Algebra liniowa 2

dr Joanna Jureczko

Zestaw zadań nr 5

Ciało Ciało $\mathbb{Z}_p$
Podciała Rozszerzenia ciał
Ciało Galois proste i rozszerzone

5.1. Sprawdzić, czy wielomiany są nierozkładalne w podanym pierścieniu:

a) $x^8 + x^4 + x^3 + x + 1$ w $\mathbb{Z}_2[x]$,

b) $x^3 + x^2 + 2$ w $\mathbb{Z}_3[x]$,

c) $4x^3 + 3x^2 + x + 1$ w $\mathbb{Z}_5[x]$.

5.2. Znaleźć wszystkie nierozkładalne wielomiany: a) stopnia 5 nad $\mathbb{Z}_2$, b) stopnia 2 nad $\mathbb{Z}_5$, c) stopnia 3 nad $\mathbb{Z}_7$.

5.3. Udowodnić, że liczba a jest liczbą algebraiczną, gdy a) $a = 2+\sqrt{3}$, b) $a = \sqrt{2}+\sqrt{5}$.

5.4. Znaleźć wielomian minimalny danej liczby algebraicznej: a) $\sqrt{2}$, b) $4+\sqrt{3}$, c) $\sqrt[3]{5}$, d) $\frac{\sqrt[4]{5}}{2}$

5.5. Sprawdzić, że wielomian $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ jest nierozkładalny nad ciałem $\mathbb{Z}_2$. Wypisać wszystkie elementy ciała $CG(4)$ rozumianego jako ciało reszt z dzielenia przez $x^2 + x + 1$ w pierścieniu $\mathbb{Z}_2[x]$ i zapisać je w postaci pozycyjnej. Utworzyć tabelę dodawania i mnożenia w $CG(4)$.

5.6. Sprawdzić, że wielomian $f = x^3 + x + 1 \in \mathbb{Z}_2[x]$ jest nierozkładalny nad ciałem $\mathbb{Z}_2$. Wypisać wszystkie elementy ciała $CG(8)$ rozumianego jako ciało reszt z dzielenia przez $x^3 + x + 1$ w pierścieniu $\mathbb{Z}_2[x]$ i zapisać je w postaci pozycyjnej. Utworzyć tabelę dodawnia i mnożenia w $CG(8)$.

5.7. Sprawdzić, że wielomian $f = x^2 + 1 \in \mathbb{Z}_3[x]$ jest nierozkładalny nad ciałem $\mathbb{Z}_3$. Wypisać wszystkie elementy ciała $CG(9)$ rozumianego jako ciało reszt z dzielenia przez x^2+1 w pierścieniu $\mathbb{Z}_3[x]$ i zapisać je w postaci pozycyjnej. Utworzyć tabelę dodawania i mnożenia w $CG(9)$.

5.8. a) Znaleźć element pierwotny w ciałach $CG(5)$ oraz $CG(7)$.
b) Znaleźć element pierwotny w ciałach $CG(4)$ oraz $CG(8)$.

5.9. Elementy ciała $CG(4)$ przedstawić w postaci potęgowej. To samo uczynić dla $CG(8)$ oraz $CG(9)$.

5.10. Utworzyć za pomocą elementu pierwotnego tablice dodawania i mnożenia w $CG(4)$.

5.11. Wiedząc, że wielomian $x^4 + x + 1$ jest nierozkładalny w ciele $CG(16)$ przedstawić jego elementy w postaci wielomianowej, pozycyjnej i potęgowej.

5.12.* Dla $g = 2, 3, 5, 7, 11$ znaleźć taką liczbę pierwszą $p > g$, że g jest pierwiastkiem pierwotnym modulo p.

5.13.* Udowodnić, że pierścień klas reszt $\mathbb{Z}/m\mathbb{Z}$ jest ciałem wtedy i tylko wtedy, m jest liczbą pierwszą.

Odpowiedzi:

5.1. a) tak, b) tak, c) tak.

5.2. $x^5 + x^3 + 1, x^5 + x^2 + 1, x^5 + x^4 + x^3 + x^2 + 1, x^5 + x^4 + x^3 + x + 1, x^5 + x^4 + x^2 + x + 1, x^5 + x^3 + x^2 + x + 1,$

b) $x^2+2, x^2+3, 2x^2+4, 3x^2+1, 4x^2+3, 2x^2+1, 3x^2+4, 4x^2+2$, dodatkowo sprawdzić, czy $ax^2 + bx + c$ dla $c \neq 0$ są jeszcze jakieś, c) $x^3 + 2$.

5.3. $x^2 - 1$.

5.4. a) $x^2 - 2$, b) $x^2 - 4x + 13$, c) $x^3 - 5$, d) $x^4 - \frac{5}{16}$.

5.5. $f(0) = 1, f(1) = 1$, $CG(4) = CG(2^2) = \{0, 1, x, x + 1\}$.

5.6. $f(0) = 1, f(1) = 1$, $CG(8) = CG(2^3) = \{0, 1, x, x+1, x^2, x^2+x, x^2+1, x^2+x+1\}$.

5.7. $f(0) = 1, f(1) = 2, f(2) = 2$, $CG(8) = CG(2^3) = \{0, 1, 2, x, 2x, x + 1, 2x + 1, 2x + 2, x + 2\}$.

5.8. a) $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 3$; $\alpha = 2, \alpha^{-1} = 3$, bo $CG(5) = \mathbb{Z}_5$. $2^1 = 2, 2^2 = 4, 2^3 = 1$, $3^1 = 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$; $\alpha = 3, \alpha^{-1} = 5$, bo $CG(7) = \mathbb{Z}_7$. b) analogicznie.

5.9. $CG(4) = CG(2^2)$

0	0
1	α^0
x	α^1
x+1	α^2

Analogicznie $CG(8) = CG(2^3)$ oraz $CG(9) = CG(3^2)$.

5.10.

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

$\cdot$	α^0	α^1	α^2
α^0	α^0	α^1	α^2
α^1	α^1	α^2	α^0
α^2	α^2	α^0	α^1

$\cdot$	1	x	x+1
1	1	x	x+1
x	x	x+1	1
x+1	x+1	1	x

5.11.

	pozycyjna	potęgowa	wielomianowa
0	0000	-	0
1	1000	α^0	1
x	0100	α^1	x
x^2	0010	α^2	x^2
x^3	0001	α^3	x^3
x^4	1100	α^4	$1+x$
x^5	0110	α^5	$x+x^2$
x^6	0011	α^6	x^2+x^3
x^7	1101	α^7	$1+x+x^3$
x^8	1010	α^8	$1+x^2$
x^9	0101	α^9	$x+x^3$
x^{10}	1110	α^{10}	$1+x+x^2$
x^{11}	0111	α^{11}	$x+x^2+x^3$
x^{12}	1111	α^{12}	$1+x+x^2+x^3$
x^{13}	1011	α^{13}	$1+x^2+x^3$
x^{14}	1001	α^{14}	$1+x^3$
x^{15}	1000	α^{15}	1