6. Rozszerzenia. Produkt i produkt półprosty

Zdefiniowaliśmy pojęcie podgrupy normalnej. Jeżeli $N \trianglelefteq G$, to zdefiniowana jest grupa ilorazowa i rzutowanie $\pi : G \longrightarrow G/N$. Powstaje pytanie, do jakiego stopnia struktura grupy G jest zdeterminowana przez grupy N i G/N. Czy klasa izomorfizmu grupy G jest wyznaczona jednoznacznie przez N i G/N? Czy może jest tak przy jakichś jeszcze dodatkowych założeniach o położeniu podgrupy N w grupie G? A może przy jeszcze jakichś dodatkowych informacjach?

Przejdziemy do sytuacji, gdy grupa G *posiada* podgrupę normalną N, o której na razie nic więcej nie zakładamy. Wówczas N jest oczywiście jądrem rzutowania π grupy G na iloraz G/N. Możemy to zapisać w następującej postaci:

$$N \longrightarrow G \xrightarrow{\pi} G/N.$$

Bardziej ogólnie:

6.1. Definicja. *Mówimy, że grupa G jest* **rozszerzeniem grupy** N **za pośrednictwem grupy** H, *jeżeli istnieją: monomorfizm i oraz epimorfizm π, $N \xrightarrow{i} G \xrightarrow{\pi} H$, takie że* $\ker \pi = \operatorname{im} i$.

Oczywiście z twierdzenia o homomorfizmie wynika, że jeżeli grupa G jest rozszerzeniem grupy N za pośrednictwem grupy H, to H jest izomorficzna z grupą ilorazową G/N. Definicja dopuszcza możliwości $N = 1$ i $N = G$. Rozszerzenia $G \xrightarrow{id} G \longrightarrow 1$ i $1 \longrightarrow G \xrightarrow{id} G$ są jednak mało interesujące. Oczywiście grup prostych nie można w nietrywialny sposób przedstawić jako rozszerzenie. Na drugim biegunie leżą $p-$ grupy. które można przedstawić jako kolejne rozszerzenia za pośrednictwem grupy $\mathbb{Z}_p$.

6.2. Twierdzenie. *Jeżeli G jest p-grupą i $|G| = p^m$, to istnieje ciąg podgrup*

$$\mathbf{1} = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_{m-1} \leqslant G_m = G,$$

taki że $G_i \trianglelefteq G$ i $|G_i| = p^i$.

Dowód. Zastosujemy indukcję ze względu na m. Teza jest oczywista dla $m = 0$. Załóżmy, że teza jest prawdziwa dla $m-1$, gdzie $m > 0$. Niech z będzie nietrywialnym elementem rzędu p w centrum grupy G (istnienie takiego elementu wynika z nietrywialności $Z(G)$ i z twierdzenia Cauchy'ego). Niech $G_1 = \langle z \rangle$. Oczywiście $G_1 \trianglelefteq G$, bo $G_1 \leqslant Z(G)$. Grupa G/G_1 jest rzędu p^{m-1}, zatem na mocy założenia indukcyjnego istnieje ciąg podgrup normalnych $H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{m-2} \leqslant H_{m-1} = G/G_1$. Przyjmując $G_0 = \mathbf{1}$, a dla $i \geq 1$, $G_i = \pi^{-1}(H_{i-1})$, gdzie $\pi : G \longrightarrow G/G_1$, otrzymujemy szukany ciąg podgrup grupy G. $\square$

Jak można się spodziewać, informacja że G jest rozszerzeniem grupy N za pośrednictwem grupy H nie wystarczy do zidentyfikowania typu izomorficznego grupy G.

Przykłady

a) $\mathbb{Z}_2 \trianglelefteq \mathbb{Z}_4 \to \mathbb{Z}_2$.
b) $\mathbb{Z}_2 \trianglelefteq \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$.
c) $SO(n) \trianglelefteq O(n) \to Z_2$.

d) $\mathbb{R}^n \trianglelefteq Aff(n) \to GL(n, \mathbb{R}^n)$, gdzie $Aff(n)$ jest grupą izomorfizmów afinicznych przestrzeni $\mathbb{R}^n$.
e) Grupa $\mathbb{R}^n \trianglelefteq Iso(n) \to O(n)$, gdzie $Iso(n)$ jest grupą izometrii przestrzeni $\mathbb{R}^n$ (wyposażonej w iloczyn skalarny).
4) $A_n \trianglelefteq \Sigma_n \to \mathbb{Z}_2$
e) $J \trianglelefteq D_{2n} \to \mathbb{Z}_2$.

