Symetrie – XII Szkoła Matematyki Poglądowej, Miętne, 28.01.–01.02.1994

Automorfizmy grup

Kazimierz SZYMICZEK, Katowice

1. Grupa automorfizmów

Co to jest automorfizm? Przede wszystkim należy ustalić obiekt, na którym ma działać automorfizm. Obiektem tym może być zbiór, grupa, ciało, przestrzeń liniowa, przestrzeń euklidesowa, przestrzeń topologiczna, lub ogólnie, obiekt dowolnej *kategorii*. W kategorii, do której należy nasz obiekt, jest określone pojęcie *izomorfizmu* obiektów. A więc będą to wzajemnie jednoznaczne odwzorowania zbiorów (w kategorii zbiorów), izomorfizmy grup, ciał i przestrzeni liniowych (w kategoriach grup, ciał i przestrzeni liniowych, odpowiednio), izometrie (w kategorii rzeczywistych przestrzeni liniowych z iloczynem skalarnym), czy też homeomorfizmy w kategorii przestrzeni topologicznych.

Każdy izomorfizm

$$\sigma : X \to X$$

obiektu X na siebie nazywamy *automorfizmem* obiektu X. Łatwo sprawdza się, że zbiór $\mathrm{Aut}X$ wszystkich automorfizmów obiektu X tworzy grupę ze względu na składanie automorfizmów (składanie morfizmów w kategorii, do której należy obiekt X).

Automorfizmy obiektu X można traktować jako swoiste *symetrie* obiektu X, a grupę automorfizmów $\mathrm{Aut}X$ można traktować jako miarę symetryczności obiektu X. Jeśli grupa $\mathrm{Aut}X$ jest trywialna, to znaczy jej jedynym elementem jest automorfizm tożsamościowy id_X, to obiekt X jest bardzo niesymetryczny.

Rozpatrzymy teraz kilka standardowych przykładów grup automorfizmów.

Przykład 1.1. Niech X będzie zbiorem. Wtedy grupa $\mathrm{Aut}X$ automorfizmów zbioru X jest grupą wszystkich bijekcji zbioru X na siebie. Nazywa się ją zwykle *grupą symetryczną* zbioru X i oznacza $S(X)$. Zbiory są więc krańcowo symetryczne: każda bijekcja jest automorfizmem.

Przykład 1.2. Niech X będzie ciałem. W grupie automorfizmów $\mathrm{Aut}X$ ciała X rozpatruje się zwykle podgrupę złożoną z wszystkich automorfizmów, które pozostawiają na miejscu każdy element pewnego wybranego podciała K ciała X. Tę podgrupę oznacza się $\mathrm{Gal}\ X/K$ i nazywa się ją grupą Galois rozszerzenia X ciała K. Teoria Galois pokazuje, jak kapitalne znaczenie dla struktury obiektu X może mieć struktura grupy automorfizmów obiektu X. Na przykład, krata podciał ciała X zawierających ciało K jest całkowicie zdeterminowana przez kratę podgrup grupy $\mathrm{Gal}\ X/K$.

Przykład 1.3. Niech X będzie n-wymiarową przestrzenią euklidesową *liniową*. Automorfizmami przestrzeni euklidesowej X są automorfizmy przestrzeni liniowej X, które zachowują iloczyn skalarny. Nazywamy je izometriami przestrzeni euklidesowej, a grupę $\mathrm{Aut}X$ nazywa się grupą izometrii przestrzeni euklidesowej liniowej X lub grupą ortogonalną i oznacza się ją $O(X)$ lub $O(n)$. Przestrzeń euklidesowa jest bardzo symetryczna: dla każdych dwóch wektorów x i y o tej samej długości, istnieje automorfizm przestrzeni euklidesowej przeprowadzający wektor x na wektor y. W grupie $O(n)$ wyróżnia się podgrupę *obrotów* składającą się z tych automorfizmów przestrzeni euklidesowej, które mają wyznacznik równy 1. Oznacza się ją $SO(n)$. Klasycznym rezultatem jest wyznaczenie wszystkich podgrup skończonych grupy obrotów $SO(3)$. Okazuje się, że są to jedynie grupy cykliczne, czyli grupy obrotów n-kątów foremnych w ich płaszczyznach, grupy diedralne, czyli grupy obrotów n-kątów foremnych w przestrzeni, i trzy grupy symetrii pięciu brył platońskich (te ostatnie mają rzędy 12, 24 i 60 i są izomorficzne z grupami permutacji A_4 [czworościan], S_4 [sześcian i ośmiościan] i A_5 [dwunastościan i dwudziestościan], zob. Armstrong, str. 105, lub Kostrykin, str. 270).

Możemy także rozpatrywać n-wymiarową przestrzeń euklidesową *afiniczną*, którą zwykle oznacza się E^n. Grupa $\mathrm{Aut}E^n$ jest grupą wszystkich izometrii przestrzeni E^n. Jej strukturę można opisać jako iloczyn półprosty podgrupy translacji i podgrupy obrotów (zob. §5).

Przykład 1.4. Niech X będzie grupą. A więc $X = (G, \cdot, 1)$, gdzie G jest zbiorem, $\cdot$ jest działaniem grupowym oraz 1 jest elementem neutralnym, czyli jedynką grupy X. Jak zwykle grupę X oznaczamy i nazywamy nazwą zbioru G. W dalszym ciągu zajmować się będziemy wyłącznie automorfizmami grup, czyli wzajemnie jednoznacznymi odwzorowaniami (bijekcjami) σ zbioru G, które zachowują działanie w grupie:

$$\sigma(ab) = \sigma(a) \cdot \sigma(b)$$

dla każdych $a, b \in G$. Automorfizm σ zachowuje wszelkie relacje pomiędzy elementami grupy G. Jeśli, na przykład, dla $a_1, \ldots, a_k \in G$ mamy

$$a_1^{n_1} \cdots a_k^{n_k} = 1$$

dla pewnych liczb całkowitych $n_1, \ldots, n_k$, to mamy także

$$\sigma(a_1)^{n_1} \cdots \sigma(a_n)^{n_k} = 1.$$

Ponieważ $\sigma(1) = 1$ dla każdego automorfizmu σ grupy G, więc grupy jedno- i dwu-elementowe mają tylko jeden automorfizm, mianowicie identycznościowy id_G. Okazuje się, że są to jedyne grupy, które są całkowicie niesymetryczne (zob. twierdzenie 2.1).

2. Przykłady automorfizmów grup

Wskażemy teraz trzy najprostsze przykłady nietrywialnych automorfizmów grup. Umawiamy się najpierw, że w grupach abelowych stosować będziemy terminologię addytywną, a więc działanie grupowe nazywamy dodawaniem i oznaczamy $+$, a element neutralny 0. Jest rzeczą celową podzielić grupy abelowe na dwie klasy. Pierwsza składa się z tak zwanych elementarnych 2−grup, a więc grup G o własności $2x = 0$ dla każdego $x \in G$. Taką grupę można w sposób naturalny traktować jako przestrzeń liniową nad ciałem 2−elementowym $\mathbf{F}_2$. Druga klasa składa się z grup abelowych, w których $2x \neq 0$ przynajmniej dla jednego elementu $x \in G$. Wtedy także $x \neq -x$.

