Notatka do Egzaminu z Matematyki 3 (EiTI PW)

Przygotowana na podstawie materiałów wykładowych i ćwiczeniowych

Czerwiec 2025

Spis treści

1 Wprowadzenie

Ta notatka ma na celu przystępne wyjaśnienie kluczowych pojęć z algebry abstrakcyjnej, które są wymagane na egzaminie z Matematyki 3. Skupimy się na grupach, pierścieniach, ciałach i arytmetyce modularnej. Zrozumienie tych koncepcji jest fundamentalne dla dalszych zagadnień, takich jak przestrzenie wektorowe czy odwzorowania liniowe.

2 Grupy

2.1 Definicja Grupy

Grupa to zbiór niepusty G wraz z jednym działaniem binarnym $\cdot : G \times G \to G$, spełniającym następujące warunki:

1. **Łączność (Asocjatywność):** Dla każdych $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
2. **Element neutralny (Jedność):** Istnieje element $e \in G$ (nazywany elementem neutralnym), taki że dla każdego $a \in G$, $a \cdot e = e \cdot a = a$.
3. **Element odwrotny:** Dla każdego elementu $a \in G$ istnieje element $a^{-1} \in G$ (nazywany elementem odwrotnym do a), taki że $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Jeśli dodatkowo działanie jest przemienne, tzn. $a \cdot b = b \cdot a$ dla wszystkich $a, b \in G$, to grupę nazywamy **grupą abelową** (przemienną).

2.2 Właściwości Grup

- W grupie istnieje dokładnie jeden element neutralny.
- Dla każdego elementu w grupie istnieje dokładnie jeden element do niego odwrotny.
- Dla każdego $a \in G$, $(a^{-1})^{-1} = a$.
- Dla każdych $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.
- **Rząd elementu:** Rząd elementu $a \in G$ to najmniejsza dodatnia liczba całkowita r, taka że $a^r = e$ (element neutralny). Jeśli taka liczba nie istnieje, mówimy, że element ma rząd nieskończony.
- **Twierdzenie Lagrange'a:** Rząd (liczba elementów) dowolnego elementu $a \in G$ jest dzielnikiem rzędu tej grupy (jeśli grupa jest skończona).

2.3 Podgrupy Normalne

Definicja 1. Podgrupa $(H, \cdot)$ grupy $(G, \cdot)$ jest **podgrupą normalną**, jeśli dla każdego $a \in G$ zachodzi równość warstw: $aH = Ha$.

Uwaga 1. Wszystkie podgrupy grup przemiennych są normalne.

2.4 Iloczyny Proste Grup

Dla grup $(G, \cdot_G)$ i $(H, \cdot_H)$, iloczyn prosty $(G \times H, \cdot)$ jest grupą, gdzie działanie jest zdefiniowane element po elemencie: $(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$.

3 Pierścienie i Ciała

3.1 Definicja Pierścienia

Trójkę $(P, +, \cdot)$ nazywamy **pierścieniem**, jeśli spełnia następujące warunki:

1. $(P, +)$ jest grupą przemienną (tzw. grupa addytywna pierścienia). Element neutralny tej grupy nazywamy **zerem pierścienia** i oznaczamy 0.
2. Działanie $\cdot$ jest łączne: dla każdych $a, b, c \in P$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. Działanie $\cdot$ jest obustronnie rozdzielne względem działania $+$: dla każdych $a, b, c \in P$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ oraz $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

Jeśli w pierścieniu istnieje element neutralny mnożenia (tzw. **jedynka pierścienia**, oznaczana 1), to pierścień nazywamy **pierścieniem z jedynką**. Jeśli działanie mnożenia jest przemienne ($a \cdot b = b \cdot a$), to pierścień nazywamy **pierścieniem przemiennym**.

Uwaga 2. Pierścień trywialny to pierścień, którego jedynym elementem jest 0.

3.2 Definicja Ciała

Pierścień $(P, +, \cdot)$ z jedynką (gdzie $1 \neq 0$) nazywamy **ciałem**, jeśli każdy niezerowy element $a \in P$ ma element odwrotny względem mnożenia, tzn. $(P \setminus \{0\}, \cdot)$ jest grupą przemienną.

Uwaga 3. Każde ciało jest pierścieniem przemiennym.

3.3 Przykłady Pierścieni i Ciał

- $(\mathbb{Z}, +, \cdot)$ - pierścień liczb całkowitych (jest pierścieniem przemiennym z jedynką, ale nie jest ciałem, bo np. 2 nie ma elementu odwrotnego w $\mathbb{Z}$).
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ - ciało liczb wymiernych, rzeczywistych, zespolonych.
- $(\mathbb{Z}_n, +_n, \cdot_n)$ - pierścień klas reszt modulo n. Jest to ciało wtedy i tylko wtedy, gdy n jest liczbą pierwszą.
- $K[x]$ - pierścień wielomianów nad ciałem K.

