Algebra 2020/21 — Egzamin

Czas: 180 minut.

Liczba zadań: 9.

Każde zadanie należy złożyć w osobnym pliku w systmie SKOS. W przypadku zadań rachunkowych rozwiązanie powinno zawierać opis dokonywanych operacji oraz kroki pośrednie obliczeń; *zadanie nie spełniające tego warunku mogą nie być sprawdzane.* W przypadku dowodu rozwiązanie powinno być czytelną wypowiedzią, a nie jedynie zbiorem symbolicznych przekształceń.

Zadanie 1.

Pokaż, że macierz jest odwracalna wtedy i tylko wtedy, gdy nie ma wartości własnej 0.

Pokaż, że dla macierzy odwracalnej A liczba λ jest wartością własną wtedy i tylko wtedy, gdy λ^{-1} jest wartością własną macierzy A^{-1} i że mają one te same krotności geometryczne.

Rozwiązanie

- Wiemy, że λ jest wartością własną macierzy $M \iff \det(M - \lambda \,\mathrm{Id}) = 0$
- macierz M jest odwracalna $\iff \det(M) \neq 0$

Podstawiając λ w pierwszym punkcie i negując obie strony dostajemy
0 nie jest wartością własną $M \iff \det M \neq 0 \iff M$ jest odwracalna, co daje pierwszą część zadania.

Pokażemy, że $\vec{V}$ jest wektorem własnym M dla wartości własnej $\lambda \neq 0$ wtedy i tylko wtedy, gdy $\vec{V}$ jest wektorem własnym dla wartości własnej λ^{-1} macierzy M^{-1}. Ty samym przestrzenie wektorów własnych M dla λ i M^{-1} dla λ^{-1} są takie same. W szczególności mają ten sam wymiar, czyli maje λ dla M i λ^{-1} dla m^{-1} mają te same krotności geometryczne.
$\vec{V}$ jest wektorem własnym dla wartości własnej λ (dla macierzy M)

$\iff$

$M\vec{V} = \lambda V$

$\implies$ (mnożemy obie strony przez $\lambda^{-1} m^{-1}$)

$\lambda^{-1}\vec{V} = M^{-1}\vec{V}$

To pokazuje, że jeśli $\vec{V}$ jest wektorem własnym dla wartości własnej λ dla macierzy M, to również $\vec{V}$ jest wektorem własnym dla wartości własnej λ^{-1} dla macierzy M^{-1}.

Analogicznie pokazujemy w drugą stronę, tj. jeśli $\vec{V}$ jest wektorem własnym dla wartości własnej λ^{-1} dla macierzy M^{-1} to $\vec{V}$ jest wektorem własnym dla wartości własnej λ dla macierzy M, co kończy dowód.

Zadanie 2.
Dla grupy permutacji $G \leq S_n$ niech $G_p \subseteq G$ będzie zbiorem wszystkich permutacji parzystych z G. Pokaż, że G_p jest podgrupą G oraz że G_p ma albo $|G|$ albo $|G|/2$ elementów.

Rozwiązanie Sprawdamy warunki bycia podgrupą:

niepustość Permutacja identycznościowa jest parzysta;

zamknięcie na działanie Iloczyn dwóch permutacji parzystych jest permutacją parzystą

element odwrotny w grupie skończonej element odwrotny do g jest dodatnią potęgą g, tak wiec ten punkt wynika z poprzedniego.

Jeśli $G_p = G$ to oczywiście $|G_p| = |G|$. Jeśli nie, to niech $g \in G \setminus G_p$. Oczywiscie g jest permutacją nieparzystą. Wtedy gG_p zawiera same permutacje nieparzyste oraz $|G_p| = |gG_p|$ (bo są to warstwy tej samej grupy). Pokażemy, że $G = G_p \cup gG_p$. Weźmy dowolne $h \in G$. Jeśli jest parzyste, to $h \in G_p$. Jeśli jest nieparzyste, to $g^{-1}h$ jest parzyste i tym samym $g^{-1}h \in G_p$ i w takim razie $h = gg^{-1}h \in gG_p$, co kończy dowód.

