Literatura:

1. R.R.Andruszkiewicz, ,,Wykłady z algebry ogólnej I", Wydawnictwo UwB, Białystok 2005.

2. Cz. Bagiński, ,,Wstęp do teorii grup", Wydawnictwo Script, Warszawa 2002.

3. M. Bryński i J. Jurkiewicz, ,,Zbiór zadań z algebry", PWN, Warszawa 1978.

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

5. J. Rutkowski, ,,Algebra abstrakcyjna w zadaniach", PWN, Warszawa 2006.

Oznaczenia:

Dodatnie liczby całkowite nazywamy liczbami naturalnymi. Zbiór wszystkich liczb naturalnych oznaczamy symbolem $\mathbb{N}$. Zatem $\mathbb{N} = \{1, 2, 3, \ldots\}$. Ponadto $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$.

Dla $m \in \mathbb{N}$ i liczby całkowitej a przez $[a]_m$ oznaczamy resztę z dzielenia a przez m.

UWAGA! Ten wykład opiera się bardzo mocno na znajomości Elementarnej teorii liczb! Będziemy też wykorzystywali wiedzę z Algebry liniowej i troszkę wiedzy z geometrii elementarnej ze szkoły średniej.

Wykład 1
Pojęcie grupy

Definicja 1.1. *Działaniem* w niepustym zbiorze A nazywamy każde odwzorowanie zbioru $A \times A$ w zbiór A. Jeżeli $\circ$ jest działaniem w zbiorze A i $a, b \in A$, to $\circ((a, b))$ oznaczamy przez $a \circ b$ i nazywamy *wynikiem działania* $\circ$ na parze (a, b).

Działania będziemy oznaczali symbolami: $\circ$, $\cdot$, $+$, $\oplus$, itd.

Definicja 1.2. *Systemem algebraicznym* nazywamy układ postaci $(A,\circ_1, \ldots ,\circ_n, e_1, \ldots, e_k)$, w którym A jest niepustym zbiorem, $\circ_1, \ldots, \circ_n$ są działaniami w A oraz $e_1, \ldots, e_k \in A$ są wyróżnionymi elementami zbioru A.

Działaniu w zbiorze skończonym A można przyporządkować tabelkę

$\circ$	a	b	c	$\ldots$
a	$a \circ a$	$a \circ b$	$a \circ c$	$\ldots$
b	$b \circ a$	$b \circ b$	$b \circ c$	$\ldots$
c	$c \circ a$	$c \circ b$	$c \circ c$	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

wpisując w lewym górnym rogu oznaczenie działania i 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 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. Wynika stąd w szczególności, że w zbiorze n-elementowym można określić dokładnie n^{n^2} różnych działań.

Zagadka 1. Wypisz tabelki wszystkich działań w zbiorze dwuelementowym $A = \{0, 1\}$.

Zagadka 2. Załóżmy, że potrafimy wypisać jedną tabelkę działania w zbiorze 3-elementowym A w ciągu 10 sekund. Ile czasu zajmie nam wypisanie tabelek wszystkich działań w tym zbiorze?

Niech $\circ$ będzie działaniem w zbiorze A. Powiemy, że
(1) działanie $\circ$ jest *łączne*, jeżeli $\forall_{a,b,c\in A}\ (a \circ b) \circ c = a \circ (b \circ c)$,

(2) działanie $\circ$ jest *przemienne*, jeżeli $\forall_{a,b\in A}\ a\circ b = b\circ a$,
(3) $e\in A$ jest *elementem neutralnym* działania $\circ$, jeżeli $\forall_{a\in A}\ e\circ a = a\circ e = a$.

Zagadka 3. Czy działanie $\circ$ w zbiorze $\mathbb{N}$ dane wzorem $a\circ b = a^b$ jest łączne? Czy $\circ$ jest przemienne? Czy $\circ$ posiada element neutralny?

Zagadka 4. Jak na podstawie tabelki działania w zbiorze skończonym rozpoznać element neutralny tego działania?

Twierdzenie 1.3. Jeżeli $\circ$ jest działaniem łącznym w zbiorze A, to wynik tego działania na układzie elementów $a_1, a_2, \ldots, a_n \in A$ nie zależy od sposobu rozstawienia nawiasów.

Dowód. Zastosujemy indukcję względem n przy dowolnych $a_1, \ldots, a_n \in A$. Dla $n = 1$ przyjmijmy formalnie, że wynik działania $\circ$ na układzie a_1 jest równy a_1. Dla $n = 2$ teza też zachodzi, bo mamy tylko jedną możliwość: $a_1 \circ a_2$. Dla $n = 3$ mamy dwie możliwości rozstawienia nawiasów w układzie a_1, a_2, a_3: $a_1 \circ (a_2 \circ a_3)$ i $(a_1 \circ a_2) \circ a_3$, które prowadzą do tego samego wyniku na mocy łączności działania $\circ$ i ten wynik oznaczymy przez $a_1 \circ a_2 \circ a_3$.

Niech teraz $n > 3$ będzie taką liczbą naturalną, że dla każdego naturalnego $k < n$ wynik działania $\circ$ na dowolnych elementach $x_1, \ldots, x_k \in A$ nie zależy od sposobu nawiasów i jego wartość oznaczmy symbolem $x_1 \circ \ldots \circ x_k$. Weźmy dowolne $a_1, a_2, \ldots, a_n \in A$. Niech a będzie wynikiem działania $\circ$ na układzie elementów $a_1, a_2, \ldots, a_n$ przy pewnym rozstawieniu nawiasów. Jeśli w tym rozstawieniu nawiasów za elementem a_n z prawej strony stoi nawias), to $a = b \circ (... \circ a_n)...)$, gdzie b jest wynikiem działania $\circ$ na układzie $a_1, \ldots, a_k$ dla pewnego naturalnego $k < n-1$, zaś $c = (... \circ a_n)...)$ jest wynikiem działania $\circ$ na układzie $a_{k+1}, \ldots, a_n$. Zatem na mocy założenia indukcyjnego i łączności działania $\circ$ mamy, że $a = b \circ ((a_{k+1} \circ \ldots \circ a_{n-1}) \circ a_n) = (b \circ (a_{k+1} \circ \ldots \circ a_{n-1})) \circ a_n = (a_1 \circ \ldots \circ a_{n-1}) \circ a_n$. Jeśli zaś za elementem a_n nie ma nawiasu), to $a = c \circ a_n$, gdzie c jest wynikiem działania $\circ$ na układzie $a_1, \ldots, a_{n-1}$ przy pewnym rozstawieniu nawiasów. Zatem z założenia indukcyjnego c nie zależy od sposobu rozstawienia nawiasów, więc $c = a_1 \circ \ldots \circ a_{n-1}$ i $a = (a_1 \circ \ldots \circ a_{n-1}) \circ a_n$. Kończy to dowód tego, że wynik działania $\circ$ na układzie elementów $a_1, a_2, \ldots, a_n$ nie zależy od sposobu rozstawienia nawiasów. $\square$

