## Zadanie 1

Sprawdź jakie własności mają w $\mathbb{Z}$ następujące działania:

$a, b, c \in \mathbb{Z}$

### 1.a)

$a \circ b = a - b$

1. ~~łączność~~: $(a - b) - c \neq a - (b - c)$
2. ~~element neutralny~~: $\exists e \in \mathbb{Z} : a - e = a = e - a \Rightarrow -e = 0 = e - 2a$ sprzeczność
3. ~~element symetryczny~~: nie ma elementu neutralnego
4. ~~przemienność~~: $a - b = b - a \Rightarrow a = b$

### 1.b)

$a \circ b = a^2 + b^2$

1. łączność: $\left(a^2 + b^2\right) + c^2 = a^2 + \left(b^2 + c^2\right)$
2. ~~element neutralny~~: $\exists e \in \mathbb{Z} : a^2 + e^2 = a = e^2 + a^2$ sprzeczność
3. ~~element symetryczny~~: nie ma elementu neutralnego
4. przemienność: $a^2 + b^2 = b^2 + a^2$

### 1.c)

$a \circ b = 2(a + b)$

1. ~~łączność~~: $2(2(a + b) + c) = 2(a + 2(b + c))$
   $4a + 4b + 2c = 2a + 4b + 4c$ sprzeczność
2. ~~element neutralny~~: $\exists e \in \mathbb{Z} : 2(a + e) = a = 2(e + a) \Rightarrow 2e = -a$ sprzeczność
3. ~~element symetryczny~~: nie ma elementu neutralnego
4. przemienność: $2(a + b) = 2(b + a)$

### 1.d)

$a \circ b = -a - b$

1. ~~łączność~~: $-(-a - b) - c = -a - (-b - c)$ sprzeczność
2. ~~element neutralny~~: $\exists e \in \mathbb{Z} : -a - e = a = -e - a \Rightarrow e = -2a$ sprzeczność
3. ~~element symetryczny~~: nie ma elementu neutralnego
4. przemienność: $-a - b = -b - a$

**Zadanie 2**

W zbiorze liczb rzeczywistych określamy działanie $x \circ y := x + y + xy$. Czy $(\mathbb{R}, \circ)$ jest grupą? Czy jest grupą para $(\mathbb{R} \setminus \{-1\}, \circ)$?

1. działanie wewnętrzne: $\forall x, y \in \mathbb{R} : x + y + xy \in \mathbb{R}$
2. łączność: $\forall x, y, z \in \mathbb{R} : (x \circ y) \circ z = x \circ (y \circ z)$

$$
\begin{gathered}
(x + y + xy) + z + (x + y + xy)z = x + (y + z + yz) + x(y + z + yz) \\
x + y + xy + z + xz + yz + xyz = x + y + z + yz + xy + xz + xyz
\end{gathered}
$$

3. element neutralny: $\exists e \in \mathbb{R} : \forall x \in \mathbb{R} : x \circ e = x = e \circ x$

$$
\begin{aligned}
x + e + xe = x &= e + x + ex \\
e + xe &= 0 \\
e(1 + x) &= 0 \\
e = 0 &\vee x = -1
\end{aligned}
$$

Element neutralny $e = 0$ działa także dla $x = -1 : x - 1 - x = -1 = -1 + x - x$

4. element symetryczny: $\forall x \in \mathbb{R} : \exists x' \in \mathbb{R} : x \circ x' = 0 = x' \circ x$

$$
\begin{gathered}
x + x' + xx' = x' + x + x'x = 0 \\
x'(1 + x) = -x \\
x' = \frac{-x}{1 + x}, \text{ jeśli } x \neq -1
\end{gathered}
$$

Dla $x = -1$ :

$$
\begin{gathered}
1 + x' - x' = 0 \\
1 = 0 \\
\text{sprzeczność}
\end{gathered}
$$

Czyli $(\mathbb{R}, \circ)$ nie jest grupą.

Żeby sprawdzić czy $(\mathbb{R} \setminus \{-1\}, \circ)$ jest grupą, należy sprawdzić czy $\circ$ jest wewnętrzne w $\mathbb{R} \setminus \{-1\}$ oraz czy elementem symetrycznym do żadnego $x$ nie jest $-1$.

