Wstęp do matematyki
Zbiory, liczby, struktury

Zadania

Bohdan Grell

Pamięci Andrzeja Mostowskiego (1913–1975)

Spis treści

Przedmowa

Książka ta jest w pewnym sensie uzupełnieniem mojego *Wstępu do matematyki* z 2006 roku. Jest jednak od tej ostatniej pozycji całkowicie niezależna. Ma na celu dostarczenie wszystkim zainteresowanym matematyką jako całością, przede wszystkim nauczycielom i studentom matematyki, zbioru zadań uzupełniających i rozszerzających materiał części I i II wspomnianej książki (zbiory i relacje, liczby porządkowe i kardynalne, kategorie, podstawowe struktury matematyczne).

Część zadań ma charakter techniczny, ale starałem się unikać zadań banalnych; w zamierzeniu zadania powinny być raczej trudne, ciekawe i inspirujące – mają propagować metody, „chwyty", a także nowe pojęcia i ich własności. Zadania trudniejsze są oznaczone gwiazdką.

Wszystkie zadania zaopatrzono w mniej lub bardziej rozbudowane odpowiedzi i niekiedy komentarze. Zaleca się odczytywać odpowiedzi, szczególnie do zadań trudniejszych i bardziej rozbudowanych, partiami, stopniowo – starając się szukać rozwiązań samodzielnie. Zadania są w dużej części standardowe i w związku z tym nie podaję ich pochodzenia (podręczniki, monografie, zbiory zadań).

Prezentowany zbiór zawiera dziewięć rozdziałów, z których każdy składa się z trzech części:

1. Wstęp – podstawowe definicje, oznaczenia i twierdzenia
2. Tematy zadań
3. Odpowiedzi.

Starałem się zachować w miarę możności terminologię i oznaczenia ze wspomnianego *Wstępu do matematyki* z 2006 roku. Wprowadziłem jednak niewielkie modyfikacje, dążąc do zachowania złotego środka między racjonalnością a tradycją.

W poszczególnych rozdziałach zdarzają się powtórzenia, zwykle ze względu na rozszerzenie znaczenia danego terminu lub oznaczenia – ewentualne wątpliwości rozstrzyga kontekst.

Odesłania do literatury mają postać: [**Mostowski 48**] w przypadku jednego autora, [**Graham... 02**], gdy autorów jest więcej.

1

Język teorii mnogości, elementy logiki, dedukcja naturalna

1.1. Wstęp

Alfabet języka elementarnego (pierwszego rzędu) $\mathrm{L}_{\mathrm{set}}$ *teorii mnogości* składa się z następujących symboli:

$$\in,\quad =,\quad \neg\,,\quad \vee,\quad \wedge,\quad \Longrightarrow,\quad \Longleftrightarrow,\quad \exists,\quad \forall,\quad (,\quad),\quad \Box,\quad \Box',\quad \Box'',\quad \ldots$$

Są to: *przynależność* (dokładniej — *symbol przynależności*), *równość*, *negacja*, *alternatywa*, *koniunkcja*, *implikacja*, *równoważność*, *kwantyfikator istnienia* (*mały, egzystencjalny*), *kwantyfikator ogólności* (*duży, uniwersalny*), *nawiasy — lewy i prawy*, oraz *zmienne*, których jest nieskończenie wiele (potencjalnie) i są one ustawione — jak mówimy — w *porządku naturalnym* (*leksykograficznym*).

Symbole przynależności i równości to *predykaty* — lub inaczej: *symbole relacyjne* (*dwuargumentowe*). Pozostałe symbole alfabetu języka $\mathrm{L}_{\mathrm{set}}$ to *symbole logiczne*; w szczególności pięć symboli — od negacji do równoważności — to *spójniki* (*funktory*) zdaniowe.

Symbol równości (*identyczności*) też jest zaliczany do symboli logicznych, gdyż występuje on we wszystkich rozważanych w praktyce matematycznej językach elementarnych, chociaż samo pojęcie identyczności nie jest jednoznaczne i oczywiste (identyczność cząstek elementarnych, sprzężenie kwantowe). Najbliższa intuicji jest definicja Leibniza mówiąca o identyczności nieodróżnialnych (*identitas indiscernibilium*). Jedynym symbolem pozalogicznym (matematycznym) języka $\mathrm{L}_{\mathrm{set}}$ jest więc symbol przynależności.

Słowem nazywamy dowolny skończony ciąg symboli naszego alfabetu. *Katenacją* (*złożeniem*) słów A, B nazywamy słowo AB.

Formułą atomiczną lub *formułą klasy 0* nazywamy każde słowo postaci $x \in y$ (czytamy: x *należy* do y, y *obejmuje* x) lub $x = y$, gdzie x i y są zmiennymi.

W powyższym sformułowaniu użycie liter A, B, x, y jest — jak mówimy — *metajęzykowe*. Formuły atomiczne możemy ustawić w ciąg w porządku leksykograficznym:

$$\Box \in \Box,\quad \Box = \Box,\quad \Box \in \Box',\quad \Box = \Box',\quad \Box' \in \Box,\quad \Box' = \Box$$
$$\Box' \in \Box',\quad \Box' = \Box',\quad \Box \in \Box'',\quad \Box = \Box'',\quad \Box' \in \Box'', \ldots$$

Zakładamy, że w metajęzyku, którym jest dla nas odpowiednio rozbudowany i uściślony język polski, dysponujemy *matematyką naturalną*, inaczej *finitystyczną*.

Zawiera ona arytmetykę *liczb naturalnych* $0, 1, 2, \ldots$ łącznie z *zasadą indukcji* i *twierdzeniem o definiowaniu indukcyjnym*. W matematyce naturalnej dopuszczamy tylko *nieskończoność potencjalną*: $n \mapsto n+1$, dla $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$. Nie przyjmujemy *nieskończoności aktualnej*: $\mathcal{P}\mathbb{N} = \{X : X \subset \mathbb{N}\} = ?$ (zob. [**Mostowski 48**, s. 172, 220, 266]).

W metajęzyku długość słowa A oznaczać będziemy przez $|A|$, np. $|\Box \in \Box'| = 3$. Dokładniej, słowo A jest funkcją (ciągiem) $A : I_n \longrightarrow \text{Alfabet}$, gdzie dla $n \in \mathbb{N}$, $I_n = \{1, \ldots, n\} = \{k \in \mathbb{N} | 1 \leqslant k \leqslant n\}$, i wówczas $|A| = n$, zaś dla $k \in I_n$, $A(k)$ jest k-tym znakiem (wyrazem) słowa A.

Oczywiście dla dwóch słów A i B, $|AB| = |A| + |B|$.

W powyższych zapisach symbole $\in$ i $=$ oznaczają przynależność i równość w metajęzyku — w zasadzie należałoby używać jakichś innych oznaczeń, na przykład stosować pogrubienie: $\boldsymbol{\in}$, $\boldsymbol{=}$ itp. W praktyce używa się tych samych symboli, odwołując się do kontekstu.

Słowo A nazywamy *formułą klasy* $n+1$, gdzie $n \in \mathbb{N}$, gdy jest ono formułą klasy n lub ma jedną z postaci: $\neg B$, $(B \vee C)$, $(B \ \wedge \ C)$, $(B \implies C)$, $(B \iff C)$, $\exists\, x\; B$, $\forall\, x\; B$, gdzie B i C są formułami klasy n, zaś x jest zmienną. Słowo A nazywamy *formułą*, gdy dla pewnego naturalnego n jest formułą klasy n; najmniejsze takie n nazywamy *stopniem złożenia* lub *złożonością* formuły A.

Dla zmiennej x i formuły A określamy indukcją na złożoność A zbiór liczb naturalnych $\mathrm{Bd}(x, A) \subset \mathbb{N}$ zwany *zakresem związania zmiennej x w formule A*:

1° Jeżeli A jest zmienną atomiczną, to $\mathrm{Bd}(x, A) = \varnothing =$ *zbiór pusty*.
2° Dla formuł B, C i dwu różnych zmiennych x i y ($x \neq y$):
- jeśli $A = \neg B$, to $\mathrm{Bd}(x, A) = 1 + \mathrm{Bd}(x, A) := \{1 + k | k \in \mathrm{Bd}(x, A)\}$
- jeśli $A = (B \vee C)$, to $\mathrm{Bd}(x, A) = (1 + \mathrm{Bd}(x, B)) \cup (2 + |B| + \mathrm{Bd}(x, C))$ i analogicznie dla spójników $\wedge$, $\implies$, $\iff$
- jeśli $A = \exists\, x\; B$ lub $A = \forall\, x\; B$, to $\mathrm{Bd}(x, A) = \{1, 2, \ldots, 2 + |B|\}$
- jeśli $A = \exists\, y\; B$ lub $A = \forall\, y\; B$, to $\mathrm{Bd}(x, A) = 2 + \mathrm{Bd}(x, B)\}$.

Liczbę k nazywamy *wystąpieniem* zmiennej x w formule A, gdy $k \in \{1, 2, \ldots, |A|\}$ i $A(k) = x$; wystąpienie takie nazywamy *związanym*, gdy $k \in \mathrm{Bd}(x, A)$, w przeciwnym wypadku mówimy, że wystąpienie jest *wolne*. Ogół wystąpień wolnych zmiennej x w formule A oznaczamy $\mathrm{Fr}(x, A)$; tak więc:

$$\mathrm{Fr}(x, A) = \{k \in I_{|A|} | A(k) = x \ \wedge \ k \notin \mathrm{Bd}(x, A)\}.$$

Mówimy, że zmienna x jest *wolna* w formule A, gdy $\mathrm{Fr}(x, A) \neq \varnothing$; ogół takich zmiennych oznaczamy $\mathrm{Fr}(A)$. Formułę A nazywamy *zdaniem*, gdy $\mathrm{Fr}(A) = \varnothing$.

Dla dowolnej formuły A oznaczamy przez $\forall \ldots A$ jej *domknięcie uniwersalne*, to jest zdanie $\forall\, x_1 \ldots \forall\, x_n A$, gdzie $x_1, \ldots, x_n$ są wszystkimi w kolejności alfabetycznej zmiennymi wolnymi formuły A. W dalszym ciągu, mówiąc o jakiejś formule jako o zdaniu, będziemy mieli na myśli domknięcie uniwersalne tej formuły.

Dla dwu zmiennych x, y i formuły A oznaczamy przez $[A, x \mapsto y]$ formułę otrzymaną przez *podstawienie* zmiennej y w miejsce każdego wolnego wystąpienia zmiennej x w formule A (dokładna definicja — indukcja na złożoność A); podstawienie takie nazywamy *poprawnym* (lub *akceptowalnym*), gdy $\mathrm{Fr}(x, A) \cap \mathrm{Bd}(y, A) = \varnothing$.

Jako *aksjomatykę teorii mnogości* przyjmujemy zbiór zdań oznaczony jako ZFC i opisany w rozdziale 3 wraz z poniższymi czterema zdaniami zwanymi *aksjomatami równości*, gdzie x, y, z, t to kolejne zmienne $\square, \square', \ldots$:

1. $x = x$ (*zwrotność*)
2. $x = y \implies y = x$ (*symetria*)
3. $(x = y \ \wedge \ y = z) \implies x = z$ (*przechodniość*)
4. $(x = y \ \wedge \ z = t) \implies (x \in z \iff y \in t)$ (*podstawianie równych za równe*).

Zdanie A nazywamy *twierdzeniem* lub *zdaniem prawdziwym*, gdy można je udowodnić, wychodząc z aksjomatów za pomocą *dedukcji logicznej* (*naturalnej*). Ścisła definicja jest indukcyjna:

1. Aksjomaty są *twierdzeniami klasy 0*.

2. Dla ustalonego $n = 0, 1, 2\ldots$ zdanie A jest *twierdzeniem klasy* $n+1$ wtt (= wtedy i tylko wtedy), gdy istnieje ciąg formuł $\neg A = F_0, F_1, \ldots, F_m$ (*dowód nie wprost* zdania A), taki, że:

1° w ciągu $F_0, F_1, \ldots, F_m$ wystąpiła *sprzeczność*, tzn. $F_i = \neg F_j$ dla pewnych $i, j \in \{0, 1, \ldots, m\}$

2° dla każdego $k \in \{1, \ldots, m\}$ formuła F_k jest twierdzeniem klasy n lub można ją otrzymać z formuł $F_0, F_1, \ldots, F_{k-1}$, stosując jedną z poniższych szesnastu *pierwotnych reguł wnioskowania*:

R1 Istnieją $i, j \in \{0, 1, \ldots, k-1\}$ oraz takie formuły B i C, że $F_i = (B \implies C)$, $F_j = B$, $F_k = C$. Mówimy, że jest to *reguła odrywania implikacji* (*modus ponens*); notujemy ją krótko: $(B \Rightarrow C), B \vdash C$. Znak $\vdash$ jest metajęzykowym *symbolem dedukcji*. Podobnie w krótki już sposób podamy pozostałe reguły (B, C — formuły, x, y — zmienne):

R2 $\neg\neg B \vdash B$

R3 $\neg(B \implies C) \vdash (B \ \wedge \ \neg C)$

R4 $(B \vee C), \neg B \vdash C$

R5 $(B \vee C), \neg C \vdash B$

R6 $\neg(B \vee C) \vdash (\neg B \ \wedge \ \neg C)$

R7 $(B \ \wedge \ C) \vdash B$

R8 $(B \ \wedge \ C) \vdash C$

R9 $\neg(B \ \wedge \ C) \vdash (\neg B \vee \neg C)$

R10 $(B \iff C) \vdash (B \implies C)$

R11 $(B \iff C) \vdash (C \implies B)$

R12 $\neg(B \iff C) \vdash ((B \ \wedge \ \neg C) \vee (C \ \wedge \ \neg B))$

R13 $\exists x \ B \vdash [B, x \mapsto y]$, jeśli podstawienie $x \mapsto y$ jest poprawne w B oraz zmienna y nie występuje wolno w żadnej z formuł $F_0, F_1, \ldots, F_{k-1}$ poprzedzających formułę $F_k = [B, x \mapsto y]$

R14 $\forall x \, B \vdash [B, x \mapsto y]$, jeśli podstawienie $x \mapsto y$ jest poprawne w formule B

R15 $\neg\exists x \, B \vdash \forall x \, \neg B$

R16 $\neg\forall x \, B \vdash \exists x \, \neg B$.

3° Zdanie A jest twierdzeniem, jeżeli dla pewnego n jest twierdzeniem klasy n.

Łatwo widać, że twierdzenie klasy n jest twierdzeniem klasy $n+1$ ⟨Dowód nie wprost zdania A: $\neg A, A$⟩ oraz że każde twierdzenie jest twierdzeniem klasy 2, a więc istnieją tylko trzy klasy twierdzeń: 0-a, 1-a i 2-a. Jest to tzw. (meta)*twierdzenie o redundancji* (*o zbyteczności*) ⟨Stosując indukcję na n, stwierdzamy, że wystarczy udowodnić, iż twierdzenia A klasy 3 jest twierdzeniem klasy 2. Niech $\neg A = F_0, F_1, \dots, F_m$ będzie dowodem nie wprost zdania A jako twierdzenia klasy 3. Zastosujemy indukcję na liczbę twierdzeń dokładnie klasy 2 występujących w ciągu $F_1, \dots, F_m$. Jeżeli F_k jest pierwszym takim twierdzeniem, to bierzemy jego dowód nie wprost jako twierdzenia klasy 2: $\neg F_k = G_0, G_1, \dots, G_p$. Oznaczmy przez $C_1, \dots, C_r$ wszystkie twierdzenia klasy 1 występujące w ciągu $G_1, \dots, G_p$. Wówczas, jak łatwo sprawdzić, zdanie $D = (C_1 \implies (C_2 \implies \dots C_r \implies F_k) \dots)$ jest twierdzeniem klasy 1. Jeżeli teraz w ciągu $F_1, \dots, F_m$ w miejsce F_k wpiszemy zdanie D, a następnie zdanie $C_1, \dots, C_r$, to stosując r razy regułę *modus ponens*, dojdziemy do zdania F_k; zmniejszamy w ten sposób o 1 liczbę twierdzeń klasy 2 w naszym dowodzie zdania A⟩.

Samo pojęcie klasy twierdzenia ma w naszym systemie charakter techniczny — wprowadza się je w celu ścisłego sformułowania definicji prawdziwości (formalnej) zdania — wystarczy, żeby w dowodzie nie wprost zdania A, $\neg A = F_0, F_1, \dots, F_m$ w ciągu $F_1, \dots, F_m$ występowały jedynie twierdzenia już poprzednio udowodnione.

Zauważmy jeszcze, że w przedstawionym powyżej systemie dedukcji naturalnej *dowód wprost* zdania A może być traktowany jako szczególny przypadek dowodu nie wprost $\neg A = F_0, F_1, \dots, F_m$, w którym nie wykorzystuje się początkowego założenia $F_0 = \neg A$, zwanego *hipotezą dowodu nie wprost*.

Definicje — traktowane jako metajęzykowe skróty — będą notowane w postaci $A := B$ lub $A \;:\iff\; B$, gdzie zapis A jest skrótem dla formuły B (w zasadzie należałoby pisać $A \mathrel{\mathbf{:=}} B$).

Na przykład $x \notin y :\iff \neg x \in y$ lub $x \subset y \;:\iff\; \forall\, z(z \in x \implies z \in y)$. W tej ostatniej definicji *inkluzji* litera z oznacza pierwszą leksykograficznie zmienną różną od zmiennych x, y. Jest to ogólna zasada wprowadzona dla zapewnienia jednoznaczności odczytu skrótu definicyjnego — w dalszym ciągu jej stosowanie będzie domyślne.

Oprócz tych definicji ścisłych będziemy stosować różne ogólnie przyjęte skróty umowne.

W szczególności:

1° Opuszczanie zewnętrznych nawiasów (np. $A \vee B$ oznaczać będzie $(A \vee B)$).

2° Domyślne łączenie nawiasów od strony prawej w wieloczłonowych alternatywach i koniunkcjach (np. $A \vee B \vee C$ oznaczać będzie $A \vee (B \vee C)$).

3° Przyjęcie zasady, że spójniki $\vee$ i $\wedge$ wiążą silniej niż $\implies$ i $\iff$ (np. $\neg A \vee B \implies C$ oznaczać będzie $(\neg A \vee B) \implies C$).

4° Przyjęcie zasady blokowania symboli jednomiennych; $\forall\, x\, y\; A$ oznacza $\forall\, x\; \forall\, y\; A$, $x, y \in z$ oznacza $x \in z \wedge y \in z$ itp.

5° Użycie kwantyfikatorów z ograniczonym zakresem; $\exists\, \underset{A}{x}\; B \;:\iff\; \exists\, x\; (A \wedge B)$, $\forall\, \underset{A}{x}\; B \;:\iff\; \forall\, x\; (A \implies B)$ i dalsze tego rodzaju skróty, np. $\forall\, x \in z\; A \;:\iff\; \forall\, x\; (x \in z \implies A)$.

W przekształceniach logicznych kwantyfikatory z ograniczonym zakresem zachowują się tak jak zwykłe kwantyfikatory, np. $\neg \forall\, x \in z\; A \iff \exists\, x \in z\; \neg A$.

Twierdzenie, w którego dowodzie nie korzysta się z żadnych aksjomatów, nazywamy *tautologią czystą*; takimi są np. zdania $(A \implies B) \implies (\neg B \implies \neg A)$, $\exists\, x\, \forall\, y\ A \implies \forall\, y\, \exists\, x\ A$, gdzie A i B są dowolnymi formułami.

Dopuszczając aksjomaty równości, będziemy mówili o *tautologiach*.

Każde twierdzenie postaci $A_1 \implies (A_2 \implies \ldots (A_n \implies B)\ldots)$ prowadzi do reguły wtórnej $A_1, \ldots, A_n \vdash B$. Ogólnie *regułą wtórną* nazywamy każdy skrót dowodowy pozwalający opuszczać bloki (ciągi formuł) w dowodach formalnych. Tak na przykład tautologia $(A \implies B) \implies (\neg B \implies \neg A)$ prowadzi do reguły wtórnej $A \implies B, \neg B \vdash \neg A$ zwanej *modus tollens*.

Poniższe dwie reguły wtórne są szczególnie ważne:

— *Reguła dołączenia dodatkowego założenia* (*reguła rozpatrywania przypadków*).

Jeżeli, budując dowód formalny $F_0, F_1, \ldots, F_m$, dołączymy do niego formułę $\neg G$ i rozwijając ciąg $F_0, F_1, \ldots, F_m, \neg G$ przez stosowanie reguł i dopisywanie twierdzeń dojdziemy do sprzeczności, to do ciągu wyjściowego można *poprawnie* dopisać formułę G, zwaną w tej sytuacji *dodatkowym założeniem* (formuły $\neg G$ i G to przypadki; oczywiście przypadków może być więcej — indukcja), tzn. ciąg formuł $F_0, F_1, \ldots, F_m$ można przedłużyć, stosując reguły i dopisując twierdzenia, aż uzyskamy G.

Dzieje się tak, gdyż — jak łatwo sprawdzić — zdanie $F_0 \implies (F_1 \implies \ldots \implies (F_m \implies G)\ldots)$ jest wówczas twierdzeniem.

— *Reguła podstawiania równych za równe*.

Jeżeli podstawienia $x \mapsto y$ i $x \mapsto z$ w formule F są poprawne, to zdanie:

$$y = z \implies ([F, x \mapsto y] \iff [F, x \mapsto z])$$

jest tautologią.

Można to łatwo wykazać indukcją na złożoność formuły F.

Na zakończenie zauważmy, że współczesne kryterium ścisłości to możliwość pełnej formalizacji — dowody powinny być tak zredagowane, żeby czytelnik orientujący się w przedmiocie był przekonany o możliwości pełnej ich formalizacji.

W dalszym ciągu skrót HP: (od HIPOTEZA) oznaczać będzie początek dowodu nie wprost, a znak $\lightning$ („zaiskrzyło") jego zakończenie, tj. stwierdzenie pojawienia się sprzeczności. Zapis $\exists\, x)F$ lub $\exists)\, x \ldots\ F$ w przypadku użycia kwantyfikatora z ograniczonym zakresem sygnalizować będzie użycie reguły oderwania małego kwantyfikatora (**R13**) z podstawieniem tożsamościowym $x \mapsto x$ (czytamy: „istnieje x $(\ldots)$ takie, że F; ustalmy takie x").

Dowody zapisywać będziemy w nawiasach: $\langle\ ,\ \rangle$. Ze względu na regułę dołączania dodatkowego założenia możliwe są „spiętrzenia" $\langle \ldots\ \langle \ldots \rangle \ldots \rangle$, ale w przypadku bardziej złożonych dowodów lepiej jest formułować pomocnicze twierdzenia, tak zwane *lematy*.

1.2. Tematy

1*. Określimy *system formalny*:

— *alfabet*: $X = \{a, b\}$, $a \neq b$

— *słowa* (zamiast aa piszemy a^2 itp.); zbiór wszystkich słów to $W = \{\varnothing, a, b, a^2, ab, ba, b^2, a^3, a^2b, aba, \ldots\}$

— dla $T \subset W$ definiujemy zbiór $\mathcal{C}(T)$ *konsekwencji* T (*twierdzeń teorii* T) jako najmniejszy zbiór słów zawierający T i zamknięty ze względu na poniższe *reguły pierwotne*, gdzie A, B oznaczają dowolne słowa ($A, B \in W$):

R1. $Aa \mapsto Aab$
R2. $A \mapsto A^2 = AA$
R3. $Aa^3B \mapsto AbB$
R4. $Ab^2B \mapsto AB$.

1) Powyżej wypisano dziesięć kolejnych słów $\varnothing, a, \ldots, aba$ w *porządku leksykograficznym*: $a \mapsto 1$, $b \mapsto 2$. Wypisać w tym porządku następne dziesięć słów.

2) Podać ścisłą definicję indukcyjną liczby $|A|$ = długość słowa A.

3) Dla danej liczby naturalnej n wyznaczyć, ile jest słów długości n.

4) Dla $T = \{a\}$ podać wszystkie słowa o długości $\leqslant 2$ będące twierdzeniami teorii T.
Czy teoria ta jest *rozstrzygalna*, tzn. czy istnieje *algorytm* (= mechaniczna procedura) pozwalający dla danego słowa A wyjaśnić, czy $A \in \mathcal{C}(a)$, czy też nie (piszemy $\mathcal{C}(a)$ zamiast $\mathcal{C}(\{a\})$ itp.)? Czy $b \in \mathcal{C}(a)$?

5) Wyjaśnić, dlaczego *klasyczny rachunek logiczny*, przez który rozumiemy tutaj nasz system dedukcji naturalnej z wyłączeniem jakichkolwiek aksjomatów (również aksjomatów identyczności), jest *nierozstrzygalny*, tzn. nie istnieje algorytm ustalający, czy dane zdanie jest tautologią, czy też nie. (wynik A. Churcha z 1936 roku, zob. np. [**Grell 06**, s. 346]).

2. Zdanie języka teorii mnogości

$$A = \forall\, x\ (\exists\, y\ y \in x \implies \exists\, y\ (y \in x \wedge \exists\, z\ (z \in y \implies \neg z \in x)))$$

wyraża jeden z aksjomatów ZFC (aksjomat A8; rozdział 3).

1) Opisać słownie jego sens, mówiąc o zmiennych jako o zbiorach.

2) Dla dowolnej formuły F określić indukcyjnie liczbę $\deg F :=$ stopień złożenia formuły F oraz zbiór $\operatorname{Sub} F$ podformuł formuły F. Wyznaczyć $\deg A$, $|A|$ oraz liczbę elementów (inaczej: moc) zbioru $\operatorname{Sub} A$.

3) Podać zbiory $Z(x, A)$, $Z(y, A)$, $Z(z, A)$.

3. Dla formuły F i zmiennych x, y podać ścisłą definicję indukcyjną formuły $[F, x \mapsto y]$.

4. Zbudować zdanie wyrażające aksjomat wyboru (A7, *Axiom of Choice*, AC) w oryginalnej postaci, czyli zdanie mówiące, że zbiór o elementach niepustych i parami rozłącznych dopuszcza tzw. selekcję, to jest zbiór, który z każdym elementem danego zbioru ma dokładnie jeden element wspólny.

5. Niech A i B będą dwiema różnymi formułami atomicznymi. Wypisać wszystkie formuły o złożoności 1, które można utworzyć z formuł A i B, używając tylko spójników zdaniowych $\neg$ i $\vee$. Ile jest takich formuł o złożoności 2, 3 i ogólnie o złożoności n dla dowolnie ustalonej liczby naturalnej n? Oznaczając tę ostatnią liczbę przez α_n, wykazać, że $\alpha_n \geqslant 2^{2^n}$.

6. Dane są zmienne x, y oraz formuła A. Podać wkw (= warunek konieczny i wystarczający) równoważności formuł $[[A, x \mapsto y], y \mapsto x]$ i A.

7. Udowodnić, że aksjomatyka identyczności ((1)–(4)) ze wstępu jest równoważna aksjomatyce (1), (4), (∗), gdzie (∗) jest zdaniem:

$$x = y \wedge z = t \implies (x = z \iff y = t).$$

8. Dane są zdania A, B, C. Udowodnić, że poniższe zdania są *tautologiami zdaniowymi*, to jest tautologiami czystymi, w których dowodach formalnych (pełnych) wykorzystuje się jedynie reguły zdaniowe **R1**–**R12** (ogólniej, A, B, C mogłyby być dowolnymi formułami i wtedy zdania (1)–(15) byłyby postaci $\forall \dots F$, gdzie F jest formułą bezkwantyfikatorową zbudowaną z formuł A, B i C).

(1) $(A \implies B) \implies [(B \implies C) \implies (A \implies C)]$ (*sylogizm hipotetyczny*)
(2) $(A \implies B) \iff (\neg B \implies \neg A)$ (*prawo transpozycji*)
(3) $(\neg A \implies A) \implies A$ (*prawo Claviusa*)
(4) $\neg A \implies (A \implies B)$ (*prawo Dunsa Scotusa*)
(5) $[(A \implies B) \implies A] \implies A$ (*prawo Pierce'a*)
(6) $A \vee \neg A$ (*prawo wyłączonego środka*)
(7) $\neg(a \wedge \neg A$ (*prawo sprzeczności*)
(8) $\neg\neg A \iff A$ (*prawo podwójnej negacji*)
(9) $A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C)$ (*rozdzielność koniunkcji względem alternatywy*)
(10) $A \vee (B \wedge C) \iff (A \vee B) \wedge (A \vee C)$ (*rozdzielność alternatywy względem koniunkcji*)
(11) $(A \vee B \implies C) \implies (A \implies C) \vee (B \implies C))$
(12) $(A \iff B) \implies [(A \wedge C) \implies (B \wedge C)]$
(13) $(A \implies B) \implies [(B \implies A) \implies (A \iff B)]$
(14) $(A \implies B \vee C) \iff B \implies (A \vee C)$
(15) $(A \implies B \vee \neg C) \iff (A \wedge C \implies B)$.

9. Dane są formuły A, B, C i dwie zmienne x, y takie, że podstawienie $x \mapsto y$ w formule A jest poprawne oraz zmienna x nie występuje wolno w formule C. Udowodnić, że poniższe zdania są tautologiami czystymi i naszkicować ich dowody formalne.

