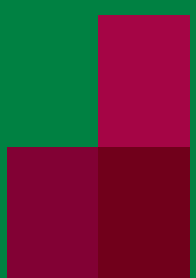
Andrzej Białynicki-Birula

ALGEBRA



WYDAWNICTWO NAUKOWE PWN

ALGEBRA

Andrzej Białynicki-Birula

ALGEBRA

Wydanie czwarte

WYDAWNICTWO NAUKOWE PWN
WARSZAWA 2009

Książka ukazała się w latach 1971–1980 nakładem Państwowego Wydawnictwa Naukowego
jako tom 40 serii BIBLIOTEKA MATEMATYCZNA

Projekt okładki i stron tytułowych
Małgorzata Podziomek

Redaktor inicjujący
Izabela Ewa Mika

ISBN 978-83-01-15817-0

Wydawnictwo Naukowe PWN SA
ul. Miodowa 10, 00-251 Warszawa
tel. 022 69 54 321
faks 022 69 54 031
e-mail: pwn@pwn.com.pl; www.pwn.pl

Wydawnictwo Naukowe PWN SA
Wydanie IV
Arkuszy drukarskich 17,25
Druk ukończono w lutym 2009 r.
Druk i oprawa: ZPW „Pozkal”
88-100 Inowrocław, ul. Cegielna 10/12

PRZEDMOWA
DO WYDANIA PIERWSZEGO

Niniejsza książka przeznaczona jest dla słuchaczy pierwszego roku studiów matematycznych jako podręcznik do wykładu „Algebra I" i w związku z tym jest dostosowana do obecnie obowiązującego programu tego wykładu. Niemal wszystkie punkty programu ramowego zostały tu omówione, a oprócz tego przedstawione w książce zagadnienia nie wyprowadzają w zasadzie poza jego tematykę. Z punktów przewidzianych przez program pominięto tu jedynie działania na macierzach i iloczyny proste grup z myślą omówienia tych tematów w wykładzie „Algebra II". Oprócz tego przewidziane programem pojęcie algebry abstrakcyjnej zastąpiono tu nieco węższym (i łatwiejszym) pojęciem systemu algebraicznego. Pozostałe zagadnienia zostały potraktowane obszernie i z właściwą współczesnej algebrze ogólnością. Starałem się jednak wykazać w tej książce, że to dążenie do ogólności i abstrakcji jest usprawiedliwione różnorodnością zastosowań tak sformułowanych rezultatów i nie jest celem samym w sobie, lecz służy przede wszystkim lepszemu zrozumieniu i opracowaniu doskonalszych metod badania własności pewnych konkretnych obiektów algebraicznych (w szczególności liczb). Z tych względów określenie ogólnego pojęcia czy sformułowanie ogólnego twierdzenia jest w książce często poprzedzane omówieniem jego szczególnych przypadków. Tym też tłumaczyć można wstrzemięźliwość we wprowadzaniu definicji abstrakcyjnych pojęć i formułowaniu ogólnych rezultatów dopóki nie jest jeszcze zgromadzony szczegółowy materiał dający podstawę do uogólnień i stanowiący ich źródło. Dotyczy to nawet takich sytuacji, w których odbywa się to kosztem zwięzłości tekstu.

Książka składa się z 11 rozdziałów. W pierwszych trzech omówione są podstawowe pojęcia teorii ciał i przedstawione są najważniejsze przykłady ciał. Rozdział IV zawiera teorię równań liniowych wraz ze wstępem do algebry liniowej. W rozdziale V omówione są najprostsze własności pierścieni, a rozdział VI zawiera omówienie pierścieni wielomianów, istotną część zajmuje tu tzw. arytmetyka pierścienia wielomianów i własności zbioru pierwiastków danego wielomianu. W rozdziale VII wprowadzone jest pojęcie homomorfizmu pierścienia i badane są związki między homomorfizmem a jego jądrem. Konstrukcje pierścienia ilorazowego i ciała ułam-

ków podane są w rozdziale VIII. Rozdział IX zawiera podstawy teorii rozkładu elementów pierścienia na iloczyny, a rozdział X jest wstępem do teorii rozszerzeń algebraicznych ciał (a więc i do teorii Galois). W ostatnim, XI rozdziale wprowadzone są podstawowe pojęcia teorii grup. Nadrzędnym tematem książki, wiążącym wszystkie jej rozdziały, jest teoria równań.