Twierdzenie 1.3 pozwala na pomijanie nawiasów dla działania łącznego $\circ$ i używanie zapisu $a_1 \circ a_2 \circ \ldots \circ a_n$ dla dowolnej liczby naturalnej n. Ponadto wówczas dla $a \in A$ i $n \in \mathbb{N}$ możemy stosować zapis $a^n = \underbrace{a \circ a \circ \ldots \circ a}_{n}$ (oczywiście $a^1 = a$).

Wniosek 1.4. Jeżeli $\circ$ jest działaniem łącznym w zbiorze A, to dla dowolnego $a \in A$ i dla dowolnych $n, m \in \mathbb{N}$:
(i) $a^n \circ a^m = a^{n+m}$ oraz (ii) $(a^n)^m = a^{nm}$.

Dowód. (i) W zapisie $a^n \circ a^m$ element a występuje dokładnie $n + m$ razy, więc na

mocy Twierdzenia 1.3, $a^n \circ a^m = a^{n+m}$.

(ii) W zapisie $(a^n)^m$ element a^n występuje dokładnie m razy, zaś w zapisie a^n element a występuje dokładnie n razy. Zatem w zapisie $(a^n)^m$ element a występuje dokładnie nm razy, więc na mocy Twierdzenia 1.3, $(a^n)^m = a^{nm}$. $\square$

Wniosek 1.5. Niech $\circ$ będzie działaniem łącznym w zbiorze A i niech $a, b \in A$ będą takie, że $a \circ b = b \circ a$. Wtedy dla dowolnych $m, n \in \mathbb{N}$:

(i) $a \circ b^m = b^m \circ a$, (ii) $a^n \circ b^m = b^m \circ a^n$, (iii) $(a \circ b)^n = a^n \circ b^n$.

Dowód. (i). Stosujemy indukcję względem m. Dla $m = 1$ teza wynika wprost z założenia. Załóżmy, że dla pewnego $m \in \mathbb{N}$ jest $a \circ b^m = b^m \circ a$. Wtedy na mocy Wniosku 1.4, $b^{m+1} = b^m \circ b$, więc na mocy łączności $\circ$ i założenia indukcyjnego, $a \circ b^{m+1} = (a \circ b^m) \circ b = (b^m \circ a) \circ b = b^m \circ (a \circ b) = b^m \circ (b \circ a) = (b^m \circ b) \circ a = b^{m+1} \circ a$. Zatem teza zachodzi dla liczby $m + 1$.

(ii). Wynika od razu z (i). (iii). Stosujemy indukcję względem n. Dla $n = 1$ teza jest oczywista. Załóżmy, że teza zachodzi dla pewnego $n \in \mathbb{N}$. Wtedy na mocy Twierdzenia 1.3 i założenia indukcyjnego oraz (i), $(a \circ b)^{n+1} = (a \circ b)^n \circ (a \circ b) = a^n \circ b^n \circ a \circ b = a^n \circ a \circ b^n \circ b = a^{n+1} \circ b^{n+1}$, czyli teza zachodzi dla liczby $n + 1$. $\square$

Zagadka 5. Spośród działań z zagadki 1 wypisz wszystkie działania
(a) łączne, (b) przemienne, (c) posiadające element neutralny.

Uwaga 1.6. Łatwo zauważyć, że działanie w zbiorze skończonym jest przemienne wtedy i tylko wtedy, gdy jego tabelka jest symetryczna względem głównej przekątnej. W szczególności w zbiorze n-elementowym istnieje dokładnie $n^{\frac{n(n+1)}{2}}$ różnych działań przemiennych.

Uwaga 1.7. Każde działanie w zbiorze A może posiadać co najwyżej jeden element neutralny. Rzeczywiście, niech e i f będą elementami neutralnymi działania $\circ$ w zbiorze A. Wtedy w szczególności $e \circ a = a$ oraz $b \circ f = b$ dla dowolnych $a, b \in A$. Podstawiając $a = f$ i $b = e$ uzyskamy stąd, że $e \circ f = f$ i $e \circ f = e$, skąd $e = f$.

Definicja 1.8. *Grupą* nazywamy system algebraiczny $(G, \circ, e)$ spełniający następujące warunki (aksjomaty):

(G1.) $\forall_{a,b,c \in G}\ (a \circ b) \circ c = a \circ (b \circ c)$,

(G2.) $\forall_{a \in G}\ e \circ a = a \circ e = a$,

(G3.) $\forall_{a \in G} \exists_{x \in G}\ a \circ x = x \circ a = e$.

Definicja 1.9. Grupę $(G, \circ, e)$ nazywamy *abelową*, jeżeli działanie $\circ$ jest przemienne.

Nazwa *grupa abelowa* pochodzi od nazwiska norweskiego matematyka Nielsa Henrika Abela (1802-1829), który jako pierwszy prowadził systematyczne badania wykorzystujące własności grup przemiennych.

Uwaga 1.10. W dowolnej grupie $(G, \circ, e)$ zachodzą następujące *prawa skracania równości*:
(I) $\forall_{a,b,c\in G}\ [a \circ b = a \circ c \Rightarrow b = c]$ oraz (II) $\forall_{a,b,c\in G}\ [b \circ a = c \circ a \Rightarrow b = c]$.

Rzeczywiście, na mocy **(G3)** istnieje $x \in G$ taki, że $x \circ a = a \circ x = e$, więc jeżeli $a \circ b = a \circ c$, to $x \circ (a \circ b) = x \circ (a \circ c)$, skąd z **(G1)** $(x \circ a) \circ b = (x \circ a) \circ c$, czyli $e \circ b = e \circ c$. Zatem z **(G2)** $b = c$, co dowodzi (I). Dowód (II) jest analogiczny.