Zadanie 3.
Dla jakich wartości parametru $\lambda \in \mathbb{Z}_2$ poniższa macierz o elementach z ciała $\mathbb{Z}_2$ jest odwracalna? Dla jednej z takich wartości λ podaj macierz odwrotną do zadanej.

$$\begin{bmatrix} 1 & \lambda & 1 & \lambda \\ 1 & 1 & 1 & 1 \\ 0 & 0 & \lambda & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Zadanie 4.
Układamy łańcuszek zawierający $2p$ korali, gdzie p jest nieparzystą liczbą pierwszą. Koraliki są z jednej strony białe, a z drugiej czarne. Łańcuszek można obracać, oraz „przekładać na drugą stronę”, przy czym przełożenie na drugą stronę powoduje zmianę koralików białych na czarne i odwrotnie, np. po przełożeniu na drugą stronę łańcuszek składający się z jednego białego i $2p-1$ czarnych korali będzie miał jeden koral czarny i $2p-1$ białych. Łańcuszki uznajemy za nierozróżnialne, jeżeli jeden można uzyskać z drugiego przez obracanie i/lub przekładanie na drugą stronę, i za rozróżnialne w przeciwnym przypadku.

Ile jest rozróżnialnych łańcuszków?

Przykładowo, jest jeden rozróżnialny łańcuszek, który ma wszystkie korale tego samego koloru oraz jeden, który ma jeden koral jednego koloru oraz pozostałe drugiego koloru.

Rozwiązanie Jeśli ustawimy korale łańcuszka we wierzchołkach $2p$-kąta foremnego, to grupę działającą na zbiór łańcuszków będzie można utożsamić z grupą izometrii tego wielokąta, zawierającą po $2p$ obrotów oraz odbić. Działanie tej grupy na łańcuszki jest klasyczne za wyjątkiem (niektórych) odbić, ze względu na „zmienianie się kolorów” korali.

Ponieważ oczywiście chcemy policzyć orbity tego działania za pomocą lematu Burnside’a, sklasyfikujmy elementy tej grupy pod względem mocy zbiorów ich punktów stałych.

- Identyczność (obrót o 0 korali): wszystkie $2p$ korali dobieramy niezależnie, $|\operatorname{fix}(e)| = 2^{2p}$.
- Pozostałe $p-1$ obrotów o parzystą liczbę korali: korale przechodzą na siebie w ramach dwóch rozłącznych zbiorów ułożonych naprzemiennie na łańcuszku, których kolory dobieramy niezależnie, $|\operatorname{fix}(g)| = 2^2$.
- Obrót o kąt π, tj. p korali: korale przechodzą na siebie w p parach położonych po przeciwnych stronach łańcuszka; ich kolory dobieramy niezależnie, $|\operatorname{fix}(g)| = 2^p$.
- Pozostałe $p-1$ obrotów o nieparzystą liczbę korali: wszystkie korale przechodzą na siebie nawzajem; wybieramy tylko jeden kolor, $|\operatorname{fix}(g)| = 2$.
- p odbić względem osi przechodzących przez środki przeciwległych boków: korale przechodzą na siebie (zmieniając kolor!) w p parach równo odległych od boków, które przecina oś symetrii; stany tych par dobieramy niezależnie, $|\operatorname{fix}(g)| = 2^p$.
- p odbić względem osi przechodzących przez przeciwległe wierzchołki: brak punktów stałych, ponieważ nie da się ustalić koloru korali leżących na osi symetrii; $|\operatorname{fix}(g)| = 0$.

Zauważmy, że w stosunku do „typowego” działania grupy izometrii na łańcuszek zwyczajnych, jednokolorowych korali, opis zmienił się tylko dla odbić, a wynik – tylko dla ostatniego typu odbić.