3.4 Ciała Skończone (Ciała Galois)

Ciało skończone ma p^n elementów, gdzie p jest liczbą pierwszą (charakterystyka ciała), a n jest liczbą naturalną. Oznaczamy je jako $GF(p^n)$ (Galois Field).

Uwaga 4. Ciało $GF(p)$ jest izomorficzne z $(\mathbb{Z}_p, +_p, \cdot_p)$.

3.4.1 Charakterystyka Ciała

Definicja 2. Charakterystyka ciała F to najmniejsza dodatnia liczba całkowita n, taka że $n \cdot 1 = 0$, gdzie 1 jest jedynką ciała, a 0 zerem ciała. Jeśli taka liczba nie istnieje, mówimy, że charakterystyka wynosi 0.

Uwaga 5. Charakterystyka każdego ciała skończonego jest liczbą pierwszą. Charakterystyka ciała $GF(p^n)$ wynosi p.

3.4.2 Konstrukcja Ciał Skończonych

Ciała $GF(p^n)$ można skonstruować jako pierścienie ilorazowe $K[x]/(f(x))$, gdzie $K = \mathbb{Z}_p$ i $f(x)$ jest wielomianem nieredukowalnym stopnia n nad K. Elementy ciała to klasy reszt z dzielenia wielomianów przez $f(x)$.

4 Arytmetyka Modularna

4.1 Kongruencje

Definicja 3. Liczba całkowita a przystaje modulo n do liczby całkowitej b ($a \equiv_n b$) wtedy i tylko wtedy, gdy $n|(a-b)$. Innymi słowy, a i b dają tę samą resztę z dzielenia przez n.

Uwaga 6. Relacja kongruencji $\equiv_n$ jest relacją równoważności.

4.2 Właściwości Kongruencji

Dla $a, b, c, d \in \mathbb{Z}$ i $n \in \mathbb{N}$:

- Jeśli $a \equiv_n b$ i $c \equiv_n d$, to $a \pm c \equiv_n b \pm d$.
- Jeśli $a \equiv_n b$ i $c \equiv_n d$, to $a \cdot c \equiv_n b \cdot d$.
- Jeśli $a \equiv_n b$, to dla każdego $k \in \mathbb{N}$, $a^k \equiv_n b^k$.

4.3 Twierdzenie Eulera

Jeśli $a, n \in \mathbb{N}$ oraz $\text{NWD}(a, n) = 1$, to $a^{\varphi(n)} \equiv_n 1$, gdzie $\varphi(n)$ jest funkcją Eulera, która zlicza liczby naturalne mniejsze od n i względnie pierwsze z n.

4.4 Małe Twierdzenie Fermata

Jest to szczególny przypadek twierdzenia Eulera. Jeśli p jest liczbą pierwszą, a a jest liczbą całkowitą niepodzielną przez p, to $a^{p-1} \equiv_p 1$.

4.5 Twierdzenie Wilsona

Liczba naturalna $p > 1$ jest pierwsza wtedy i tylko wtedy, gdy $(p-1)! + 1 \equiv_p 0$.

4.6 Chińskie Twierdzenie o Resztach (CTR)

Chińskie Twierdzenie o Resztach jest fundamentalne w arytmetyce modularnej. Mówi ono, że jeśli mamy układ kongruencji: $x \equiv_{n_1} a_1$ $x \equiv_{n_2} a_2$ ... $x \equiv_{n_k} a_k$ gdzie $n_1, n_2, \ldots, n_k$ są parami względnie pierwsze, to istnieje dokładnie jedno rozwiązanie x modulo $N = n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

5 Przestrzenie Wektorowe

Choć nie są bezpośrednio grupami, pierścieniami czy ciałami, przestrzenie wektorowe opierają się na pojęciu ciała (skalarów) i grupy abelowej (wektorów z dodawaniem).

5.1 Definicja Przestrzeni Wektorowej

Przestrzenią wektorową nad ciałem $\mathbb{K} = (K, +_K, \cdot)$ nazywamy trójkę $((V, +), \mathbb{K}, \bullet)$, gdzie:

1. $(V, +)$ jest grupą przemienną (elementy V to wektory, 0 to wektor zerowy).
2. $\mathbb{K}$ jest ciałem (elementy K to skalary).
3. $\bullet : K \times V \to V$ jest działaniem mnożenia wektora przez skalar, spełniającym dla $\lambda, \mu \in K$ i $v, u \in V$:
   - $(\lambda +_K \mu) \bullet v = \lambda \bullet v + \mu \bullet v$
   - $\lambda \bullet (v + u) = \lambda \bullet v + \lambda \bullet u$
   - $\lambda \bullet (\mu \bullet v) = (\lambda \cdot \mu) \bullet v$
   - $1 \bullet v = v$ (gdzie 1 to jedynka ciała K)

5.2 Baza i Wymiar Przestrzeni Wektorowej

Definicja 4. Układ B wektorów nazywa się **bazą** przestrzeni $V(K)$, jeśli B jest układem liniowo niezależnym i $V(K) = \mathcal{L}(B)$ (liniowa otoczka B).

