

Uproszczenie wyrażeń

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

Spotkania z Matematyką – p. 3

Uproszczenie wyrażeń. Szczegóły

$$\begin{aligned} 2x + (y - x) &= \\ &= 2x + (y + (-x)) \\ &= 2x + ((-x) + y) \\ &= (2x + (-x)) + y \\ &= (2x + (-1) \cdot x) + y \\ &= (2 + (-1)) \cdot x + y \\ &= 1 \cdot x + y \\ &= x + y \end{aligned}$$

Spotkania z Matematyką – p. 4

Spotkania z Matematyką ***Zastosowanie teorii pierścieni*** ***w praktyce***

Aleksander Denisiuk

`denisjuk@matman.uwm.edu.pl`

Uniwersytet Warmińsko-Mazurski w Olsztynie

Wydział Matematyki i Informatyki

ul. Słoneczna 54, pok. E1/7

10-561 Olsztyn

Spotkania z Matematyką – p. 1

Zastosowanie teorii pierścieni ***w praktyce***

Najnowsza wersja tego dokumentu dostępna jest pod adresem

<http://wmii.uwm.edu.pl/~denisjuk/uwm/>

Spotkania z Matematyką – p. 2

Układy, dla których spełniono 1–8

- ⑥ $\mathbb{Z}$
- ⑥ $\mathbb{Q}$
- ⑥ $\mathbb{R}$
- ⑥ reszty modulo 6
- ⑥ reszty modulo n

Wniosek 2. We wszystkich tych układach prawdziwy jest wzór
 $(a + b)^2 = a^2 + 2ab + b^2$

Spotkania z Matematyką – p. 7

Pierścienie

Definicja 3. Zbiór X , na którym określone są dodawanie i mnożenie, spełniające warunki 1–8 nazywa się *przemiennym pierścieniem z jedyneką*

Uwaga 4. *Pierścieniem* nazywa się zbiór, na którym określone są dodawanie i mnożenie, spełniające warunki 1–8 bez 6 i 7

Spotkania z Matematyką – p. 8

Uproszczenie wyrażeń. Zasady

1. łączność dodawania $(a + b) + c = a + (b + c)$
2. przemienność dodawania $a + b = b + a$
3. istnieje zero 0, takie że $a + 0 = 0 + a = a$
4. istnieje liczba przeciwna $-a$, taka że
 $a + (-a) = (-a) + a = 0$
5. łączność mnożenia $a(bc) = (ab)c$
6. przemienność mnożenia $ab = ba$
7. istnieje jedynka 1, taka, że $a \cdot 1 = 1a = a$
8. rozdzielczość mnożenia
 $a(b + c) = ab + ac$
 $(a + b)c = ac + bc$

Spotkania z Matematyką – p. 5

Twierdzenie

Twierdzenie 1.

$$(a + b)^2 = a^2 + 2ab + b^2$$

Dowód. Za pomocą zasad 1–8

□

Spotkania z Matematyką – p. 6

Dzielenie

9. jeżeli $a \neq 0$, to istnieje a^{-1} , element *odwrotny*, taki że
 $a \cdot a^{-1} = a^{-1} \cdot a = 1$

10. $0 \neq 1$

Definicja 7. Jeżeli dodawanie i mnożenie określone na X spełniają warunki 1–10, to X nazywa się *ciałem* (niekiedy się mówi *przemiennym ciałem*)

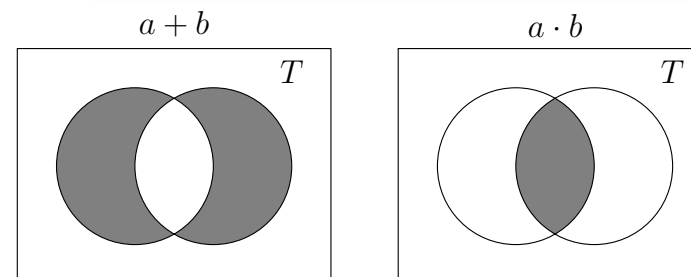
Przykłady ciał

- ⊙ $\mathbb{Q}$
- ⊙ $\mathbb{R}$
- ⊙ reszty modulo n , jeżeli n jest liczbą pierwszą
- ⊙ liczby *algebraiczne*
- ⊙ liczby algebraiczne postaci $a + \sqrt{2}b$, gdzie $a, b \in \mathbb{Q}$

Przykład pierścienia

- ⊙ Niech dany będzie niepusty zbiór T
- ⊙ X będzie zbiorem podzbiorów T
 - △ $A + B = (A \cup B) \setminus (A \cap B)$
 - △ $A \cdot B = A \cap B$