Przykład 2.1. Niech G będzie elementarną 2−grupą, której rząd jest przynajmniej 4. Wtedy G jest co najmniej 2−wymiarową przestrzenią liniową nad ciałem $\mathbf{F}_2$, i możemy wziąć automorfizm tej przestrzeni liniowej, który w dowolnie wybranej bazie tej przestrzeni liniowej permutuje dwa wektory bazowe, pozostawiając pozostałe wektory bazowe na miejscu. W ten sposób otrzymujemy nietożsamościowy automorfizm σ, który ma w grupie $\mathrm{Aut}G$ rząd dwa: $\sigma^2 = \mathrm{id}_G$.

Przykład 2.2. Jeśli G jest grupą abelową, ale nie jest elementarną 2−grupą, to operacja brania elementu przeciwnego:

$$x \mapsto -x$$

jest nietrywialnym automorfizmem grupy G. Także ten automorfizm ma w grupie $\mathrm{Aut}G$ rząd 2.

Przykład 2.3. Niech teraz G będzie grupą nieabelową. Oznacza to, że *centrum* $Z(G)$ grupy G, czyli podgrupa określona następująco

$$Z(G) := \{a \in G : ax = xa \ \ \forall x \in G\},$$

nie pokrywa się z całą grupą G. Obieramy więc element $a \in G$, który nie należy do centrum grupy G i rozpatrujemy odwzorowanie

$$i_a : G \to G, \quad i_a(g) = aga^{-1}.$$

Łatwo sprawdza się, że i_a jest nietrywialnym automorfizmem grupy G. Automorfizm i_a nazywamy automorfizmem *wewnętrznym* grupy G.

Sumując rezultaty naszych trzech przykładów otrzymujemy więc następujące twierdzenie.

Twierdzenie 2.1. *Każda grupa G rzędu większego niż dwa ma nietrywialny automorfizm.*

A więc grupy są dość symetryczne! Tylko grupa 2-elementowa jest nietrywialna i niesymetryczna.

3. Grupa automorfizmów grupy

Dla dowolnej grupy G jej grupa automorfizmów $\mathrm{Aut}G$ może być traktowana jako pewna podgrupa grupy symetrycznej zbioru $G^* := G \setminus \{1\}$, gdyż każdy automorfizm pozostawia na miejscu jedynkę 1 grupy G. Dokładniej, przyporządkowanie

$$\mathrm{Aut}G \to S(G^*), \quad \sigma \mapsto \sigma|_{G^*} \tag{1}$$

jest monomorfizmem grup, więc jego obraz jest podgrupą grupy symetrycznej $S(G^*)$ izomorficzną z grupą $\mathrm{Aut}G$. Wynika stąd w szczególności, że dla grupy skończonej G mamy następujący związek pomiędzy rzędem grupy G i rzędem grupy $\mathrm{Aut}G$:

(2) Jeśli $|G| = n$, to $|\mathrm{Aut}G|$ jest dzielnikiem $(n-1)!$.

Grupa G jest niewątpliwie maksymalnie symetryczna, gdy monomorfizm (1) jest *epimorfizmem*, to znaczy, gdy jest on izomorfizmem grup: $\mathrm{Aut}G \cong S(G^*)$. Przykładem grupy, która ma tę własność jest grupa czwórkowa Kleina $V_4 = \mathbf{Z}_2 \times \mathbf{Z}_2$, która jest elementarną 2–grupą. Łatwo sprawdzić, że każda permutacja jej niezerowych elementów wyznacza automorfizm tej grupy, a więc mamy izomorfizm

$$\mathrm{Aut}V_4 \cong S_3 \cong S(V_4^*).$$

Twierdzenie 3.1. *Grupa czwórkowa Kleina $G = V_4$ jest jedyną grupą G rzędu co najmniej 4, której grupa automorfizmów $\mathrm{Aut}G$ składa się z wszystkich bijekcji zbioru G pozostawiających jedynkę grupy G na miejscu.*

Dowód. Jeśli $|G| > 4$ oraz a, b, ab, c są czterema różnymi elementami zbioru G^*, to istnieje bijekcja zbioru G^* na siebie taka, że

$$a \mapsto a, \quad b \mapsto b, \quad ab \mapsto c,$$

Taka bijekcja zbioru G^* na siebie nie może być zacieśnieniem do G^* żadnego automorfizmu grupy G. Jeśli natomiast $|G| = 4$ i grupa G nie jest grupą czwórkową Kleina, to jest grupą cykliczną $\mathbf{Z}_4$ i ma 2–elementową grupę automorfizmów. ■

A więc nierówność $|\mathrm{Aut}G| \leq (n-1)!$ dla grupy G rzędu n, wynikająca z (2) realizuje się jako równość tylko dla $n \leq 4$, przy czym dla $n = 4$ tylko dla $G = V_4$. Można udowodnić całkiem elementarnie następujące silniejsze ograniczenie dla rzędu grupy $\mathrm{Aut}G$.

Twierdzenie 3.2. *Niech G będzie grupą rzędu $n \geq 2$ i niech $k = [\log_2 n]$. Wtedy*

$$|\mathrm{Aut}G| \leq \prod_{i=0}^{k-1} (n - 2^i).$$

Dowód. Niech k będzie najmniejszą liczbą elementów grupy G tworzących układ generatorów grupy G. Każdy taki k–elementowy układ generatorów $\{g_1, \ldots, g_k\}$ grupy G ma następującą własność: dla każdego $i = 1, \ldots, k-1$, element g_{i+1} nie należy do podgrupy G_i generowanej przez elementy $g_1, \ldots, g_i$. Wynika stąd, że podgrupa G_i zawiera przynajmniej 2^i elementów, w szczególności więc

$$n = |G| = |G_k| \geq 2^k.$$

Jeśli σ jest dowolnym automorfizmem grupy G, to $\{\sigma(g_1), \ldots, \sigma(g_k)\}$ jest także zbiorem generatorów grupy G. Liczba automorfizmów grupy G nie przekracza więc liczby zbiorów generatorów mających po k elementów. Ile jest k–elementowych zbiorów generatorów w grupie G? Aby skonstruować taki zbiór, obieramy dowolny element g_1 grupy, różny od jedynki: daje to $n-1$ możliwości wyboru. Następny element g_2 w naszym zbiorze musi być różny

od 1 i od g_1, mamy więc $n-2$ możliwości wyboru. Kolejny element musi być różny od czterech elementów $1, g_1, g_2, g_1g_2$. Kontynuując to postępowanie otrzymamy co najwyżej $\prod_{i=0}^{k-1}(n-2^i)$ układów generatorów, skąd wynika już nasze twierdzenie. ■

Zauważmy jeszcze, że gdybyśmy szacowali liczbę k–elementowych układów generatorów grupy G znacznie mniej dokładnie, oceniając, że każdy generator g_i można wybrać na nie więcej niż n sposobów, to otrzymalibyśmy następujące oszacowanie dla rzędu grupy $\mathrm{Aut}G$:

$$|\mathrm{Aut}G| \leq n^k \leq n^{\log_2 n}.$$

Z drugiej strony rezultatu twierdzenia 3.2 nie można ulepszyć, gdyż dla elementarnych 2–grup abelowych, czyli dla grup

$$\mathbf{Z}_2^k = \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2,$$

rzędu $n = 2^k$, rząd grupy automorfizmów jest *równy* $\prod_{i=0}^{k-1}(n-2^i)$ (zob. *Zbiór...* **122**(a), **325**(b)).