Definicja 5. Jeśli $V(K)$ ma skończoną bazę, to mówimy, że jest **przestrzenią skończenie wymiarową**. Liczbę elementów (dowolnej) bazy nazywamy **wymiarem** tej przestrzeni i oznaczamy $\dim V(K)$.

Uwaga 7. Wszystkie bazy danej przestrzeni skończenie wymiarowej są równoliczne.

Przykład 1.
- $\dim \mathbb{R}^n(\mathbb{R}) = n$.
- $\dim K_n[x](K) = n + 1$ (przestrzeń wielomianów stopnia co najwyżej n nad ciałem K).

5.3 Odwzorowania Liniowe (Homomorfizmy Przestrzeni Wektorowych)

Definicja 6. Odwzorowanie $F : V(K) \to W(K)$ jest **liniowe** (homomorfizmem), jeśli dla każdych $\lambda \in K$ i $v, u \in V$:

1. $F(v + u) = F(v) + F(u)$ (addytywność)
2. $F(\lambda \bullet v) = \lambda \bullet F(v)$ (jednorodność)

Twierdzenie 1. *Dla dowolnego odwzorowania liniowego $F \in \mathrm{Hom}(V(K), W(K))$, zawsze zachodzi $F(0) = 0$.*

Uwaga 8. Izomorfizm przestrzeni wektorowych to liniowe odwzorowanie odwracalne. Dwie przestrzenie $V(K)$ i $W(K)$ są izomorficzne ($V(K) \cong W(K)$) wtedy i tylko wtedy, gdy $\dim V(K) = \dim W(K)$.

6 Macierze i Wyznaczniki

6.1 Definicja Wyznacznika

Dla macierzy kwadratowej $A \in M_n^n(\mathbb{K})$ (macierzy o elementach z ciała $\mathbb{K}$), wyznacznik macierzy A, oznaczany $\det A$, jest elementem ciała $\mathbb{K}$ zdefiniowanym jako:

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot a_{1\sigma(1)} \cdot \dots \cdot a_{n\sigma(n)}$$

gdzie S_n to zbiór wszystkich permutacji zbioru $\{1, \dots, n\}$, a $\operatorname{sgn}(\sigma)$ to znak permutacji σ.

7 Przykładowe Zadania z Rozwiązaniami

Tutaj przedstawione są kluczowe typy zadań, które powinieneś umieć, aby być dobrze przygotowanym do egzaminu.

7.1 Zadania z Grup i Pierścieni

7.1.1 Zadanie 1: Weryfikacja Własności Grupy Abelowej

Dana jest grupa $(G, \cdot)$ taka, że każdy jej element jest rzędu 2. Pokazać, że $(G, \cdot)$ jest grupą abelową.

Rozwiązanie: Aby grupa $(G, \cdot)$ była grupą abelową, musi spełniać cztery warunki: łączność, istnienie elementu neutralnego, istnienie elementu odwrotnego oraz przemienność. Trzy pierwsze warunki są spełnione z definicji grupy. Pozostaje wykazać warunek przemienności.

Z założenia, każdy element $g \in G$ ma rząd 2. Oznacza to, że jeśli element g pomnożymy przez samego siebie, otrzymamy element neutralny e. Możemy to zapisać jako:

$$g \cdot g = e$$

Pokażmy teraz, że w tej grupie każdy element jest swoim własnym elementem odwrotnym, tzn. $g = g^{-1}$. 1. Zaczynamy od definicji rzędu 2 dla elementu g: $g \cdot g = e$. 2. Mnożymy obie strony równania z lewej strony przez element odwrotny do g, czyli g^{-1}: $g^{-1} \cdot (g \cdot g) = g^{-1} \cdot e$ $(g^{-1} \cdot g) \cdot g = g^{-1}$ (na mocy łączności i definicji elementu neutralnego) $e \cdot g = g^{-1}$ $g = g^{-1}$

Teraz, aby pokazać, że grupa jest abelowa, musimy wykazać, że dla dowolnych $a, b \in G$, $a \cdot b = b \cdot a$. Rozważmy element $a \cdot b$. Zgodnie z tym, co wykazaliśmy, $a \cdot b$ jest rzędu 2, więc: $(a \cdot b) \cdot (a \cdot b) = e$ Mnożymy obie strony równania przez $(a \cdot b)^{-1}$ z prawej strony: $(a \cdot b) \cdot (a \cdot b) \cdot (a \cdot b)^{-1} = e \cdot (a \cdot b)^{-1}$ $a \cdot b = (a \cdot b)^{-1}$

Wiemy również, że $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ (jedna z podstawowych właściwości grup). Zatem: $a \cdot b = b^{-1} \cdot a^{-1}$ Ponieważ każdy element jest swoim własnym elementem odwrotnym ($a = a^{-1}$ i $b = b^{-1}$), możemy podstawić: $a \cdot b = b \cdot a$

Pokazaliśmy, że działanie w grupie jest przemienne. Ponieważ wszystkie pozostałe warunki grupy są spełnione, grupa $(G, \cdot)$ jest grupą abelową.

