Podstawy matematyki – egzamin 2 lutego 2024

1. Niech $\mathsf{P}_{\text{fin}}(\mathbb{N})$ oznacza zbiór wszystkich skończonych podzbiorów zbioru $\mathbb{N}$. Relacja $\sim$ w zbiorze funkcji $\mathbb{N} \to \mathsf{P}_{\text{fin}}(\mathbb{N})$ jest określona tak: $f \sim g$ zachodzi wtedy i tylko wtedy, gdy dla każdego $n \in \mathbb{N}$ zbiory $f(n)$ i $g(n)$ mają tyle samo elementów.

   (a) Udowodnić, że $\sim$ jest relacją równoważności.

   (b) Jaka jest moc zbioru ilorazowego relacji $\sim$?

   (c) Jakie liczby kardynalne są mocami klas abstrakcji relacji $\sim$?

2. Dla dowolnego $n \in \mathbb{N}$, przez $\phi(n)$ oznaczymy zbiór wszystkich dzielników[1] liczby n, tj. $\phi(n) = \{k \in \mathbb{N} \mid k \,|\, n\}$. Niech $g : \mathsf{P}(\mathbb{N}) \to \mathsf{P}(\mathbb{N})$ będzie taka, że $g(A) = \bigcup_{n \in A} \phi(n)$, dla $A \in \mathsf{P}(\mathbb{N})$.

   (a) Czy funkcja g jest różnowartościowa?

   (b) Czy funkcja g jest na $\mathsf{P}(\mathbb{N})$?

   (c) Udowodnić, że funkcja g jest retrakcją, tj. $g \circ g = g$.

   (d) Jakiej mocy jest zbiór wszystkich punktów stałych[2] funkcji g?

3. Niech $X = \{a, b\}^*$. Dla $w \in X$ oraz $x \in \{a, b\}$ przez $\#_x(w)$ oznaczmy liczbę wystąpień litery x w słowie w. W zbiorze X określamy relację $\sqsubseteq$ następująco: dla $w, v \in X$ przyjmujemy $w \sqsubseteq v$ wtedy i tylko wtedy, gdy

$$w \preceq v \wedge \langle \#_a(w), \#_b(w) \rangle \leq \langle \#_a(v), \#_b(v) \rangle,$$

   gdzie $\preceq$ oznacza porządek leksykograficzny w X (przy czym $a \prec b$), a $\leq$ oznacza porządek leksykograficzny w $\mathbb{N}^2$. Wiadomo, że $\sqsubseteq$ jest częściowym porządkiem w X.

   (a) Czy w $\langle X, \sqsubseteq \rangle$ istnieje nieskończony antyłańcuch?

   (b) Czy zbiór $A = \{ab^n \mid n \in \mathbb{N}\}$ ma kres górny w $\langle X, \sqsubseteq \rangle$?

   (c) Czy istnieje taki zbiór $V \subseteq X$, że porządek $\langle V, \sqsubseteq \rangle$ jest izomorficzny z $\langle \mathbb{N}^2, \leq \rangle$?

   (d) Czy istnieje taki zbiór $U \subseteq X$, że porządek $\langle U, \sqsubseteq \rangle$ jest izomorficzny z $\langle X, \preceq \rangle$?

Uwaga: W rozwiązaniach można się powoływać na ogólnie znane fakty (np. z wykładu, skryptu, wspólnych zadań domowych).

---

[1] Uwaga: $k \,|\, n$ wtedy i tylko wtedy, gdy istnieje takie $\ell \in \mathbb{N}$, że $k \cdot \ell = n$. Przy tej definicji $\phi(0) = \mathbb{N}$.

[2] Punkt stały, to takie B, że $g(B) = B$.

Rozwiązania

1a: Relacja $\sim$ jest jądrem przekształcenia $F : (\mathbb{N} \to \mathsf{P}_{\text{fin}}(\mathbb{N})) \to (\mathbb{N} \to \mathbb{N})$, które każdej funkcji $f : \mathbb{N} \to \mathsf{P}_{\text{fin}}(\mathbb{N})$ przypisuje operację $F(f) = \lambda n.\,\overline{\overline{f(n)}}$.

