WIKIPEDIA

Grupa (matematyka)

Grupa – struktura algebraiczna definiowana jako zbiór z określonym na nim łącznym i odwracalnym dwuargumentowym działaniem wewnętrznym[1]; szczególny przypadek monoidu, w którym każdy element ma element odwrotny (zob. *Podobne struktury*). Dział matematyki badający własności grup nazywa się teorią grup.

Spis treści

Motywacja
Definicja
Charakteryzacje
Konwencje zapisu
Właściwości
Przykłady
Pojęcia
Podobne struktury
Zobacz też
Uwagi
Przypisy
Bibliografia
Linki zewnętrzne

Motywacja

Rys historyczny opisujący motywacje twórców teorii wraz zastosowaniami można znaleźć w artykule dotyczącym teorii grup.

W zbiorze liczb całkowitych $\mathbb{Z}$ z ich dodawaniem można wyodrębnić następujące własności:

- $+$ jest działaniem dwuargumentowym określonym na $\mathbb{Z}$, tzn. dla dowolnych $a, b \in \mathbb{Z}$ jest $a + b \in \mathbb{Z}$;
- dla dowolnych $a, b, c \in \mathbb{Z}$ zachodzi $(a + b) + c = a + (b + c)$;
- liczba całkowita $0 \in \mathbb{Z}$ spełnia $a + 0 = a$ dla wszystkich $a \in \mathbb{Z}$;
- dla każdej liczby $a \in \mathbb{Z}$ istnieje przeciwna do niej liczba całkowita $-a$, tzn. taka że $a + (-a) = 0$.

Rozpatrując zbiór $\mathbb{Z}_n$, gdzie n jest liczbą naturalną, z działaniem dodawania modulo n (zob. arytmetyka modularna) okazuje się, że:

- $+$ jest działaniem dwuargumentowym na $\mathbb{Z}_n$, tzn. dla dowolnych $\overline{a}, \overline{b} \in \mathbb{Z}_n$ jest $\overline{a} + \overline{b} \in \mathbb{Z}_n$;
- dla dowolnych $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$ zachodzi $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$;
- liczba całkowita modulo n $\overline{0} \in \mathbb{Z}_n$ spełnia $\overline{a} + \overline{0} = \overline{a}$ dla wszystkich $\overline{a} \in \mathbb{Z}_n$;
- dla każdej liczby całkowitej modulo n $\overline{a} \in \mathbb{Z}_n$ istnieje przeciwna do niej liczba całkowita modulo n $\overline{-a}$, tzn. taka że $\overline{a} + (\overline{-a}) = \overline{0}$.

Niech $\mathbb{R}_+$ oznacza zbiór dodatnich liczb rzeczywistych wraz z działaniem mnożenia, które przejawia własności analogiczne do powyższych:

- $\cdot$ jest działaniem dwuargumentowym na $\mathbb{R}_+$, tzn. dla dowolnych $a, b \in \mathbb{R}_+$ jest $a \cdot b \in \mathbb{R}_+$;
- dla dowolnych $a, b, c \in \mathbb{R}_+$ zachodzi $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- liczba $1 \in \mathbb{R}_+$ ma własność $a \cdot 1 = a$ dla wszystkich $a \in \mathbb{R}_+$;
- dla każdej liczby $a \in \mathbb{R}_+$ istnieje odwrotna do niej dodatnia liczba rzeczywista $1/a$, tzn. taka że $a \cdot \frac{1}{a} = 1$.

Niech X oznacza niepusty zbiór, zaś S_X jest zbiorem wszystkich wzajemnie jednoznacznych przekształceń zbioru X na siebie. Rozważając składanie przekształceń z S_X można zauważyć, że:

- $\circ$ jest działaniem dwuargumentowym na S_X, ponieważ jeśli σ, τ są wzajemnie jednoznacznymi przekształceniami X na siebie, to $\sigma \circ \tau$ również;
- dla dowolnych $\sigma, \tau, \mu \in S_X$ zachodzi $(\sigma \circ \tau) \circ \mu = \sigma \circ (\tau \circ \mu)$;
- przekształcenie tożsamościowe $\iota \in S_X$ spełnia $\sigma \circ \iota = \sigma$ dla wszystkich $\sigma \in S_X$;
- dla każdego $\sigma \in S_X$ istnieje odwrotne do niego przekształcenie $\sigma^{-1} \in S_X$, tzn. takie że $\sigma \circ \sigma^{-1} = \iota$.

Wszystkie powyższe przykłady opisują grupy; w każdym przypadku dany jest niepusty zbiór, na którym określono działanie dwuargumentowe o szczególnych własnościach — tak niżej zostaną zdefiniowane grupy. Dlaczego bada się struktury, które spełniają powyższe/poniższe cztery własności, nie zaś inne; z jakiego powodu wybrano właśnie tę kombinację własności, a nie tylko ich część bądź jakąś dodatkową? Nie ma powodu, by wykluczać te, czy inne możliwości — w istocie rozpatruje się inne teorie i wiele ze wspomnianych kombinacji własności ma swoje nazwy (zob. *Podobne struktury*), jednakże są one dużo mniej ważne niż struktury spełniające wyróżnione cztery własności.

Teoria matematyczna, aby mogła być uznana za ważną, musi być dostatecznie ogólna, a zarazem mieć znaczenie informatywne. Teoria, której postulaty są w wielu przypadkach zbyt ograniczające, okaże się nieistotna w obszarach, w których nie sposób je zapewnić, co ostatecznie przełoży się na ograniczone nią zainteresowanie. Interesujące teorie są ogólne, jednakże ogólność ma cenę: treść. Umożliwiając spełnienie aksjomatów teorii w różnych obszarach i wielu kontekstach, należy zdawać sobie sprawę, że teoria dotyczyć będzie tylko tego, co jest w nich wspólne – może się wtedy okazać, że nie ma takich rzeczy. Istnieje więc niebezpieczeństwo, że teoria będzie się sprowadzać do listy nieciekawych parafraz postulatów pozbawionych głębi. Nakładanie ograniczeń zmniejsza zakres użycia i zainteresowanie teorią, znoszenie ograniczeń prowadzi do pustej teorii. Wyważenie między ogólnością a treścią jest trudnym zagadnieniem, a teoria grup jest jedną z tych, w których udało się osiągnąć równowagę – dzięki temu znajduje ona zastosowanie w matematyce czystej i stosowanej, fizyce teoretycznej oraz innych naukach przyrodniczych (zob. teoria grup). Ponadto pełna jest ona głębokich, interesujących i pięknych wyników. To właśnie wskazuje na to, że wybór czterech własności przedstawionych w definicji można uważać za rozsądny; zastosowania podobnych struktur nie okazały się tak owocne, jak grup.

Definicja

Zbiór G z (dobrze[a]) określonym na nim dwuargumentowym działaniem $\circ$ nazywa się **grupą**, jeżeli ma on następujące własności (spełnia poniższe aksjomaty):

- *Wewnętrzność*: dla dowolnych elementów a, b ze zbioru G ich wynik $a \circ b$ również należy do zbioru G; mówi się wtedy, że zbiór G jest *zamknięty* ze względu na $\circ$.
- *Łączność*: dla wszystkich a, b, c należących do G musi zachodzić $(a \circ b) \circ c = a \circ (b \circ c)$.
- *Element neutralny*: istnieje element e w zbiorze G spełniający dla dowolnego elementu a z tego zbioru warunek $a \circ e = a$.
- *Odwracalność*: dla każdego $a \in G$ musi istnieć $x \in G$, dla których $a \circ x = e$.

Grupa to para uporządkowana $(G, \circ)$, a więc zbiór G, nazywany *nośnikiem*, z działaniem $\circ$. Dlatego grupy $(G, \circ)$ oraz $(H, \star)$ są równe, o ile $G = H$ oraz $\circ = \star$ jako funkcje (relacje) na tym zbiorze; na zbiorze G mogą istnieć dwa różne działania $\circ$ oraz $\star$, ze względu na które G będzie tworzyć grupę, wtedy $(G, \circ)$ oraz $(G, \star)$ są różnymi grupami.

Charakteryzacje

Wprost z definicji można wywieść kilka trywialnych, choć ważnych obserwacji. Warunek łączności oznacza, że kolejność obliczania (nawiasowanie elementów) nie ma wpływu na ostateczny wynik; dzięki napis postaci $a \circ b \circ c$ ma sens i może jednoznacznie wskazywać element $(a \circ b) \circ c = a \circ (b \circ c)$[b]. Postulat istnienia elementu neutralnego oznacza, że nośnik grupy nie może być zbiorem pustym[c].

W definicji nie zapewnia się nic ponad istnienie (co najmniej jednego) *prawostronnego elementu neutralnego*, który służy zagwarantowaniu istnienia (co najmniej jednego) *prawostronnego elementu odwrotnego* do danego[d]. Mimo to wynika z niej[e], że grupa $(G, \circ)$ ma jeden i tylko jeden prawostronny element neutralny, który równocześnie jest jednoznacznie wyznaczonym lewostronnym elementem neutralnym; w związku z tym mówi się po prostu o *elemencie neutralnym* grupy. Podobnie dowolny $a \in G$ ma jednoznacznie wyznaczony prawostronny element odwrotny, który jest jednoznacznie wyznaczonym lewostronnym elementem odwrotnym do a; dlatego nazywa się go *elementem odwrotnym* do a i wprowadza dla niego oznaczenie a^{-1}.

W świetle tych obserwacji przyjmuje się często definicje:

- *Element neutralny**: istnieje jednoznacznie wyznaczony element e w zbiorze G spełniający dla dowolnego elementu a z tego zbioru warunek $a \circ e = e \circ a = a$.
- *Odwracalność**: dla każdego $a \in G$ musi istnieć jednoznacznie wyznaczony $x \in G$, dla których $a \circ x = x \circ a = e$.

Ich przyjęcie zwalnia z dowodzenia wyżej przedstawionych własności, jednak podejście to wymaga sprawdzenia dużo większej liczby warunków zawartych w definicji[f]; uzasadnia to też definiowanie grupy jako uporządkowanej czwórki $(G, \circ, ^{-1}, e)$, której trzeci element oznacza (jednoargumentowe) działanie odwracania, a czwarty – (wyróżniony) element neutralny.