Każdy z rozdziałów podzielony jest na paragrafy. W zakończeniu każdego paragrafu umieszczone są ćwiczenia pomyślane jako rodzaj testu dla sprawdzenia, czy czytelnik właściwie rozumie wprowadzone pojęcia. Nieliczne trudniejsze ćwiczenia oznaczone zostały gwiazdką. Przerobienie podanych ćwiczeń nie wystarczy zapewne do należytego przyswojenia wprowadzonych pojęć i nabrania właściwych intuicji z nimi związanych.

W książce stosowana jest jednolita dwuliczbowa numeracja definicji, twierdzeń, lematów i wniosków. Pierwsza liczba pokrywa się z numerem paragrafu. Powołując się na wcześniejszy materiał piszemy np. „definicja 3.2", gdy chodzi o definicję o numerze 3.2 danego rozdziału (znajduje się ona w § 3) oraz „definicja 3.2 rozdz. VII", gdy chodzi o definicję o numerze 3.2 z (§ 3) rozdziału VII. Podobnie, powołując się na przykład 3 danego paragrafu piszemy „przykład 3", jeśli natomiast chodzi nam o przykład 3 innego paragrafu danego rozdziału, podajemy dodatkowo numer tego paragrafu, a jeśli przykład, o który chodzi, podany jest w innym rozdziale, podajemy jeszcze numer tego rozdziału.

Wydaje się, że trudno byłoby przedstawić cały materiał objęty książką w ramach wykładu „Algebra I". Wobec tego wykładowca, który zechce posłużyć się tym podręcznikiem przy opracowywaniu wykładu, będzie musiał dokonać pewnego wyboru materiału. Dotyczy to w szczególności tematów poruszanych w trzech ostatnich rozdziałach książki. Oprócz tego pewne tematy z poprzednich rozdziałów mogą być omówione na wykładzie z mniejszą dokładnością lub ogólnością (np. §§ 4, 7 i 9 rozdz. VI, §§ 10, 11, i 12 rozdz. VII, § 1, rozdz. VIII) z myślą o podaniu ewentualnych uzupełnień na ćwiczeniach. Sądzę, że na ćwiczeniach powinny być też omówione (pominięte w książce, lecz ważne i związane z jej materiałem) wzory Viète'a oraz różniczkowanie wielomianów (wraz z zastosowaniami do badania krotności pierwiastków).

Tekst książki oparty jest w dużej mierze na skrypcie *Algebra I* wydanym dwukrotnie przez Uniwersytet Warszawski. Pierwsze wydanie tego skryptu ukazało się w roku 1966, a jego autorami byli profesor Andrzej Mostowski, docent Wacław Zawadowski i autor niniejszej książki; drugie wydanie będące nowym opracowaniem, ukazało się w roku 1968.

Składam gorące podziękowanie profesorowi Andrzejowi Mostowskiemu za zgodę na wykorzystanie w tej książce obszernych fragmentów skryptu, których był autorem. Równie gorąco dziękuję profesorowi Stanisławowi Balcerzykowi za wnikliwe

przestudiowanie maszynopisu i zaproponowanie mi wielu poprawek i ulepszeń tekstu oraz docentowi Marcelemu Starkowi za cenne uwagi krytyczne dotyczące pierwszych rozdziałów. Dziękuję również za współpracę i cenne uwagi doktorowi Maciejowi Bryńskiemu, doktorowi Juliuszowi Brzezińskiemu, magistrowi Andrzejowi Mąkowskiemu i docentowi Wacławowi Zawadowskiemu.

