^{-1} = (h_1^{-1} h_2^{-1})^{-1}$$

Przypuśćmy, że istnieje $1 \neq g \in H_1 \cap H_2$.

Wówczas $\phi(1, g) = g = \phi(g, 1)$, wbrew założeniu, że ϕ jest izomorfizmem, a więc injekcją.

(2) $\Rightarrow$ (3) : Wystarczy udowodnić, że $H_1 \triangleleft G$ i $H_2 \triangleleft G$.

Ustalmy $g \in G$ i niech $g = h_1 h_2$ dla $h_1 \in H_1$, $h_2 \in H_2$.

Ustalmy $h \in H_1$.

Wówczas:

$$\begin{aligned} ghg^{-1} &= h_1 h_2 h (h_1 h_2)^{-1} = h_1 h_2 h h_2^{-1} h_1^{-1} \\ &= h_1 h_2 h_2^{-1} h h_1^{-1} = h_1 h h_1^{-1} \in H_1, \end{aligned}$$

a zatem $gH_1g^{-1} \subset H_1$.

Podobnie pokazujemy, że $H_2 \triangleleft G$.

(3) $\Rightarrow$ (1) : Ponieważ G jest słabym iloczynem prostym wewnętrznym, a więc w szczególności słabym iloczynem wewnętrznym, więc odwzorowanie ϕ jest dobrze określoną bijekcją.

Ustalmy $(h_1, h_2), (h'_1, h'_2) \in H_1 \times H_2$.

Wówczas:

$$\begin{aligned}\phi((h_1, h_2) \cdot (h'_1, h'_2)) &= \phi(h_1 h'_1, h_2 h'_2) = h_1 h'_1 h_2 h'_2 \\ &= h_1 h_2 h'_1 h'_2 = \phi(h_1, h_2) \phi(h'_1, h'_2),\end{aligned}$$

a więc ϕ jest homomorfizmem.

Definicja

Niech H_1, H_2 będą grupami. Grupę $H_1 \times H_2$ nazywamy **iloczynem (sumą) prostym zewnętrznym grup H_1 i H_2** .

Oznaczenie:

Gdy H_1 i H_2 zapisane są w notacji addytywnej, piszemy $H_1 \oplus H_2$ zamiast $H_1 \times H_2$.

Ze względu na izomorfizm z Uwagi 0.3, będziemy na ogół mówić po prostu o iloczynach (sumach) prostych, bez rozróżniania między słabymi iloczynami (sumami) prostymi wewnętrznymi a iloczynami (sumami) prostymi zewnętrznymi.

Opisane konstrukcje w naturalny sposób przenoszą się na dowolną skończoną liczbę grup.

W ten sposób mówimy o iloczynach (sumach) prostych grup $H_1, \dots, H_n$, które oznaczać będziemy przez $H_1 \times \dots \times H_n$, lub $H_1 \oplus \dots \oplus H_n$ w notacji addytywnej.

Konstrukcje te przenoszą się także na nieskończoną liczbę grup, nie będziemy się jednak nimi zajmować

Torsyjne grupy abelowe;
grupy abelowe skończone.

Definicja

*Grupe nazywamy **torsyjną**, jeżeli każdy element ma rząd skończony.*

*Jeżeli rzędy elementów są wspólnie ograniczone, to ograniczenie to nazywamy **wykładnikiem** grupy.*

*Grupe nazywamy **beztorsyjną**, gdy każdy element ma rząd nieskończony.*

Definicja

Niech $(A, +)$ będzie grupą abelową. Zbiór wszystkich elementów grupy A o skończonym rzędzie nazywamy **częścią torsyjną** grupy i oznaczamy $T(A)$.

Uwaga

Niech $(A, +)$ będzie grupą abelową. Wówczas:

1. $T(A) < A$,
2. $T(T(A)) = T(A)$,
3. jeżeli $B < A$, to $T(B) = B \cap T(A)$,
4. jeżeli $A \cong B$, to $T(A) \cong T(B)$,
5. $T(A \oplus B) = T(A) \oplus T(B)$.

Definicja

Niech $(A, +)$ będzie grupą abelową, niech p będzie liczbą pierwszą. Zbiór wszystkich elementów grupy A , których rząd jest potęgą liczby p nazywamy **p -komponentą** (lub **p -składową**) grupy A i oznaczamy $T_p(A)$.