Uwaga 1.11. Element x w aksjomacie **(G3)** jest wyznaczony jednoznacznie przez element a, gdyż jeżeli dodatkowo $y \in G$ spełnia warunek $a \circ y = y \circ a = e$, to $a \circ x = a \circ y$, więc z Uwagi 1.10, $x = y$. Ten dokładnie jeden element x nazywamy *elementem odwrotnym (przeciwnym)* do a i oznaczamy przez a^{-1} (przez $-a$, gdy $\circ = +$). Z Uwagi 1.8 wynika od razu, że x jest elementem odwrotnym do a wtedy i tylko wtedy, gdy $a \circ x = e$. Ponieważ $a^{-1} \circ a = e$, więc a jest elementem odwrotnym do a^{-1}, skąd mamy wzór

$$(a^{-1})^{-1} = a \text{ dla każdego } a \in G.$$

Ponadto dla dowolnych $a, b \in G$ zachodzi wzór:

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$

Rzeczywiście, wystarczy zauważyć, że $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$. Z łączności działania $\circ$ mamy $(a \circ b) \circ (b^{-1} \circ a^{-1}) = ((a \circ b) \circ b^{-1}) \circ a^{-1} = (a \circ (b \circ b^{-1})) \circ a^{-1} = (a \circ e) \circ a^{-1} = a \circ a^{-1} = e$.

Przez prostą indukcję uzyskujemy stąd, że dla dowolnej liczby naturalnej n i dla dowolnych elementów $a_1, \ldots, a_n$ grupy G zachodzi wzór:

$$(a_1 \circ a_2 \circ \ldots \circ a_n)^{-1} = a_n^{-1} \circ \ldots \circ a_2^{-1} \circ a_1^{-1}.$$

Uwaga 1.12. Niech $(G, \circ, e)$ będzie grupą i niech $a \in G$. Oznaczmy przez l_a odwzorowanie zbioru G w siebie dane wzorem $l_a(x) = a \circ x$ dla $x \in G$ oraz oznaczmy przez r_a odwzorowanie zbioru G w siebie dane wzorem $r_a(x) = x \circ a$ dla $x \in G$. Pokażemy, że wówczas l_a i r_a są bijekcjami G na G. Z Uwagi 1.10 wynika od razu, że przekształcenia l_a i r_a są różnowartościowe. Ponadto dla każdego $b \in G$ jest $l_a(a^{-1} \circ b) = a \circ a^{-1} \circ b = e \circ b = b$ oraz $r_a(b \circ a^{-1}) = b \circ a^{-1} \circ a = b \circ e = b$, więc przekształcenia l_a i r_a są „na".

Rzędem grupy $(G, \circ, e)$ nazywamy moc zbioru G. Rząd grupy $(G, \circ, e)$ będziemy oznaczali przez $|G|$. Jeśli $|G|$ jest liczbą naturalną, to mówimy, że grupa $(G, \circ, e)$ jest *skończona*. Z Uwagi 1.12 wynika, że jeżeli $(G, \circ, e)$ jest grupą skończoną, to w każdym wierszu i w każdej kolumnie tabelki działania $\circ$ występują wszystkie elementy zbioru G.

Zagadka 6. W oparciu o podane wyżej wiadomości utwórz tabelkę działania $\circ$ w zbiorze 3-elementowym $A = \{a, b, c\}$ wiedząc, że $(A, \circ, a)$ jest grupą.

1 Całkowita potęga elementu grupy

I. Niech $(G, \cdot, e)$ będzie grupą. Wówczas dla $a \in G$, a^{-1} jest elementem odwrotnym do a. Całkowitą potęgę elementu a określamy następująco:
1. $a^0 = e$,
2. $a^1 = a$,
3. $a^{n+1} = a^n \cdot a$ dla $n = 1, 2, \ldots$
4. $a^{-n} = (a^{-1})^n$ dla $n = 1, 2, \ldots$

Zatem dla $n = 1, 2, \ldots$

$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n}.$$

Twierdzenie 1.13. Dla dowolnego elementu a grupy $(G, \cdot, e)$ i dla dowolnych $k, l \in \mathbb{Z}$ zachodzą wzory:

(a) $a^k \cdot a^l = a^{k+l}$, (b) $(a^k)^l = a^{kl}$.

Dowód. (a). Na mocy Wniosku 1.4 wzór (a) zachodzi dla wszystkich $k, l \in \mathbb{N}$. Dla $k = 0$, $a^k \cdot a^l = e \cdot a^l = a^l = a^{k+l}$. Dla $l = 0$, $a^k \cdot a^l = a^k \cdot e = a^k = a^{k+l}$. Jeśli $k, l < 0$, to $k = -n$ i $l = -m$ dla pewnych $m, n \in \mathbb{N}$. Zatem na mocy Wniosku 1.4, $a^k \cdot a^l = a^{-n} \cdot a^{-m} = (a^{-1})^n \cdot (a^{-1})^m = (a^{-1})^{n+m} = a^{-(n+m)} = a^{k+l}$. Pozostaje zatem do rozważenia przypadek, gdy liczby całkowite k i l są różnych znaków. Ale $a \cdot a^{-1} = a^{-1} \cdot a$, więc na mocy Wniosku 1.5 możemy zakładać, że $k > 0$ i $l < 0$. Stąd $l = -m$ dla pewnego $m \in \mathbb{N}$ i $k \in \mathbb{N}$. Jeśli $k = m$, to na mocy Wniosku 1.5, $a^k \cdot a^l = a^k \cdot a^{-k} = a^k \cdot (a^{-1})^k = (a \cdot a^{-1})^k = e^k = e = a^{k+l}$. Jeśli $k > m$, to $a^k \cdot a^l = a^{k-m} \cdot a^m \cdot a^{-m} = a^{k-m} \cdot e = a^{k-m} = a^{k+l}$. W końcu, jeśli $k < m$, to $a^k \cdot a^l = a^k \cdot a^{-k} \cdot a^{-(m-k)} = e \cdot a^{k-m} = a^{k-m} = a^{k+l}$. Kończy to dowód wzoru (a).