Andrzej Białynicki-Birula

PRZEDMOWA
DO WYDANIA DRUGIEGO

Wydanie II tej książki nie różni się istotnie od wydania I. Wprowadzone zostały jednak pewne uzupełnienia związane z tematami, które znalazły się w nowym programie wykładu algebry. Usuniętych zostało również wiele błędów stylistycznych i przeoczeń, które wkradły się do pierwszego wydania. Wykrycie znacznej części tych usterek zawdzięczam doc. doc. J. Browkinowi oraz K. Szymiczkowi, którym składam za to gorące podziękowanie.

Andrzej Białynicki-Birula

Warszawa, grudzień 1974

WSTĘP

Algebra była do końca wieku XIX głównie nauką o rozwiązaniach równań. Teoria równań pozostała do dziś ważnym działem algebry oraz źródłem nowych pojęć i teorii, ale sformułowanie, rozumienię i zakres tego problemu z biegiem czasu uległy bardzo istotnym zmianom. Ponadto w toku prac nad tym zagadnieniem matematycy stworzyli pewne ogólne pojęcia, które badane są obecnie niezależnie od ich powiązań z teorią równań i które znalazły również szerokie zastosowania w badaniu innych, nieraz odległych, problemów. Zaczątki tych pojęć spotykamy w pracach matematyków wieku XIX, ale ich ostateczne określenie i opracowanie przyniosła pierwsza połowa obecnego stulecia. W niniejszym wykładzie będziemy omawiać te ogólne pojęcia wskazując również na ich zastosowania do teorii równań.

ROZDZIAŁ I

POJĘCIE CIAŁA

W rozdziale tym wprowadzimy najpierw terminologię ogólnej teorii działań. Następnie określimy jedno z podstawowych pojęć współczesnej algebry — pojęcie ciała.

§ 1. Działania i systemy algebraiczne

Rozpatrywać będziemy zbiory o jakichkolwiek elementach, np. zbiór wszystkich liczb wymiernych (tj. liczb postaci m/n, gdzie m i n są liczbami całkowitymi $0, \pm 1, \pm 2, \ldots$ i $n \neq 0$) albo zbiór wszystkich liczb rzeczywistych, albo zbiór złożony tylko z dwu liczb 0 i 1, albo np. zbiór złożony z trzech przedmiotów $0, *, \square$. *Zbiory* oznaczać będziemy zwykle dużymi literami np. $A, B, G, K, L, P, \ldots, Z$. Zamiast pisać, że przedmiot *a jest elementem zbioru A*, piszemy $a \in A$; jeśli *a nie jest elementem zbioru A*, to piszemy $a \notin A$. Zbiór nie zawierający żadnego elementu nazywamy *zbiorem pustym*.

Przypomnijmy, że zgodnie z oznaczeniami przyjętymi w teorii zbiorów, jeśli φ jest *odwzorowaniem* (*przekształceniem*) *zbioru X w zbiór Y*, to piszemy $\varphi\colon X \to Y$. A dalej, że odwzorowanie $\varphi\colon X \to Y$ nazywamy *odwzorowaniem na zbiór Y*, gdy $\varphi(X) = Y$, tj. gdy każdy element $y \in Y$ równa się $\varphi(x)$ dla pewnego elementu $x \in X$. Odwzorowanie $\varphi\colon X \to Y$ nazywamy *różnowartościowym*, gdy dla dowolnych dwóch różnych elementów $x_1, x_2 \in X$ wartości $\varphi(x_1)$ i $\varphi(x_2)$ też są różne. Odwzorowanie $\varphi\colon X \to Y$ nazywamy *wzajemnie jednoznacznym* (lub *odwracalnym*), gdy jest to różnowartościowe odwzorowanie X na Y. Każde wzajemnie jednoznaczne odwzorowanie $\varphi\colon X \to Y$ ma *odwzorowanie odwrotne* $\varphi^{-1}\colon Y \to X$ przekształcające w sposób wzajemnie jednoznaczny zbiór Y na X i jednoznacznie scharakteryzowane równością $\varphi^{-1}\varphi(x) = x$ dla każdego $x \in X$ ($\varphi^{-1}\varphi$ jest wtedy *przekształceniem identycznościowym* zbioru X) i $\varphi\varphi^{-1}(y) = y$, dla każdego $y \in Y$ ($\varphi\varphi^{-1}$ jest wtedy przekształceniem identycznościowym zbioru Y). Odwrotnie, jeśli dla danego odwzorowania $\varphi\colon X \to Y$ istnieje odwzorowanie $\psi\colon Y \to X$ o tej własności, że $\varphi\psi$ i $\psi\varphi$ są odwzorowaniami identycznościowymi odpowiednio zbiorów Y oraz X, to φ jest odwzorowaniem wzajemnie jednoznacznym i $\psi = \varphi^{-1}$. Przekształcenia identycznościowe