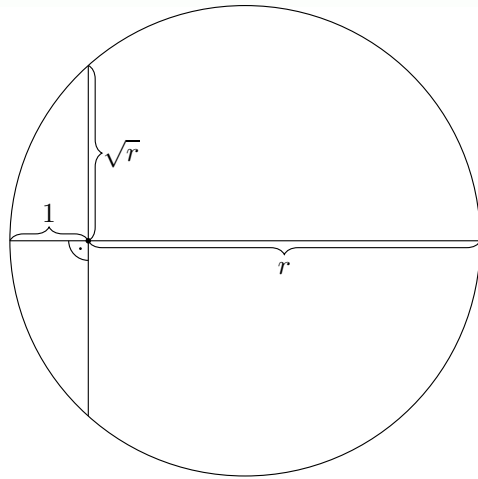
Działania w pierścieniu X



Twierdzenie 5. X jest przemiennym pierścieniem z jedyneką

Wniosek 6. $\forall a, b \in X: (a + b)^2 = a^2 + 2ab + b^2$

Obliczenie pierwiastka kwadratowego



Spotkania z Matematyką – p. 15

Jakie liczby można skonstruować?

- 1, 2, 3, ..., $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, ... — ciało $\mathbb{Q}$
- liczby $p + q\sqrt{r}$, gdzie $p, q, r \in \mathbb{Q}$ — ciało $\mathbb{F}_1$
- liczby $p + q\sqrt{s}$, gdzie $p, q, s \in \mathbb{F}_1$ — ciało $\mathbb{F}_2$
- i tak dalej: $\mathbb{Q} \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3 \subset \dots \subset \mathbb{F}_{k-1} \subset \mathbb{F}_k \subset \dots$

Twierdzenie 11. Każda konstruowalna liczba należy do jednego z ciał $\mathbb{F}_i$ przy odpowiednio dobranych $r, s, \dots$

Spotkania z Matematyką – p. 16

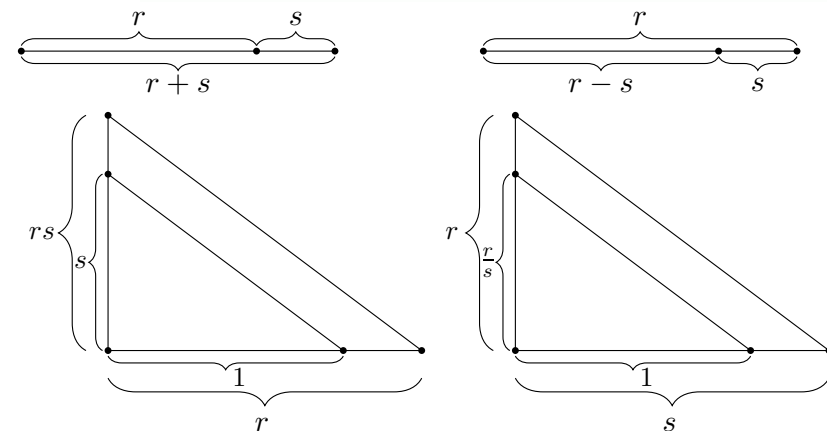
Podwojenie sześcianu

Zadanie 8. Zbudować sześcián o objętości dwa razy większej, niż dany sześcián

Zadanie 9. Dany jest odcinek długości 1. Skonstruować (za pomocą cyrkla i linijki) odcinek długości $\sqrt[3]{2}$

Spotkania z Matematyką – p. 13

Konstrukcje geometryczne



Wniosek 10. Zbiór K konstruowalnych liczb tworzy ciało (podciało $\mathbb{R}$).

Spotkania z Matematyką – p. 14

Pierścień $\mathbb{Z}_7$

- dni są podzielone na klasy: poniedziałek, wtorek, środa, czwartek, piątek, sobota, niedziela
- przykładowo, środa = $\{\dots, -11, -4, 3, 10, 17, \dots\}$ — wszystkie liczby, kongruentne z 3 modulo 7, $7q + 3$
- niech $[x]$ będzie zbiorem liczb, kongruentnych z x modulo 7
- dodawanie $[x] + [y] = [x + y]$
- mnożenie $[x] \cdot [y] = [x \cdot y]$
- pierścień $\mathbb{Z}_7$

Pierścień $\mathbb{Z}_n$

- niech $[x]$ będzie zbiorem liczb, kongruentnych z x modulo n
- dodawanie $[x] + [y] = [x + y]$
- mnożenie $[x] \cdot [y] = [x \cdot y]$
- pierścień $\mathbb{Z}_n$