Uwaga

Niech $(A, +)$ będzie grupą abelową. Wówczas:

1. $T_p(A) < T(A) < A$,
2. $T_p(T_p(A)) = T_p(A) = T_p(T(A))$,
3. jeżeli $B < A$, to $T_p(B) = B \cap T_p(A)$,
4. jeżeli $A \cong B$, to $T_p(A) \cong T_p(B)$,
5. $T_p(A \oplus B) = T_p(A) \oplus T_p(B)$,
6. jeżeli A jest skończenie generowaną torsyjną grupą abelową, to $T_p(A) = \{0\}$ dla prawie wszystkich liczb pierwszych p ,
7. $T_p(A/T_p(A)) = \{0\}$

Twierdzenie

Niech $(A, +)$ będzie grupą abelową torsyjną, niech $p_1, \dots, p_n$ będą wszystkimi liczbami pierwszymi, dla których $T_{p_i}(A) \neq \{0\}$, $i \in \{1, \dots, n\}$. Wówczas:

1. A jest sumą prostą wszystkich swoich p -komponent:

$$A = T_{p_1}(A) \oplus \dots \oplus T_{p_n}(A),$$

2. jeżeli A jest sumą prostą pewnych p -grup $B(p)$, $p \in \{q_1, \dots, q_m\}$, $A = B(q_1) \oplus \dots \oplus B(q_m)$, to $\{p_1, \dots, p_n\} = \{q_1, \dots, q_m\}$ oraz:

$$T_{p_i}(A) = B(p_i), \text{ dla } i \in \{1, \dots, n\}.$$

Dowód:

1. Pokażemy, że $A = T_{p_1} + \dots + T_{p_n}(A)$.

Ustalmy $a \in A$.

Niech $r(a) = n = p_1^{s_1} \cdot \dots \cdot p_k^{s_k}$, dla pewnych liczb pierwszych $p_1, \dots, p_k$, $k \geq n$.

Niech $n_i = \frac{n}{p_i^{s_i}}$, $i \in \{1, \dots, k\}$.

Wówczas $NWD(n_1, \dots, n_k) = 1$, więc istnieją $x_1, \dots, x_k \in \mathbb{Z}$ takie, że

$$n_1x_1 + \dots + n_kx_k = 1.$$

Zatem:

$$n_1x_1a + \dots + n_kx_ka = a.$$

Ponadto dla $i \in \{1, \dots, k\}$, $p_i^{s_i}n_ix_ia = p_i^{s_i}\frac{n}{p_i^{s_i}}x_ia = x_ina = 0$,

a więc $r(n_ix_ia) | p_i^{k_i}$, więc $n_ix_ia \in T_{p_i}(A)$.

Pokażemy, że $A = T_{p_1} \oplus \dots \oplus T_{p_n}(A)$.

Przypuśćmy, że dla pewnego $a \in A$, po ewentualnej zmianie numeracji:

$$a = a_1 + \dots + a_n = b_1 + \dots + b_n, a_i, b_i \in T_{p_i}(A), i \in \{1, \dots, n\},$$

przy czym $a_1 \neq b_1$.

Wówczas:

$$a_1 - b_1 = (b_2 - a_2) + \dots + (b_n - a_n)$$

oraz $a_1 - b_1 \in T_{p_1}(A)$.

Z drugiej strony

$$\begin{aligned} r((b_2 - a_2) + \dots + (b_n - a_n)) & \mid NWW(r(b_2 - a_2), r(b_n - a_n)) \\ & = NWW(p_2^{l_2}, \dots, p_n^{l_n}), \end{aligned}$$

dla pewnych $l_2, \dots, l_n \in \mathbb{N}$.

Zatem $r(a_1 - b_1) = 1$, czyli $a_1 - b_1 = 0$, a więc $a_1 = b_1$, co doprowadza nas do sprzeczności.

