1. GRUPA

W licealnym kursie geometrii spotykamy się często z pojęciem grupy przekształceń. Na przykład grupami przekształceń są wszystkie izometrie płaszczyzny (lub przestrzeni), wszystkie przesunięcia płaszczyzny (lub przestrzeni) i wszystkie obroty płaszczyzny dokoła ustalonego punktu O.

Symetrie osiowe nie stanowią grupy przekształceń, bo złożenie dwóch symetrii osiowych nie jest symetrią osiową (jest przesunięciem albo obrotem).

W każdym z tych przykładów mamy dany zbiór P przekształceń, dla którego:

1) złożenie dowolnych dwóch przekształceń należących do P jest przekształceniem należącym do P,

2) przekształcenie tożsamościowe należy do P,

3) każde przekształcenie należące do P ma przekształcenie odwrotne, również należące do P.

Inaczej mówiąc:

1) każdej parze elementów z P przyporządkowany jest pewien element P (każdej parze przekształceń odpowiada ich złożenie),

2) w zbiorze P jest wyróżniany pewien element e o tej własności, że dla każdego $f \in P$

$$f \circ e = e \circ f = f$$

3) dla każdego $f \in P$ istnieje przekształcenie f^{-1} spełniające warunek

$$f \circ f^{-1} = f^{-1} \circ f = e$$

Ponadto ze sposobu określenia złożenia przekształceń wynika, że jest spełniony warunek łączności

$$f \circ (g \circ h) = (f \circ g) \circ h$$

działanie $\circ$

Przykład ten zachęca do następujących uogólnień. Przypuśćmy, że w zbiorze X określone jest działanie $\circ$, tj. każdej parze elementów $a, b \in X$ jest przyporządkowany element $a \circ b \in X$.

łączność działania $\circ$

Działanie $\circ$ jest łączne, jeśli dla dowolnych elementów $a, b, c \in X$ zachodzi wzór

$$(a \circ b) \circ c = a \circ (b \circ c)$$

element jednostkowy

Działanie określone w zbiorze liczb rzeczywistych wzorem

$$a \circ b = \frac{a+b}{2}$$

nie jest łączne, bo na przykład

$$(1 \circ 3) \circ 7 = \frac{1+3}{2} \circ 7 =$$

$$= 2 \circ 7 = \frac{2+7}{2} = \frac{9}{2}$$

$$1 \circ (3 \circ 7) = 1 \circ \frac{3+7}{2} =$$

$$= 1 \circ 5 = \frac{1+5}{2} = 3$$

Działania dodawania i mnożenia liczb są działaniami łącznymi, także składanie przekształceń jest działaniem łącznym.

Element $e \in X$ nazywany elementem jednostkowym względem działania $\circ$, jeśli dla każdego elementu $a \in X$ jest spełniony warunek

$$a \circ e = e \circ a = a$$

Na przykład jedynka jest elementem jednostkowym względem mnożenia liczb, zero — względem dodawania liczb, przekształcenie identycznościowe — względem składania przekształceń.

Okazuje się, że w każdym zbiorze X, w którym jest określone działanie $\circ$, istnieje najwyżej jeden element jednostkowy względem tego działania. Gdyby bowiem dla elementów $e, e' \in X$

$$a \circ e = e \circ a = a \text{ dla każdego } a \in X$$

oraz

$$a \circ e' = e' \circ a = a \text{ dla każdego } a \in X$$

to kładąc w pierwszej równości $a = e'$, w drugiej zaś $a = e$, otrzymalibyśmy

$$e' \circ e = e \circ e' = e'$$

oraz

$$e \circ e' = e' \circ e = e$$

więc $e = e'$.

grupa

Znaki $\bigwedge_x$, $\bigvee_x$ nazywają się kwantyfikatorami i stanowią odpowiednio symbole zwrotów „dla każdego x" oraz „istnieje taki x, że".

Możemy teraz sformułować następującą definicję: grupą nazywamy zbiór G, w którym jest określone działanie $\circ$ spełniające następujące warunki:

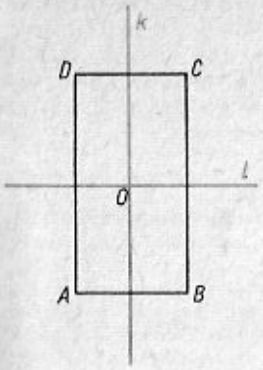
1. $\bigwedge_{a,b,c \in G} (a \circ b) \circ c = a \circ (b \circ c)$

2. $\bigvee_{e \in G} \bigwedge_{a \in G} a \circ e = e \circ a = a$

3. $\bigwedge_{a \in G} \bigvee_{a' \in G} a \circ a' = a' \circ a = e$

Z warunku 2 oraz wcześniejszego rozumowania wynika, że istnieje dokładnie jeden element jednostkowy w grupie G. Podobnie można wykazać, że dla danego a istnieje tylko jeden element a' spełniający warunek 3. Element ten nazywamy elementem odwrotnym do a i oznaczamy go symbolem a^{-1}.

Dla uproszczenia zapisu często działanie w grupie G nazywa się mnożeniem, zaś wynik tego działania na dwóch elementach — iloczynem tych elementów. W przypadkach gdy nie prowadzi to do nieporozumienia, używamy na oznaczenie iloczynu elementów a, b symbolu $a \circ b$ lub ab.



Rys. 1

W przypadku gdy grupa ma skończoną liczbę elementów, można działanie zapisać przy użyciu tabelki. Tabelka taka jest kwadratową siatką pól, po lewej jej stronie i nad nią wypisujemy wszystkie elementy danego zbioru. W polu znajdującym się na poziomie elementu x i pod elementem y wypisujemy wynik działania $x \circ y$.

Przykłady

1. Zbiór liczb całkowitych tworzy grupę względem dodawania.
2. Zbiór liczb wymiernych dodatnich tworzy grupę względem mnożenia.
3. Rozważmy na płaszczyźnie dowolny prostokąt $ABCD$ i izometrie płaszczyzny przekształcające ten prostokąt na ten sam prostokąt: identyczność I, symetrię S_k względem wspólnej symetrialnej k odcinków $\overline{AB}$ i $\overline{CD}$, symetrię S_l względem wspólnej symetrialnej l odcinków $\overline{BC}$ i $\overline{DA}$ oraz symetrię środkową S_0 względem punktu przecięcia O prostych k i l (rys. 1).

Izometrie te stanowią grupę przekształceń, w której działanie opisuje tabelka

	I	S_k	S_l	S_0
I	I	S_k	S_l	S_0
S_k	S_k	I	S_0	S_l
S_l	S_l	S_0	I	S_k
S_0	S_0	S_l	S_k	I

Zadania

1.1 Który z następujących zbiorów liczb $\{0\}$, $\{1\}$, $\{0, 1\}$ stanowi grupę względem mnożenia? Który z tych zbiorów stanowi grupę względem dodawania?