W definicji można zastąpić istnienie prawostronnych elementów neutralnych i odwrotnych na lewostronne nie zmieniając jej sensu; okazuje się jednak, że zmiana musi dotyczyć obu rodzajów elementów jednocześnie: istnienie prawostronnego elementu neutralnego i lewostronnych elementów odwrotnych nie zawsze zapewnia istnienie struktury grupy w zbiorze[h] (por. *Przykłady*), podobnie dotyczy to lewostronnego elementu neutralnego i prawostronnych elementów odwrotnych.

Przytoczona definicja nie jest jedyną, która wprowadza w zbiorze strukturę grupy. Poza istnieniem łącznego działania dwuargumentowego $\circ$ można założyć dla każdego $a \in G$ istnienie elementu $a^{-1} \in G$ spełniającego warunek $a^{-1} \circ (a \circ b) = b = (b \circ a) \circ a^{-1}$ dla dowolnych $a, b \in G$[z]; inną możliwością jest wprowadzenie obok działania $\circ$ dwóch innych działań dwuargumentowych: $a \backslash b$ oraz a/b[i], które dla dowolnych $a, b \in G$ spełniają $a \circ (b \backslash a) = (b/a) \circ a = (a \circ b) \backslash a = (b \circ a)/a = b$[j][3].

Grupę $(G, \circ)$ spełniającą piąty aksjomat:

- *Przemienność*: dla dowolnych elementów a, b zbioru G spełniona jest równość $a \circ b = b \circ a$;

nazywa się *grupą przemienną* (lub *abelową*[k]); powyższy warunek dotyczy ściśle rzecz ujmując działania dwuargumentowego określonego na G, które nazywa się *przemiennym* – grupa przemienna jest więc grupą z działaniem przemiennym[l]. Warunek przemienności jest na tyle silny, iż umożliwił rozwój teorii grup przemiennych w oderwaniu od ogólnej teorii grup jako dość samodzielnego działu matematyki[m].

Konwencje zapisu

Badanie grupy polega na dociekaniu, w jaki sposób $a \circ b$ zależy od elementów a oraz b, nie zaś od nazwy, czy znaku samego działania. Mając to na uwadze przyjęło się pomijać znak działania zastępując go zestawieniem: zamiast $a \circ b$ pisze się ab (czasami $a \cdot b$). Samo działanie nazywa się *mnożeniem*, rozumianym w związku z tym w szerokim sensie. Może ono oznaczać mnożenie liczb, ale też złożenie odwzorowań, branie różnic symetrycznych zbiorów, czy też jakąkolwiek inną bardziej wymyślną definicję (por. *Przykłady*). Mówi się wtedy, że w grupie używa się zapisu *multiplikatywnego* bądź że jest ona *grupą multiplikatywną*. Dlatego też, mówi się też o *iloczynie* ab elementów a oraz b. Ponadto element neutralny oznacza się często cyfrą 1, przy czym nie musi to być liczba 1: może to być odwzorowanie tożsamościowe, zbiór pusty, czy obiekt innego rodzaju. Nie stosuje się jednak zapisu $\frac{1}{a}$ zamiast a^{-1} dla elementu odwrotnego do a. Opisany sposób zapisu będzie wykorzystywany w dalszej części artykułu (zachowane zostanie oznaczenie e dla elementu neutralnego).

Obok zapisu multiplikatywnego stosuje się również zapis *addytywny*, w szczególności, gdy grupa jest przemienna. Działanie oznacza się w nim znakiem „+" i nazywa *dodawaniem*, rozumianym – podobnie jak mnożenie – w szerokim sensie. Element $a + b$ nazywa się *sumą* elementów a oraz b. W *grupie addytywnej* element neutralny oznacza się cyfrą 0, przy czym znowu nie musi on oznaczać liczby 0. Ponadto element odwrotny do a zapisuje się $-a$ i nazywa *elementem przeciwnym* do a.

Zwyczajowo grupą nazywa się nie parę grupa–działanie, a sam nośnik – zbiór G – o ile nie prowadzi to do niejasności: jak wspomniano wcześniej, na zbiorze można często określić wiele grup; w takim przypadku sformułowania „grupa addytywna" i „grupa multiplikatywna" służą wyróżnieniu jednej z nich[n].

Własności

Niech G będzie grupą i $a, b, c \in G$. Wówczas:

- istnieje jeden i tylko jeden $x \in G$, dla którego $ax = b$ oraz jeden i tylko jeden $y \in G$, dla którego $ya = b$[o][p];
- obowiązują *prawa skracania*: jeżeli $ab = ac$, to $b = c$ (skracanie lewostronne) oraz: jeżeli $ba = ca$, to $b = c$ (skracanie prawostronne)[q][r];
- zachodzi $(a^{-1})^{-1} = a$[s][t] oraz $(ab)^{-1} = b^{-1}a^{-1}$[u][v].

W definicji grupy określa się iloczyn dwóch elementów; wcześniej wprowadzony został jednoznaczny iloczyn trzech elementów[w]; podobnie można wprowadzić iloczyn czterech elementów[x]. W celu uproszczenia notacji w podobny sposób wprowadza się ogólny iloczyn n elementów $a_1, \ldots, a_n$ grupy G ($n > 2$) definiowany poprzez $n - 1$-krotny iloczyn dwóch elementów; nawiasy można wstawić na wiele sposobów[y], jednak dzięki łączności wszystkie one dają ten sam wynik[z]: $a_1 \ldots a_n$[aa] równy $a_1(a_2 \ldots a_n) = (a_1a_2)(a_3 \ldots a_n) = \cdots = (a_1 \ldots a_{n-1})a_n$. Jeśli $a_1, \ldots, a_n$ ($n \in \mathbb{N}$) są wszystkie równe $a \in G$, to pisze się a^n; w szczególności $a^1 = a$, a przy tym $a^n = a^{n-1}a = aa^{n-1}$. Tę obserwację można wyrazić więc w postaci $a^m a^n = a^{m+n}$ (dla $a \in G$ i $m, n \in \mathbb{N}$); ponadto $(a^m)^n = a^{mn}$ ($a \in G$; $m, n \in \mathbb{N}$)[ab].

Własności te rozszerza się na wykładniki całkowite; przyjmuje się, że $a^0 = e$ (element neutralny) oraz $a^{-m} = (a^m)^{-1}$ (element odwrotny do a^m) dla $a \in G$ oraz $m \in \mathbb{N}$. Ze względu na to, dla wszystkich $a \in G$ oraz $m, n \in \mathbb{Z}$:

- zachodzi równość $a^m a^n = a^{m+n}$[ac],
- prawdą jest $(a^{-1})^m = a^{-m}$[ad],
- obowiązuje tożsamość $(a^m)^n = a^{mn}$[ae].

Dodatkowo dla $a_1, a_2, \ldots, a_n \in G$ zachodzi $(a_1a_2 \ldots a_n)^{-1} = a_n^{-1} \ldots a_2^{-1}a_1^{-1}$[af]; obserwacja ta dowodzi też $(a^{-1})^m = (a^m)^{-1}$. Jeżeli $a, b \in G$ są elementami, dla których $ab = ba$, to $ab^n = b^n a$[ag], a stąd $a^m b^n = b^n a^m$[ah] dla wszystkich $m, n \in \mathbb{Z}$[ai]. Jeśli $a^2 = e$ dla dowolnego $a \in G$, to grupa G jest przemienna[ai].

W przypadku grup addytywnych zamiast a^n pisze się na dla $n \in \mathbb{N}$ i definiuje $0a = e$ oraz $(-m)a = -(ma)$ dla $m \in \mathbb{Z}$. Określa to na dla $a \in G$ oraz $n \in \mathbb{Z}$. Poprzednie obserwacje zapisuje się wtedy odpowiednio: $ma + na = (m + n)a$. $(-m)a = m(-a)$ oraz $n(ma) = (nm)a$, ponadto $n(a + b) = na + nb$ ($a, b \in G$, $m, n \in \mathbb{Z}$; w ostatniej tożsamości istotne jest założenie przemienności grupy).

Przykłady

1. Niech dla dowolnych elementów (a, b) oraz (c, d) zbioru $\mathbb{Z} \times \mathbb{Z}$ będzie $(a, b) \diamondsuit (c, d) = (a, b + d)$; czy $(\mathbb{Z} \times \mathbb{Z}, \diamondsuit)$ jest grupą?

   - Wewnętrzność: $\diamondsuit$ jest działaniem wewnętrznym w $\mathbb{Z}$, ponieważ $a \in \mathbb{Z}$ i $b + d \in \mathbb{Z}$, o ile $a, b, c, d \in \mathbb{Z}$, tzn. $\mathbb{Z} \times \mathbb{Z}$ jest zamknięty ze względu na $\diamondsuit$.
   - Łączność: czy dla dowolnych (a, b), (c, d), $(g, h) \in \mathbb{Z} \times \mathbb{Z}$ zachodzi $[(a, b) \diamondsuit (c, d)] \diamondsuit (g, h) = (a, b) \diamondsuit [(c, d) \diamondsuit (g, h)]$? Ponieważ $(a, b + d) \diamondsuit (g, h) = (a, b) \diamondsuit (c, d + h)$, czyli $(a, (b + d) + h) = (a, b + (d + h))$, to działanie $\diamondsuit$ jest łączne, gdyż działanie $+$ jest łączne w $\mathbb{Z}$.
   - Element neutralny: czy istnieje w $\mathbb{Z} \times \mathbb{Z}$ element, niech to będzie (a_0, b_0), dla którego $(a, b) \diamondsuit (a_0, b_0) = (a, b)$ dla wszystkich $(a, b) \in \mathbb{Z} \times \mathbb{Z}$? Jest to prawdą, o ile $(a, b + b_0) = (a, b)$, co jest równoważne $b_0 = 0$; przy tym brak jakiegokolwiek warunku na a_0. Przykładowo $(0, 0)$ oraz $(1, 0)$ są prawostronnymi elementami neutralnymi[ak]; w rzeczywistości dowolny element $(n, 0) \in \mathbb{Z} \times \mathbb{Z}$ jest prawostronnym elementem neutralnym.

     Ponieważ grupa ma jeden i tylko jeden prawostronny element neutralny[al], to $\mathbb{Z} \times \mathbb{Z}$ nie jest grupą ze względu na $\diamondsuit$. Z drugiej strony, przykładowo względem $(0, 0)$ (w zasadzie względem dowolnego prawostronnego elementu neutralnego), każdy element $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ ma lewostronny element odwrotny $(0, -b)$: $(0, -b) \diamondsuit (a, b) = (0, -b + b) = (0, 0)$ (względem $(n, 0)$ lewostronnym elementem

2. Dla dowolnych dwóch elementów $a, b \in \mathbb{Q} \setminus \{1\}$ niech $a \circ b = ab - a - b + 2$; czy $\mathbb{Q} \setminus \{1\}$ jest grupą ze względu na $\circ$?