1b: Jest to zbiór mocy continuum. Ponieważ zbiór $\mathbb{N} \to \mathsf{P}_{\text{fin}}(\mathbb{N})$ jest mocy $\aleph_0^{\aleph_0} = \mathfrak{C}$, więc nierówność $\overline{\overline{(\mathbb{N} \to \mathsf{P}_{\text{fin}}(\mathbb{N}))/_\sim}} \leq \mathfrak{C}$ jest oczywista. Aby oszacować moc z dołu, określimy dla każdego $A \in \mathsf{P}(\mathbb{N})$ funkcję $\xi_A = \lambda n.\,\texttt{if}\ n \in A\ \texttt{then}\ \{0\}\ \texttt{else}\ \varnothing$. Wtedy dla każdego zbioru A klasa $[\xi_A]_\sim$ jest inna, bo $\overline{\overline{\xi_A(n)}} = \texttt{if}\ n \in A\ \texttt{then}\ 1\ \texttt{else}\ 0$. A więc mamy różnowartościowe przyporządkowanie $\zeta : \mathsf{P}(\mathbb{N}) \xrightarrow{1-1} (\mathbb{N} \to \mathsf{P}_{\text{fin}}(\mathbb{N}))/_\sim$ określone tak: $\zeta(A) = [\xi_A]_\sim$.

1c: Dla $f : \mathbb{N} \to \mathsf{P}_{\text{fin}}(\mathbb{N})$ niech $A_f = \{n \mid f(n) \neq \varnothing\}$. Niech $\mathsf{P}_{\text{fin+}}(\mathbb{N}) = \mathsf{P}_{\text{fin}}(\mathbb{N}) - \{\varnothing\}$ i niech $H(g) = g{\restriction}_{A_f}$, dla $g \sim f$. Wtedy H jest injekcją $H : [f]_\sim \xrightarrow{1-1} (A_f \to \mathsf{P}_{\text{fin+}}(\mathbb{N}))$. Istotnie, jeśli $g_1, g_2 \in [f]_\sim$, to $g_1(n) = g_2(n) = \varnothing$ dla $n \notin A_f$, więc jeśli funkcje g_1, g_2 są różne, to tylko dlatego, że $g_1{\restriction}_{A_f} \neq g_2{\restriction}_{A_f}$.

A zatem moc klasy $[f]_\sim$ jest ograniczona z góry przez moc zbioru funkcji $A_f \to \mathsf{P}_{\text{fin+}}(\mathbb{N})$, czyli przez $\aleph_0^{\mathfrak{m}}$, gdzie $\mathfrak{m} = \overline{\overline{A_f}}$. Pokażemy, że także $\aleph_0^{\mathfrak{m}} \leq \overline{\overline{[f]_\sim}}$, konstruując funkcję różnowartościową $G : (A_f \to \mathbb{N}) \xrightarrow{1-1} [f]_\sim$. Dla wygody przyjmijmy takie oznaczenie: jeśli $A \subseteq \mathbb{N}$, $k \in \mathbb{N}$, to $A + k = \{a + k \mid a \in A\}$. Na przykład $\{1, 3, 4\} + 2 = \{3, 5, 6\}$. Dla dowolnego $\xi : A_f \to \mathbb{N}$ przyjmijmy teraz $G(\xi)(n) = f(n) + \xi'(n)$, gdzie $\xi'(n) = \texttt{if}\ n \in A_f\ \texttt{then}\ \xi(n)\ \texttt{else}\ 0$. Wtedy $G(\xi) \sim f$, bo moc zbioru $A + k$ jest zawsze taka sama jak moc zbioru A, więc G jest dobrze określona. Jest też rożnowartościowa, bo jeśli $\xi_1(n) \neq \xi_2(n)$ dla jakiegoś $n \in A_f$, to także $G(\xi_1)(n) \neq G(\xi_2)(n)$.