1. działanie wewnętrzne: $\forall x, y \in \mathbb{R} \setminus \{-1\}$ :

$$
\begin{aligned}
x + y + xy &\neq -1 \\
x + y + xy + 1 &\neq 0 \\
(x + 1)(y + 1) &\neq 0 \\
x \neq -1 &\wedge y \neq -1
\end{aligned}
$$

2. element symetryczny: $\forall x \in \mathbb{R} \setminus \{-1\}$ :

$$
\begin{aligned}
x' = \frac{-x}{1+x} &\neq -1 \\
-x &\neq -1 - x \\
0 &\neq -1
\end{aligned}
$$

Wszystkie przekształcenia były równoważne, czyli $(\mathbb{R} \setminus \{-1\}, \circ)$ jest grupą.

**Zadanie 3**

W zbiorze liczb całkowitych określamy działanie $x \circ y := x + y + 2$. Czy $(\mathbb{Z}, \circ)$ jest grupą?

1. działanie wewnętrzne: $\forall x, y \in \mathbb{Z} : x + y + 2 \in \mathbb{Z}$
2. łączność: $\forall x, y, z \in \mathbb{Z} : (x \circ y) \circ z = x \circ (y \circ z)$

$$(x + y + 2) + z + 2 = x + (y + z + 2) + 2$$

3. element neutralny: $\exists e \in \mathbb{Z} : \forall x \in \mathbb{Z} : x \circ e = x = e \circ x$

$$
\begin{aligned}
x + e + 2 = x &= e + x + 2 \\
e &= -2
\end{aligned}
$$

4. element symetryczny: $\forall x \in \mathbb{Z} : \exists x' \in \mathbb{Z} : x \circ x' = -2 = x' \circ x$

$$
\begin{aligned}
x + x' + 2 = -2 &= x' + x + 2 \\
x' &= -x - 4
\end{aligned}
$$

$(\mathbb{Z}, \circ)$ jest grupą.

**Zadanie 4**

Które z następujących zbiorów liczb są grupami:

**4.a)**

liczby wymierne ze względu na dodawanie, mnożenie

$x, y, z \in \mathbb{Q}$

1. działanie wewnętrzne: $x = \frac{a}{b}, y = \frac{c}{d}, a, b, c, d \in \mathbb{Z}, b, c \neq 0$

$$
\begin{aligned}
x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} \in \mathbb{Q} \\
xy = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}
\end{aligned}
$$

2. łączność:

$$(x+y)+z = x+y+z = x+(y+z)$$
$$(xy)z = xyz = x(yz)$$

3. element neutralny:

$$x+0 = x = 0+x$$
$$x \cdot 1 = x = 1 \cdot x$$

4. element symetryczny:

$$x+(-x) = 0 = (-x)+x$$
$$x \cdot \frac{1}{x} = 1 = \frac{1}{x} \cdot x, x \neq 0$$
$$x = 0 \Rightarrow 0 \cdot x' = 1 \text{ sprzeczność}$$

$(\mathbb{Q}, +)$ jest grupą, a $(\mathbb{Q}, \cdot)$ nie jest.

> **4.b)**
>
> liczby niewymierne ze względu na dodawanie, mnożenie

1. działanie wewnętrzne:

   $\forall x, y \in \mathbb{IQ} : x + y \in \mathbb{IQ}$
   kontrprzykład: $\sqrt{2} + \left(-\sqrt{2}\right) = 0 \notin \mathbb{IQ}$

   $\forall x, y \in \mathbb{IQ} : x \cdot y \in \mathbb{IQ}$
   kontrprzykład: $\sqrt{2} \cdot \sqrt{2} = 2 \notin \mathbb{IQ}$

$(\mathbb{Q}, +)$ i $(\mathbb{Q}, \cdot)$ nie są grupami.

> **4.c)**
>
> liczby zespolone o module równym 1 ze względu na mnożenie

1. działanie wewnętrzne:$z_1, z_2 \in \mathbb{C}, |z_1| = |z_2| = 1$

$$z_1 \cdot z_2 \in \mathbb{C}$$
$$|z_1 \cdot z_2| = |z_1| \cdot |z_2| = 1 \cdot 1 = 1$$

2. łączność:

$$\left(e^{i\varphi_x} \cdot e^{i\varphi_y}\right) \cdot e^{i\varphi_z} = e^{i\left(\varphi_x+\varphi_y+\varphi_z\right)} = e^{i\varphi_x} \cdot \left(e^{i\varphi_y} \cdot e^{i\varphi_z}\right)$$

3. element neutralny:

$$\forall z \in \mathbb{C} : z \cdot 1 = z = 1 \cdot z$$

4. element symetryczny: $z \in \mathbb{C}, |z| = 1$

$$\overline{z} \in \mathbb{C}, |\overline{z}| = 1$$
$$z \cdot \overline{z} = |z|^2 = 1$$

$(X, \cdot)$ jest grupą.