(b). Weźmy dowolne ustalone $k \in \mathbb{Z}$. Wtedy $(a^k)^0 = e$ i $a^{k \cdot 0} = a^0 = e$, więc wzór (b) zachodzi dla $l = 0$. Załóżmy, że wzór (b) zachodzi dla pewnego $l \in \mathbb{N}_0$. Stąd i na mocy (a): $(a^k)^{l+1} = (a^k)^l \cdot a^k = a^{kl} \cdot a^k = a^{kl+k} = a^{k(l+1)}$, czyli wzór (b) zachodzi wówczas także dla liczby $l + 1$. Zatem przez indukcję mamy, że wzór (b) zachodzi dla dowolnych $k \in \mathbb{Z}$ i $l \in \mathbb{N}_0$. Dalej, na mocy (a) mamy, że $a^k \cdot a^{-k} = a^{k-k} = a^0 = e$, więc $(a^k)^{-1} = a^{-k}$. Wobec tego dla każdego $n \in \mathbb{N}$: $(a^k)^{-n} = [(a^k)^{-1}]^n = (a^{-k})^n = a^{(-k)n} = a^{k(-n)}$, czyli wzór (b) zachodzi też dla wszystkich całkowitych liczb ujemnych l. Kończy to dowód wzoru (b). □

Twierdzenie 1.14. Niech a, b będą elementami grupy G takimi, że $a \cdot b = b \cdot a$. Wówczas dla dowolnych $k, l \in \mathbb{Z}$ zachodzą wzory:

(a) $a^l \cdot b^k = b^k \cdot a^l$, (b) $(a \cdot b)^k = a^k \cdot b^k$.

Dowód. Mnożąc równość $a \cdot b = b \cdot a$ z lewej strony przez a^{-1}, a następnie mnożąc otrzymaną równość z lewej strony przez a^{-1} uzyskamy, że $b \cdot a^{-1} = a^{-1} \cdot b$. Podobnie pokazujemy, że $a \cdot b^{-1} = b^{-1} \cdot a$ i $a^{-1} \cdot b^{-1} = b^{-1} \cdot a^{-1}$.

(a). Dla $l = 0$, $a^l \cdot b^k = e \cdot b^k = b^k = b^k \cdot e = b^k \cdot a^l$. Podobnie dla $k = 0$, $a^l \cdot b^k = a^l \cdot e = a^l = e \cdot a^l = b^k \cdot a^l$. Ponadto na mocy Wniosku 1.5 wzór (a) zachodzi dla wszystkich $k, l \in \mathbb{N}$. Jeśli $k, l < 0$, to $k = -n$ i $l = -m$ dla pewnych $m, n \in \mathbb{N}$. Zatem na mocy Wniosku 1.5, $a^l \cdot b^k = a^{-n} \cdot b^{-m} = (a^{-1})^m \cdot (b^{-1})^n = (b^{-1})^n \cdot (a^{-1})^m = b^k \cdot a^l$. Jeśli $k < 0$ i $l > 0$, to $k = -n$ dla pewnego $n \in \mathbb{N}$. Ale $a \cdot b^{-1} = b^{-1} \cdot a$, więc na mocy Wniosku 1.5, $a^k \cdot b^l = a^k \cdot (b^{-1})^n = (b^{-1})^n \cdot a^l = b^k \cdot a^l$. W końcu dla $k > 0$ i $l < 0$, $l = -m$ dla pewnego $m \in \mathbb{N}$. Ale $a^{-1} \cdot b = b \cdot a^{-1}$, więc na mocy Wniosku 1.5, $a^l \cdot b^k = (a^{-1})^m \cdot b^k = b^k \cdot (a^{-1})^m = b^k \cdot a^l$.

(b). Dla $k = 0$ nasz wzór zachodzi, bo $(a \cdot b)^0 = e$ i $a^0 \cdot b^0 = e \cdot e = e$. Ponadto na mocy Wniosku 1.5 nasz wzór zachodzi dla $k \in \mathbb{N}$. Jeśli $k < 0$, to $k = -n$ dla pewnego $n \in \mathbb{N}$. Ale $a^{-1} \cdot b^{-1} = b^{-1} \cdot a^{-1}$, więc na mocy Wniosku 1.5 oraz (a), $(a \cdot b)^k = (a \cdot b)^{-n} = ((a \cdot b)^{-1})^n = (b^{-1} \cdot a^{-1})^n = (b^{-1})^n \cdot (a^{-1})^n = b^k \cdot a^k = a^k \cdot b^k$. $\square$

Zapis użyty w **I** nazywamy *multiplikatywnym* (od łacińskiego *mutiplicare* — mnożyć). W tym zapisie często element neutralny e oznacza się przez 1, chociaż nie musi to być liczba naturalna 1.

II. Niech $(G, +, 0)$ będzie grupą. Wówczas dla $a \in G$, $-a$ jest elementem przeciwnym do a. Całkowitą wielokrotność elementu a określamy następująco:

1'. $0 \cdot a = 0$,

2'. $1 \cdot a = a$,

3'. $(n + 1) \cdot a = n \cdot a + a$ dla $n = 1, 2, \ldots$

4'. $(-n) \cdot a = n \cdot (-a)$ dla $n = 1, 2, \ldots$

Taki zapis nazywamy *addytywnym* (od łacińskiego *addere* — dodawać) i z reguły jest on stosowany jedynie w przypadku grup abelowych. W tym zapisie element neutralny grupy jest oznaczany przez 0, chociaż nie musi to być liczba całkowita 0.

Z **I** wynika, że dla dowolnych liczb całkowitych m, n i dla każdego $a \in G$ zachodzą wzory:

$$(1)' \; n \cdot a + m \cdot a = (n + m) \cdot a \text{ oraz } (2)' \; n \cdot (m \cdot a) = (nm) \cdot a.$$

Jeżeli napiszemy *niech G będzie grupą*, to będziemy mieli na myśli grupę multiplikatywną z działaniem oznaczonym kropką, którą — tak jak w przypadku wyrażeń algebraicznych — często będziemy pomijać.

2 Przykłady grup

Przykład 1.15. Niech $G = \{a\}$ będzie dowolnym zbiorem jednoelementowym. W zbiorze tym można określić tylko jedno działanie: $a \cdot a = a$. Wówczas $(G, \cdot, a)$ jest grupą. Nazywamy ją *grupą trywialną*.