   - Wewnętrzność: sprawdzenie, że dla dowolnych $a, b \in \mathbb{Q} \setminus \{1\}$ zachodzi $a \circ b = ab - a - b + 2 \in \mathbb{Q}$ nie wystarcza — należy również wykazać, że $a \circ b \neq 1$. Niech $a, b \in \mathbb{Q}$, $a \neq 1 \neq b$; zakładając $a \circ b = 1$ wykazana zostanie sprzeczność. Otóż jeśli $a \circ b = 1$, to $ab - a - b + 2 = 1$, czyli $ab - a - b + 1 = 0$, a więc $(a - 1)(b - 1) = 0$, co oznacza, że $a = 1$ lub $b = 1$, sprzeczność. Zatem $a \circ b \in \mathbb{Q} \setminus \{1\}$, czyli $\circ$ jest działaniem wewnętrznym w $\mathbb{Q} \setminus \{1\}$.
   - Łączność: czy dla dowolnych $a, b, c \in \mathbb{Q} \setminus \{1\}$ jest $(a \circ b) \circ c = a \circ (b \circ c)$? Rozpisując obie strony równania otrzymuje się kolejno: $(ab - a - b + 2) \circ c = a \circ (bc - b - c + 2)$, następnie
     $(ab - a - b + 2)c - (ab - a - b + 2) - c + 2 = a(bc - b - c + 2) - a - (bc - b - c + 2) + 2$
     oraz
     $abc - ac - bc + 2c - ab + a + b - 2 - c + 2 = abc - ab - ac + 2a - a - bc + b + c - 2 + 2$,
     co oznacza, że $\circ$ jest łączne.
   - Element neutralny: szukany jest element $e \in \mathbb{Q} \setminus \{1\}$, który dla dowolnego $a \in \mathbb{Q} \setminus \{1\}$ spełnia

odwrotnym do (a, b) jest $(n, -b)$).

W ten sposób $(\mathbb{Z} \times \mathbb{Z}, \diamond)$ jest strukturą, w której istnieje prawostronny element neutralny oraz lewostronne elementy odwrotne względem każdego elementu, mimo to nie jest grupą (zob. *Charakteryzacje*).

3. Czy definiując na $\mathbb{Z}$ działanie $*$ dane wzorem $a * b = a + b + 2$ dla wszystkich $a, b \in \mathbb{Z}$ otrzymuje się grupę $(\mathbb{Z}, *)$?

- Wewnętrzność: dla dowolnych $a, b \in \mathbb{Z}$ element $a * b = a + b + 2$ jest liczbą całkowitą, zatem $\mathbb{Z}$ jest zamknięty ze względu na $*$.
- Łączność: dla wszystkich $a, b, c \in \mathbb{Z}$ ma być spełnione $(a * b) * c = a * (b * c)$; istotnie $(a * b) * c = (a + b + 2) * c = (a + b + 2) + c + 2 = a + (b + 2 + c) + 2 = a + (b + c + 2) + 2 = a + (b * c) + 2 = a * (b * c)$, czyli $*$ jest łączne.
- Element neutralny: czy istnieje $e \in \mathbb{Z}$, dla której $a * e = a$ dla każdego $a \in \mathbb{Z}$? Równość daje $a + e + 2 = a$, czyli $e = -2$. Liczba -2 istotnie jest prawostronnym elementem neutralnym, gdyż $a * -2 = a + (-2) + 2 = a$ dla każdego $a \in \mathbb{Z}$.
- Element odwrotny: czy liczba całkowita a ma prawostronny element odwrotny w $\mathbb{Z}$? Warunek $a * x = -2$ daje $a + x + 2 = -2$, tj. $x = -4 - a \in \mathbb{Z}$. Liczba $-4 - a$ rzeczywiście jest prawostronnym elementem odwrotnym do a, ponieważ $a * (-4 - a) = a + (-4 - a) + 2 = -2$.

W rzeczy samej, zbiór $\mathbb{Z}$ jest grupą względem działania $*$.

$a \circ e = a$. Zakładając, że taki element e istnieje, otrzymuje się $ae - a - e + 2 = a$, skąd $ae - e = 2a - 2$, czyli $(a - 1)e = 2(a - 1)$, a więc $e = 2$ (ponieważ $a - 1 \neq 0$). Nie dowodzi to jeszcze, że $2 \in \mathbb{Q} \setminus \{1\}$ jest prawostronnym elementem neutralnym; poprzednie rozumowanie przekonuje jedynie, że prawostronny element neutralny, o ile istnieje, musi być równy 2. Aby przekonać się, że 2 istotnie jest prawostronnym elementem neutralnym należy zauważyć, że $a \circ 2 = a2 - a - 2 + 2 = 2a - a = a$ dla każdego $a \in \mathbb{Q} \setminus \{1\}$; ponieważ $2 \in \mathbb{Q} \setminus \{1\}$, to istotnie jest to prawostronny element neutralny w $\mathbb{Q} \setminus \{1\}$.

- Element odwrotny: dla każdego $a \in \mathbb{Q} \setminus \{1\}$ należy znaleźć $x \in \mathbb{Q} \setminus \{1\}$ spełniający $a \circ x = 2$; daje to $ax - a - x + 2 = 2$, czyli $ax - a - x + 1 = 1$, tj. $(a - 1)(x - 1) = 1$, skąd $x - 1 = 1/(a - 1)$, tzn. $x = a/(a - 1)$, co ma sens, gdyż $a - 1 \neq 0$. Nie oznacza to, że $a/(a - 1)$ jest prawostronnym elementem odwrotnym do $a \in \mathbb{Q} \setminus \{1\}$, a jedynie to, że o ile taki element istnieje, musi mieć podaną wartość. Dlatego należy wykazać, że $a \circ a/(a - 1) = 2$ dla każdego $a \in \mathbb{Q} \setminus \{1\}$ oraz że $a/(a - 1) \in \mathbb{Q} \setminus \{1\}$. Otóż $a \circ a/(a - 1) = a(a/(a - 1)) - a - (a/(a - 1)) + 2 = (a - 1)(a/(a - 1)) - a + 2 = 2$, a ponadto $a \circ a/(a - 1) \neq 1$, gdyż $a/(a - 1) \in \mathbb{Q}$ oraz $a/(a - 1) = 1$ oznaczałyby, że $a = a - 1$, czyli $0 = 1$, dawałoby sprzeczność.

Ponieważ spełnione są wszystkie aksjomaty grupy, to $\mathbb{Q} \setminus \{1\}$ tworzy grupę z określonym wyżej działaniem $\circ$.

4. Niech A oznacza niepusty zbiór, a $\mathcal{P}(A)$ oznacza zbiór wszystkich podzbiorów A. Zbiór $\mathcal{P}(A)$ tworzy grupę z działaniem różnicy symetrycznej $\triangle$, ponieważ spełnione są aksjomaty grupy:

- Wewnętrzność: dla dowolnych $S, T \in \mathcal{P}(A)$ zbiór $S \triangle T$ jest podzbiorem A, czyli $S \triangle T \in \mathcal{P}(A)$, a więc $\mathcal{P}(A)$ jest zamknięty ze względu na $\triangle$.
- Łączność: $\triangle$ jest łączne.
- Element neutralny: podzbiór pusty $\varnothing$ jest prawostronnym elementem neutralnym.
- Element odwrotny: każdy element ma $S \in \mathcal{P}(A)$ ma prawostronny element odwrotny, mianowicie samego siebie, ponieważ $S \triangle S = \varnothing$ dla dowolnego $S \in \mathcal{P}(A)$.

Najprostszą, a zarazem najmniejszą grupą jest grupa trywialna złożona z jednego elementu[am]. Dalsze przykłady obejmują *grupę przekształceń* ustalonego zbioru (ostatni przykład w *Motywacja*); *grupę euklidesową*, czyli grupę izometrii ustalonej przestrzeni euklidesowej; *grupę symetrii* danej figury przestrzeni euklidesowej, czyli grupę izometrii własnych tej figury (tzn. izometrii odwzorowujących figurę na siebie); *grupę diedralną*, tzn. grupę symetrii wybranego wielokąta foremnego[an] (wszystkie z działaniem składania przekształceń). Ze względu na możliwość reprezentacji elementów grupy jako macierzy, ważnym przykładem są różnorodne *grupy macierzy* (odwracalnych z działaniem ich mnożenia, np. wygodna reprezentacja macierzowa *grupy kwaternionów*).

Pojęcia

Struktura

Wśród podanych wyżej przykładów grup niektóre z nich mają nośnik będący zbiorem skończonym, inne – zbiorem nieskończonym. Liczbę elementów grupy G, a dokładniej jego moc zbioru G, nazywa się *rzędem* tej grupy i oznacza symbolem $|G|$. Jeżeli $|G|$ jest skończony, to grupę G również nazywa się *skończoną*, jeśli $|G|$ jest nieskończony, to mówi się, że grupa G jest *nieskończoną*[4]. Niekiedy rozróżnia się różne rodzaje nieskończoności, ale często przyjmuje się, że jeśli rząd grupy G jest nieskończony, to pisze się $|G| = \infty$, gdzie symbol ∞ reprezentuje wszystkie typy nieskończoności.

Grupa jako zbiór (z określonym na nim działaniem dwuargumentowym spełniającym pewne własności) ma podzbiory; spośród wszystkich podzbiorów bardziej interesujące są te podzbiory, które odzwierciedlają strukturę algebraiczną grupy, gdyż pomagają zrozumieć jej budowę. Wyróżnione miejsce zajmują pośród nich te, które same są grupami (ze względu na to samo działanie): nazywa się je *podgrupami* danej grupy. Wśród innych podzbiorów grupy istotne miejsce zajmują *warstwy* względem określonej podgrupy, które stanowią rozbicie nośnika na rozłączne podzbiory; liczbę warstw względem wybranej podgrupy nazywa się *indeksem* tej podgrupy w grupie (podobnie jak w przypadku rzędu można rozróżniać rodzaje nieskończoności, jednak częstokroć się tego nie czyni). Ponieważ warstwy danej grupy względem jej ustalonej podgrupy są równoliczne, to rząd grupy jest równy iloczynowi rzędu podgrupy oraz indeksu podgrupy w grupie; w szczególności jeśli grupa jest skończona, to rząd podgrupy jest dzielnikiem rzędu grupy — ta ważna obserwacja nazywana jest twierdzeniem Lagrange'a.