> **4.d)**
>
> liczby zespolone o module równym 1 ze względu na następujące działanie: $z_1 \circ z_2 = |z_1|z_2$

$z_1, z_2, z_3 \in \mathbb{C}, |z_1| = |z_2| = |z_3| = 1$
$z_1 \circ z_2 = |z_1|z_2 = 1 \cdot z_2 = z_2$

1. działanie wewnętrzne: $||z_1|z_2| = |1 \cdot z_2| = 1$
2. łączność: $||z_1|z_2|z_3 = |z_2|z_3 = z_3 = |z_1||z_2|z_3$
3. element neutralny: $|z|e = z \Rightarrow e = z$
   Nie ma jednego elementu neutralnego.

Nie jest to grupa.

> **4.e)**
>
> liczby całkowite ze względu na odejmowanie

1. łączność: $(x - y) - z = x - (y - z)$
   Kontrprzykład: $x = 0, y = 0, z = 1 : (0 - 0) - 1 \neq 0 - (0 - 1)$

$(\mathbb{Z}, -)$ nie jest grupą.

> **Zadanie 5**
>
> Niech $E_n$ będzie zbiorem wszystkich pierwiastków $n$-tego stopnia (w $\mathbb{C}$) z jedności. Udowodnij, że $(E_n, \cdot)$ jest grupą.

$E_n = \left\{ e^{i \frac{2k\pi}{n}} : k = 0, ..., n - 1 \right\}$

1. działanie wewnętrzne:

$$z \in E_n \Leftrightarrow z^n = 1$$
$$z_1, z_2 \in E_n$$
$$(z_1 \cdot z_2)^n = z_1^n \cdot z_2^n = 1 \cdot 1 = 1$$
$$z_1 \cdot z_2 \in E_n$$

2. łączność: Mnożenie jest łączne w $\mathbb{C}$, a więc także w $E_n \subset \mathbb{C}$.
3. element neutralny: $z \cdot 1 = 1 \cdot z = z$
4. element symetryczny: $e^{i \frac{2k\pi}{n}} \cdot e^{i \frac{2(n-k)\pi}{n}} = e^{i \frac{2n\pi}{n}} = e^{i \cdot 2\pi} = e^{i \cdot 0} = 1$

### Zadanie 6

Niech $D$ będzie zbiorem wszystkich całkowitych potęg liczby 2. Sprawdź (i uzasadnij) czy struktura $(D, \circ)$, gdzie $a \circ b := \frac{a \cdot b}{2}$, jest grupą.

$a, b, c \in \mathbb{Z}$

1. działanie wewnętrzne:

$$\left(2^a \circ 2^b\right) = \frac{2^a \cdot 2^b}{2} = \frac{2^{a+b}}{2} = 2^{a+b-1} \in D$$

2. łączność:

$$\left(2^a \circ 2^b\right) \circ 2^c = \frac{\frac{2^a \cdot 2^b}{2} \cdot 2^c}{2} = 2^{a+b+c-2} = \frac{2^a \cdot \frac{2^b \cdot 2^c}{2}}{2} = 2^a \circ \left(2^b \circ 2^c\right)$$

3. element neutralny:

$$2^a \circ 2^1 = \frac{2^a \cdot 2^1}{2} = 2^a = \frac{2^1 \cdot 2^a}{2} = 2^1 \circ 2^a$$

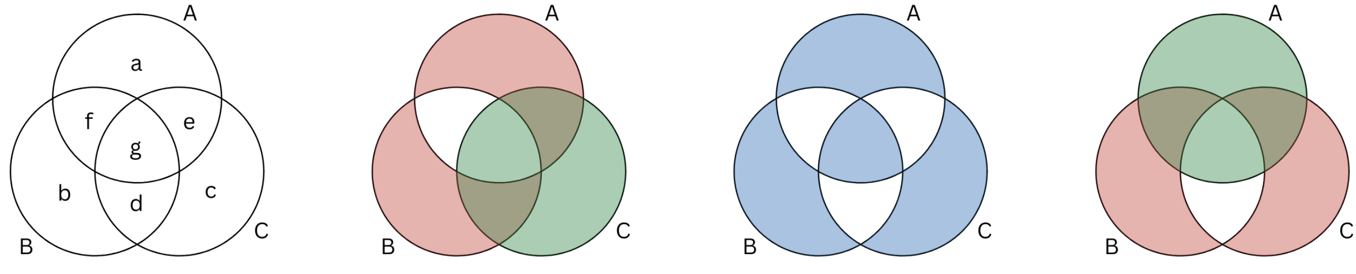
4. element symetryczny:

$$2^a \circ 2^{-a+2} = \frac{2^a \cdot 2^{-a+2}}{2} = \frac{2^2}{2} = 2^1$$

### Zadanie 7

Niech $\triangle$ oznacza różnicę symetryczną, tj., dla dowolnych zbiorów $A$ i $B$, $A \triangle B := (A \setminus B) \cup (B \setminus A)$. Sprawdź, czy dla dowolnie ustalonego zbioru $X \neq \emptyset$, para $(2^X, \triangle)$ jest grupą abelową.

1. Oczywistym jest, że $\triangle$ jest działaniem wewnętrznym w $2^X$.
2. łączność:




$$(A \triangle B) \triangle C = ((a \cup e) \cup (b \cup d)) \triangle (c \cup e \cup d \cup g) = (a \cup b) \cup (c \cup g) = a \cup b \cup c \cup g$$

$$A \triangle (B \triangle C) = (a \cup e \cup f \cup g) \triangle ((b \cup f) \cup (c \cup e)) = (a \cup g) \cup (b \cup c) = a \cup b \cup c \cup g$$

3. element neutralny: $\emptyset \in 2^X$

$$\forall A \in 2^X : A \triangle \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A \cup \emptyset = A = \emptyset \triangle A$$

4. element symetryczny do $A \in 2^X$: $A$

$$A \triangle A = (A \setminus A) \cup (A \setminus A) = \emptyset \cup \emptyset = \emptyset$$

5. przemienność:

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B) = B \triangle A$$

### Zadanie 8

Niech $(G, *)$ będzie grupą z elementem neutralnym $e$ taką, że: $a * a = e$ dla każdego $a \in G$. Wykaż, że $(G, *)$ jest grupą abelową.

Musimy pokazać przemienność $*$, czyli $\forall a, b \in G : a * b = b * a$.

Ponieważ $(G, *)$ jest grupą, a $e$ elementem neutralnym, to $\forall a \in G : \exists a' \in G : a * a' = e$

Ponadto, z faktu, że $a * a = e$ mamy:

$$\begin{aligned}
e = a * a' &= a * a \\
a' * (a * a') &= a' * (a * a) \\
(a' * a) * a' &= (a' * a) * a \quad (* \text{ jest łączne}) \\
e * a' &= e * a \\
a' &= a
\end{aligned}$$

Z tego wynika, że:

$$a * b = b * a \Leftrightarrow (a * b)' = b * a = b' * a'$$

Czyli wystarczy pokazać, że $(a * b)' = b' * a'$:

$$\begin{aligned}
(a * b) * (a * b)' &= e \\
(b' * a') * (a * b) * (a * b)' &= (b' * a') * e \\
b' * (a' * a) * b * (a * b)' &= b' * (a' * e) \\
b' * e * b * (a * b)' &= b' * a' \\
b' * b * (a * b)' &= b' * a' \\
e * (a * b)' &= b' * a' \\
(a * b)' &= b' * a'
\end{aligned}$$

Co kończy dowód.

### Zadanie 9

Czy następujące zbiory są ciałami ze względu na dodawanie i mnożenie:

**9.a)**

$A = \left\{a + b\sqrt[3]{5} : a, b \in \mathbb{Q}\right\}$

$\left(a_1 + b_1\sqrt[3]{5}\right)\left(a_2 + b_2\sqrt[3]{5}\right) = a_1a_2 + (a_1b_2 + a_2b_1)\sqrt[3]{5} + b_1b_2\sqrt[3]{5}^2$

*Hipoteza:*

$$\begin{aligned}
\sqrt[3]{5}^2 &= a + b\sqrt[3]{5}, a, b \in \mathbb{Q} \\
a &= \sqrt[3]{5}^2 - b\sqrt[3]{5} \\
a &= \sqrt[3]{5}\left(\sqrt[3]{5} - b\right) \\
a\left(\sqrt[3]{5} + b\right) &= \sqrt[3]{5}\left(\sqrt[3]{5}^2 - b^2\right) \\
a\left(\sqrt[3]{5} + b\right) &= 5 - b^2\sqrt[3]{5} \\
a\sqrt[3]{5} + ab &= 5 - b^2\sqrt[3]{5} \\
\sqrt[3]{5}(a + b^2) &= 5 - ab \\
\sqrt[3]{5} &= \frac{5 - ab}{a + b^2} \in \mathbb{Q} \text{ sprzeczność}
\end{aligned}$$

Jeżeli $b_1 \neq 0 \land b_2 \neq 0$ to $b_1b_2\sqrt[3]{5}^2 \notin A \Rightarrow \left(a_1 + b_1\sqrt[3]{5}\right)\left(a_2 + b_2\sqrt[3]{5}\right) \notin A$

Mnożenie nie jest wewnętrzne w $A$, więc $(A, +, \cdot)$ nie może być ciałem.