Dla opisania struktury grupy jest rzeczą niezbędną poznanie jej podgrup. Gdy G jest grupą nieabelową, najważniejszą podgrupą grupy $\mathrm{Aut}G$ jest z pewnością grupa automorfizmów wewnętrznych $\mathrm{Inn}G$. Jest to istotnie podgrupa, gdyż dla dowolnych automorfizmów wewnętrznych i_a oraz i_b mamy

$$i_a \circ i_b = i_{ab}, \quad i_a^{-1} = i_{a^{-1}}.$$

Jest rzeczą naturalną rozważyć odwzorowanie

$$f : G \to \mathrm{Inn}G, \quad f(a) = i_a$$

i zauważyć, że jest ono homomorfizmem grup. Ponadto, jądro tego homomorfizmu składa się z elementów $a \in G$, takich, że $i_a = \mathrm{id}_G$, to znaczy $axa^{-1} = x$ dla każdego $x \in G$. Zatem jądrem homomorfizmu f jest centrum $Z(G)$ grupy G i otrzymujemy następujący opis grupy $\mathrm{Inn}G$:

$$\mathrm{Inn}G \cong G/Z(G). \tag{3}$$

Warto też zauważyć, że $\mathrm{Inn}G$ jest podgrupą *normalną* w grupie $\mathrm{Aut}G$, gdyż

$$\sigma \circ i_a \circ \sigma^{-1} = i_{\sigma(a)} \tag{4}$$

jak wynika z następującego rachunku:

$$\begin{aligned}(\sigma \circ i_a \circ \sigma^{-1})(g) &= \sigma(a\sigma^{-1}(g)a^{-1}) = \sigma(a)g\sigma(a^{-1}) \\ &= \sigma(a)g\sigma(a)^{-1} = i_{\sigma(a)}(g),\end{aligned}$$

dla dowolnych $\sigma \in \mathrm{Aut}G$, $a, g \in G$.

Można zatem rozpatrywać grupę ilorazową

$$\mathrm{Out}G := \mathrm{Aut}G/\mathrm{Inn}G,$$

którą nazywa się grupą *automorfizmów zewnętrznych* grupy G, chociaż jej elementy nie są automorfizmami (lecz zbiorami automorfizmów) grupy G. Każdy automorfizm grupy G, który nie jest automorfizmem wewnętrznym (jeśli taki istnieje) nazywa się automorfizmem *zewnętrznym* grupy G. Grupa abelowa G ma wyłącznie automorfizmy zewnętrzne, natomiast istnieją grupy nieabelowe, które w ogóle nie mają automorfizmów zewnętrznych (zob. §6).

Wyznaczenie grupy automorfizmów danej grupy jest na ogół dość trudne. Jeśli grupa ta ma strukturę iloczynu prostego grup, to przydatna jest znajomość grup automorfizmów czynników tego iloczynu. Mamy bowiem dla dowolnych grup G, H monomorfizm grup

$$\mathrm{Aut}G \times \mathrm{Aut}H \to \mathrm{Aut}(G \times H),$$

który parze automorfizmów (σ, ρ) przyporządkowuje automorfizm $\sigma \times \rho$, określony następująco:

$$(\sigma \times \rho)(g, h) = (\sigma(g), \rho(h)).$$

Jeśli grupy G i H są skończone i ich rzędy są względnie pierwsze to ten monomorfizm jest izomorfizmem grup (zob. *Zbiór...* **335**). A więc w tym przypadku struktura grupy $\mathrm{Aut}(G \times H)$ jest całkowicie określona przez strukturę grup $\mathrm{Aut}G$ i $\mathrm{Aut}H$.

Metoda ta może być użyta do opisu grup automorfizmów skończonych grup abelowych, gdyż jak wiadomo, każda skończona grupa abelowa G rzędu $n = p_1^{n_1} \cdots p_k^{n_k}$, gdzie $p_1, \ldots, p_k$ są różnymi liczbami pierwszymi, jest sumą prostą abelowych p-grup:

$$G = G_{p_1} \oplus \cdots \oplus G_{p_k},$$

których rzędy są odpowiednio równe $p_1^{n_1}, \ldots, p_k^{n_k}$. Składniki proste tego rozkładu mają więc rzędy parami względnie pierwsze, skąd wynika, że

$$\mathrm{Aut}G \cong \mathrm{Aut}G_{p_1} \oplus \cdots \oplus \mathrm{Aut}G_{p_k}.$$

W ten sposób problem został zredukowany do opisu grup automorfizmów p-grup abelowych. Jak wiadomo, każda skończona p-grupa abelowa jest sumą prostą cyklicznych p-grup, ale tu już struktura produktowa nie przenosi się na grupę automorfizmów. Natomiast dla wyznaczenia grupy automorfizmów można tutaj próbować posłużyć się metodą, którą zastosowaliśmy do dowodu twierdzenia 3.2.

Podamy teraz listę grup automorfizmów wszystkich grup rzędu nie większego niż 15. Lista ta została sporządzona na podstawie *Zbioru zadań z teorii grup* (rozdział 3), gdzie można znaleźć dalsze informacje o automorfizmach grup oraz o grupach występujących w tej klasyfikacji.

Stosujemy tu następujące standardowe oznaczenia:

$\mathbf{Z}_n$ grupa cykliczna rzędu n,
S_n grupa symetryczna zbioru n-elementowego,
A_n grupa alternująca permutacji parzystych zbioru n-elementowego,
D_n grupa izometrii n-kąta foremnego (grupa diedralna),
Q_{2n} uogólniona grupa kwaternionów rzędu $4n$,
$\mathrm{GL}(n, \mathbf{Z}_p)$ grupa macierzy odwracalnych nad ciałem $\mathbf{Z}_p$,
$\mathrm{Af}(n, \mathbf{Z}_m)$ grupa afiniczna stopnia n nad pierścieniem $\mathbf{Z}_m$.