*1.2 Dane są grupy G i H. Czy zbiór par (g, h) gdzie $g \in G$, $h \in H$, stanowi grupę względem działania

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

4. Niech n będzie ustaloną liczbą naturalną. Rozpatrzmy zbiór $C_n = \{0, 1, \ldots, n-1\}$ i określmy w nim działanie $\underset{n}{+}$ następująco:

$a \underset{n}{+} b$ = reszta z dzielenia liczby $a+b$ przez n.

Dla uproszczenia zapisu będziemy resztę z dzielenia liczby c przez n oznaczać symbolem $(c)_n$. Zatem

$$a \underset{n}{+} b = (a+b)_n$$

Działanie $\underset{n}{+}$ jest istotnie określone w zbiorze $\{0, 1, \ldots, n-1\}$. Sprawdzimy, czy są spełnione wymagania definicji grupy

1. $(a \underset{n}{+} b) \underset{n}{+} c = a \underset{n}{+} (b \underset{n}{+} c)$

Wykażemy najpierw, że

$$(a \underset{n}{+} b) \underset{n}{+} c = (a+b+c)_n$$

Ponieważ

$$a+b = q\cdot n+(a+b)_n$$

gdzie: q jest ilorazem, $(a+b)_n$ – resztą z dzielenia $a+b$ przez n, więc reszta z dzielenia liczby $(a+b)+c$ przez n jest równa reszcie z dzielenia liczby $(a+b)+c$ przez n.

Wobec tego

$$(a+b+c)_n = [(a+b)+c]_n = [(a\dot{+}b)+c]_n = (a\dot{+}b)\dot{+}c$$

Analogicznie stwierdzamy, że

$$a\dot{+}(b\dot{+}c) = (a+b+c)_n$$

Wobec tego

$$(a\dot{+}b)\dot{+}c = a\dot{+}(b\dot{+}c)$$

2. Element 0 ma własność

$$a\dot{+}0 = 0\dot{+}a = a$$

dla każdego elementu a rozważanego zbioru.

3. Ponieważ $0\dot{+}0 = 0$ oraz dla $a \in C_n$, $a \neq 0$

$$a\dot{+}(n-a) = 0$$

więc dla każdego a istnieje element odwrotny względem działania $\dot{+}$.

grupa przemienna

Grupę G nazywa się przemienną, jeśli

$$\bigwedge_{a,b\in G} ab = ba$$

Grupy w powyższych przykładach są przemienne. Grupa wszystkich izometrii płaszczyzny nie jest przemienna*.

* Aby stwierdzić, że grupa izometrii płaszczyzny nie jest przemienna, rozważmy symetrie osiowe S_1 i S_2 o osiach będących prostymi równoległymi l_1 i l_2. Przekształcenie złożone S_2S_1 jest przesunięciem o wektor prostopadły do prostych l_1, l_2, mający długość równą podwojonej odległości między tymi prostymi i skierowany od l_1 do l_2. Natomiast przekształcenie S_1S_2 jest przesunięciem o wektor przeciwny.

2. PODGRUPA

podgrupa

Podzbiór H grupy G nazywamy podgrupą, jeśli H jest grupą ze względu na to samo działanie co G.

Przykłady

1. Zbiór liczb parzystych stanowi podgrupę grupy liczb całkowitych względem dodawania.

2. Przesunięcia płaszczyzny stanowią podgrupę grupy wszystkich izometrii.

3. Podzbiór złożony z elementu jednostkowego danej grupy G stanowi podgrupę grupy G.

Aby zbadać, czy dany podzbiór H grupy G jest podgrupą, nie musimy sprawdzać wszystkich aksjomatów.

Twierdzenie. *Niepusty podzbiór H grupy G jest podgrupą wtedy i tylko wtedy, gdy dla dowolnych $a, b \in H$ element ab^{-1} należy do H.*

Dowód. Jeśli H jest podgrupą, to oczywiście warunek ten jest spełniony.

Przypuśćmy, że niepusty podzbiór $H \subset G$ spełnia warunek

$$\bigwedge_{a,b\in H} ab^{-1} \in H, \qquad (*)$$

Weźmy dowolny element $c \in H$. Z warunku $(*)$ wynika, że $e = c\cdot c^{-1}$ należy do H. Następnie dla dowolnego $b \in H$ $b^{-1} = e\cdot b^{-1}$, więc $b^{-1} \in H$

oraz dla dowolnych $a, b \in H$

$$ab = a(b^{-1})^{-1} \in H$$

Wykazaliśmy w ten sposób, że w H określone jest działanie grupowe, element jednostkowy e należy do H i wreszcie dla każdego elementu $b \in H$ element odwrotny b^{-1} też należy do H. Ponadto działanie w H jest łączne, bo jest ono łączne dla dowolnych elementów G.

Jeśli a jest ustalonym elementem grupy G, to również elementy $a \circ a$, $a \circ a \circ a$, ..., a^{-1}, $a^{-1} \circ a^{-1}$, $a^{-1} \circ a^{-1} \circ a^{-1}$, ... należą do G. Dla uproszczenia zapisu element $\underbrace{a \circ a \circ \ldots \circ a}_{n}$ oznaczamy symbolem a^n,

element $\underbrace{a^{-1} \circ a^{-1} \circ \ldots \circ a^{-1}}_{n}$ symbolem a^{-n},

ponadto przyjmujemy $a^0 = e$.

Można udowodnić, że obowiązuje wzór

$$a^n \circ a^m = a^{n+m}$$

gdzie $a \in G$, m, n są dowolnymi liczbami całkowitymi. Element a^n nazywamy n-tą potęgą elementu a.

Zbiór liczb nieparzystych nie stanowi podgrupy grupy liczb całkowitych względem dodawania, gdyż suma liczb nieparzystych jest liczbą parzystą. Zbiór liczb wymiernych dodatnich nie stanowi podgrupy grupy liczb wymiernych względem dodawania, ponieważ elementem odwrotnym do liczby dodatniej a względem tego działania jest liczba ujemna $-a$. Zbiór liczb wymiernych dodatnich stanowi natomiast podgrupę grupy liczb wymiernych różnych od zera względem mnożenia.

Zadania

2.1 Wykazać, że każda podgrupa grupy liczb całkowitych względem dodawania jest cykliczna.

2.2 Wykazać, że każda podgrupa grupy cyklicznej jest cykliczna.

2.3 Rozstrzygnąć, czy grupa liczb wymiernych względem dodawania jest cykliczna.

2.4 Rozważamy na płaszczyźnie obroty dokoła ustalonego punktu O o kąty $k\cdot 2\pi/n^m$, gdzie: n jest ustaloną liczbą naturalną, k, m są dowolnymi liczbami całkowitymi. Wykazać, że wszystkie te obroty stanowią grupę, która nie jest cykliczna, ale każda jej podgrupa różna od całej grupy jest cykliczna.