7.1.2 Zadanie 2: Sprawdzenie, czy struktura jest grupą (M3_C2.pdf, Zadanie 1a)

Sprawdzić, czy operacja $a * b := a + b - ab$ określa grupę na zbiorze $A = \{a \in \mathbb{R} | a \neq 1\}$. Które z tych grup są przemienne?

Rozwiązanie: Zbiór $A = \mathbb{R} \setminus \{1\}$.

1. **Zamkniętość:** Czy dla $a, b \in A$, $a * b \in A$? Zakładamy, że $a, b \in A$, czyli $a \neq 1$ i $b \neq 1$. Chcemy sprawdzić, czy $a + b - ab \neq 1$. Przypuśćmy, że $a + b - ab = 1$. $a + b - ab - 1 = 0$ $a(1 - b) - (1 - b) = 0$ $(a - 1)(1 - b) = 0$ To równanie jest prawdziwe, jeśli $a = 1$ lub $b = 1$. Ale założyliśmy, że $a \neq 1$ i $b \neq 1$. Zatem $a+b-ab$ nigdy nie jest równe 1. Operacja jest zamknięta w A.

2. **Łączność:** Czy $(a * b) * c = a * (b * c)$? $(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c = a + b - ab + c - ac - bc + abc$ $a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a(b + c - bc) = a + b + c - bc - ab - ac + abc$ Lewa strona jest równa prawej stronie. Operacja jest łączna.

3. **Element neutralny:** Czy istnieje $e \in A$ takie, że $a * e = a$ dla każdego $a \in A$? $a + e - ae = a$ $e - ae = 0$ $e(1 - a) = 0$ Ponieważ $a \neq 1$, to $1 - a \neq 0$. Zatem $e = 0$. Element neutralny to 0. Sprawdzamy, czy $0 \in A$. Tak, $0 \neq 1$.

4. **Element odwrotny:** Czy dla każdego $a \in A$ istnieje $a^{-1} \in A$ takie, że $a * a^{-1} = e = 0$? $a + a^{-1} - aa^{-1} = 0$ $a^{-1}(1 - a) = -a$ $a^{-1} = \frac{-a}{1-a} = \frac{a}{a-1}$ Sprawdzamy, czy $a^{-1} \in A$, tzn. czy $a^{-1} \neq 1$. Przypuśćmy, że $\frac{a}{a-1} = 1$. $a = a - 1$ $0 = -1$, co jest sprzecznością. Zatem $a^{-1} \neq 1$, więc $a^{-1} \in A$.

5. **Przemienność:** Czy $a * b = b * a$? $a * b = a + b - ab$ $b * a = b + a - ba$ Ponieważ dodawanie i mnożenie liczb rzeczywistych są przemienne, $a + b - ab = b + a - ba$. Operacja jest przemienna.

Wszystkie warunki są spełnione, więc $(A, *)$ jest grupą abelową.

7.1.3 Zadanie 3: Element odwrotny w pierścieniu (M3_C3.pdf, Zadanie 2)

Znaleźć element odwrotny do 35 w pierścieniu $(\mathbb{Z}_{101}, +_{101}, \cdot_{101})$.

Rozwiązanie: Pierścień $(\mathbb{Z}_{101}, +_{101}, \cdot_{101})$ jest ciałem, ponieważ 101 jest liczbą pierwszą. Szukamy elementu $y \in \mathbb{Z}_{101}$ takiego, że $35 \cdot_{101} y \equiv_{101} 1$. To równanie kongruencji $35y \equiv 1 \pmod{101}$ jest równoważne znalezieniu liczb całkowitych y i k takich, że $35y + 101k = 1$. Użyjemy rozszerzonego algorytmu Euklidesa:

1. $101 = 2 \cdot 35 + 31$
2. $35 = 1 \cdot 31 + 4$
3. $31 = 7 \cdot 4 + 3$
4. $4 = 1 \cdot 3 + 1$ (reszta wynosi 1, więc $\text{NWD}(35, 101) = 1$, element odwrotny istnieje)
5. $3 = 3 \cdot 1 + 0$