G	$\lvert G\rvert$	$\mathrm{Aut}G$	$\lvert\mathrm{Aut}G\rvert$
$\mathbf{Z}_2$	2	1	1
$\mathbf{Z}_3$	3	$\mathbf{Z}_2$	2
$\mathbf{Z}_4$	4	$\mathbf{Z}_2$	2
$\mathbf{Z}_2 \times \mathbf{Z}_2$	4	S_3	6
$\mathbf{Z}_5$	5	$\mathbf{Z}_4$	4
$\mathbf{Z}_6$	6	$\mathbf{Z}_2$	2
S_3	6	S_3	6
$\mathbf{Z}_7$	7	$\mathbf{Z}_6$	6
$\mathbf{Z}_8$	8	$\mathbf{Z}_2 \times \mathbf{Z}_2$	4
$\mathbf{Z}_4 \times \mathbf{Z}_2$	8	D_4	8
$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$	8	$\mathrm{GL}(3, \mathbf{Z}_2)$	168
D_4	8	D_4	8
Q_4	8	S_4	24
$\mathbf{Z}_9$	9	$\mathbf{Z}_6$	6
$\mathbf{Z}_3 \times \mathbf{Z}_3$	9	$\mathrm{GL}(2, \mathbf{Z}_3)$	48
$\mathbf{Z}_{10}$	10	$\mathbf{Z}_4$	4
D_5	10	$\mathrm{Af}(1, \mathbf{Z}_5)$	20
$\mathbf{Z}_{11}$	11	$\mathbf{Z}_{10}$	10
$\mathbf{Z}_{12}$	12	$\mathbf{Z}_2 \times \mathbf{Z}_2$	4
$\mathbf{Z}_6 \times \mathbf{Z}_2$	12	$\mathbf{Z}_2 \times S_3$	12
D_6	12	D_6	12
Q_6	12	$\mathrm{Af}(1, \mathbf{Z}_6)$	12
A_4	12	S_4	24
$\mathbf{Z}_{13}$	13	$\mathbf{Z}_{12}$	12
$\mathbf{Z}_{14}$	14	$\mathbf{Z}_6$	6
D_7	14	$\mathrm{Af}(1, \mathbf{Z}_7)$	42
$\mathbf{Z}_{15}$	15	$\mathbf{Z}_4 \times \mathbf{Z}_2$	8

4. Porównanie własności grup G i Aut$G$

Przede wszystkim można zapytać jakie własności grupy G przenoszą się na jej grupę automorfizmów Aut$G$. Jedną z niewielu rzeczy, które się zachowują, jest brak centrum:

Twierdzenie 4.1. $Z(G) = 1 \Rightarrow Z(\mathrm{Aut}G) = 1$.

Dowód. Jeśli $Z(G) = 1$, to $Z(\mathrm{Inn}G) = Z(G/Z(G)) = Z(G) = 1$. Stąd wynika, że także $Z(\mathrm{Aut}G) = 1$. Jeśli bowiem σ jest dowolnym automorfizmem grupy G i σ jest przemienny z każdym automorfizmem wewnętrznym i_a grupy G, to mamy

$$i_a = \sigma \circ i_a \circ \sigma^{-1} \quad \forall a \in G.$$

A więc na podstawie (4) mamy $i_a = i_{\sigma(a)}$ dla każdego $a \in G$. Stąd wobec różnowartościowości homomorfizmu $f : G \to \mathrm{Inn}G$, $f(a) = i_a$ wynika, że $\sigma(a) = a$ dla każdego $a \in G$. A więc $\sigma = \mathrm{id}_G$ oraz $Z(\mathrm{Aut}G) = 1$. ■

Inną własnością, która zachowuje się w pewnym stopniu przy przejściu od grupy G do grupy Aut$G$ jest podzielność rzędu grupy przez liczby pierwsze. Wprawdzie nie zawsze jest prawdą, że jeśli liczba pierwsza p dzieli rząd grupy G, to dzieli także rząd grupy Aut$G$, ale okazuje się, że jeśli rząd grupy dzieli się przez dostatecznie wysoką potęgę liczby pierwszej p, to nie pozostaje to bez wpływu na rząd grupy Aut$G$.

Twierdzenie 4.2. *Niech G będzie grupą skończoną i niech p będzie liczbą pierwszą. Jeśli p^2 dzieli rząd grupy G, to p dzieli rząd grupy* Aut$G$.

Dowód. Najpierw rozważymy przypadek, gdy grupa G jest abelowa. Jeśli $p^2 \mid |G|$, to grupa G ma p-prymarny składnik prosty G_p rzędu p^α, gdzie $\alpha \geq 2$. Są tu dwa istotnie różne przypadki. Pierwszy, gdy G_p jest elementarną p-grupą, to znaczy, gdy rzędy wszystkich niezerowych elementów w G_p są równe p. Wtedy G_p jest przestrzenią liniową nad ciałem prostym $\mathbf{F}_p$ i jej grupa automorfizmów jest izomorficzna z grupą macierzy odwracalnych $\mathrm{GL}(\alpha, \mathbf{F}_p)$ (zob. *Zbiór...* **325**(b)), której rząd jest równy

$$(p^\alpha - 1)(p^\alpha - p) \cdots (p^\alpha - p^{\alpha-1})$$

(zob. *Zbiór...* **122**(a)). Liczba ta jest podzielna przez p, jeśli tylko $\alpha \geq 2$. Drugi przypadek mamy gdy grupa G_p nie jest elementarną p-grupą. Wtedy rozkładamy grupę G_p na sumę prostą p-grup cyklicznych i wśród nich musi być składnik prosty izomorficzny z $\mathbf{Z}_{p^\ell}$, gdzie $\ell \geq 2$. Mamy wtedy

$$\mathrm{Aut}\mathbf{Z}_{p^\ell} \cong \mathbf{Z}_{p^\ell}^*,$$

gdzie $\mathbf{Z}_{p^\ell}^*$ jest grupą elementów odwracalnych pierścienia $\mathbf{Z}_{p^\ell}$ (zob. *Zbiór...* **322**(b)). Jednakże wiadomo, że rząd grupy $\mathbf{Z}_{p^\ell}^*$ jest równy $p^{\ell-1}(p-1)$ (zob. *Zbiór...* **870**(c)), jest zatem podzielny przez p.

A więc w każdym przypadku grupa abelowa G ma składnik prosty, którego grupa automorfizmów ma rząd podzielny przez p. Ponieważ jednak grupa automorfizmów składnika prostego grupy G zanurza się różnowartościowo w grupę automorfizmów grupy G (zob. §3), więc wynika stąd, że $|\mathrm{Aut}G|$ dzieli się przez p.

Załóżmy teraz, że grupa G jest nieabelowa. Tutaj także są dwa istotnie różne przypadki, w zależności od tego, czy liczba pierwsza p dzieli rząd grupy ilorazowej $G/Z(G)$, czy też nie. Jeśli $p \mid |G/Z(G)|$, to na podstawie (3) liczba p dzieli rząd grupy Inn$G$ i wobec tego także rząd grupy Aut$G$.

$p^\alpha \parallel n$ oznacza, że p^α dzieli n oraz $p^{\alpha+1}$ nie dzieli n.