2. Ustalmy $i \in \{1, \dots, n\}$.

Zauważmy, że

$$T_{p_i}(B(q)) = \begin{cases} B(p_i), & \text{jeżeli } p_i = q, \\ \{0\}, & \text{jeżeli } p_i \neq q. \end{cases}$$

Wobec tego:

$$\begin{aligned} T_{p_i}(A) &= T_{p_i}(B(q_1) \oplus \dots \oplus B(q_m)) \\ &= T_{p_i}(B(q_1)) \oplus \dots \oplus T_{p_i}(B(q_m)) = B(p_i). \end{aligned}$$

Wniosek (II twierdzenie strukturalne)

Niech $(A, +)$ będzie grupą abelową skończoną, niech $|A| = p_1^{k_1} \cdot \dots \cdot p_n^{k_n}$, gdzie $p_1, \dots, p_n$ są parami różnymi liczbami pierwszymi. Wówczas grupa A ma jednoznaczne przedstawienie w postaci sumy prostej p -grup:

$$A = T_{p_1}(A) \oplus \dots \oplus T_{p_n}(A).$$

Oznaczenie:

Niech $(A, +)$ będzie grupą abelową, niech $p \in \mathbb{P}$ będzie liczbą pierwszą. Oznaczamy:

$$pA = \{pa : a \in A\}.$$

Uwaga

Niech $(A, +)$ będzie grupą abelową, niech $p \in \mathbb{P}$ będzie liczbą pierwszą. Wówczas:

1. $pA < A$,
2. jeżeli A jest skończoną grupą cykliczną oraz $|A| = p^k$, to pA jest grupą cykliczną i $|pA| = p^{k-1}$,
3. jeżeli $B < A$, to $pB = B \cap pA$,
4. jeżeli $A \cong B$, to $pA \cong pB$,
5. $p(A \times B) = pA \times pB$,
6. odwzorowanie $\phi : A \rightarrow pA$ dane wzorem $\phi(a) = pa$ jest surjektywnym homomorfizmem,
7. jeżeli A jest grupą abelową skończoną, to:
 - ▶ gdy $p \mid |A|$, to $|pA| < |A|$,
 - ▶ gdy $p \nmid |A|$, to $|pA| = |A|$.

Twierdzenie

Niech $(A, +)$ będzie skończoną p -grupą abelową. Wówczas grupa A jest sumą prostą p -grup cyklicznych.

Dowód:

Niech $|A| = p^n$.

Dowód prowadzimy indukcyjnie względem n .

Jeżeli $n = 1$, to $|A| = p$, a zatem $A \cong \mathbb{Z}_p$ i A nie ma właściwych podgrup, a sama jest grupą cykliczną. Jeżeli $n > 1$, to założmy, że twierdzenie jest prawdziwe dla wszystkich liczb $l \in \mathbb{N}$, $l < n$.

Wobec ostatniej części Uwagi 0.6, $|pA| < |A|$, niech więc $|pA| = p^l$, dla $l < n$.

Wobec założenia indukcyjnego

$$pA = \langle a_1 \rangle \oplus \dots \oplus \langle a_r \rangle,$$

dla pewnych elementów $a_1, \dots, a_r \in pA$ o rzędach będących potęgami liczby p .

Niech $x_1, \dots, x_r \in A$ będą takimi elementami, że $a_1 = px_1, \dots, a_r = px_r$.

Pokażemy, że $\langle x_1 \rangle + \dots + \langle x_r \rangle$ jest grupą, która jest sumą prostą grup $\langle x_1 \rangle, \dots, \langle x_r \rangle$.

Sprawdzenie, że jest to istotnie grupa, pozostawiamy jako ćwiczenie, a dla udowodnienia, że jest to suma prosta, przypuśćmy, że

$$k_1 x_1 = k_2 x_2 + \dots + k_r x_r,$$

dla pewnych $k_1, \dots, k_r \in \mathbb{N}$.

Wówczas

$$k_1 p x_1 = k_2 p x_2 + \dots + k_r p x_r,$$

i ponieważ $\langle a_1 \rangle \oplus \dots \oplus \langle a_r \rangle$ jest sumą prostą, więc

$k_1 = k_2 = \dots = k_r = 0$ i tym samym

$$\langle x_1 \rangle \cap (\langle x_2 \rangle + \dots + \langle x_r \rangle) = \{0\}.$$

Podobnie sprawdzamy, że

$$\langle x_i \rangle \cap (\langle x_1 \rangle + \dots + \langle x_{i-1} \rangle + \langle x_{i+1} \rangle + \dots + \langle x_r \rangle) = \{0\}, \text{ dla } i \in \{2, \dots, r\}.$$

Niech zatem $H = \langle x_1 \rangle \oplus \dots \oplus \langle x_r \rangle$.

Rozważmy rodzinę

$$\mathcal{B} = \{B < A : B \cap H = \{0\}\}.$$

Jako rodzina podgrup grupy skończonej $\mathcal{B}$ jest skończona, w szczególności zawiera element maksymalny.