będziemy też czasem nazywać *przekształceniami tożsamościowymi* lub krócej *identycznościami* albo *tożsamościami*.

W dalszym ciągu będziemy w miarę potrzeby korzystać i z innych pojęć oraz oznaczeń zaczerpniętych z teorii zbiorów. Będziemy to czasem czynić bez dokładnych omówień użytych terminów i symboli zakładając, że czytelnik równocześnie poznaje podstawy teorii zbiorów w oparciu o książkę H. Rasiowej, *Wstęp do matematyki współczesnej* [R].

Niech A będzie zbiorem. Każdą funkcję określoną na zbiorze A o wartościach w zbiorze A nazywamy *działaniem jednoargumentowym*. Przykładem działania jednoargumentowego określonego w zbiorze liczb wymiernych Q (lub w zbiorze liczb rzeczywistych R) jest funkcja, która każdej liczbie x przyporządkowuje liczbę $-x$ (lub np. liczbę x^3+x+1). Przykładem działania jednoargumentowego określonego w zbiorze różnych od zera liczb wymiernych (lub w zbiorze różnych od zera liczb rzeczywistych) jest funkcja, która każdej różnej od zera liczbie x przyporządkowuje liczbę $1/x$ (lub np. liczbę x^3+x+1/x).

Mówimy, że w zbiorze A określiliśmy *parę elementów*, jeśli wyróżniliśmy dwa elementy tego zbioru i wskazaliśmy, który z nich uważamy za pierwszy. Jeśli wyróżniliśmy elementy $a, b \in A$ i a uważamy za pierwszy element, to parę tę oznaczamy symbolem (a, b). Jeśli więc $a \neq b$, to pary (a, b) i (b, a) są *różne*, gdyż pierwszym elementem pary (a, b) jest element a, pierwszym zaś elementem pary (b, a) jest element b. Może się zdarzyć, że oba elementy pary są równe.

Przypuśćmy, że każdej parze elementów zbioru A jest przyporządkowany, przez jakieś prawo, pewien element należący do zbioru A. Mówimy wówczas, że w A jest określone *przekształcenie dwuargumentowe* (lub *funkcja dwuargumentowa*) o wartościach w zbiorze A lub że w A określone jest *działanie dwuargumentowe*. Działania dwuargumentowe nazywać będziemy krótko *działaniami* i oznaczać zwykle symbolami $+$, $\cdot$, $-$, $\circ$, $\square$, $\odot$ itp. Działanie oznaczone przez $\cdot$ nazywać będziemy najczęściej *mnożeniem*, oznaczone przez $+$ *dodawaniem*, oznaczone przez $-$ *odejmowaniem*, a oznaczone przez : (lub przez /) *dzieleniem*.