**9.b)**

liczby wymierne, które nie są całkowite

$\frac{1}{2} + \frac{1}{2} = 1 \in \mathbb{Z}$

Dodawanie nie jest wewnętrzne, więc nie jest to ciało.

**9.c)**

zbiór $A$ liczb zespolonych postaci $a + ib\sqrt{2}, a, b \in \mathbb{Q}$

$a_1 + ib_1\sqrt{2} + a_2 + ib_2\sqrt{2} = (a_1 + b_2) + (b_1 + b_2)i\sqrt{2} \in A$

$\left(a_1 + ib_1\sqrt{2}\right)\left(a_2 + ib_2\sqrt{2}\right) = (a_1a_2 - 2b_1b_2) + (a_1b_2 + b_1a_2)i\sqrt{2} \in A$

Dodawanie i mnożenie są działaniami wewnętrznymi w $A$. Ponieważ $A \subset \mathbb{C}$, to są też łączne i przemienne, a mnożenie jest rodzielne względem dodawania: $(z_1 + z_2) \cdot z_3 = z_1z_3 + z_2z_3$.

Istnieją elementy neutralne względem dodawania ($0 = 0 + 0\sqrt{2}$) i mnożenia ($1 = 1 + 0\sqrt{2}$).

Dla każdego $z \in A$ istnieje element przeciwny:

$a + ib\sqrt{2} + z' = 0 \Rightarrow z' = -a - ib\sqrt{2} \in A$

Dla każdego $z \in A\{0\}$ istnieje element odwrotny:
$\left(a + ib\sqrt{2}\right) \cdot z' = 1 \Rightarrow z' = \frac{1}{a+ib\sqrt{2}} = \frac{a-ib\sqrt{2}}{a^2+2b^2} = \frac{a}{a^2+2b^2} + i\frac{-b}{a^2+2b^2}\sqrt{2} \in A$

$(A, +, \cdot)$ jest ciałem.

**Zadanie 10**

W zbiorze $\mathbb{Z}/k$ (tj. zbiorze ilorazowym ze względu na relację przystawania modulo $k$) określamy działania $+, \cdot$ następująco:

$$[a] + [b] = [a + b],\ [a] \cdot [b] = [a \cdot b].$$

**10.a)**

Sprawdź, czy $(\mathbb{Z}/12, +, \cdot)$ jest pierścieniem przemiennym z jedynką ale z dzielnikami zera.

Dodawanie i mnożenie są wewnętrzne, łączne oraz przemienne w $\mathbb{Z}/12$ co jest oczywiste.

Elementami neutralnymi są $[0]$ i $[1]$: $[a] + [0] = [a + 0] = 0$, $[a] \cdot [1] = [a \cdot 1] = [a]$.

Każdy element ma swój element przeciwny: $[a] + [12 - a] = [12] = [0]$.

Zachodzi rozdzielność mnożenia względem dodawania (obustronna, bo mnożenie jest przemienne):
$([a] + [b]) \cdot [c] = [a + b] \cdot [c] = [(a + b) \cdot c] = [a \cdot c + b \cdot c] =$
$[a \cdot c] + [b \cdot c] = ([a] \cdot [c]) + ([b] \cdot [c])$

Z tego wynika, że $(\mathbb{Z}/12, +, \cdot)$ jest pierścieniem przemiennym z jednością.

Dzielniki zera: $[3] \cdot [4] = [12] = [0]$, $[2] \cdot [6] = [12] = [0]$

**10.b)**

Wykaż, że $(\mathbb{Z}/7, +, \cdot)$ jest pierścieniem całkowitym.

W analogiczny sposób co w **10.a** pokazujemy, że $\mathbb{Z}/7, +, \cdot)$ jest pierścieniem przemiennym z jednością.