Założmy, że $\sqrt[3]{2}$ można skonstruować

- $\sqrt[3]{2} \notin \mathbb{Q}$
- istnieje taki ciąg ciał $\mathbb{Q} \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3 \subset \dots \subset \mathbb{F}_{k-1} \subset \mathbb{F}_k \subset \dots$, że $\sqrt[3]{2} \notin \mathbb{F}_{k-1}$ oraz $\sqrt[3]{2} \in \mathbb{F}_k$
- $\sqrt[3]{2} = p + q\sqrt{t}$, gdzie $p, q, t \in \mathbb{F}_{k-1}$, $\sqrt{t} \notin \mathbb{F}_{k-1}$
- $(p^3 + 3pq^2t - 2) + (3p^2q + q^3t)\sqrt{t} = 0$
- $p^3 + 3pq^2t - 2 = 0$ oraz $3p^2q + q^3t = 0$
- więc $p - q\sqrt{t}$ też jest pierwiastkiem trzeciego stopnia z dwójki
- z czego wynika, że $\sqrt[3]{2} \in \mathbb{F}_{k-1}$, czyli sprzeczność

Inne geometryczne zagadnienia

- Trysekcja kąta
 - w przypadku kąta 60° : skonstruować pierwiastek równania $x^3 - 3x = 1$
- Kwadratura koła
 - skonstruować liczbę π
- Wielokąt foremny
 - można skonstruować wtedy i tylko wtedy, gdy liczba boków równa jest $2^n \cdot p_1 \cdot \dots \cdot p_b$, gdzie p_i są różne liczby pierwsze postaci $2^{2^c} + 1$ (liczby Fermata)
 - przykładowo, 65 537-kąt można skonstruować
 - $(2^{2^{32}} + 1)$ -kąt nie można

Ciało de Bruijna

⑥ $X = \{0, 1, p, q\}$

+	0	1	p	q
0	0	1	p	q
1	1	0	q	p
p	p	q	0	1
q	q	p	1	0

×	0	1	p	q
0	0	0	0	0
1	0	1	p	q
p	0	p	q	1
q	0	q	1	p

⑥ $p^2 + p + 1 = 0$

Współrzędne na planszy

		(-1, 3)	(0, 3)	(1, 3)		
		(-1, 2)	(0, 2)	(1, 2)		
(-3, 1)	(-2, 1)	(-1, 1)	(0, 1)	(1, 1)	(2, 1)	(3, 1)
(-3, 0)	(-2, 0)	(-1, 0)	(0, 0)	(1, 0)	(2, 0)	(3, 0)
(-3, -1)	(-2, -1)	(-1, -1)	(0, -1)	(1, -1)	(2, -1)	(3, -1)
		(-1, -2)	(0, -2)	(1, -2)		
		(-1, -3)	(0, -3)	(1, -3)		

Liczby zespolone

⑥ $a + bi$, gdzie $i^2 = -1$

⑥ wprowadźmy liczby zespolone analogicznie do pierścienia $\mathbb{Z}_7$

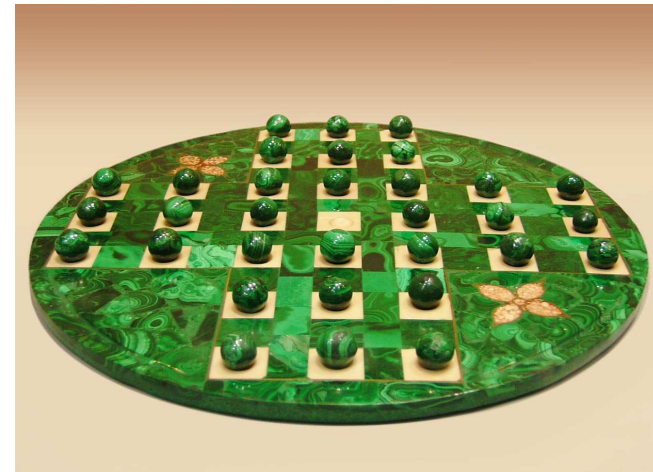
⑥ w pierścieniu $\mathbb{Z}_7$ obowiązuje $7 = 0 \Rightarrow$ kongruencja modulo 7

⑥ w liczbach zespolonych powinno być $x^2 + 1 = 0 \Rightarrow$ kongruencja modulo $x^2 + 1$

⑥ pytanie: co jest kongruentne?

⑥ odpowiedź: pierścień wielomianów, $\mathbb{R}[x]$

Gra samotnik (solitaire)



⑥ Gdzie może się znajdować ostatni pionek?

Niezmenniki stanów planszy

- ⑥ $A(S) = \sum p^{k+l}$
- ⑥ $B(S) = \sum p^{k-l}$
- ⑥ na początku gry $A(S) = B(S) = 1$
- ⑥ a więc na końcu $p^{k+l} = p^{k-l} = 1$
- ⑥ czyli k i l są wielokrotnościami trójki
- ⑥ możliwe stany: $(-3, 0)$, $(0, 3)$, $(3, 0)$, $(0, -3)$ oraz $(0, 0)$
- ⑥ (wszystkie są osiągalne)