Będziemy więc odtąd zakładać, że liczba pierwsza p nie dzieli rzędu grupy $G/Z(G)$. Oznacza to, że jeśli $p^\alpha \parallel |G|$, to także $p^\alpha \parallel |Z(G)|$. Niech S będzie p-podgrupą Sylowa grupy $Z(G)$. A więc $|S| = p^\alpha$ i wobec tego S jest także p-podgrupą Sylowa grupy G. Ponieważ każde dwie p-podgrupy Sylowa grupy G są sprzężone, są więc one wszystkie *równe* S. Na podstawie pierwszej części dowodu wiemy już, że rząd grupy Aut$S$ dzieli się przez p. Wystarczy więc udowodnić, że

(5) Grupa S jest składnikiem prostym grupy G.

Najpierw uzasadnimy następujące kryterium przynależności elementu g grupy G do grupy S :

$$g \in S \quad \Leftrightarrow \quad g^{p^\alpha} = 1 \tag{6}$$

Ponieważ p^α jest rzędem grupy S, każdy element grupy S ma rząd będący dzielnikiem liczby p^α, a więc $g^{p^\alpha} = 1$. Na odwrót, jeśli $g \in G$ oraz $g^{p^\alpha} = 1$, to podgrupa cykliczna $\langle g \rangle$ jest p-grupą, zawiera się więc w pewnej p-podgrupie Sylowa grupy G. Jak już stwierdziliśmy wyżej, grupa S jest jedyną p-podgrupą Sylowa grupy G, zatem $\langle g \rangle \subseteq S$, skąd wynika, że $g \in S$. Dowodzi to (6).

Możemy teraz przejść do dowodu (5). Załóżmy, że $|G| = p^\alpha \cdot m$. Wtedy m jest niepodzielną przez p liczbą naturalną i wobec tego istnieją takie liczby całkowite a, b, że $p^\alpha a + mb = 1$. A więc dla dowolnego elementu $g \in G$ mamy

$$g = g^{p^\alpha a} \cdot g^{mb}.$$

Tutaj drugi czynnik należy na podstawie (6) do grupy S, gdyż

$$(g^{mb})^{p^\alpha} = 1,$$

natomiast pierwszy czynnik należy do podzbioru R grupy G złożonego z wszystkich potęg elementów grupy G o wykładniku $p^\alpha a$. Udowodnimy, że zbiór R jest podgrupą grupy G. Niech $g, h \in G$. Wtedy obok powyższego rozkładu elementu g mamy także

$$h = h^{p^\alpha a} \cdot h^{mb},$$

$$gh = (gh)^{p^\alpha a} \cdot (gh)^{mb}.$$

Z drugiej strony, uwzględniając, że S jest podgrupą centrum grupy G mamy

$$gh = g^{p^\alpha a} \cdot g^{mb} \cdot h^{p^\alpha a} \cdot h^{mb} = g^{p^\alpha a} \cdot h^{p^\alpha a} \cdot (gh)^{mb}.$$

Porównując te dwa wyrażenia dla iloczynu gh widzimy, że zbiór R jest zamknięty ze względu na mnożenie i, jako podzbiór grupy skończonej, jest podgrupą grupy G. Zauważmy jeszcze, że

$$R \cap S = 1,$$

gdyż każdy element $g^{p^\alpha a} \in R$ ma rząd będący dzielnikiem liczby m, podczas gdy S jest p-grupą oraz p nie dzieli m. Ponadto, $rs = sr$ dla każdych $r \in R$ oraz $s \in S$, gdyż S jest podgrupą centrum grupy G. Sumując stwierdzamy, że

$$G = R \oplus S,$$

co dowodzi (5), i kończy dowód twierdzenia. ■

Warto zauważyć, że udowodnione przez nas twierdzenie jest szczególnym przypadkiem ogólniejszego rezultatu Ledermana i Neumanna, którzy wykazali, że dla każdej liczby pierwszej p istnieje funkcja

$$f_p : \mathbf{N} \to \mathbf{N}$$

taka, że dla każdej grupy skończonej G i dla każdej liczby naturalnej n,

Jeśli $p^{f_p(n)} \mid |G|$, to $p^n \mid |\mathrm{Aut}G|$.

Green wykazał, że

$$f_p(n) \leq \frac{1}{2}n(n+3) + 1.$$

Gdybyśmy chcieli z tych rezultatów uzyskać pewność, że $p \mid |\mathrm{Aut}G|$, to musielibyśmy zakładać, że rząd grupy G dzieli się przez p^3, gdyż według Greena, $f_p(1) \leq 3$.

Własności grupy G nie przenoszą się jednak na ogół na grupę $\mathrm{Aut}G$. A oto typowe przykłady braku wspólnych własności grup G i $\mathrm{Aut}G$.

Grupa automorfizmów grupy abelowej może być nieabelowa, np. $\mathrm{Aut}V_4 = S_3$.

Grupa automorfizmów grupy nieabelowej może być abelowa, chociaż tutaj znacznie trudniej wskazać jakiś prosty przykład.

Łatwo natomiast stwierdzić, że dla grupy nieabelowej G, grupa $\mathrm{Aut}G$ nie może być grupą cykliczną. Gdyby bowiem grupa $\mathrm{Aut}G$ była cykliczna, to cykliczna byłaby także jej podgrupa $\mathrm{Inn}G$, podczas gdy $\mathrm{Inn}G$ jest izomorficzna z $G/Z(G)$, a o tej grupie udowodnimy, że nie jest cykliczna.

Twierdzenie 4.3. *Jeśli grupa G jest nieabelowa, to grupa ilorazowa $G/Z(G)$ nie jest cykliczna.*

Dowód. Niech $G/Z(G) = \langle aZ(G)\rangle$ i niech $b, c \in G$. Wtedy $b = a^k z_1, c = b^l z_2$, gdzie $z_1, z_2 \in Z(G)$ oraz $k, l \in \mathbf{Z}$. Wtedy $bc = a^{k+l} z_1 z_2 = cb$. A więc cykliczność $G/Z(G)$ pociąga, że G jest abelowa, sprzeczność. ■

Jeśli grupa G jest nieskończona, to jej moc może być różna od mocy grupy $\mathrm{Aut}G$. Tak więc, na przykład, grupa automorfizmów grupy nieskończonej $\mathbf{Z}$ liczb całkowitych, jest grupą 2−elementową $\mathbf{Z}_2$.

Może się także zdarzyć, że grupa przeliczalna ma nieprzeliczalną grupę automorfizmów. Na przykład, multyplikatywna grupa liczb wymiernych dodatnich $\mathbf{Q}^+$ ma nieprzeliczalną grupę automorfizmów $\mathrm{Aut}\mathbf{Q}^+$, gdyż każda bijekcja zbioru liczb pierwszych na siebie wyznacza automorfizm grupy $\mathbf{Q}^+$.