Teraz cofamy się w algorytmie, aby wyrazić 1 jako kombinację liniową 101 i 35: Z równania (4): $1 = 4 - 1 \cdot 3$ Podstawiamy 3 z równania (3): $1 = 4 - 1 \cdot (31 - 7 \cdot 4) = 4 - 31 + 7 \cdot 4 = 8 \cdot 4 - 31$ Podstawiamy 4 z równania (2): $1 = 8 \cdot (35 - 1 \cdot 31) - 31 = 8 \cdot 35 - 8 \cdot 31 - 31 = 8 \cdot 35 - 9 \cdot 31$ Podstawiamy 31 z równania (1): $1 = 8 \cdot 35 - 9 \cdot (101 - 2 \cdot 35) = 8 \cdot 35 - 9 \cdot 101 + 18 \cdot 35 = 26 \cdot 35 - 9 \cdot 101$

Mamy równanie $26 \cdot 35 + (-9) \cdot 101 = 1$. Porównując z $35y + 101k = 1$, widzimy, że $y = 26$ i $k = -9$. Zatem elementem odwrotnym do 35 w $\mathbb{Z}_{101}$ jest 26. Sprawdzenie: $35 \cdot 26 = 910$. $910 \pmod{101}$. $910 = 9 \cdot 101 + 1$. Zatem $910 \equiv 1 \pmod{101}$. Wynik jest poprawny.

7.1.4 Zadanie 4: Sprawdzenie, czy pierścień jest ciałem (M3_C2.pdf, Zadanie 19)

Dla $(a, b), (c, d) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ zdefiniujmy $(a, b) \oplus (c, d) = (a +_2 c, b +_2 d)$ oraz $(a, b) \odot (c, d) = (a \cdot_2 c, b \cdot_2 d)$. Czy $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus, \odot)$ tworzy ciało?

Rozwiązanie: Zbiór $\mathbb{Z}_2 \times \mathbb{Z}_2$ składa się z elementów: $\{(0, 0), (0, 1), (1, 0), (1, 1)\}$. Aby struktura była ciałem, każdy niezerowy element musi mieć element odwrotny względem mnożenia. Elementem neutralnym dodawania (zerem pierścienia) jest $(0, 0)$. Elementem neutralnym mnożenia (jedynką pierścienia) jest $(1, 1)$, ponieważ $(a, b) \odot (1, 1) = (a \cdot_2 1, b \cdot_2 1) = (a, b)$.

Sprawdźmy, czy każdy niezerowy element ma element odwrotny względem mnożenia:

- Dla $(0, 1)$: Szukamy (x, y) takie, że $(0, 1) \odot (x, y) = (1, 1)$. $(0 \cdot_2 x, 1 \cdot_2 y) = (1, 1)$ $(0, y) = (1, 1)$ Wynika z tego, że $0 = 1$, co jest sprzecznością w $\mathbb{Z}_2$. Zatem element $(0, 1)$ nie ma elementu odwrotnego względem mnożenia.

Ponieważ znaleźliśmy niezerowy element, który nie ma elementu odwrotnego względem mnożenia, struktura $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus, \odot)$ **nie jest ciałem**. Jest to pierścień przemienny z jedynką.

7.1.5 Zadanie 5: Charakterystyka Ciała (M3_C2.pdf, Zadanie 20)

Znaleźć charakterystyki ciał $GF(121)$, $GF(256)$, $GF(625)$.

Rozwiązanie: Charakterystyka ciała $GF(p^n)$ jest zawsze liczbą pierwszą p.

- Dla $GF(121)$: $121 = 11^2$. Zatem $p = 11$. Charakterystyka wynosi **11**.
- Dla $GF(256)$: $256 = 2^8$. Zatem $p = 2$. Charakterystyka wynosi **2**.
- Dla $GF(625)$: $625 = 5^4$. Zatem $p = 5$. Charakterystyka wynosi **5**.

7.2 Zadania z Arytmetyki Modularnej

7.2.1 Zadanie 6: Obliczanie reszty z dzielenia (M3_C1.pdf, Zadanie 3a)

Obliczyć resztę z dzielenia liczby 59^{45} przez 13.

Rozwiązanie: Chcemy obliczyć $59^{45} \pmod{13}$. Najpierw zredukujemy podstawę modulo 13: $59 = 4 \cdot 13 + 7$, więc $59 \equiv_{13} 7$. Teraz problem sprowadza się do obliczenia $7^{45} \pmod{13}$. Ponieważ 13 jest liczbą pierwszą, możemy użyć Małego Twierdzenia Fermata, które mówi, że dla liczby pierwszej p i liczby całkowitej a niepodzielnej przez p, $a^{p-1} \equiv_p 1$.

W naszym przypadku $p = 13$, więc $p-1 = 12$. Zatem $7^{12} \equiv_{13} 1$. Teraz dzielimy wykładnik 45 przez 12: $45 = 3 \cdot 12 + 9$. Więc, $7^{45} = 7^{3 \cdot 12+9} = (7^{12})^3 \cdot 7^9$. $7^{45} \equiv_{13} (1)^3 \cdot 7^9 \equiv_{13} 7^9$.