(1) $(\exists x\, A \implies B) \implies \forall x\, (A \implies B)$
(2) $(\exists x\, A \implies C) \iff \forall x\, (A \implies C)$
(3) $(\forall x\, A \implies C) \iff \exists x\, (A \implies C)$
(4) $(C \implies \exists x\, A) \iff \exists x\, (C \implies A)$
(5) $(C \implies \forall x\, A) \iff \forall x\, (C \implies A)$
(6) $\exists x\, (B \implies A) \implies (\forall x\, B \implies \exists x\, A)$
(7) $\exists x\, (A \wedge (\neg A \vee B)) \iff \exists x\, (A \wedge B)$
(8) $\exists x\, A \vee \exists x\, B \iff \exists x\, (A \vee B)$
(9) $\forall x\, A \wedge \forall x\, B \iff \forall x\, (A \wedge B)$
(10) $\exists x\, (A \wedge B) \implies \exists x\, A \wedge \exists x\, B$
(11) $\exists x\, (A \wedge C) \iff \exists x\, A \wedge C$
(12) $\forall x\, A \vee \forall x\, B \implies \forall x\, (A \vee B)$
(13) $\forall x\, A \vee C \iff \forall x\, (A \vee C)$

10. Dla formuł A i B mówimy, że są *równoważne*, gdy zdanie $A \iff B$ (tj. zdanie $\forall \ldots (A \iff B)$) jest tautologią czystą; notujemy: $A \equiv B$.
(a) Wykazać, że relacja $\equiv$ jest zwrotna, przechodnia i symetryczna (mówimy w tej sytuacji, że jest równoważnością) w zbiorze Form wszystkich formuł; to znaczy, że $A \equiv A$, $A \equiv B \implies B \equiv A$ i $A \equiv B \wedge B \equiv C \implies A \equiv C$ dla dowolnych formuł A, B i C.
(b) Wykazać, że dla formuł A, B i zmiennej x:

(1) $A \wedge B \equiv \neg(\neg A \vee \neg B), A \vee B \equiv \neg(\neg A \wedge \neg B)$
(2) $A \implies B \equiv \neg A \vee B \equiv \neg(A \wedge \neg B)$
(3) $A \wedge B \equiv \neg(A \implies \neg B), A \vee B \equiv \neg A \implies B \equiv \neg B \implies A$
(4) $\forall x\, A \equiv \neg \exists x\, \neg A, \exists x\, A \equiv \neg \forall x\, \neg A$.

(c) Dla formuły A określamy zbiór $\Gamma(A) \subset$ Form *równoważników* formuły A indukcją na złożoność A:

(1) dla formuły atomicznej A: $\Gamma(A) = \{A\}$
(2) $\Gamma(\neg A) = \{\neg B \mid B \in \Gamma(A)\}$, $\Gamma(A \vee B) = \{C \vee D \mid C \in \Gamma(A), D \in \Gamma(B)\}$ i analogicznie dla pozostałych spójników zdaniowych
(3) $\Gamma(\exists x\, A) = \{\exists y\, [B, x \mapsto y] \mid B \in \Gamma(A), y \in \{x\} \cup (\mathrm{Var} \setminus \mathrm{Fr}\, B)$, podstawienie $x \mapsto y$ jest poprawne w $B\}$ i analogicznie dla dużego kwantyfikatora.
Tak więc przejście od danej formuły do jej równoważnika polega na poprawnej wymianie zmiennych związanych w tej formule (pozorność zmiennej związanej!).

Wykazać, że $B \in \Gamma(A) \implies A \equiv B \wedge \mathrm{Fr}\, A = \mathrm{Fr}\, B$.
(d) Wykazać, że dla formuły A i zmiennych x, y istnieje równoważnik B formuły A taki, że podstawienie $x \mapsto y$ jest poprawne w B.

11. O formule mówimy, że jest *bezkwantyfikatorowa*, jeżeli utworzono ją z formuł atomicznych jedynie przez stosowanie spójników zdaniowych. Indukcyjnie określimy pojęcie *formuły normalnej*:

1° formuła bezkwantyfikatorowa jest normalna
2° jeżeli formuła A jest normalna oraz zmienna x jest w niej wolna, to formuły $\exists x\, A$, $\forall x\, A$ są normalne
3° żadnych innych formuł normalnych nie ma.

Tak więc formuły normalne są postaci $Q^1 x_1 \ldots Q^n x_n A$, gdzie $Q^1, \ldots, Q^n$ są kwantyfikatorami $\exists$ lub $\forall$, zmienne $x_1, \ldots, x_n$ są parami różne, formuła A jest bezkwantyfikatorowa oraz $\mathrm{Fr}\, A = \{x_1, \ldots, x_n\}$; liczbę naturalną n nazywamy *stopniem* naszej formuły normalnej.

Udowodnić, że dla każdej formuły A istnieje formuła normalna B taka, że $A \equiv B$ i $\mathrm{Fr}\, A = \mathrm{Fr}\, B$; każdą taką formułę nazywamy *postacią normalną* formuły A.

12. Dana jest formuła bezkwantyfikatorowa A i występujące w niej wolno dwie zmienne x, y. Sprowadzić do postaci normalnej formuły

(1) $\exists x\, \forall y\, A \implies \forall y\, \exists x\, A$
(2) $\forall y\, \exists x\, A \implies \exists x\, \forall y\, A$
(3) $\exists x\, \exists y\, A \implies \exists y\, [A, x \mapsto y]$
(4) $\forall x\, \forall y\, A \implies \forall y\, [A, x \mapsto y]$.

Przy dodatkowym założeniu $\mathrm{Fr}\, A = \{x, y\}$ wskazać, które ze zdań (1)–(4) są tautologiami.

13*. Rachunek zdań.

Określimy system formalny zwany *rachunkiem zdań*:
— Alfabet $L = \{\neg, \vee, \wedge, \implies, \iff, (,), \vartriangle, \vartriangle', \dots\}$; oprócz spójników zdaniowych mamy w nim nieskończony ciąg tzw. *zmiennych zdaniowych* (możemy je interpretować jako zdania lub formuły ustalonego języka elementarnego, np. języka teorii mnogości).
— W zbiorze W wszystkich słów nad alfabetem L (por. zadanie 1) określamy podzbiór $\mathcal{F}$, którego elementy nazywać będziemy *formułami*: $\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_1 \cup \dots$, gdzie $\mathcal{F}_0 = \{\vartriangle, \vartriangle', \dots\}$ = ogół zmiennych zdaniowych (*formuły atomiczne*), $\mathcal{F}_{n+1} = \mathcal{F}_n \cup \{\neg A, (A \vee B), (A \wedge B), (A \implies B), (A \iff B) \mid A, B \in \mathcal{F}_n\}$. Dla $A \in \mathcal{F}$ najmniejsze n takie, że $A \in \mathcal{F}_n$, nazywamy *stopniem złożenia* lub *złożonością* formuły A.
— W zbiorze $\mathcal{F}$ wyróżniamy podzbiór *tautologii* (*tautologie dedukcyjne*) $\mathcal{T}$: $\mathcal{T} = \mathcal{T}_0 \cup \mathcal{T}_1 \cup \dots$, gdzie $\mathcal{T}_0 = \varnothing$, $\mathcal{T}_{n+1} = \{A \in \mathcal{F} \mid \exists\, m \in \mathbb{N}, F : \{0, 1, \dots, m\} \longrightarrow \mathcal{F}\ [F_0 = \neg A \wedge \exists\, i, j \in \{0, \dots, m\}\ (F_i = \neg F_j) \wedge \forall\, k \in \{1, \dots, m\}\ (F_k \in \mathcal{T}_n$ lub F_k powstaje z jednej albo z dwu formuł $F_0, \dots, F_{k-1}$ przez zastosowanie jednej z *reguł zdaniowych* **R1**–**R12** opisanych we wstępie do tego rozdziału) $]\}$.

Analogicznie jak we wstępie dowodzimy, że $\mathcal{T}_0 \subset \mathcal{T}_1 \subset \mathcal{T}_2 = \mathcal{T}_3 = \dots$ Reguła wtórna dołączenia dodatkowego założenia też pozostaje w mocy. Przyjmujemy też skróty umowne ze wstępu. Litery $p, q, r, s, p', \dots$ oznaczać będą dowolne parami różne zmienne zdaniowe.

1) Dla formuły $A = (p \vee q \implies r) \implies (p \implies r)$ wykazać, że $A \in \mathcal{T}_2 \setminus \mathcal{T}_1$.

2) Funkcję $\varphi : \mathcal{F}_0 \longrightarrow \{0, 1\}$ zwaną *wartościowaniem zmiennych zdaniowych* rozszerzamy do funkcji $\varphi \subset \overline{\varphi} : \mathcal{F} \longrightarrow \{0, 1\}$ indukcyjnie: $\overline{\varphi} = \varphi_0 \cup \varphi_1 \cup \dots$, gdzie $\varphi_0 = \varphi$, i jeżeli mamy już $\varphi_n : \mathcal{F}_n \longrightarrow \{0, 1\}$, to określamy $\varphi_n \subset \varphi_{n+1} : \mathcal{F}_{n+1} \longrightarrow \{0, 1\}$, kładąc dla $A, B \in \mathcal{F}_n$: $\varphi_{n+1}(\neg A) = 1 - \varphi_n(A)$, $\varphi_{n+1}(A \vee B) = \max\{\varphi_n(A), \varphi_n(B)\} = \varphi_n(A) + \varphi_n(B) - \varphi_n(A) \cdot \varphi_n(B)$, $\varphi_{n+1}(A \wedge B) = \min\{\varphi_n(A), \varphi_n(B)\} = \varphi_n(A) \cdot \varphi_n(B)$, $\varphi_{n+1}(A \implies B) = \varphi_{n+1}(\neg A \vee B)$, $\varphi_{n+1}(A \iff B) = \varphi_{n+1}(A \implies B) \cdot \varphi_{n+1}(B \implies A)$. W dalszym ciągu dla $A \in \mathcal{F}$ piszemy $\varphi(A)$ zamiast $\overline{\varphi}(A)$.
Wykazać, że $\mathcal{T} \subset \mathcal{T}^{01} := \{A \in \mathcal{F} \mid \forall\, \varphi : \mathcal{F}_0 \longrightarrow \{0, 1\}\ \varphi(A) = 1\}$ ($\mathcal{T}^{01}$ to *tautologie zerojedynkowe*).

3) Dla formuły $B = ((p \wedge q) \implies r) \wedge (p \wedge q) \implies \neg r)) \implies \neg(p \vee q \vee r)$ wykazać, że $B \notin \mathcal{T}$.

4) Dla $p \in \mathcal{F}_0$ oznaczmy $p^0 = p$, $p_1 = p^\neg := \neg p$. Przez $\mathcal{N}_0$ oznaczmy ogół formuł postaci $p_1^{\alpha_1} \vee \dots \vee p_n^{\alpha_n}$ (*alternatywy elementarne. Formuła normalna (koniunkcyjno–alternatywna)* to formuła postaci $A_1 \wedge \dots \wedge A_m$, gdzie $m \in \mathbb{N}^* = \{1, 2, 3, \dots\}$, $A_j \in \mathcal{N}_0$; ogół takich formuł oznaczamy przez $\mathcal{N}$. Dla $A, B \in \mathcal{F}$ notujemy $A \equiv B$, gdy $(A \iff B) \in \mathcal{T}$. Łatwo widać, że relacja $\equiv$ jest równoważnością w zbiorze $\mathcal{F}$ wszystkich formuł. Relacja ta jest zgodna ze wszystkimi spójnikami zdaniowymi, to znaczy, jeżeli $A \equiv B$ i $C \equiv D$, to $\neg A \equiv \neg B$, $A \vee C \equiv B \vee D$ itd. Zbiory $\mathcal{T}$ i $\mathcal{T}^{01}$ są zamknięte ze względu na relację $\equiv$, to znaczy $\mathcal{T} \ni A \equiv B \implies B \in \mathcal{T}$ i analogicznie dla $\mathcal{T}^{01}$. Wykazać, że $\forall\, A \in \mathcal{F}\ \exists\, P \in \mathcal{N} : A \equiv P$; każdą taką formułę P nazywamy *postacią normalną* formuły A.

5) Wykazać, że $\mathcal{T}^{01} \cap \mathcal{N} \subset \mathcal{T}$.

6) Wykazać, że $\mathcal{T} \subset \mathcal{T}^{01}$.
Równość ta oznacza, że rachunek zdań jest rozstrzygalny; dla $A \in \mathcal{F}$, $\varphi : \mathcal{F}_0 \longrightarrow \{0,1\}$ wartość $\varphi(A)$ zależy tylko od wartości $\varphi(p_1), \ldots, \varphi(p_n)$, gdzie $p_1, \ldots, p_n$ są wszystkimi zmiennymi zdaniowymi występującymi w formule A. Dla sprawdzenia, czy $A \in \mathcal{T}$, wystarczy więc sprawdzić, czy $\varphi(A) = 1$ dla 2^n wartościowań wyznaczonych przez wszystkie zerojedynkowe ciągi długości n, co jest procedurą mechaniczną. Można udowodnić ([**Church 96**]), że pełny rachunek logiczny — ze zmiennymi i kwantyfikatorami — nie jest już rozstrzygalny (przyczyna tego tkwi w możliwości dopisywania tautologii).

14*. Rachunek zdań c.d.

Zachowujemy oznaczenia z 13*.

Dla $n = 1, 2, 3\ldots$, $p \in \mathcal{F}_0$ i ciągu zerojedynkowego $\alpha : I_n \longrightarrow \{0,1\}$, $\alpha = \alpha_1 \ldots \alpha_n$ określamy formułę $p_\alpha \in \mathcal{F}$ indukcją na n:

I dla $n = 1$: $p^0 = p$, $p^1 = p^\neg$ (piszemy $p^\neg$ zamiast $\neg p$)

II jeżeli $\alpha : I_{n+1} \longrightarrow \{0,1\}$, to $p^\alpha = p^{\alpha|I_n} \implies p^{\alpha_{n+1}}$; tak np. $p^{1010} = ((p^\neg \implies p) \implies p^\neg) \implies p$.

Wyznaczyć zbiór wszystkich ciągów $\alpha : I_n \longrightarrow \{0,1\}$, $n \in \mathbb{N}^*$, dla których p^α jest tautologią ($p^\alpha \in \mathcal{T}$).

Ile jest takich ciągów o długości 8?

Wypisać wszystkie takie ciągi o długości 4.

15. Są dwie bramki — jedna dobra, druga zła. Przed każdą z bramek stoi strażnik — jeden prawdomówca (zawsze mówi prawdę), a drugi kłamca (zawsze kłamie). Bramki są nieodróżnialne, strażnicy też. Ponadto nie wiadomo, czy prawdomówny stoi przy bramce dobrej, czy przy złej.

Wolno podejść do jednej z bramek i zadać stojącemu przy niej strażnikowi tylko jedno pytanie, na które może on odpowiedzieć jedynie TAK lub NIE.

Jakie pytanie należy zadać, aby po uzyskaniu odpowiedzi bezbłędnie wskazać bramkę dobrą?

1.3. Odpowiedzi

1*.

1) $ab^2, ba^2, bab, b^2a, b^3, a^4, a^3b, a^2ba, a^2b^2, aba^2, \ldots$
2) $|\varnothing| = 0$, $|Aa| = |Ab| = |A| + 1$.
3) 2^n $\langle$Dowód indukcja na $n\rangle$.
4) a, a^2, ab, ba.

Teoria $T\{a\}$ jest rozstrzygalna. Rozpisując drzewo generowania słów tej teorii, zauważamy, że $\mathcal{C}(a) = \{A \in W \mid 3 \nmid \alpha(A)\}$, gdzie $\alpha(A) =$ liczba wystąpień a w A, to jest $\alpha : W \longrightarrow \mathbb{N}$, $\alpha(\varnothing) = 0$, $\alpha(Aa) = \alpha(A) + 1$, $\alpha(Ab) = \alpha(A)$; zapis $3 \nmid \alpha(A)$ oznacza, że 3 nie jest dzielnikiem liczby $\alpha(A)$. Tak więc $b \notin \mathcal{C}(a)$, $b^2 \notin \mathcal{C}(a)$.

$\langle$ Oznaczmy $S = \{A \in W \mid 3 \nmid \alpha(A)\}$. $\mathcal{C}(a) \subset S$, gdyż $a \in S$ i wszystkie cztery reguły pierwotne nie wyprowadzają z S.

Dla dowodu inkluzji $S \subset \mathcal{C}(a)$ wystarczy wykazać, że:

$$(*) \qquad \forall\, n \in \mathbb{N} : 3 \nmid n \implies a^n \in \mathcal{C}(a)$$

$\langle$ dla słowa $A \in S$, zastępując w A każde wystąpienie b przez a^3, otrzymamy słowo postaci a^n, gdzie $3 \nmid n$. Według $(*)$: $a^n \in \mathcal{C}(a)$. Teraz, stosując do słowa a^n odpowiednią ilość razy regułę **R4**, dojdziemy do słowa A, czyli $A \in \mathcal{C}(a)$ $\rangle$.

Dowód lematu $(*)$:

Według **R2**: $\forall\, k \in \mathbb{N} : a^{2^k} \in \mathcal{C}(a)$ $\quad\langle$Indukcja na $k\rangle$, a więc — według **R1** również $a^{2^k} b \in \mathcal{C}(a)$. Uwzględniając **R3** i **R4** widzimy, że wystarczy udowodnić następujący lemat teorioliczbowy:

$$(**) \qquad \forall_{\substack{n \in \mathbb{N} \\ 3 \nmid n}} \exists\, k, l \in \mathbb{N} : n = 2^k - 3l$$

$\langle$ $2^k = n + 3l$; $a^{2^k}, a^{2^k} b \in \mathcal{C}(a)$, a więc $a^n a^{3l}, a^n a^{3l} b \in \mathcal{C}(a)$. Stosując l razy regułę **R3**, otrzymujemy $a^n b^l, a^n b^{l+1} \in \mathcal{C}(a)$. Jedna z liczb l, $l+1$ jest równa $2m$; $m \in \mathbb{N}$. Mamy więc $a^n b^{2m} \in \mathcal{C}(a)$, i stosując m razy regułę **R4**, otrzymujemy $a^n \in \mathcal{C}(a)$ $\rangle$.

Dowód lematu $(**)$ — indukcja na n:

$\langle$ I. $n = 0, 1, 2$. $1 = 2^0 - 3 \cdot 0$, $2 = 2^1 - 3 \cdot 0$.
II. Jeśli $n \geqslant 3, 3 \nmid n$ i dla $n' < n$ teza zachodzi, to $n - 3 = 2^k - 3l$. Jeśli $l > 0$, to $n = 2^k - 3(l-1)$; jeśli zaś $l = 0$, to $n = 2^k + 3 = 2^{k+2} - 3(2^k - 1)$ $\rangle$ $\rangle$.

5) Nierozstrzygalność wynika z możliwości dołączania do dowodu jakichś poprzednio udowodnionych tautologii (czystych) — należy rozstrzygnąć jakich...

Teoretycznie możliwa jest maszyna (maszyna Turinga), która po wpisaniu do niej zdania A będzie produkować w ustalonej kolejności coraz dłuższe „ciągi dedukcyjne" zaczynające się od $\neg A$ (w sensie punktu 2. ze wstępu), szukając sprzeczności. Jeżeli zdanie A jest tautologią czystą, to w skończonym czasie otrzymamy jego dowód formalny — w przeciwnym wypadku maszyna nie zatrzyma się, i nie istnieje algorytm (maszyna) ustalający, który z tych przypadków ma miejsce (nierozstrzygalność problemu STOP maszyny Turinga).

2.

1) W każdym zbiorze niepustym istnieje element minimalny ze względu na przynależność.

2) Dla formuły atomicznej F : $\deg F = 0$, $\operatorname{Sub} F = \{F\}$; $\deg(\neg F) = 1 + \deg F$, $\operatorname{Sub}(\neg F) = \{\neg F\} \cup \operatorname{Sub} F$, $\deg(F \vee G) = 1 + \max(\deg F, \deg G)$, $\operatorname{Sub}(F \vee G) = \{F \vee G\} \cup \operatorname{Sub} F \cup \operatorname{Sub} G$ i analogicznie dla spójników zdaniowych $\wedge$, $\implies$ i $\iff$; $\deg(\forall\, x \;\; F) = 1 + \deg F$, $\operatorname{Sub}(\exists\, x \;\; F) = \{\exists\, x \;\; F\} \cup \operatorname{Sub} F$ (i analogicznie dla $\forall$). $\deg A = 7$, $|A| = 30$, $|\operatorname{Sub} A| = 12$.

3) $Z(x, A) = \{1, 2, \ldots, 30\}$, $Z(y, A) = \{4, 5, \ldots, 8\} \cup \{10, 11, \ldots, 29\}$, $Z(z, A) = \{17, 18, \ldots, 28\}$.

3. Najpierw dla dowolnej zmiennej z określamy

$$[z, x \mapsto y] = \begin{cases} y, \text{ gdy } z = x \\ z, \text{ gdy } z \neq x. \end{cases}$$

Teraz określamy formułę $[F, x \mapsto y]$ indukcją na złożoność F (G, H — formuły; x, y, z, t — zmienne);

1) Dla formuł atomicznych: $[z \in t, x \mapsto y] = [z, x \mapsto y] \in [t, x \mapsto y]$ i analogicznie dla formuły $z = t$.

2) $[\neg G, x \mapsto y] = \neg[G, x \mapsto y]$
$[(G \vee H), x \mapsto y] = [G, x \mapsto y] \vee [H, x \mapsto y]$ i analogicznie dla $\wedge$, $\implies$ i $\iff$
$$[\exists\, z\; G, x \mapsto y] = \begin{cases} \exists\, z\; G, \text{ gdy } z = x \\ \exists\, z\; [G, x \mapsto y], \text{ gdy } z \neq x. \end{cases}$$

4. $\forall\, x\; ((\forall\, y\; (y \in x \implies \exists\, z\; z \in y) \wedge \forall\, y\; \forall\, z\; (((y \in x \wedge z \in x) \wedge \neg y = z) \implies \neg \exists\, t\; (t \in y \wedge t \in z))) \implies \exists\, y\; \forall\, z\; (z \in x \implies \exists\, t\; \forall\, u\; ((u \in y \wedge u \in z) \iff u = t)))$.

5. $\neg A$, $\neg B$, $(A \vee A)$, $(A \vee B)$, $(B \vee A)$, $(B \vee B)$. Tak więc $\alpha_0 = 2, \alpha_1 = 6$. Jeżeli $F_1, F_2, \ldots, F_{\alpha_n}$ są wszystkimi takimi formułami o złożoności n, to ogół takich formuł o złożoności $n+1$ rozpada się na trzy rozłączne klasy:

1) formuły postaci $\neg F_i$
2) formuły $(F_i \vee F_j)$
3) formuły postaci $(F_i \vee G)$ lub $(G \vee F_i$, gdzie G jest formułą o złożoności mniejszej od n, $i, j \in \{1, 2, \ldots, \alpha_n\}$.

Zatem
$$\alpha_{n+1} = \alpha_n + \alpha_n^2 + 2\alpha_n(\alpha_0 + \alpha_1 + \ldots + \alpha_{n-1}).$$
Tak więc $\alpha_2 = 6 + 6^2 + 2 \cdot 6 \cdot 2 = 66$, $\alpha_3 = 66 + 66^2 + 2 \cdot 66 \cdot (2 + 6) = 5478$. Nierówność $\alpha_n \geqslant 2^{2^n}$ udowodnimy indukcją na n: $\alpha_0 = 2 \geqslant 2^{2^0}$; jeżeli nierówność zachodzi dla n, to $\alpha_{n+1} \geqslant \alpha_n^2 \geqslant (2^{2^n})^2 = 2^{2^{n+1}}$.

6. Podstawienie $x \mapsto y$ w formule A jest poprawne oraz zmienna y nie występuje wolno w formule A.

7. Łatwo sprawdzić, że zdanie (*) jest twierdzeniem. Należy jeszcze wykazać, że po przyjęciu zdań (1), (4) i (*) jako aksjomatyki identyczności zdania (2) i (3) staną się twierdzeniami.
Ad (2). HP: $\exists\, x\, y)\; x = y, y \neq x$. Odrywając w zdaniu (*) duże kwantyfikatory z podstawieniami $z \mapsto x$ i $t \mapsto x$, otrzymujemy formułę $x = y \wedge x = x \implies (x = x \iff y = x)$, skąd już łatwo uzyskamy równość $y = x$ ↯.
Ad (3). HP: $\exists\, x\, y\, z)\; x = y, y = z, x \neq z$. Odrywając w (*) kwantyfikatory z podstawieniami $x \mapsto x$, $t \mapsto y$, otrzymujemy formułę

$$x = y \wedge z = y \implies (x = z \iff y = y),$$

skąd, wykorzystując (2) i mechanizm dedukcji naturalnej, otrzymamy: $x = z$ ↯.

8. W przedstawionym systemie dedukcji naturalnej dowody tautologii (1)–(15) przebiegają niemal automatycznie. Na przykład naszkicujmy dowód formalny tautologii

(11): $\neg \ldots, A \vee B \implies C, \ldots, \neg(A \implies C), \neg(B \implies C), \ldots, A, B, \neg C, A \implies (B \implies (A \vee B))$ (dopisana tautologia klasy 1), $\ldots, A \vee B, C$ ϟ.

9. Dowody tautologii (1)–(13) nie są już automatyczne, w przeciwieństwie do dowodów tautologii zdaniowych z 8; nie powinny jednak sprawić większych trudności. Dla przykładu naszkicujmy dowód formalny tautologii (12). Przyjmijmy dla ułatwienia nieistotne założenie, że formuły $A : B$ nie mają zmiennych wolnych różnych od x i y. (W przeciwnym wypadku trzeba by stosować odpowiednią ilość razy reguły **R16** i **R13**). Tak więc: $\neg(\ldots \implies \ldots)$, $\forall x\ A \vee \forall x\ B$, $\neg\forall x(A \vee B)$. Teraz stosujemy regułę wtórną dołączenia dodatkowego założenia — przypadki: $\forall x\ A$, $\neg\forall x\ A$ — i stosując reguły pierwotne, dochodzimy do sprzeczności. Chcąc przedstawić pełny dowód formalny zdania (12) jako tautologii czystej klasy 2, dopisujemy w tym miejscu odpowiednią tautologię czystą klasy 1, na przykład: $(\forall x\ A \ \vee\ \forall x\ B) \implies (\neg\forall x\ (A \vee B) \implies \forall x\ A)$ $\langle$oto szkic dowodu formalnego tej ostatniej tautologii: $\neq \ldots, \forall x\ A \vee \forall x\ B$, $\neg\forall x\ (A \vee B)$, $\neg\forall x\ A$, $\forall x\ B$ (wg **R4**), $\exists x)\, \neg(A \vee B)$, $\neg A \wedge \neg B$, $\neg B$, B ϟ$\rangle$. Po dwukrotnym zastosowaniu reguły **R1** dochodzimy do $\forall x\ A$, i dalej: $\exists x)\, \neg(A \vee B)$, $\neg A \wedge \neg B$, $\neg A$, A ϟ.

10. Dowody (a) i (b) są mechaniczne i bezproblemowe (por. zadanie 9):
Ad (c) Indukcja na złożoność formuły A. Rozpatrzmy krok z dołączeniem $\exists$. Zakładamy, że $A \equiv B$, $\mathrm{Fr}\, A = \mathrm{Fr}\, B$ i spełnione są założenia z (3).

Dla wykazania, że $\exists x\ A \equiv \exists y\ [B, x \mapsto y]$, wystarczy udowodnić, iż tautologiami są dwie implikacje:

1° $\exists x\ A \implies \exists y\ [B, x \mapsto y]$
Szkic dowodu: $\neg \ldots$, $\exists x\ A$, $\neg\exists y\ [B, x \mapsto y]$, A, $\forall y\ \neg[B, x \mapsto y]$, $[\neg[B, x \mapsto y], y \mapsto x]$ (podstawienie $y \mapsto x$ w formule $[B, \mapsto y]$ jest poprawne na mocy założeń z (3)), a ponadto $[[B, x \mapsto y], y \mapsto x] = B$ (por. zadanie 6), mamy więc $\neg B$, teraz dopisujemy tautologię $A \implies B$, i według reguły **R1** otrzymujemy B ϟ.

2° $\exists y\ [B, x \mapsto y] \implies \exists x\ A$
Szkic dowodu: $\exists y\ [B, x \mapsto y]$, $\neg\exists x\ A$, $\forall x\ \neg A$, $[[B, x \mapsto y], y \mapsto x] = B$ (tak samo na mocy założeń z (3)), $\neg A$, $B \implies A$ (dopisana tautologia), A ϟ.

Równość $\mathrm{Fr}(\exists x\ A) = \mathrm{Fr}(\exists y\ [B, x \mapsto y])$ także wynika z przyjętych w (3) założeń oraz z założenia indukcyjnego: $\mathrm{Fr}\, A = \mathrm{Fr}\, B$.
Ad d) Podobnie jak w (c), przy ustalonych zmiennych x i y, indukcją na złożoność formuły A i, wykorzystując (c)(3), dowodzimy, że istnieje formuła $B \in \Gamma(A)$ taka, iż podstawienie $x \mapsto y$ jest poprawne w B.

11. Dowód indukcją na złożoność formuły A. Trudniejszym jego fragmentem jest przypadek alternatywy (pozostałe dwuargumentowe spójniki zdaniowe można sprowadzić do alternatywy — por. zadanie 10 punkt b). Wygodnie będzie sformułować lemat:

$$\forall A, B \in \mathrm{Norm}\ \exists C \in \mathrm{Norm} : A \vee B \equiv C, \mathrm{Fr}(A \vee B) = \mathrm{Fr}\, C,$$

gdzie Norm := ogół formuł normalnych.

Dowód lematu prowadzimy indukcją na $\alpha + \beta$, gdzie α i β są odpowiednio stopniami formuł normalnych A i B.

I Jeśli $\alpha+\beta=0$, to $\alpha=\beta=0$, formuły A i B są bezkwantyfikatorowe i wystarczy wziąć $C = A \vee B$.

II Załóżmy, że $\alpha+\beta>0$ i dla liczb mniejszych od $\alpha+\beta$ teza zachodzi.

