3. Wykład

Stwierdzenie 3.1. *Niech H i K będą grupami i niech $\alpha : K \to \operatorname{Aut}(H)$ będzie homomorfizmem. Wówczas*

$$G_H = \{(x, e_K) \,|\, x \in H\} \qquad \text{oraz} \qquad G_K = \{(e_H, p) \,|\, p \in K\}$$

są podgrupami w $G = H \rtimes_\alpha K$. Ponadto G_K jest izomorficzna z K, a G_H jest podgrupą normalną izomorficzną z H, mamy

$$G_H \cap G_K = \{(e_H, e_K)\} = \{e_G\}$$

i każdy element $H \rtimes_\alpha K$ można zapisać jako iloczyn ab elementów $a \in G_H$, $b \in G_K$.

Twierdzenie 3.2. *Niech G będzie grupą i niech H i K będą podgrupami grupy G. Załóżmy, że H jest podgrupą normalną i oznaczmy przez ι_K włożenie K w G. Wówczas następujące warunki są równoważne:*

(1) *każdy element grupy G można zapisać jako iloczyn ab dla pewnego $a \in H$ i $b \in K$ oraz $H \cap K = e$,*
(2) *każdy element grupy G można zapisać jako iloczyn ba dla pewnego $a \in H$ i $b \in K$ oraz $H \cap K = e$,*
(3) *każdy element grupy G można zapisać na dokładnie jeden sposób jako iloczyn ab dla pewnego $a \in H$ i $b \in K$,*
(4) *każdy element grupy G można zapisać na dokładnie jeden sposób jako iloczyn ba dla pewnego $a \in H$ i $b \in K$,*
(5) *złożenie $q_H \circ \iota_K$ jest izomorfizmem $K \to G/H$,*
(6) *istnieje homomorfizm $\phi : G \to K$, taki, że $\phi \circ \iota_K = \mathrm{id}_K$ i $\ker \phi = H$,*
(7) *istnieje homomorfizm $\alpha : K \to \operatorname{Aut}(H)$ i izomorfizm $\Phi : H \rtimes_\alpha K \to G$ taki, że $\Phi(a, e) = a$ i $\Phi(e, b) = b$.*

Dowód. Wykażemy następujące implikacje:

$$\begin{tikzcd}
& (6) \arrow[r, Leftrightarrow] \arrow[d, Rightarrow] & (5) \\
& (1) \arrow[r, Leftrightarrow] \arrow[d, Leftrightarrow] & (3) \arrow[ul, Rightarrow] \arrow[d, Rightarrow] \\
(4) \arrow[r, Leftrightarrow] & (2) & (7) \arrow[ul, Rightarrow]
\end{tikzcd}$$

"(1)⇒(3)" Niech $x \in G$. Jeśli $x = ab = a'b'$ dla $a, a' \in H$, $b, b' \in K$. Wówczas

$$e = x^{-1}x = (ab)^{-1}a'b' = b^{-1}a^{-1}a'b' = \big((b^{-1}a^{-1}b)(b^{-1}a'b)\big)(b^{-1}b') = a_0 b_0$$

gdzie $a_0 \in H$ (bo H jest normalna), $b_0 \in K$. Ale to oznacza, że $b_0 = a_0^{-1} \in H$, czyli $b_0 \in H \cap K$. Stąd, jeśli $H \cap K = \{e\}$, to $b_0 = e$, a co za tym idzie $b = b'$ i $a = a'$.

"(3)⇒(1)" Niech $y \in H \cap K$. Wówczas dla $a = y \in H$, $a' = e \in H$, oraz $b = e \in K$, $b' = y \in K$ mamy $y = ab = a'b'$. Skoro przedstawienie y w postaci iloczynu elementu H i K jest jednoznaczne, dostajemy $y = e$.

Tak samo jak równoważności (1)⇔(3) dowodzimy (2)⇔(4).