*Hipoteza:*
Istnieją dzielniki zera: $[a], [b] \in \mathbb{Z}/7, [a], [b] \neq 0 \land [a] \cdot [b] = [0]$

$a = 7k + r_1, k \in \mathbb{Z}, r_1 \in \{1, 2, 3, 4, 5, 6\}$
$b = 7l + r_2, l \in \mathbb{Z}, r_2 \in \{1, 2, 3, 4, 5, 6\}$

$[a] \cdot [b] = [a \cdot b] = [0] \Leftrightarrow a \cdot b = 7m, m \in \mathbb{Z}$

$(7k + r_1)(7l + r_2) = \underbrace{49kl + 7kr_2 + 7kr_1}_{\text{podzielne przez 7}} + r_1r_2 \Rightarrow 7|r_1r_2$ sprzeczność

Skoro nie ma dzielników zera to $(\mathbb{Z}/7, +, \cdot)$ jest pierścieniem całkowitym.

## Zadanie 11

### 11.a)

Wykaż, że zbiór $A = \left\{x = a + b\sqrt{3} : a, b \in \mathbb{Z}\right\}$ z działaniami dodawania i mnożenia jest pierścieniem.

Dodawanie i mnożenie są działaniami wewnętrznymi w $A$:

$\left(a_1 + b_1\sqrt{3}\right) + \left(a_2 + b_2\sqrt{3}\right) = (a_1 + a_2) + (b_1 + b_2)\sqrt{3}$

$\left(a_1 + b_1\sqrt{3}\right)\left(a_2 + b_2\sqrt{3}\right) = (a_1a_2 + 3b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{3}$

Dodawanie i mnożenie są łączne w $\mathbb{Z}$, a także zachodzi obustronna rozdzielność mnożenia względem dodawania. $A \subset \mathbb{Z}$, więc tam również.

Względem dodawania istnieją elementy neutralny $(0 = 0 + 0\sqrt{3})$ i symetryczne $(-a - b\sqrt{3})$.

Z tego wynika, że $(A, +, \cdot)$ jest pierścieniem.

### 11.b)

Wykaż, że zbiór $B = \left\{x = a + b\sqrt{3}, a, b \in \mathbb{Q}\right\}$ z działaniami dodawania i mnożenia jest ciałem.

Analogicznie do **11.a** pokazujemy, ze $(B, +, \cdot)$ jest pierścieniem.

Istnieje element neutralny względem mnożenia $(1 = 1 + 0\sqrt{3})$.

Dla każdego $x = a + b\sqrt{3} \neq 0$ istnieje element odwrotny $x'$:

$\left(a + b\sqrt{3}\right) \cdot x' = 1 \Rightarrow x' = \frac{1}{a+b\sqrt{3}} = \frac{a-b\sqrt{3}}{a^2-3b^2} = \frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3}, a^2 - 3b^2 \neq 0.$

$a^2 - 3b^2 = 0 \Rightarrow a^2 = 3b^2 \Rightarrow a = \pm b\sqrt{3}$ sprzeczność, bo $a, b \in \mathbb{Q}$

Z tego wynika, że $(B, +, \cdot)$ jest ciałem.

### 11.c)

Udowodnij, że odwzorowanie $f : x = a + b\sqrt{3} \to \tilde{x} = a - b\sqrt{3}$ jest automorfizmem pierścienia $(A, +, \cdot)$ w siebie.

Niech $x, y \in A, x = a_1 + b_1\sqrt{3}, y = a_2 + b_2\sqrt{3}$

$$
\begin{aligned}
f(x+y) &\stackrel{?}{=} f(x)+f(y) \\
f\left(a_1+b_1\sqrt{3}+a_2+b_2\sqrt{3}\right) &= a_1+a_2-(b_1+b_2)\sqrt{3} \\
f\left(a_1+b_1\sqrt{3}\right)+f\left(a_2+b_2\sqrt{3}\right) &= a_1-b_1\sqrt{3}+a_2-b_1\sqrt{3}
\end{aligned}
$$

$$
\begin{aligned}
f(x\cdot y) &\stackrel{?}{=} f(x)\cdot f(y) \\
f\left(\left(a_1+b_1\sqrt{3}\right)\left(a_2+b_2\sqrt{3}\right)\right) &= (a_1a_2+3b_1b_2)-(a_1b_2+a_2b_1)\sqrt{3} \\
f\left(a_1+b_1\sqrt{3}\right)\cdot f\left(a_2+b_2\sqrt{3}\right) &= \left(a_1-b_1\sqrt{3}\right)\left(a_2-b_1\sqrt{3}\right) \\
&= (a_1a_2+3b_1b_2)-(a_1b_2+a_2b_1)\sqrt{3}
\end{aligned}
$$

Z tego wynika, że $f$ jest homomorfizmem $(A, +, \cdot)$ w siebie.