Zliczając wkłady poszczególnych typów elementów grupy do wzoru z lematu Burnside’a, otrzymujemy wynik:

$$\#\text{orbit} = \frac{1}{|G|}\sum_{g\in G} |\operatorname{fix}(g)| = \frac{2^{2p} + (p-1)\cdot 2^2 + 2^p + (p-1)\cdot 2 + p\cdot 2^p + p\cdot 0}{4p}.$$

Czy ten wynik jest całkowity?

Tak. Licznik można przedstawić jako $(4^p - 4) + (2^p - 2) + (2^p + 6)p$ (gdzie dwa pierwsze nawiasy są podzielne przez p na mocy małego twierdzenia Fermata, a reszta jawnie) lub jako $2^p(2^p+p+1)+6(p-1)$ (gdzie składniki są podzielne przez 4, ponieważ p jest odpowiednio nie mniejsze niż 2 oraz nieparzyste).

Trochę bardziej systematycznie o klasyfikacji obrotów

Dla łańcuszka o k koralach przyjmujących jeden z c kolorów obrót g rzędu r przeprowadza na siebie nawzajem zbiory korali mocy r (które dla elementów $\mathrm{fix}(g)$ muszą być jednego koloru) rozmieszczonych co k/r. Takich zbiorów jest więc k/r i $|\,\mathrm{fix}(g)| = c^{k/r}$.

Konieczne jest określenie liczby obrotów o danym rzędzie $r|k$: są to obroty o n korali, gdzie $0 < n \le k$ oraz $\mathrm{nwd}(n,k) = k/r$ (bo jest to „odległość” między najbliższymi różnymi koralami przeprowadzanymi na siebie nawzajem). Równoważnie, dla $n' = nr/k$ (to jest liczba całkowita, bo k/r jest dzielnikiem n) mamy $0 < n' \le r$ oraz $\mathrm{nwd}(n', r) = 1$. Takich n' jest więc z definicji $\varphi(r)$.

W naszym przykładzie mamy $k = 2p$ (oraz $c = 2$) i następujące możliwości:

- $r = 1$: $\varphi(1) = 1$ obrót trywialny, $|\,\mathrm{fix}(e)| = 2^{2p/1}$;
- $r = 2$: $\varphi(2) = 1$ obrót o kąt π, $|\,\mathrm{fix}(g)| = 2^{2p/2}$;
- $r = p$: $\varphi(p) = p - 1$ obrotów o parzyście wiele korali, $|\,\mathrm{fix}(g)| = 2^{2p/p}$;
- $r = 2p$: $\varphi(2p) = \varphi(2)\varphi(p) = p - 1$ obrotów o nieparzyście wiele korali, $|\,\mathrm{fix}(g)| = 2^{2p/2p}$.

Zadanie 5.

Najmniejsza wspólna wielokrotność dwóch wielomianów $f, g \in \mathbb{F}[x]$ o współczynnikach z ciała $\mathbb{F}$ to taki wielomian $h \in \mathbb{F}[x]$, że

- $f|h$ i $g|h$
- dla dowolnego wielomianu $h' \in \mathbb{F}[x]$ jeśli $f|h'$ i $g|h'$ to $h|h'$.

Pokaż, że dla $f, g \in \mathbb{F}[x]$ ich najmniejsza wspólna wielokrotność istnieje i przedstaw, jak ją można wydajnie policzyć.

Rozwiązanie Pokażmy najpierw pomocniczy fakt: jeśli $p_1, \ldots, p_k$ są wielomianami nierozkładalnymi, takimi że $\text{nwd}(p_i, p_j) = 1$ dla $i \neq j$ to dla ciągów liczb naturalnych $\alpha_1, \ldots, \alpha_k$ oraz $\beta_1, \ldots, \beta_k$ zachodzi

$$\prod_{i=1}^{k} p_i^{\alpha_i} | \prod_{i=1}^{k} p_i^{\beta_i} \iff \forall_i \alpha_i \leq \beta_i$$

Fakt ten zapewne bym pokazywany na ćwiczeniach przy oakzji listy 14.