Łatwo stwierdzić, że grupy izomorficzne mają izomorficzne grupy automorfizmów. W związku z tym można rozpatrywać przyporządkowanie, które każdą grupę (klasę grup izomorficznych) przeprowadza na jej grupę (klasę izomorficznych grup) automorfizmów:

$$G \mapsto \mathrm{Aut}G.$$

To odwzorowanie nie jest injektywne (różnowartościowe), gdyż grupy automorfizmów nieizomorficznych grup mogą być izomorficzne. Na przykład $\mathbf{Z}$ i $\mathbf{Z}_3$ mają tę samą (z dokładnością do izomorfizmu) grupę automorfizmów $\mathbf{Z}_2$. Okazuje się, że odwzorowanie to nie jest też surjektywne, gdyż nie każda grupa może być grupą automorfizmów grupy.

Twierdzenie 4.4. *Grupy cykliczne rzędów nieparzystych > 1, nie są grupami automorfizmów grup. Dokładniej, żadna grupa cykliczna nie jest grupą automorfizmów grupy nieabelowej, oraz, żadna grupa skończona rzędu nieparzystego > 1 nie jest grupą automorfizmów grupy abelowej.*

Dowód. Dla grupy nieabelowej G, grupa $\mathrm{Inn}G$ nie jest cykliczna, więc także grupa $\mathrm{Aut}G$ nie może być cykliczna. Natomiast, jeśli grupa G jest abelowa, to na podstawie przykładów 2.1 i 2.2 grupa G ma automorfizm rzędu 2. Jeśli zatem grupa $\mathrm{Aut}G$ jest skończona, to ma rząd parzysty. ■

Istnieją też *nieabelowe* grupy skończone, które nie są grupami automorfizmów wewnętrznych żadnej grupy (zob. *Zbiór...* **287**, **330**).

Widzimy więc, że grupy automorfizmów grup nie wyczerpują klasy wszystkich grup. W związku z tym powstaje wątpliwość, czy traktowanie grup jako miary symetrii różnych obiektów jest słuszne. Gdyby okazało się, że istnieją grupy, które nie są grupami automorfizmów żadnych obiektów, to powiedzenie, że "liczby mierzą wielkości, a grupy mierzą symetrie" nie byłoby całkiem uprawnione. Okazuje się jednak, że grupy bardzo dobrze pełnią swoją rolę miernika symetrii. Można bowiem udowodnić, że każda grupa jest grupą automorfizmów pewnej algebry uniwersalnej, a nawet pewnej kraty dystrybutywnej (G. Birkhoff, 1946) [zob. Plotkin, str. 117]. Ponadto:

Każda grupa jest grupą wszystkich automorfizmów pewnego pierścienia
(J. de Groot, 1958) [zob. Plotkin, str. 118].

Każda grupa jest grupą wszystkich automorfizmów pewnego grafu
(G. Sabidussi, 1957) [zob. Plotkin, str. 118].

5. Holomorf grupy

Niech A będzie podgrupą normalną grupy G. Wtedy

$$gAg^{-1} = A$$

dla każdego $g \in G$. Wynika stąd, że automorfizm wewnętrzny i_g grupy G, zacieśniony do podgrupy A, jest automorfizmem (ale już niekoniecznie wewnętrznym) grupy A. Nasuwa się pytanie, czy dla każdej grupy A istnieje

grupa G zawierająca A jako podgrupę normalną i taka, że *każdy* automorfizm grupy A jest zacieśnieniem do A pewnego automorfizmu *wewnętrznego* grupy G.

Aby odpowiedzieć na to pytanie, trzeba najpierw uzmysłowić sobie w jaki sposób ulokowana w grupie G może być jej podgrupa normalna A. Pierwszym pomysłem jest niewątpliwie rozważenie przypadku, gdy grupa A jest *czynnikiem prostym* grupy G. Oznacza to, że obok podgrupy normalnej A mamy drugą podgrupę normalną B w grupie G oraz

$$G = A \cdot B = \{a \cdot b : \ a \in A, \ b \in B\}, \quad A \cap B = 1.$$

Wtedy każdy element $a \in A$ jest przemienny z każdym elementem $b \in B$, gdyż

$$\begin{aligned} aba^{-1}b^{-1} &= a \cdot ba^{-1}b^{-1} \in A \\ &= aba^{-1} \cdot b^{-1} \in B. \end{aligned}$$

A więc komutator $aba^{-1}b^{-1} \in A \cap B = 1$, skąd wynika, że $ab = ba$, dla każdych $a \in A$, $b \in B$. Wobec tego jeśli $g = ab \in G$ jest dowolnym elementem grupy G, to dla każdego $x \in A$ mamy

$$i_g(x) = i_{ab}(x) = abxb^{-1}a^{-1} = axa^{-1},$$

gdyż $x \in A$ jest przemienny z elementem $b \in B$. Wynika stąd jednak, że i_g działa na podgrupie A dokładnie tak samo jak automorfizm wewnętrzny grupy A wyznaczony przez $a \in A$. Jeśli grupa A ma automorfizm zewnętrzny, to nie jest on zacieśnieniem do A automorfizmu wewnętrznego grupy G. Stwierdzamy więc, że gdy A jest czynnikiem prostym grupy G, to grupa G nie rozwiązuje naszego problemu.

Przeprowadzamy więc następny eksperyment polegający na osłabieniu warunków narzuconych na A i B w pierwszym, nieudanym eksperymencie. A więc zakładamy, że

$$G = AB, \quad A \lhd G, \quad B < G, \quad A \cap B = 1.$$

Zrezygnowaliśmy więc z założenia, że B jest podgrupą normalną. W tej sytuacji grupa G jest *iloczynem półprostym* podgrupy normalnej A i podgrupy B. Istnieją liczne przykłady grup, które rozkładają się na iloczyn półprosty, ale nie mają rozkładu na iloczyn prosty nietrywialnych podgrup normalnych. A więc, na przykład,

$$\begin{aligned} D_n &= \mathrm{Obr}(n) \cdot \mathrm{Odb}(n), \\ S_n &= A_n \cdot \{1, (12)\}, \\ O(n) &= SO(n) \cdot \{1, \tau\}, \\ \mathrm{Izom}E^n &= \mathrm{Tran}E^n \cdot \mathrm{Obr}E^n, \\ \mathrm{Af}(n, K) &= \mathrm{TAf}(n, K) \cdot \mathrm{CAf}(n, K). \end{aligned}$$

Tutaj użyliśmy następujących oznaczeń: $\mathrm{Obr}(n)$ oznacza n-elementową podgrupę obrotów i $\mathrm{Odb}(n)$ jakąkolwiek 2–elementową podgrupę zawierającą odbicie n-kąta foremnego, τ oznacza jakąkolwiek nietrywialną symetrię względem hiperpłaszczyzny w przestrzeni euklidesowej, Tran i Obr oznaczają odpowiednio podgrupę translacji i podgrupę obrotów w grupie izometrii przestrzeni euklidesowej afinicznej, TAf i CAf oznaczają podgrupę translacji i podgrupę środkowo-afiniczną w grupie przekształceń afinicznych n-wymiarowej przestrzeni liniowej nad ciałem K. W każdym rozkładzie pierwszy czynnik jest podgrupą normalną, natomiast drugi nie jest podgrupą normalną w rozpatrywanej grupie.