Na mocy twierdzenia Cantora-Bernsteina, klasa $[f]_\sim$ jest dokładnie mocy $\aleph_0^{\mathfrak{m}}$. Są trzy możliwości. Jeśli $A_f = \varnothing$, to $\mathfrak{m} = 0$, $\aleph_0^0 = 1$ i klasa $[f]_\sim$ ma jeden element (jest to funkcja stale równa $\varnothing$). Jeśli zbiór A_f jest skończony i ma $k > 0$ elementów, to $\overline{\overline{[f]_\sim}} = \aleph_0^k = \aleph_0$. A jeśli zbiór A_f jest nieskończony, to ma moc $\aleph_0$ i wtedy $\overline{\overline{[f]_\sim}} = \aleph_0^{\aleph_0} = \mathfrak{C}$. Szukane liczby kardynalne to 1, $\aleph_0$ i $\mathfrak{C}$.

2a: Nie, na przykład $g(\{1, 2\}) = g(\{2\}) = \{1, 2\}$.

2b: Nie, na przykład $\{0\} \notin \mathrm{Rg}(g)$. Istotnie, ponieważ $1 \in \phi(n)$ dla każdego n, więc $1 \in g(A)$, dla każdego niepustego A. Ponadto $g(\varnothing) = \varnothing$.

2c: Mamy udowodnić, że $g(g(B)) = g(B)$ dla dowolnego zbioru B. Najpierw zauważmy, że skoro $g(B) = \bigcup\{\phi(n) \mid n \in B\}$, to mamy taką równoważność:

$$x \in g(B) \Leftrightarrow \exists n.\, n \in B \wedge x \,|\, n.$$

A zatem jeśli $x \in g(g(B))$, to istnieje takie $n \in g(B)$, że x dzieli n. Ale skoro $n \in g(B)$, to istnieje takie $b \in B$ że n dzieli b. No ale wtedy x dzieli b, więc $x \in g(B)$. Inkluzja odwrotna wynika z ogólniejszej obserwacji, że $X \subseteq g(X)$ dla każdego X. W rzeczy samej, jeśli $x \in X$, to także $x \in g(X)$, bo $x \,|\, x \in X$.

2d: Należy ustalić moc zbioru $\mathcal{Z} = \{B \mid g(B) = B\}$.

Z części 2c wynika, że $\mathcal{Z} = \mathrm{Rg}(g)$. Oczywiście $\mathcal{Z} \subseteq \mathsf{P}(\mathbb{N})$, więc $\overline{\overline{\mathcal{Z}}} \leq \mathfrak{C}$. Aby zobaczyć, że również zachodzi $\overline{\overline{\mathcal{Z}}} \geq \mathfrak{C}$, rozpatrzmy obcięcie funkcji g do zbioru $\mathsf{P}(\mathcal{P})$, gdzie $\mathcal{P}$ to zbiór wszystkich liczb pierwszych. To obcięcie jest różnowartościowe, bo jeśli $\varnothing \neq A \subseteq \mathcal{P}$, to $g(A) = A \cup \{1\}$, a jeśli $A = \varnothing$, to $g(A) = \varnothing$. A zatem obraz $g(\mathsf{P}(\mathcal{P}))$ jest mocy continuum, skąd $\overline{\overline{\mathcal{Z}}} \geq \mathfrak{C}$.

3a: Przykładem nieskończonego antyłańcucha jest zbiór $\{a^n b \mid n \in \mathbb{N}\}$. Jeśli bowiem $n < m$, to $a^n b \succ a^m b$, ale $\langle \#_a(a^n b), \#_b(a^n b)\rangle = \langle n, 1\rangle < \langle m, 1\rangle = \langle \#_a(a^m b), \#_b(a^m b)\rangle$ i w konsekwencji słowa $a^n b$ i $a^m b$ są nieporównywalne.