Teraz obliczamy $7^9 \pmod{13}$ krok po kroku: $7^1 \equiv_{13} 7$ $7^2 = 49 \equiv_{13} 10 \equiv_{13} -3$ $7^3 \equiv_{13} 7 \cdot (-3) = -21 \equiv_{13} 5$ $7^4 \equiv_{13} 7 \cdot 5 = 35 \equiv_{13} 9 \equiv_{13} -4$ $7^5 \equiv_{13} 7 \cdot (-4) = -28 \equiv_{13} -2 \equiv_{13} 11$ $7^6 \equiv_{13} 7 \cdot (-2) = -14 \equiv_{13} -1$ (Alternatywnie, wiedząc $7^6 \equiv_{13} -1$, możemy policzyć $7^9 = 7^6 \cdot 7^3 \equiv_{13} (-1) \cdot 5 = -5 \equiv_{13} 8$). Dokończmy obliczanie 7^9 bez pośredniego -1: $7^7 \equiv_{13} 7 \cdot 11 = 77 \equiv_{13} 12 \equiv_{13} -1$ (co potwierdza $7^6 \equiv_{13} -1$ bo $7^7 \equiv_{13} 7^1 \cdot (7^2)^3 \equiv_{13} 7 \cdot (49)^3 \equiv_{13} 7 \cdot (10)^3 \equiv_{13} 7 \cdot 1000 \equiv_{13} 7 \cdot (13 \cdot 76 + 12) \equiv_{13} 7 \cdot 12 \equiv_{13} 84 \equiv_{13} 6 \cdot 13 + 6 \equiv_{13} 6 \pmod{13}$. Błąd w obliczeniach, co pokazuje jak łatwo o pomyłki, sprawdzam ponownie: $7^1 \equiv_{13} 7$ $7^2 \equiv_{13} 49 \equiv_{13} 10$ $7^3 \equiv_{13} 7 \cdot 10 = 70 \equiv_{13} 5 \cdot 13 + 5 \equiv_{13} 5$ $7^4 \equiv_{13} 7 \cdot 5 = 35 \equiv_{13} 9$ $7^5 \equiv_{13} 7 \cdot 9 = 63 \equiv_{13} 4 \cdot 13 + 11 \equiv_{13} 11$ $7^6 \equiv_{13} 7 \cdot 11 = 77 \equiv_{13} 5 \cdot 13 + 12 \equiv_{13} 12 \equiv_{13} -1$ OK, $7^6 \equiv_{13} -1$ jest poprawne. $7^9 = 7^6 \cdot 7^3 \equiv_{13} (-1) \cdot 5 = -5 \equiv_{13} 8$.

Reszta z dzielenia liczby 59^{45} przez 13 wynosi **8**.

7.2.2 Zadanie 7: Znajdowanie elementu odwrotnego (Mat3_Egzamin0_zadanie4.pdf)

Znajdź element odwrotny do $x = 43$ w ciele $(\mathbb{Z}_{79}, +, \cdot)$.

Rozwiązanie: Chcemy znaleźć takie $y \in \mathbb{Z}_{79}$, dla którego spełnione jest równanie kongruencji: $43 \cdot y \equiv 1 \pmod{79}$. Do znalezienia elementu odwrotnego wykorzystamy rozszerzony algorytm Euklidesa. Chcemy znaleźć takie liczby całkowite y i k, dla których spełnione jest równanie: $43y + 79k = 1$.

Kroki algorytmu Euklidesa dla NWD$(79, 43)$:

1. $79 = 1 \cdot 43 + 36$
2. $43 = 1 \cdot 36 + 7$
3. $36 = 5 \cdot 7 + 1$ (Reszta wynosi 1, co oznacza, że NWD$(79, 43) = 1$, a więc element odwrotny istnieje)
4. $7 = 7 \cdot 1 + 0$

Teraz, cofamy się w algorytmie (podstawiamy reszty z równań w górę), aby wyrazić 1 jako kombinację liniową 79 i 43: Z równania (3): $1 = 36 - 5 \cdot 7$ Z równania (2), podstawiamy $7 = 43 - 1 \cdot 36$: $1 = 36 - 5 \cdot (43 - 1 \cdot 36)$ $1 = 36 - 5 \cdot 43 + 5 \cdot 36$ $1 = 6 \cdot 36 - 5 \cdot 43$ Z równania (1), podstawiamy $36 = 79 - 1 \cdot 43$: $1 = 6 \cdot (79 - 1 \cdot 43) - 5 \cdot 43$ $1 = 6 \cdot 79 - 6 \cdot 43 - 5 \cdot 43$ $1 = 6 \cdot 79 - 11 \cdot 43$

Mamy równanie $1 = (-11) \cdot 43 + 6 \cdot 79$. Porównując to z $43y + 79k = 1$, otrzymujemy $y = -11$. Ponieważ działamy w $\mathbb{Z}_{79}$, musimy zredukować -11 modulo 79: $-11 \equiv_{79} -11 + 79 \equiv_{79} 68$. Zatem elementem odwrotnym do 43 w $\mathbb{Z}_{79}$ jest **68**.