Dla grupy G oraz $a \in G$ zbiór $\langle a \rangle = \{a^n \in G : n \in \mathbb{Z}\}$ wszystkich potęg całkowitych elementu a jest niepusty, a ponadto tworzy podgrupę w G[ao] – nazywa się go *podgrupą cykliczną* grupy G *generowaną przez element* a. Gdy $\langle a \rangle = G$, to G nazywa się *grupą cykliczną*, a element a nazywa się *generatorem* tej grupy. Rząd $|\langle a \rangle|$ tej podgrupy nazywa się *rzędem* elementu a i oznacza $\mathrm{ord}(a)$ (jak wyżej, zwykło się przyjmować, że wartość ta jest liczbą naturalną albo nieskończonością). Jeżeli G jest skończona, to każdy element $a \in G$ ma skończony rząd, a dokładnie $\mathrm{ord}(a) \mid |G|$ na mocy twierdzenia Lagrange'a; w grupach nieskończonych mogą istnieć tak elementy rzędu skończonego, jak i nieskończonego. Definicję generowania podgrupy przez element rozszerza się na zbiory elementów: jeżeli $X \subseteq G$, to $\langle X \rangle = \{x_1^{m_1} \ldots x_k^{m_k} \in G : k \in \mathbb{N},\ x_i \in X,\ m_i \in \mathbb{Z} \text{ dla } i = 1, \ldots, k\}$ nazywa się *podgrupą generowaną* przez X i składa się ze wszystkich skończonych iloczynów elementów w X oraz ich odwrotności (przyjmuje się, że $\langle \varnothing \rangle$ jest trywialna; ponadto $\langle \{a\} \rangle = \langle a \rangle$, a $\langle \{x_1, \ldots, x_n\} \rangle$ oznacza się $\langle x_1, \ldots, x_n \rangle$); jeżeli $X \subseteq G$ oraz $\langle X \rangle = G$, to X nazywa się *zbiorem generatorów* grupy G, a o grupie G mówi się, że jest *generowana* przez X; jeśli grupa G ma skończony zbiór generatorów, to nazywa się ją *skończenie generowaną*.

Przekształcenia

Zbiór warstw względem podgrupy szczególnego rodzaju, tzw. *podgrupy normalnej*, można wyposażyć w naturalnie określone działanie, względem którego będzie on tworzyć grupę nazywaną *grupą ilorazową* (danej grupy przez wspomnianą podgrupę normalną). Oprócz tego, że mogą one służyć do tworzenia kolejnych, mniejszych grup (zachowując przy tym własności grupy wyjściowej, np. przemienność, czy cykliczność)[ap] umożliwiają one wniknięcie w budowę grupy za pomocą *homomorfizmów grup*, tzn. przekształceń zachowujących strukturę algebraiczną grup; centralną rolę pełni tu twierdzenie o izomorfizmie (wraz z nieco ogólniejszym twierdzeniem o homomorfizmie). Podgrupy mogą być wkomponowane w grupę we względnie prosty bądź w dość złożony sposób, przedstawiając grupę w postaci iloczynów jej podgrup: ogólnego, półprostego, czy prostego (można je opisać za pomocą tzw. *iloczynu kompleksowego*). Ogólnie wszystkie wspomniane pojęcia, przede wszystkim grupy ilorazowe i podgrupy, można wykorzystać do opisu grupy za pomocą jej *prezentacji*: dowolna grupa jest ilorazem *grupy wolnej* nad zbiorem generatorów danej grupy przez podgrupę relacji spełnianych w tej grupie[aq].

Automorfizmy grupy to przekształcenia, które można uważać za uogólnienie izometrii własnych figur geometrycznych (por. *Przykłady*). Podgrupy normalne to podgrupy, które „wyglądają tak samo niezależnie od sposobu patrzenia"; formalizację tej intuicji umożliwia relacja sprzężenia elementów (elementy sprzężone mają te same własności, np. ten sam rząd) oraz klasa automorfizmów nazywanych *wewnętrznymi* (wyznaczanych przez sprzężenia). W ogólności *podgrupy sprzężone* (jedna z drugą) należy rozumieć jako podgrupy, które „wyglądają tak samo zmieniwszy sposób patrzenia" (z tego powodu podgrupy normalne nazywa się czasem „samosprzężonymi"); formalnie dwie podgrupy są sprzężone, gdy jedna jest obrazem drugiej w pewnym automorfizmie wewnętrznym. Automorfizmy grupy G tworzą grupę $\mathrm{Aut}(G)$ ze względu na składanie przekształceń, a automorfizmy wewnętrzne grupy G tworzą podgrupę (normalną) $\mathrm{Inn}(G)$ we wspomnianej grupie automorfizmów.

Centrum grupy G to podgrupa (normalna) $\mathrm{Z}(G)$ elementów przemiennych z dowolnym elementem grupy G, jej rozmiar mówi więc o stopniu przemienności grupy; związek między centrum a automorfizmami wewnętrznymi ustala grupa ilorazowa G przez $\mathrm{Z}(G)$, która ma tę samą strukturę, co grupa $\mathrm{Inn}(G)$. Innym pojęciem służącym określeniu stopnia przemienności, czy też raczej nieprzemienności, grupy jest *komutator* dwóch elementów; podgrupa generowana przez wszystkie komutatory, nazywana *pochodną* grupy (lub jej *komutantem*), jest trywialna, gdy grupa jest przemienna. Podgrupa ta umożliwia wskazanie przemiennych grup ilorazowych: są nimi te grupy ilorazowe, których pochodna zawiera się w podgrupie normalnej będącej dzielnikiem; pozostałe grupy ilorazowe są nieprzemienne. *Podgrupa charakterystyczna* (będąca przypadkiem szczególnym podgrupy normalnej) to podgrupa, która „wygląda symetrycznie" (strukturę pierwszych zachowują wszystkie automorfizmy grupy, podczas gdy drugich jedynie część z nich – tylko wewnętrzne). Przykładami są m.in. wspomniane centrum, czy pochodna grupy[ar].

Działanie

W sekcji *Przykłady* zasygnalizowano istnienie grup funkcji, np. grupy przekształceń $\mathfrak{S}_X$ danego zbioru X, grupy izometrii przestrzeni euklidesowej, wyżej wspomniano również o grupie $\mathrm{Aut}(G)$ funkcji zachowujących mnożenie w G. Ogólnie, jeśli X jest zbiorem z określoną na nim pewną strukturą (algebraiczną, geometryczną, analityczną, topologiczną, czy inną), odwzorowania określone na X, które zachowują tę strukturę, tworzą grupę. *Działanie grupy na zbiorze* pozwala na uchwycenie funkcyjnego charakteru elementów grupy, który mogą one przejawiać; o elementach grupy G można myśleć właśnie jako o funkcjach określonych na zbiorze X. W gruncie rzeczy dowolne działanie grupy na zbiorze X można rozumieć jako homomorfizm grupy G w grupę $\mathfrak{S}_X$ (tzw. *reprezentacja permutacyjna* grupy G). Wykorzystując pojęcie działania grupy na zbiorze można w czytelny sposób uzasadnić twierdzenie Cayleya: grupa G ma tę samą strukturę, co pewna podgrupa przekształceń (wzajemnie jednoznacznych) zbioru G. Wiele informacji o grupie można pozyskać rozważając działanie grupy G na zbiorze G poprzez sprzężenia (zob. *klasa sprzężoności*).

Rozkłady

Proste odwrócenie twierdzenia Lagrange'a jest fałszywe: jeśli k jest dzielnikiem rzędu $|G|$ grupy skończonej G, to G nie musi mieć podgrupy rzędu k; nałożenie dodatkowego warunku na k, by było potęgą liczby pierwszej (grupy o rzędzie wyrażającym się potęgą liczby pierwszej to tzw. *grupy pierwsze*) i było względnie pierwsze z $|G|/k$ sprawia, że teza twierdzenia staje się prawdziwa – jest to pierwsze z trzech twierdzeń Sylowa. Wspomniana podgrupa (pierwsza) rzędu k nazywana jest *podgrupą Sylowa*[as]; drugie twierdzenie Sylowa mówi, że podgrupy Sylowa są sprzężone; trzecie opisuje liczbę możliwych podgrup Sylowa.

Grupy zawierające podgrupy normalne można rozłożyć na iloraz oraz wspomnianą podgrupę normalną[at]. Nietrywialną grupę nazywa się *prostą*, jeżeli nie ma ona nietrywialnych, właściwych podgrup normalnych – definicja ta przywodzi na myśl liczby pierwsze: podobnie jak liczby pierwsze są „budulcem" liczb całkowitych, tak grupy proste są „budulcem" pewnego rodzaju grup; analogii tej nie należy jednak posuwać zbyt daleko, gdyż różne grupy mogą składać się z tych samych elementów składowych – problem konstrukcji grupy znany jako *problem rozszerzenia* nadal oczekuje na rozwiązanie. Proste grupy przemienne to dokładnie grupy cykliczne o rzędzie będącym liczbą pierwszą (zob. klasyfikacja skończonych grup przemiennych); innym przykładem są grupy alternujące (grupa permutacji parzystych z działaniem ich składania) stopnia piątego i wyższych.