Wystarczy rozpatrzyć przypadek, gdy A jest postaci $\exists x\ A'$ lub $\forall x\ A'$, gdzie $A' \in \mathrm{Norm}$, $x \in \mathrm{Fr}(A')$; niech na przykład $A = \exists x\ A'$. Weźmy równoważnik formuły A (zob. poprzednie zadanie) postaci $\exists y\ [A', x \mapsto y]$, gdzie zmienna y w ogóle nie występuje w formułach A i B. Wówczas $A \equiv \exists y\ [A', x \mapsto y]$, $[A', x \mapsto y] \in \mathrm{Norm}$, stopień $[A', x \mapsto y] = \alpha - 1$.

$$A \vee B \equiv \exists y\ [A', x \mapsto y] \vee B \equiv \exists y([A', x \mapsto y] \vee B).$$

Stosując do formuły $[A', x \mapsto y] \vee B$ założenie indukcyjne, otrzymamy tezę.

12. Niech z i t będą zmiennymi niewystępującymi w formule A. Będziemy pisać $A(z,t)$ zamiast $[A, x \mapsto z, y \mapsto t]$ itp.

$$\begin{aligned}(1)\ &\equiv \neg\exists x\,\forall y\ A \quad \vee \quad \forall y\,\exists x\ A\\ &\equiv \forall x\,\exists y\ \neg A \quad \vee \quad \forall t\,\exists z\ A(z,t)\\ &\equiv \forall x\,\exists t\,\exists y\,\exists z\ (\neg A \vee A(z,t)).\end{aligned}$$

Kwantyfikatory można też wyprowadzać w innej kolejności, np.:
$(1) \equiv \forall x\,\exists y\,\forall z\,\exists t\ (\neg A \vee A(z,t))$,
postać normalna danej formuły nie jest więc na ogół wyznaczona jednoznacznie.

$$\begin{aligned}(2)\ &\equiv \exists y\,\exists z\,\forall x\,\forall t\ (\neg A \vee A(z,t))\\ (3)\ &\equiv \forall x\,\forall y\,\exists z\ (\neg A \vee A(z,z))\\ (4)\ &\equiv \exists x\,\exists y\,\forall z\ (\neg A \vee A(z,z)).\end{aligned}$$

Tautologiami są, jak łatwo widać, zdania (1) i (4). Zdania (2) i (3) nie są tautologiami; wynika to z twierdzenia Gödla o pełności. Na mocy tego twierdzenia wystarczy wskazać jakąś odpowiadającą danemu językowi strukturę, w której dane zdanie nie jest spełnione.

W naszym przypadku wystarczy wziąć dowolną strukturę nietrywialną, to jest taką, w której uniwersum mamy co najmniej dwa różne elementy. Dla formuły $A = (x \neq y)$ zdania (2) i (3) nie będą w takiej strukturze spełnione.

13*.

1) $A \in \mathcal{T}_2$, odpowiedni ciąg F, to: $\neg A$, $(p \vee q \implies r) \wedge \neg(p \implies r)$, $p \vee q \implies r$, $\neg(p \implies r)$, $p \wedge \neg r$, p, $\neg r$; w tym miejscu widać, że już żadnej z reguł R1–12 nie da się zastosować, dopisujemy formułę $B = (p \vee g \implies r) \implies (\neg r \implies \neg(p \vee q))$ należącą do $\mathcal{T}_1$ i kontynuujemy nasz ciąg; $\neg r \implies \neg(p \vee q)$, $\neg(p \vee q)$, $\neg p \wedge \neg q$, $\neg p$ ↯.

2) Indukcją na n wykażemy, że $\mathcal{T}_n \subset \mathcal{T}^{01}$

$\mathcal{T}_0 = \varnothing \subset \mathcal{T}^{01}$. Jeżeli $\mathcal{T}_n \subset \mathcal{T}^{01}$ i $A \in \mathcal{T}_{n+1}$, to $\exists)\, n \in \mathbb{N}$, $F : \{0,1,\ldots,n\} \longrightarrow \mathcal{F} \ldots$ (jak w określeniu $\mathcal{T}_{n+1}$)

HP: $A \notin \mathcal{T}^{01}$. $\exists)\, \varphi : \mathcal{F}_0 \longrightarrow \{0,1\}$ $[\varphi(A) = 0]$. Wówczas $\varphi(\neg A) = 1$, czyli $\varphi(F_0) = 1$. Załóżmy, że dla $k \in \{1,\ldots,n\}$: $\varphi(F_0) = \varphi(F_1) = \ldots = \varphi(F_{k-1}) = 1$. Wówczas $\varphi(F_k) = 1$, bo jeżeli $F_k \in \mathcal{T}_n$, to $\varphi(F_k) = 1$ na mocy założenia indukcyjnego, natomiast jeśli formuła F_k powstaje z poprzedzających ją formuł $F_0, \ldots, F_{k-1}$ przez zastosowanie jednej z reguł **R1**–**R12**, to przekształcając po kolei te reguły i korzystając z założenia o φ otrzymujemy: $\varphi(F_k) = 1$. Na przykład, jeśli zastosowano **R1**, to dla pewnych i, $j < k$ $F_i \implies (F_j \implies F_k)$, przy czym $\varphi(F_i) = \varphi(F_j) = 1$, a więc $1 = \varphi(F_j \implies F_k) = \max\{1 - \varphi(F_j), \varphi(F_k)\} = \max\{0, \varphi(F_k)\} = \varphi(F_k)$. Tak więc $\varphi(F_k) = 1$ dla wszystkich $k = 0, 1, \ldots, n$, co daje sprzeczność, gdyż $F_i = \neg F_j$ dla pewnych $i, j < n$.

3) Według 2) wystarczy wykazać, że $B \notin \mathcal{T}^{01}$, a więc wskazać wartościowanie φ takie, że $\varphi(B) = 0$. Wystarczy wziąć $\varphi : \mathcal{F}_0 \longrightarrow \{0,1\}$, $\varphi(p) = \varphi(q) = 0$, $\varphi(r) = 1$.

4) Dowód przebiega indukcją na złożoność formuły A. Jeżeli na przykład $A \equiv \neg P$, gdzie $P \in \mathcal{N}$, $P = (p^\neg \vee q) \wedge (p \vee r)$, to $\neg A \equiv \neg P \equiv Q$, gdzie $Q = (p \vee p^\neg) \wedge (p \vee r^\neg) \wedge (p^\neg \vee q^\neg) \wedge (q^\neg \vee r^\neg)$ (oczywiście wówczas też $\neg P = (p \vee r^\neg) \wedge (p^\neg \vee q^\neg) \wedge (q^\neg \vee r^\neg)$).

5) Niech $B = A_1 \wedge \ldots \wedge A_m \in \mathcal{T}^{01} \cap \mathcal{N}$, gdzie $A_j \in \mathcal{N}_0 (j = 1, \ldots, m)$. Wówczas $A_j \in \mathcal{T}^{01}$ dla $j = 1, \ldots, m$ $\langle$gdyż $\varphi(B) = \varphi(A_1) \cdot \ldots \cdot \varphi(A_m)$, dla każdego wartościowania $\varphi\rangle$. Jeżeli dla ustalonego j $A_j = p_1^{\alpha_1} \vee \ldots \vee p_n^{\alpha_n}$, to $p_i = \neg p_k$ dla pewnych i, k spośród $1, \ldots n$ $\langle$bo w przeciwnym wypadku można by tak dobrać wartościowanie φ, żeby $\varphi(A_j) = \max\{\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_n^{\alpha_n})\} = 0)\rangle$, skąd wynika, że $A_j \in \mathcal{T}$ dla $j = 1, \ldots, n$, i dalej: $B \in \mathcal{T}$.

6) Według 2) wystarczy wykazać, że $T^{01} \subset T$.

Niech $A \in \mathcal{T}^{01}$. Według 4) $A \equiv P$ dla pewnej formuły $P \in \mathcal{N}$. Wówczas $P \in \mathcal{T}^{01}$ i według 5) $P \in \mathcal{T}$, a więc $A \in \mathcal{T}$.

14*. Będziemy stosować te same oznaczenia w metajęzyku co w języku formalnym L rachunku zdań (zadanie 13*), odwołując się do kontekstu.

Oznaczmy przez C ogół skończonych i niepustych ciągów zerojedynkowych, $C = \{0, 1, 00; 01, 10, 11, \ldots, 000, 001, \ldots\}$; C_n niech oznacza ogół takich ciągów o długości $n = 1, 2, \ldots$, oczywiście $|C_n| = 2^n$.

Chcemy wyznaczyć zbiór $A = \{\alpha \in C \mid p^\alpha \in \mathcal{T}\}$ lub, co na jedno wychodzi, zbiory $A_n = A \cap C_n$. $|A_8| = ?$ Natychmiast widać, że $A_1 = \varnothing$, $A_2 = \{00, 11\}$, $A_3 = \{011, 100\}$.

Dla $\alpha = \alpha_1 \ldots \alpha_n \in C_n$ oznaczmy $\bar{\alpha}_1 \ldots \bar{\alpha}_n$ ciąg dopełniający, $\bar{0} = 1, \bar{1} = 0$. Zauważmy, że $\alpha \in A_n \iff \bar{\alpha} \in A_n$ $\langle$Jeśli dla $\varphi : \mathcal{F}_0 \longrightarrow \{0,1\}$ weźmiemy wartościowanie dopełniające $\bar{\varphi} : \mathcal{F}_0 \longrightarrow \{0,1\}$, $\bar{\varphi}(q) = 1 - \varphi(q)$, to $\varphi(p^{\bar{\alpha}}) = \bar{\varphi}(p^\alpha)\rangle$. Wystarczy więc wyznaczyć zbiór $\tilde{A}_n = \{\alpha \in A_n | \alpha_n = 0\}$, bo wówczas:

$$A_n = \tilde{A}_n \cup \{\bar{\alpha} \in \tilde{A}_n\}, |A_n| = 2|\tilde{A}_n|. \tag{1}$$

Jeżeli $n \geqslant 2$ i $\alpha = \alpha_1 \ldots \alpha_n \in C_n$, to oznaczając $\alpha' = \alpha | I_{n-1} = \alpha_1 \ldots \alpha_{n-1}$, mamy $p^\alpha = (p^{\alpha'} \implies p^{\alpha_n})$, a więc

$$\alpha_n = 0 \implies \big[\alpha \in \tilde{A}_n \iff \forall\, \varphi : \mathcal{F}_0 \longrightarrow \{0,1\}\ (\varphi(p) = 0 \implies \varphi(p^{\alpha'}) = 0)\big].$$

Oznaczając dla $n \in 1, 2, \ldots$ $B_n = \{\beta \in C_n \mid \forall_{\substack{\varphi : \mathcal{F}_0 \longrightarrow \{0,1\} \\ \varphi(p) = 0}} : \varphi(p^\beta) = 0\}$ będziemy mieli:

$$n \geqslant 2, \alpha \in C_n, \alpha_n = 0 \implies [\alpha \in \tilde{A}_n \iff \alpha' \in B_n], \tag{2}$$

wystarczy więc wyznaczyć zbiory B_n. $B_1 = \{0\}$, $B_2 = \{10\}$.

Niech $n \geqslant 3$, $\beta \in C_n$; wówczas $p^\beta = (p^{\beta'} \implies p^{\beta_n})$, a więc $\beta \in B_n \iff \forall_{\substack{\varphi:\mathcal{F}_0 \longrightarrow \{0,1\} \\ \varphi(p)=0}} [\varphi(p^{\beta'}) = 1, \beta_n = 0]$, i ponieważ $p^{\beta'} = (p^{\beta''} \implies p^{\beta_{n-1}})$, więc

$$\beta \in B_n \iff \beta_n = 0 \wedge \forall_{\substack{\varphi:\mathcal{F}_0 \longrightarrow \{0,1\} \\ \varphi(p)=0}} [\varphi(p^{\beta_{n-1}}) = 0 \implies \varphi(p^{\beta''}) = 0],$$

czyli ostatecznie, dla $n > 3$:

$$\beta \in B_n \iff \beta_n = 0 \wedge [(\beta_{n-1} = 0 \wedge \beta'' \in B_{n-2}) \vee \beta_{n-1} = 1]. \tag{3}$$

Oznaczając $b_n = |B_n|$ mamy: $b_1 = b2 = 1$, $n \geqslant 3 \implies b_n = b_{n-2} + 2^{n-2}$, skąd $b_3 = 1 + 2 = 3, \ldots, b_7 = 43$, a więc $|A_8| = 2|\tilde{A}_8| = 2b_7 = 86$. W postaci zwartej: $b_n = 1 + \frac{2}{3}(4^{[\frac{n}{2}]} - 1)$ dla n nieparzystych i $b_n = \frac{1}{3}(2^n - 1)$ dla n parzystych. Formuły (1)–(3) pozwalają nam wypisywać kolejno zbiory A_n, na przykład $B_3 = \{000, 010, 110\}$, a więc $A_4 = \{0000, 0100, 1100, 1111, 1011, 0011\}$.

15. Oznaczmy: A = bramka dobra, B = bramka zła, α = strażnik prawdomówny, β = kłamca. Po podejściu do którejś z bramek możliwe są cztery przypadki: $A\alpha$, $A\beta$, $B\alpha$, $B\beta$. Potrzebne jest zdanie o wartościach logicznych $1, 0, 0, 1$ (1 = prawda, 0 = fałsz), gdyż wówczas uzyskamy odpowiedzi TAK TAK, NIE NIE (bo w drugim i czwartym przypadku strażnik jest kłamcą). Zdaniem tym może być $p \iff q$, gdzie p = ta bramka jest dobra, q = jestem prawdomówny.

Pytamy więc stojącego przy wybranej bramce strażnika:

Czy ta bramka jest dobra wtedy i tylko wtedy, gdy ty jesteś prawdomówny?

(lub: *Czy zdanie, mówiące, że ta bramka jest dobra, jest równoważne zdaniu mówiącemu, że ty jesteś prawdomówny?)*

Jeżeli usłyszymy TAK, to wskazujemy bramkę, przy której stoimy; po odpowiedzi NIE wskazujemy drugą bramkę.

Zadanie to wiąże się ze znanym semantyczno-logicznym paradoksem (antynomią) kłamcy. Przypuśćmy, że po wskazaniu dobrej bramki ujawni się strażnik-kłamca i pozwoli nam zadać jeszcze jedno dowolne pytanie, na które odpowie TAK–NIE zgodnie ze swoją naturą. Jeśli go zapytamy

Czy gdy mówisz, że zawsze kłamiesz, to mówisz prawdę?

to nie będzie mógł odpowiedzieć ani TAK, ani NIE bez popadnięcia w sprzeczność.

Jak widać, pojęcie prawdy nie mieści się w ustalonym, sformalizowanym języku — trzeba przejść do metajęzyka (por. [**Tarski 95**], [**Mostowski 48**, rozdz. XIV]).

2

Klasy

2.1. Wstęp

W metajęzyku *wyrażeniem klasowym* nazywamy napis postaci $\{x \mid F\}$ — czytamy „ogół takich x, że F" — gdzie x jest zmienną, zaś F formułą. Zmienne i wyrażenia klasowe nazywamy *klasami*.

Zmiennymi wolnymi (lub *parametrami*) w klasie C nazywamy:
a) zmienne wolne formuły F różne od zmiennej x, gdy $C = \{x \mid F\}$
b) samą zmienną x, gdy $C = x$.
Klasę bez zmiennych wolnych nazywamy *stałą*. Podstawowe znaczenie mają dwie klasy stałe:

$$\mathbb{V} := \{x \mid x = x\} - \textit{klasa pełna}$$
$$\varnothing := \{x \mid x \neq x\} - \textit{klasa pusta}.$$

Z formalnego punktu widzenia wyrażenia klasowe występować będą w poniższych trzech kontekstach, gdzie: x, y to zmienne, F —formuła, C, D — klasy:

(1) $\quad y \in \{X \mid F\} := \begin{cases} [F, x \mapsto y], & \text{gdy podstawienie } x \mapsto y \text{ jest poprawne w } F, \\ \exists\, x\ (x = y \wedge F), & \text{w przeciwnym wypadku.} \end{cases}$

(2) $\quad C = D := \forall\, x\ (x \in C \iff x \in D)$ przy dodatkowym założeniu, że jedna z klas C, D jest wyrażeniem klasowym — x jest leksykograficznie pierwszą zmienną różną od zmiennych wolnych w klasach C i D — ten ostatni warunek będzie się stale powtarzał przy definicjach formalnych (dla zapewnienia jednoznaczności przy eliminacji symboli wprowadzanych definicyjnie) i w dalszym ciągu — jako oczywisty — będzie opuszczany.

(3) $\quad C \in D := \exists\, x\ (x = C \wedge x \in D)$ przy dodatkowym założeniu, że C jest wyrażeniem klasowym.

Dla dowolnych klas A, B przyjmiemy następujące oznaczenia i terminologię:

$A \subset B := \forall\, x\ (x \in A \implies x \in B)$ — A *jest zawarte* w B, B *zawiera* A (*inkluzja*)

$A \subsetneq B := A \subset B \wedge A \neq B$ — A *jest silnie zawarte* w B, B *silnie zawiera* A (*silna inkluzja*)

$A \cup B := \{x \mid x \in A \vee x \in B\}$ — *suma mnogościowa* A i B lub *połączenie* A i B

$A \cap B := \{x \mid x \in A \wedge x \in B\}$ — *iloczyn mnogościowy* A i B lub *przecięcie* A i B

$A \setminus B := \{x \mid x \in A \wedge x \notin B\}$ — *różnica mnogościowa* A i B

$A^{\neg} := \mathbb{V} \setminus A$ — *dopełnienie* (*absolutne*) A; często jeżeli wszystkie rozważane klasy są zawarte w pewnej ustalonej klasie V, to $A^{\neg}$ oznacza $V \setminus A$ (kontekst!)

$\bigcup A := \{x \mid \exists\, a \in A : x \in a\}$ — *unia* A

$\bigcap A := \{x \mid \forall\, a \in A : x \in a\}$ — *intersekcja* A.

Jeżeli $A = A_t$ jest klasą, w której występuje wolno zmienna (parametr) t, to

$\bigcup_{t\in T} A_t := \{x \mid \exists\, t \in T : x \in A_t\}$

$\bigcap_{t\in T} A_t := \{x \mid \forall\, t \in T : x \in A_t\}$.

$\mathcal{P}A := \{x \mid x \subset A\}$ — *potęga* A.

Z ważnych tautologii dotyczących wyżej wprowadzonych pojęć wymieńmy zwrotność i przechodniość inkluzji (antysymetria jedynie wówczas gdy jedna ze stron jest wyrażeniem klasowym) oraz

$$x \in \mathbb{V}, x \notin \varnothing, \mathbb{V} \neq \varnothing, \varnothing \subset A \subset \mathbb{V}$$

$$A \subset B \iff B^{\neg} \subset A^{\neg} \iff A \cup B = B \iff A \cap B = A \iff A \setminus B = \varnothing.$$

Następnie łączność, przemienność i wzajemną rozdzielność działań $\cup$ i $\cap$ oraz *prawa de Morgana*:

$$(A \cup B)^{\neg} = A^{\neg} \cap B^{\neg}, \qquad (A \cap B)^{\neg} = A^{\neg} \cup B^{\neg}.$$

Wreszcie trzy tautologie dotyczące działań $\bigcup$, $\bigcap$, $\mathcal{P}$: $\bigcup \varnothing = \varnothing$, $\bigcap \varnothing = \mathbb{V}$, $\mathcal{P}\mathbb{V} = \mathbb{V}$.

W dalszym ciągu litery x, X, ξ, y, Y, η, z, Z, ζ, x', ... oznaczać będą zmienne. Pozostałe litery a, A, α, b, B, ... — dowolne klasy chyba że z kontekstu lub ustanowienia będzie wynikało inaczej.

Formułę $A \in \mathbb{V}$ będziemy odczytywać: A jest *zbiorem* lub — A jest klasą *małą*; klasę, która nie jest mała (formuła: $A \notin \mathbb{V}$), nazywamy *dużą* lub *właściwą*.
Zdanie „$A \in \mathbb{V} \iff \exists\, x\ x = A$" jest tautologią.

Słynna *antynomia* (*paradoks*) Russella to tautologia:

$$\{x \mid x \notin x\} \notin \mathbb{V}.$$

Tak więc naturalny pozornie postulat, żeby każda klasa była zbiorem (*Schema of Axioms of Comprehension*), prowadzi do teorii sprzecznej, a więc bezwartościowej. Konieczna jest aksjomatyzacja teorii mnogości.

2.2. Tematy

1. Przyjmując, że x, y są pierwszymi leksykograficznie zmiennymi ($x = \square$, $y = \square'$), zapisać zdanie $\varnothing \in \mathbb{V}$ w języku formalnym teorii mnogości — bez skrótów definicyjnych.

Jaka jest długość i stopień złożenia tego zdania?

2. Które z poniższych zdań, a właściwie schematów zdań, gdyż A, B, C, D, ... oznaczają (tu i dalej) dowolne klasy, są tautologiami?

(1) $(A \setminus B) \cup (A \setminus C) \cup (B \setminus C) = A \cap C \iff A \cup B \subset C \wedge A \cap B = \varnothing$
(2) $(A \cup B) \setminus C = (A \setminus C) \cup B \iff B \cap C = \varnothing$
(3) $((A \cap B) \cup C) \setminus A = (A \cap B) \setminus C \iff A \cap B \subset C \subset A$
(4) $A \setminus (B \setminus (C \setminus D)) = (A \cap C) \setminus D \iff A \setminus B \subset (A \cap C) \setminus D$.

3. Określamy *różnicę symetryczną* $A \dot{-} B := (A \setminus B) \cup (B \setminus A)$.
Wykazać, że:

(1) $(A \dot{-} B) \dot{-} C = A \dot{-} (B \dot{-} C)$ (*łączność*)
(2) $A \dot{-} B = B \dot{-} A$ (*przemienność*)
(3) $A \dot{-} \varnothing = A$ (*neutralność* $\varnothing$)
(4) $A \dot{-} A = \varnothing$ (*dopełnienie do* $\varnothing$)
(5) $A \cap (B \dot{-} C) = (A \cap B) \dot{-} (A \cap C)$ (*rozdzielność* mnożenia względem różnicy symetrycznej)
(6) $(A \dot{-} B) \cup (B \dot{-} C) \cup (C \dot{-} A) = (A \setminus B) \cup (B \setminus C) \cup (C \setminus A), \ldots$

4. Wykazać, że dla klas $A_1, \ldots, A_n, B_1, \ldots, B_n$, gdzie $n = 2, 3, \ldots$, zachodzi inkluzja:

$$(A_1 \cup \ldots \cup A_n) \dot{-} (B_1 \cup \ldots \cup B_n) \subset (A_1 \dot{-} B_1) \cup \ldots \cup (A_n \dot{-} B_n).$$

5. Ustalmy klasę V. Dla klas $A, B, C \subset V$ oznaczamy: $A^0 = A$, $A^1 = A^\urcorner = V \setminus A$, $AB = A \cap B$, $AB \cup C = (AB) \cup C$ itp.

Ustalmy trzy klasy (ogólnie: n klas, gdzie $n = 1, 2, \ldots$), A_1, A_2, $A_3 \subset V$. Każdą z klas $A_1^{\alpha_1} A_2^{\alpha_2} A_3^{\alpha_3}$, gdzie $\alpha_1, \alpha_2, \alpha_3 = 0, 1$, nazywamy *składową* układu klas A_1, A_2, A_3.

Różnych składowych jest co najwyżej $2 \times 2 \times 2 = 8$ (ogólnie 2^n).

Łatwo widać, że klasa V jest sumą wszystkich składowych, składowe są parami rozłączne, i każda z klas A_i jest sumą tych składowych, dla których $\alpha_i = 1$.

Zilustrować powyższą sytuację rysunkiem — będzie to tak zwany *diagram Venna*.

Mówimy, że dany układ klas jest *niezależny* (lub też, że klasy te są *w położeniu ogólnym*), gdy wszystkie składowe tego układu są niepuste.

Udowodnić, że mając dane klasy A, B, $C \subset V$ i wykonując na nich „działania boole'owskie" $\cup$, $\cap$, $\urcorner$, $\setminus$ można uzyskać co najwyżej 2^8 (ogólnie 2^{2^n}) różnych podklas klasy V; dokładnie 2^8 (2^{2^n}), gdy układ A, B, C jest niezależny.

6*. Dane są klasy $A_1, A_2, \ldots, A_n \subset V$, $n \geqslant 2$. Wykazać, że klasa $A_1 \dot{-} A_2 \dot{-} \ldots \dot{-} A_n$ (według 3(1) nawiasy można opuszczać) jest sumą wszystkich składowych $A_1^{\alpha_1} \ldots A_n^{\alpha_n}$ (zob. 5.), dla których zbiór $\{i \mid \alpha_i = 0\}$ ma nieparzystą liczbę elementów.

7. Naszkicować dowody tautologii: $\bigcup \varnothing = \varnothing$, $\bigcap \varnothing = \mathbb{V}$, $\mathcal{P}\mathbb{V} = \mathbb{V}$.

8. Litery A i B oznaczają dowolne klasy. Ustalić, który ze znaków $\subset$, $\supset$, $=$ można wstawić w miejsce „?", aby otrzymać tautologię:

(1) $A \subset B \implies \bigcup A \ ? \bigcup B$
(2) $A \subset B \implies \bigcap A \ ? \bigcap B$
(3) $A \subset B \implies \mathcal{P}A \ ? \ \mathcal{P}B$
(4) $\bigcup(A \cup B) \ ? \bigcup A \cup \bigcup B$
(5) $\bigcup(A \cap B) \ ? \bigcup A \cap \bigcup B$
(6) $\bigcap(A \cup B) \ ? \bigcap A \cap \bigcap B$
(7) $\bigcap(A \cap B) \ ? \bigcap A \cup \bigcap B$
(8) $\mathcal{P}(A \cup B) \ ? \ \mathcal{P}A \cup \mathcal{P}B$

(9) $\mathcal{P}(A \cap B) \mathbin{?} \mathcal{P}A \cap \mathcal{P}B$
(10) $A \mathbin{?} \bigcup \mathcal{P}A$
(11) $A \mathbin{?} \mathcal{P} \bigcup A$
(12) $\bigcup A \mathbin{?} \bigcup \mathcal{P} \bigcup A$.

9. Klasę A nazywamy *tranzytywną*, gdy $\forall\, x, y : x \in y \in A \implies x \in A$.
Wykazać, że poniższe trzy warunki są równoważne:
(1) A — klasa tranzytywna
(2) $A \subset \mathcal{P}A$
(3) $\bigcup A \subset A$.

10. Napisać pełny dowód formalny zdania Russella $\{x \mid x \notin x\} \notin \mathbb{V}$ jako tautologii czystej klasy 2.

11. Wyrażenia klasowe wraz z symbolem przynależności można wprowadzić w dowolnym języku elementarnym niebędącym rozszerzeniem języka $\mathrm{L}_{\mathrm{set}}$. W ogólnym przypadku takiego języka dopuszczamy też symbole funkcyjne, z których tworzymy termy.

Przykładowo rozważmy *język elementarny arytmetyki*: L_{ar}. W języku tym symbol równości jest jedynym predykatem; natomiast wprowadzamy cztery symbole funkcyjne: $0^\bullet$ (zero), S (następnik), $+$, $\cdot$ (symbole dodawania i mnożenia).

Termy określamy indukcyjnie:
1) termy klasy 0 to zmienne (x, y, z,...)
2) dla naturalnego n, termy klasy $n+1$ to termy klasy n oraz słowa postaci: $0^\bullet$, St, $(t+s)$, $(t \cdot s)$, gdzie t, s są termami klasy n
3) słowo t jest termem, jeżeli dla pewnego n jest termem klasy n; najmniejsze takie n to *stopień złożenia*, krócej — *złożoność* termu t.

Formuły atomiczne języka L_{ar} są postaci $t = s$, gdzie t i s są termami.

Rozszerzamy definicję podstawiania: możemy podstawiać termy w miejsce zmiennych, przy czym podstawienie $x \mapsto t$ w formule A jest *poprawne* — tylko takie będziemy dopuszczać — gdy dla każdej zmiennej y występującej w termie t: $\mathrm{Fr}(x, A) \cap \mathrm{Bd}(y, A) = \varnothing$. Należy również zmodyfikować regułę wnioskowania **R14**: $\forall\, x \; A \vdash [A, x \mapsto t]$.
Odpowiednio też zmieniamy punkty (1), (2) i (3) we wprowadzeniu wyrażeń klasowych, które nazywamy po prostu klasami (termy odpowiadają liczbom naturalnym):

$$(1)\; t \in \{x \mid F\} :\Leftrightarrow \begin{cases} [F, x \mapsto t], & \text{gdy podstawienie } x \mapsto t \text{ w formule } F \text{ jest poprawne} \\ \exists\, x\; (x = t \wedge F) & \text{w przeciwnym wypadku.} \end{cases}$$

W punktach (2) i (3) zarówno C jak i D muszą być klasami (tj. wyrażeniami klasowymi).

Klasa pełna to $\mathbb{N} := \{x \mid x = x\}$. Szczególne znaczenie mają termy stałe (tj. bez zmiennych) postaci $n^\bullet := \underbrace{S \ldots S}_{n\text{-razy}} 0^\bullet$ $(n = 0, 1, \ldots)$ zwane *liczebnikami*.

W metajęzykowym zapisie używa się powszechnie przyjętych skrótów i konwencji, pisząc np. $x + yz$ zamiast $(x + (y \cdot z))$. Często też opuszcza się kropkę w oznaczeniu liczebnika, odwołując się do kontekstu.

Aksjomatami identyczności w L_{ar} są zdania:

(1) $x = x$

(2) $x = y \implies y = x$

(3) $x = y \wedge y = z \implies y = z$

(4) $x = y \implies Sx = Sy$

(5) $x = y \wedge z = t \implies x + z = y + t$

(6) $x = y \wedge z = t \implies xz = yt$, gdzie x, y, z, t są kolejnymi zmiennymi $\square$, $\square'$, ...