Z kolei równoważność (1)⇔(2) mamy stosując odwrotność: jeśli każdy $x \in G$ można zapisać jako ab dla $a \in H$, $b \in K$, to zapisujemy tak element x^{-1}, czyli mamy $x^{-1} = ab$. Wówczas $x = b^{-1}a^{-1}$. W ten sposób wykazaliśmy implikację ⇒. Przeciwnej implikacji dowodzimy tak samo.

"(5)⇒(6)" Niech $\phi = (q_H \circ \iota_K)^{-1} \circ q_H$. Wówczas $\ker \phi = H$, gdyż $(q_H \circ \iota_K)^{-1}$ jest izomorfizmem $G/H \to K$. Oczywiście mamy również

$$\phi \circ \iota_K = (q_H \circ \iota_K)^{-1} \circ q_H \circ \iota_H = \mathrm{id}_K.$$

"(6)⇒(5)" Na mocy twierdzenia 2.4 z wykładu 2 istnieje monomorfizm $\varphi : G/H \to K$ taki, że

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "q_H"'] & K \\ G/H \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Skoro $\phi \circ \iota_K = \mathrm{id}_K$, odwzorowanie φ jest izomorfizmem. Stąd

$$q_H \circ \iota_K = (\varphi^{-1} \circ \phi) \circ \iota_K = \varphi^{-1} \circ (\phi \circ \iota_K) = \varphi^{-1}$$

jest izomorfizmem.

"(6)⇒(1)" Niech $x \in G$. Połóżmy $b = \phi(x)$ i $a = xb^{-1}$. Mamy oczywiście $x = ab$. Ponadto

$$\phi(a) = \phi(x)\phi(b^{-1}) = bb^{-1} = e_K,$$

więc $a \in \ker\phi = H$. Niech teraz $t \in H \cap K$. Wówczas $\phi(t) = e$, bo $t \in \ker\phi$ i $\phi(t) = t$, bo $t \in K$. Stąd $t = e$ i mamy $H \cap K = e$.

"(3)⇒(6)" Dla $x \in G$ mamy $x = ab$ dla jedynej pary $(a, b) \in H \times K$. Połóżmy $\phi(x) = b$. Jest jasne, że $\phi \circ \iota_K = \mathrm{id}_K$ i $\phi^{-1}(\{e\}) = H$. Sprawdzamy, że ϕ jest homomorfizmem: niech $x, y \in G$ mają rozkłady $x = ab$, $y = a'b'$. Wtedy

$$xy = aba'b' = (aba'b^{-1})bb'$$

i element $aba'b^{-1}$ należy do H (normalność). Oznacza to, że $\phi(xy) = bb' = \phi(x)\phi(y)$.

Implikacja (7)⇒(1) jest treścią stwierdzenia 3.1.

"(3)⇒(7)" Zdefiniujmy $\alpha : K \to \mathrm{Aut}(H)$ kładąc

$$\alpha_b(a) = bab^{-1}.$$

Wówczas α jest homomorfizmem. Niech $\Phi(a, b) = ab$. Odwzorowanie Φ jest bijekcją i odwzorowanie odwrotne dane jest przez $G \ni x = ab \mapsto (a, b)$. Sprawdzamy, że Φ jest homomorfizmem:

$$\Phi(a, b)\Phi(a', b') = aba'b' = (aba'b^{-1})bb' = a\alpha_b(a')bb' = \Phi\big(a\alpha_b(a'), bb'\big) = \Phi\big((a, b)(a', b')\big).$$

□

3.0.1. *Przykłady.*

(1) $S_3 = \mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_2$, $\alpha_1(k) = -k$.
(2) $D_{2n} = \mathbb{Z}_n \rtimes_\alpha \mathbb{Z}_2$, $\alpha_1(k) = -k$.
(3) Grupa wszystkich odwzorowań $\mathbb{R} \to \mathbb{R}$ postaci $f(x) = ax + b$ gdzie $a, b \in \mathbb{R}$, $a \neq 0$ jest iloczynem półprostym grupy $\mathbb{R}$ przez $\mathbb{R}^\times$ (grupa liczb rzeczywistych różnych od zera z mnożeniem jako działaniem grupowym).
(4) Grupa izometrii $\mathbb{R}^2 \to \mathbb{R}^2$ (nie koniecznie liniowych) jest iloczynem półprostym grupy translacji (izomorficznej z $\mathbb{R}^2$) przez grupę liniowych izometrii $\mathbb{R}^2 \to \mathbb{R}^2$, tj. odwzorowań ortogonalnych $\mathbb{R}^2 \to \mathbb{R}^2$. Ta ostatnia grupa też jest iloczynem półprostym (jakim?).
(5) Fizyka dostarcza niezliczonych przykładów.