Jeżeli H jest podgrupą w G, to skończony ciąg podgrup w G (zawierający H oraz G) nazywa się *ciągiem* (*podnormalnym*) od H do G, gdy każda podgrupa ciągu jest podgrupą normalną kolejnej. Elementy ciągu nazywa się jego *wyrazami*, a grupy ilorazowe kolejnych wyrazów – jego *ilorazami* (lub *faktorami*); ciąg od podgrupy trywialnej do G nazywa się krótko ciągiem G. Jeśli każdy wyraz ciągu jest normalny/charakterystyczny w G, to cały ciąg nazywa się *normalnym/charakterystycznym*; gdy ciąg nie zawiera powtórzeń (zawieranie właściwe podgrup), to ciąg nazywa się *właściwym*. Ciąg (2) od H do G nazywa się *zagęszczeniem* ciągu (1) od H do G, jeżeli każdy wyraz (1) jest również wyrazem (2); zagęszczenie ciągu (1) można więc uzyskać poprzez wstawienie dodatkowych grup – niekoniecznie różnych od wyrazów ciągu (1) – między kolejne wyrazy ciągu (1). Gdy jednak (2) jest zagęszczeniem (1) i co najmniej jeden wyraz (2) nie był wyrazem (1), to (2) nazywa się *zagęszczeniem właściwym* (1). Ciąg G nazywa się *ciągiem kompozycyjnym*, jeśli jest ciągiem właściwym G i nie ma zagęszczenia właściwego (ilorazy ciągu kompozycyjnego to *ilorazy kompozycyjne*); ciąg kompozycyjny grupy G można scharakteryzować jako ciąg G, w którym wszystkie ilorazy są proste. Dwa ciągi grupy G są *równoważne*, gdy mają tę samą liczbę wyrazów i ilorazy pierwszego ciągu mają, w pewnym porządku, tę samą strukturę co ilorazy drugiego ciągu (a więc niekoniecznie odpowiadające sobie wyrazy ciągów). Twierdzenie Jordana–Höldera mówi, że dowolne dwa ciągi kompozycyjne danej grupy są równoważne (o ile tylko grupa ma ciąg kompozycyjny[au]); w istocie prawdziwe jest dużo mocniejsze twierdzenie Schreiera, które zapewnia, że dowolne dwa ciągi grupy mają równoważne zagęszczenia (wniosek: każdy ciąg właściwy grupy ma zagęszczenie będące ciągiem kompozycyjnym)[av]. Przytoczone wyniki są elementem szerszej klasyfikacji skończonych grup prostych[aw].

Ciąg od H do G nazywa się *abelowym*, gdy wszystkie ilorazy są abelowe (przemienne). Grupę nazywa się *rozwiązalną*, jeśli ma ciąg abelowy[k]. Każda grupa przemienna jest rozwiązalna, choć istnieją rozwiązalne grupy nieprzemienne; ponadto podgrupy i grupy ilorazowe grup rozwiązalnych również są rozwiązalne, z drugiej strony jeśli rozwiązalna jest podgrupa normalna i iloraz grupy przez nią, to rozwiązalna jest i sama grupa. Przykładami grup nierozwiązalnych są znowu grupy alternujące stopnia piątego i wyższych, rozwiązalne są z kolei skończone grupy przemienne. Ogólniej: ponieważ rozwiązalne grupy proste to grupy cykliczne rzędu będącego liczbą pierwszą, to skończone grupy rozwiązalne to grupy, w których każdy iloraz kompozycyjny ma rząd wyrażający się liczbą pierwszą. Wynika stąd, że grupy permutacji stopnia piątego i wyższych również są nierozwiązalne. Obserwacja ta pełni kluczową rolę w dowodzie tego, że równanie wielomianowe stopnia większego niż cztery nie może być rozwiązane za pomocą pierwiastników (tzn. czterech działań arytmetycznych i pierwiastkowania, tj. potęg i pierwiastków o wykładniku/stopniu naturalnym) – jest to tzw. twierdzenie Abela–Ruffiniego.

Zbiór elementów skończonego rzędu grupy przemiennej G tworzy podgrupę nazywaną *podgrupą torsyjną* $\mathrm{T}(G)$, iloraz G przez $\mathrm{T}(G)$ poza elementem neutralnym zawiera wyłącznie elementy nieskończonego rzędu. Ogólnie dowolną grupę G nazywa się *torsyjną*, o ile tylko zawiera wyłącznie elementy skończonego rzędu; grupę, w której każdy element poza neutralnym ma rząd nieskończony nazywa się *beztorsyjną* (w ten sposób jedyną grupą jednocześnie torsyjną i beztorsyjną jest grupa trywialna; każda grupa skończona jest torsyjna, choć torsyjna jest również nieskończona grupa ilorazowa $\mathbb{Q}$ przez $\mathbb{Z}$; grupy, które nie są ani torsyjne, ani beztorsyjne nazywa się *mieszanymi*). Twierdzenie klasyfikacyjne są w matematyce bardzo pożądane, lecz niezmiernie rzadkie: nie mniej istnieje wyczerpująca klasyfikacja skończenie generowanych grup przemiennych (twierdzenie Frobeniusa–Stickelbergera). Wystarczy więc zbadać dwie klasy grup przemiennych: torsyjne i beztorsyjne, a następnie znaleźć sposób na skonstruowanie z nich grupy przemiennej. Nie obędzie się jednak bez dodatkowych warunków nałożonych na G: jeśli przyjąć, że G jest skończenie generowana, to $\mathrm{T}(G)$ jest skończona. Wtedy badanie skończonych grup przemiennych sprowadza się do badania skończonych, przemiennych grup pierwszych[ax] oraz beztorsyjnych grup przemiennych – wykorzystuje się do tego pojęcia *niezależności*, *bazy* (niezależnego zbioru generującego grupę, o ile nie zawiera on elementu neutralnego) oraz *rangi grupy* (jednoznacznie wyznaczonej liczby elementów w bazie)[ay]. Złączenie części torsyjnej i beztorsyjnej przebiega w najprostszy możliwy sposób: poprzez iloczyn prosty – struktura skończenie generowanej grupy przemiennej G wyznaczona jest w zupełności przez zbiór liczb całkowitych w jednoznaczny sposób.

Podobne struktury

Niech G będzie dowolnym zbiorem z określonym na nim działaniem dwuargumentowym $\star$. Istnieje szereg podobnych struktur mających osobne nazwy, które spełniają aksjomaty podobne do aksjomatów grupy; struktura $(G, \star)$ jest:

- grupoidem bez dodatkowych założeń,
- półgrupą, gdy działanie $\star$ jest łączne,
- monoidem, gdy działanie $\star$ półgrupy ma element neutralny[az],
- quasi-grupą, gdy dla każdego elementu istnieje element do niego odwrotny względem $\star$,
- pętlą (lupą), gdy działanie $\star$ w quasi-grupie ma element neutralny.
- grupą przemienną (abelową), gdy działanie $\star$ w grupie jest przemienne.

Struktury grupopodobne

	Wewnętrzność	Łączność	E. neutralny	Odwrotność	Przemienność
Grupoid	✓	…	…	…	…
Półgrupa	✓	✓	…	…	…
Monoid	✓	✓	✓	…	…
Grupa	✓	✓	✓	✓	…
~ przemienna	✓	✓	✓	✓	✓
Pętla	✓	…	✓	✓	…
Quasi-grupa	✓	…	…	✓	…

✓ — warunek wymagany; … — warunek niekonieczny

Zobacz też

- pierścień, ciało
- teoria Galois (grupa Galois)
- algebra Liego (grupa Liego)
- grupa topologiczna

Uwagi

a. Sformułowanie „dobrze określone" oznacza, że działanie jest funkcyjne, tzn. dowolnym dwóm elementom przypisuje jednoznacznie trzeci element. Mogłoby się wydawać, że wymaganie to jest oczywiste, jednak możliwe jest podanie nie budzącego początkowo zastrzeżeń przykładu, w którym przypisywany element zależy nie od samych elementów, ale od sposobu ich identyfikacji („nazw"); zasadniczo sytuacja ta pojawia się zwykle w wyniku utożsamiania ze sobą elementów (zob. relacja równoważności, grupa ilorazowa, warstwa – *Przykłady*).

b. Przyjęcie takiej umowy byłoby błędem, gdyby działanie nie było łączne. Przykładowo dzielenie $:$ nie jest działaniem łącznym na $\mathbb{Q} \setminus \{0\}$, poza przypadkiem $c = 1$ (tutaj $a, b, c \in \mathbb{Q} \setminus \{0\}$): wyrażenie $a : b : c$ jest niejednoznaczne.

c. *De facto* najmniejszymi grupami w sensie liczby elementów są grupy jednoelementowe (zob. *Przykłady*).

d. Definicja nie mówi zatem, że istnieje tylko jeden element będący prawostronnym elementem neutralnym (choć faktycznie tak jest, zob. dalej). Co więcej w definicji nie wspomina się o *lewostronnych elementach neutralnych*, ich istnieniu, czy związkach między nimi. Podobnie definicja nie wyklucza istnienia wielu prawostronnych elementów neutralnych o tej własności, przy czym część z nich może ją mieć, a część nie. Ponadto część (lub wszystkie) elementy mogą mieć więcej niż jedną odwrotność względem części (lub wszystkich) prawostronnych elementów neutralnych.

e. **Lemat**
Z definicji grupy wynika, że:
1. element e jest jedynym elementem idempotentnym w G;
2. e jest jednoznacznie wyznaczonym prawostronnym elementem neutralnym w G;
3. prawostronny element odwrotny elementu z G jest również lewostronnym elementem odwrotnym tego samego elementu;
4. e jest lewostronnym elementem neutralnym w G;
5. e jest jednoznacznie wyznaczonym lewostronnym elementem neutralnym w G;
6. każdy element ma jednoznacznie wyznaczony prawostronny element odwrotny w G;

7. każdy element ma jednoznacznie wyznaczony lewostronny element odwrotny w G;
8. jednoznacznie wyznaczony prawostronny element odwrotny dowolnego elementu $a \in G$ jest równy jednoznacznie wyznaczonemu lewostronnemu elementowi odwrotnemu elementu a.