Poniższy zbiór siedmiu zdań języka $\mathrm{L_{ar}}$ nazywamy *aksjomatyką Robinsona*; w skrócie RA:

RA1 $Sx = Sy \implies x = y$

RA2 $Sx \neq 0^\bullet$

RA3 $x + 0^\bullet = x$

RA4 $x + Sy = S(x + y)$

RA5 $x \cdot 0^\bullet = 0^\bullet$

RA6 $x \cdot Sy = xy + x$

RA7 $x \neq 0^\bullet \implies \exists\, y\; x = Sy$.

Tak więc w *arytmetyce Robinsona* korzystamy z $6 + 7 = 13$ aksjomatów — aksjomatyka jest skończona.

W dalszym ciągu zakładamy, że RA jest niesprzeczna.

1) Przyjmując, że x, y są dowolnymi zmiennymi, wypisać wszystkie termy o złożoności 1.

2) Dla zdania A języka $\mathrm{L_{ar}}$ zapis $\vdash A$ oznaczać będzie, że zdanie A jest twierdzeniem arytmetyki Robinsona. Udowodnić, że $\forall a, b \in \mathbb{N}$:
(i) $a \neq b \iff \vdash a^\bullet \neq b^\bullet$
(ii) $a = b \iff \vdash a^\bullet = b^\bullet$
(iii) $\vdash (a + b)^\bullet = a^\bullet + b^\bullet$
(iv) $\vdash (ab)^\bullet = a^\bullet b^\bullet$
(v) $\vdash \forall\, x\; Sx + a^\bullet = x + (a + 1)^\bullet$.

3) Dla termów t, s określamy nierówność:

$$t < s \;:\!\iff \exists\, x\; Sx + t = s.$$

Wykazać, że $\forall\, a, b \in \mathbb{N}$:
(i) $a < b \iff \vdash a^\bullet < b^\bullet$
(ii) $\vdash \neg\exists\, x\; x < 0^\bullet$
(iii) $\vdash x < (a + 1)^\bullet \implies x = 0^\bullet \vee \ldots \vee x = a^\bullet$
(iv) $\vdash a^\bullet < x \implies (a + 1)^\bullet < x \vee (a + 1)^\bullet = x$
(v) $\vdash x < a^\bullet \vee x = a^\bullet \vee a^\bullet < x$.

4) Jeżeli aksjomat RA7 zastąpimy tak zwanym *schematem aksjomatów indukcji*:

$$0^\bullet \in C \wedge \forall\, x\, (x \in C \implies Sx \in C) \implies C = \mathbb{N}$$

(C jest tutaj dowolną klasą, mamy nieskończenie wiele aksjomatów), to otrzymamy teorię zwaną *arytmetyką Peana*, w skrócie PA.

Udowodnić, że zdanie RA7 jest twierdzeniem arytmetyki Peana.
KOMENTARZ.

Aksjomatykę RA wprowadził Raphael Mitchel Robinson jako system Q, badając dowód twierdzenia o reprezentowalności funkcji rekursywnych (=algorytmicznie obliczalnych wg *tezy Churcha*) w PA. Odkrył on, że schemat aksjomatów indukcji wykorzystuje się w tym dowodzie jedynie do uzyskania zdania RA7. Twierdzenie o reprezentowalności jest punktem wyjścia do podstawowego twierdzenia limitacyjnego (Gödel, Tarski i inni) o nierozstrzygalności i niezupełności RA (teorię formalną T nazywamy *zupełną*, jeśli jest niesprzeczna, i dla każdego zdania A tej teorii: $T \vdash A$ lub $T \vdash \neg A$; oczywiście z zupełności teorii wynika jej rozstrzygalność) i wszystkich niesprzecznych i rekursywnie aksjomatyzowalnych teorii bogatszych — w szczególności PA i ZFC (zob. np. [**Grell 06**, s. 366]).

2.3. Odpowiedzi

1. $\exists x\, (\forall y\, (y \in x \iff \neg y = y) \wedge x = x)$, 20, 5.

2. Wszystkie cztery.

Na przykład, używając uproszczonej notacji: $AB = A \cap B$, $AB \cup C = (A \cap B) \cup C$, $A^\neg = \mathbb{V} \setminus A$, równoważność (2) możemy zapisać w postaci

$$AC^\neg \cup BC^\neg = AC^\neg \cup B \iff BC = \varnothing.$$

Implikację „$\Rightarrow$” otrzymamy, mnożąc obie strony równości przez C.
Implikacja „$\Leftarrow$” wynika z równoważności: $BC = \varnothing \iff B \subset C^\neg \iff BC^\neg = B$.

Możemy też „działać na argumentach”.

Na przykład: dowodzimy implikacji „$\Rightarrow$” w (1). Chcąc dowieść, że $A \cap B = \varnothing$, rozumujemy nie wprost: HP: $A \cap B \neq \varnothing, \exists)\, x \in A \cap B, x \in A, x \in B$; rozpatrując teraz przypadki 1) $x \in C$, 2) $x \notin C$ za każdym razem dochodzimy do sprzeczności.

3. Używając uproszczonej notacji z rozwiązania poprzedniego zadania, przekształcamy lewą stronę równości (1):

$$\begin{aligned} L &= (AB^\neg \cup A^\neg B) \dot{-} C \\ &= (AB^\neg \cup AB^\neg)^\neg C \cup (AB^\neg \cup A^\neg B)C^\neg \\ &= (A^\neg \cup B)(A \cup B^\neg)C \cup AB^\neg C^\neg \cup A^\neg BC^\neg \\ &= (A^\neg B^\neg \cup AB)C \cup AB^\neg C^\neg \cup A^\neg BC^\neg \\ &= ABC \cup A^\neg B^\neg C \cup AB^\neg C^\neg \cup A^\neg BC^\neg. \end{aligned}$$

Analogicznie przekształcamy prawą stronę, $P = \ldots$, i stwierdzamy, że $L = P$.

Podobnie możemy uzasadnić pozostałe równości.

4. Zastosujmy indukcję na n (skrótowe oznaczenia — jak w zadaniach 2 i 3):

(i) $n = 2$

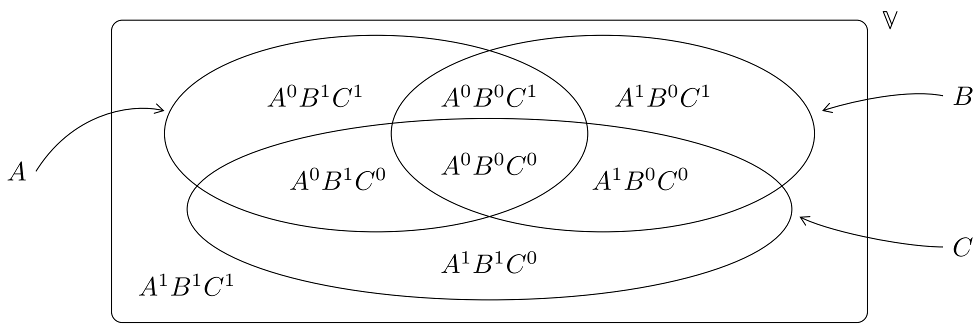
$(A \cup B) \dot{-} (C \cup D) = (A \cup B)C^\neg D^\neg \cup A^\neg B^\neg (C \cup D) = ABC^\neg \cup ABD^\neg \cup A^\neg B^\neg C \cup A^\neg B^\neg D \subset AC^\neg \cup BD^\neg \cup A^\neg C \cup B^\neg D = (A \dot{-} C) \cup (B \dot{-} D)$.

(ii) Zakładamy, że $n \geqslant 3$, i inkluzja zachodzi dla $n - 1$.

$(A_1 \cup \ldots \cup A_n) \dot{-} (B_1 \cup \ldots \cup B_n) = ((A_1 \cup \ldots \cup A_{n-1}) \cup A_n) \dot{-} ((B_1 \cup \ldots \cup B_{n-1}) \cup B_n) \subset$

$((A_1 \cup \ldots \cup A_{n-1}) \dot{-} (B_1 \cup \ldots \cup B_{n-1})) \cup (A_n \dot{-} B_n) \subset (A_1 \dot{-} B_1) \cup \ldots \cup (A_{n-1} \dot{-} B_{n-1}) \cup (A_n \dot{-} B_n)$.

5.



Można ograniczyć się do działań $\cup$ i $^\urcorner$, gdyż $A \cap B = (A^\urcorner \cup B^\urcorner)^\urcorner$, $A \setminus B = A \cap B^\urcorner$.

Ponieważ dopełnienie składowej jest sumą pozostałych składowych, więc każdą podklasę tego rodzaju można przedstawić jako sumę składowych (indukcja na złożoność „wyrażenia boole'owskiego"); jest więc ich co najwyżej tyle, ile jest podzbiorów 8-elementowego zbioru: 000, 001, 010, 011, 100, 101, 110, 111, a więc co najwyżej 2^8 (ogólnie 2^{2^n}), dokładnie 2^8 (2^{2^n}), gdy nasz układ jest niezależny.

6*. Indukcja na n:

I Dla $n = 2$, $A_1 \dot{-} A_2 = A_1^0 A_2^1 \cup A_1^1 A_2^0$.

II Zakładamy, że $n \geqslant 3$ dla $n-1$ jest tak jak w tezie. $A_1 \dot{-} A_2 \dot{-} \ldots \dot{-} A_n = (A_1 \dot{-} \ldots \dot{-} A_{n-1}) \dot{-} A_n = (A_1 \dot{-} \ldots \dot{-} A_{n-1}) A_n^1 \cup (A_1 \dot{-} \ldots \dot{-} A_{n-1})^\urcorner A_n^0$.

Składowe pierwszego składnika są postaci $A_1^{\alpha_1} \ldots A_{n-1}^{\alpha_{n-1}} A_n^{\alpha_n}$, gdzie $\alpha_n = 1$, a więc dla każdej z nich liczba zer wśród $\alpha_1, \ldots, \alpha_n$ jest taka sama jak liczba zer wśród $\alpha_1, \ldots, \alpha_{n-1}$, czyli — na mocy założenia indukcyjnego — nieparzysta.

Również na mocy założenia indukcyjnego składowe klasy $(A_1 \dot{-} \ldots \dot{-} A_{n-1})^\urcorner$ są postaci $A_1^{\alpha_1} \ldots A_{n-1}^{\alpha_{n-1}}$ z parzystą liczbą zer wśród $\alpha_1, \ldots, \alpha_{n-1}$, a więc składowe drugiego składnika, będąc postaci $A_1^{\alpha_1} \ldots A_{n-1}^{\alpha_{n-1}} A_n^{\alpha_n}$, gdzie $\alpha_n = 0$, też mają nieparzystą liczbę zer wśród $\alpha_1, \ldots, \alpha_{n-1}, \alpha_n$.

Jeżeli jednak jakaś składowa układu klas $A_1, \ldots, A_n$ jest postaci $A_1^{\alpha_1} \ldots A_n^{\alpha_n}$ z nieparzystą liczbą zer wśród $\alpha_1, \ldots, \alpha_n$, to rozpatrując dwa przypadki: $\alpha_1 = 0$ i $\alpha_1 = 1$, wnioskujemy, że jest ona składową pierwszego lub drugiego składnika.

7. Dowody są niemal mechaniczne.

Na przykład dla tautologii: $\bigcap \varnothing = \mathbb{V}$. HP: $\neg \ldots, \exists) \, x \notin \bigcap \varnothing$, $\neg \forall y \; (y \in \varnothing \;\Rightarrow\; x \in y)$, $\exists y) \, \neg (y \in \varnothing \;\Rightarrow\; x \in y)$, $y \in \varnothing$, $y \neq y, y = y$ (aksjomat identyczności (1), zob. 11) $\lightning$.

8.

(1) $A \subset B \implies \bigcup A \subset \bigcup B$

(2) $A \subset B \implies \bigcap A \supset \bigcap B$

(3) $A \subset B \implies \mathcal{P}A \subset \mathcal{P}B$

(4) $\bigcup(A \cup B) = \bigcup A \cup \bigcup B$
(5) $\bigcup(A \cap B) \subset \bigcup A \cap \bigcup B$
(6) $\bigcap(A \cup B) = \bigcap A \cap \bigcap B$
(7) $\bigcap(A \cap B) \supset \bigcap A \cup \bigcap B$
(8) $\mathcal{P}(A \cup B) \supset \mathcal{P}A \cup \mathcal{P}B$
(9) $\mathcal{P}(A \cap B) = \mathcal{P}A \cap \mathcal{P}B$
(10) $A \supset \bigcup \mathcal{P}A$
(11) $A \subset \mathcal{P} \bigcup A$
(12) $\bigcup A = \bigcup P \bigcup A.$

9. Bezpośrednio z definicji: (1) $\iff$ (2), (1) $\iff$ (3).

10.

(0) $\neg \ldots$	
(1) $\{x \mid x \notin x\} \in \mathbb{V}$	(0), **R2**
(2) $\exists x)\ x = \{x \mid x \notin x\} \wedge x \in \mathbb{V}$	(1), **R13**
(3) $x = \{x \mid x \notin x\}$	(2), **R7**
(4) $x \in x \iff x \notin x$	(3), **R14**
(5) $\forall x\ ((x \in x \iff x \notin x) \implies x \in x)$	dopisana tautologia czysta klasy 1
(6) $(x \in x \iff x \notin x) \implies x \in x$	(5), **R14**
(7) $x \in x$	(4), (6), **R1**
(8) $x \in x \implies x \notin x$	(4), **R10**
(9) $x \notin x$	(7), (8), **R1**
	$\lightning$ (7), (9).

Dowód zdania (5):

(0) $\neg \ldots$	
(1) $\exists x\ \neg((x \in x \iff x \notin x) \implies x \in x)$	(0), **R16**
(2) $\neg((x \in x \iff x \notin x) \implies x \in x)$	(1), **R13**
(3) $(x \in x \iff x \notin x) \wedge x \notin x$	(2), **R3**
(4) $x \in x \iff x \notin x$	(3), **R7**
(5) $x \notin x$	(3), **R8**
(6) $x \notin x \implies x \in x$	(4), **R11**
(7) $x \in x$	(5), (6), **R1**
	$\lightning$ (5), (7).

11.

1) $0^\bullet, Sx, x + y, xy$
2) Ad (i):

$\Leftarrow$) Wniosek z aksjomatu równości (1).
$\Rightarrow$) Można przyjąć: $a < b$ $\quad\langle$aksjomat równości (2)$\rangle$.
Indukcja na a:

I) $a = 0$.
Wówczas $b > 0$, $\exists)\, d \in \mathbb{N} : b = d + 1, b^\bullet = Sd^\bullet$, więc według RA2 $Sd^\bullet \neq 0^\bullet$, czyli $b^\bullet \neq a^\bullet$, $a^\bullet \neq b^\bullet$ (znów według aksjomatu równości (2)).
II) $a = c + 1$ i $\forall\, d \in \mathbb{N} : c < d \implies \vdash c^\bullet \neq d^\bullet$.
Wówczas znów $\exists)\, d \in \mathbb{N} : b = d{+}1, c < d$, a więc $\vdash c^\bullet \neq d^\bullet$ i, według RA1 $\vdash Sc^\bullet \neq Sd^\bullet$, czyli $\vdash a^\bullet \neq b^\bullet$.
(ii) jest natychmiastowym wnioskiem z (i).
(iii) i (iv) dowodzimy prostą indukcją na b, wykorzystując odpowiednio RA3, RA4, i RA5, RA6.
Ad (v) Indukcja na a:
I) $a = 0$.
HP: $\exists x)\ Sx + 0^\bullet \neq x + S0^\bullet$, $Sx + 0^\bullet = Sx$, $x + S0^\bullet = S(x + 0^\bullet) = Sx$ ↯
II) HP: $Sx + (a+1)^\bullet \neq x + (a+2)^\bullet$, $Sx + a^\bullet = x + (a+1)^\bullet$, $S(Sx + a^\bullet) = Sx + Sa^\bullet = Sx + (a+1)^\bullet = S(x + (a+1)^\bullet) = x + S(a+1)^\bullet = x + (a+2)^\bullet$ ↯.
3) Podobnie jak w 2) dowody są bezproblemowe.
W dowodzie zdania (ii) po raz pierwszy trzeba skorzystać z RA7 ⟨HP: $\exists x)\ x < 0^\bullet$, $\exists y)\ Sy + x = 0^\bullet$, $x \neq 0^\bullet$ ⟨HP: $x = 0^\bullet$, $Sy + 0^\bullet = 0^\bullet$, $Sy = 0^\bullet$ ↯ (RA3, RA2)⟩, $\exists z)\ x = Sz$ (RA7), $Sy + Sz = 0^\bullet$, $S(Sy + z) = 0^\bullet$ (RA4), ↯(RA2)⟩.

W dowodzie indukcyjnym (iii) w kroku wstępnym ($a = 0$) wykorzystujemy (ii); w kroku indukcyjnym trzeba rozpatrywać odpowiednią liczbę przypadków.

⟨HP: $x < (a{+}2)^\bullet, x \neq 0^\bullet, \ldots, x \neq a^\bullet, x \neq (a{+}1)^\bullet$. $\exists y)\ Sy{+}x = (a{+}2)^\bullet$, $\exists z)\ x = Sz$ (RA7). Tak więc $Sy + Sz = S(a+1)^\bullet$, $S(Sy + z) = S(a+1)^\bullet$, $Sy + z = (a+1)^\bullet$ (RA1); czyli $z < (a{+}1)^\bullet$. Zatem, według założenia indukcyjnego $z = 0^\bullet \vee \ldots \vee z = a^\bullet$, i teraz trzeba rozpatrzyć $a+1$ przypadków. Dla ustalonego $c \in \{0, \ldots, a\}$ odpowiedni przypadek ma postać $z = c^\bullet$, i wówczas $x = Sz = Sc^\bullet = (c+1)^\bullet$ ↯⟩.

4) W schemacie aksjomatów indukcji bierzemy

$$C = \{x \mid x \neq 0^\bullet \implies \exists\, y\ x = Sy\}.$$

Wówczas $0^\bullet \in C$ i $\forall\, x\ (x \in C \implies Sx \in C)$

⟨HP: $\exists x)\ x \in C, Sx \notin c$. Tak więc $\neg(Sx \neq 0^\bullet \implies \exists\, y\ Sx = Sy)$, czyli $Sx \neq 0^\bullet$, $\neg\exists\, y\ Sx = Sy$, $\forall\, y\ Sx \neq Sy$, skąd $Sx \neq Sx$ ↯⟩, a więc $C = \mathbb{N}$.

3

Aksjomatyczna teoria mnogości ZFC

3.1. Wstęp

Aksjomatyka ZFC (Zermelo–Fraenkel + Axiom of Choice) składa się z niżej wymienionych zdań (jednocześnie ustalimy podstawową symbolikę i terminologię teorii mnogości): $A1, \ldots, A5, A6(H,x)$ (H – formuła, x – zmienna), $A7$, $A8$, $A9$.

A1 (*Aksjomat zakresu*, *aksjomat ekstensjonalności*) $x \subset y \wedge y \subset x \implies x = y$.

A2 (*Aksjomat zbioru pustego*) $\varnothing \in \mathbb{V}$.

Tak więc twierdzeniami są zdania: $A \subset B \wedge B \subset A \iff A = B$ (A, B – dowolne klasy) oraz $\exists\, y\ \forall\, x\ x \notin y$ i $(\forall\, x\ x \notin y) \wedge (\forall\, x\ x \notin z) \implies y = z$. Zbiór pusty jest jedynym „elementem pierwotnym”, z którego są zbudowane wszystkie inne zbiory.

Singletony, *dubletony* i ogólniej *układy nieuporządkowane* określamy następująco: (a, b, … – dowolne klasy): $\{a\} := \{x \mid a \in \mathbb{V} \implies x = a\}$ ([**Kelley 57**, Appendix]), $\{a,b\} := \{a\} \cup \{b\}$, $\{a,b,c\} := \{a\} \cup \{b,c\}$ itd.
Wówczas $a \notin \mathbb{V} \implies \{a\} = \mathbb{V}$, $a \notin \mathbb{V} \vee b \notin \mathbb{V} \implies \{a,b\} = \mathbb{V}$ itd. (symbol $\mathbb{V}$ klasy pełnej odgrywa rolę *uniwersalnego symbolu nieoznaczoności*) oraz
$a \in \mathbb{V} \implies (x \in \{a\} \iff x = a)$
$(a,b) \in \mathbb{V} \implies (x \in \{a,b\} \iff x = a \vee x = b)$ itd.

Ponadto $a, b \in \mathbb{V} \implies \bigcup\{a\} = \bigcap\{a\} = a$, $\bigcup\{a,b\} = a \cup b$, $\bigcap\{a,b\} = a \cap b$ itd.

A3 (*Aksjomat dubletona*) $\{x,y\} \in \mathbb{V}$.

A4 (*Aksjomat unii*) $\bigcup x \in \mathbb{V}$.

A5 (*Aksjomat potęgi*) $\mathcal{P}x \in \mathbb{V}$.

Zachodzą równości: $\{x\} \in \mathbb{V}$, $x \cup y \in \mathbb{V}$, $\bigcup \mathbb{V} = \mathbb{V}$, $\bigcap \mathbb{V} = \varnothing$.
Parę uporządkowaną (podwójne oznaczenie) określamy na sposób Wienera–Kuratowskiego:

$$(a,b) = a \mapsto b := \{\{a\},\{a,b\}\}, \text{ i dalej}$$
$$(a,b,c) := (a,(b,c)), \ldots.$$

Wówczas $(x,y) \in \mathbb{V}$ oraz $(x,y) = (z,t) \iff x = z \wedge y = t$.
Określamy *iloczyn kartezjański* $A \times B := \{(a,b) \mid a \in A, b \in B\}$; zapis po prawej stronie jest skrótem dla $\{x \mid \exists\, a,b :\ a \in A \wedge b \in B \wedge x = (a,b)\}$. Tego rodzaju skróty dla wyrażeń klasowych będą w dalszym ciągu powszechnie używane.
$A \times B \times C := A \times (B \times C), \ldots$. $A^2 = A \times A$ ($A^{2\times}$ w razie niejasności)…
Dodatkowo $A^1 := A$, $A^0 := \{\varnothing\}$.

R – relacja $:\Leftrightarrow R \subset \mathbb{V}^2$. Tak więc *relacją* nazywamy dowolną klasę par. Ogólniej dla $R \subset \mathbb{V}^n (n = 0, 1, 2, \dots)$ mówimy o *relacji n-argumentowej*.

Zamiast „$(a, b) \in R$" piszemy też: $a\ R\ b$, $R : a \mapsto b$, $a \underset{R}{\mapsto} b$, $a \underset{R}{\leqslant} b$; przy znanym R: $a \mapsto b$, $a \leqslant b$.

Przyjmujemy następujące oznaczenia i terminologię:
$\mathrm{id} := \{x \mid \exists\, y\ x = (y, y)\}$ — *identyczność*
$R^{-1} := \{(y, x) \mid (x, y) \in R\}$ — *odwrotność* R
$S \circ R := \{(x, z) \mid \exists\, y\ (x, y) \in R \wedge (y, z) \in S\}$ — *złożenie*, *superpozycja* R z S.
Niewygodna kolejność — od prawej do lewej — w notacji superpozycji jest tradycyjna i wynika z ogólnie przyjętego zapisu funkcyjnego (np. $\sin x$ zamiast $x \sin$). Można wprowadzić dodatkowe oznaczenie $R \odot S := S \circ R$.
$\mathrm{Dom}\, R := \{x \mid \exists\, y\ (x, y) \in R\}$ — *dziedzina* R
$\mathrm{Im}\, R := \{y \mid \exists\, x\ (x, y) \in R\}$ — *obraz* R.

Wówczas:
R — relacja $\implies R \circ \mathrm{id} = \mathrm{id} \circ R = R\ \wedge\ (R^{-1})^{-1} = R$
$T \circ (S \circ R) = (T \circ S) \circ R$, $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$
$\mathrm{Dom}\, R^{-1} = \mathrm{Im}\, R$, $\mathrm{Im}\, R^{-1} = \mathrm{Dom}\, R$.

Relację f nazywamy *funkcją* lub *odwzorowaniem*, gdy spełnia *warunek jednoznaczności*: $\forall\, x\ y\ z\ (x, y), (x, z) \in f \implies y = z$; zapis: f — funkcja.

A6(H, x) (*Schemat aksjomatów zastępowania*)
f — funkcja $\wedge\, \mathrm{Dom}\, f \in \mathbb{V} \implies \mathrm{Im}\, f \in \mathbb{V}$, gdzie $f = \{x \mid H\}$, H — formuła, x — zmienna.

Twierdzenie o podzbiorach $A \subset B \in \mathbb{V} \implies A \in \mathbb{V}$.
$\langle$HP: $A \notin \mathbb{V}$. Wówczas, wg A2, $A \neq \varnothing$, $\exists)\, a \in A$, $f := \{x \mapsto x \mid x \in A\} \cup \{x \mapsto a \mid x \in B \setminus A\}$ jest funkcją, $\mathrm{Dom}\, f = B \in V$, $\mathrm{Im}\, f = A$, a więc wg A6, $A \in \mathbb{V}$ ↯$\rangle$.
(W pierwszej aksjomatyce teorii mnogości, którą podał Zermelo w 1908 roku, powyższe twierdzenie występowało jako *schemat aksjomatów wyróżniania* i dopiero Fraenkel w roku 1922 sformułował mocniejszy schemat A6).

Z pojęciem funkcji zwiążemy poniższe oznaczenia i terminy:

1) $f : A \multimap\!\!\to B :\Leftrightarrow f$ funkcja $\wedge\, \mathrm{Dom}\, f \subset A \wedge \mathrm{Im}\, f \subset B$ — f – *funkcja częściowa z A w B*
2) $f : A \longrightarrow B :\Leftrightarrow f : A \multimap\!\!\to B \wedge \mathrm{Dom}\, f = A$ — f – *funkcja z A w B*;
3) $f : A \twoheadrightarrow B :\Leftrightarrow f : A \longrightarrow B \wedge \mathrm{Im}\, f = B$ — f – *funkcja z A na B*, f – *surjekcja A na B*
4) f – *injekcja* $:\Leftrightarrow f$ – funkcja $\wedge\ f^{-1}$ – funkcja
5) $f : A \hookrightarrow B :\Leftrightarrow f : A \longrightarrow B \wedge f$ – injekcja — f – *injekcja A w B*
6) $f : A \hookrightarrow\!\!\!\!\!\twoheadrightarrow B :\Leftrightarrow f : A \twoheadrightarrow B \wedge f : A \hookrightarrow B$ — f – *bijekcja A na B*
7) $f|A := f \cap (A \times \mathbb{V})$ — *zacieśnienie* (*restrykcja*) *f do A*; oznaczamy też $f_A = F|A$;
8) $\mathrm{Map}^\circ(A, B) := \{f \mid f : A \multimap\!\!\to B\}$, $\mathrm{Map}(A, B) := \{f \mid f : A \longrightarrow B\}$ i analogicznie $\mathrm{Sur}(A, B)$, $\mathrm{Inj}(A, B)$, $\mathrm{Bij}(A, B)$
9) $\mathrm{Map}^\circ(A) := \mathrm{Map}^\circ(A, A)$ i analogicznie $\mathrm{Map}(A), \mathrm{Sur}(A), \mathrm{Inj}(A), \mathrm{Bij}(A) = \mathrm{Perm}(A)$, bijekcję $f : A \hookrightarrow\!\!\!\!\!\twoheadrightarrow A$ nazywamy *permutacją* lub *przekształceniem* klasy A

10) $\mathrm{val}(f,a) := \bigcap\{y \mid (a,y) \in f\}$ — *wartość f na argumencie a*; w dalszym ciągu zamiast $\mathrm{val}(f,a)$ będziemy pisali tradycyjnie $f(a)$, fa lub f_a.

Zanotujmy najważniejsze wnioski z aksjomatów A1–6; będą one dotyczyć przede wszystkim pojęcia funkcji.

(1) $\mathbb{V} \notin \mathbb{V} \quad \langle V \supset \{x \mid x \notin x\} \notin \mathbb{V}\rangle$

(2) $a \notin \mathbb{V} \vee b \notin \mathbb{V} \implies (a,b) = \mathbb{V}$

(3) $A \neq \varnothing \implies \bigcap A \in \mathbb{V} \quad \langle(\exists)\, x \in A\ \bigcap A \subset x \in \mathbb{V}\rangle$

(4) $a \notin \mathrm{Dom}\, f \implies f(a) = V$

(5) $a \in \mathrm{Dom}\, f \iff f(a) \neq \mathbb{V} \iff f(a) \in \mathbb{V}$

(6) $a \in \mathrm{Dom}\, f \wedge f-$ funkcja $\implies (a, f(a)) \in f \wedge f(a) \in \mathrm{Im}\, f$

(7) jeżeli f jest funkcją, to $y = f(x) \iff (x,y) \in f$ i $f = \{(x,y) \mid y = f(x)\}$

(8) dla funkcji f i g:
$f \subset g \iff \forall x \in \mathrm{Dom}\, f : f(x) = g(x)$,
$f = g \iff \forall x\ f(x) = g(x)$

(9) $A, B \in \mathbb{V} \implies A \times B$, $\mathrm{Map}(A,C)$, $\mathrm{Map}^\circ(A,B) \in V \quad \langle A \times B \subset \mathcal{P}\mathcal{P}(A \cup B), \mathrm{Map}(A,B) \subset \mathrm{Map}^\circ(A,B) \subset \mathcal{P}(A \times B)\rangle$

(10) $f : A \multimap\!\!\to B \wedge g : B \multimap\!\!\to C \implies g \circ f : A \multimap\!\!\to C$ i analogicznie dla $\longrightarrow$, $\twoheadrightarrow$ i $\hookrightarrow\!\!\!\!\twoheadrightarrow$

(11) $f : A \longrightarrow B \wedge g : B \longrightarrow A \wedge g \circ f = \mathrm{id}_A \implies f : A \hookrightarrow B \wedge g : B \twoheadrightarrow A$

(12) $f : A \longrightarrow B \wedge g : B \longrightarrow A \wedge g \circ f = \mathrm{id}_A \wedge f \circ g = \mathrm{id}_B \implies f : A \hookrightarrow\!\!\!\!\twoheadrightarrow B \wedge g : B \hookrightarrow\!\!\!\!\twoheadrightarrow A \wedge g = f^{-1}$

(13) $(g \circ f)|A = g \circ (f|A)$.

