Teoria grup I

Wykład 2

1 Wprowadzenie do wykładu, cz. II

Grupy „dyskretne”: $\mathbb{Z}^n$, „symetrie podłogi” (nieskończone), S_n, D_n (skończone).

Grupy „ciągłe”: $(\mathbb{R}^n, +), (\mathbb{R}_{>0}, \cdot), (\mathbb{R}_{\neq 0}, \cdot), (\mathbb{C}_{\neq 0}, \cdot), GL(X), SL(X), O(1,3)$ (niezwarte), $U(1), O(X)$, $SO(X)$ (zwarte).

Grupy topologiczne (Liego): Są to grupy (G, μ) takie, że G jest wyposażone w strukturę przestrzeni topologicznej (rozmaitości rózniczkowej) o tej własności, że odwzorowanie $\mu : G \times G \to G$ oraz odwzorowanie $\epsilon : g \mapsto g^{-1} : G \to G$ są ciągłe (gładkie).

Uwaga: Jeśli G jest grupa topologiczną (Liego), w poniższych definicjach wymagamy ciąłości (gładkości) wszystkich odwzorowań.

Reprezentacja grupy G w przestrzeni liniowej X: działanie $\nu : G \times X \to X$ takie, że dla każdego $g \in G$ odwzorowanie $\nu(g, \cdot) : X \to X$ jest liniowe.

Przykład: naturalna reprezentacja grup $GL(X), SL(X), O(X), SO(X), O(1,3), D_n$ w przestrzeni X.

Homomorfizm grup: Odwzorowanie $f : G_1 \to G_2$ pomiędzy dwiema grupami o własnościach:

$$f(e_1) = e_2, \;\; f(a \cdot_1 b) = f(a) \cdot_2 f(b) \;\; \forall a, b \in G_1.$$

Izomorfizm grup: Homomorfizm $f : G_1 \to G_2$ będący bijekcją. *Uwaga:* Odwrotne odwzorowanie $f^{-1} : G_2 \to G_1$ automatycznie jest homomorfizmem: $f^{-1}(c \cdot d) = f^{-1}(f(f^{-1}(c)) \cdot f(f^{-1}(d))) = f^{-1}(f(f^{-1}(c) \cdot f^{-1}(d))) = f^{-1}(c) \cdot f^{-1}(d)$.
Grupa automorfizmów grupy G: Nawiasem mówiąc, otrzymaliśmy jeszcze jeden przykład grupy $S_{X,\mathfrak{S}}$: $\mathfrak{S}$ jest strukturą grupy na zbiorze $X = G$, a $S_{X,\mathfrak{S}}$ grupą izomorfizmów z G w G, które nazywamy *automorfizmami* G. Oznaczamy $\mathrm{Aut}(G) := S_{G,\mathfrak{S}}$.

PRZYKŁAD: Dla dowolnej G odwzorowanie $\mathrm{Id}_G : G \to G$ jest przykładem izomorfizmu, a odwzorowanie $f : G \to \{*\}$ homomorfizmu.

PRZYKŁAD: $\exp(\cdot) : (\mathbb{R}, +) \to (\mathbb{R}_{\neq 0}, \cdot)$ homomorfizm, $\exp(\cdot) : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ izomorfizm.

PRZYKŁAD: $\exp(2\pi i \cdot) : (\mathbb{R}, +) \to (\mathbb{C}_{\neq 0}, \cdot)$ homomorfizm.

PRZYKŁAD: $f : U(1) \to SO(\mathbb{R}^2)$ izomorfizm, tutaj $SO(\mathbb{R}^2)$ grupa obrotów płaszczyzny, f odwzorowuje liczbę $e^{i\phi}$ w obrót o kąt ϕ.

Równoważność działań: Działania $\nu_1 : G_1 \times X_1 \to X_1$ i $\nu_2 : G_2 \times X_2 \to X_2$ nazywają się równoważnymi, jeśli istnieje izomorfizm grup $f : G_1 \to G_2$ oraz bijekcja $h : X_1 \to X_2$ takie, że następujący diagram jest przemienny:

$$\begin{tikzcd} G_1 \times X_1 \arrow[r, "\nu_1"] \arrow[d, "f\times h"] & X_1 \arrow[d, "h"] \\ G_2 \times X_2 \arrow[r, "\nu_2"] & X_2 \end{tikzcd}$$

czyli $h(\nu_1(g,x)) = \nu_2(f(g), h(x)) \quad \forall\, g \in G_1, x \in X_1$.

Ważne pytania matematyczne:

1. Sklasyfikować grupy z dokładnością do izomorfizmu;
2. Sklasyfikować działania (w tym reprezentacje) z dokładnością do równoważności.

„Sklasyfikować" w ideale oznacza: 1) sporządzić listę „cegiełek", czyli „prostych"[1] obiektów (grup w przypadku 1., czy w przypadku 2. działań ustalonej grupy), których strukturę znamy; 2) określić procedurę budowania z „cegiełek" bardziej skomplikowanych obiektów; 3) podać kryteria, kiedy wybrany obiekt jest izomorficzny (równoważny) z jednym z obiektów zbudowanych z „cegiełek".