3b: Kresem górnym tego zbioru jest słowo baa. Jest ono ograniczeniem górnym zbioru A ponieważ $ab^n \preceq baa$ oraz $\langle \#_a(ab^n), \#_b(ab^n)\rangle = \langle 1, n\rangle < \langle 2, 1\rangle = \langle \#_a(baa), \#_b(baa)\rangle$. Aby udowodnić, że to kres, rozpatrzmy dowolne ograniczenie górne w zbioru A, tj. takie w, że $ab^n \sqsubseteq w$, dla każdego n. W szczególności $a \sqsubseteq w$, zatem słowo w jest niepuste.

Przypadek 1: $w = av$, dla pewnego v. Z tego, że $ab^n \sqsubseteq av$, wynika w szczególności, że $b^n \preceq v$. A to niemożliwe dla wszystkich n.

Przypadek 2: $w = bv$, dla pewnego v. Wtedy $\langle \#_a(ab^n), \#_b(ab^n)\rangle = \langle 1, n\rangle \leq \langle \#_a(v), \#_b(v) + 1\rangle$, dla dowolnego n. To jest możliwe tylko wtedy, gdy v ma co najmniej dwie litery a. (Nie może być tylko jedna, bo $n \not\leq \#_b(v) + 1$ dla dostatecznie dużych n.) Wtedy oczywiście $aa \preceq v$, skąd $baa \preceq bv = w$. Ponadto $\langle \#_a(baa), \#_b(baa)\rangle = \langle 2, 1\rangle \leq \langle \#_a(bv), \#_b(bv)\rangle$, więc ostatecznie $w = bv \sqsubseteq baa$, i możemy napisać $baa = \sup A$.

3c: Na przykład $V = \{b^n a^n b^k \mid n, k \in \mathbb{N} \wedge n > 0\}$. Przyporządkowanie $\alpha : \mathbb{N} \times \mathbb{N} \to V$ określone równaniem $\alpha(n, k) = b^{n+1}a^{n+1}b^k$ jest żądanym izomorfizmem. Istotnie, jeśli $\langle m, k\rangle \leq \langle n, \ell\rangle$ to albo $m < n$ albo $m = n$ i $k \leq \ell$. W obu przypadkach $b^{m+1}a^{m+1}b^k \preceq b^{n+1}a^{n+1}b^\ell$ oraz $\langle m + 1, m + k\rangle \leq \langle n + 1, n + \ell\rangle$.

W drugą stronę: jeśli $b^{m+1}a^{m+1}b^k \sqsubseteq b^{n+1}a^{n+1}b^\ell$, to w szczególności $m \leq n$. Przy tym jeśli $m = n$, to $k \leq \ell$. Czyli $\langle m, k\rangle \leq \langle n, \ell\rangle$.

3d: Nie, nie istnieje taki podzbiór U. Porządek $\sqsubseteq$ jest dobrze ufundowany. Istotnie, gdyby istniał nieskończony ciąg malejący $w_1 \sqsupset w_2 \sqsupset \ldots$ to mielibyśmy w szczególności nieskończony ciąg $\langle \#_a(w_1), \#_b(w_1)\rangle \geq \langle \#_a(w_2), \#_b(w_2)\rangle \geq \ldots$ Ponieważ porządek leksykograficzny w $\mathbb{N} \times \mathbb{N}$ jest dobrze ufundowany, więc ciąg ten od pewnego miejsca byłby stały. A zatem od tego miejsca wszystkie słowa miałyby tę samą liczbę liter a i tę samą liczbę liter b. To jest niemożliwe, bo takich słów jest tylko skończenie wiele, wiec nie mogą tworzyć nieskończonego ciągu ściśle malejącego.

Z kolei w porządku $\preceq$ można stworzyć nieskończony ciąg malejący, np. $b \succ ab \succ aab \succ \ldots$ a zatem nie może istnieć monotoniczna injekcja z porządku $\langle X, \preceq\rangle$ w porządek $\langle X, \sqsubseteq\rangle$. A tym bardziej izomorfizm.