Ważne jest następujące *twierdzenie o sklejaniu funkcji:*

(14) $C \subset \mathrm{Map}^\circ(A,B) \implies [\bigcup C : A \multimap\!\!\to B \iff \forall f,g \in C\ \forall x \in \mathrm{Dom}\, f \cap \mathrm{Dom}\, g : f(x) = g(x)] \wedge [\bigcup C : A \multimap\!\!\to B \implies \mathrm{Dom} \bigcup C = \bigcup\{\mathrm{Dom}\, f \mid f \in C\}]$.

Klasę $\mathrm{Im}(f|A)$ nazywamy *obrazem A przez f* i notujemy skrótowo $f(A)$ lub fA. Klasę $f^{-1}(A)$ nazywamy *przeciwobrazem A przez f.*

(15) f – funkcja $\implies f(A) = \{f(x) \mid x \in A\}, f^{-1}(A) = \{x \mid f(x) \in A\}$.

Zanotujmy podstawowe fakty dotyczące obrazów i przeciwobrazów. Niech $f : X \longrightarrow Y$; X, Y – klasy; $A, B \subset X$, $C, D \subset Y$.

Wówczas:

(16) $F(A \cup B) = fA \cup fB$

(17) $f(A \cap B) \subset fA \cap fB$

(18) $f(A \setminus B) \supset fA \setminus fB$

(19) $f^{-1}(C \cup D) = f^{-1}C \cup f^{-1}D$

(20) $f^{-1}(C \cap D) = f^{-1}C \cap f^{-1}D$

(21) $f^{-1}(C \setminus D) = f^{-1}C \setminus f^{-1}D$

(22) $f\, f^{-1}C \subset C$

(23) $f : X \twoheadrightarrow Y \implies f\, f^{-1}C = C$

(24) $f^{-1}fA \supset A$

(25) $f: X \hookrightarrow Y \implies f^{-1}fA = A$.

Dla $A : I \longrightarrow \mathbb{V}$ mówimy też, że A jest rodziną zbiorów indeksowaną przez klasę indeksów I; w tej sytuacji notujemy często: $\bigcup\limits_{i\in I} A_i := \bigcup \operatorname{Im} A = \bigcup\{A_i \mid i \in I\}$, i analogicznie dla $\bigcap\limits_{i\in I} A_i$.

Prawa (16), (17) i (19), (20) można uogólnić na tego rodzaju sumy i iloczyny; na przykład, jeśli $I \neq \varnothing$ i $A : I \longrightarrow \mathcal{P}X$, to $f(\bigcap\limits_{i\in I} A_i) \subset \bigcap\limits_{i\in I} f(A_i)$.

Powyższej notacji używa się też w sytuacji, gdy A_i jest klasą (właściwą), zaś i jest zmienną (parametrem):

$$\bigcup_{i\in I} A_i := \{x \mid \exists\, i \in I : x \in A_i\}, \text{ i analogicznie dla } \bigcap_{i\in I} A_i.$$

Wygodną postać przyjmują wówczas np. *prawa de Morgana*:

$$I \neq \varnothing \wedge \forall\, i \in I\ A_i \subset X \implies (\bigcup_{i\in I} A_i)^{\neg} = \bigcap_{i\in I} A_i^{\neg} \wedge (\bigcap_{i\in I} A_i)^{\neg} = \bigcup_{i\in I} A_i^{\neg}.$$

A7 (*Aksjomat regularności*, *aksjomat o fundowaniu*):
$x \neq \varnothing \implies \exists\, y \in x : x \cap y = \varnothing$.

Z A7 wynika, że:

(26) $x \notin x$, $\neg(x \in y \wedge y \in x)$, $\neg(x \in y \wedge y \in z \wedge z \in x)$ ... ⟨Rozumując nie wprost stwierdzamy, że w zbiorach $\{x\}$, $\{x, y\}$, $\{x, y, z\}$, ... nie ma elementu minimalnego ze względu na przynależność — wbrew A7⟩.

Określamy *następnik* (*sekwens*) klasy a jako

$$\operatorname{seq} a := a \cup \{a\}.$$

Wówczas $a \notin \mathbb{V} \implies \operatorname{seq} a = \mathbb{V}$; natomiast $a \in \mathbb{V} \implies (x \in \operatorname{seq} a \iff x \in a \vee x = a)$, tak więc dla zbioru a zbiór $\operatorname{seq} a$ jest *standardowym rozszerzeniem zbioru a o jeden element* ($a \notin a$, $a \in \operatorname{seq} a$).

Zauważmy, że:

(27) $x = y \iff \operatorname{seq} x = \operatorname{seq} y$
⟨HP: $\operatorname{seq} x = \operatorname{seq} y, x \neq y$. Wówczas $x \in \operatorname{seq} x = \operatorname{seq} y = y \cup \{y\}$, a więc $x \in y$. Analogicznie $y \in x$ ↯⟩.

Możemy teraz określić indywidualnie *liczby naturalne*: $\bar{0} := \varnothing$, $\bar{1} := \operatorname{seq} \bar{0} = \{\varnothing\} = \{\bar{0}\}$, $\bar{2} := \operatorname{seq} \bar{1} = \{\varnothing, \{\varnothing\}\} = \{\bar{0}, \bar{1}\}$, ...
W dalszym ciągu będziemy zwykle pisali 0, 1, 2, ... zamiast $\bar{0}$, $\bar{1}$, $\bar{2}$, ..., zdając się na kontekst (w odróżnieniu języka od metajęzyka).

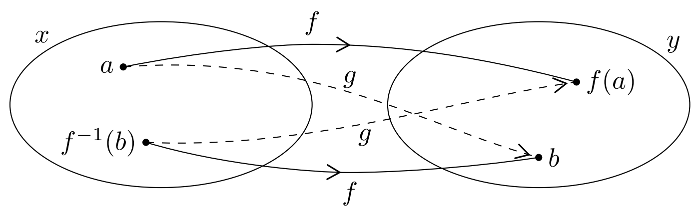
Jeżeli dla $m, n = 0, 1, 2 \ldots$ jest $m \neq n$, to twierdzeniem jest zdanie $\bar{m} \neq \bar{n}$ ⟨dowód indukcją na $\max(m, n)$ — oczywiście w metajęzyku⟩.

Mamy więc twierdzenia: $0 \neq 1$, $0 \neq 2$, $1 \neq 2$, $0 \neq 3$, ... — w bardziej ścisłym zapisie: $\bar{0} \neq \bar{1}$, $\bar{0} \neq \bar{2}$, ... — inaczej mówiąc, dysponujemy ciągiem parami różnych elementów 0, 1, 2, ...
Zbiory x, y nazywamy *równolicznymi*, co notujemy: $x \sim y$, gdy $\exists\, f : x \hookrightarrow\!\!\!\!\rightarrow y$.

Dla ustalonej liczby naturalnej n zbiór x nazywamy *n-elementowym*, gdy $x \sim n$; dla dowolnej klasy C oznaczamy $\mathcal{P}_n C := \{x \subset C \mid x \sim n\}$, tak np. $\mathcal{P}_0 \mathbb{V} = \{0\}$, $\mathcal{P}_1 \mathbb{V} = \{\{t\} \mid t = t\}$, $\mathcal{P}_2 \mathbb{V} = \{\{t, s\} \mid t \neq s\}$, ...

Zauważmy, że:

(28) $x \sim y \wedge a \in x \wedge b \in y \implies \exists\, f : x \hookrightarrow\!\!\!\!\rightarrow y\ (f(a) = b)$ $\quad\langle$HP: $\neg \ldots \exists)\, f : x \hookrightarrow\!\!\!\!\rightarrow y$.
Wówczas $g = (f \setminus \{a \mapsto f(a), f^{-1}(b) \mapsto b\}) \cup \{a \mapsto b, f^{-1}(b) \mapsto f(a)\} : x \hookrightarrow\!\!\!\!\rightarrow y$



oraz $g(a) = b$ ↯$\rangle$.

Z prawa (28) wynika analogon równoważności (27):

(29) $x \sim y \iff \operatorname{seq} x = \operatorname{seq} y$

$\langle$HP: $\operatorname{seq} x \sim \operatorname{seq} y$, $x \not\sim y$. $\exists)\, f : \operatorname{seq} x \hookrightarrow\!\!\!\!\rightarrow \operatorname{seq} y$, $f(x) = y$. Wówczas $f|x : x \hookrightarrow\!\!\!\!\rightarrow y$, a więc $x \sim y$ ↯$\rangle$.

A8 (*Aksjomat wyboru*, *Axiom of Choice*, AC)
$\varnothing \notin x \implies \exists\, f : x \longrightarrow \bigcup x\ \forall\, z \in x :\ f(z) \in z$
(f — *funkcja wyboru dla* x).

Do sformułowania w naturalny sposób aksjomatu nieskończoności potrzebna będzie definicja *uniwersum* (*klasy uniwersalnej*, *klasy teoriomnogościowo domkniętej*):
A — *uniwersum* $:\iff$ $A \subset \mathcal{P}A$ (tj. A — klasa tranzytywna) $\wedge\ \varnothing \in A \wedge \forall\, x, y \in A\ (\{x, y\}, \bigcup x, \mathcal{P}x \in A) \wedge \forall\, f : A \multimap A\ (\operatorname{Dom} f \in A \implies \operatorname{Im} f \in A)$.

Oczywiście: $\mathbb{V}$ — uniwersum. Oznaczmy:
Univ $:= \{u \mid u$ – uniwersum $\}$ (klasa wszystkich zbiorów uniwersalnych).

A9 (*Aksjomat nieskończoności*) Univ $\neq \varnothing$.
Z definicji klasy Univ natychmiast wynika, że $\varnothing \neq A \subset \mathrm{Univ} \implies \bigcap A \in \mathrm{Univ}$; stąd i z aksjomatu nieskończoności otrzymujemy, że $\bigcap \mathrm{Univ} \in \mathrm{Univ}$.
Zbiór $\bigcap \mathrm{Univ}$ jest najmniejszym uniwersum; nazywamy go *uniwersum zbiorów dziedzicznie skończonych*.

Wszystkie własności $\mathbb{V}$ wynikające z aksjomatów A1–A6 przenoszą się na dowolne uniwersum U — ich dowody są kopiami odpowiednich dowodów dla $\mathbb{V}$ — aksjomaty A7 i A8 również są — jak łatwo widać — spełnione w U, uniwersum U jest — jak to się mówi — modelem dla aksjomatyki A1–A8.

3.2. Tematy

1. Dane są klasy $A_1, \ldots, A_n \subset V$, gdzie V jest ustaloną klasą — zwyczajowo nazywamy ją *przestrzenią* — zaś n jest ustaloną niezerową liczbą naturalną.

Mówimy, że klasa $C \subset V$ jest *algebraiczna* (lub że jest wyrażeniem boole'owskim) ze względu na układ klas $A_1, \ldots, A_n$, jeżeli jest utworzona z klas $A_1, \ldots, A_n$ „w sposób boole'owski", to znaczy jedynie przy użyciu operacji $\cup$, $\cap$, $^\neg$, gdzie operacja $^\neg$ jest dopełnieniem w przestrzeni V, $C^\neg = V \setminus C$.

Bardziej dokładna definicja (w metajęzyku) jest indukcyjna:

1° Każda z klas $A_1, \ldots, A_n$ jest algebraiczna ze względu na układ klas $A_1, \ldots, A_n$ — w dalszym ciągu będziemy mówili krótko „algebraiczna", gdy wiadomo, jaki układ klas mamy na myśli.

2° Jeżeli klasy $C, D \subset V$ są algebraiczne, to klasy $C \cup D$ i $C^\neg = V \setminus C$ też są algebraiczne (warunek z iloczynem można opuścić, gdyż $C \cap D = (C^\neg \cup D^\neg)^\neg$). Podobnie $C \setminus D = C \cap D^\neg$.

3° Żadnych innych klas algebraicznych nie ma.

Jeśli szukamy klasy $X \subset V$ spełniającej układ równań

$$(*) \qquad \begin{cases} F_1 = G_1 \\ \cdots\cdots\cdots \\ F_m = G_m \end{cases},$$

gdzie $F_1, \ldots, F_m, G_1, \ldots, G_m$ są klasami (wyrażeniami boole'owskimi) algebraicznymi ze względu na układ $A_1, \ldots, A_n, X$, to możemy postępować w niżej opisany sposób:

1) Korzystając z równoważności

$$C = D \iff C \dot{-} D = \varnothing,$$

gdzie $C \dot{-} D$ jest różnicą symetryczną klas C i D; $C \dot{-} D = (C \setminus D) \cup (D \setminus C)$, możemy nasz układ zapisać w postaci:

$$\begin{cases} H_1 = \varnothing \\ \cdots\cdots\cdots \\ H_m = \varnothing \end{cases},$$

gdzie $H_1, \ldots, H_m$ są klasami algebraicznymi ze względu na układ $A_1, \ldots, A_n, X$.

2) Korzystając z równoważności

$$H_1 = \varnothing \wedge \cdots \wedge H_m = \varnothing \iff H_1 \cup \cdots \cup H_m = \varnothing$$

możemy nasz układ zapisać w postaci jednego równania: $H = \varnothing$ (H − klasa algebraiczna).

3) Stosując wprowadzone w poprzednim rozdziale składowe układu klas $A_1, \ldots, A_n, X$, znajdujemy równoważnik układu $(*)$ w postaci:

$$(C \cap X) \cup (D \cap X^\neg) = \varnothing,$$

gdzie klasy C, $D \subset V$ są algebraiczne ze względu na układ $A_1, \ldots, A_n$.

4) Równość z 3) jest równoważna koniunkcji

$$C \cap X = \varnothing \wedge D \cap X^\neg = \varnothing,$$

która z kolei jest równoważna podwójnej inkluzji:

$$(**) \qquad D \subset X \subset C^\neg.$$

Tak więc układ $(*)$ ma rozwiązanie — jak mówimy, jest *niesprzeczny* wtt (= wtedy i tylko wtedy), gdy spełniony jest warunek:

$$D \subset C^{\urcorner} = V \setminus C$$

i jeżeli tak jest, to rozwiązaniem układu $(*)$ jest każda klasa X spełniająca podwójną inkluzję $(**)$.

W praktyce często możemy rachunki uprościć na etapie 1). Przyrównując do $\varnothing$ składniki stałe w sumach mnogościowych $H_1, \ldots, H_n$ (po wprowadzeniu składowych) otrzymamy warunek konieczny (wk) niesprzeczności, który następnie wykorzystujemy.

Stosując tę metodę do klas $A, B, C \subset V$, wyznaczyć klasy $X \subset V$ spełniające układ równań:

$$(\diamond) \qquad \begin{cases} A \cap X = B \setminus X \\ C \cup X = X \setminus A. \end{cases}$$

Podać wkw niesprzeczności układu $(\diamond)$ i narysować odpowiedni diagram Venna.

2. Dane są klasy $A, B, C \subset V$.

Stosując metodę z zadania 1, rozwiązać dane układy równań. Szukamy klasy $X \subset V$.

Za każdym razem podać wkw istnienia rozwiązania i ewentualnie naszkicować diagram Venna.

$$(1) \quad \begin{cases} A \cup X = B \\ B \cup X = C \\ C \cup X = A \end{cases} \qquad (4) \quad \begin{cases} A \cap X = B \\ A \cup X = C \end{cases}$$

$$(2) \quad \begin{cases} A \cup X = V \setminus B \\ B \cup X = V \setminus C \\ C \cup X = V \setminus A \end{cases} \qquad (5) \quad \begin{cases} A \setminus X = B \\ X \setminus A = C. \end{cases}$$

$$(3) \quad \begin{cases} A \cap X = B \cap C \\ B \cap X = C \cap A \\ C \cap X = A \cap B \end{cases}$$

3. Dane są klasy $A, B, C, D \subset V$.

Rozwiązać układ równań

$$(*) \qquad \begin{cases} A \cap X = B \\ C \cap X = D \end{cases} \qquad (X \subset V).$$

Podać wkw niesprzeczności układu $(*)$ i narysować odpowiedni diagram Venna.

4. Dane są klasy $A, B \subset V$.

Scharakteryzować klasy $X \subset V$ takie, że:

$$A \cap B \cap X \neq \varnothing \wedge (A \cap B) \setminus X \neq \varnothing \wedge A \cap X \not\subset B \wedge B \cap X \not\subset A.$$

Narysować odpowiedni diagram Venna.

5*. W zadaniu 1 dla ustalonej klasy V (tzw. przestrzeń) i układu klas $A_1, \dots, A_n \subset V$ ($n = 1, 2, \dots$) określiliśmy niezbyt ściśle pojęcie klasy $C \subset V$ algebraicznej ze względu na dany układ. Definicja ścisła wymaga wprowadzenia (w metajęzyku oczywiście) *języka elementarnego algebry klas*. W języku tym symbolami pozalogicznymi mogą na przykład być: symbol stały $\varnothing$ dla zbioru pustego, symbol funkcyjny jednoargumentowy $^\urcorner$ na operację dopełnienia i dwa symbole funkcyjne dwuargumentowe $\cup$ i $\cap$.

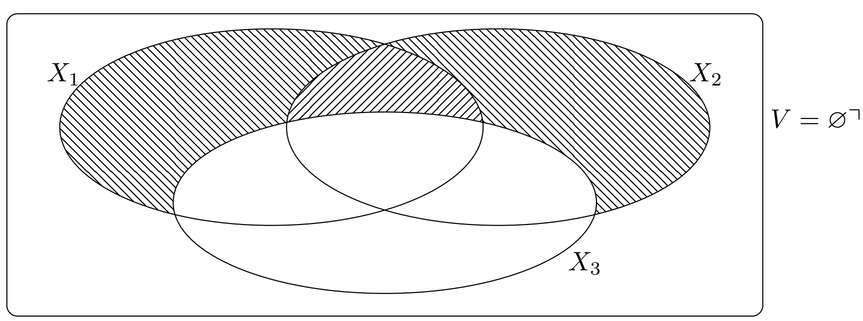
Termy (zwane też *wyrażeniami boole'owskimi*) to zmienne i symbol stały $\varnothing$ (traktowane jako słowa o długości 1) oraz słowa postaci $T^\urcorner$, $T \cup S$, $T \cap S$, gdzie T i S są termami o mniejszej złożoności (naśladujemy definicję indukcyjną z rozdziału 1). Formuły atomiczne są postaci $T = S$, gdzie T i S są termami.

Jako aksjomaty przyjmujemy aksjomaty równości (zwrotność, symetria, przechodniość oraz $X = Y \iff X^\urcorner = Y^\urcorner$ i analogiczne dwa zdania dla $\cup$ i $\cap$), a także odpowiednio dobrane prawa algebry klas (aksjomatyka algebry Boole'a — zob. rozdział 4, zadanie 35).

Przyjmujemy wszystkie powszechnie stosowane skróty i konwencje, w szczególności $T \setminus S = T \cap S^\urcorner$, $T \dot{-} S = (T \setminus S) \cup (S \setminus T)$.

W dalszym ciągu rozpatrujemy tylko te termy, w których mogą występować jedynie ustalone zmienne $X_1, \dots, X_n$. Oznaczmy: $X_i^0 = X_i$, $X_i^1 = X_i{}^\urcorner$. Term postaci $X_1^{\alpha_1} \cap \dots \cap X_n^{\alpha_n}$, gdzie $\alpha_1, \dots, \alpha_n = 0, 1$, nazywamy *elementarnym*. Termy normalne to term stały $\varnothing$ i termy postaci $U_1 \cup \dots \cup U_m$ ($m = 1, 2, \dots, 2^n$), gdzie $U_1, \dots, U_m$ są różnymi termami elementarnymi.

Dowodzimy (indukcja na złożoność termu), że dla każdego termu T istnieje term normalny U taki, że $T = U$ jest twierdzeniem, co notujemy $\vdash T = U$ (por. zadanie 5 o składowych z rozdziału 2); każdy taki term U nazywamy *postacią normalną* termu T. Na przykład dla $n = 3$ postacią normalną termu $T = (X_1 \cup X_2) \setminus X_3$ jest term $U = (X_1 \cap X_2 \cap X_3{}^\urcorner) \cup (X_1 \cap X_2{}^\urcorner \cap X_3{}^\urcorner) \cup (X_1{}^\urcorner \cap X_2 \cap X_3{}^\urcorner)$.



Dla ustalonej przestrzeni V i układu klas $A_1, \dots, A_n \subset V$ termowi $T = T(X_1, \dots, X_n)$ odpowiada klasa $T[A_1, \dots, A_n]_V \subset V$ zwana *wartością* termu T w przestrzeni V dla układu klas $A_1, \dots, A_n$. Przy ścisłej definicji operacji wartościowania — indukcja na złożoność termu T — termowi stałemu $\varnothing^\urcorner$ odpowiada klasa V.

Zachodzi tak zwane *twierdzenie o prawdzie*:
Dla dwóch termów T i S, jeżeli $\vdash T = S$, to $T[A_1, \dots, A_n]_V = S[A_1, \dots, A_n]_V$. ⟨Dowód indukcją na złożoność termów⟩.

Przyjmując powyższe definicje i fakty, udowodnić, że dla termu $T = T(X_1, \ldots, X_n)$ i pewnego niezależnego układu klas $A_1, \ldots, A_n \subset V$, jeżeli $T[A_1, \ldots, A_n]_V = \varnothing$ (każdą równość lub układ równości algebry klas można przedstawić równoważnie w tej postaci — por. zadanie 1), to dla dowolnej klasy W i układu klas $B_1, \ldots, B_n \subset W$ zachodzi równość $T[B_1, \ldots, B_n]_W = \varnothing$. Wynika stąd, że dla sprawdzenia, czy zachodzi jakaś tożsamość boole'owska, wystarczy narysować diagram Venna dla tych klas w położeniu ogólnym.

6. Przyjmując, że $x, y, z, t, \ldots$ są kolejnymi zmiennymi $\square, \square', \square'', \square''', \ldots$, wyznaczyć długość formuły „x–funkcja", to jest długość formuły

$$(x \subset \mathbb{V}^2 \wedge \forall y\, \forall z\, \forall t\, (((y, z) \in x \wedge (y, t) \in x) \implies z = t))$$

zapisanej wyłącznie symbolami języka $\mathrm{L}_{\mathrm{set}}$.

7. Zbadać zależność między klasami $A \cup B$ i $\bigcup\bigcup(A \times B)$ (A, B są dowolnymi klasami). Kiedy zachodzi równość?

8.

(a) Wykazać, że $A \neq \varnothing \neq B \wedge (A \times B) \cup (B \times A) = C \times D \implies A = B = C = D$.

(b) Uprościć wyrażenie $(C \times D) \circ (A \times B)$, rozpatrując przypadki: 1) $B \times C = \varnothing$, 2) $B \times C \neq \varnothing$.

9. Zbadać zależność między klasami $(A \setminus B) \cap (C \setminus D)$ i $(A \cap C) \setminus (B \cap D)$. Kiedy zachodzi równość? Podać możliwie najprostszy (tzw. minimalny) przykład inkluzji silnej.

10. Wykazać, że dla dowolnej klasy A:

(i) $\bigcup A \in \mathbb{V} \implies A \in \mathbb{V}$

(ii) $\mathcal{P}A \in \mathbb{V} \implies A \in \mathbb{V}$.

11. Dowieść, że:

(1) $A \times B = \varnothing \iff A = \varnothing \vee B = \varnothing$

(2) $A \times B = B \times A \iff A = B \vee A = \varnothing \vee B = \varnothing$

(3) $A \neq \varnothing \neq B \implies [A \times B \subset C \times D \iff A \subset C \wedge B \subset D]$

(4) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$

(5) $(A \cup B) \times (C \cup D) \supset (A \times C) \cup (B \times D)$

(6) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

(7) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.

12. Ustalić, który ze znaków $\subset$, $\supset$, $=$ należy wstawić w miejsce „?", aby otrzymać twierdzenie:

a) $(R \cup S)^{-1}$? $R^{-1} \cup S^{-1}$

b) $(R \cap S)^{-1}$? $R^{-1} \cap S^{-1}$

c) $(R^{\neg})^{-1}$? $(R^{-1})^{\neg}$

d) $T \circ (S \cup R)$? $(T \circ S) \cup (T \circ R)$

e) $T \circ (S \cap R)$? $(T \circ S) \cap (T \circ R)$

f) $T \circ (S \setminus R)$? $(T \circ S) \setminus (T \circ R)$.

13. Wykazać, że jeżeli $R \subset X \times Y$, $S \subset Y \times X$, $S \circ R = \mathrm{id}_X$, $R \circ S = \mathrm{id}_Y$, to $R : X \lhook\joinrel\longrightarrow\!\!\!\!\rightarrow Y$, $S : Y \lhook\joinrel\longrightarrow\!\!\!\!\rightarrow X$, $S = R^{-1}$.

14. Udowodnić twierdzenia (10)–(15) ze wstępu do tego rozdziału.

15. Niech $f : X \longrightarrow Y$; $A, B \subset X$; $C, D \subset Y$. Naszkicować dowody praw (16)–(25) ze wstępu. Udowodnić, że:

(a) $f^{-1} f f^{-1} C = f^{-1} C$
(b) $f f^{-1} f A = f A$
(c) $f(A \cap f^{-1} C) = f A \cap C$
(d) $f(A \setminus f^{-1} C) = f A \setminus C$.

16. Niech $f : X \longrightarrow Y$, $A \subset X$, $B \subset Y$. Wykazać, że:

(a) $f^{-1}(B \setminus f A) \subset f^{-1} B \setminus A$
(b) $f : X \lhook\joinrel\longrightarrow Y \implies f^{-1}(B \setminus f A) = f^{-1} B \setminus A$.

17. Wykazać, że:

$$f : X \longrightarrow\!\!\!\!\rightarrow X, f \circ f = f \implies f = \mathrm{id}_X .$$

Czy założenie surjektywności jest konieczne?

18. Wykazać, że:

(a) $(S \cap R) \circ T \subset (S \circ T) \cap (R \circ T)$
(b) $T : \mathbb{V} \multimap\!\!\!\!\rightarrow \mathbb{V} \implies (S \cap R) \circ T = (S \circ T) \cap (R \circ T)$
(c) $[T \subset \mathbb{V}^2 \wedge \forall\, R, S\ (S \cap R) \circ T = (S \circ T) \cap (R \circ T)] \implies T : \mathbb{V} \multimap\!\!\!\!\rightarrow \mathbb{V}$.

19. Wykazać, że dla funkcji częściowych $f : X \multimap\!\!\!\!\rightarrow Y$ i $g : Y \multimap\!\!\!\!\rightarrow Z$, jeżeli $g \circ f : X \longrightarrow Z$, to $f : X \longrightarrow Y$, ale niekoniecznie $g : Y \longrightarrow Z$.

20. Dane są zbiory A, B i funkcja $f : A \longrightarrow B$.
Określamy odwzorowanie:

$$\varphi = \{X \mapsto \mathrm{Im}(f|X) \mid X \subset A\} : \mathcal{P}A \longrightarrow \mathcal{P}B.$$

Wykazać, że:

(a) $\varphi : \mathcal{P}A \lhook\joinrel\longrightarrow \mathcal{P}B \iff f : A \lhook\joinrel\longrightarrow B$
(b) $\varphi : \mathcal{P}A \longrightarrow\!\!\!\!\rightarrow \mathcal{P}B \iff f : A \longrightarrow\!\!\!\!\rightarrow B$.

21. Dane są funkcje $X \xrightarrow{f} Y \xrightarrow{g} Z$.
Wykazać, że:

(a) $g \circ f : X \lhook\joinrel\longrightarrow Z \implies f : X \lhook\joinrel\longrightarrow Y$
(b) $g \circ f : X \longrightarrow\!\!\!\!\rightarrow Z \implies g : Y \longrightarrow\!\!\!\!\rightarrow Z$.

22. Dane są funkcje:

$$\begin{tikzcd} & Z \arrow[dl, "h"'] & \\ X \arrow[rr, "f"] & & Y \arrow[ul, "g"'] \end{tikzcd}$$

Wykazać, że jeżeli wszystkie trzy złożenia $h \circ g \circ f$, $g \circ f \circ h$, $f \circ h \circ g$ są injekcjami lub surjekcjami, przy czym jest wśród nich zarówno injekcja, jak i surjekcja, to funkcje f, g, h są bijekcjami. (Wskazówka: wykorzystać zadanie 21).

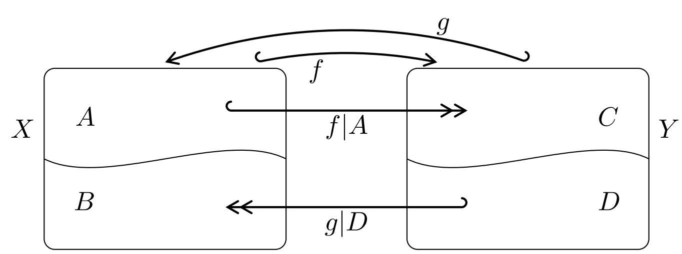
23. Używając liczb naturalnych jako parami różnych elementów, podać „minimalne" przykłady na inkluzje silne (znaku inkluzji nie można zastąpić znakiem równości) we wzorach:

(a) $T \circ (S \cap R) \subset (T \circ S) \cap (T \circ R)$

(b) $T \circ (S \setminus R) \subset (T \circ S) \setminus (T \circ R)$.