W rzeczywistości, takie listy „cegiełek" istnieją, ale istnieją też obiekty nie „poddające się klasyfikacji".

Naszym najbliższym celem będzie zdefiniowanie „cegiełek" w przypadku grup.

Jądro homomorfizmu $f : G_1 \to G_2$: $\ker f := f^{-1}(e_2)$.

Podgrupa normalna: Podgrupę $H \subset G$ nazywamy *normalną*, jeśli $gHg^{-1} \subset H$ dla wszystkich $g \in G$.

Związek pomiędzy grupami normalnymi a jądrami homomorfizmów:

TWIERDZENIE *Podzbiór $H \subset G$ grupy G jest podgrupą normalną wtedy i tylko wtedy gdy jest jądrem pewnego homomorfizmu $f : G \to G_2$.*

Dowód: ($\Longleftarrow$) Niech $f : G \to G_2$ będzie homomorfizmem, a $H := \ker f$. Wtedy

$$a, b \in H \Longrightarrow f(a) = e_2, f(b) = e_2 \Longrightarrow f(ab) = f(a)f(b) = e_2e_2 = e_2 \Longrightarrow ab \in H;$$

$$a \in H \Longrightarrow f(a^{-1}) = (f(a))^{-1} = e_2^{-1} = e_2 \Longrightarrow a^{-1} \in H;$$

$$f(gHg^{-1}) = f(g)f(H)f(g^{-1}) = f(g)e_2(f(g))^{-1} = e_2 \Longrightarrow gHg^{-1} \subset H.$$

Dowód implikacji ($\Longrightarrow$) pokrywa się z następującą konstrukcją.

Grupa ilorazowa G/H i homomorfizm naturalny $G \to G/H$: Niech G będzie grupą z działaniem $\mu : G \times G \to G$ a $H \subset G$ będzie dowolną podgrupą. Wtedy ograniczenie $\mu|_{G\times H}$ daje prawe działanie grupy H na zbiorze G. Orbita elementu $g \in G$ pod względem tego działania ma postać

[1] Słowo „prostych" piszemy w cudzysłowie, ponieważ „cegiełki" mogą mieć dosyć skomplikowaną strukturę. Na przykład tzw. grupa *Potwór* (ang. Monster), będąca grupą prostą w sensie definicji, którą poznamy za moment, liczy $2^{46}\cdot 3^{20}\cdot 5^9\cdot 7^6\cdot 11^2\cdot 13^3\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71 = 808017424794512875886459904961710757005754368000000000 \approx 8\cdot 10^{53}$ elementów, zob. http://en.wikipedia.org/wiki/Monster_group

$gH = \{gh \mid h \in H\}$ i nazywa się *prawą* warstwą g ze względu na H. Zbiór takich warstw oznaczamy G/H. Zbiór G jest sumą rozłączną warstw (jako że dowolny zbiór z działaniem grupy jest sumą rozłączną orbit). Ponadto, wszystkie warstwy mają jednakową moc, równą mocy H: odwzorowanie $H \ni h \mapsto gh \in gH$ jest bijekcją.

LEMAT *Niech $H \subset G$ będzie podgrupą normalną. Wtedy:*

1. *każda prawa warstwa gH pokrywa się z lewą warstwą $Hg := \{hg \mid h \in H\}$;*
2. *wzór $gH \cdot g'H = (g \cdot g')H$ zadaje poprawnie określone działanie $\bar{\mu} : G/H \times G/H \to G/H$ spełniające aksjomaty działania grupowego;*
3. *odwzorowanie $\pi : G \to G/H$, $\pi(g) := gH$ jest homomorfizmem grup.*

Dowód: 1. $gHg^{-1} \subset H \iff gHg^{-1} = H \iff gH = Hg$
2. Poprawność: niech $g_1 \in gH, g_1' \in g'H$, wtedy istnieją $h \in H, h' \in H'$ takie, że $g_1 = gh, g_1' = g'h'$. Mamy $g_1H \cdot g_1'H = (g_1 \cdot g_1')H = ghg'h'H = ghg'H = ghHg' = gHg' = gg'H$.
Łączność: $(gH \cdot g'H) \cdot g''H = (gg')H \cdot g''H = (gg')g''H = g(g'g'')H = gH \cdot (g'g'')H = gH \cdot (g'H \cdot g''H)$.
Element neutralny: $eHgH = egH = gH = geH = gHeH$.
Element odwrotny: $g^{-1}HgH = g^{-1}gH = eH = gg^{-1}H = gHg^{-1}H$.
3. $\pi(gg') = gg'H = gHg'H = \pi(g)\pi(g'), \pi(e) = eH$. $\square$

Uwaga I: Homomorfizm π jest epimorfizmem (czyli jest surjektywny). *Uwaga II:* Żeby jakiś epimorfizm $f : G_1 \to G_2$ był izomofrizmem, wystarczy i dosyć, żeby jego jądro było trywialne (tj. $\ker f = \{e_1\}$) (*Ćwiczenie*).