$\Leftarrow$ Taz jest oczywista, gdyż

$$\prod_{i=1}^{k} p_i^{\beta_i} = \prod_{i=1}^{k} p_i^{\alpha_i} \cdot \prod_{i=1}^{k} p_i^{\beta_i - \alpha_i}$$

i z warunku $\forall_i \beta_i \geq \alpha_i$ dostajemy, że $\prod_{i=1}^{k} p_i^{\beta_i - \alpha_i}$ jest wielomianem, czyli $\prod_{i=1}^{k} p_i^{\alpha_i} | \prod_{i=1}^{k} p_i^{\beta_i}$.

$\Rightarrow$ Skoro $\prod_{i=1}^{k} p_i^{\alpha_i} | \prod_{i=1}^{k} p_i^{\beta_i}$, to dla każdego i mamy, że $p_i^{\alpha_i} | \prod_{j=1}^{k} p_j^{\beta_j}$. Przedstawmy wielomian $\prod_{j=1}^{k} p_j^{\beta_j}$ jako iloczyn $\beta = \sum_{i=1}^{k} \beta_i$ wielomianów nierozkładalnych $p_1 \cdot p_1 \cdots p_2 \cdots p_k$. Wtedy z Zadania z listy 14 istnieją liczby $\gamma_1, \ldots, \gamma_\beta$, takie że $p_i^{\gamma_j}$ dzieli j-ty element powyższego ciągu oraz suma wszystkich γ_j to α_i. Ale dla wyrazów odpowiadających p_i odpowiadajace γ_j to najwyżej 1, zaś dla pozostałych: 0 (bo $p_i \nmid p_j$ dla $i \neq j$). Czyli otrzymujemy, że $\alpha_i \leq \beta_i$, co należało pokazać.

Przejdźmy do właściwej treści zadania. Bez zmniejszenia ogólności możemy założyć, że wielomiany f, g mają wiodący współczynnik 1: przemnożenie przez stałą nie wpływa na podzielność. Wielomiany te można przedstawić (twierdzenie z listy ćwiczeniowej) jako iloczyny potęg wielomianów nierozkładalnych, gdzie $\text{nwd}(p_i, p_j) = 1$ dla $i \neq j$: niech

$$f = \prod_{i=1}^{k} p_i^{\alpha_i}$$
$$g = \prod_{i=1}^{k} p_i^{\beta_i}$$

gdzie $\alpha_i, \ldots, \alpha_k$ oraz $\beta_1, \ldots, \beta_k$ są liczbami naturalnymi (może być, że któraś potęga to 0, uzupełniamy listy wielomianów nierozkładalnych dla f, g do jednej wspólnej). Rozpatrzmy wielomian

$$h = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$$

Z pokazanego faktu dostajemy od razu, że $f|h$ oraz $g|h$. Niech wielomian h' (o wiodącym współczynniku) będzie taki, że $f|h', g|h'$, przedstawmy go jako iloczyn potęg wielomianów nierozkładalnych (o wiodących współczynnikach 1), uwzględnijmy w tym iloczynie wszystkie wielomiany $p_1, \ldots, p_k$, z potęgami 0, jeśli nie było ich w rozkładzie h'. Wtedy

$$h' = \prod_{i=1}^{k'} p_i^{\gamma_i}$$

Z pokazanego faktu, skoro $f|h'$ oraz $g|h'$ to dla $i = 1, \ldots, k$ mamy $\alpha_i, \beta_i \leq \gamma_i$. Ale w takim razie (ponownie z pokazanego faktu), również $h|h'$, co należało pokazać.