Dalsze rozważania poprzedzimy następującą obserwacją.

6.3. Uwaga. *Niech $N \trianglelefteq G$ i niech $K \leqslant G$. Wówczas:*
a) zbiór $K \cdot N = \{kn : k \in K, n \in N\}$ jest podgrupą. Jest to podgrupa generowana przez $K \cup N$. W szczególności $K \cdot N = N \cdot K$.
b) jeżeli dodatkowo $K \cap N = \{1\}$, to przedstawienie elementu $K \cdot N$ w postaci iloczynu $k \cdot n$, $k \in K$, $n \in N$ jest jednoznaczne.

Dowód.
a) Wystarczy sprawdzić, że działania grupowe nie wyprowadzają poza zbiór $K \cdot N$:

$$k_1 n_1 k_2 n_2 = k_1 k_2 \underbrace{k_2^{-1} n_1 k_2}\, n_2 = k_1 k_2 n_1' n_2 \text{ gdzie } n_1' = k_2^{-1} n_1 k_2 \in N$$

$$(kn)^{-1} = n^{-1} k^{-1} = k^{-1} \underbrace{k n^{-1} k^{-1}} = k^{-1} n' \text{ gdzie } n' = k n^{-1} k^{-1} \in N.$$

Ponieważ $K \cdot N \subset < K \cup N >$ i $K \cdot N$ jest podgrupą, to $K \cdot N =< K \cup N >$. Równość $K \cdot N = N \cdot K$ jest oczywista.
b) Jeżeli $k_1 n_1 = k_2 n_2$, to $k_2^{-1} k_1 = n_2 n_1^{-1} \in K \cap N$. Zatem $k_2^{-1} k_1 = n_2 n_1^{-1} = 1$ i $k_1 = k_2$, $n_1 = n_2$. □

Niech $N \trianglelefteq G$ i załóżmy, że podgrupa normalna jest położona w rozpatrywanej grupie w szczególnie dobry sposób, opisany w następującej definicji.

6.4. Definicja. *Niech $N \trianglelefteq G$. Podgrupę $K \leqslant G$ nazywamy* **dopełnieniem** *podgrupy N wtedy i tylko wtedy, gdy $N \cap K = 1$ i $N \cdot K = G$. Grupę G nazywamy wówczas* **produktem półprostym wewnętrznym** *podgrupy normalnej N i jej dopełnienia K.*

Odnotujmy jeszcze przydatny wniosek dla grup skończonych.

6.5. Wniosek. *Jeżeli $N \trianglelefteq G$, $K \leqslant G$, $N \cap K = 1$ i $|N| \cdot |K| = |G| < \infty$, to $NK = G$, czyli G jest produktem półprostym wewnętrznym N i K.*

Dowód. Na mocy Uwagi 6.3 b) zbiór ND ma $|N| \cdot |D| = |G|$ elementów, czyli rzeczywiście $ND = G$. □

Przypomnijmy następujące oznaczenie: φ_x jest automorfizmem wewnętrznym grupy G zadanym wzorem $\varphi_x(a) = xax^{-1}$. Jeżeli $N \trianglelefteq G$ i $K \leqslant G$ jest podgrupą, to mamy homomorfizm $\Phi : K \to Aut(N)$, który elementowi $k \in K$ przyporządkowuje element φ_k. Zauważmy, że jeżeli G jest produktem półprostym wewnętrznym N i K, to struktura grupy G jest wyznaczona przez strukturę grupy N, grupy K oraz homomorfizm $\Phi : K \to Aut(N)$:

$$n_1 k_1 n_2 k_2 = n_1 \underbrace{k_1 n_2 k_1^{-1}}\, k_1 k_2 = n_1 \varphi_{k_1}(n_2) k_1 k_2$$

$$(nk)^{-1} = k^{-1} n^{-1} = \underbrace{k^{-1} n^{-1} k}\, k^{-1} = \varphi_{k^{-1}}(n^{-1}) k^{-1}.$$