Element przyporządkowany parze elementów przez dane działanie nazywa się wynikiem działania na tej parze. Wynik działania $\circ$ ($\cdot$, $+$, $\square$ itp.) na parze (x, y) oznaczamy symbolem $x \circ y$ ($x \cdot y$, $x+y$, $x \square y$ itd.). Wynik mnożenia nazywamy *iloczynem*, dodawania *sumą*, odejmowania *różnicą*, a dzielenia *ilorazem*. Zamiast $x \cdot y$ pisać będziemy często xy.

Przykłady. 1. Niech Q będzie zbiorem liczb wymiernych, a R niech będzie zbiorem liczb rzeczywistych. W zbiorach Q i R możemy określić działania przyporządkowując parze (x, y) elementów zbioru Q lub R ich sumę określoną w zwykły sposób. Otrzymane tak działanie w zbiorze Q nazywamy *zwykłym* (lub *arytmetycznym*) *dodawaniem liczb wymiernych*, a otrzymane tak działanie w zbiorze R nazywamy *zwykłym* (lub *arytmetycznym*) *dodawaniem liczb rzeczywistych*. Przyporządkowując każdej parze liczb wymiernych (lub rzeczywistych) ich zwykły iloczyn otrzymujemy inne działanie nazywane *zwykłym* (lub *arytmetycznym*) *mnożeniem*

liczb wymiernych (odpowiednio: *rzeczywistych*). Natomiast zwykłe dzielenie nie jest działaniem określonym ani w zbiorze Q, ani w zbiorze R, gdyż nie każdej parze elementów zbioru Q można przyporządkować ich iloraz (dzielenie nie jest wykonalne, gdy dzielnik jest zerem). Zwykłe dzielenie jest działaniem określonym w zbiorze liczb wymiernych (i w zbiorze liczb rzeczywistych) różnych od zera.

2. Niech R będzie zbiorem liczb rzeczywistych. Wzór $\sin(x+y)$ określa działanie w R przyporządkowujące dowolnym dwom liczbom sinus ich sumy. Natomiast wzór $\sqrt{x+y}$ nie określa działania, gdyż nie przyporządkowuje każdej parze liczb rzeczywistych x, y liczby rzeczywistej. W przypadku gdy $x+y<0$, wyrażenie $\sqrt{x+y}$ nie ma wartości rzeczywistej.

3. Działaniu w zbiorze skończonym A można przyporządkować tabelkę wypisując dwukrotnie elementy zbioru A: raz w pierwszym rzędzie poziomym i raz w pierwszym rzędzie pionowym, a następnie wpisując na przecięciu rzędu poziomego odpowiadającego elementowi a i rzędu pionowego odpowiadającego elementowi b wynik omawianego działania na parze (a, b). Odwrotnie, każda tabelka, która w pierwszym rzędzie poziomym i pierwszym rzędzie pionowym zawiera wszystkie elementy danego skończonego zbioru A napisane tylko jeden raz, a na pozostałych miejscach ma wpisane w dowolny sposób pewne elementy ze zbioru A, określa w A działanie. Wynikiem tego działania na parze (a, b) jest element stojący w rzędzie poziomym odpowiadającym a i rzędzie pionowym odpowiadającym b. Na przykład, jeśli K składa się z liczb 0, 1, to następująca tabelka określa działanie w zbiorze K:

	0	1
0	0	0
1	0	1

Niepusty zbiór, z wyróżnionym skończonym układem działań określonych w tym zbiorze oraz wyróżnionym skończonym układem elementów, nazywamy *systemem algebraicznym.*

Zarówno układ działań, jak i układ wyróżnionych elementów systemu algebraicznego mogą być puste. Wobec tego zarówno dowolny niepusty zbiór, w którym nie określiliśmy żadnych działań i nie wyróżniliśmy żadnego elementu, jak i niepusty zbiór z wyróżnionym jednym elementem (ale z pustym układem działań) są systemami algebraicznymi. Z drugiej strony, dowolny zbiór skończony z układem wszystkich działań określonych na tym zbiorze (jest ich skończenie wiele!) i wyróżnionym układem wszystkich swoich elementów jest systemem algebraicznym. Wynika stąd, że pojęcie systemu algebraicznego jest bardzo szerokie, obejmuje wiele przykładów, a wśród nich przykłady mało interesujące bądź bardzo dziwaczne. W algebrze podstawową rolę grają następujące trzy systemy algebraiczne:

(a) *zbiór* Q wszystkich liczb wymiernych ze zwykłymi działaniami $+$ i $\cdot$ oraz z wyróżnionymi elementami liczbą zero i liczbą jeden.