Wykażemy, że zbiór wszystkich potęg ustalonego elementu a grupy G stanowi podgrupę grupy G. Istotnie dla potęg a^n, a^m element

$$a^n \circ (a^m)^{-1} = a^n \circ a^{-m} = a^{n-m}$$

też jest potęgą elementu a. Wobec tego na mocy powyższego twierdzenia, potęgi elementu a stanowią podgrupę grupy G.

podgrupa cykliczna generowana przez a

Podgrupę złożoną ze wszystkich potęg elementu a nazywamy podgrupą cykliczną generowaną przez a.

Przykłady

1. Zbiór liczb podzielnych przez 5 jest podgrupą cykliczną generowaną przez 5, grupy wszystkich liczb całkowitych.

2. Niech G będzie grupą izometrii płaszczyzny. Rozpatrzmy obrót f dokoła ustalonego punktu O o kąt 90°. Zbiór wszystkich potęg tego elementu zawiera cztery różne przekształcenia: f – obrót o 90°, f^2 – obrót o 180°, f^3 – obrót o 270° i $e = f^4$ – obrót o 360° (tożsamość). Podgrupa cykliczna generowana przez f ma cztery elementy.

grupa cykliczna

Grupa jest cykliczna, jeśli istnieje w niej taki element a, że wszystkie elementy grupy G są potęgami elementu a.

3. RZĄD GRUPY, WARSTWY

rząd grupy

Liczbę elementów grupy nazywamy rzędem grupy. Wobec tego rząd grupy G wynosi n (piszemy $\mathrm{rz}G = n$), jeśli G ma dokładnie n elementów, natomiast rząd grupy G jest nieskończony (piszemy $\mathrm{rz}G = \infty$), jeśli elementów G jest nieskończenie wiele.

rząd elementu

Rzędem elementu $a \in G$ nazywamy rząd podgrupy cyklicznej generowanej przez a.

Można wykazać [2], że rząd elementu $a \in G$ wynosi n wtedy i tylko wtedy, gdy n jest najmniejszą taką liczbą naturalną, że $a^n = e$.

Aby wyznaczyć zależność między rzędem grupy a rzędem jej podgrupy wprowadzimy następujące pojęcie. Dla grupy G

warstwa lewostronna elementu

warstwą lewostronną elementu $a \in G$ względem podgrupy H nazywamy zbiór $\{ah, h \in H\}$. Warstwę tę oznaczamy przez aH.

Przykład

W grupie liczb całkowitych rozważmy podgrupę H liczb podzielnych przez 3. Warstwa elementu 5 względem podgrupy H składa się ze wszystkich liczb mających postać $5+3k$, gdzie k jest liczbą całkowitą, a więc z liczb dających przy dzieleniu przez 3 resztę 2. Widać, że zbiór liczb całkowitych rozpada się na trzy warstwy: pierwsza składa się z liczb podzielnych przez 3, druga – z liczb dających przy dzieleniu przez 3 resztę 1, trzecia – z liczb dających przy dzieleniu przez 3 resztę 2.

Pokażemy, że każdy element grupy G należy do dokładnie jednej warstwy względem podgrupy H. Oczywiście element a należy do warstwy aH. Załóżmy, że $a \in bH$. Pokażemy, że $aH = bH$. Z założenia wynika, że $a = bh$ dla pewnego $h \in H$. Dowolny element warstwy aH ma postać $c = ah_1$, gdzie $h_1 \in H$. Zatem

$$c = ah_1 = (bh)h_1 = b \circ (hh_1) \in bH$$

Wynika stąd, że $c \in bH$, a więc $aH \subset bH$.

Z drugiej strony $b = ah^{-1}$, więc $b \in aH$ i prowadząc analogiczne rozumowanie, stwierdzimy, że $bH \subset aH$. Stąd $aH = bH$.

Z powyższego wynika dla grup skończonych

Twierdzenie (Lagrange). *Rząd podgrupy jest dzielnikiem rzędu grupy.*

Dowód. Niech $\mathrm{rz}G = n$. Każdy element grupy G należy do dokładnie jednej warstwy lewostronnej względem podgrupy H. Ponadto przyporządkowanie

$$f: H \to aH, \qquad f(h) = ah$$

ustala odpowiedniość wzajemnie jednoznaczną między elementami podgrupy H a elementami warstwy aH (gdyby $ah_1 = ah_2$, to mnożąc przez a^{-1} z lewej strony oba wyrażenia równości, otrzymamy $h_1 = h_2$). Stąd wynika, że liczba elementów warstwy aH równa jest liczbie $\mathrm{rz}H$. Wobec tego rząd grupy G jest iloczynem rzędu podgrupy H i liczby warstw lewostronnych. ■

Zadania

3.1 Podać przykład grupy nieskończonej, której każdy element różny od elementu jednostkowego ma rząd nieskończony.

3.2 Podać przykład grupy nieskończonej, której każdy element ma rząd skończony.

3.3 Podać przykład grupy, która dla każdej liczby naturalnej n zawiera elementy rzędu n.

3.4 Wykazać, że grupa, której rząd jest liczbą pierwszą, jest grupą cykliczną.

warstwa prawostronna elementu

Warstwą prawostronną elementu $a \in G$ względem podgrupy H nazywamy $Ha = \{ha, h \in H\}$. Własności tej warstwy są podobne do własności warstwy lewostronnej.

4. HOMOMORFIZM, PODGRUPA NORMALNA, GRUPA ILORAZOWA

W teorii grup wyróżnia się te przekształcenia, które zachowują działanie grupowe. Niech G będzie grupą względem działania $\circ$, G' – grupą względem działania $\square$.

homomorfizm

Przekształcenie $f: G \to G'$ nazywamy homomorfizmem, jeśli dla dowolnych elementów $a, b \in G$

$$f(a \circ b) = f(a) \square f(b)$$

Przykłady

1. Przyporządkowując każdemu elementowi grupy G element jednostkowy e' grupy G', określamy homomorfizm G w G'.

2. Przyporządkujmy każdej liczbie parzystej element 0, a każdej liczbie nieparzystej element 1 grupy C_2. Aby sprawdzić, czy jest to homomorfizm grupy liczb całkowitych w C_2, zauważmy, że suma liczb o tej samej parzystości jest liczbą parzystą, zaś suma liczb o różnej parzystości – liczbą nieparzystą. W grupie C_2

$$0 \overset{+}{_2} 0 = 0, \quad 1 \overset{+}{_2} 1 = 0, \quad 1 \overset{+}{_2} 0 = 0 \overset{+}{_2} 1 = 1$$

Jeśli $f: G \to G'$ jest homomorfizmem, to obrazem elementu jednostkowego e grupy G jest element jednostkowy grupy G'. Istotnie, z faktu $e \circ e = e$ wynika, że $f(e)$ spełnia warunek $f(e) \square f(e) = f(e)$. Stąd wniosek, że $f(e)$ jest elementem jednostkowym grupy G'. Mogą jednak istnieć różne od e elementy grupy G, które homomorfizm f przekształca na element jednostkowy grupy G'.

jądro homomorfizmu

Przyjmiemy następujące określenie: jądrem homomorfizmu $f: G \to G'$ nazywamy zbiór

$$\{a \in G : f(a) = e'\}$$

gdzie e' jest elementem jednostkowym grupy G'. Jądro homomorfizmu f oznaczamy symbolem $\ker f$.