Jest oczywiste, że $\pi : G = N \cdot K \to K$ zadane wzorem $\pi(nk) = k$ jest epimorfizmem o jądrze N. Zatem produkt półprosty wewnętrzny N i K jest rozszerzeniem

$$N \trianglelefteq N \cdot K \xrightarrow{\pi} K.$$

Wśród wymienionych powyżej przykładów tylko a) czyli $\mathbb{Z}_2 \trianglelefteq \mathbb{Z}_4$ nie ma dopełnienia. Pozostałe przykłady są produktami półprostymi wewnętrznymi. Z przykładów tych wynika też, że dopełnienie nie jest wyznaczone jednoznacznie. W przykładach b) i c) dla n nieparzystego można znaleźć dopełnienie, które jest podgrupą normalną. Jeżeli *tak jest*, to jest to sytuacja już nam znana:

6.6. Definicja. *Jeżeli $M, N \trianglelefteq G$, $N \cap M = 1$ i $N \cdot M = G$, to grupę G nazywamy* **produktem prostym wewnętrznym** *podgrup N i M.*

Pojęcie produktu prostego wewnętrznego jest bardzo zbliżone do pojęcia produktu grup, zdefiniowanego w rozdziale 1.

6.7. Twierdzenie. *Jeżeli grupa G jest produktem prostym wewnętrznym podgrup $M, N \trianglelefteq G$, to G jest izomorficzna z produktem $M \times N$. Odwzorowanie $f : M \times N \to G$ zadane wzorem $f(m, n) = mn$ jest izomorfizmem.*

Dowód. Zaczniemy od wykazania, że $\forall_{x \in M} \forall_{y \in N}\ xy = yx$. Oczywiście $xy = yx \Leftrightarrow xyx^{-1}y^{-1} = 1$. Zauważmy, że

$$xyx^{-1}y^{-1} = (xyx^{-1})y^{-1}.$$

Ale $xyx^{-1} \in N$, bo N jest podgrupą normalną. Również $y^{-1} \in N$. Zatem

$$xyx^{-1}y^{-1} \in N. \tag{1}$$

Analogicznie, wykorzystując normalność M, pokazujemy, że

$$x(yx^{-1}y^{-1}) \in M. \tag{2}$$

Zestawiając fakty (1) i (2) wnioskujemy, że $xyx^{-1}y^{-1} \in M \cap N = \mathbf{1}$, czyli $xyx^{-1}y^{-1} = 1$, a więc istotnie $xy = yx$. Teraz już łatwo sprawdzić, że $f((m_1, n_1)(m_2, n_2)) = f(m_1m_2, n_1n_2) = m_1m_2n_1n_2 = (m_1n_1)(m_2n_2) = f(m_1, n_1)f(m_2, n_2)$, co dowodzi, że f jest homomorfizmem. Zatem jest też *izo*morfizmem, bo oczywiście jest bijekcją (co wynika z Uwagi 6.3). □

Zauważmy, że dla grup skończonych mamy następujące użyteczne kryterium:

6.8. Wniosek. *Jeżeli $N \trianglelefteq G$, $D \trianglelefteq G$, $N \cap D = 1$ i $|N| \cdot |D| = |G| < \infty$, to G jest produktem prostym wewnętrznym N i D.*

Na koniec zauważmy jeszcze, że prawdziwa jest następująca:

6.9. Uwaga. *Niech $M \leqslant G$, $N \leqslant G$ i zbiór $M \cdot N = G$. Jeżeli dla każdego $x \in M$, każdego $y \in N$, $xy = yx$, to $M \trianglelefteq G$ i $N \trianglelefteq G$.*

Dowód. Niech $g \in G$. Musimy pokazać, że $gMg^{-1} \subset M$. Niech $m \in M$. Mamy $g = xy$, $x \in M$, $y \in N$. Mamy $gmg^{-1} = xymy^{-1}x^{-1}$, ale elementy z M i N są przemienne, więc $x \underbrace{ym}y^{-1}x^{-1} = xmx^{-1} \in M$. Dla $N \leqslant G$ rachunek jest analogiczny. □

6.10. Definicja. *Gupa G nazywa się nierozkładalna jeżeli nie jest produktem wewnętrznym swoich podgrup właściwych.*