Sprawdzenie: $43 \cdot 68 = 2924$. $2924 \pmod{79}$: $2924 = 37 \cdot 79 + 1$. $2924 \equiv_{79} 1$. Wynik jest poprawny.

7.2.3 Zadanie 8: Chińskie Twierdzenie o Resztach (M3_C1.pdf, podobne do Zadania 1c, ale z CTR)

Rozwiązać układ kongruencji: $x \equiv_3 2$ $x \equiv_5 3$ $x \equiv_7 2$

Rozwiązanie: Mamy $n_1 = 3, a_1 = 2$; $n_2 = 5, a_2 = 3$; $n_3 = 7, a_3 = 2$. Moduły są parami względnie pierwsze (NWD$(3, 5) = 1$, NWD$(3, 7) = 1$, NWD$(5, 7) = 1$). Obliczamy $N = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 5 \cdot 7 = 105$. Obliczamy $N_i = N/n_i$: $N_1 = 105/3 = 35$ $N_2 = 105/5 = 21$ $N_3 = 105/7 = 15$

Teraz znajdujemy $N_i^{-1} \pmod{n_i}$ (elementy odwrotne):

- Dla $N_1 = 35 \pmod 3$: $35 \equiv_3 2$. Szukamy y_1 takie, że $2y_1 \equiv_3 1$. $2 \cdot 2 = 4 \equiv_3 1$. Zatem $y_1 = 2$.
- Dla $N_2 = 21 \pmod 5$: $21 \equiv_5 1$. Szukamy y_2 takie, że $1y_2 \equiv_5 1$. Zatem $y_2 = 1$.
- Dla $N_3 = 15 \pmod 7$: $15 \equiv_7 1$. Szukamy y_3 takie, że $1y_3 \equiv_7 1$. Zatem $y_3 = 1$.

Rozwiązanie x jest dane wzorem: $x \equiv_N a_1N_1y_1 + a_2N_2y_2 + a_3N_3y_3 \pmod N$ $x \equiv_{105} 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}$ $x \equiv_{105} 140 + 63 + 30 \pmod{105}$ $x \equiv_{105} 233 \pmod{105}$

Zredukujmy $233 \pmod{105}$: $233 = 2 \cdot 105 + 23$. $x \equiv_{105} 23$.

Sprawdzenie: $23 \pmod 3$: $23 = 7 \cdot 3 + 2 \implies 23 \equiv_3 2$ (OK) $23 \pmod 5$: $23 = 4 \cdot 5 + 3 \implies 23 \equiv_5 3$ (OK) $23 \pmod 7$: $23 = 3 \cdot 7 + 2 \implies 23 \equiv_7 2$ (OK)

Rozwiązaniem jest $x \equiv 23 \pmod{105}$.

7.3 Zadania z Macierzy i Przestrzeni Wektorowych

7.3.1 Zadanie 9: Rząd macierzy (M3_C3.pdf, Przykład na końcu strony)

Znaleźć rząd macierzy (przekształcając ją do postaci schodkowej):

$$A = \begin{pmatrix} 2 & 1 & -1 & 1 & 3 & -1 \\ 0 & 1 & 7 & -5 & 1 & 5 \\ 2 & 2 & 6 & -4 & 4 & 4 \\ -2 & -1 & 1 & -1 & -3 & 1 \\ 0 & -1 & -7 & 5 & 2 & 1 \end{pmatrix}$$

Rozwiązanie: Rząd macierzy to liczba niezerowych wierszy w jej postaci schodkowej. Wykonujemy operacje elementarne na wierszach (jak w przykładzie w pliku): $R_3 \leftarrow R_3 - R_1$ $R_4 \leftarrow R_4 + R_1$ $R_5 \leftarrow R_5 + 0 \cdot R_1$ (już jest 0 w pierwszej kolumnie, więc nie trzeba zmieniać)

$$A \sim \begin{pmatrix} 2 & 1 & -1 & 1 & 3 & -1 \\ 0 & 1 & 7 & -5 & 1 & 5 \\ 0 & 1 & 7 & -5 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -7 & 5 & 2 & 1 \end{pmatrix}$$

Teraz: $R_3 \leftarrow R_3 - R_2$ $R_5 \leftarrow R_5 + R_2$

$$A \sim \begin{pmatrix} 2 & 1 & -1 & 1 & 3 & -1 \\ 0 & 1 & 7 & -5 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 6 \end{pmatrix}$$

Teraz, aby uzyskać postać schodkową, zamieniamy wiersze R_3 i R_5: $R_3 \leftrightarrow R_5$

$$A \sim \begin{pmatrix} 2 & 1 & -1 & 1 & 3 & -1 \\ 0 & 1 & 7 & -5 & 1 & 5 \\ 0 & 0 & 0 & 0 & 3 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Otrzymana macierz ma 3 niezerowe wiersze. Zatem rząd macierzy wynosi **3**.