Jądro homomorfizmu $f: G \to G'$ jest podgrupą grupy G. Aby to wykazać, wystarczy stwierdzić, że jeśli $a, b \in \ker f$, to $ab^{-1} \in \ker f$.

Istotnie

$$f(ab^{-1}) = f(a) \cdot f(b^{-1}) = f(a) \cdot f(b)^{-1} = e \cdot (e)^{-1} = e$$

więc $ab^{-1} \in \ker f$.

Nasuwa się tu naturalne pytanie: czy każda podgrupa grupy G jest jądrem pewnego homomorfizmu? Okazuje się, że nie.

podgrupa normalna

Podgrupę H grupy G nazywamy podgrupą normalną, jeżeli

$$\bigwedge_{g \in G} \bigwedge_{h \in H} g^{-1} h g \in H$$

Przykładem grupy, której pewna podgrupa nie jest jądrem żadnego homomorfizmu, jest grupa izometrii przekształcających dany trójkąt równoboczny na ten sam trójkąt. Grupa ta składa się z przekształcenia tożsamościowego I, symetrii S_a, S_b, S_c względem symetralnych kolejnych boków oraz obrotów O_1, O_2 dokoła środka ciężkości trójkąta o kąty odpowiednio 120° i 240°.

Powyższy warunek równoważny jest następującemu warunkowi: każda warstwa lewostronna względem H jest równa odpowiedniej warstwie prawostronnej. Istotnie, jeśli $gH = Hg$, to dla dowolnego $h \in H$, $hg \in gH$, a więc $hg = gh_1$, $g^{-1}hg = h_1 \in H$. Jeśli natomiast $g^{-1} hg \in H$, to $hg \in gH$, więc $Hg \subset gH$ i analogicznie $gH \subset Hg$.

Twierdzenie. *Jeśli $f: G \to G'$ jest homomorfizmem, to $\ker f$ jest podgrupą normalną grupy G.*

Działanie w tej grupie podaje tabelka

	I	S_a	S_b	S_c	O_1	O_2
I	I	S_a	S_b	S_c	O_1	O_2
S_a	S_a	I	O_1	O_2	S_b	S_c
S_b	S_b	O_2	I	O_1	S_c	S_a
S_c	S_c	O_1	O_2	I	S_a	S_b
O_1	O_1	S_c	S_a	S_b	O_2	I
O_2	O_2	S_b	S_c	S_a	I	O_1

Rozważmy podgrupę H złożoną z elementów I, S_a. Warstwa lewostronna elementu O_1 względem podgrupy H składa się z elementów O_1, S_c, podczas gdy warstwa prawostronna elementu O_1 względem H składa się z elementów O_1, S_b. Zatem $O_1 \cdot H \neq H \cdot O_1$, skąd wynika, że podgrupa H nie jest podgrupą normalną. Na podstawie twierdzenia wynika stąd, że H nie jest jądrem żadnego homomorfizmu.

Nie można w analogiczny sposób określić działania na warstwach względem podgrupy, która nie jest normalna. Rozpatrzmy w grupie izometrii trójkąta równobocznego podgrupę $H = \{I, S_a\}$ oraz warstwy $O_1 \cdot H$ i $O_2 \cdot H$. Ponieważ $O_1 \cdot H = \{O_1, S_c\}$, $O_2 \cdot H = \{O_2, S_b\}$, więc biorąc z pierwszej warstwy O_1, z drugiej O_2, i mnożąc te elementy, otrzymujemy $O_1 O_2 = I$. Natomiast biorąc z pierwszej warstwy S_c, z drugiej S_b, i mnożąc, otrzymujemy $S_c S_b = O_2$. Elementy I oraz O_2 nie należą do jednej warstwy (ani lewostronnej, ani prawostronnej) względem podgrupy H. Okazuje się więc, że w tym przypadku iloczyn elementów wybranych z warstw nie wyznacza jednoznacznie warstwy.

Dowód. Stwierdziliśmy wyżej, że $\ker f$ jest podgrupą grupy G. Przypuśćmy, że $g \in G$, $h \in \ker f$. Wobec tego

$$f(g^{-1}hg) = f(g^{-1}) \cdot f(h) \cdot f(g) = f(g^{-1}) \cdot e \cdot f(g) =$$
$$= f(g^{-1}) \cdot f(g) = f(g^{-1} \cdot g) = f(e) = e'$$

Wynika stąd, że $g^{-1} hg \in \ker f$.

Przykład

W grupie liczb całkowitych C podgrupa liczb podzielnych przez ustaloną liczbę n jest jądrem homomorfizmu odwzorowującego C na C_n i przyporządkowującego liczbie m resztę z dzielenia m przez n. Podgrupa liczb podzielnych przez n jest więc podgrupą normalną.

Wykażemy obecnie, że dla każdej grupy G i jej podgrupy normalnej H istnieje grupa G' oraz homomorfizm $f: G \to G'$, którego jądrem jest H, tj. krótko mówiąc, każda podgrupa normalna jest jądrem pewnego homomorfizmu.

Rozpatrzmy zbiór warstw (dla ustalenia uwagi – warstw lewostronnych) w grupie G względem podgrupy normalnej H. W dalszym ciągu będziemy mówić krótko „warstwy", opuszczając słowo „lewostronne", gdyż dla podgrupy normalnej warstwy lewostronne są również prawostronne. W zbiorze warstw określmy działanie wzorem

$$aH \circ bH = (ab)\, H$$

Wzór ten podaje następującą zasadę: aby wykonać działanie na dwóch warstwach, do których należą odpowiednio a i b, mnożymy a przez b i za wynik działania na warstwach bierzemy tę warstwę, do której należy ab. Aby upewnić się czy ta reguła jest poprawnie określona, a więc czy wynik działania nie zależy od sposobu wyboru elementów z warstw, musimy wykazać, że jeżeli $a' \in aH$, $b' \in bH$, to

$$(a'b')\, H = (ab)\, H$$

Ponieważ $a' \in aH$, więc $a' = ah_1$ dla pewnego $h_1 \in H$. Podobnie $b' = bh_2$ dla pewnego $h_2 \in H$. Wobec tego

$$a'b' = (ah_1)\,(bh_2) = a\,(h_1\, b)\, h_2$$

Ponieważ $h_1 b \in Hb$ oraz $Hb = bH$, więc element $h_1 b$ należy do bH.