Obraz homomorfizmu:

LEMAT *Obraz $H_2 := \operatorname{im} f$ homomorfizmu $f : G_1 \to G_2$ jest pogrupą w G_2 izomorficzną z G_1/H_1, gdzie $H_1 := \ker f$.*

Dowód: Jeśli $a, b \in H_2$, to istnieją $a_1, b_1 \in G_1$ takie, że $f(a_1) = a, f(b_1) = b$. Wtedy $f(a_1b_1) = f(a_1)f(b_1) = ab$, czyli $H_2 \cdot H_2 \subset H_2$. Z kolei, $f(a_1^{-1}) = (f(a_1))^{-1} = a^{-1}$ implikuje $(H_2)^{-1} = H_2$.

Szukany izomorfizm określimy wzorem $G_1/H_1 \ni gH_1 \overset{\bar{f}}{\mapsto} f(g) \in H_2$. Odwzorowanie $\bar{f}$ jest określone poprawnie: jeśli $g' \in gH$ inny przedstawiciel warstwy, to $g'g^{-1} = h$ dla pewnego $h \in H$, i $f(g')(f(g))^{-1} = f(h) = e_2$ skąd $f(g') = f(g)$. Podobnie sprawdzamy, że jest homomorfizmem oraz że ma trywialne jądro. $\square$

PRZYKŁAD: Każda podgrupa H grupy abelowej G jest normalna. W szczególności, jeśli weźmiemy $G = \mathbb{Z}, H = n\mathbb{Z}$, otrzymujemy grupę *cykliczną* $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

PRZYKŁAD: Obrazem homomorfizmu $\exp(2\pi i \cdot) : (\mathbb{R}, +) \to (\mathbb{C}_{\neq 0}, \cdot)$ jest podgrupa $U(1) \subset (\mathbb{C}_{\neq 0}, \cdot)$, a jego jądrem podgrupa $(\mathbb{Z}, +)$. Mamy więc izomorfizm $\mathbb{R}/\mathbb{Z} \cong U(1)$.

PRZYKŁAD: Niech $\operatorname{sign} : S_n \to (\mathbb{R}_{\neq 0}, \cdot)$ homomorfizm odwzorowujący permutację τ w ± 1 w zależności od znaku τ. Jądrem jest tutaj grupa *alternująca* A_n permutacji parzystych, a obrazem grupa 2-elmentowa $\{\pm 1\}$ izomorficzna z $\mathbb{Z}_2$. Mamy izomorfizm $S_n/A_n \cong \mathbb{Z}_2$.

PRZYKŁAD: Niech G będzie dowolną grupą. Określmy odwzorowanie $\phi : G \to \operatorname{Aut}(G)$ wzorem $g \mapsto A_g, A_g(h) := ghg^{-1}$ (poprawność: $A_g(hh') = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = A_g(h)A_g(h'), A_g(e) =$

$e, A_g^{-1} = A_{g^{-1}}$). Ponadto, samo ϕ jest homomorfizmem: $A_{gg'} = A_g \circ A_{g'}, A_e = \mathrm{Id}_G$. Jego obraz $\mathrm{Int}(G) \subset \mathrm{Aut}(G)$ nazywamy grupą *automorfizmów wewnętrznych*.

Okazuje się, że $\mathrm{Int}(G)$ podgrupa normalna w $\mathrm{Aut}(G)$: jeśli $f : G \to G$ dowolny automorfizm, to $f \circ A_g \circ f^{-1}(h) = f(g[f^{-1}(h)]g^{-1}) = f(g)f[f^{-1}(h)]f(g^{-1}) = A_{f(g)}(h)$, czyli $f \circ \mathrm{Int}(G) \circ f^{-1} \subset \mathrm{Int}(G)$.

Grupę ilorazową $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Int}(G)$ nazywamy grupą *automorfizmów zewnętrznych* grupy G.

Grupy proste: Są to grupy G nie posiadające nietrywialnych (czyli rożniących się od G i $\{e\}$) podgrup normalnych.

Uwaga: W przypadku grup topologicznych lub Liego w definicji grup prostych dopuszczamy istnienie nietrywialnych normalnych podgrup *dyskretnych*[2]. Np. prosta grupa Liego $SL(\mathbb{R}^2)$ ma nietrywialną dyskretną podgrupę normalną $\{\pm I\}$.

To właśnie grupy proste są cegiełkami, „dającymi się sklasyfikować”.

[2]Dyskretność podgrupy $H \subset G$ oznacza dyskretność H jako przestrzeni topologicznej, czyli istnienie dla każdego punktu $h \in H$ otoczenia nie przecinającego się z otoczeniami innych punktów z H.