Powracamy teraz do iloczynu półprostego $G = AB$. Tutaj także każdy element g grupy G ma jednoznaczne przedstawienie w postaci iloczynu $g = ab$, gdzie $a \in A$, $b \in B$. Jeśli także $g_1 = a_1b_1$, gdzie $a_1 \in A$, $b_1 \in B$, to mamy

$$g \cdot g_1 = ab \cdot a_1b_1 = a \cdot ba_1b^{-1} \cdot bb_1.$$

Dla porównania, jeśli $G = AB$ jest iloczynem prostym, to elementy podgrup A i B są przemienne, i wobec tego

$$g \cdot g_1 = ab \cdot a_1b_1 = a \cdot ba_1 \cdot b_1 = aa_1 \cdot bb_1.$$

Tak więc zapisanie elementu $g \cdot g_1$ w 'prawidłowej' postaci, to znaczy jako iloczynu elementów z A i B jest łatwiejsze w przypadku iloczynu prostego, ale jest także całkiem przejrzyste w przypadku iloczynu półprostego.

Idąc dalej tym tropem uzyskamy pełne rozwiązanie tego problemu. Przede wszystkim zauważmy, że nasza wiedza o iloczynie półprostym grup daje się też sformułować następująco. Jeśli $G = AB$ jest iloczynem półprostym, to na iloczynie kartezjańskim $A \times B$ zbiorów A i B można określić działanie mnożenia następująco:

$$(a, b) \cdot (a_1, b_1) = (a \cdot ba_1b^{-1},\ bb_1).$$

Łatwe sprawdzenie pokazuje, że z tak określonym działaniem zbiór $A \times B$ staje się grupą izomorficzną z iloczynem półprostym $G = AB$. Co więcej, założenie, że $G = AB$ jest iloczynem półprostym jest wykorzystane tylko dla zapewnienia, że $i_b(a_1) \in A$, co gwarantuje, iż iloczyn dwóch par z $A \times B$ jest znowu elementem tego zbioru. Sugeruje to przeprowadzenie następnego eksperymentu, w którym zaryzykujemy już pełną ogólność sytuacji.

Niech więc A i B będą *dowolnymi* grupami i niech dany będzie homomorfizm

$$h : B \to \mathrm{Aut}A,$$

który każdemu elementowi $b \in B$ przyporządkowuje automorfizm $h(b)$ grupy A (w naszym eksperymencie z iloczynem półprostym mieliśmy $h(b) = i_b$). Taki homomorfizm h nazywa się też *działaniem grupy B na grupie A*. Na iloczynie kartezjańskim $A \times B$ zbiorów A i B definiujemy działanie następująco:

$$(a, b) \cdot (a_1, b_1) = (a \cdot h(b)(a_1),\ bb_1).$$

W tej definicji rozpoznajemy rozpatrywany wyżej przypadek iloczynu półprostego, w którym w miejsce automorfizmu $h(b)$ mieliśmy automorfizm wewnętrzny i_b. Sprawdzamy teraz bez większego trudu, że zbiór $A \times B$ z tak określonym mnożeniem jest grupą! Grupa ta zależy oczywiście od wybranego przez nas działania h grupy B na grupie A. Nazywa się ją *iloczynem półprostym grup A i B* wyznaczonym przez działanie h grupy B na grupie A. Oznaczamy ją następująco:

$$A \bowtie_h B.$$

Łatwo można stwierdzić, że odwzorowania

$$a \mapsto (a, 1) \quad \text{oraz} \quad b \mapsto (1, b)$$

są monomorfizmami grup A i B w grupę $A \bowtie_h B$. W tej sytuacji utożsamimy element a grupy A z jego obrazem $(a, 1)$, oraz element b grupy B z jego obrazem $(1, b)$ w grupie $A \bowtie_h B$. W ten sposób każdy element (a, b) iloczynu półprostego $A \bowtie_h B$ można przedstawić w postaci

$$(a, b) = (a, 1) \cdot (1, b) = a \cdot b.$$

Reguła mnożenia w grupie $A \bowtie_h B$ zapisze się teraz następująco:

$$ab \cdot a_1b_1 = a \cdot h(b)(a_1) \cdot bb_1.$$

Stąd, skracając lewostronnie a oraz prawostronnie b_1 oraz mnożąc prawostronnie przez b^{-1} otrzymujemy następującą równość

$$ba_1b^{-1} = h(b)(a_1)$$

dla każdego $a_1 \in A$, $b \in B$. A więc automorfizm $h(b)$ grupy A jest zacieśnieniem automorfizmu wewnętrznego i_b grupy $A \bowtie_h B$ do podgrupy A. Pozostaje teraz wybrać odpowiednio grupę B i homomorfizm $h : B \to \mathrm{Aut}A$ tak, by $h(b)$ przebiegał *wszystkie* automorfizmy grupy A. Istnieje prosty i uniwersalny sposób spełnienia tych postulatów: wystarczy wziąć $B = \mathrm{Aut}A$ zaś w charakterze homomorfizmu h wziąć homomorfizm tożsamościowy $\mathrm{id} : \mathrm{Aut}A \to \mathrm{Aut}A$. Otrzymany w ten sposób iloczyn półprosty $A \bowtie_{\mathrm{id}} \mathrm{Aut}A$ nazywamy *holomorfem* grupy A i oznaczamy

$$\mathrm{Hol}(A).$$

Udowodniliśmy więc następujące twierdzenie, które rozwiązuje postawiony wcześniej problem.

Twierdzenie 5.1. *Dla każdej grupy A istnieje grupa* $\mathrm{Hol}(A)$ *zawierająca A jako podgrupę normalną i mająca następującą własność. Każdy automorfizm grupy A jest zacieśnieniem do A pewnego automorfizmu wewnętrznego grupy* $\mathrm{Hol}(A)$.

Jako przykład rozważmy grupę cykliczną $A = \mathbf{Z}_n$. Jej grupa automorfizmów jest izomorficzna z multyplikatywną grupą $\mathbf{Z}_n^*$ reszt pierwszych względem n. Zatem

$$\mathrm{Hol}(\mathbf{Z}_n) \cong \mathbf{Z}_n \bowtie \mathbf{Z}_n^* \cong \mathrm{Af}(1, \mathbf{Z}_n),$$

gdzie $\mathrm{Af}(1, \mathbf{Z}_n)$ jest grupą afiniczną stopnia n nad pierścieniem $\mathbf{Z}_n$ reszt modulo n. Ponieważ $\mathrm{Aut}D_n \cong \mathrm{Af}(1, \mathbf{Z}_n)$ (zob. *Zbiór...* **331**), więc mamy także

$$\mathrm{Aut}D_n \cong \mathrm{Hol}(\mathbf{Z}_n).$$

Można także udowodnić, że dla iloczynu półprostego $G = \mathbf{Z}_n \bowtie \mathbf{Z}_m$ dwóch grup cyklicznych, jeśli $Z(G) = 1$, to $\mathrm{Aut}G \cong \mathrm{Hol}(\mathbf{Z}_n)$ (zob. Walls).