Istnieje zatem $h_3 \in H$, dla którego $h_1\, b = bh_3$. Stąd

$$a'b' = a\,(h_1 b)\, h_2 = a\,(bh_3)\, h_2 = (ab)\,(h_3 h_2) \in (ab)\, H$$

Wykazaliśmy, że $a'b' \in (ab)\, H$, stąd wynika, że $(a'b')\, H = (ab)\, H$.

Wykażemy, że zbiór warstw w grupie G względem podgrupy normalnej H stanowi grupę względem działania

$$aH \circ bH = (ab)\, H$$

1. Działanie to jest łączne

$(aH \circ bH) \circ cH = (ab)\,H \circ cH = [(ab)\,c]\,H =$

$= [a\,(bc)]\,H = aH \circ (bc)\,H = aH \circ (bH \circ cH)$

2. Elementem jednostkowym jest warstwa elementu jednostkowego $e \in G$, gdyż

$eH \circ aH = (ea)\,H = aH\,, \quad aH \circ eH = (ae)\,H = aH$

3. Dla dowolnej warstwy aH elementem odwrotnym jest warstwa $a^{-1}H$. Istotnie

$aH \circ a^{-1}H = (aa^{-1})\,H = eH\,,$

$a^{-1}H \circ aH = (a^{-1}a)\,H = eH$

Grupę warstw grupy G względem podgrupy normalnej H z działaniem określonym następująco

$aH \odot bH = (ab)\,H$

grupa ilorazowa

nazywamy grupą ilorazową grupy G modulo H i oznaczamy symbolem G/H.

Mając grupę G i podgrupę normalną H, możemy określić naturalne odwzorowanie $f: G \to G/H$, które przyporządkowuje każdemu elementowi $a \in G$ warstwę tego elementu $f(a) = aH$. Przyporządkowanie to jest homomorfizmem

$f(ab) = (ab)\,H = aH \circ bH = f(a) \circ f(b)$

a jądrem tego homomorfizmu jest zbiór

$\{a \in G, f(a) = eH\} = H$

Udowodniliśmy w ten sposób

Twierdzenie. *Jeśli H jest podgrupą normalną grupy G to przyporządkowując każdemu elementowi grupy G jego warstwę względem H, otrzymujemy homomorfizm grupy G na G/H, którego jądrem jest H.*

Przykład

W grupie liczb całkowitych rozważmy podgrupę normalną liczb podzielnych przez 3. Wyznacza ona trzy warstwy, na których działanie podaje tabelka

	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

gdzie kreseczka oznacza warstwę, np. $\bar{1} = \{3k+1\}$, $k = 0, 1, -1, 2, -2,$

Przyporządkowującka każdej liczbie n warstwę $\bar{n}$, określamy homomorfizm grupy liczb całkowitych w grupę warstw.

Zadania

4.1 Wyznaczyć wszystkie homomorfizmy odwzorowujące C_4 w grupę C_6 oraz wszystkie homomorfizmy odwzorowujące C_6 w C_4. Wyznaczyć jądro każdego z tych homomorfizmów.

4.2 Wykazać, że każda podgrupa grupy przemiennej jest podgrupą normalną.

4.3 Wykazać, że jeśli podgrupa grupy rzędu $2k$ ma rząd k, to jest podgrupą normalną.

4.4 Wykazać, że obraz homomorficzny grupy skończonej ma rząd będący dzielnikiem rzędu danej grupy.

5. GRUPY PERMUTACJI

Wśród grup skończonych na szczególną uwagę zasługują grupy permutacji.

permutacja

Przekształcenie różnowartościowe zbioru skończonego A na A nazywamy permutacją zbioru A. Permutacje zbioru n-elementowego stanowią grupę przekształceń rzędu $n!$ Oznaczamy ją przez S_n. Dla uproszczenia zapisu przyjmujemy zwykle, że $A = \{1, 2, \ldots, n\}$. Permutację przedstawiamy w postaci

$$\sigma = \begin{pmatrix} 1, & 2, & \ldots, & n \\ \sigma(1), \sigma(2), & \ldots, & \sigma(n) \end{pmatrix}$$

Na przykład permutacja

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

jest przekształceniem, w którym obrazem elementu 1 jest 3, obrazem 2 jest 1, obrazem 3 jest 2, obrazem 4 jest 4. Taki zapis umożliwia łatwe wyznaczenie przekształcenia odwrotnego oraz złożenia permutacji, np.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 1 & 2 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

Przy wyznaczaniu permutacji odwrotnej zamieniamy miejscami wiersz pierwszy i drugi, a następnie porządkujemy kolumny. Przy składaniu permutacji wyznaczamy obrazy kolejnych elementów w przekształceniu złożonym pamiętając, że zgodnie z przyjętym zwyczajem zapisywania funkcji złożonych, najpierw wykonujemy przekształcenia napisane po prawej stronie.

Każda izometria odwzorowująca kwadrat $ABCD$ na ten sam kwadrat wyznacza pewną permutację zbioru wierzchołków tego kwadratu $\{A, B, C, D\}$, np. symetria względem przekątnej AC wyznacza permutację

$$\begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}$$

Nie każdą jednak permutację zbioru A, B, C, D można uzyskać przez izometrię kwadratu, gdyż obrazami wierzchołków sąsiednich muszą być wierzchołki sąsiednie. Tak więc, np. permutacja

$$\begin{pmatrix} A & B & C & D \\ A & C & B & D \end{pmatrix}$$

nie jest wyznaczona przez żadną izometrię kwadratu.

cykl

Wygodnie również zapisywać permutacje w postaci iloczynu tzw. cykli. Permutację τ nazywamy cyklem, jeśli w zbiorze permutowanym A istnieje podzbiór $B = \{b_1, b_2, \ldots, b_k\}$ o tej własności, że

$$\tau(b_1) = b_2\,, \quad \tau(b_2) = b_3\,, \ldots, \tau(b_{k-1}) = b_k\,, \quad \tau(b_k) = b_1$$

natomiast $\tau(a) = a$ dla $a \in A - B$.

cykle rozłączne

Dwa cykle nazwiemy rozłącznymi, jeśli zbiory poruszanych przez nie elementów są rozłączne.

długość cyklu

Liczbę elementów poruszanych przez cykl nazywamy długością cyklu.