Przykład 1.16. Addytywne grupy liczbowe. Tak będziemy nazywać grupy, których elementami są pewne liczby zespolone, a działaniami — zwykłe dodawanie liczb. Najbardziej typowymi przykładami takich grup są: addytywna grupa liczb całkowitych $(\mathbb{Z}, +, 0)$ oznaczana przez $\mathbb{Z}^+$, wymiernych $(\mathbb{Q}, +, 0)$ oznaczana przez $\mathbb{Q}^+$, rzeczywistych $(\mathbb{R}, +, 0)$ oznaczana przez $\mathbb{R}^+$ i zespolonych $(\mathbb{C}, +, 0)$ oznaczana przez $\mathbb{C}^+$.

Przykład 1.17. Multiplikatywne grupy liczbowe. Elementami takich grup są pewne niezerowe liczby zespolone, natomiast działaniem — zwykłe mnożenie liczb. Wśród nich najbardziej typowymi są:

$$(\{-1, 1\}, \cdot, 1),\ (\mathbb{Q}^*, \cdot, 1),\ (\mathbb{R}^*, \cdot, 1),\ (\mathbb{C}^*, \cdot, 1),\ (\mathbb{C}_n, \cdot, 1),\ (\mathbb{C}_\infty, \cdot, 1),$$

gdzie $K^* = K \setminus \{0\}$ dla $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, natomiast $\mathbb{C}_n$ jest zbiorem wszystkich zespolonych pierwiastków stopnia n z 1, tzn.

$$\mathbb{C}_n = \{\cos \tfrac{2k\pi}{n} + i \sin \tfrac{2k\pi}{n} :\ k = 0, 1, \ldots, n-1\}$$

i wreszcie $\mathbb{C}_\infty = \bigcup_{n=1}^{\infty} \mathbb{C}_n$. Z algebry liniowej wiemy, że $|\mathbb{C}_n| = n$. Ważnym przykładem z punktu widzenia klasyfikacji grup abelowych są grupy $\mathbb{C}_{p^\infty} = \bigcup_{n=1}^{\infty} \mathbb{C}_{p^n}$, dla liczb pierwszych p.

Przykład 1.18. Jeżeli V jest przestrzenią liniową nad ciałem K, to V z dodawaniem wektorów $+$ i wyróżnionym elementem θ (wektor zerowy) tworzy grupę abelową $(V, +, \theta)$. Stąd mamy np. grupy $(K^n, +, \theta)$ dla $n = 1, 2, \ldots$.

Przykład 1.19. Jeżeli K jest ciałem, to $(K \setminus \{0\}, \cdot, 1)$ tworzy grupę abelową. Nazywamy ją grupą multiplikatywną ciała K i oznaczamy przez K^*.

Przykład 1.20. Addytywna grupa reszt modulo m. Niech m będzie dowolną liczbą naturalną i niech $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$. W zbiorze $\mathbb{Z}_m$ określamy *dodawanie modulo* m, $\oplus_m$ przyjmując, że dla dowolnych $a, b \in \mathbb{Z}_m$:

$$a \oplus_m b = \text{reszta z dzielenia } a + b \text{ przez } m.$$

W oparciu o własności kongruencji łatwo wykazać, że $(\mathbb{Z}_m, \oplus_m, 0)$ jest grupą abelową i $|\mathbb{Z}_m| = m$. Grupę tę będziemy oznaczali przez $\mathbb{Z}_m^+$.

Przykład 1.21. Multiplikatywna grupa reszt modulo m. Przy oznaczeniach Przykładu 1.20 niech

$$\mathbb{Z}_m^* = \{k \in \mathbb{Z}_m :\ NWD(k, m) = 1\}.$$

W zbiorze $\mathbb{Z}_m^*$ określamy *mnożenie modulo* m, $\odot_m$ przyjmując, że dla dowolnych $a, b \in \mathbb{Z}_m^*$:

$$a \odot_m b = \text{reszta z dzielenia } a \cdot b \text{ przez } m.$$

W oparciu o elementarną teorię liczb można łatwo wykazać, że dla $m > 1$, $(\mathbb{Z}_m^*, \odot_m, 1)$ tworzy grupę abelową. Grupę tę będziemy oznaczali przez $\mathbb{Z}_m^*$. Z elementarnej teorii liczb wiadomo, że $|\mathbb{Z}_m^*| = \varphi(m)$, gdzie φ jest funkcją Eulera.

Przykład 1.22. Niech K będzie ciałem i niech $n \in \mathbb{N}$ oraz niech $GL_n(K)$ oznacza zbiór wszystkich odwracalnych macierzy kwadratowych stopnia n nad K. Wówczas z algebry liniowej wiadomo, że macierz kwadratowa A stopnia n nad K należy do $GL_n(K)$ wtedy i tylko wtedy, gdy $\det(A) \neq 0$. Stąd łatwo wyprowadzić (przy pomocy twierdzenia Cauchy'ego), że $GL_n(K)$ ze zwykłym mnożeniem macierzy i macierzą jednostkową I_n tworzy grupę. Oznaczamy ją przez $GL_n(K)$. Dla $n \geqslant 2$ ta grupa nie jest abelowa. Rzeczywiście, niech A oznacza macierz, która ma jedynkę na głównej przekątnej oraz na drugim miejscu w pierwszym wierszu, a na pozostałych miejscach same zera i niech B oznacza macierz, która ma same jedynki na głównej przekątnej oraz na drugim miejscu w pierwszej kolumnie. Wtedy $\det(A) = \det(B) = 1$, więc $A, B \in GL_n(K)$. Ale $A \cdot B \neq B \cdot A$, gdyż macierze $A \cdot B$ i $B \cdot A$ mają inne elementy stojące w lewym górnym rogu.

Przykład 1.23. Niech X będzie dowolnym niepustym zbiorem. Oznaczmy przez $S(X)$ zbiór wszystkich bijekcji $f : X \longrightarrow X$. Niech $\circ$ oznacza składanie przekształceń w $S(X)$, tzn. dla $f, g \in S(X)$ i $x \in X$: $(f \circ g)(x) = f(g(x))$. Niech ponadto id_X oznacza przekształcenie tożsamościowe zbioru X na siebie. Ze wstępu do matematyki wynika, że wówczas $(S(X), \circ, id_X)$ tworzy grupę. Nazywamy ją *grupą symetryczną* zbioru X i oznaczamy przez $S(X)$. Można wykazać, że jeśli zbiór X ma co najmniej 3 elementy, to grupa $S(X)$ nie jest abelowa. Jeżeli $X = \{1, 2, \ldots, n\}$, to zamiast $S(\{1, 2, \ldots, n\})$ piszemy S_n i S_n nazywamy *grupą permutacji* zbioru n-elementowego. Oczywiście $|S_n| = n!$.