Działania grup

Definicja 3.3. Niech G będzie grupą i niech X będzie zbiorem. *Działaniem G na X* nazywamy homomorfizm α z grupy G w grupę S_X wszystkich bijekcji zbioru X na siebie.

3.0.2. *Standardowe oznaczenia.* Niech G będzie grupą, X zbiorem i niech $\alpha : G \to S_X$ będzie działaniem. Dla $t \in G$ wartość bijekcji $\alpha(t)$ na elemencie $x \in X$ oznaczamy symbolem $t \cdot x$, a czasem po prostu tx. Taka notacja pomija symbol "α", ale jest czasem bardzo wygodna. Fakt, że α jest homomorfizmem zapisujemy teraz tak:

$$(ts) \cdot x = t \cdot (s \cdot x) \tag{1}$$

dla wszystkich $t, s \in G$ i $x \in X$. Działanie G na X często definiuje się jako odwzorowanie

$$G \times X \ni (t, x) \longmapsto t \cdot x \in X$$

spełniające (1) i $e \cdot x = x$ dla wszystkich $x \in X$. Czytelnik łatwo sprawdzi, że obie definicje są równoważne.

3.0.3. *Przykłady.*

(1) Niech W będzie dowolnym zbiorem. Wówczas grupa S_W wszystkich bijekcji $W \to W$ działa na W.

(2) Grupa permutacji n elementów S_n działa na przestrzeni wielomianów n zmiennych: dla $\sigma \in S_n$ i $f \in \mathbb{F}[\mathfrak{X}_1, \dots, \mathfrak{X}_n]$ definiujemy

$$(\sigma \cdot f)(\mathfrak{X}_1, \dots, \mathfrak{X}_n) = f(\mathfrak{X}_{\sigma^{-1}(1)}, \dots, \mathfrak{X}_{\sigma^{-1}(n)})$$

(3) Niech X będzie przestrzenią wektorową nad pewnym ciałem $\mathbb{F}$. Zbiór $\mathrm{Aut}(X)$ jest grupą względem składania odwzorowań, a

$$\mathrm{Aut}(X) \times X \ni (U, x) \longmapsto Ux \in X$$

jest działaniem $\mathrm{Aut}(X)$ na X. W tym kontekście grupę $\mathrm{Aut}(X)$ oznaczamy symbolem $\mathrm{GL}(X)$ (oznaczenie pochodzi z języka angielskiego: general linear (group)) Jeśli X jest skończenie wymiarowa, to wybierając bazę X możemy utożsamiać odwzorowania liniowe $X \to X$ z opowiadającymi im macierzami. Wówczas $\mathrm{GL}(X)$ można utożsamić z grupą tworzoną przez wszystkie odwracalne macierze $n \times n$ o wyrazach z ciała $\mathbb{F}$ (gdzie $n = \dim X$). Wówczas używamy symbolu $\mathrm{GL}(n, \mathbb{F})$ lub $\mathrm{GL}_n(\mathbb{F})$.

(4) Rozważmy grupę $\mathrm{GL}(n, \mathbb{F})$ dla pewnego ciała $\mathbb{F}$. Odwzorowanie $\det : \mathrm{GL}(n, \mathbb{F}) \to \mathbb{F}^\times$ jest na mocy twierdzenia Cauchyego (multyplikatywność wyznacznika) homomorfizmem. Jego jądro oznaczamy symbolem $\mathrm{SL}(n, \mathbb{F})$ lub $\mathrm{SL}_n(\mathbb{F})$ (od angielskiego special linear (group)).