Przykłady

1. Permutacja

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

jest cykliczna, gdyż przyjmując $B = \{1, 3, 2, 4\}$, mamy $\pi(1) = 3$, $\pi(3) = 2$, $\pi(2) = 4$, $\pi(4) = 1$.

2. Permutacja

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

również jest cykliczna, gdyż dla $B = \{1, 2, 4\}$, mamy $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(4) = 1$, natomiast $\sigma(3) = 3$.

3. Permutacja

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

nie jest cykliczna, gdyż dla każdego $i = 1, 2, 3, 4$, $\tau(i) \neq i$. Zakładając, że byłaby to permutacja cykliczna, należałoby przyjąć $B = \{1, 2, 3, 4\}$. Tymczasem $\tau(1) = 2$, $\tau(2) = 1$.

Przyjmijmy następującą zasadę zapisywania cykli: zapis $\pi = (a_1, a_2, \ldots, a_r)$ oznacza cykl π, dla którego

$$B = \{a_1, a_2, \ldots, a_r\}, \pi(a_1) = a_2, \ldots, \pi(a_{r-1}) = a_r,$$
$$\pi(a_r) = a_1$$

Z zapisu tego nie można odczytać, jaki jest zbiór wszystkich elementów permutowanych; możemy więc stosować ten zapis tylko wtedy, gdy wiadomo w jakim zbiorze określona jest permutacja π.

Przykład

Niech $A = \{1, 2, 3, 4, 5\}$. Możemy zapisać

$$(1, 3, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}, \quad (1, 2, 3, 4, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

$$(3, 2, 4, 1) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}$$

$$(1, 4, 2) = (4, 2, 1) = (2, 1, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$$

Twierdzenie. *Każda permutacja jest cyklem lub iloczynem cykli.*

Dowód. Zastosujemy indukcję matematyczną ze względu na liczbę elementów zbioru permutowanego $A = \{a_1, a_2, \ldots, a_n\}$. Dla $n = 1$ teza twierdzenia jest oczywista, bowiem istnieje tylko jedna permutacja zbioru $A = \{a_1\}$. Jest to permutacja tożsamościowa, która jest cykliczna.

Niech $n > 1$. Przyjmijmy założenie, że każdą permutację zbioru mającego mniej niż n elementów można przedstawić w postaci iloczynu permutacji cyklicznych. Rozpatrzmy permutację π zbioru $A = \{a_1, a_2, \ldots, a_n\}$. Utwórzmy następujący ciąg elementów zbioru A

$$b_0 = a_1, \quad b_1 = \pi(a_1),$$
$$b_2 = \pi(b_1) = \pi\pi(a_1), \ldots, b_k = \pi(b_{k-1}) = \underbrace{\pi \ldots \pi}_{k}(a_1)$$

Ponieważ zbiór A jest skończony, więc pewne wyrazy tego ciągu muszą się powtarzać. Przypuśćmy, że liczba k jest najmniejszą taką liczbą, iż wyraz b_k jest równy jednemu z poprzednich. Pokażemy, że $b_k = b_0$. Zakładając, że $b_k \neq b_0$, otrzymujemy $b_k = b_s$ dla $0 < s < k$, a ponieważ $\pi(b_{s-1}) = b_s = b_k = \pi(b_{k-1})$, więc $b_{s-1} = b_{k-1}$ (bo permutacja jest funkcją równowartościową, a to przeczyłoby określeniu liczby k). Jeżeli $k = n$, to elementy

$$b_0 = a_1, \quad b_1 = \pi(a_1), \ldots, b_{k-1} = \underbrace{\pi \ldots \pi}_{k-1}(a_1)$$

są wszystkimi elementami zbioru A, więc permutacja π jest cykliczna.

Dla $k < n$ rozważmy zbiór A' złożony ze wszystkich elementów zbioru A różnych od $b_0, b_1, \ldots, b_{k-1}$.

Badaną permutację π można przedstawić w postaci iloczynu permutacji cyklicznej $(b_0, b_1, \ldots, b_{k-1})$ i pewnej permutacji τ zbioru A'. Do permutacji τ możemy zastosować założenie indukcyjne, gdyż liczba elementów zbioru A' jest mniejsza od n. W wyniku otrzymamy rozkład permutacji π na iloczyn cykli. Na mocy zasady indukcji każda permutacja jest cyklem lub iloczynem cykli. ■

Przykłady

1. Rozłożymy na cykle permutację

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 7 & 8 & 5 & 1 & 6 \end{pmatrix}$$

Obrazem elementu 1 jest 4, obrazem 4 jest 7, obrazem 7 jest 1. Otrzymujemy więc cykl (1, 4, 7) i możemy napisać

$$\pi = (1, 4, 7) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 2 & 4 & 8 & 5 & 7 & 6 \end{pmatrix} = (1, 4, 7) \begin{pmatrix} 2 & 3 & 5 & 6 & 8 \\ 3 & 2 & 8 & 5 & 6 \end{pmatrix}$$

Obrazem 2 jest 3, a obrazem 3 jest 2, więc mamy

$$\pi = (1, 4, 7)(2, 3) \begin{pmatrix} 5 & 6 & 8 \\ 8 & 5 & 6 \end{pmatrix} = (1, 4, 7)(2, 3)(5, 8, 6)$$

2. Rozłóżmy na cykle permutację

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 8 & 3 & 6 & 7 & 4 & 5 & 1 \end{pmatrix}$$

Podobnie jak poprzednio znajdujemy, że

$$\pi = (1, 2, 8) \begin{pmatrix} 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 7 & 4 & 5 \end{pmatrix} = (1, 2, 8)\,(4, 6)\,(5, 7)$$

Mnożenie permutacji nie jest przemienne, np. $(1, 2, 3)\,(1, 3, 4) = (2, 3, 4)$, natomiast $(1, 3, 4)\,(1, 2, 3) = (1, 2, 4)$.

Zauważmy jednak, że mnożenie cykli rozłącznych jest przemienne. Wobec tego porządek cykli rozłącznych, na które rozkładamy daną permutację, jest dowolny.

Cykl o długości k jest oczywiście elementem rzędu k w grupie permutacji, iloczyn rozłącznych cykli o długości $k_1, k_2, \ldots, k_m$ jest elementem, którego rząd jest równy najmniejszej wspólnej wielokrotności liczb $k_1, k_2, \ldots, k_m$.

transpozycja

Cykl o długości 2 nazywamy transpozycją. Ponieważ każdy cykl jest iloczynem transpozycji

$$(a_1, a_2, \ldots, a_{k-1}, a_k) = (a_1, a_k)\,(a_1, a_{k-1}) \ldots (a_1, a_3)\,(a_1, a_2)$$

więc każda permutacja jest iloczynem transpozycji. Rozkład na transpozycje nie jest jednoznaczny, np.

$$(1, 2) = (1, 2)\,(1, 2)\,(1, 2)$$

Okazuje się jednak, że jeśli w pewnym rozkładzie danej permutacji występuje parzysta liczba transpozycji, to każdy rozkład tej permutacji na transpozycje zawiera parzystą liczbę czynników. Przypuśćmy bowiem, że pewna permutacja π ma jednocześnie rozkład na parzystą i nieparzystą liczbę transpozycji

$$\pi = \tau_1 \tau_2 \ldots \tau_k = \sigma_1 \sigma_2 \ldots \sigma_m$$

gdzie: k jest liczbą parzystą, m – liczbą nieparzystą, zaś τ_i, σ_j są transpozycjami.