Dowód

1. Należy dowieść, że jeśli dla $g \in G$ zachodzi $g \circ g = g$, to $g = e$. Niech więc dla pewnego $g \in G$ zachodzi $g \circ g = g$; niech h oznacza prawostronny element odwrotny (istnieje z aksjomatów), tj. $g \circ h = e$. Wówczas $(g \circ g) \circ h = g \circ h$, skąd $g \circ (g \circ h) = g \circ h$ (łączność), a więc $g \circ e = e$ (gdyż $g \circ h = e$), co daje $g = e$ (e jest prawostronnym elementem neutralnym).
2. Warunek oznacza, że jeśli $f \in G$ jest prawostronnym elementem neutralnym, tzn. $a \circ f = a$ dla wszystkich $a \in G$, to $f = e$. Podstawiając w szczególności f za a otrzymuje się $f \circ f = f$, co oznacza $f = e$ z punktu 1.
3. Innymi słowy: jeżeli $a \circ x = e$, to $x \circ a = e$. Niech zatem $a \circ x = e$; wtedy element $(x \circ a) \circ (x \circ a)$ jest równy $[(x \circ a) \circ x] \circ a = [x \circ (a \circ x)] \circ a$ (dwukrotnie łączność), a z założenia jest on równy $[x \circ e] \circ a = x \circ a$, czyli dla $g = (x \circ a)$ zachodzi $g \circ g = g$, a więc z punktu 1. wynika, że $g = e$, tzn. $x \circ a = e$.
4. Należy udowodnić, że $e \circ a = a$ dla dowolnego $a \in G$; niech $a \in G$, zaś x będzie jego prawostronnym elementem odwrotnym. Wówczas $a \circ x = e$, skąd $a \circ x = x \circ a$ (punkt 3.), a stąd $(a \circ x) \circ a = (x \circ a) \circ a$, czyli $a \circ (x \circ a) = (x \circ a) \circ a$, dlatego $a \circ e = e \circ a$ i wreszcie $a = e \circ a$, co oznacza, że e jest również lewostronnym elementem neutralnym.
5. Niech $f \circ a = a$ dla wszystkich $a \in G$, czyli f będzie lewostronnym elementem neutralnym, wtedy $f = e$. W szczególności podstawiając za a element f otrzymuje się $f \circ f = f$, co z punktu 1. daje $f = e$.
6. Wiadomo, że każdy element $a \in G$ ma co najmniej jeden prawostronny element odwrotny, niech będzie to x, tzn. $a \circ x = e$. Należy wykazać, że jeżeli $a \circ y = e$, to $y = x$ (gdzie $y \in G$). Niech więc $a \circ x = e$ oraz $a \circ y = e$. Z punktu 3. jest $x \circ a = e$, skąd $(x \circ a) \circ y = e \circ y$, czyli $x \circ (a \circ y) = e \circ y$, a więc $x \circ e = e \circ y$, to jest $x = e \circ y$ i wreszcie $x = y$ (punkt 4.).
7. i 8. Niech $a \in G$, a x oznacza jego jednoznacznie wyznaczony prawostronny element odwrotny. Z punktu 3. wiadomo, że x jest także lewostronnym elementem odwrotnym do a, tj. $x \circ a = e$. Należy udowodnić, że jeśli $x \circ a = e$ oraz $y \circ a = e$, to $x = y$. Niech zatem $x \circ a = e$ oraz $y \circ a = e$; wówczas $a \circ x = e$, skąd $y \circ (a \circ x) = y \circ e$, a więc $(y \circ a) \circ x = y$, czyli $e \circ x = y$, skąd $x = y$.

f. Przy zastąpieniu warunków *Element neutralny* oraz *Odwracalność* warunkami *Element neutralny'* oraz *Odwracalność'* należy sprawdzić własności:
1. istnieje $e \in G$ spełniające $a \circ e = a$ dla każdego $a \in G$;
2. wspomniany e spełnia też $e \circ a = a$ dla każdego $a \in G$;
3. e jest jedynym elementem w G o powyższych dwóch własnościach;
4. dla dowolnego $a \in G$ istnieje $a^{-1} \in G$ spełniający $a \circ a^{-1} = e$,
5. a ponadto $a^{-1} \circ a = e$;
6. przy czym a^{-1} jest jedynym elementem G, dla którego $a \circ a^{-1} = e = a^{-1} \circ a$.

Stosując przedstawioną definicję wystarczy sprawdzić punkty 1. oraz 4.; punkty 2., 3., 5., 6. wynikają z 1. oraz 4., co znacząco ułatwia przekonanie się o tym, czy dany zbiór z działaniem tworzy grupę.

g. Niech e_{R_1}, e_{R_2} będą dwoma różnymi prawostronnymi elementami neutralnymi w strukturze algebraicznej (grupoidzie, zob. *Podobne struktury*) $(S, \bullet)$. Zakładając, że struktura ta ma (co najmniej jeden) lewostronny element neutralny e_L popada się w sprzeczność: z ich definicji jest $e_{R_1} = e_{R_1} \bullet e_L = e_L = e_{R_2} \bullet e_L = e_{R_2}$ wbrew założeniu, że e_{R_1}, e_{R_2} są różne. Stąd struktura algebraiczna z więcej niż jednym prawostronnym elementem neutralnym nie może mieć lewostronnego elementu neutralnego.

h. Niech $(S, \leftarrow)$ struktura algebraiczną (grupoid, zob. *Podobne struktury*) z działaniem danym wzorem $a \leftarrow b = a$ dla wszystkich $a, b \in S$ (działanie odpowiada rzutowi lewostronnemu dla pary uporządkowanej $(a, b) \in S \times S$). Działanie $\leftarrow$ jest wewnętrzne wprost z definicji: $a \leftarrow b = a \in S$ bez względu na wybór $a, b \in S$; działanie $\leftarrow$ jest też łączne, ponieważ z jego definicji dla dowolnych $a, b, c \in S$ zachodzi
$a \leftarrow (b \leftarrow c) = a \leftarrow b = a = a \leftarrow c = (a \leftarrow b) \leftarrow c$. Z samej definicji działania wynika także, że każdy element S jest prawostronnym elementem neutralnym. W ten sposób spełnione są trzy pierwsze aksjomaty grupy; ponadto skoro dla dowolnego $a \in S$ jest $e \leftarrow a = e$, a e jest elementem neutralnym, to spełniony jest też warunek istnienia lewostronnego elementu odwrotnego. Z istnienia więcej niż jednego prawostronnego elementu neutralnego wynika jednak brak lewostronnych elementów neutralnych[9], co przeczy ustaleniom lematu[8], zatem $(S, \leftarrow)$ nie może być grupą.

i. Odpowiadających a^{-1} o b oraz $b \circ a^{-1}$ w standardowej definicji; w szczególności $e = a \backslash a$ oraz $a^{-1} = 1 \backslash a$.

j. Do zdefiniowania grupy wystarczy jedynie działanie $/$: otóż $e = a/a$, $a^{-1} = (a/a)/a$ oraz $ab = a/((b/b)/b)$. Ponadto grupę można wtedy zdefiniować za pomocą jednego aksjomatu: dla dowolnych $a, b, c \in G$ zachodzi $a/(((a/a)/b)/c)/((a/a)/c) = b$.

k. Nazwa „abelowy" pochodzi od nazwiska Nielsa Abela (1802–1829), który podał warunki rozwiązywalności równań wielomianowych (zob. dalej) w postaci równań nazywanych jego nazwiskiem (za Jordanem i Kroneckerem); w późniejszych pracach innych autorów, operujących innymi, nowocześniejszymi narzędziami, okazało się, że wspomniane warunki były równoważne przemienności odpowiedniej grupy przekształceń pierwiastków wielomianu (tzw. grupy Galois, od nazwiska prekursora teorii grup, Évariste'a Galois, 1811–1832); jako pierwszy nazwy „grupa abelowa" na określenie grup przemiennych użył Weber.

l. Tabliczki działania (tablice Cayleya) działań przemiennych są symetryczne względem przekątnej głównej (łączącej komórki w „lewym górnym" i „prawym dolnym" rogu).

m. Teoria pierwszego rzędu grup przemiennych jest rozstrzygalna (co wynika wprost z rozstrzygalności arytmetyki Presburgera), czego nie można powiedzieć o ogólnej teorii grup. Przykładowo pojęcie podgrupy normalnej (zob. *Pojęcia*) nie odgrywa większej roli w teorii grup przemiennych, ponieważ wszystkie podgrupy są normalne, a w związku z tym różnorodne iloczyny grup stają się zwykłym iloczynem prostym. Dzięki przemienności możliwe jest sklasyfikowanie skończonych grup przemiennych, a nawet skończenie generowanych grup przemiennych (zob. dalej; rozstrzygalna jest również teoria pierwszego rzędu skończenie generowanych grup przemiennych z działaniem sumy prostej, ze względu na które ich zbiór tworzy monoid przemienny). Mimo tych sukcesów próby sklasyfikowania beztorsyjnych grup przemiennych skończonej rangi są daleko niezadowalające: obok wspomnianych grup skończenie generowanych satysfakcjonujący opis istnieje tylko dla grup o randze 1 (zob. postępy); podobnie istnieje wiele nierozwiązalnych problemów w teorii beztorsyjnych grup abelowych nieskończonej rangi (pojęcie grupy torsyjnej jest jednym z powodów niemożności sformalizowania teorii grup jako teorii pierwszego rzędu: wymagałoby to użycia zabronionej w logice pierwszego rzędu nieskończenie długiej alternatywy; z drugiej strony klasa grup torsyjnych nie jest Δ-elementarna); badania nad przeliczalnymi grupami mieszanymi są o wiele mniej zaawansowane niż nad przeliczalnymi grupami torsyjnymi (zob. *Pojęcia*).

n. Przykładowo zbiór $\mathbb{R}$, liczb rzeczywistych wyposażony jest w wiele struktur, m.in. porządkową, topologiczną, geometryczną, algebraiczną; tę bogatą strukturę oznacza się zwykle symbolem $\mathbb{R}$. W związku z tym mówi się o *grupie addytywnej* liczb rzeczywistych $\mathbb{R}^+ = (\mathbb{R}, +)$, oznaczanej często po prostu $\mathbb{R}$, i *grupie multiplikatywnej* niezerowych (odwracalnych) liczb rzeczywistych $\mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \cdot)$ (zob. *Przykłady*, por. *Motywacja*).

o. **Jednoznaczność**: Istnieje co najwyżej jeden $x \in G$, dla którego $ax = b$. Niech $ax = b = ax'$, wtedy $a^{-1}(ax) = a^{-1}(ax')$, czyli $(a^{-1}a)x = (a^{-1}a)x'$, a więc $ex = ex'$, co daje $x = x'$ na mocy lematu[8].
Istnienie: O istnieniu co najmniej jednego $x \in G$ można się przekonać kładąc $x = a^{-1}b$. Rzeczywiście, $a(a^{-1}b) = (aa^{-1})b = eb = b$.
Drugi przypadek dowodzi się analogicznie jak pierwszy.

p. Istnienie rozwiązań równania liniowego (z jedną niewiadomą) ma też interpretację w tabliczce działania (tablicy Cayleya): każdy wiersz/kolumna tablicy działania grupowego zawiera dany element grupy wyłącznie jeden raz.

q. Mnożąc lewostronnie $ab = ac$ przez a^{-1} otrzymuje się $a^{-1}(ab) = a^{-1}(ac)$, co z łączności jest równoważne $(a^{-1}a)b = (a^{-1}a)c$, czyli $eb = ec$, a ponieważ e jest elementem neutralnym, to ostatecznie $b = c$. Drugą część dowodzi się podobnie.

r. Własność skracania (bądź równoważnie: odwracalności) dla każdego elementu grupy sprawia, że tabliczka działania w grupie (tablica Cayleya grupy) jest kwadratem łacińskim: każdy element grupy pojawia się w ustalonej kolumnie i ustalonym wierszu jeden i tylko jeden raz.