(b) *zbiór* Z wszystkich liczb całkowitych ze zwykłymi działaniami $+$ i $\cdot$ oraz z wyróżnionymi elementami liczbą zero i liczbą jeden.

(c) zbiór S_A wszystkich wzajemnie jednoznacznych przekształceń zbioru A na siebie ze składaniem przekształceń jako działaniem mnożenia oraz z wyróżnionym przekształceniem identycznościowym.

System (a) nazywamy *ciałem liczb wymiernych*, system (b) *pierścieniem liczb całkowitych*, a system (c) *grupą symetryczną zbioru* A. Biorąc za wzorcowy którykolwiek z tych systemów, określa się pewien typ systemów algebraicznych, których pewne ogólne i z pewnego punktu widzenia najistotniejsze własności są takie same jak własności systemu wyjściowego. W ten sposób dochodzi się do trzech podstawowych pojęć współczesnej algebry: pojęcia ciała, pojęcia pierścienia i pojęcia grupy.

Pojęcia działania jedno- i dwuargumentowego można uogólnić w następujący sposób. Niech n będzie dowolną liczbą naturalną. *Działaniem* n*-argumentowym* określonym w zbiorze A nazywamy dowolną funkcję o wartościach w zbiorze A określoną na zbiorze wszystkich n-elementowych ciągów o elementach ze zbioru A. W przypadkach gdy $n = 1$ oraz $n = 2$, otrzymujemy w szczególności wprowadzone poprzednio definicje działań jedno- i dwuargumentowych (gdyż każdy element a można utożsamić z ciągiem jednoelementowym, którego jedynym elementem jest a, a każdą parę (a, b) z dwuelementowym ciągiem, którego pierwszym elementem jest a, natomiast drugim b). *Działaniem wieloargumentowym* nazywamy każde działanie n-argumentowe (tak więc działanie jednoargumentowe jest działaniem wieloargumentowym).

Niepusty zbiór, z wyróżnionym skończonym układem działań wieloargumentowych określonych w tym zbiorze oraz skończonym układem wyróżnionych elementów nazywamy *algebrą abstrakcyjną*. To bardzo szerokie pojęcie obejmuje w szczególności zdefiniowane poprzednio pojęcie systemu algebraicznego. W dalszym ciągu książki będziemy ograniczać rozważania do systemów algebraicznych, gdyż wszystkie algebry abstrakcyjne, które będziemy dalej rozpatrywać: ciała, pierścienie, grupy, są systemami algebraicznymi. Wszystkie dalej wprowadzone pojęcia i udowodnione twierdzenia dotyczące systemów algebraicznych łatwo można uogólnić na dowolne algebry abstrakcyjne.

ZADANIA

1. Czy w każdym niepustym zbiorze można określić pewne działanie?

Odpowiedź. Tak.

2. Ile różnych działań można określić w dowolnym zbiorze zawierającym tylko jeden element?

Odpowiedź. Tylko jedno.

§ 2. Własności działań

Załóżmy, że w zbiorze A określono działanie $\circ$. Działanie to nazywamy

(a) *przemiennym*, jeśli $x \circ y = y \circ x$ dla dowolnych elementów x, y należących do A,

(b) *łącznym*, jeśli $(x \circ y) \circ z = x \circ (y \circ z)$ dla dowolnych elementów x, y, z należących do A.

Niemal wszystkie ważniejsze działania, z którymi będziemy się stykali, będą łączne, nie zawsze jednak będą one przemienne.