Ponieważ $\sigma_j^{-1} = \sigma_j$, więc mnożąc powyższą równość z prawej strony kolejno przez $\sigma_m, \sigma_{m-1}, \ldots, \sigma_2, \sigma_1$, otrzymamy

$$\tau_1 \tau_2 \ldots \tau_k \sigma_m \sigma_{m-1}, \ldots, \sigma_2 \sigma_1 = e$$

Element jednostkowy grupy permutacji został tu przedstawiony jako iloczyn nieparzystej liczby transpozycji. Ponieważ dla $i \neq j$, $i \neq 1$, $j \neq 1$

$$(a_i, a_j) = (a_1, a_i)\,(a_1, a_j)\,(a_1, a_i)$$

więc poprzednie przedstawienie elementu jednostkowego można zastąpić przez

$$(a_1, a_{i_1})\,(a_1, a_{i_2}) \ldots (a_1, a_{i_t}) = e$$

gdzie liczba t transpozycji jest nieparzysta. Permutacja tożsamościowa przekształca każdy element a_i na ten sam element. Wynika stąd, że w ostatnim przedstawieniu liczba transpozycji (a_1, a_{i_t}) musi być parzysta. Otrzymaliśmy więc sprzeczność.

permutacja parzysta
permutacja nieparzysta

Permutację nazywamy parzystą, jeśli rozkłada się na parzystą liczbę transpozycji. Permutację nazywamy nieparzystą, jeśli jest iloczynem nieparzystej liczby transpozycji (albo jest transpozycją).

A_n jest podgrupą normalną grupy S_n. Dla $n = 1$, $A_1 = S_1$. Natomiast dla $n > 1$ są dwie warstwy lewostronne względem A_n: jedna z nich zawiera wszystkie permutacje parzyste; druga – wszystkie permutacje nieparzyste. Warstwy te są jednocześnie warstwami prawostronnymi.

Permutacje parzyste stanowią podgrupę S_n: iloczyn dwóch permutacji parzystych jest permutacją parzystą, permutacja odwrotna do permutacji parzystej (można ją zapisać jako iloczyn tych samych transpozycji, lecz ustawionych w odwrotnym porządku) jest permutacją parzystą. Podgrupę permutacji parzystych oznaczamy symbolem A_n. Dla $n > 1$ przyporządkowując permutacji parzystej π permutację $(1, 2)\,\pi$, ustalamy odpowiedniość wzajemnie jednoznaczną między zbiorem permutacji parzystych a zbiorem permutacji nieparzystych. Wobec tego liczba permutacji parzystych równa jest liczbie permutacji nieparzystych i wynosi $n!/2$.

21. GRUPY ROZWIĄZALNE

Określiliśmy grupę rozwiązalną jako grupę G, dla której istnieje ciąg podgrup $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$, spełniający dwa warunki dla $i = 1, 2, \ldots, n-1$:

1) G_{i+1} jest podgrupą normalną grupy G_i,

2) grupa ilorazowa G_i/G_{i+1} jest grupą cykliczną.

Okazuje się [1], że otrzymamy równoważną definicję, zastępując warunek 2 następującym warunkiem:

2') grupa ilorazowa G_i/G_{i+1} jest grupą przemienną.

W szczególności każda grupa przemienna jest rozwiązalna, gdyż ciąg $G \supset \{e\}$ spełnia wymagania tej zmodyfikowanej definicji.

Przykłady

1. Grupa permutacji trzech elementów S_3 jest rozwiązalna. Rozpatrzmy bowiem ciąg podgrup $S_3 \supset A_3 \supset \{I\}$, gdzie A_3 jest podgrupą permutacji parzystych. A_3 jest podgrupą indeksu 2, jest więc podgrupą normalną, grupa zaś ilorazowa ma rząd drugi, skąd wynika, że jest cykliczna. Wreszcie grupa A_3 ma rząd trzeci, więc jest cykliczna.

2. Grupa permutacji czterech elementów S_4 jest rozwiązalna. Rozważmy ciąg podgrup $S_4 \supset A_4 \supset V_4 \supset W \supset \{I\}$, gdzie A_4 jest podgrupą permutacji parzystych, $V_4 = \{I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, $W = \{I, (1,2)(3,4)\}$. Ponieważ rzędy kolejnych grup w tym ciągu wynoszą 24, 12, 4, 2, 1, więc oprócz pary $A_4 \supset V_4$, każda para dwóch sąsiednich grup ma tę własność, że mniejsza podgrupa wyznacza dwie warstwy w grupie większej, zatem jest podgrupą normalną, a grupa ilorazowa ma dwa elementy, jest więc grupą cykliczną. Sprawdzenia wymaga jedynie to, czy V_4 jest podgrupą normalną grupy A_4. Jeśli odpowiedź jest pozytywna, to grupa ilorazowa ma trzy elementy, czyli jest cykliczna.

Rozważmy jakąkolwiek permutację parzystą nie należącą do V_4, np. $(1, 2, 3)$. Jest to permutacja parzysta, bo $(1, 2, 3) = (1, 3)(1, 2)$. Wyznaczmy warstwy $(1, 2, 3) \cdot V_4$ oraz $V_4 \cdot (1, 2, 3)$. Ponieważ

$$(1, 2, 3) \cdot I = (1, 2, 3),$$
$$(1, 2, 3)(1, 2)(3, 4) = (1, 3, 4),$$
$$(1, 2, 3)(1, 3)(2, 4) = (2, 4, 3),$$
$$(1, 2, 3)(1, 4)(1, 3) = (1, 4, 2)$$

więc

$$(1, 2, 3) \cdot V_4 = \{(1, 2, 3), (1, 3, 4), (2, 4, 3), (1, 4, 2)\}$$

Natomiast

$$I \cdot (1, 2, 3) = (1, 2, 3),$$
$$(1, 2)(3, 4)(1, 2, 3) = (2, 4, 3),$$
$$(1, 3)(2, 4)(1, 2, 3) = (1, 4, 2),$$
$$(1, 4)(2, 3)(1, 2, 3) = (1, 3, 4)$$

więc

$$V_4 \cdot (1, 2, 3) = \{(1, 2, 3), (2, 4, 3), (1, 4, 2), (1, 3, 4)\}$$

a zatem

$$(1, 2, 3) \cdot V_4 = V_4 \cdot (1, 2, 3)$$

Prócz elementów tej warstwy oraz elementów V_4, pozostały jeszcze cztery permutacje parzyste (wszystkich jest 12), które