24*. Udowodnić *twierdzenie Cantora–Bernsteina* w wersji Tarskiego:

Dane są zbiory X, Y i dwie injekcje $f : X \hookrightarrow Y$, $g : Y \hookrightarrow X$. Istnieją wówczas zbiory A, B, C, D takie, że $A \cup B = X$, $A \cap B = \varnothing$, $C \cup D = Y$, $C \cap D = \varnothing$, $f(A) = C$, $g(D) = B$ (tak więc $(f|A) \cup (g|D)^{-1} : X \lhook\joinrel\twoheadrightarrow Y$).



Wskazówka: Gdybyśmy już mieli takie zbiory A, B, C, D, to jakie dwie własności miałby zbiór A? Wziąć rodzinę $\mathcal{M}$ wszystkich zbiorów $M \subset X$ o tych własnościach, i $A = \bigcap \mathcal{M}$.

Czy założenie injektywności funkcji f i g dałoby się osłabić?

25. Udowodnić *twierdzenie Cantora o zbiorze potęgowym*: $\forall\, X\ \neg\exists\, F : X \twoheadrightarrow \mathcal{P}X$. Wskazówka: w dowodzie nie wprost zastosować metodę przekątniową (rozdział 2, paradoks Russela), biorąc $A = \{x \in X \mid x \notin Fx\}$.

26. Udowodnić *prawo pełnej rozdzielności intersekcji względem unii*:

$$I, J \in \mathbb{V},\ A : I \times J \longrightarrow \mathbb{V} \implies \bigcap_{i \in I} \bigcup_{j \in J} A_{ij} = \bigcup_{\alpha \in \mathrm{Map}(I,J)} \bigcap_{i \in I} A_{i\alpha_i}.$$

Czy w dowodzie korzysta się z aksjomatu wyboru? Jeżeli tak, to w którym miejscu?

27. Czy dualne do prawa z 26. *prawo pełnej rozdzielności unii względem intersekcji*:

$$I, J \in \mathbb{V},\ A : I \times J \longrightarrow \mathbb{V} \implies \bigcup_{i \in I} \bigcap_{j \in J} A_{ij} = \bigcap_{\alpha \in \mathrm{Map}(I,J)} \bigcup_{i \in I} A_{i\alpha_i}$$

jest prawdziwe? Rola aksjomatu wyboru?

28. Dla ustalonego zbioru X rodzinę $\mathcal{A} \subset \mathcal{P}X$ nazywamy *algebrą* (*algebrą Boole'a*) *podzbiorów* X, gdy $\varnothing \in \mathcal{A} \wedge \forall\, A, B \in \mathcal{A} : A \cup B, A^{\neg} \in \mathcal{A}$ $(A^{\neg} = X \setminus A)$.
Oznaczmy przez $\operatorname{alg} X$ ogół algebr podzbiorów X; wówczas $\{\varnothing, X\}, \mathcal{P}X \in \operatorname{alg} X$ i $\forall\, \mathcal{A} \in \operatorname{alg} X : \{\varnothing, X\} \subset \mathcal{A} \subset \mathcal{P}X$, $\forall\, A, B \in \mathcal{A} : A \cap B, A \setminus B, A \dot{-} B \in \mathcal{A}$.

Udowodnić powyższe fakty.

Wyznaczyć $\operatorname{alg}\{1,2,3\}$ i $\operatorname{alg}\{1,2,3,4\}$.

Uogólnienie: $\operatorname{alg} I_n = ?$ $(n = 0, 1, 2, \ldots, I_n = \{1, \ldots, n\})$.
Wskazówka: Nazwiemy *atomem* algebry $\mathcal{A}$ minimalny względem inkluzji i niepusty zbiór $A \in \mathcal{A}$. Rozklasyfikować algebry w I_n ze względu na liczbę atomów.

29. Terminologia i oznaczenia — jak w zadaniu 28. Łatwo widać, że $\forall\, \varnothing \neq \alpha \subset \operatorname{alg} X : \bigcap \alpha \in \operatorname{alg} X$, a więc dla dowolnej rodziny $\mathcal{A} \subset \mathcal{P}X$:

$$\mathcal{A}^{-} := \bigcap \{\mathcal{B} \in \operatorname{alg} X \mid \ \mathcal{A} \subset \mathcal{B}\} \in \operatorname{alg} X \quad \langle \text{bo } \mathcal{P}X \in \operatorname{alg} X \rangle.$$

$\mathcal{A}^{-}$ nazywamy *algebrą generowaną przez rodzinę* $\mathcal{A}$.
Tak więc dla dowolnych $\mathcal{A}$, $\mathcal{B} \in \mathcal{P}X$:

(1) $\mathcal{A} \subset \mathcal{A}^{-} \in \operatorname{alg} X$
(2) $\mathcal{A} \subset \mathcal{B} \in \operatorname{alg} X \implies \mathcal{A}^{-} \subset \mathcal{B}$
(3) $\mathcal{A} \in \operatorname{alg} X \implies \mathcal{A}^{-} = \mathcal{A}$
(4) $\mathcal{A} \subset \mathcal{B} \implies \mathcal{A}^{-} \subset \mathcal{B}^{-}$
(5) $\mathcal{A}^{--} = \mathcal{A}^{-}$.

Dla trzech podzbiorów $A, B, C \subset X$ (ogólnie dla k podzbiorów, $k = 0, 1, 2, \ldots$) algebra generowana przez rodzinę $\mathcal{A} = \{A, B, C\}$ jest złożona ze wszystkich sum składowych utworzonych z tych trzech zbiorów (zob. zadanie 2.4*).

Udowodnić powyższe fakty.

Wyznaczyć $\mathcal{A}^{-}$ dla $A = \{\{1,2\}, \{1,3,4\}\} \subset \mathcal{P}I_4$.

30*. Dla dwu klas $\mathcal{A}, \mathcal{B}$ oznaczmy:

$$\mathcal{A} \mathbin{\bar{\times}} \mathcal{B} := \{A \times B \mid A \in \mathcal{A}, B \in \mathcal{B}\}.$$

Udowodnić *twierdzenie o redundancji* (*o zbyteczności*) (oznaczenia jak w zadaniu 29):

$$\forall\, X \in \mathcal{A} \subset \mathcal{P}X, Y \in \mathcal{B} \subset \mathcal{P}Y : (\mathcal{A}^{-} \mathbin{\bar{\times}} \mathcal{B}^{-})^{-} = (\mathcal{A} \mathbin{\bar{\times}} \mathcal{B})^{-}.$$

Wskazówka: dowód inkluzji „$\subset$" dwuetapowy:
Najpierw ustalamy zbiór $A \in \mathcal{A}$ i rozważamy rodzinę $\mathcal{G}_A = \{B \subset Y \mid A \times B \in (\mathcal{A} \mathbin{\bar{\times}} \mathcal{B})^{-}\}$, a następnie badamy analogiczną rodzinę dla $B \in \mathcal{B}^{-}$.

Jest to typowy schemat dowodu tego rodzaju twierdzeń.

31. Klasę A nazywamy *ekstensjonalną*, gdy spełniony jest w niej *aksjomat ekstensjonalności* A1, to znaczy

$$\forall\, x, y \in A\, [\forall\, z \in A\, (z \in x \iff z \in y) \implies x = y].$$

Udowodnić, że klasa tranzytywna jest ekstensjonalna.

Komentarz: Biorąc pod uwagę twierdzenie Mostowskiego o ściągnięciu (zob. rozdział 5, zadanie 78*) mówiące, że klasa ekstensjonalna jest w naturalny sposób „izomorficzna ze względu na przynależność" z pewną klasą tranzytywną, można w definicji uniwersum żądać tranzytywności zamiast ekstensjonalności.

Tak więc w dowolnym uniwersum U (w szczególności w $V_\omega = \bigcap \mathrm{Univ} = \{0, 1, 2, \ldots, \{1\}, \ldots\}$ — *uniwersum zbiorów dziedzicznie skończonych* — jest to najmniejsze uniwersum) są spełnione wszystkie aksjomaty A1–A8; mówimy też w takiej sytuacji, że U jest modelem dla systemu aksjomatów A1–A8, który oznaczamy ZFC_0 i nazywamy *absolutną teorią mnogości*.

3.3. Odpowiedzi

1. Używając notacji z zadania 2.2, możemy nasz układ zapisać w postaci

$$(\diamond) \qquad \begin{cases} AX = BX^\neg \\ C \cup X = A^\neg X. \end{cases}$$

Ponieważ $AXBX^\neg = \varnothing$, więc $AX \dot{-} BX^\neg = AX \cup BX^\neg$. Teraz $(C \cup X) \setminus (A^\neg X) = (C \cup X)(A^\neg X)^\neg = (C \cup X)(A \cup X^\neg) = AC \cup CX^\neg \cup AX = ACX \cup ACX^\neg \cup CX^\neg \cup AX = AX \cup CX^\neg$, natomiast $(A^\neg X) \setminus (C \cup X) = \varnothing$,
czyli $(C \cup X) \dot{-} A^\neg X = AX \cup CX^\neg$.
Zatem:

$$\begin{aligned} (\diamond) &\iff AX \cup BX^\neg \cup AX \cup CX^\neg = \varnothing \\ &\iff AX \cup (B \cup C)X^\neg = \varnothing \\ &\iff B \cup C \subset X \subset A^\neg. \end{aligned}$$

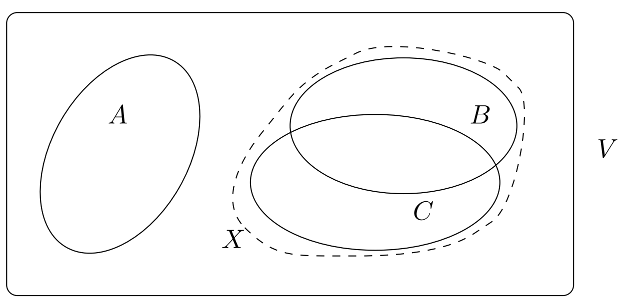
Tak więc układ $(\diamond)$ ma rozwiązanie wtt, gdy zachodzi warunek

$$B \cup C \subset V \setminus A$$

i wówczas rozwiązaniem jest każda klasa X spełniająca podwójną inkluzję:

$$B \cup C \subset X \subset V \setminus A.$$

Wynik ten można zilustrować diagramem Venna:



2. Zauważenie cykliczności w (1)–(3), $A \to B \to C \to A$, uprości rachunki.

(1) Układ ma rozwiązanie wtt, gdy $A = B = C$. Przy tym warunku rozwiązaniem jest dowolna klasa $X \subset A$.

(2) Rozwiązanie: $X = V$, przy warunku $A = B = C = \varnothing$.
(3) Warunek rozwiązalności (wkw):

$$(A \cap B) \setminus C = (B \cap C) \setminus A = (C \cap A) \setminus B = \varnothing.$$

Przy tym warunku rozwiązaniem układu jest każda klasa postaci $X = (A \cap B \cap C) \cup Z$, gdzie $Z \subset V \setminus (A \cup B \cup C)$ (zob. rysunek poniżej).

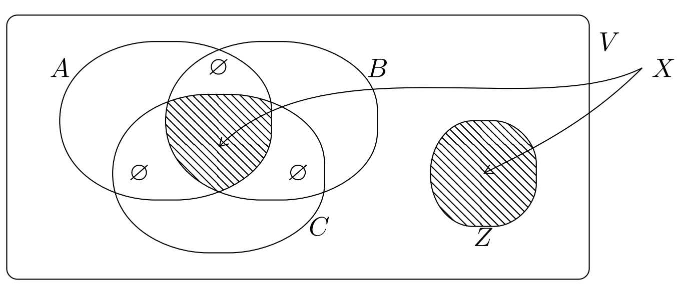
⟨W notacji z 1.:
$AX \setminus BC = AX(BC)^\neg = AX(B^\neg \cup C^\neg) = AB^\neg X \cup AC^\neg X$
$BC \setminus AX = BC(AX)^\neg = BC(A^\neg \cup X^\neg) = A^\neg BC \cup BCX^\neg = A^\neg BCX \cup A^\neg BCX^\neg \cup BCX^\neg = A^\neg BCX \cup BCX^\neg$, a więc
$AX \mathbin{\dot-} BC = (AB^\neg \cup AC^\neg \cup A^\neg BC)X \cup BCX^\neg$ i analogicznie
$BX \mathbin{\dot-} CA = (BC^\neg \cup BA^\neg \cup B^\neg CA)X \cup CAX^\neg$
$CX \mathbin{\dot-} AB = (CA^\neg \cup CB^\neg \cup C^\neg AB)X \cup ABX^\neg$.
Zatem:

$$\begin{aligned}
(3) \iff\ & [(A \mathbin{\dot-} B) \cup (B \mathbin{\dot-} C) \cup (C \mathbin{\dot-} A)]X \cup (AB \cup BC \cup CA)X^\neg = \varnothing \\
\iff\ & AB \cup BC \cup CA \subset X \subset [(A \mathbin{\dot-} B) \cup (B \mathbin{\dot-} C) \cup (C \mathbin{\dot-} A)]^\neg \\
& = (A \mathbin{\dot-} B)^\neg (B \mathbin{\dot-} C)^\neg (C \mathbin{\dot-} A)^\neg = (AB \cup A^\neg B^\neg)(BC \cup B^\neg C^\neg)(CA \cup C^\neg A^\neg) \\
& = A^\neg B^\neg C^\neg \cup ABC,
\end{aligned}$$

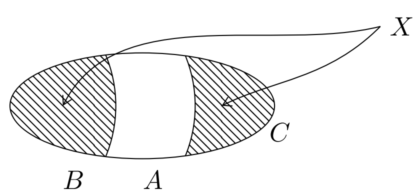
a więc

$$(3) \iff AB \cup AC \cup BC \subset X \subset ABC \cup A^\neg B^\neg C^\neg.$$

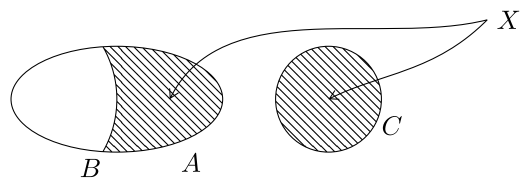
Ponieważ $(AB \cup AC \cup BC)A^\neg B^\neg C^\neg = \varnothing$, więc warunkiem koniecznym i wystarczającym (wkw) rozwiązalności układu (3) jest równość $AB \cup AC \cup BC = ABC$, czyli $AB \setminus C = AC \setminus B = BC \setminus A = \varnothing$, i wówczas $ABC \subset X \subset ABC \cup (A \cup B \cup C)^\neg$⟩.



(4) Wkw rozwiązalności: $B \subset A \subset C$, i jeśli tak jest, to $X = B \cup (C \setminus A)$.



(5) Wkw rozwiązalności: $B \subset A \wedge A \cap C = \varnothing$, i jeśli tak jest, to $X = (A \setminus B) \cup C$.



3. Układ jest niesprzeczny wtt, gdy

$$B \subset A \cap (C^\neg \cup D) \quad \wedge \quad D \subset C \cap (A^\neg \cup B).$$

Jeżeli ten warunek jest spełniony, to rozwiązaniem układu (*) jest każda klasa postaci:

$$X = B \cup D \cup Z, \text{ gdzie } Z \subset (A \cup C)^\neg.$$

$\langle AX \dot{-} B = AXB^\neg \cup (AX)^\neg B = AXB^\neg \cup (A^\neg \cup X^\neg)B = AB^\neg X \cup A^\neg B \cup X^\neg B = AB^\neg X \cup A^\neg BX \cup A^\neg BX^\neg \cup BX^\neg = (AB^\neg \cup A^\neg B)X \cup BX^\neg$, i analogicznie $CX \dot{-} D = (CD^\neg \cup C^\neg D)X \cup DX^\neg$. Zatem:

$$\begin{aligned}(*) \iff & (AB^\neg \cup A^\neg B \cup CD^\neg \cup C^\neg D)X \cup (B \cup D)X^\neg = \varnothing \\ \iff & B \cup D \subset X \subset [(A \dot{-} B) \cup (C \dot{-} D)]^\neg \\ & = (A \dot{-} B)^\neg (C \dot{-} D)^\neg = (AB \cup A^\neg B^\neg)(CD \cup C^\neg D^\neg).\end{aligned}$$

Ponieważ dla dowolnych klas A, B, C, D:

$$A \cup B \subset C \cap D \iff A \subset C \wedge A \subset D \wedge B \subset C \wedge B \subset D,$$

więc warunek rozwiązalności układu (*) można zapisać w postaci:
$B \subset A \wedge D \subset C \wedge B \subset D \cup C^\neg \wedge D \subset B \cup A^\neg$ lub równoważnie:

$$B \subset A \cap (C^\neg \cup D) \quad \wedge \quad D \subset C \cap (A^\neg \cup B).$$

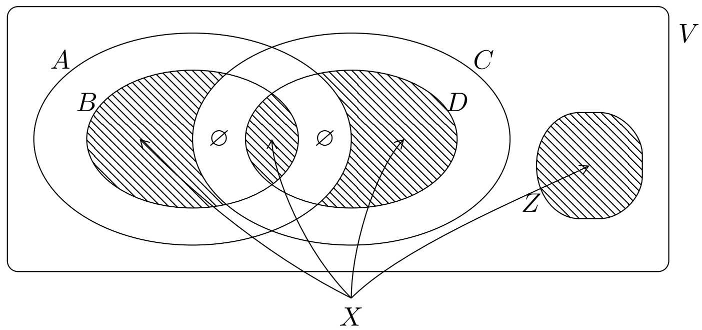
Jeśli ten warunek jest spełniony, to $(AB \cup A^\neg B^\neg)(CD \cup C^\neg D^\neg) = (A^\neg \cup B)(C^\neg \cup D)$, i rozwiązaniem układu (*) jest każda klasa X taka, że:

$$B \cup D \subset X \subset (A^\neg \cup B)(C^\neg \cup D).$$

Ponieważ

$$(A^\neg \cup B)(C^\neg \cup D) = (A \cup C)^\neg \cup A^\neg D \cup BC^\neg \cup BD \subset (A \cup C)^\neg \cup B \cup D,$$

więc rozwiązaniem układu (*) jest każda klasa postaci $X = B \cup D \cup Z$, gdzie $Z \subset (A \cup C)^{\neg}\rangle$.



4. Stosując uproszczoną notację z poprzednich zadań, dany warunek można zapisać w równoważnej postaci:

$$ABX \neq \varnothing \quad \wedge \quad ABX^{\neg} \neq \varnothing \quad \wedge \quad AX \setminus B \neq \varnothing \quad \wedge \quad BX \setminus A \neq \varnothing$$

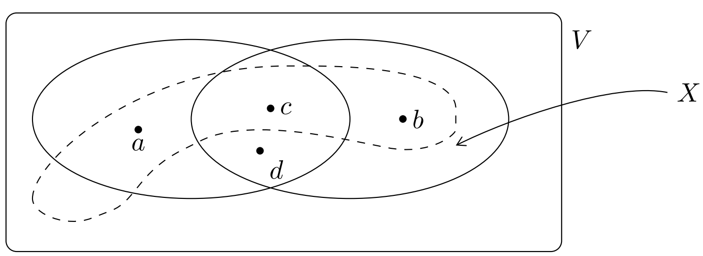
lub inaczej

(*) $$ABX \neq \varnothing \quad \wedge \quad ABX^{\neg} \neq \varnothing \quad \wedge \quad AB^{\neg}X \neq \varnothing \quad \wedge \quad A^{\neg}BX \neq \varnothing.$$

Zatem wkw istnienia klasy X spełniającej warunek (*) można zapisać w postaci:

$$\exists\, c, d \in A \cap B : c \neq d \quad \wedge \quad \exists\, a \in A \setminus B \quad \wedge \quad \exists\, b \in B \setminus A$$

i jeżeli tak jest, to warunek (*) spełnia każda klasa $\{a, b, c\} \subset X \subset V \setminus \{d\}$.



5*. Niech term U będzie postacią normalną termu T. Wówczas $\vdash T = U$, a więc według twierdzenia o prawdzie: $T[A_1, \ldots, A_n]_V = U[A_1, \ldots, A_n]_V$, czyli

$$U[A_1, \ldots, A_n] = \varnothing.$$

Gdyby term U był różny od termu $\varnothing$, to $U = (X_1^{\alpha_1} \cap \ldots \cap X_n^{\alpha_n}) \cup \ldots$, dla pewnego układu zerojedynkowych indeksów $\alpha_1, \ldots, \alpha_n$, i wówczas

$$U[A_1, \ldots, A_n]_V = (A_1^{\alpha_1} \cap \cdots \cap A_n^{\alpha_n}) \cup \ldots \neq \varnothing,$$

gdyż z niezależności układu $A_1, \ldots, A_n$ wynikałoby, że $A_1^{\alpha_1} \cap \ldots \cap A_n^{\alpha_n} \neq \varnothing$.

Zatem $U = \varnothing$, skąd — znów na mocy twierdzenia o prawdzie —

$$T[B_1, \ldots, B_n]_W = U[B_1, \ldots, B_n]_W = \varnothing.$$

6. 441
$\langle |x\text{–funkcja}| = |(x\text{–relacja} \wedge \forall\, y\, \forall\, z\, \forall\, t\, (((y,z) \in x \wedge (y,t) \in x) \;\Rightarrow\; z = t)))|$
$= |x\text{–relacja}| + 2|(y,z) \in x| + 18$
$|x\text{–relacja}| = |x \subset \mathbb{V}^2| = |\forall\, y\, (y \in x \;\Rightarrow\; y \in \mathbb{V}^2)| = |y \in \mathbb{V}^2| + 8$
$|y \in \mathbb{V}^2| = |y \in \{x \mid \exists\, y\, \exists\, z\, (y = y \wedge (z = z \wedge x = (y,z)))\}|$
$= |\exists\, x\, (y = x \wedge \exists\, y\, \exists\, z\, (y = y \wedge (z = z \wedge x = (y,z))))|$
$= |x = (y,z)| + 24$
$|x = (y,z)| = |\forall\, t\, (t \in x \iff t \in (y,z))| = |t \in (y,z)| + 8$
$|t \in (y,z)| = |t \in \{\{y\},\{y,z\}\}| = |(t \in \{\{y\}\} \vee t \in \{\{y,z\}\})|$
$= |t \in \{\{y\}\}| + |t \in \{\{y,z\}\}| + 3$
$|t \in \{\{y\}\}| = |(\{y\} \in \mathbb{V} \;\Rightarrow\; t = \{y\})| = |\{y\} \in \mathbb{V}| + |t = \{y\}| + 3$
$|\{y\} \in \mathbb{V}| = |\exists\, x\, (x = \{y\} \wedge x = x)| = |x = \{y\}| + 8$
$|x = \{y\}| = |\forall\, z\, (z \in X \iff (y = y \;\Rightarrow\; z = y))| = 17$
$|\{y\} \in \mathbb{V}| = 17 + 8 = 25$
$|t \in \{\{y\}\}| = 25 + 17 + 3 = 45.$
Analogicznie stwierdzamy, że $|(t \in \{\{y,z\}\}| = 69$, a więc:
$|t \in (y,z)| = 45 + 69 + 3 = 117$
$|x = (y,z)| = 117 + 8 = 125$
$|y \in \mathbb{V}^2| = 125 + 24 = 149$
$|x\text{–relacja}| = 149 + 8 = 157.$
Teraz $|(y,z) \in x| = |\exists\, t\, (t = (y,z) \wedge t \in x)| = |t = (y,z)| + 8 = 125 + 8 = 133$, a więc $|x\text{–funkcja}| = 157 + 2 \cdot 133 + 18 = 441\rangle$.

7.

$1^\circ)$ $\bigcup\bigcup(A \times B) \subset A \cup B$.
$\langle$Niech $x \in \bigcup\bigcup(A \times B)$. Wówczas $\exists)\, y,z : x \in y \in z \in A \times B$, $\exists)\, a \in A, b \in B : z = (a,b) = \{\{a\},\{a,b\}\}, y = \{a\} \vee y = \{a,b\}, x = a \vee x = b$, a więc $x \in A \cup B\rangle$.
$2^\circ)$ $\bigcup\bigcup(A \times B) = A \cup B \iff A \neq \varnothing \neq B \vee A = \varnothing = B$.
$\langle\Rightarrow)$ Nie wprost.
$\Leftarrow)$ Jeżeli $A \neq \varnothing \neq B$ i $x \in A \cup B$, to np. $x = a \in A$ i wówczas $\exists)\, b \in B : x \in \{a\} \in \{\{a\},\{a,b\}\} = (a,b) \in A \times B$, a więc $x \in \bigcup\bigcup(A \times B)\rangle$.

8.

(a) Jeżeli spełniony jest poprzednik tej implikacji, to $A \times B \neq \varnothing$, a więc $C \times D \neq \varnothing$, $C \neq \varnothing \neq D$. Teraz:

$C = D$ $\langle$gdyby np. $\exists)\, x \in C \setminus D$, to $\exists)\, y \in D : (x,y) \in C \times D$, $(x,y) \in (A \times B) \cup (B \times A)$, $(y,x) \in (A \times B) \cup (B \times A) = C \times D$, $x \in D$ ↯$\rangle$, i dalej $A = C$, $B = C$ $\langle$nie wprost — analogicznie$\rangle$.

(b) $(C \times D) \circ (A \times B) = \begin{cases} \varnothing, & \text{gdy } B \cap C = \varnothing \\ A \times D, & \text{gdy } B \cap C \neq \varnothing. \end{cases}$ Rachunki są mechaniczne.

Na przykład udowodnimy „$\supset$” w przypadku, gdy $B \cap C \neq \varnothing$.
Niech $(a,d) \in A \times D$. Wówczas $a \in A$, $d \in D$, $\exists)\, x \in B \cap C$, $x \in B$, $x \in C$, $(a,x) \in A \times B$, $(x,d) \in C \times D$, a więc $(a,d) \in (C \times D) \circ (A \times B)$.

Na tym przykładzie widać, jak prostsze byłyby rachunki i zapis, gdybyśmy w definicji złożenia (superpozycji) zachowali naturalny (tj. zgodny z przyjętym w cywilizacji europejskiej) kierunek „od lewej do prawej”, pisząc np. $R \odot S$ lub po prostu RS zamiast tradycyjnego zapisu: $S \circ R$.

9. Stosując uproszczoną notację z zadania 2.2 ($AB = A \cap B$, $A^{\neg} = \mathbb{V} \setminus A$) zapiszemy:
$L = (A \setminus B) \cap (C \setminus D) = AB^{\neg}CD^{\neg}$
$R = (A \cap C) \setminus (B \cap D) = AC(BD)^{\neg} = AC(B^{\neg} \cup D^{\neg})$
$= ACB^{\neg} \cup ACD^{\neg} = ACB^{\neg}(D \cup D^{\neg}) \cup ACD^{\neg}(B \cup B^{\neg})$
$= AB^{\neg}CD \cup AB^{\neg}CD^{\neg} \cup ABCD^{\neg}$.
Tak więc $L \subset R$, $L = R \iff AB^{\neg}CD \cup ABCD^{\neg} = \varnothing \iff AB^{\neg}C = ACD^{\neg} \iff ABC = ACD \iff (A \cap C) \cap B = (A \cap C) \cap D$.
Zatem $L \subsetneq R \iff (A \cap C) \cap B \neq (A \cap C) \cap D$.
Szukając najprostszego przykładu na inkluzję silną, można wziąć np. $A = B = C = \{0\}$, $D = \varnothing = 0$, i wówczas: $L = 0 \cap \{0\} = 0 \subsetneq R = \{0\} \setminus 0 = \{0\}$.
Uwaga:
Łatwo sprawdzić, że zachodzi równość:

$$(A \setminus B) \cap (C \setminus D) = (A \cap C) \setminus (B \cup D).$$

Nasza inkluzja natychmiast z niej wynika $\langle B \cap D \subset B \cup D \rangle$.

Jeśli chcemy znaleźć wkw równości $(A \cap C) \setminus (B \cup D) = (A \cap C) \setminus (B \cap D)$, można, oznaczając: $X = A \cap C$, $Y = B \cup D$, $Z = B \cap D$, poszukać wkw na równość $X \setminus Y = X \setminus Z$ przy warunku $Z \subset Y$. Rysując diagram Venna, otrzymamy warunek: $X \cap Y \subset Z$ lub równoważnie $X \cap (Y \setminus Z) = \varnothing$.

Wracając do zbiorów A, B, C, D, otrzymamy warunek konieczny i wystarczający równości

$$((A \cap C) \cap B) \cup (A \cap C) \cap D) \subset B \cap D$$

równoważny — jak łatwo sprawdzić — warunkowi:

$$(A \cap C) \cap B = (A \cap C) \cap D.$$

10.
(i) $A \subset \mathcal{P} \bigcup A \in \mathbb{V}$
(ii) $\{a \mapsto \{a\} \dots\} : A \hookrightarrow\!\!\!\!\rightarrow A' \subset \mathcal{P}A$.

11. Dowody są mechaniczne (z definicji). Na przykład dowód implikacji „$\Rightarrow$”, w (2):

HP: $A \neq B$, $A \neq \varnothing \neq B$. Np. $A \not\subset B$. Wówczas $\exists)\, a \in A \setminus B$, $\exists)\, b \in B, (a,b) \in A \times B = B \times A$, $a \in B$ ↯.

12. W a)–d) „=”, w e) „$\subset$”, w f) „$\supset$”.
⟨Udowodnimy np. inkluzję „$\supset$” w f).
HP $\exists)\, x, z : (x,z) \in T \circ S$, $(x,z) \notin T \circ R$, $(x,z) \notin T \circ (S \setminus R)$.
$\exists)\, y : (x,y) \in S, (y,z) \in T$. $(x,y) \notin R$ ⟨bo gdyby $(x,y) \in R$, to $(x,z) \in T \circ R$ ↯⟩.
Zatem $(x,y) \in S \setminus R$, $(x,z) \in T \circ (S \setminus R)$ ↯⟩.