Oznaczmy go przez B . Zauważmy, że $B + H$ jest grupą oraz wobec określenia B jest to suma prosta grup B i H .

Pokażemy, że $A = B \oplus H$. Inkluzja $(\supset)$ jest oczywista, pozostaje wykazać inkluzję $(\subset)$.

Przypuśćmy, że istnieje $a \in A$ taki, że $a \notin B + H$.

Wówczas $pa = ph$ dla pewnego $h \in H$. Ponadto $c = a - h \notin B + H$ oraz $pc = pa - pb = 0$.

Wobec maksymalności B , $\langle \{c\} \cup B \rangle \cap H \neq \{0\}$, a więc istnieją $h_1 \in H$ oraz $b_1 \in B$ takie, że

$$0 \neq h_1 = kc + b_1, \text{ oraz } 0 < k < p.$$

Ponieważ $NWD(k, p) = 1$, więc dla pewnych $s, t \in \mathbb{Z}$:

$$sk + tp = 1,$$

a więc

$$c = (sk + tp)c = skc = sh_1 - sb_1 \in H + B,$$

co daje sprzeczność.

Dla zakończenia dowodu zauważmy, że $|B| < |A|$, więc B jest sumą prostą p -grup cyklicznych.

Wobec tego B i H są sumami prostymi grup cyklicznych oraz $A = B \oplus H$. $\square$

Przykłady:

3. Rozważmy skończoną p -grupe abelową $\mathbb{Z}_2 \times \mathbb{Z}_2$. Wówczas:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (1, 1) \rangle \oplus \langle (1, 0) \rangle = \langle (1, 0) \rangle \oplus \langle (0, 1) \rangle.$$

Twierdzenie

Niech $(A, +)$ będzie skończoną p -grupą abelową. Niech

$$A = A_1 \oplus \dots \oplus A_r \text{ oraz } A = B_1 \oplus \dots \oplus B_s$$

będą dwoma różnymi rozkładami na sumy proste grup cyklicznych. Przyjmijmy, że

$$|A_1| \leq |A_2| \leq \dots \leq |A_r| \text{ oraz } |B_1| \leq |B_2| \leq \dots \leq |B_s|.$$

Wówczas $r = s$ oraz $|A_i| = |B_i|$ dla $i \in \{1, \dots, r\}$.

Dowód:

Niech $|A_i| = p^{\alpha_i}$, $|B_j| = p^{\beta_j}$, $i \in \{1, \dots, r\}$, $j \in \{1, \dots, s\}$.

Wówczas $|A| = p^{\alpha_1} \cdot \dots \cdot p^{\alpha_r} = p^{\beta_1} \cdot \dots \cdot p^{\beta_s}$, więc w szczególności $\alpha_1 + \dots + \alpha_r = \beta_1 + \dots + \beta_s$.

Dowód prowadzimy indukcyjnie względem $\alpha_1 + \dots + \alpha_r$.

Jeżeli $\alpha_1 + \dots + \alpha_r = 1$, to za bardzo nie ma czego dowodzić.

Założmy więc, że $\alpha_1 + \dots + \alpha_r > 1$ i że twierdzenie jest prawdziwe dla p -grup A rzędów mniejszych od $p^{\alpha_1 + \dots + \alpha_r}$.

Niech $0 \leq k \leq r$ oraz $0 \leq l \leq s$ będą takimi liczbami, że

$$|A_1| = \dots = |A_k| = p \text{ oraz } |B_1| = \dots = |B_l| = p.$$

Wówczas $|A| = p^{k+\alpha_{k+1}+\dots+\alpha_r} = p^{l+\beta_{l+1}+\dots+\beta_s}$.

Ponadto:

$$pA = pA_1 \oplus \dots \oplus pA_r = pA_{k+1} \oplus \dots \oplus pA_r$$

oraz

$$pA = pB_1 \oplus \dots \oplus pB_s = pB_{l+1} \oplus \dots \oplus pB_s,$$

a zatem

$$pA_{k+1} \oplus \dots \oplus pA_r = pB_{l+1} \oplus \dots \oplus pB_s,$$

przy czym pA_i i pB_j , $i \in \{k+1, \dots, r\}$, $j \in \{l+1, \dots, s\}$ są grupami cyklicznymi, których rzędy spełniają zależności:

$$|pA_i| = p^{\alpha_i-1}, i \in \{k+1, \dots, r\} \text{ oraz } |pB_j| = p^{\beta_j-1}, j \in \{l+1, \dots, s\}.$$