Przykład 1.24. Izometrią płaszczyzny Π nazywamy każde odwzorowanie Π na Π zachowujące odległość punktów. Jeżeli $F \subseteq \Pi$, to izometrią własną figury F nazywamy taką izometrię f płaszczyzny Π, że $f(F) = F$. Niech $\circ$ oznacza składanie przekształceń i niech I będzie przekształceniem tożsamościowym Π na siebie. Wówczas dla każdej figury $F \subseteq \Pi$ zbiór $\mathbb{I}(F)$ wszystkich izometrii własnych figury F tworzy grupę ze względu na składanie przekształceń z wyróżnionym elementem id_Π. Dla $n = 3, 4, \ldots$ przez D_n będziemy oznaczali grupę izometrii własnych n-kąta foremnego. Łatwo zauważyć, że $|D_n| = 2n$ oraz grupa D_n nie jest abelowa. Ponadto grupa $\mathbb{I}(\Pi)$ jest nieskończona i nie jest abelowa.

(a) **Grupa izometrii własnych trójkąta równobocznego.** Niech będzie dany na płaszczyźnie trójkąt równoboczny ABC. Oznaczmy przez a symetralną odcinka BC, przez b-symetralną odcinka AC, przez c-symetralną odcinka AB i przez O punkt przecięcia tych trzech prostych (czyli środek ciężkości tego trójkąta). Ponieważ izo-

metrie własne figury geometrycznej zachowują wierzchołki tej figury oraz dwie izometrie płaszczyzny przyjmujące te same wartości w trzech niewspółliniowych punktach są równe, więc grupa D_3 izometrii własnych trójkąta równobocznego ABC ma rząd 6 oraz $D_3 = \{e, S_a, S_b, S_c, O_1, O_2\}$, gdzie S_a jest symetrią osiową względem prostej a, S_b jest symetrią osiową względem prostej b, S_c jest symetrią osiową względem prostej c, O_1 jest obrotem względem punktu O o kąt 120 stopni, zaś O_2 jest obrotem wokół punktu O o kąt 240 stopni. Nietrudno sprawdzić, że tabelka składania przekształceń w grupie D_3 wygląda następująco:

$\circ$	e	S_a	S_b	S_c	O_1	O_2
e	e	S_a	S_b	S_c	O_1	O_2
S_a	S_a	e	O_1	O_2	S_b	S_c
S_b	S_b	O_2	e	O_1	S_c	S_a
S_c	S_c	O_1	O_2	e	S_a	S_b
O_1	O_1	S_c	S_a	S_b	O_2	e
O_2	O_2	S_b	S_c	S_a	e	O_1

(b) **Grupa czwórkowa Kleina.** Niech dany będzie na płaszczyźnie prostokąt $ABCD$ nie będący kwadratem. Niech a będzie symetralną odcinka AB i niech b będzie symetralną odcinka BC oraz niech O będzie punktem przecięcia się prostych a i b. Rozumując podobnie jak w przykładzie (a) można wykazać, że grupa K izometrii własnych prostokąta $ABCD$ ma rząd 4 i $K = \{e, S_a, S_b, S_O\}$, gdzie S_a jest symetrią osiową względem prostej a, S_b jest symetrią osiową względem prostej b, zaś S_O jest symetrią środkową względem punktu O. Tabelka składania przekształceń w grupie K wygląda następująco:

$\circ$	e	S_a	S_b	S_O
e	e	S_a	S_b	S_O
S_a	S_a	e	S_O	S_b
S_b	S_b	S_O	e	S_a
S_O	S_O	S_b	S_a	e

Otrzymaną w ten sposób grupę K nazywamy **grupą czwórkową Kleina** lub grupą izometrii własnych prostokąta nie będącego kwadratem i oznaczamy przez K.

(c) **Grupa izometrii własnych kwadratu.** Niech będzie dany na płaszczyźnie kwadrat $ABCD$. Rozumując podobnie jak w przykładzie (a) można wykazać, że grupa D_4 izometrii własnych kwadratu ma rząd 8 i $D_4 = \{e, S_1, S_2, S_3, S_4, O_1, P_2, P_3\}$, gdzie S_1 jest symetrią osiową względem prostej AC, S_2 jest symetrią osiową względem prostej BD, S_3 jest symetrią osiową względem symetralnej odcinka AB, S_4 jest symetrią osiową względem symetralnej odcinka BC, O_1, O_2 i O_3 są obrotami wokół środka tego kwadratu o kąty odpowienio równe 90, 180 i 270 stopni. Nietrudno sprawdzić, że tabelka składania przekształceń w grupie D_4 wygląda następująco:

$\circ$	e	S_1	S_2	S_3	S_4	O_1	O_2	O_3
e	e	S_1	S_2	S_3	S_4	O_1	O_2	O_3
S_1	S_1	e	O_2	O_3	O_1	S_4	S_2	S_3
S_2	S_2	O_2	e	O_1	O_3	S_3	S_1	S_4
S_3	S_3	O_1	O_3	e	O_2	S_1	S_4	S_2
S_4	S_4	O_3	O_1	O_2	e	S_2	S_3	S_1
O_1	O_1	S_3	S_4	S_2	S_1	O_2	O_3	e
O_2	O_2	S_2	S_1	S_4	S_3	O_3	e	O_1
O_3	O_3	S_4	S_3	S_1	S_2	e	O_1	O_2

Przykład 1.25. Grupa kwaternionów. Niech $Q_8 = \{e, -e, i, -i, j, -j, k, -k\}$ będzie podzbiorem zbioru $M_2(\mathbb{C})$, gdzie

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},\ j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\ k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}. \tag{1}$$

Łatwo zauważyć, że każda z macierzy należących do Q_8 ma wyznacznik równy 1. Wobec tego $Q_8 \subseteq GL_2(\mathbb{C})$. Proste sprawdzenie pokazuje, że mnożenie macierzy jest wykonalne w zbiorze Q_8 i mamy następującą tabelkę:

$\cdot$	e	$-e$	i	$-i$	j	$-j$	k	$-k$
e	e	$-e$	i	$-i$	j	$-j$	k	$-k$
$-e$	$-e$	e	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	$-e$	e	k	$-k$	$-j$	j
$-i$	$-i$	i	e	$-e$	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	$-e$	e	i	$-i$
$-j$	$-j$	j	k	$-k$	e	$-e$	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	$-e$	e
$-k$	$-k$	k	$-j$	j	i	$-i$	e	$-e$

Ponieważ mnożenie macierzy jest łączne i jest wykonalne w zbiorze Q_8, $e \in Q_8$ i e jest elementem neutralnym mnożenia macierzy nawet w $M_2(\mathbb{C})$ oraz dla każdego $x \in Q_8$ mamy, że $x^{-1} \in Q_8$, więc Q_8 jest grupą. Nazywamy ją **grupą kwaternionów** i oznaczamy przez Q_8.

Uwaga 1.26. Niech $(G, \cdot, e)$ będzie grupą i niech $f\colon G \to A$ będzie bijekcją zbioru G na zbiór A. W zbiorze A wprowadzamy działanie $\circ$ przy pomocy wzoru:

$$a \circ b = f(f^{-1}(a) \cdot f^{-1}(b)) \text{ dla } a, b \in A.$$

Niech $\epsilon = f(e)$. Wówczas $(A, \circ, \epsilon)$ jest grupą. Rzeczywiście, dla dowolnych $a, b, c \in A$ mamy

$$a \circ (b \circ c) = a \circ f(f^{-1}(b) \cdot f^{-1}(c)) = f(f^{-1}(a) \cdot f^{-1}(f(f^{-1}(b) \cdot f^{-1}(c)))) =$$
$$= f(f^{-1}(a) \cdot (f^{-1}(b) \cdot f^{-1}(c))) = f((f^{-1}(a) \cdot f^{-1}(b)) \cdot f^{-1}(c))$$

oraz

$$(a \circ b) \circ c = f(f^{-1}(a) \cdot f^{-1}(b)) \circ c = f(f^{-1}(f(f^{-1}(a) \cdot f^{-1}(b))) \cdot f^{-1}(c)) =$$
$$= f((f^{-1}(a) \cdot f^{-1}(b)) \cdot f^{-1}(c)).$$

Zatem działanie $\circ$ jest łączne. Ponadto dla $a \in A$ mamy, że $a \circ \epsilon = f(f^{-1}(a) \cdot f^{-1}(\epsilon)) = f(f^{-1}(a) \cdot e) = f(f^{-1}(a)) = a$ oraz $\epsilon \circ a = f(f^{-1}(\epsilon) \cdot f^{-1}(a)) = f(e \cdot f^{-1}(a)) = f(f^{-1}(a)) = a$, więc ϵ jest elementem neutralnym działania $\circ$. W końcu dla $a \in A$ oraz dla $x = f([f^{-1}(a)]^{-1})$ mamy

$$a \circ x = f(f^{-1}(a) \cdot f^{-1}(f([f^{-1}(a)]^{-1}))) = f(f^{-1}(a) \cdot [f^{-1}(a)]^{-1}) = f(e) = \epsilon$$

oraz

$$x \circ a = f(f^{-1}(f([f^{-1}(a)]^{-1})) \cdot f^{-1}(a)) = f([f^{-1}(a)]^{-1} \cdot f^{-1}(a)) = f(e) = \epsilon,$$

więc każdy element $a \in A$ jest odwracalny i ostatecznie $(A, \circ, \epsilon)$ tworzy grupę.

Przykład 1.27. Wykorzystując znane przykłady grup skończonych i Uwagę 1.26 jesteśmy w stanie wypisywać inne abstrakcyjne grupy. Np. niech $A = \{e, x, y, z\}$ będzie zbiorem 4-elementowym i niech $f\colon K \to A$ będzie bijekcją taką, że $f(e) = e$, $f(S_a) = x$, $f(S_b) = y$ i $f(S_O) = z$. Wówczas na mocy Uwagi 1.26 i Przykładu 1.24 (b), $(A, \square, e)$ jest grupą, gdy $\square$ zadane jest tabelką:

$\circ$	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

Zagadka 7. Czy zbiór 4-elementowy $A = \{a, b, c, d\}$ z działaniem $\circ$ zadanym tabelką

$\circ$	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

tworzy grupę?

Dodatek dla leniwych

1. W nawiązaniu do Przykładu 1.20 uzasadnimy, że $(\mathbb{Z}_m, \oplus_m, 0)$ jest grupą abelową. Wykorzystamy proste własności kongruencji:

(a) $a \equiv b(mod\ m) \iff [a]_m = [b]_m$ dla dowolnych $a, b \in \mathbb{Z}$,

(b) $a \equiv [a]_m(mod\ m)$ dla dowolnego $a \in \mathbb{Z}$.

Z (a) wynika od razu:

(c) $a \equiv b(mod\ m) \iff a = b$ dla dowolnych $a, b \in \mathbb{Z}_m$.

I. Sprawdzamy łączność działania $\oplus_m$. Weźmy dowolne $a, b, c \in \mathbb{Z}_m$. Wtedy korzystając kilka razy z (b) uzyskujemy, że

$a \oplus_m (b \oplus_m c) \equiv a + (b \oplus_m c) \equiv a + (b + c) \equiv a + b + c(mod\ m)$ oraz

$(a \oplus_m b) \oplus_m c \equiv (a \oplus_m b) + c \equiv (a + b) + c \equiv a + b + c(mod\ m)$, skąd $a \oplus_m (b \oplus_m c) \equiv (a \oplus_m b) \oplus_m c(mod\ m)$, więc na mocy (c), $a \oplus_m (b \oplus_m c) = (a \oplus_m b) \oplus_m c$.

II. Sprawdzamy, że działanie $\oplus_m$ jest przemienne. Weźmy dowolne $a, b \in \mathbb{Z}_m$. Wtedy $a \oplus_m b = [a + b]_m = [b + a]_m = b \oplus_m a$, bo dodawanie liczb całkowitych jest przemienne.