13. Wystarczy wykazać, że $R : X \to Y$, $S : Y \to X$. Ze względu na symetrię sytuacji można ograniczyć się do R.

Należy wykazać, że:

1°) R – funkcja

2°) $\operatorname{Dom} R = X$.

Ad 1°) HP: $\exists\, x, y, z)\ xRy, xRz, y \neq z$. Wówczas $zR^{-1}x$, ale $R^{-1} \subset S$ $\quad\langle$HP: $\exists\, x, y)\ yR^{-1}x$, $\neg ySx$. xRy, $(y, y) \in \mathrm{id}_Y = R \circ S$, $\exists\, t)\ ySt, tRy$. $(x, t) \in S \circ R = \mathrm{id}_X$, $x = t$, ySx ↯$\rangle$, a więc zSx, $(z, y) \in R \circ S = \mathrm{id}_Y$, $y = z$ ↯.
Ad 2°) HP: $\exists)\, x \in X \setminus \operatorname{Dom} R$. $(x, x) \in \mathrm{id}_X = S \circ R$. $\exists\, y)\ xRy, ySz, x \in \operatorname{Dom} R$ ↯.

14. Dowody są bezproblemowe.
Udowodnimy np. (14), to jest twierdzenie o sklejaniu funkcji.
Niech $C \subset \mathrm{Map}^\circ(A, B)$.
Pierwszy człon koniunkcji:

$\Rightarrow$) HP: $\bigcup C = F : A \multimap\!\!\to B$ i $\exists)\, f, g \in C; x, y \in \operatorname{Dom} f \cap \operatorname{Dom} g : fx \neq gx$. $(x, fx) \in f \subset F$, $(x, gx) \in g \subset F$, $fx = gx$ ↯.

$\Leftarrow$) HP: $\ldots, \neg F : A \multimap\!\!\to B$. $\exists\, x, y, z : (x, y), (x, z) \in F$, $y \neq z$, $\exists)\, f, g \in C : (x, y) \in f$, $(x, z) \in g$. $y = fx = gx = z$ ↯.

Drugi człon koniunkcji: Zakładamy, że $F = \bigcup C = A \multimap\!\!\to B$.

$\subset$) HP: $\exists)\, x \in \operatorname{Dom} F : x \notin \bigcup\{\operatorname{Dom} f \mid f \in C\}$. $\exists\, y) : (x, y) \in F$. $\exists)\, f \in C : (x, y) \in f$. $x \in \operatorname{Dom} f$ ↯.

$\supset$) $\ldots$

15. Podobnie jak w zadaniu 14 dowody są niemal mechaniczne.
Udowodnimy na przykład (c):

$\subset$) $f(A \cap f^{-1}C) \subset fA \cap ff^{-1}C \subset fA \cap C$.

$\supset$) HP: $\exists)\, a \in A : fa \in C$, $fa \notin f(A \cap f^{-1}C)$.
$a \in f^{-1}C$, $a \in A \cap f^{-1}C$, $fa \in f(A \cap f^{-1}C)$ ↯.

16.

(a) HP: $\exists\, x) x \in f^{-1}(B \setminus fA)$, $x \notin f^{-1}B \setminus A$.
$fx \in B \setminus fA$, $fx \in B$, $x \in f^{-1}B$, $x \notin (f^{-1}B) \cap A^\neg$, $x \notin A^\neg$, $x \in A$, $fx \in fA$ ↯.
(b) HP: $f^{-1}B \setminus A \not\subset f^{-1}(B \setminus fA)$.
$\exists\, x)\ x \in f^{-1}B \setminus A$, $x \notin f^{-1}(B \setminus fA)$.
$fx \in B$, $x \notin A$, $fx \notin B \setminus fA = B \cap (fA)^\neg$.
$fx \notin (fA)^\neg$, $fx \in fA$, $\exists\, a \in A)\ fx = fa$, $x = a$ $\quad\langle$gdyż f jest injekcją$\rangle$, $x \in A$ ↯.

17. Hp: $\exists)\, x \in X, fx \neq x$. $\exists\, t \in X, x = ft$. $fft \neq x$, $(f \circ f)t \neq x$, $ft \neq x$ ↯. Założenie surjektywności jest konieczne.
Przykład: $X = \{0, 1\}$, $f = \{0 \mapsto 0, 1 \mapsto 0\} : X \to X$.

18.

(a) HP: $\exists)\, (x, y) \in (S \cap R) \circ T$, $(x, y) \notin (S \circ T) \cap (R \circ T)$.
$\exists\, z)\ (x, z) \in T, (z, y) \in S \cap R$; $(x, y) \in (S \circ T) \cap (R \circ T)$ ↯.
(b) HP: $(S \circ T) \cap (R \circ T) \not\subset (S \cap R) \circ T$.
$\exists)\, (x, z) \in (S \circ T) \cap (R \circ T), (x, z) \notin (S \cap R) \circ T$.

$\exists\, y, y')\ (x,y) \in T, (y,z) \in S, (x,y') \in T, (y',z) \in R$.
$y = y'$ $\langle$bo T jest funkcją$\rangle$, a więc $(y,z) \in S \cap R$, $(x,z) \in (S \cap R) \circ T$ ↯.
(c) HP: $\exists\, x, u, v)\ (x,u), (x,v) \in T, u \neq v$.
Niech $R = \{(u,x)\}$, $S = \{(v,x)\}$. Wówczas $(x,x) \in (S \circ T) \cap (R \circ T)$, a więc $(x,x) \in (S \cap R) \circ T$. $\exists\, w)\ (x,w) \in T$, $(w,x) \in S \cap R$, $w = u = v$ ↯.

19. $X = \mathrm{Dom}(g \circ f) \subset \mathrm{Dom}\, f \subset X$, a więc $\mathrm{Dom}\, f = X$, czyli $f : X \longrightarrow Y$.
Jeżeli $f : X \longrightarrow Y$ oraz $\mathrm{Im}\, f \subset \mathrm{Dom}\, g \subsetneq Y$, to $g \circ f : X \longrightarrow Z$ i $\neg g : Y \longrightarrow Z$. Tak będzie np., gdy $X = Y = Z = \{0,1\}$, $f = \{0 \mapsto 0, 1 \mapsto 0\}$, $g = \{0 \mapsto 0\}$.

20.

(a) Implikacje „$\Leftarrow$" wynikają z własności operacji obrazu i przeciwobrazu (prawa (23) i (25) ze Wstępu), gdyż $\forall\, X \subset A\ f^{-1} f X = X$, a więc ...
Implikacje „$\Rightarrow$":
HP: $\exists)\, a, c \in A : a \neq c \wedge f(a) = f(c)$. Wówczas $\varphi(\{a\}) = \{f(a)\} = \{f(c)\} = \varphi(\{c\})$, a więc $\{a\} = \{c\}$, $a = c$ ↯.
(b) Implikacja „$\Leftarrow$" — analogicznie jak w (a).
Implikacja „$\Rightarrow$":
HP: $\exists\, b)\ b \in B$, $b \notin \mathrm{Im}\, f$. Ponieważ $\{b\} \in \mathrm{Im}\, \varphi$, więc $\exists\, X \subset A)\ \{b\} = \varphi(X) = fX$, czyli $b \in fX \subset \mathrm{Im}\, f$ ↯.

21.

(a) HP: $\exists\, a, b \in X)\ a \neq b, f(a) = f(b)$.
Wówczas $g(f(a)) = g(f(b))$, $(g \circ f)(a) = (g \circ f)(b)$, $a = b$ ↯.
(b) HP: $\exists)\, z \in Z \setminus \mathrm{Im}\, g$.
Wówczas $z \in \mathrm{Im}(g \circ f)$, $\exists)\, x \in X : z = (g \circ f)(x) = g(f(x)) \in \mathrm{Im}\, g$ ↯.

22. Notujmy $fg := g \circ f$, $f_{\hookrightarrow} :\Leftrightarrow f : X \hookrightarrow Y$ itp.
W 21 udowodniliśmy, że $fg_{\hookrightarrow} \implies f_{\hookrightarrow}$, $fg_{\twoheadrightarrow} \implies g_{\twoheadrightarrow}$.
Możliwe są dwa przypadki:
(a) Dokładnie jedna z funkcji fgh, ghf, hfg jest injekcją.
Na przykład $fgh_{\hookrightarrow}$, $ghf_{\twoheadrightarrow}$, $hfg_{\twoheadrightarrow}$. Wówczas $f_{\hookrightarrow}$, $f_{\twoheadrightarrow}$, a więc $f_{\hookrightarrow\!\!\!\!\twoheadrightarrow}$. Również $fg_{\hookrightarrow}$, $fg_{\twoheadrightarrow}$, a więc $fg_{\hookrightarrow\!\!\!\!\twoheadrightarrow}$, $g = f^{-1} fg_{\hookrightarrow\!\!\!\!\twoheadrightarrow}$.
Wreszcie $h = (fg)^{-1} fgh_{\hookrightarrow}$, $h = hfg(fg)^{-1}{}_{\twoheadrightarrow}$, czyli $h_{\hookrightarrow\!\!\!\!\twoheadrightarrow}$.
(b) Dokładnie jedna z funkcji fgh, ghf, hfg jest surjekcją: Na przykład $fgh_{\twoheadrightarrow}$, $ghf_{\hookrightarrow}$, $hfg_{\hookrightarrow}$. Wówczas $h_{\twoheadrightarrow}$, $h_{\hookrightarrow}$, a więc $h_{\hookrightarrow\!\!\!\!\twoheadrightarrow}$. Również $gh_{\twoheadrightarrow}$, $gh_{\hookrightarrow}$, a więc $gh_{\hookrightarrow\!\!\!\!\twoheadrightarrow}$, $g = gh\, h^{-1}{}_{\hookrightarrow\!\!\!\!\twoheadrightarrow}$.
Wreszcie $f = fgh(gh)^{-1}{}_{\twoheadrightarrow}$, $f = (gh)^{-1} ghf_{\hookrightarrow}$, czyli $f_{\hookrightarrow\!\!\!\!\twoheadrightarrow}$.

23.

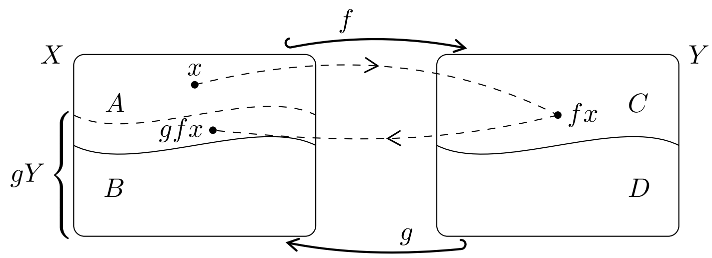
(a) Próbujemy dowodzić inkluzji „$\supset$" do momentu zablokowania (ogólna metoda!).
HP: $\exists)\ (x,y) \in (T \circ S) \cap (T \circ R)$, $(x,y) \notin T \circ (S \cap R)$.
$\exists\, z, t)\ (x,z) \in S$, $(z,y) \in T$, $(x,t) \in R$, $(t,y) \in T$. Jeżeli $z \neq t$, to sprzeczności nie otrzymujemy. Wystarczy więc wziąć $x = y = z = 0$, $t = 1$, czyli $R = \{(0,1)\}$, $S = \{(0,0)\}$, $T = \{(0,0),(1,0)\}$, i wówczas:

$$T \circ (S \cap R) = T \circ \varnothing = \varnothing \subsetneq (T \circ S) \cap (T \circ R) = \{(0,0)\}.$$

(b) Analogicznie. Przy tych samych R, S, T co w (a):

$$T \circ (R \setminus S) = T \circ R = \{(0,0)\} \supsetneq (T \circ R) \setminus (T \circ S) = \varnothing.$$

24*. Jeżeli A, B, C, D są takimi zbiorami, to $gfA \subset A$ oraz $X \setminus gY \subset A$ ($gfA = g(f(A))$ itp.).



Niech $\mathcal{M} = \{M \subset X \;\mid gfM \cup (X \setminus gY) \subset M\}$.
$\mathcal{M} \neq \varnothing$, gdyż $X \in \mathcal{M}$, zatem $A := \bigcap \mathcal{M} \subset X$.
Niech $C = fA$, $D = Y \setminus C$, $B = gD$.
Należy wykazać, że: 1°) $A \cup B = X$, 2°) $A \cap B = \varnothing$.

Ad 1°) HP: $\exists)\, x \in X \setminus (A \cup B)$.
Ponieważ $x \notin A$ i, jak łatwo sprawdzić, $A \in \mathcal{M}$, więc $x \in X \setminus A \subset gY$, $\exists)\, y \in Y : x = gy$. Ponieważ $x \notin B$, więc $y \notin D$, $y \in C$, $\exists)\, a \in A : y = fa$, skąd $x = gfa \in gfA \subset A$ $\lightning$. Zatem $A \cup B = X$.

Ad 2°) HP: $\exists)\, x \in A \cap B$.
$x \in B$, $\exists)\, y \in D : x = gy$; $y \notin C = fA$, więc $x \notin gfA$ $\langle$HP: $X \in gfA$. $\exists)\, z \in fA : x = gz$, $gy = gz$, $y = z$ $\langle$bo g jest injekcją$\rangle$, $y \in fA$ $\lightning\rangle$. Tak więc $x \notin M := gfA \cup (X \setminus B)$. Ale $M \in \mathcal{M}$ $\langle$Według 1°) $X \setminus B \subset A$; również $gfA \subset A$, czyli $M \subset A$, $gfM \subset gfA \subset M$. Ponadto $B = gD \subset gY$, więc $X \setminus gY \subset X \setminus B \subset M\rangle$, zatem $A \subset M$, skąd $x \in M$ $\lightning$.

Założenie injektywności obu funkcji f i g dałoby się osłabić do: *Jedna z funkcji f i g jest injekcją* $\langle$w powyższym dowodzie korzystaliśmy z injektywności funkcji g, ale sytuacja jest symetryczna względem funkcji f i $g\rangle$. Oczywiście uzyskujemy wtedy tylko surjekcję.

25. $\exists)\, a \in X : A = F_a$. $\forall\, x \in X : x \in F_a \Leftrightarrow x \notin F_x$. W szczególności $a \in F_a \Leftrightarrow a \notin F_a$ $\lightning$.

26. Dowód inkluzji: „$\supset$" jest automatyczny.
W dowodzie inkluzji „$\subset$" musimy skorzystać z aksjomatu wyboru: Jeżeli $x \in \bigcap_{i \in I} \bigcup_{j \in J} A_{ij}$, to $\forall\, i \in I\; \exists\, j \in J : x \in A_{ij}$, a więc $\forall\, i \in I : \{j \in J \mid x \in A_{ij}\} \neq \varnothing$.
Na mocy aksjomatu wyboru $\exists)\, f : \mathcal{P}J \setminus \{\varnothing\} \longrightarrow J\; \forall \varnothing \neq B \subset J : f(B) \in B$.
Określamy dla każdego takiego x funkcję $\alpha : I \longrightarrow J$, $\alpha_i = f(\{j \in J \mid\; x \in A_{ij}\})$; wówczas $\forall\, i \in I : x \in A_{i,\alpha_i}$, a więc $x \in \bigcup_{\alpha \in \mathrm{Map}(I,J)} \bigcap_{i \in I} A_{i\alpha_i}$.

27. Prawo dualne do prawa z 26. też jest prawdziwe. Aksjomat wyboru interweniuje w dowodzie inkluzji „$\supset$”.

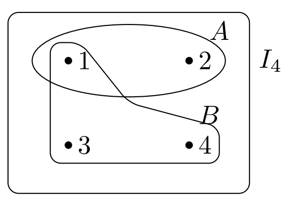
28. Dla $\mathcal{A} \in \operatorname{alg} X$: at A = *atomy* algebry $\mathcal{A} := \{A \in \mathcal{A} \mid A \neq \varnothing \wedge \forall B \in \mathcal{A}\ (B \subset A \Rightarrow B = \varnothing \vee B = A)\}$. Dla $X = I_4 = \{1,2,3,4\}$ (i ogólnie dla $X = I_n$) rodziny $\mathcal{A} \in \operatorname{alg} X$ rozklasyfikujemy według liczby k atomów:

$$\begin{array}{ll}
k=1) & \{\varnothing, I_4\} \\
k=2) & \left.\begin{array}{l}
\{\varnothing,\{1\},\{2,3,4\},I_4\} \\
\{\varnothing,\{2\},\{1,3,4\},I_4\} \\
\{\varnothing,\{3\},\{1,2,4\},I_4\} \\
\{\varnothing,\{4\},\{1,2,3\},I_4\} \\
\{\varnothing,\{1,2\},\{3,4\},I_4\} \\
\{\varnothing,\{1,3\},\{2,4\},I_4\} \\
\{\varnothing,\{1,4\},\{2,3\},I_4\}
\end{array}\right\} 7 \\
k=3) & \left.\begin{array}{l}
\{\varnothing,\{1\},\{2\},\{3,4\},\{1,2\},\{1,3,4\},\{2,3,4\},I_4\} \\
\ldots\ldots \\
\{\varnothing,\{3\},\{4\},\{1,2\},\{3,4\},\{1,2,3\},\{1,2,4\},I_4\}
\end{array}\right\} 6 \\
k=4) & \mathcal{P}I_4.
\end{array}$$

Ogółem $1+7+6+1 = 15$ algebr. Ogólnie algebry Boole'a na zbiorze I_n można utożsamiać z podziałami tego zbioru; jest ich więc B_n = n-ta liczba Bella (zob. rozdział 5 zadanie 45).

29. Dowody są bezproblemowe — w oparciu o definicje.

Chcąc znaleźć $\mathcal{A}^-$, wypisujemy wpierw wszystkie niepuste składowe układu zbiorów $A, B \subset I_4$, gdzie $A = \{1,2\}$, $B = \{1,3,4\}$.



Są to (oznaczenia z rozdziału 2, zadanie 4*): $A^0B^0 = \{1\}$, $A^0B^1 = \{2\}$, $A^1B^0 = \{3,4\}$ ($A^1B^1 = \varnothing$).
Zatem $\mathcal{A} = \{\varnothing, \{1\}, \{2\}, \{3,4\}, \{1,2\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}\}$.

30*. Dowód inkluzji „$\subset$”:

1) Dla ustalonego $A \in \mathcal{A}$ oznaczmy:

$$\mathcal{G}_A = \{B \subset Y \mid A \times B \in (\mathcal{A} \,\bar{\times}\, \mathcal{B})^-\}.$$

Sprawdzamy, że:

1°) $\mathcal{G}_A \in \operatorname{alg} Y$.
$\langle$Jeśli $B \in \mathcal{G}_A$, tzn. $B \subset Y$ i $A \times B \in (\mathcal{A} \,\bar{\times}\, \mathcal{B})^-$, to $B^\neg \in \mathcal{G}_A$, gdyż $A \times B^\neg = (A \times Y) \setminus (A \times B) \in (\mathcal{A} \,\bar{\times}\, \mathcal{B})^-, \ldots\rangle$.

2°) $\mathcal{B} \subset \mathcal{G}_A$ $\quad \langle$gdyż $\mathcal{A} \mathbin{\bar{\times}} \mathcal{B} \subset (\mathcal{A} \mathbin{\bar{\times}} \mathcal{B})^- \rangle$.
Zatem $\mathcal{B}^- \subset \mathcal{G}_A$, czyli:

$$\forall\, A \in \mathcal{A}, B \in \mathcal{B}^- : A \times B \in (\mathcal{A} \mathbin{\bar{\times}} \mathcal{B})^-.$$

2) Dla ustalonego $B \in \mathcal{B}^-$ oznaczmy:

$$\mathcal{H}_B = \{A \subset X \mid A \times B \in (\mathcal{A} \mathbin{\bar{\times}} \mathcal{B})^-\}.$$

I znów:

1°) $\mathcal{H}_B \in \operatorname{alg} X$
$\langle A \in \mathcal{H}_B \implies A^\neg \times B = (X \times B) \setminus (A \times B) \in (\mathcal{A} \mathbin{\bar{\times}} \mathcal{B})^- \ldots \rangle$.

2°) $\mathcal{A} \subset \mathcal{H}_B$ $\quad \langle$według 1)$\rangle$.
Zatem $\mathcal{A}^- \subset \mathcal{H}_B$, $\mathcal{A}^- \mathbin{\bar{\times}} \mathcal{B}^- \subset (\mathcal{A} \mathbin{\bar{\times}} \mathcal{B})^-$, a więc $(\mathcal{A}^- \mathbin{\bar{\times}} \mathcal{B}^-)^- \subset (\mathcal{A} \mathbin{\bar{\times}} \mathcal{B})^-$.

31. HP: $\exists)\, x, y \in A, \forall\, z \in A\ (z \in x \Leftrightarrow z \in y), x \neq y$.
Na przykład $x \not\subset y$. $\exists\, z) z \in x, z \notin y$.
Z tranzytywności klasy A wynika jednak, że $x \subset A$, skąd $z \in A$, ale dla takiego z: $z \in X \iff z \in Y$, a więc $z \in y$ ↯.

4

Relacje porządkujące, równoważności

4.1. Wstęp

W tym rozdziale będziemy rozpatrywać różne rodzaje relacji. Definicje — jak zwykle — sformułujemy dla dowolnych klas A, R,...

(1) R – *zwrotna* w A $:\Longleftrightarrow$ $\forall\, x \in A : x\; R\; x$

(2) R – *przechodnia* w A $:\Longleftrightarrow$ $\forall\, x, y, z \in A : x\; R\; y \wedge y\; R\; z \;\Rightarrow\; x\; R\; z$

(3) R – *symetryczna* w A $:\Longleftrightarrow$ $\forall\, x, y \in A : x\; R\; y \;\Rightarrow\; y\; R\; x$

(4) R – *antysymetryczna* w A $:\Longleftrightarrow$ $\forall\, x, y \in A : x\; R\; y \wedge y\; R\; x \;\Rightarrow\; x = y$

(5) R – *spójna* w A $:\Longleftrightarrow$ $\forall\, x, y \in A : x\; R\; y \vee y\; R\; x$

(6) R – *równoważność* w A $:\Longleftrightarrow$ $(1) \wedge (2) \wedge (3)$

(7) R – *porządek* w A $:\Longleftrightarrow$ $(1) \wedge (2) \wedge (4)$

(8) R – *porządek liniowy* w A $:\Longleftrightarrow$ $(1) \wedge (7) \wedge (5)$.

W sytuacji (7) mówimy też, że porządek jest *częściowy*.

Będziemy również używać notacji (głównie dla relacji będących porządkami) $x \underset{R}{\leqslant} y$ zamiast $x\; R\; y$ lub $(x, y) \in R$; opuszczając literę R, gdy z kontekstu wiadomo, o jaką relację chodzi; $x < y$ $:\Longleftrightarrow$ $x \leqslant y \wedge x \neq y$.

Podobnie będziemy opuszczać znak klasy, gdy wiadomo, w jakiej klasie daną relację rozpatrujemy. Jeżeli klasa A nie jest dana, to przyjmujemy: $A = \mathbb{V}$.

(9) a – *R-minimum* A $:\Longleftrightarrow$ $a \in A \wedge \forall\, x \in A : a \leqslant x$

(10) a – *R-maksimum* A $:\Longleftrightarrow$ $a \in A \wedge \forall\, x \in A : x \leqslant a$

(11) a – *element R-minimalny* A $:\Longleftrightarrow$ $a \in A \wedge \forall\, x \in A : \neg x < a$

(12) a – *element R-maksymalny* A $:\Longleftrightarrow$ $a \in A \wedge \forall\, x \in A : \neg a < x$

(13) B – *R-odcinek* A (lewy *R-odcinek* A) $:\Longleftrightarrow$ $B \subset A \wedge \forall\, x, y \in A : x \leqslant y \wedge y \in B \;\Rightarrow\; x \in B$

(14) $S_a(A, R) := \{x \in A \mid x \underset{R}{<} a\}$ – *segment*

(15) f – *R–S-rosnąca* $:\Longleftrightarrow$ $\forall\, x, z \in \operatorname{Dom} f : x \underset{R}{\leqslant} z \;\Rightarrow\; f(x) \underset{S}{\leqslant} f(z)$

(16) f – *R–S-silnie rosnąca* $:\Longleftrightarrow$ $\forall\, x, z \in \operatorname{Dom} f : x \underset{R}{<} z \;\Rightarrow\; f(x) \underset{S}{<} f(z)$.

Z powyższych definicji łatwo wynika, że:

(17) R – porządek w $A \wedge a$ – R-minimum $A \implies (b$ – element R-minimalny $A \Leftrightarrow b = a)$

(18) R – porządek liniowy w $A \implies (a$ – R-minimum $A \Leftrightarrow a$ – element R-minimalny $A)$

(19) R – porządek w $A \wedge a \in A \Rightarrow S_a(A,R)$ – R-odcinek A

(20) R – porządek liniowy w $A \wedge B$ – R-odcinek $A \wedge a$ – R-minimum $A \setminus B \Rightarrow B = S_a(A,R)$

(21) R – porządek w $A \wedge S$ – porządek w $B \wedge f : A \hookrightarrow B \wedge f$ – R–S-rosnąca $\implies f$ – R–S-silnie rosnąca

(22) R – porządek liniowy w $A \wedge S$ – porządek w $B \wedge f : A \to B \wedge f$ – R–S-rosnąca $\implies$ (f – R–S-silnie rosnąca $\Leftrightarrow f : A \hookrightarrow B$)

(23) R – porządek liniowy w $A \wedge S$ – porządek w $B \wedge f : A \hookrightarrow\!\!\!\!\rightarrow B \wedge f$ – R–S-rosnąca $\implies f^{-1}$ – S–R-rosnąca.

Dla zbioru X oznaczamy:

(24) $\operatorname{Equ} X := \{R \subset X^2 \mid R$ – równoważność w $X\}$

(25) $\operatorname{Part} X := \{\mathcal{A} \mid \bigcup \mathcal{A} = X \wedge \varnothing \notin \mathcal{A} \wedge \forall A, B \in \mathcal{A}\ (A \neq B \Rightarrow A \cap B = \varnothing)\}$ – *podziały* X

(26) Określamy *bijekcję kanoniczną* $\varphi : \operatorname{Equ} X \hookrightarrow\!\!\!\!\rightarrow \operatorname{Part} X$, kładąc dla $R \in \operatorname{Equ} X$: $\varphi(R) := \{[x]_R \mid x \in X\}$, gdzie dla $x \in R$: $[x]_R := \{y \mid x\ R\ y\}$ – *warstwa* x *względem* R.

⟨ 1) Określamy funkcję $\varphi : \operatorname{Equ} X \longrightarrow \operatorname{Part} X$ powyższym wzorem i sprawdzamy, że definicja ta jest poprawna, tzn. $\varphi(R) \in \operatorname{Part} X$ dla $R \in \operatorname{Equ} X$.
2) Określamy funkcję $\psi : \operatorname{Part} X \to \operatorname{Equ} X$, kładąc dla $\mathcal{A} \in \operatorname{Part} X$: $\psi(\mathcal{A}) = \{(x,y) \in X^2 : \exists A \in \mathcal{A} : x, y \in \mathcal{A}\}$. Sprawdzamy poprawność tej definicji.
3) Dowodzimy, że $\psi \circ \varphi \subset \mathrm{id}$, tzn. $\psi(\varphi(R)) = R$, dla $R \in \operatorname{Equ} X$.
4) Dowodzimy, że $\varphi \circ \psi \subset \mathrm{id}$, tzn. $\varphi(\psi(A)) = \mathcal{A}$, dla $\mathcal{A} \in \operatorname{Part} X$.

Z 1)–4) wynika, że $\varphi : \operatorname{Equ} X \hookrightarrow\!\!\!\!\rightarrow \operatorname{Part} X$, $\psi = \varphi^{-1}$⟩.

Dla $R \in \operatorname{Equ} X$ podział $\varphi(R)$ zbioru X nazywamy *zbiorem ilorazowym* (*ilorazem*) lub *faktorzbiorem* X przez R i oznaczamy X/R; mamy przy tym *surjekcję naturalną* $\operatorname{nat}_R : X \twoheadrightarrow X/R$, $\operatorname{nat}_R(x) = [x]_R$.

Mając dany zbiór X, porządek R w X i podzbiór $A \subset X$ oznaczamy:

(27) $m(A) := \{x \in X \mid \forall a \in A : x \leqslant a\}$ – *minoranty* A, dla $A = \{a, b\}$ piszemy $m(a,b)$ itp.

(28) $M(A) := \{x \in X \mid \forall a \in A : a \leqslant x\}$ - *majoranty* A

(29) $\min A := \bigcap\{a \mid a$ – R-minimum $A\}$ – *minimum* A

(30) $\max A := \bigcap\{a \mid a$ – R-maksimum $A\}$ – *maksimum* A

(31) $\sup A := \min M(A)$ – *supremum* A, *kres górny* A

(32) $\inf A := \max m(A)$ – *infimum* A, *kres dolny* A.

(33) Poniższe dwa warunki są równoważne:
   (a) $\forall A \subset X : \sup A \in X$
   (b) $\forall B \subset X : \inf B \in X$

$\langle$(a) $\Rightarrow$ (b) Niech $b = \sup m(B)$. Wówczas $b = \inf B$, gdyż

1°) $b \in m(B)$ $\quad\langle \forall\, x \in m(B)\ \forall\, y \in B : x \leqslant y$, a więc $B \subset M(m(B))$, $\forall\, y \in B : b \leqslant y\rangle$.

2°) $b = \max m(B)$ $\quad\langle \forall\, x \in m(B) : x \leqslant b\rangle$.

Dowód implikacji (b) $\Rightarrow$ (a) jest dualny$\rangle$.