7.3.2 Zadanie 10: Odwzorowanie liniowe (Mat3_wyklad_4_slajdy_2024.pdf, Przykład na stronie 18)

Sprawdź, czy odwzorowanie $F : \mathbb{R}^2 \to \mathbb{R}^2$, zdefiniowane jako $F([x_1, x_2]) = [3x_1 + x_2 + 1, 2x_1 - 3x_2]$, jest odwzorowaniem liniowym.

Rozwiązanie: Aby odwzorowanie było liniowe, musi spełniać dwa warunki: addytywność i jednorodność. Alternatywnie, wystarczy sprawdzić, czy $F(0) = 0$. Jeśli $F(0) \neq 0$, to odwzorowanie na pewno nie jest liniowe.

Sprawdzamy $F([0, 0])$: $F([0, 0]) = [3 \cdot 0 + 0 + 1, 2 \cdot 0 - 3 \cdot 0] = [1, 0]$. Ponieważ $F([0, 0]) = [1, 0] \neq [0, 0]$ (wektor zerowy w $\mathbb{R}^2$), odwzorowanie F **nie jest** odwzorowaniem liniowym.

Jeśli chcesz, możemy również sprawdzić to za pomocą definicji addytywności (co też pokaże, dlaczego nie jest liniowe): Weźmy $u = [u_1, u_2]$ i $v = [v_1, v_2]$. $F(u + v) = F([u_1 + v_1, u_2 + v_2]) = [3(u_1 + v_1) + (u_2 + v_2) + 1, 2(u_1 + v_1) - 3(u_2 + v_2)]$ $F(u + v) = [3u_1 + 3v_1 + u_2 + v_2 + 1, 2u_1 + 2v_1 - 3u_2 - 3v_2]$

Teraz obliczamy $F(u) + F(v)$: $F(u) = [3u_1 + u_2 + 1, 2u_1 - 3u_2]$ $F(v) = [3v_1 + v_2 + 1, 2v_1 - 3v_2]$ $F(u) + F(v) = [(3u_1 + u_2 + 1) + (3v_1 + v_2 + 1), (2u_1 - 3u_2) + (2v_1 - 3v_2)]$ $F(u) + F(v) = [3u_1 + u_2 + 3v_1 + v_2 + 2, 2u_1 - 3u_2 + 2v_1 - 3v_2]$

Porównując $F(u + v)$ i $F(u) + F(v)$: Pierwsza składowa: $(3u_1 + 3v_1 + u_2 + v_2 + 1)$ vs $(3u_1 + u_2 + 3v_1 + v_2 + 2)$. Różnią się stałą $+1$. Zatem $F(u + v) \neq F(u) + F(v)$, co potwierdza, że F nie jest odwzorowaniem liniowym.

8 Wskazówki do Egzaminu

- **Definicje:** Naucz się na pamięć definicji grupy, pierścienia, ciała, podgrupy normalnej, przestrzeni wektorowej, bazy i odwzorowania liniowego. Zrozumieć każdy warunek!
- **Przykłady i kontrprzykłady:** Zrozumienie, dlaczego pewne zbiory z działaniami są lub nie są grupami/pierścieniami/ciałami jest kluczowe. Przykłady z $\mathbb{Z}_n$ i $\mathbb{R}$ są podstawą.
- **Algorytm Euklidesa:** Musisz umieć sprawnie używać rozszerzonego algorytmu Euklidesa do znajdowania elementu odwrotnego w $\mathbb{Z}_n$.
- **Twierdzenia Eulera i Fermata:** Wiedz, kiedy ich używać i jak upraszczać potęgi modulo n.
- **Chińskie Twierdzenie o Resztach:** Zrozumiej i przećwicz kroki rozwiązywania układów kongruencji.
- **Wymiar i baza:** Umieć znajdować bazę i wymiar przestrzeni wektorowej.
- **Rząd macierzy:** Bądź w stanie przekształcać macierz do postaci schodkowej w celu określenia jej rzędu.
- **Odwzorowania liniowe:** Wiedz, jak sprawdzać, czy dane odwzorowanie jest liniowe. Pamiętaj o warunku $F(0) = 0$.

Mam nadzieję, że ta notatka będzie dla Ciebie pomocna w przygotowaniach do egzaminu! Powodzenia!