III. Sprawdzamy, że 0 jest elementem neutralnym działania $\oplus_m$. Weźmy dowolne $a \in \mathbb{Z}_m$. Wtedy na mocy II, $0 \oplus_m a = a \oplus_m 0 = [a+0]_m = [a]_m = a$, czyli $0 \oplus_m a = a \oplus_m 0 = a$ dla każdego $a \in \mathbb{Z}_m$.

IV. Weźmy dowolne $a \in \mathbb{Z}_m$. Jeśli $a \neq 0$, to $a \geq 1$, skąd $m - a \in \mathbb{Z}_m$ i na mocy II, $a \oplus_m (m - a) = (m - a) \oplus_m a = [(m - a) + a]_m = [m]_m = 0$. Ponadto na mocy III, $0 \oplus_m 0 = 0$. Zatem każdy element $a \in \mathbb{Z}_m$ posiada element przeciwny $\ominus_m a$, przy czym dla $a \neq 0$, jest $\ominus_m a = m - a$ (i oczywiście $\ominus_m 0 = 0$).

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Wskazówka do Zagadki 7.

Zastosować Uwagę 1.26 i funkcję $f\colon \mathbb{Z}_4 \to \{a, b, c, d\}$ taką, że $f(0) = a$, $f(1) = b$, $f(2) = d$, $f(3) = c$.

2. W nawiązaniu do Przykładu 1.20 udowodnimy najpierw, że działanie $\odot_m$ jest łączne w zbiorze $\mathbb{Z}_m$. Postępujemy podobnie jak w **1.**: dla dowolnych $a, b, c \in \mathbb{Z}_m$ mamy, że $a \odot_m (b \odot_m c) \equiv a \cdot (b \odot_m c) \equiv a \cdot (b \cdot c) \equiv a \cdot b \cdot c(mod\ m)$ oraz

$(a \odot_m b) \odot_m c \equiv (a \odot_m b) \cdot c \equiv (a \cdot b) \cdot c \equiv a \cdot b \cdot c(mod\ m)$, skąd $a \odot_m (b \odot_m c) \equiv (a \odot_m b) \odot_m c(mod\ m)$, więc na mocy (c), $a \odot_m (b \odot_m c) = (a \odot_m b) \odot_m c$.

Następnie udowodnimy przemienność działania $\odot_m$ w zbiorze $\mathbb{Z}_m$: weźmy dowolne $a, b \in \mathbb{Z}_m$, wtedy $b \odot_m a = [b \cdot a]_m = [a \cdot b]_m = a \odot_m b$, na mocy przemienności mnożenia liczb całkowitych.

Dalej, dla dowolnego $a \in \mathbb{Z}_m$, $1 \odot_m a = a \odot_m 1 = [a \cdot 1]_m = [a]_m = a$, więc 1 jest elementem neutralnym działania $\odot_m$ w zbiorze $\mathbb{Z}_m$.

Teraz udowodnimy, że działanie $\odot_m$ jest rozdzielne względem działania $\oplus_m$, tzn. dla dowolnych $a, b, c \in \mathbb{Z}_m$ mamy, że $a \odot_m (b \oplus_m c) = (a \odot_m b) \oplus_m (a \odot_m c)$. Rzeczywiście, $a \odot_m (b \oplus_m c) \equiv a \cdot (b \oplus_m c) \equiv a \cdot (b + c) \equiv ab + ac (mod\ m)$ i $(a \odot_m b) \oplus_m (a \odot_m c) \equiv (a \odot_m b) + (a \odot_m c) \equiv ab + ac (mod\ m)$, więc $a \odot_m (b \oplus_m c) \equiv (a \odot_m b) \oplus_m (a \odot_m c) (mod\ m)$, skąd na mocy (c), $a \odot_m (b \oplus_m c) = (a \odot_m b) \oplus_m (a \odot_m c)$.

Weźmy teraz dowolne $a, b \in \mathbb{Z}_m^*$. Wtedy $a, b \in \mathbb{Z}_m$ i $NWD(a, m) = NWD(b, m) = 1$. Stąd na mocy elementarnej teorii liczb, $NWD(a \cdot b, m) = 1$ i $NWD([ab]_m, m) = 1$, czyli $NWD(a \odot_m b, m) = 1$. Ponadto $a \odot_m b \in \mathbb{Z}_m$, więc $a \odot_m b \in \mathbb{Z}_m^*$, czyli działanie $\odot_m$ jest wykonalne w zbiorze $\mathbb{Z}_m^*$. Ponadto z wcześniejszych naszych rozważań mamy, że działanie $\oplus_m$ jest łączne i przemienne w zbiorze $\mathbb{Z}_m^*$ i 1 jest elementem neutralnym tego działania, przy czym $1 \in \mathbb{Z}_m^*$, bo $m > 1$.

Pozostaje do wykazania odwracalność wszystkich elementów $a \in \mathbb{Z}_m^*$. Ale z elementarnej teorii liczb wiadomo, że ponieważ $NWD(a, m) = 1$, to istnieją $x, y \in \mathbb{Z}$ takie, że $ax + my = 1$. Liczby x, y można wyznaczyć np. przy pomocy Algorytmu Euklidesa. Stąd $NWD(x, m) = 1$, więc też $NWD([x]_m, m) = 1$ i $a \cdot [x]_m \equiv 1 (mod\ m)$. Zatem $[x]_m \in \mathbb{Z}_m^*$ i $a \odot [x]_m = 1$, czyli $[x]_m$ jest elementem odwrotnym do a względem działania $\odot_m$.

Kończy to dowód tego, że $(\mathbb{Z}_m^*, \odot_m, 1)$ jest grupą abelową.

Wypiszmy przykładowo wszystkie elementy grupy $\mathbb{Z}_{30}^*$. Mamy, $30 = 2 \cdot 3 \cdot 5$, więc $\varphi(30) = 1 \cdot 2 \cdot 4 = 8$. Zatem nasza grupa ma dokładnie 8 elementów. Wszystkie te elementy są liczbami, które występują w ciągu $0, 1, 2, \ldots, 29$ i nie dzielą się ani przez 2, ani przez 3, ani przez 5. Zatem $\mathbb{Z}_{30}^* = \{1, 7, 11, 13, 17, 19, 23, 29\}$. Dobrym ćwiczeniem jest teraz sporządzenie tabelki działania $\odot_{30}$ w tej grupie!