Ponadto $|pA| < |A|$ i zachodzi

$$|pA_{k+1}| \leq \dots \leq |pA_r| \text{ oraz } |pB_{l+1}| \leq \dots \leq |pB_s|.$$

Wobec założenia indukcyjnego $r - k = s - l$ oraz

$$|pA_{k+1}| = |pB_{l+1}|, \dots, |pA_r| = |pB_s|,$$

skąd $p^{\alpha_{k+1}-1} = p^{\beta_{l+1}-1}, \dots, p^{\alpha_r-1} = p^{\beta_s-1}$, więc i $p^{\alpha_{k+1}} = p^{\beta_{l+1}}, \dots, p^{\alpha_r} = p^{\beta_s}$, skąd $\alpha_{k+1} = \beta_{l+1}, \dots, \alpha_r = \beta_s$. Tym samym z równości

$$k + \alpha_{k+1} + \dots + \alpha_r = l + \beta_{l+1} + \dots + \beta_s$$

wynika $k = l$, czyli $|A_i| = |B_i|$ dla $i \in \{1, \dots, r\}$. $\square$

Wniosek (I twierdzenie strukturalne)

Niech $(A, +)$ będzie grupą abelową skończoną. Wówczas istnieje przedstawienie A w postaci sumy prostej p -grup cyklicznych

$$A = A_{11} \oplus \dots \oplus A_{1k_1} \oplus A_{21} \oplus \dots \oplus A_{2k_2} \oplus \dots \oplus A_{s1} \oplus \dots \oplus A_{sk_s},$$

przy czym $|A_{11}| = p_1^{t_{11}}, \dots, |A_{1k_1}| = p_1^{t_{1k_1}},$

$|A_{21}| = p_2^{t_{21}}, \dots, |A_{2k_2}| = p_2^{t_{2k_2}}, \dots,$

$|A_{s1}| = p_s^{t_{s1}}, \dots, |A_{sk_s}| = p_s^{t_{sk_s}},$ gdzie $p_1, \dots, p_s$ są parami

różnymi liczbami pierwszymi, wykładniki dobrane są tak, aby

$t_{11} \leq \dots \leq t_{1k_1}, t_{21} \leq \dots \leq t_{2k_2}, \dots, t_{s1} \leq \dots \leq t_{sk_s}$ oraz ciąg liczb $t_{11}, \dots, t_{1k_1}, t_{21}, \dots, t_{2k_2}, \dots, t_{s1}, \dots, t_{sk_s}$ jest jednoznacznie wyznaczony przez grupę A . W szczególności:

$$|A| = p_1^{t_{11} + \dots + t_{1k_1}} p_2^{t_{21} + \dots + t_{2k_2}} \cdot \dots \cdot p_s^{t_{s1} + \dots + t_{sk_s}}.$$

Ciąg

$$(p_1^{t_{11}}, \dots, p_1^{t_{1k_1}}, p_2^{t_{21}}, \dots, p_2^{t_{2k_2}}, \dots, p_s^{t_{s1}}, \dots, p_s^{t_{sk_s}})$$

występujący w I twierdzeniu strukturalnym nazywamy **typem** skończonej grupy abelowej A , a jego elementy **niezmiennikami**.

Przykłady:

4. Rozważmy skończoną grupę abelową $\mathbb{Z}_{60}$. Wówczas, skoro $60 = 2^2 \cdot 3 \cdot 5$, to

$$\mathbb{Z}_{60} = T_2(\mathbb{Z}_{60}) \oplus T_3(\mathbb{Z}_{60}) \oplus T_5(\mathbb{Z}_{60}).$$

$T_2(\mathbb{Z}_{60}), T_3(\mathbb{Z}_{60}), T_5(\mathbb{Z}_{60})$, jako podgrupy grupy cyklicznej o rzędach, odpowiednio, 4, 3 i 5 są cykliczne, a więc $T_2(\mathbb{Z}_{60}) \cong \mathbb{Z}_4, T_3(\mathbb{Z}_{60}) \cong \mathbb{Z}_3, T_5(\mathbb{Z}_{60}) \cong \mathbb{Z}_5$. Tym samym

$$\mathbb{Z}_{60} = \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

i $\mathbb{Z}_{60}$ ma typ $(4, 3, 5)$.