Jeśli działanie $\circ$ jest łączne, to wynik tego działania na układzie elementów $a_1, \ldots, a_n$ zbioru A nie zależy od rozmieszczenia nawiasów. Na przykład,

$$(a_1 \circ (a_2 \circ a_3)) \circ a_4 = (a_1 \circ a_2) \circ (a_3 \circ a_4) = a_1 \circ (a_2 \circ (a_3 \circ a_4)) =$$
$$= a_1 \circ ((a_2 \circ a_3) \circ a_4) = ((a_1 \circ a_2) \circ a_3) \circ a_4.$$

Pozwala to na pomijanie nawiasów i używanie zapisu $a_1 \circ \ldots \circ a_n$ dla dowolnej liczby naturalnej n. Jeśli ponadto działanie $\circ$ jest przemienne, to wynik nie zależy od kolejności ustawienia elementów $a_1, \ldots, a_n$. Na przykład, $a_1 \circ a_2 \circ a_3 = a_3 \circ a_2 \circ a_1$.

Element $i \in A$ nazywamy *elementem neutralnym działania* $\circ$, gdy $i \circ a = a \circ i = a$ dla każdego elementu $a \in A$. Zauważmy, że *działanie może mieć co najwyżej jeden element neutralny*. Istotnie, jeśli elementy i oraz j są elementami neutralnymi działania $\circ$, to $i = i \circ j = j$.

Jeśli działanie $\circ$ określone w zbiorze A ma element neutralny i oraz $a \in A$, to element $b \in A$ nazywamy *przeciwnym do* a (ze względu na działanie $\circ$), gdy $a \circ b = b \circ a = i$. Wobec tego jeśli b jest elementem przeciwnym do a, to a jest elementem przeciwnym do b (i odwrotnie). Element przeciwny do elementu a nazywamy *elementem odwrotnym* elementu a (lub *odwrotnością* elementu a), gdy rozpatrywane działanie nazywamy mnożeniem. Jeśli działanie $\circ$ jest łączne, to element $a \in A$ może mieć co najwyżej jeden element przeciwny. Istotnie, jeśli elementy $b_1, b_2 \in A$ są przeciwne do a, to $b_1 = b_1 \circ i = b_1 \circ (a \circ b_2) = (b_1 \circ a) \circ b_2 = i \circ b_2 = b_2$. Jeśli działanie $\circ$ jest przemienne, a i jest elementem neutralnym tego działania, to element b jest elementem przeciwnym elementu a (ze względu na $\circ$) wtedy i tylko wtedy, gdy $a \circ b = i$.

Załóżmy, że prócz działania $\circ$ w zbiorze A jest określone jeszcze działanie $\square$, na ogół rzecz biorąc, różne od $\circ$. Mówimy, że działanie $\square$ jest

(c) *rozdzielne lewostronnie względem* $\circ$, jeśli $x \square (y \circ z) = (x \square y) \circ (x \square z)$ dla dowolnych elementów x, y, z należących do A.

Podobnie określamy rozdzielność prawostronną: działanie $\square$ jest *rozdzielne prawostronnie względem* $\circ$, jeśli $(y \circ z) \square x = (y \square x) \circ (z \square x)$ dla dowolnych $x, y, z \in A$.

W przypadku gdy działanie $\square$ jest przemienne, wówczas rozdzielność lewostronna jest równoważna rozdzielności prawostronnej. Jeśli działanie $\square$ jest rozdzielne prawostronnie i lewostronnie względem działania $\circ$, to mówimy krócej, że działanie $\square$ jest *rozdzielne względem działania* $\circ$.

PRZYKŁADY. 1. W zbiorze liczb całkowitych różnych od 0 określmy działanie przyporządkowując każdej parze liczb całkowitych a i b ich *największy wspólny dzielnik* NWD(a, b), tzn. taką liczbę naturalną n, która jest wspólnym dzielnikiem