$f : A \to A$ jest bijekcją, więc $f$ jest izomorfizmem.

Z tych dwóch faktów wynika, że $f$ jest automorfizmem.

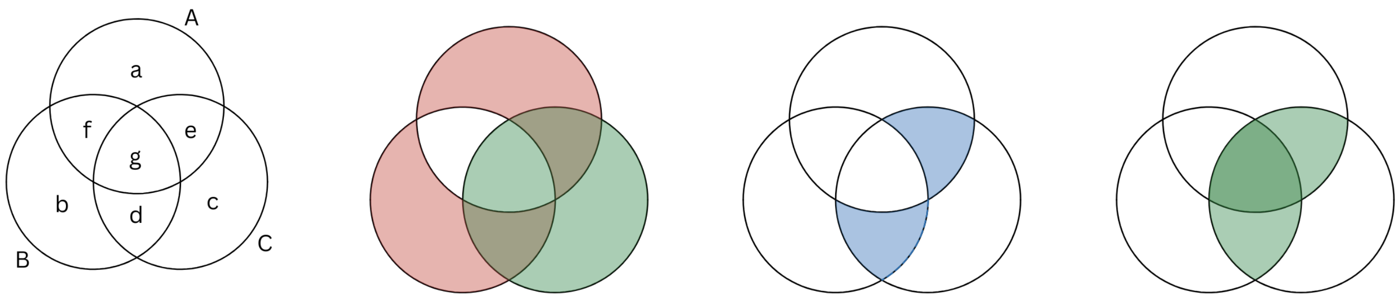
## Zadanie 12

Dla danego zbioru $X \neq \emptyset$, definiujemy strukturę $(2^X, \triangle, \cap)$, gdzie „$\triangle$" oznacza różnicę symetryczną a „$\cap$" - przecięcie zbiorów. Sprawdź czy ta struktura jest:

### 12.a)

pierścieniem?

W zadaniu **7** pokazaliśmy, że $(2^X, \triangle)$ to grupa abelowa.




$A, B, C \in 2^X$

$\cap$ jest łączne:

$(A \cap B) \cap C = (f \cup g) \cap (c \cup d \cup e \cup g) = g$
$A \cap (B \cap C) = (a \cup e \cup f \cup g) \cap (d \cup g) = g$

$\cap$ jest rozdzielnie względem $\triangle$:

$(A \triangle B) \cap C = (a \cup e \cup b \cup d) \cap (c \cup d \cup e \cup g) = d \cup e$

$(A \cap C) \triangle (B \cap C) = (e \cup g) \triangle (d \cup g) = e \cup d = d \cup e$

Analogicznie pokazujemy rozdzielność lewostronną.

Z tego wynika, że $(2^X, \triangle, \cap)$ jest pierścieniem.

> **12.b)**
>
> pierścieniem przemiennym?

Tak, ponieważ $\cap$ jest przemienne: $A \cap B = B \cap A$.

> **12.c)**
>
> pierścieniem z jednością?

$A \in 2^X$

$A \cap \mathbf{1} = \mathbf{1} \cap A = A \Rightarrow \mathbf{1} = \emptyset \in 2^X$

> **12.d)**
>
> pierścieniem z całkowitym?

Pierścień całkowity to pierścień przemienny, z jednością i bez dzielników zera.

$\mathbf{0} = \emptyset$, bo $A \triangle \emptyset = (A \setminus \emptyset) \cup (\emptyset \setminus A) = A$

Dla dowolnych dwóch niepustych, rozłącznych $A \in 2^X$ i $B \in 2^X : A \cap B = \emptyset$, czyli $A$ i $B$ są dzielnikami zera.

Gdy $X$ jest zbiorem jednoelementowym nie ma dzielników zera.

> **12.e)**
>
> ciałem?

Dla dowolnego $A \in 2^X, A \neq \emptyset$ istnieje $A^{-1} : A \cap A^{-1} = \mathbf{1} = \emptyset$

$A^{-1} = X \setminus A$, bo $A \cap A^{-1} = A \cap (X \setminus A) = \emptyset$

$(2^X, \triangle, \cap)$ jest ciałem.

> ## Zadanie 13
>
> W zbiorze $\mathbb{R}^2$ wprowadzamy działania: $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, $(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 + p y_1 y_2, x_1 y_2 + x_2 y_1)$. Dla jakich $p \in \mathbb{R}$ struktura $(\mathbb{R}^2, +, \cdot)$ jest ciałem?