Co do obliczeń, analogicznie (symetrycznie) pokazujemy, że

$$\mathrm{nwd}(f,g) = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)}$$

i tym samym (korzystając z równości $a + b = \min(a,b) + \max(a,b)$) dostajemy, że

$$h \cdot \mathrm{nwd}(f,g) = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)+\min(\alpha_i,\beta_i)} = \prod_{i=1}^{k} p_i^{\alpha_i+\beta_i} = fg$$

i w takim razie

$$h = \frac{fg}{\mathrm{nwd}(f,g)}$$

i możemy wyliczyć h w następujący sposób: wyliczyć $\mathrm{nwd}(f,g)$, wyliczyć $f/gcd(f,g)$ i pomnożyć przez g.

Zadanie 6.
Dane są dwa układy wektorów w przestrzeni $\mathbb{R}^5$ (nad ciałem $\mathbb{R}$): $S = \left\{ \begin{bmatrix} 3 & -1 & 1 & 1 & 5 \end{bmatrix}^T, \begin{bmatrix} 0 & 5 & -2 & 4 & -1 \end{bmatrix}^T \right\}$ i $T = \left\{ \begin{bmatrix} 1 & -5 & 3 & -3 & 3 \end{bmatrix}^T, \begin{bmatrix} -1 & -3 & 3 & -2 & 0 \end{bmatrix}^T \right\}$. Ile wynoszą wymiary $\mathrm{LIN}(S \cup T)$ oraz $\mathrm{LIN}(S) \cap \mathrm{LIN}(T)$? Podaj dowolną bazę $\mathrm{LIN}(S \cup T)$.

Zadanie 7.
Dane jest ciało skończone $\mathbb{F}$ o n elementach. Pokaż, że dla $0 < d < n - 1$ zachodzi

$$\sum_{\alpha \in \mathbb{F}} \alpha^d = 0$$

Wskazówka: Co wiesz o grupie $\mathbb{F}^*$?

Rozwiązanie Grupa multiplikatywna ciała skończonego jest cykliczna, więc dla jej ustalonego generatora g mamy

$$\sum_{\alpha \in \mathbb{F}} \alpha^d = 0^d + \sum_{\alpha \in \mathbb{F}^*} \alpha^d = \sum_{i=1}^{n-1} g^{id}.$$

Jest to suma szeregu geometrycznego (o ilorazie $g^d \neq 1$ ze względu na warunek na d) równa $g^d(1 - g^{d(n-1)})(1 - g^d)^{-1}$, co z kolei równe jest 0, gdyż $(g^{n-1})^d = 1^d = 1$.

Jeśli użycie pojęcia szeregu geometrycznego w abstrakcyjnym ciele budzi niepokój (i nie pamiętamy wyprowadzenia zwartego wzoru na sumę na tyle dobrze, by wiedzieć, że można je przeprowadzić również tu), możemy zamiast tego (właściwie powtarzając to wyprowadzenie) przemnożyć tę sumę przez $1 - g^d$ i otrzymać

$$\sum_{i=1}^{n-1} g^{id} - \sum_{i=2}^{n} g^{id} = g^d - g^{nd} = g^d(1 - (g^{n-1})^d) = 0.$$

Ponieważ $1 - g^d \neq 0$, możemy z powrotem podzielić strony otrzymanej równości przez jego odwrotność i po raz kolejny stwierdzić, że nasza suma jest równa 0.

Zadanie 8.
Ile rozwiązań ma poniższy układ równań nad $\mathbb{Z}_{13}$ w zależności od parametru $\lambda \in \mathbb{Z}_{13}$?

$$\begin{cases} x + y + \lambda z = \lambda \\ (3-\lambda)x + 2y + (1+\lambda)z = 1 \\ 5x + 3y + 2z = 2 \end{cases}.$$

Zadanie 9.
Rozważmy macierz

$$\frac{1}{6} \cdot \begin{bmatrix} 5 & -2 & 1 \\ -2 & 2 & 2 \\ 1 & 2 & 5 \end{bmatrix}$$

oraz indukowane przekształcenie liniowe P.

1. Pokaż, że P jest rzutem.

2. Oblicz bazę $\ker P$.

3. Pokaż, że P jest rzutem prostopadłym.

Wskazówka: W trzecim punkcie możesz skorzystać z punktu drugiego.