Ponieważ każdy automorfizm ciała rozkładu wielomianu f nad ciałem K polega na pewnej permutacji pierwiastków wielomianu f, więc wskazanie grupy nierozwiązalnej wśród grup permutacji (przy jednoczesnym wskazaniu wielomianu, dla którego ta grupa jest grupą Galois ciała rozkładu) da nam przykład wielomianu, którego pierwiastki nie wyrażają się przez pierwiastniki względem ciała K.

wobec tego należą do następnej warstwy lewostronnej, a także prawostronnej. Wynika stąd, że każda warstwa lewostronna jest równa odpowiedniej warstwie prawostronnej, a zatem V_4 jest podgrupą normalną grupy A_4.

Natomiast grupy permutacji większej liczby elementów nie są rozwiązalne. Przedstawimy tu dowód nierozwiązalności grupy S_5, który po niewielkich modyfikacjach obowiązuje dla wszystkich S_n, gdzie $n \geqslant 5$. W tym celu korzystamy z lematu, którego dowód można znaleźć w [1].

Lemat. *Podgrupa grupy rozwiązalnej jest rozwiązalna.*

Z lematu wynika, że gdyby S_5 była grupą rozwiązalną, to jej podgrupa A_5 również byłaby rozwiązalna. Pokażemy, że grupa A_5 nie ma podgrup normalnych różnych od A_5 i podgrupy jednostkowej. Ponieważ A_5 nie jest przemienna, np. $(1,2)(3,4)\cdot(1,2)(3,5) = (3,5,4)$; $(1,2)(3,5)\cdot(1,2)(3,4) = (3,4,5)$, więc wyniknie stąd, że A_5 nie jest rozwiązalne.

Niech więc $H \subset A_5$ będzie podgrupą normalną, $H \neq \{e\}$. Wobec tego do H należy pewien element $a \neq e$. Rozłóżmy element a na cykle rozłączne i rozważmy kolejne przypadki.

1. a jest cyklem o długości 4 lub 5. Zmieniając ewentualnie oznaczenia elementów permutowanych, możemy przyjąć $a = (1,2,3,4)$ lub $a = (1,2,3,4,5)$. Weźmy element $b = (2,3,4) \in A_5$.

Zatem $a^{-1}b^{-1}ab \in H$, gdyż $a^{-1} \in H$, $b^{-1}ab \in H$, przy tym

$$a^{-1}b^{-1}ab = (4,3,2,1)(4,3,2)(1,2,3,4)(2,3,4) = (1,3,4)$$

lub

$$a^{-1}b^{-1}ab = (5,4,3,2,1)(4,3,2)(1,2,3,4,5)(2,3,4) = (1,3,4)$$

Wobec tego w tym przypadku cykl o długości 3 należy do H.

2. W rozkładzie na cykle najdłuższy cykl ma długość 3. Ponieważ cykle są rozłączne, więc mógłby być jeszcze tylko jeden cykl o długości 2, ale wtedy permutacja byłaby nieparzysta, bo cykl o długości 3 jest iloczynem dwóch transpozycji. a jest więc cyklem o długości 3. Zatem i w tym przypadku do H należy cykl o długości 3.

Przyjmijmy więc $a = (1,2,3) \in H$. Biorąc $b = (2,3,4) \in A_5$, otrzymamy znów $a^{-1}b^{-1}ab \in H$

$$a^{-1}b^{-1}ab = (3,2,1)(4,3,2)(1,2,3)(2,3,4) = (1,4)(2,3)$$

Wobec tego iloczyn dwóch rozłącznych transpozycji należy do H.

3. Jeśli w rozkładzie a na cykle rozłączne nie ma cyklu o długości większej lub równej 3, to a jest iloczynem dwóch rozłącznych transpozycji.

Powyższe przypadki wyczerpały wszystkie możliwości i w każdym z nich dochodzimy do wniosku, że H zawiera iloczyn pewnych dwóch rozłącznych transpozycji. Przyjmijmy, że $c = (1,2)(3,4) \in H$. Pokażemy, że iloczyn każdych dwóch transpozycji należy do H.

Jeśli $(r,s)(t,u)$ jest iloczynem rozłącznych transpozycji, to niech b będzie permutacją

$$\begin{pmatrix} r & s & t & u & w \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Jedna z permutacji b, $(1,2)b$ jest parzysta oraz

$$((1,2)b)^{-1}c\,((1,2)b) = b^{-1}cb =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ r & s & t & u & w \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} r & s & t & u & w \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} =$$

$$= (r,s)(t,u)$$

skąd wynika, że $(r,s)(t,u) \in H$. Stwierdziliśmy w ten sposób, że iloczyn dowolnych dwóch rozłącznych transpozycji należy do H.

Zadania

21.1 Wykazać rozwiązalność grupy Galois rozkładu wielomianu $x^4 - 2$.

21.2 Wyjaśnić, dlaczego każde równanie stopnia czwartego można rozwiązać przez pierwiastniki. Pierwiastki jakich stopni należy wyciągać przy rozwiązywaniu równania stopnia czwartego?

Niech wreszcie $(r,s)(r,t)$ będzie iloczynem dwóch nierozłącznych transpozycji. Wśród liczb 1, 2, 3, 4, 5 istnieją liczby u, w, różne od r, s, t. Ponieważ $(r,s)(r,t) = (r,s)(u,w)(u,w)$ więc $(r,s)(r,t)$ należy do H jako iloczyn elementów $(r,s)(u,w)$ (r,t), i $(u,w)(r,t)$. Elementy te będąc iloczynami par rozłącznych transpozycji, należą do H na mocy poprzedniego. Ostatecznie więc iloczyn każdych dwóch transpozycji należy do H, a wobec tego iloczyn każdej parzystej liczby transpozycji, tj. dowolna permutacja parzysta, należy do H. ■

22. RÓWNANIA NIEROZWIĄZALNE PRZEZ PIERWIASTNIKI

Omówimy teraz najprostsze przykłady równań, których pierwiastki nie wyrażają się przez pierwiastniki. Do tego jednak jest nam potrzebna znajomość następujących lematów.

Lemat 1. *Jeśli K jest podciałem ciała liczb rzeczywistych, $f = x^n + a_3 x^{n-3} + \ldots + a_n$ jest wielomianem o współczynnikach z ciała K mającym wszystkie pierwiastki rzeczywiste, to $f = x^n$.*