6. Wieża grup automorfizmów

Będziemy teraz rozpatrywać iteracje operacji przejścia od grupy G do jej grupy automorfizmów wewnętrznych $\mathrm{Inn}G$ lub grupy wszystkich automorfizmów $\mathrm{Aut}G$. Jest rzeczą interesującą zbadać, jaka jest struktura grupy symetrii (automorfizmów) grupy, a następnie, jakie prawa rządzą symetriami grupy symetrii, itd. W pierwszej kolejności rozpatrzymy przypadek grup automorfizmów wewnętrznych. A więc dla danej grupy G określamy ciąg grup I^nG następująco:

$$I^0G := G, \quad I^nG = \mathrm{Inn}(I^{n-1}G), \quad n \geq 1.$$

Ponieważ grupa $\mathrm{Inn}G$ jest homomorficznym obrazem grupy G, więc można byłoby oczekiwać, że ciąg I^nG osiągnie dla odpowiednio dużych n grupę jednostkową, przynajmniej gdy grupa G jest skończona. Okazuje się, że ma to miejsce tylko dla grup o specjalnych własnościach:

$$I^nG = 1 \quad \Leftrightarrow \quad G \text{ jest nilpotentna stopnia } \leq n.$$

Zob. *Zbiór...* **687**.

Natomiast całkiem inaczej wygląda sytuacja, gdy iterujemy operację przejścia od grupy G do grupy $\mathrm{Aut}G$. Rozpatrzymy najbardziej regularny przypadek, gdy $Z(G) = 1$. Wtedy homomorfizm

$$G \to \mathrm{Aut}G, \quad a \mapsto i_a$$

ma jądro $Z(G) = 1$, jest zatem monomorfizmem. Możemy więc utożsamić obraz tego homomorfizmu z grupą G i w ten sposób traktować grupę G jako podgrupę grupy $\mathrm{Aut}G$. Podkreślmy, że przy tym utożsamieniu element $a \in G$ identyfikujemy z automorfizmem wewnętrznym i_a grupy G.

Jeśli jednak G ma trywialne centrum, to grupa $\mathrm{Aut}G$ też ma trywialne centrum (twierdzenie 4.1). Zatem grupę $\mathrm{Aut}G$ możemy identyfikować z podgrupą automorfizmów wewnętrznych grupy $\mathrm{Aut}(\mathrm{Aut}G)$, która też ma trywialne centrum. A więc jeśli $Z(G) = 1$, to otrzymujemy *wieżę grup automorfizmów* grupy G:

$$G \subseteq \mathrm{Aut}G \subseteq \mathrm{Aut}(\mathrm{Aut}G) \subseteq \cdots$$

Będziemy mówili, że wieża ta jest skończona, jeśli pojawi się w niej na miejscu z numerem skończonym grupa D taka, że $D \cong \mathrm{Aut}D$. Wtedy oczywiście wszystkie następujące po D grupy w wieży są izomorficzne z D. Mówimy też wtedy, że wieża *stabilizuje się* na grupie D. Nie ma żadnych oczywistych powodów aby oczekiwać, iż wieża grup automorfizmów stabilizuje się. Przeciwnie, jeśli grupa ma trywialne centrum, to jest izomorficzna z grupą automorfizmów wewnętrznych, i wobec tego tylko w wyjątkowej sytuacji, gdy nie ma automorfizmów zewnętrznych, nie produkuje wyższego piętra w wieży grup automorfizmów. Jednakże wbrew tym naiwnym intuicjom, wieża grup automorfizmów grupy skończonej nie wymyka się spod kontroli, mamy bowiem następujący słynny rezultat teorii grup skończonych.

Twierdzenie 6.1. (Twierdzenie Wielandta)

Niech G będzie grupą skończoną z trywialnym centrum. Wtedy wieża grup automorfizmów grupy G jest skończona.

Dowód. Zobacz Robinson, str. 397. ■

Grupę D, na której stabilizuje się wieża grup automorfizmów, czyli taką, że $Z(D) = 1$ oraz $D \cong \mathrm{Aut}D$, nazywa się grupą *doskonałą*. Tak więc dla każdej grupy skończonej z trywialnym centrum istnieje skończona wieża grup automorfizmów kończąca się na grupie doskonałej.

Grupa symetryczna S_n dla $n \geq 3$ i $n \neq 6$ jest doskonała. Jest to twierdzenie Höldera z 1895 roku. Hölder wykazał także, że grupa symetryczna S_6 nie jest doskonała. Wobec tego, że grupy symetryczne S_n dla $n \geq 3$ mają trywialne centrum, oznacza to, że nie wszystkie automorfizmy grupy S_6 są wewnętrzne. Inaczej mówiąc, grupa S_6 ma automorfizm zewnętrzny. Konstrukcji tego automorfizmu poświęconych jest kilka prac, zob. Fournelle i cytowane tam prace. Istnieją też inne grupy doskonałe. Można, na przykład, udowodnić, że każda nieabelowa grupa prosta ma doskonałą grupę automorfizmów. Jest to twierdzenie Burnside'a (zob. Robinson, str. 399).

Dla grup nieskończonych z trywialnym centrum można zbudować wieżę pozaskończoną grup automorfizmów. Nie wiadomo, czy dla każdej grupy z trywialnym centrum wieża ta stabilizuje się. Istnieją jednak przykłady grup nieskończonych, których wieża grup automorfizmów jest nieskończona. Taką grupą jest grupa $D_\infty = \mathrm{Af}(1, \mathbf{Z})$. Jej wieża grup automorfizmów stabilizuje się jednak na holomorfie grupy liczb wymiernych o mianownikach będących potęgami liczby 2 (zob. Robinson, str. 400).

Nie wiadomo więc, jak bardzo symetryczne są grupy nieskończone.

Literatura

M.A. Armstrong, *Groups and symmetry.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo 1988.

T.A. Fournelle, Symmetries of the cube and outer automorphisms of S_6. *Amer. Math. Monthly* **100**(1993), 377–380.

J.A. Green, On the number of automorphisms of a finite group. *Proc. Roy. Soc.* **A237**(1956), 574–581.

A.I. Kostrykin, *Wstęp do algebry.* PWN Warszawa 1984.

W. Lederman, B.H. Neumann, On the order of the automorphism group of a finite group. II. *Proc. Roy. Soc.* **A235**(1956), 235–246.

B.I. Plotkin, *Grupy automorfizmów systemów algebraicznych* (j. ros.). Moskwa 1966.

D.J.S. Robinson, *A course in the theory of groups.* Graduate Texts in Mathematics, vol. 80. Springer-Verlag, New York, Heidelberg, Berlin 1982.

K. Szymiczek, *Zbiór zadań z teorii grup.* PWN Warszawa 1989.

G.L. Walls, Automorphism groups, *Amer. Math. Monthly* **93**(1986), 459–462.