Algebra Abstrakcyjna i Kodowanie

przykładowe zadania na egzamin

Jacek Cichoń
Politechnika Wrocławska
WPPT

4 czerwca 2017

Na egzaminie będziecie mieli do zrobienia 6 zadań. Cztery będą miały charakter rachunkowy, zaś dwa z nich będą wymagały przeprowadzenia jakiego rozumowania. Wszystkie odpowiedzi (nawet na te rachunkowe zadania) będą wymagały uzasadnienia. Argument typu: *to znalazłem na jakiejś stronie* lub *tak pokazał Wolfram Alpha* nie będą, oczywiście, uznane za poprawne. Rozwiązania zadań za pomocą programu przeglądającego wszystkie potencjalne rozwiązania (taki pomysł może wam przyjść jeśli obliczenia będziemy mieli przeprowadzić w skończone strukturze) również nie będą akceptowane.

1 Struktury algebraiczne

Zadanie 1. Ile generatorów ma grupa C_{4000}?

Zadanie 2. Wyznacz wszystkie pogrupy grupy $\mathbb{Z}_{11}^*$.

Zadanie 3. Ile jest elementów rzędu 100 w grupie C_{4000}?

Zadanie 4. Wyznacz pogrupę G grupy $\mathbb{Z}^2 = (\mathbb{Z}, +) \times (\mathbb{Z}, +)$ generowaną przez zbiór $\{(4, 0), (10, 0), (-18, 0)\}$ oraz wyznacz rzędy elementów w grupie ilorazową $\mathbb{Z}^2/G$.

Zadanie 5. Czy grupy $\mathbb{Z}_8^*$ oraz $\mathbb{Z}_{10}^*$ są izomorficzne?

Zadanie 6. Ile podgrup ma grupa S_3?

Zadanie 7. Rozważamy grupę $T = (\{z \in \mathbb{C} : |z| = 1\}, \cdot)$. Niech $f(x) = x^2$. Pokaż, że f jest endomomorfizmem T. Wyznacz jądro f oraz grupę ilorazową $T/ker(f)$.

2 Elementy Teorii Liczb

Zadanie 1. Jakie wartości przyjmuje funkcja $f(n) = (n-1)! \mod n$?.

Zadanie 2. Pokaż, że dla dowolnej liczby naturalnej n mamy $n|\phi(n^2)$.

Zadanie 3. Wyznacz najmniejszą liczbę naturalną n taką, że $n \equiv 1 \mod 3$, $n \equiv 2 \mod 5$ i $n \equiv 3 \mod 8$.

Zadanie 4. Rozwiąż układ równań: $2x \equiv 1 \mod 5$, $3x \equiv 9 \mod 6$, $4x \equiv 1 \mod 7$.

Zadanie 5. Pokaż, że $(\forall a \in \mathbb{N})(\exists b, c \in \mathbb{N})(a^3 = b^2 - c^2)$.

Zadanie 6. Wyznacz zbiór $\{(a^2 - b^2) \mod 4 : a, b \in \mathbb{N}\}$.

Zadanie 7. Pokaż, że jeśli liczby naturalne a i b są sumami dwóch kwadratów to również liczba $a \cdot b$ jest sumą dwóch kwadratów.

Zadanie 8. Niech $p > 2$ będzie liczbą pierwszą. Niech a, b będą dwoma różnymi generatorami grupy multiplikatywnej Z_p^*. Pokaż, że ab nie jest generatorem grupy $\mathbb{Z}_p^*$.

3 Pierścienie i ciała

Zadanie 1. Niech $n \geq 1$ będzie liczbą naturalną. Wyznacz $NWD(x^{6n} + x + 1, x^2 + 1)$ w pierścieniu $\mathbb{Z}_3[x]$.

Zadanie 2. Korzystając z tego, że wielomian x^3+x+1 jest nierozkładalny w ciele $\mathbb{Z}_5$ rozszerzamy ciało $\mathbb{Z}_5$ o taki element j, że $j^3 = 4j+4$. Ile elementów ma to ciało? Znajdź element odwrotny i przeciwny do elementu $1 + j + j^2$ w tym ciele.

Zadanie 3. Niech $f : \mathbb{Q}[x] \to \mathbb{Q}(i)$ będzie określone wzorem $f(w) = w(2i)$. Korzystając z tego, że $\mathbb{Q}[x]$ jest pierscieniem ideałow głównych wyznacz jądro $ker(f)$.

Zadanie 4. Znajdź w pierścieniu $\mathbb{Z}_8[x]$ element odwrotny do wielomianu $w(x) = 1 + 2x^2$.

Zadanie 5. Niech K będzie ciałem charakterystyki p. Pokaż, że funkcja $f(x) = x^p$ jest różnowartościowym homomorfizmem z K do K.

Zadanie 6. Niech K będzie ciałem charakterystyki p. Wyznacz zbiór $\{x \in K : x^p = x\}$.

4 Kody korekcyjne

Zadanie 1. Z przestrzeni liniowej $\mathbb{Z}_7 \times \mathbb{Z}_7$ konstruujemy płaszczyznę rzutową. Ile jest punktów w tej przestrzeni? Ile jest linii w tej przestrzeni?

Zadanie 2. Czy istnieje kod liniowy o parametrach $[10, 5, 5]$?

Zadanie 3. Pokaż,że zbiór $\mathcal{C} = \{(0,0), (1,2), (2,4), (3,1), (4,3)\} \subseteq \mathbb{Z}_5$ jest kodem liniowym nad ciałem $\mathbb{Z}_5$. Wyznacz kod dualny do kodu $\mathcal{C}$.

Zadanie 4. Niech

$$G = \begin{bmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 3 & 5 \end{bmatrix}$$

będzie macierzą generującą kod $\mathcal{C}$ długości 4 nad ciałem $\mathbb{Z}_7$. Pokaż, że $\mathcal{C}^{\perp} = \mathcal{C}$.

Zadanie 5. Przekształć macierz kodu o macierzy generującej

$$G = \begin{bmatrix} 3 & 2 & 1 & 2 & 3 & 1 \\ 1 & 0 & 1 & 3 & 4 & 1 \end{bmatrix}$$

będzie macierzą generującą kod $\mathcal{C}$ nad ciałem $\mathbb{Z}_5$. Przekształć macierz G do postaci standardowej. Wyznacz parametry tego kodu.

Zadanie 6. Korzystając ze wzoru Stirlinga wyznacz asymptotykę liczb $\binom{3n}{n}$.