Tak zdefiniowane dodawanie to dodawanie wektorów w $\mathbb{R}^2$. Łatwo zauważyć, że jest to grupa abelowa, z elementem neutralnym $(0, 0)$.

Łatwo zauważyć również, że mnożenie jest wewnętrzne. Łączność mnożenia i rozdzielność względem dodawania można pokazać ale to dużo liczenia.

Elementem neutralnym względem mnożenia jest $(1,0)$:

$$(x,y)\cdot(1,0)=(x\cdot 1+p\cdot y\cdot 0, x\cdot 0+y\cdot 1)=(x,y)$$

Dla każdego $(x,y)\neq(0,0)$ znajdźmy element odwrotny $(x',y')$.

$$xx'+pyy'=1\wedge xy'+x'y=0$$
$$y'=-x'\frac{y}{x}$$
$$xx'+py\cdot\left(-x'\frac{y}{x}\right)=1$$
$$x'\left(x-\frac{py^2}{x}\right)=1$$

Jeżeli $x-\frac{py^2}{x}=0$ to element odwrotny nie istnieje, czyli struktura nie może być ciałem.

$x-\frac{py^2}{x}=0\Leftrightarrow x^2=py^2$. Równanie to jest sprzeczne tylko dla $p<0$. W tym wypadku:

$$x'=\frac{1}{x-\frac{py^2}{x}}=\frac{x}{x^2-py^2}$$
$$y'=-\frac{x}{x^2-py^2}\cdot\frac{y}{x}=-\frac{y}{x^2-py^2}$$

*Interpretacja liczbami zespolonymi*:

Para $(x,y)$ reprezentuje liczbę zespoloną $x+y\sqrt{-p}\cdot i$ ($x+y\sqrt{p}$ dla $\sqrt{-1}=i$).

$$(x_1,y_1)+(x_2,y_2)=(x_1+y_1\sqrt{-p}\cdot i)+(x_2+y_2\sqrt{-p}\cdot i)=(x_1+x_2)+(y_1+y_2)\sqrt{-p}\cdot i$$
$$(x_1,y_1)\cdot(x_2,y_2)=(x_1+y_1\sqrt{-p}\cdot i)\cdot(x_2+y_2\sqrt{-p}\cdot i)=$$
$$(x_1x_2+y_1y_2(-p)i^2)+(x_1y_2+x_2y_1)\sqrt{-p}\cdot i=(x_1x_2+py_1y_2)+(x_1y_2+x_2y_1)\sqrt{-p}\cdot i$$

Czyli mamy doczynienia z liczbami zespolonymi, przyczym oś $\mathfrak{I}$ została przeskalowana o $\sqrt{-p}$.

## Zadanie 14

### 14.a)

Wykaż, że zbiór $A=\{x=m+ni : m,n\in\mathbb{Z}\}$ jest grupą ze względu na dodawanie.

$(m_1+n_1i)+(m_2+n_2i)=(m_1+m_2)+(n_1+n_2)i\in A$

$A\subset\mathbb{C}$ więc zachodzi łączność oraz istnieje element neutralny $0\in A$.

Dla każdego $x=m+ni\in A$ istnieje element symetryczny $x'=-m-ni\in A$.

### 14.b)

Wykaż, że zbiór $B = \{x = 2^n 3^m : m, n \in \mathbb{Z}\}$ jest grupą ze względu na mnożenie.

Wewnętrzność, i łączność oczywista.

Element neutralny to $1 = 2^0 \cdot 3^0$.

Dla każdego $x = 2^n 3^m \in B$ istnieje element symetryczny $x' = 2^{-n} 3^{-m} \in B$.

### 14.c)

Udowodnij, że $A$ i $B$ są izomorficzne.

Niech $h : A \to B$ będzie odwozorwaniem grupy $(A, +)$ w grupę $(B, \cdot)$:

$h(n + mi) = 2^n 3^m$

Dla każdych $x, y \in A, x = a + bi, y = c + di$:

$h(x + y) = h((a + c) + (b + d)i) = 2^{a+b} \cdot 3^{b+d}$

$h(x) \cdot h(y) = h(a + bi) \cdot h(c + di) = 2^a 3^b \cdot 2^c 3^d = 2^{a+b} \cdot 3^{b+d}$

Czyli $h$ jest homomorfizmem.

Każdy element z $B$ jest osiągalny i każdemy odpowiada tylko jeden element z $A$, więc jest to homomorfizm bijektywny, czyli $A$ i $B$ są izomorficzne.