s. Z definicji a^{-1} jest $aa^{-1} = e$, zatem a jest lewostronnym elementem odwrotnym do a^{-1}, co (z lematu[8]) oznacza, że a jest elementem odwrotnym do a^{-1}.

t. Własność ta mówi więc, że odwracanie elementów traktowane jako działanie jednoargumentowe $\cdot^{-1} : G \to G$ jest inwolucją (ponadto jest ono naturalnym antyizomorfizmem grupy i jej grupy przeciwnej, zob. homomorfizm grup).

u. Ponieważ $(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$, to $b^{-1}a^{-1}$ jest elementem odwrotnym do ab.

v. Równość $(ab)^{-1} = a^{-1}b^{-1}$ zachodzi tylko wtedy, gdy $a^{-1}b^{-1} = b^{-1}a^{-1}$ (co jest równoważne $ab = ba$, a więc nie jest ogólną prawidłowością).

w. Iloczyn trzech elementów a, b, c w tej właśnie kolejności obliczany jest za pomocą dwóch iloczynów: najpierw ab, następnie przez c, bądź najpierw bc, następnie przez a. Dzięki łączności otrzymywane wyniki są równe, dzięki czemu można pisać abc bez nawiasów.

x. Iloczyn czterech elementów a, b, c, d oblicza się za pomocą trzech kolejnych iloczynów, co można zrobić na pięć różnych sposobów: $a(b(cd))$, $a((bc)d)$, $(ab)(cd)$, $((ab)c)d$, $(a(bc))d$, które są jednak równe dzięki łączności: pierwsze dwa iloczyny są równe, gdyż $b(cd) = (bc)d$, ostatnie dwa są równe, ponieważ $(ab)c = a(bc)$; ponadto $a(b(cd)) = (ab)(cd)$ oraz $(ab)(cd) = ((ab)c)d$ (wystarczy położyć odpowiednio $cd = f$ oraz $ab = g$, by uzyskać $a(bf) = (ab)f$ oraz $g(cd) = (gc)d$). Umożliwia to opuszczenie nawiasów i pisanie $abcd$ na oznaczenie iloczynu elementów a, b, c, d w tej właśnie kolejności.

y. Dokładnie na $(4n - 6)!!/n!$ (zob. silnia)

z. Poniższe rozumowanie jest prawdziwe nie tylko dla grup, w związku z tym zostanie wyrażone w ogólniejszej postaci.

Lemat

Niech G będzie niepustym zbiorem z określonym na nim działaniem dwuargumentowym oznaczanym przez zestawienie. Iloczyny elementów $a_1, \ldots, a_n \in G$ są niezależne od sposobu wstawiania nawiasów. Oznacza to, co następuje. Niech

$$P_1(a_1) = \{a_1\},$$
$$P_2(a_1, a_2) = \{a_1 a_2\},$$
$$P_3(a_1, a_2, a_3) = \{(a_1 a_2)a_3, a_1(a_2 a_3)\} = \{xy : x \in P_1(a_1), y \in P_2(a_2, a_3) \text{ lub } x \in P_2(a_1, a_2), y \in P_1(a_3)\}$$
$$P_4(a_1, a_2, a_3, a_4) = \{((a_1 a_2)a_3)a_4), a_1((a_2 a_3)a_4), (a_1 a_2)(a_3 a_4), ((a_1 a_2)a_3)a_4), (a_1((a_2 a_3)a_4))a_4\} =$$
$$= \{xy : x \in P_1(a_1), y \in P_3(a_2, a_3, a_4) \text{ lub } x \in P_2(a_1, a_2), y \in P_2(a_3, a_4) \text{ lub } x \in P_3(a_1, a_2, a_3), y \in P_1(a_4)\}$$
$$\ldots$$
$$P_n(a_1, \ldots, a_n) = \{xy : x \in P_1(a_1, \ldots, a_i), y \in P_{n-i}(a_{i+1}, \ldots, a_n) \text{ dla pewnego } 1 \leqslant i \leqslant n-1\}$$

dla $k = 1, \ldots, n$ P_k są więc podzbiorami G zawierającymi iloczyny $a_1, \ldots, a_k$ zredukowanymi do $k - 1$ kolejnych mnożeń dwóch elementów z G).
Teza: dla każdego $n \in \mathbb{N}$ i wszystkich $a_1, \ldots, a_n \in G$ zbiór $P_n(a_1, \ldots, a_n)$ zawiera jeden i tylko jeden element.

Dowód

Dowód przez indukcję względem n. Dla $n = 1, 2$ jest oczywiste, że tak $P_1(a_1)$ jak i $P_2(a_1, a_2)$ mają nie mniej, nie więcej jeden element. Dla $n = 3$ teza to inna postać warunku łączności; dla $n = 4$ teza wynika z rozumowania opisanego w jednej z poprzednich uwag (użyto tam wyłącznie łączności działania!).
Niech $n \geqslant 5$ i lemat będzie prawdziwy dla $1, \ldots, n - 1$. Niech $u, v \in P_n(a_1, \ldots, a_n)$; należy udowodnić $u = v$. Z definicji $P_n(a_1, \ldots, a_n)$ jest $u = xy$ oraz $v = st$, gdzie

$$x \in P_i(a_1, \ldots, a_i),\ y \in P_{n-i}(a_{i+1}, \ldots, a_n),\ i = 1, \ldots, n-1;$$
$$s \in P_j(a_1, \ldots, a_j),\ t \in P_{n-j}(a_{j+1}, \ldots, a_n),\ j = 1, \ldots, n-1.$$

Dowiedzione zostanie $u = v$, najpierw przy założeniu $i = j$. Na mocy indukcji zbiór $P_i(a_1, a_2, \ldots, a_i)$ zawiera jeden i tylko jeden element; zatem $x = s$. Stosując hipotezę indukcyjną dla $n - i$, dla elementów $a_{i+1}, \ldots, a_n$, również można stwierdzić, że $P_{n-i}(a_{i+1}, \ldots, a_n)$ również ma jeden i tylko jeden element; daje to $y = t$. W ten sposób $u = xy = sy = st = v$, teza jest więc prawdziwa w przypadku $i = j$.
Niech teraz $i \neq j$; bez utraty ogólności można założyć, że $i < j$. Niech $j = i + h$ dla $h \in \mathbb{N}$. Stosując hipotezę indukcyjną dla j, dla elementów $a_1, \ldots, a_j$ otrzymuje się dokładnie jeden element w $P_j(a_1, \ldots, a_j)$ oznaczany dalej s. Również z indukcji zastosowanej dla i, dla elementów $a_1, \ldots, a_i$ istnieje dokładnie jeden element w $P_i(a_1, \ldots, a_i)$, mianowicie x. Raz jeszcze z indukcji zastosowanej do h, dla elementów $a_{i+1}, \ldots, a_j$ istnieje dokładnie jeden element w $P_h(a_{i+1}, \ldots, a_j)$, niech to będzie b. Z definicji $P_j(a_1, \ldots, a_j)$ jest $xb \in P_j(a_1, \ldots, a_j)$, czyli $xb = s$.
Jest $n - i = h + (n - j)$. Z indukcji zastosowanej do $n - i$, dla elementów $a_{i+1}, \ldots, a_n$ zbiór $P_{n-i}(a_{i+1}, \ldots, a_n)$ ma jeden i tylko jeden element nazywany dalej y. Również z indukcji zastosowanej dla h, dla elementów $a_{i+1}, \ldots, a_j$ istnieje dokładnie jeden element w $P_h(a_{i+1}, \ldots, a_j)$, mianowicie b. Znowu z indukcji zastosowanej do $n - j$, dla elementów $a_{j+1}, \ldots, a_n$ zbiór $P_{n-j}(a_{j+1}, \ldots, a_n)$ ma dokładnie jeden element, niech to będzie t. Z definicji $P_{n-i}(a_{i+1}, \ldots, a_{i+h}, a_{j+1}, \ldots, a_n)$ jest $bt \in P_{n-i}(a_{i+1}, \ldots, a_n)$, a więc $bt = y$.
Stąd $xb = s$ oraz $bt = y$; daje to $u = xy = x(bt) = (xb)t = st = v$, co kończy dowód.

aa. Oznaczany również $\prod_{i=1}^{n} a_i$, a w zapisie addytywnym $\sum_{i=1}^{n} a_i$.

ab. Dowód przez indukcję ze względu na n. Przypadek $n = 1$ jest trywialny, dla $n = 2$ jest $(a^m)^2 = a^m a^m = a^{m+m} = a^{2m} = a^{m2}$. Niech $n \geqslant 3$ oraz $(a^{m-1})^n = a^{(m-1)n}$ dla wszystkich $a \in G$; należy wykazać, że $(a^m)^n = a^{mn}$ dla wszystkich $a \in G$. Ponieważ $(a^m)^n = (a^m)^{1+(n-1)} = (a^m)^1 (a^m)^{n-1} = a^m (a^m)^{n-1}$ z założenia (podstawiono kolejno $a^m, 1, n - 1$ w miejsca a, m, n), to $(a^m)^n = a^m a^{m(n-1)} = a^m a^{mn-m} = a^{m(mn-m)}$ z założenia (kolejno $a, m, mn - m$ w miejsca a, m, n), co kończy dowód.

ac. Jeśli $m \geqslant 1, n \geqslant 1$, to $a^m a^n = a^{m+n}$ wynika z powyższej uwagi. Jeśli $m = 0$, to $a^0 a^n = ea^n = a^n = a^{0+n}$ dla każdego $n \in \mathbb{Z}$; jeśli zaś $n = 0$, to $a^m a^0 = a^m e = a^m = a^{m+0}$ dla każdego $m \in \mathbb{Z}$. Zatem

$$a^m a^n = a^{m+n} \text{ o ile } m, n \geqslant 0 \quad (*)$$

Należy dowieść tej relacji również dla $m \geqslant 0, n \leqslant 0$; $m \leqslant 0, n \geqslant 0$; $m \leqslant 0, n \leqslant 0$;
Zmieniając notację (zastępując m, n przez $|m|, |n|$) należy dowieść: (i) $(a^m)^{-n} = a^{m(-n)}$, (ii) $(a^{-m})^n = a^{(-m)n}$, (iii) $(a^{-m})^{-n} = a^{(-m)(-n)}$ dla wszystkich $m, n \geqslant 0$.
Zapisując $(*)$ z a^{-1} w miejsce a i korzystając z poprzedniego punktu otrzymuje się $(a^m)^{-n} = [(a^m)^{-1}]^n = (a^{-m})^n = [(a^{-1})^m]^n = (a^{-1})^{mn} = a^{(-mn)} = a^{m(-n)}$, co dowodzi (i). Jest też $(a^{-m})^n = a^{(-mn)} = a^{(-m)n}$, co dowodzi (ii). Wreszcie jest $(a^{-m})^{-n} = [(a^m)^{-1}]^{-n} = (a^{-m})^n = \{[(a^m)^{-1}]^{-1}\}^n = (a^m)^n = a^{mn} = a^{(-m)(-n)}$, co dowodzi (iii).
Stąd $(a^m)^n = a^{mn}$ dla wszystkich $m, n \in \mathbb{Z}$.

