

Ćwiczenia do wykładów 12 i 13

Zadanie 1. (ALI w ALG1)

Niech A będzie pierścieniem przemiennym z jedynką i niech $R=M_{n,n}(A)$ będzie pierścieniem macierzy $n \times n$ o współczynnikach z A . **(1)** Załóżmy, że $\mathcal{I}$ jest ideałem obustronnym pierścienia R . Pokazać, że w A istnieje ideał I taki, że $\mathcal{I}=M_{n,n}(I)$. W szczególności, jeżeli A jest ciałem, to w R nie ma obustronnych ideałów właściwych. **Wskazówka.** Jeśli $B=[b_{ij}] \in M_{n,n}(A)$, to $E_{p,r} B E_{s,q}$ jest macierzą, która na przecięciu p -tego wiersza i q -tej kolumny ma b_{rs} , a w pozostałych miejscach ma zera. $E_{i,j}$ oznacza tutaj macierz, która na przecięciu i -tego wiersza i j -tej kolumny ma 1, a w pozostałych miejscach zera. Dla ideału $\mathcal{I}$ z Zadania, rozważyć zbiór I złożony z takich $a \in A$, że $a=b_{11}$ dla pewnego $B=[b_{ij}] \in \mathcal{I}$. **(2) Definicja.** **Centrum pierścienia** R nazywamy zbiór $Z(R)$ złożony z $a \in R$ takich, że dla każdego $b \in R$ jest $ab = ba$. Sprawdzić czy centrum pierścienia jest ideałem. **(3)** Pokazać, że centrum pierścienia macierzy $R=M_{n,n}(K)$ o współczynnikach z ciała K składa się z macierzy diagonalnych αI_n , gdzie $\alpha \in K$.

Zadanie 2. (Twierdzenie chińskie o resztach w $\mathbf{Z}$)

Niech $m_1, m_2, \dots, m_n$ będą liczbami naturalnymi, które są parami względnie pierwsze. Niech będą dane liczby całkowite: $a_1, a_2, \dots, a_n$.

- (a) Dowieść, że istnieje liczba $x \in \mathbf{Z}$ taka, że spełniony jest układ kongruencji $x \equiv a_i \pmod{m_i}$ dla $1 \leq i \leq n$ oraz, że x jest określona jednoznacznie modulo $m = m_1 m_2 \dots m_n$.
- (b) Przyjmijmy oznaczenie $m'_i = \frac{m}{m_i}$, gdzie $1 \leq i \leq n$. Zauważmy, że $(m_i, m'_i) = 1$. Niech $t_i \in (\mathbf{Z}/m_i)^\times$ będzie takie, że $m'_i t_i \equiv 1 \pmod{m_i}$, gdzie $1 \leq i \leq n$. Klasę reszt t_i łatwo możemy znaleźć za pomocą algorytmu Euklidesa. Pokazać, że $x = a_1 m'_1 t_1 + a_2 m'_2 t_2 + \dots + a_n m'_n t_n$ jest rozwiązaniem układu kongruencji z (a).
- (c) Korzystając z (b) rozwiązać dwa układy kongruencji:

$$(1) \quad x \equiv 1 \pmod{8} \quad x \equiv 2 \pmod{25} \quad x \equiv 3 \pmod{81}$$

$$(2) \quad x \equiv 5 \pmod{8} \quad x \equiv 12 \pmod{25} \quad x \equiv 43 \pmod{81}.$$

Zadanie 3.

Niech p będzie liczbą pierwszą, $d \in \mathbf{Z}$ liczbą, która nie jest kwadratem liczby całkowitej. W pierścieniu $\mathbf{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbf{Z}\}$ rozważmy ideał główny $I = (p) = p\mathbf{Z}[\sqrt{d}]$. Dowieść, że I jest ideałem pierwszym wtedy i tylko wtedy, gdy klasa d reszt modulo p nie jest kwadratem w ciele $\mathbf{F}_p$.

Zadanie 4*

Niech p będzie liczbą pierwszą, $f(x) \in \mathbf{F}_p[x]$ unormowanym wielomianem nierozkładalnym stopnia n .

- (1) Dowieść, że ideał główny $I = (f(x))$ jest maksymalny oraz, że pierścień ilorazowy $\mathbf{F}_p[x]/I$ jest ciałem, które składa się z p^n elementów.
- (2) Niech $A = \mathbf{F}_p[x]/I^m$ dla pewnego $m \in \mathbf{N}$. Wyznaczyć elementy nilpotentne pierścienia A oraz liczbę elementów odwracalnych w A .
- (3) Z ilu elementów składa się grupa jedności pierścieni ilorazowych: $\mathbf{F}_2[x]/(x^6-1)$ i $\mathbf{F}_3[x]/(x^6-1)$?