af. Dowód przez indukcję względem n. Jeśli $n = 2$, teza zachodzi na podstawie poprzedniego rozumowania[11]. Gdy $n \geqslant 3$ oraz $(a_1 a_2 \ldots a_{n-1})^{-1} = a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$, to

$$(a_1 a_2 \ldots a_{n-1} a_n)^{-1} = ((a_1 a_2 \ldots a_{n-1}) a_n)^{-1} =$$
$$= a_n^{-1} (a_1 a_2 \ldots a_{n-1} a_{n-1})^{-1} =$$
$$= a_n^{-1} (a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}) =$$
$$= a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1},$$

co należało wykazać.

ag. Przypadek $n = 0$ jest trywialny. Z kolei $ab^n = ab = ba = b^1 a$ z założenia, a więc stwierdzenie jest prawdziwe dla $n = 1$. Niech $n \geqslant 2$ i stwierdzenie będzie dowiedzione dla $n - 1$, czyli $ab^{n-1} = b^{n-1} a$. Wówczas

$$ab^n = a(b^{n-1} b) = (ab^{n-1})b = (b^{n-1} a)b = b^{n-1}(ab) = b^{n-1}(ba) = (b^{n-1} b)a = b^n$$

Na mocy indukcji jest $ab^n = b^n a$ dla każdego $n \in \mathbb{N}$. Mnożąc tę zależność z lewej i z prawej strony przez b^{-n} otrzymuje się $b^{-n} a = ab^{-n}$ dla wszystkich $n \in \mathbb{N}$, skąd $ab^n = b^n a$ jest prawdziwa również dla $n \leqslant -1$. Zatem $ab^n = b^n a$ dla wszystkich $n \in \mathbb{Z}$.

ah. Biorąc właśnie dowiedzioną tożsamość $ab^n = b^n a$ jako założenie i zastępując w niej a, b, n odpowiednio przez b^n, a, m otrzymuje się $a^m b^n = b^n a^m$ dla wszystkich $m, n \in \mathbb{Z}$.

ai. Dowody tych własności pozostają poprawne, gdy G jest zbiorem z działaniem dwuargumentowym (tzn. jest grupoidem, zob. *Podobne struktury*) dla $m, n \in \mathbb{N}$; również w przypadku $m = n = 0$, o ile w G istnieje jednoznacznie wyznaczony element neutralny e (tzn. $ce = ec$ dla dowolnego $c \in G$) i przyjąć, że $a^0 = e$ dla dowolnego $a \in G$ (tzn. G jest monoidem, zob. *Podobne struktury*).

aj. Niech $a^2 = e$ dla dowolnego $a \in G$. Wówczas
$ab = e(ab)e = b^2(ab)a^2 = bb(ab)aa = b(baba)a = b(ba)^2 a = bea = ba$, czyli $ab = ba$ dla dowolnych $a, b \in G$, a zatem G jest przemienna.

ak. Ponieważ $(a, b) \diamond (0, 0) = (a, b + 0) = (a, b)$ oraz $(a, b) \diamond (1, 0) = (a, b + 0) = (a, b)$ dla wszystkich $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.

al. Zgodnie z lematem[8].

am. Jeśli G zawiera wyłącznie element g, to jedynym możliwym działaniem jest $gg = g$. Wewnętrzność: działanie jest wewnętrzne wprost z tożsamości, gdyż $g \in G$. Łączność: ponieważ aksjomat przyjmuje postać $(gg)g = g(gg)$, a dzięki tożsamości jest $(gg)g = gg = g(gg)$ dla jedynego $g \in G$. Element neutralny: z lematu[8] wynika, że g musi być prawostronnym elementem neutralnym. Element odwrotny: g jest prawostronnym elementem odwrotnym do siebie na podstawie tożsamości.

an. Grupa euklidesowa jest podgrupą przekształceń przestrzeni euklidesowej; podobnie kolejne wymienione grupy są podgrupami (zob. *Pojęcia*) poprzednio wymienionych.

ao. Por. kryterium bycia podgrupą: jeżeli $a^m, a^n \in \langle a \rangle$, to $a^m a^n = a^{m+n} \in \langle a \rangle$, gdyż $m + n \in \mathbb{Z}$ dla $m, n \in \mathbb{Z}$ oraz jeśli $a^m \in \langle a \rangle$, to $(a^m)^{-1} = a^{-m} \in \langle a \rangle$, gdyż $-m \in \mathbb{Z}$ dla $m \in \mathbb{Z}$.

ap. Grupa ilorazowa przez daną podgrupę normalną ma nie więcej elementów niż grupa będąca dzielną; grupa ilorazowa nie jest jednak podzbiorem, czy podgrupą grupy wyjściowej (grupy te mają one różne nośniki i działania).

aq. Grupa jest „wolna" w sensie braku nałożonych na nią, w postaci wspomnianych relacji, więzów; w ilorazie dzielnikiem musi być podgrupa normalna: w związku z tym jego rolę pełni najmniejsza podgrupa normalna zawierająca podgrupę (tzw. domknięcie normalne tej podgrupy) opisującą relację.

ar. Pochodna, w przeciwieństwie do centrum, jest w istocie zawsze *podgrupą całkowicie charakterystyczną* (albo *w pełni charakterystyczną/niezmienniczą*), czyli odwzorowywaną w siebie przy każdym homomorfizmie grupy w siebie (zawężenie charakterystyczności; taką podgrupę można rozumieć jako „stabilną" w grupie). Więcej: pochodne, obok wyrazów *dolnego ciągu centralnego*, czy *podgrup potęgowych* (złożonych z elementów będących ustalona potęgą elementów grupy), są przykładami podgrup o właściwościach uszczegóławiających całkowitą charakterystyczność, tzw. *podgrup werbalnych* generowanych za pomocą „słów" (skąd pochodzi nazwa), czyli iloczynów elementów ustalonej postaci („dopełnieniem" podgrup werbalnych są *podgrupy marginalne*, np. centrum); zob. rozmaitość grup.

as. Ogólnie podgrupy Sylowa to „maksymalne" podgrupy pierwsze (skończone), czyli grupy, których rząd jest najwyższą możliwą potęgą danej liczby pierwszej.

at. W przypadku przemiennym rozkład jest iloczynem prostym (sumą prostą) podgrupy normalnej i grupy ilorazowej, w przypadku ogólnym – iloczyn półprosty (zob. rozkład i iloczyny grup).

au. Przykładowo każda grupa skończona, np. w przeciwieństwie do (nieskończonej) grupy liczb całkowitych, ma ciąg kompozycyjny.

av. Użyte wcześniej stwierdzenie „różne grupy mogą składać się z tych samych elementów składowych" (niejednoznaczność rozwiązania problem rozszerzenia) oznacza, że grupy niemające tej samej struktury mogą mieć ten sam ciąg kompozycyjny.

aw. Klasyfikacja ta jest wynikiem dziesiątek tysięcy stron w kilkuset publikacjach napisanych przez ponad stu autorów, w większości w latach 1955–2004.

ax. Faktycznie: podgrup Sylowa – skończona grupa przemienna jest ich iloczynem prostym.

ay. Ranga grupy przemiennej jest uogólnieniem *rangi* grupy przemiennej wolnej będącej obiektem wolnym w kategorii grup przemiennych; jej odpowiednikiem w kategorii wszystkich grup jest grupa wolna — ze względu na różne kategorie pojęcia te mają ze sobą mało wspólnego: pokrywają się tylko w przypadku grupy trywialnej i grupy cyklicznej nieskończonej (odpowiednio ranga 0 i 1, grupy wolny o wyższych rangach nie są przemienne; por. algebra wolna).

az. Nazywa się je także „półgrupą z jedynką".

Przypisy

1. Czesław Bagiński: *Wstęp do teorii grup*. Warszawa: SCRIPT, 2005, s. 9. ISBN 83-904564-9-4.
2. Marshall Hall, Jr.: *The theory of groups*. Moskwa: 1962, s. 18. (ros.)
3. Aleksander Kurosz: *Algebra ogólna. Wykłady z lat 1969–1970*. Moskwa: 1974, s. 17–19. (ros.)
4. Jerzy Browkin: *Teoria reprezentacji grup skończonych*. Warszawa: 2010, s. 6. ISBN 978-83-01-16051-7.

Bibliografia

- David Easdown, Cheryl E. Praeger. *On minimal faithful permutation representations of finite groups* (https://www.cambridge.org/core/services/aop-cambridge-core/content/view/S0004972700027489). „Bull. Aust. Math. Soc.". 38, s. 207–220, 1988. ISSN 0004-9727 (http://worldcat.org/issn/0004-9727). [dostęp 2017-04-30].
- Witold Więsław: *Matematyka Hoene-Wrońskiego za jego czasów (http://www.impan.gov.pl/~pragacz/download/Wieslaw.pdf)*. Wrocław: Instytut Matematyczny UW. [dostęp 2017-04-30].

Linki zewnętrzne

- L.G. Kovács, Cheryl E. Praeger. *On minimal faithful permutation representations of finite groups* (https://www.cambridge.org/core/services/aop-cambridge-core/content/view/S0004972700018797). „Bull. Aust. Math. Soc.". 62, s. 207–220, 2000. [dostęp 2017-04-30].

Źródło: „https://pl.wikipedia.org/w/index.php?title=Grupa_(matematyka)&oldid=51541716"

Tę stronę ostatnio edytowano 16:19, 14 sty 2018. Tekst udostępniany na licencji Creative Commons: uznanie autorstwa, na tych samych warunkach (http://creativecommons.org/licenses/by-sa/3.0/deed.pl), z możliwością obowiązywania dodatkowych ograniczeń. Zobacz szczegółowe informacje o warunkach korzystania (http://wikimediafoundation.org/wiki/Warunki_korzystania).