(34) Porządek R w zbiorze X nazywamy *kratowym zupełnym*, gdy spełnia warunek (a) (lub (b)) z (33). Porządek R nazywamy *kratowym*, gdy $\forall\, a, b \in X : a \vee b := \sup\{a, b\} \in X$ i $a \wedge b := \inf\{a, b\} \in X$.

Oczywiście porządek liniowy jest porządkiem kratowym ($a \vee b = \max\{a, b\}$, $a \wedge b = \min\{a, b\}$); na odwrót niekoniecznie ($X = 4$, $R = id_X \cup \{(0,1), (0,2), (1,3), (2,3), (0,3)\}$).

(35) Parę (X, R), gdzie $X \in \mathbb{V}$, $R \subset X^2$ nazywamy:

(i) *zbiorem częściowo uporządkowanym*, lub *posetem* (od ang. *partially ordered set*), gdy R jest porządkiem w X

(ii) *zbiorem liniowo uporządkowanym* lub *łańcuchem*, gdy R jest porządkiem liniowym w X

(iii) *kratą*, gdy R jest porządkiem kratowym w X

(iv) *kratą zupełną*, gdy R jest porządkiem kratowym zupełnym w X.

Zamiast (X, R) piszemy zazwyczaj X i wtedy dla $a, b \in X$: $a \leqslant b$ oznacza $a \underset{R}{\leqslant} b$.

Dla kraty zupełnej X i podzbioru $A \subset X$ często piszemy zwyczajowo: $\bigvee A := \sup A$, $\bigwedge A := \inf A$ (dokładniej $\bigvee_X A = \inf_X A$ itp.).

Izomorfizmem posetu (X, R) na poset (Y, S) nazywamy każdą bijekcję $f : X \hookrightarrow\!\!\!\rightarrow Y$ taką, że f – R–S-rosnąca $\wedge f^{-1}$ – S–R-rosnąca (równoważnie: $\forall\, x, z \in X : x \underset{R}{\leqslant} z \iff f(x) \underset{S}{\leqslant} f(z)$); jeżeli taki izomorfizm istnieje, to mówimy, że posety są *izomorficzne*, lub też (zwyczajowo), że są *podobne*. Notacja: $(X, R) \simeq (Y, S)$, $f : (X, R) \xrightarrow{\sim} (Y, S)$.

Łatwo widać, że izomorfizm zachowuje wszystkie własności i pojęcia związane z posetami.

Poset (X, R^{-1}) nazywamy *dualnym* do posetu (X, R). Jeżeli te dwa posety są izomorficzne (podobne), to każdy z nich nazywamy *autodualnym*. Na przykład dla dowolnego zbioru X poset $(\mathcal{P}X, \subset)$ jest autodualny (odpowiednim izomorfizmem jest operacja dopełnienia $\{A \mapsto A^{\neg} = X \setminus A \mid A \subset X\}$): $(\mathcal{P}X, \subset) \xrightarrow{\sim} (\mathcal{P}X, \supset)$.

Jednym z najważniejszych pojęć w matematyce jest pojęcie *dobrego porządku*.

(36) R – dobry porządek w A $:\iff$ R – porządek liniowy w $A \wedge \forall\, Z\ (\varnothing \neq Z \subset A \Rightarrow \exists\, x$ – R-minimum $Z) \wedge \forall\, a \in A : S_a(A, R) \in \mathbb{V}$.

Trzeci warunek w koniunkcji stanowiącej definicję dobrego porządku wprowadzony został po to, aby spełniona była *zasada minimum*:

(37) R – dobry porządek w $A \wedge \varnothing \neq B \subset A \implies \exists\, x$ – R-minimum B.
$\langle$HP: $\neg \ldots \exists$) $a \in B$. $Z := B \cap S_a(A, R) \neq \varnothing$, $\exists\, x)$ x – R-minimum Z; wówczas x – R-minimum B $\lightning\rangle$.

Łatwo sprawdzić, że warunki występujące w definicji dobrego porządku można osłabić:

Kryterium Tarskiego:

(38) R – dobry porządek w $A \Leftrightarrow R$ – spójna w $A \wedge \forall\, Z\ (\varnothing \neq Z \subset A \ \Rightarrow\ \exists\, x$ – element R-minimalny $Z) \wedge \forall\, a \in A : S_a(A,R) \in \mathbb{V}$.
⟨Dla dowodu implikacji „$\Leftarrow$" wystarczy wykazać, że R jest porządkiem liniowym w A, HP: $\neg \ldots$ ↯⟩.

Często wykorzystywany jest poniższy *lemat o przesunięciu w prawo*:

(39) R – dobry porządek w $A \wedge B$ – R-odcinek $A \wedge f : B \hookrightarrow A \wedge f$ – R–R-silnie rosnąca $\implies \forall\, x \in B : x \leqslant f(x)$, (tu „$\leqslant$" oznacza oczywiście „$\underset{R}{\leqslant}$").
⟨HP: $\neg \ldots$ Zatem $C := \{x \in B \mid f(x) < x\} \neq \varnothing$, i według zasady minimum $\exists)\, c$ – R-minimum C. $c \in C$, $f(c) < c$, $f(f(c)) < f(c)$, $f(c) \in C$, $c \leqslant f(c)$ ⟨bo c – R-minimum C⟩ ↯⟩.

4.2. Tematy

1. Udowodnić prawa (17)-(23) i (26) ze Wstępu.

2. Dana jest klasa X i relacje $R \subset S \subset X^2$. Udowodnić, że:

1) R – spójna (w X) $\wedge$ S – antysymetryczna $\implies R = S$
2) R – symetryczna $\wedge$ S – antysymetryczna $\implies R$ – przechodnia
3) R – symetryczna $\iff R = R^{-1}$.

3. Udowodnić, że dla dwu relacji symetrycznych R i S zachodzi równoważność:

$$S \circ R \text{ – symetryczna} \iff S \circ R = R \circ S.$$

4. Dla zbioru n-elementowego $X = I_n$, gdzie $n = 0, 1, 2, \ldots$, relację $R \subset X^2$ możemy zobrazować *diagramem Hassego*: punkty zbioru przedstawiamy jako kropki, pary $(x, y) \in R$ jako strzałki od x do y.

Zilustrować diagramem Hassego dla $R \subset X^2$ (n, R możliwie najmniejsze), relację spełniającą warunki (w zbiorze X, np. $X = I_n$):

1) R – zwrotna $\wedge$ R – przechodnia $\wedge \neg R$ – symetryczna
2) R – zwrotna $\wedge$ R – symetryczna $\wedge \neg R$ – przechodnia
3) R – zwrotna $\wedge$ R – antysymetryczna $\wedge \neg R$ – przechodnia
4) R – antysymetryczna $\wedge$ R – przechodnia $\wedge \neg R$ – zwrotna
5) R – symetryczna $\wedge$ R – przechodnia $\wedge \neg R$ – zwrotna.

5. Określamy relację równoliczności zbiorów:

$$A \sim B \ :\iff\ \exists\, f : A \lhook\joinrel\twoheadrightarrow B.$$

Wykazać, że jest ona równoważnością w klasie pełnej $\mathbb{V}$. Udowodnić, że dla dowolnych zbiorów A, B, C:

(a) $\mathrm{Map}(A, B \times C) \sim \mathrm{Map}(A, B) \times \mathrm{Map}(A, C)$
(b) $\mathrm{Map}(A, \mathrm{Map}(B, C)) \sim \mathrm{Map}(A \times B, C)$

(c) $A \cap B = \varnothing \implies \mathrm{Map}(A \cup B, C) \sim \mathrm{Map}(A, C) \times \mathrm{Map}(B, C)$
(d) $\mathrm{Map}^{\circ}(A, B) \sim \mathrm{Map}(A, \operatorname{seq} B)$.

6. Ideałem na zbiorze X nazywamy każdy zbiór $\mathcal{I} \subset \mathcal{P}X$ taki, że:
1° $\varnothing \in \mathcal{I}$
2° $A,\, B \in \mathcal{I} \Rightarrow A \cup B \in \mathcal{I}$
3° $A \subset B \in \mathcal{I} \Rightarrow A \in \mathcal{I}$.

Intuicja: zbiory należące do ideału są „małe", „nieistotne". Na przykład może być $\mathcal{I} = \mathcal{P}Y$ dla pewnego $Y \subset X$; mówimy wówczas, że $\mathcal{I}$ jest *ideałem głównym generowanym przez* Y.
Dla ideału $\mathcal{I}$ na zbiorze X określamy w $\mathcal{P}X$ relację *przystawania modulo* $\mathcal{I}$:

$$A \equiv B \pmod{\mathcal{I}} \iff A \dot{-} B \in \mathcal{I}, \text{ gdzie } A \dot{-} B = (A \setminus B) \cup (B \setminus A).$$

Wykazać, że relacja ta jest równoważnością w $\mathcal{P}X$.

7. Pojęciem dualnym do pojęcia ideału jest pojęcie *filtru* na zbiorze X – jest to taki zbiór $F \subset \mathcal{P}X$, że:
1° $X \in \mathcal{F}$
2° $A,\, B \in \mathcal{F} \Rightarrow A \cap B \in \mathcal{F}$
3° $\mathcal{F} \ni B \subset A \subset X \Rightarrow A \in \mathcal{F}$.

Zredagować tekst odpowiadający „dualnie" wypowiedzi poprzedniego zadania. Zakończyć opisem relacji przystawania podzbiorów zbioru X modulo filtr.

Wskazać bijekcję kanoniczną zbioru $\alpha(X) = \{\mathcal{I} \mid \mathcal{I} - \text{ideał na } X\}$ na zbiór $\beta(X) = \{\mathcal{F} \mid \mathcal{F} - \text{filtr na } X\}$.

8. Dane są zbiory X, Y oraz filtr $\mathcal{F}$ na zbiorze X. Wykazać, że relacja $\underset{\mathcal{F}}{\equiv}$ w zbiorze $\mathrm{Map}(X, Y)$ określona wzorem:

$$f \underset{\mathcal{F}}{\equiv} g \;:\Longleftrightarrow\; \mathrm{Ker}(f, g) \in \mathcal{F},$$

gdzie $\mathrm{Ker}(f, g) = \{x \mid f(x) = g(x)\}$, jest równoważnością. Mówimy, że równoważność ta jest *indukowana* w zbiorze $\mathrm{Map}(X, Y)$ przez filtr $\mathcal{F}$ na zbiorze X.

9. Dany jest zbiór X i równoważności R, S w X.
(a) Czy prawdziwa jest równoważność:

$$S \circ R = X^2 \iff R = X^2 \vee S = X^2?$$

(b) Wykazać, że $S \circ R = X^2 \implies R \circ S = X^2$.

10. Udowodnić, że dla zbioru X i rownoważności R, S w X poniższe trzy warunki są równoważne:
(a) $R \subset S$
(b) $\forall \xi \in X/R \; \exists \eta \in X/S : \xi \subset \eta$
(c) $\forall \eta \in X/S : \eta = \bigcup\{\xi \in X/S \mid \xi \subset \eta\}$.

Dla podziałów $\mathcal{A}, \mathcal{B} \in \operatorname{Part} X$, $\mathcal{A} = X/R$, $\mathcal{B} = X/S$ mówimy, że $\mathcal{A}$ jest *słabszy* od $\mathcal{B}$ ($\mathcal{B}$ jest *silniejszy* od $\mathcal{A}$), gdy zachodzi jeden z tych trzech warunków.

W zbiorze $\operatorname{Part} X$ istnieje podział najsilniejszy $\{X\} = X/X^2$ i istnieje podział najsłabszy $\{\{x\} \mid x \in X\} = X/\mathrm{id}_X$. ($\mathrm{id}_X = \{(x,y) \in X^2 \mid x = y\}$).

O zbiorze $E \subset X$ mówimy, że jest wysycony ze względu na równoważność R, gdy $E = \bigcup\{\xi \in X/R \mid \xi \subset E\}$; tak więc warunek (c) oznacza, że każda warstwa równoważności S jest wysycona ze względu na R.

11. Dany jest zbiór X i odwzorowanie $f : X \longrightarrow \mathbb{V}$.

Równoważność $\ker f := \{(x,z) \in X^2 \mid f(x) = f(z)\}$ w zbiorze X nazywamy *jądrem* (kernel) odwzorowania f.

Udowodnić, że:

(i) $\exists!\, g : X/kerf \longrightarrow \mathbb{V}\ [f = g \circ \mathrm{nat}]$, gdzie $\mathrm{nat} = \mathrm{nat}_{\ker f} : X \twoheadrightarrow X/\ker f$.
(ii) Odwzorowanie g z (i) jest bijekcją zbioru $X/\ker f$ na zbiór $\operatorname{Im} f$; nazywany je bijekcją indukowaną przez f.
Diagram komutatywny

$$\begin{tikzcd} X \arrow[r, two heads, "f"] \arrow[d, two heads, "\mathrm{nat}"'] & \operatorname{Im} f \\ X/\ker f \arrow[ur, hook, two heads, "g"'] & \end{tikzcd}$$

nazywamy *rozkładem kanonicznym* odwzorowania f.

12. Dane są zbiory X, Y, odwzorowanie $f : X \longrightarrow Y$ i równoważność R w zbiorze X.
Wykazać, że:

$$(\exists\, h : X/R \longrightarrow Y\ [f = h \circ \mathrm{nat}_R]) \iff R \subset \ker f.$$

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, two heads, "\mathrm{nat}_R"'] & Y \\ X/R \arrow[ur, "h"'] & \end{tikzcd}$$

Inkluzję „$R \subset \ker f$” nazywamy *warunkiem faktoryzacji* odwzorowania f przez równoważność R; jeżeli ten warunek jest spełniony, to mówimy, że f *faktoryzuje się* przez R — o jednoznacznie wyznaczonym odwzorowaniu h mówimy, że jest *indukowane* przez f.

13. Dany jest zbiór X i równoważności R, S w X takie, że $R \subset S$. W tej sytuacji odwzorowanie $\mathrm{nat}_S : X \twoheadrightarrow X/S$ faktoryzuje się przez równoważność $R = \ker \mathrm{nat}_R$ (zadanie 12). Mamy więc jednoznacznie wyznaczone odwzorowanie $h : X/R \longrightarrow X/S$ takie, że $\mathrm{nat}_S = h \circ \mathrm{nat}_R$.

$$\begin{tikzcd} X \arrow[r, two heads, "\mathrm{nat}_S"] \arrow[d, two heads, "\mathrm{nat}_R"'] & X/S \\ X/R \arrow[ur, two heads, "h"'] \arrow[r, two heads, "\mathrm{nat}_{\ker h}"'] & (X/R)/\ker h \arrow[u, hook, two heads, "g"'] \end{tikzcd}$$

Oznaczmy przez g bijekcję indukowaną przez h (zadanie 11) i oznaczmy $S/R = \ker h$; tak więc:

$$g : (X/R)/(S/R) \hookrightarrow\!\!\!\!\rightarrow X/S.$$

W ten sposób dla ustalonej równoważności $R \in \operatorname{Equ} X$ uzyskaliśmy odwzorowanie

$$\varphi : \{S \in \operatorname{Equ} X \mid R \subset S\} \longrightarrow \operatorname{Equ}(X/R), \quad \varphi(S) = S/R.$$

Wykazać, że odwzorowanie φ jest bijekcją; jest to tzw. *bijekcja kanoniczna* (utożsamienie) zbioru $\{S \in \operatorname{Equ} X \mid R \subset S\}$ na zbiór $\operatorname{Equ}(X/R)$.

14. Dany jest zbiór X i relacja $R \subset X^2$. Wykazać, że:

(a) R – równoważność w $X \iff R \circ R = R = R^{-1} \wedge \mathrm{id}_X \subset R \iff R = (R \circ R^{-1}) \cup \mathrm{id}_X$

(b) R – porządek w $X \iff R \circ R \subset R \wedge R \cap R^{-1} = \mathrm{id}_X$

(c) R – funkcja ($R : X \multimap X$) $\iff R \circ R^{-1} \subset \mathrm{id}_X$

(d) R – injekcja ($R : X \hookrightarrow X$) $\iff (R \circ R^{-1}) \cup (R^{-1} \circ R) \subset \mathrm{id}_X$

(e) $R : X \twoheadrightarrow X \iff R \circ R^{-1} \subset \mathrm{id}_X \subset R^{-1} \circ R$

(f) $R : X \hookrightarrow\!\!\!\!\rightarrow X \iff R \circ R^{-1} = \mathrm{id}_X = R^{-1} \circ R$.

15. Dany jest zbiór X i równoważności $R,\ S \in \operatorname{Equ} X$. Wykazać, że:

(a) $R \cup S \in \operatorname{Equ} X \iff R \cup S = S \circ R$

(b) $R \cup S \in \operatorname{Equ} X \implies S \circ R = R \circ S = R \cup S$

(c) $S \circ R \in \operatorname{Equ} X \iff S \circ R = R \circ S$.

16. Ustalmy zbiór X. Ponieważ $X^2 = X \times X \in \operatorname{Equ} X$ oraz $\varnothing \neq \mathcal{R} \subset \operatorname{Equ} X \Rightarrow \bigcap \mathcal{R} \in \operatorname{Equ} X$ $\langle$bezpośredni wniosek z definicji równoważności w $X\rangle$, więc dla dowolnej relacji $R \subset X^2$ relacja $R^- := \bigcap\{S \in \operatorname{Equ} X \mid S \subset R\}$ jest najmniejszą równoważnością w X zawierającą R (tzn. $R^- \in \operatorname{Equ} X \wedge \forall\, S \in \operatorname{Equ} X\ [R \subset S \Rightarrow R^- \subset S]$); równoważność R^- nazywany *domknięciem równoważnościowym* relacji R w zbiorze X.

Łatwo widać, że dla $R,\ S \subset X^2$:

(i) $R \subset S \implies R^- \subset S^-$

(ii) $R \subset R^-$

(iii) $R^{--} = R^-$

(iv) $(R \cup S)^- \supset R^- \cup S^-$.

Wykazać, że:

$$R, S \in \operatorname{Equ} X \wedge S \circ R = R \circ S \implies (R \cup S)^- = S \circ R.$$

17. Sugerując się zadaniem 16, można sformułować dla ustalonego zbioru X dwie ogólne definicje:

(a) *Operacją domknięcia* w X nazywamy każdą funkcję $\varphi : \mathcal{P}X \longrightarrow \mathcal{P}X$ taką, że:

$$\forall\, A, B \subset X\ [A \subset B \Rightarrow \varphi A \subset \varphi B \wedge A \subset \varphi A \wedge \varphi\varphi A = \varphi A].$$

(b) *Rodziną zbiorów domkniętych* w X nazywamy każdą rodzinę $\mathcal{F} \subset \mathcal{P}X$ taką, że:

$$X \in \mathcal{F} \wedge \forall \varnothing \neq \mathcal{A} \subset \mathcal{F} : \bigcap \mathcal{A} \in \mathcal{F}.$$

Oznaczmy:

(a) $\alpha(X)$ = ogół operacji domknięcia w X

(b) $\beta(X)$ = ogół rodzin zbiorów domkniętych w X.

Wskazać — z uzasadnieniem — *bijekcję kanoniczną*

$$f : \alpha(X) \hookrightarrow\!\!\!\!\rightarrow \beta(X).$$

18. Dany jest zbiór X i odwzorowanie $\psi : \mathcal{P}X \longrightarrow \mathcal{P}X$. Określamy $\varphi : \mathcal{P}X \longrightarrow \mathcal{P}X$, kładąc dla $A \subset X$: $\varphi A = A \cup \psi A$. Wykazać, że φ jest operacją domknięcia w X wtw, gdy ψ spełnia warunek

(*) $$\forall\, A, B \subset X\ [A \subset B \cup \psi B \ \Rightarrow\ \psi A \subset B \cup \psi B].$$

19. Dla posetu X i elementów $a, b \in X$ oznaczamy:

$[a, b] := \{x \mid a \leqslant x \leqslant b\}$ – *przedział domknięty* od a do b

$(a, b) := \{x \mid a < x < b\}$ – *przedział otwarty* od a do b

$[a, b) := \{x \mid a \leqslant x < b\}$, $\quad (a, b] := \{x \mid a < x \leqslant b\}$

$[\,\cdot\,, a] := \{x \mid x \leqslant a\}$, $\quad [\,\cdot\,, a) = S_a(X) := \{x \mid x < a\}$

$[a, \cdot\,] := \{x \mid a \leqslant x\}$, $\quad [a, \cdot\,) := \{x \mid a < x\}$

(dokładniej: $[a, b]_X$ itp.).

Wykazać, że odwzorowanie $f : X \hookrightarrow \mathcal{P}X$, $f(a) = [\,\cdot\,, a]$ spełnia warunek:

(*) $$\forall\, a, b \in X : a \leqslant b \Leftrightarrow f(a) \subset f(b),$$

a więc odwzorowanie to jest izomorfizmem posetu X na poset $\{[\,\cdot\,, a] \mid a \in X\} \subset \mathcal{P}X$; mówimy w tej sytuacji, że f jest *włożeniem* posetu X w poset $(\mathcal{P}X, \subset)$.

Czy włożenie to zachowuje kresy, w tym sensie, że:

$$\forall\, a, b, c \in X \begin{pmatrix} a \vee b = c \ \Rightarrow\ [\,\cdot\,, a] \cup [\,\cdot\,, b] = [\,\cdot\,, c] \\ a \wedge b = c \ \Rightarrow\ [\,\cdot\,, a] \cap [\,\cdot\,, b] = [\,\cdot\,, c] \end{pmatrix}?$$

20. Poset n-elementowy X ($n = 0, 1, 2, \dots$) można określić diagramem Hassego *relacji pokrywania*:

$$a \prec b \ :\Longleftrightarrow\ a < b \wedge \neg\exists\, x \in X\ a < x < b.$$

Narysować takie diagramy dla wszystkich n-elementowych posetów nieizomorficznych, dla:

(a) $n = 3$

(b) $n = 4$.

Wskazówka: Klasyfikować najpierw według liczby składowych, a następnie według największej długości łańcucha.

Które z tych posetów są autodualne?

Wskazówka: Odwrócenie strzałek daje taki sam diagram.

21. Dla zbioru n-elementowego

$$X = I_n = \{1, 2, \dots, n\} \qquad (\text{dla } 0, 1, 2, \dots)$$

oznaczmy przez α_n liczbę w s z y s t k i c h porządków (częściowych) w X.

Początkowe wyrazy ciągu α_n są następujące:

n	0	1	2	3	4	5	6
α_n	1	1	3	19	219	4231	130023

(Sloane: oeis A 001035).

(i) Wykorzystując poprzednie zadanie 20, wypisać *explicite* wszystkie porządki w zbiorze $I_3 = \{1, 2, 3\}$.

(ii) Udowodnić, że wszystkie liczby α_n są nieparzyste.

Wskazówka: Określić odpowiednio relację równoważności w zbiorze

$$E = \{R \subset X^2 \mid R - \text{porządek w } X\}$$

wszystkich porządków (częściowych) w X $(= I_n)$.

22. Niech X, Y będą klasami (niekoniecznie zbiorami) $R \subset X \times Y$.
Dla $A \subset X$, $B \subset Y$ oznaczmy:

$$A^+ := \{y \in Y \mid \forall\, a \in A : a\ R\ y\}$$
$$B^- := \{x \in X \mid \forall\, b \in B : x\ R\ b\} \qquad \text{(Dualność!)}.$$

Wykazać, że:

(i) $A \subset C \subset X \implies A^+ \supset C^+$
$B \subset D \subset Y \implies B^- \supset D^-$

(ii) $A \subset X \implies A \subset A^{+-}$
$B \subset Y \implies B \subset B^{-+}$

(iii) $A \subset X \implies A^{+-+} = A^+$
$B \subset Y \implies B^{-+-} = B^-$.

Zatem dla $A, C \subset X$:

(i') $A \subset C \subset X \implies A^{+-} \supset C^{+-}$

(ii') $A \subset A^{+-}$

(iii') $A \subset X \implies A^{+-+-} = A^{+-}$.

Są to postulaty nałożone na operację domknięcia (zob. zadanie 17); klasę $A \subset X$ nazywamy *domkniętą*, gdy $A^{+-} = A$. Dualnie, klasę $B \subset Y$ nazywamy *domkniętą*, gdy $B^{-+} = B$.

Wykazać, że klasy domknięte w X są postaci B^- dla $B \subset Y$ i, dualnie, klasy domknięte w Y są postaci A^+ dla $A \subset X$. Jeżeli ograniczymy się do klas domkniętych $A \subset X$, $B \subset Y$, to odpowiedniość ta jest jedno-jednoznaczna (bijektywna), jest to tak zwana *odpowiedniość Galois* pomiędzy klasami domkniętymi w X i klasami domkniętymi w Y (nazwa ta ma swoje źródło w teorii Galois, zob. np. [**Browkin 68**]).

23. Dany jest poset X. Opisać odpowiedniość Galois odpowiadającą relacji porządku w X.
Dla $a \in X$ znaleźć odpowiedniki $(X \supset A \mapsto A^+, A^-, \dots)$ zbiorów: $\{a\}$, $[\,\cdot\,, a]$, $[a, \,\cdot\,]$.

24*. Pozostając przy oznaczeniach z zadań 21 i 22, rozważmy dla posetu X zbiór

$$\mathcal{F} = \{A \subset X \mid A^{+-} = A\} = \text{ ogół podzbiorów } (+-)\text{-domkniętych zbioru } X.$$

W szczególności $\mathcal{F} \supset \{[\,\cdot\,, a] \mid a \in X\}$.

Wykazać, że:

(a) poset $(\mathcal{F}, \subset)$ jest kratą zupełną

(b) injekcja $\varphi = \{a \mapsto [\,\cdot\,, a] \mid a \in x\} : X \hookrightarrow \mathcal{F}$ jest włożeniem X w $\mathcal{F}$ zachowującym kresy, tzn.:

1) $\forall\, a, b \in X : a \leqslant b \iff \varphi(a) \subset \varphi(b)$
2) $\forall_{\substack{A \subset X \\ c=\sup A \in X}} : \sup \varphi(A) = \varphi(c)$
3) $\forall_{\substack{A \subset X \\ d=\inf A \in X}} : \inf \varphi(A) = \varphi(d)$.

Kratę zupełną $\mathcal{F}$ nazywamy *rozszerzeniem minimalnym* posetu X (zob. [**Kuratowski... 78**, s. 160]).

25. Dany jest łańcuch (zbiór liniowo uporządkowany) i podzbiory $\varnothing \neq A \subset X$, $\varnothing \neq B \subset X$ takie, że $\sup A = \alpha \in X$ i $\sup B = \beta \in X$. Udowodnić równość:

$$\sup(A \cup B) = \max\{\sup A, \sup B\}.$$

26. Dane są kraty zupełne X, Y, podzbiór $A \subset X$ i odwzorowanie rosnące $f : X \to Y$.

Zbadać zależność między $f(\sup A)$ i $\sup f(A)$.

27. Dany jest poset X, zbiory A, B oraz funkcje $f : A \longrightarrow X$, $g : A \times B \longrightarrow X$.

Zakładamy, że:

(a) $\sup\limits_{a \in A} f(a) := \sup f(A) = \alpha \in X$

(Skróty, takie jak powyższy, będą w dalszym ciągu stale stosowane)

(b) $\forall\, a \in A : \sup\limits_{b \in B} g(a, b) = f(a)$.

Wykazać, że:

$$\sup_{(a,b) \in A \times B} g(a, b) = \alpha.$$

Komentarz: Wynik ten (i dualnie dla kresu dolnego) zwany *twierdzeniem o kresach iterowanych* zapisuje się krótko:

$$\sup_{(a,b) \in A \times B} g(a, b) = \sup_{a \in A} \sup_{b \in B} g(a, b)$$

przy założeniu, że prawa strona istnieje (tzn. jest elementem zbioru X).

28. Dana jest krata X (tzn. X jest posetem, w którym każdy dubleton ma kres górny i kres dolny). Dla $a, b \in X$ notujemy: $a \vee b = \sup\{a, b\}$, $a \wedge b = \inf\{a, b\}$. Udowodnić, że dla dowolnych $a, b, c \in X$:

(i) $(a \vee b) \vee c = a \vee (b \vee c)$
$(a \wedge b) \wedge c = a \wedge (b \wedge c)$ (*łączność, asocjatywność*)

(ii) $a \vee b = b \vee a$
$a \wedge b = b \wedge a$ (*przemienność, komutatywność*)

(iii) $a \vee a = a$
$a \wedge a = a$ (*idempotentność*)

(iv) $a \vee (a \wedge b) = a$
$a \wedge (a \vee b) = a$ *(absorpcja)*

(v) $a \wedge (b \vee c) \geqslant (a \wedge b) \vee (a \wedge c)$
$a \vee (b \wedge c) \leqslant (a \vee b) \wedge (a \vee c)$.

UWAGA: W (i)–(v) wystarczy udowodnić jedną z dwu przedstawionych zależności. Jest tak na mocy *zasady dualności* dla krat (ogólniej — dla posetów): jeżeli jakieś zdanie jest spełnione w każdej kracie, to *zdanie dualne*, otrzymane przez wymianę $\leqslant \leftrightarrow \geqslant$, $\vee \leftrightarrow \wedge$, też ma tę własność.

29. *Kratą* nazywany również zbiór X wraz z działaniami $\vee, \wedge : X^2 \to X$ spełniającymi postulaty (i), (ii), (iv) z zadania 28, gdyż w tej sytuacji relacja $\leqslant$ w zbiorze X określona wzorem $a \leqslant b \;:\Longleftrightarrow\; a \vee b = b$ (lub $a \leqslant b \;:\Longleftrightarrow\; a \wedge b = a$) jest porządkiem kratowym i przejścia:

$$(X, \leqslant) \rightleftarrows (X, \vee, \wedge)$$

są *zgodne*, to znaczy:

1°) $(X, \leqslant) \longmapsto (X, \vee, \wedge) \longmapsto (X, \leqslant') = (X, \leqslant)$

2°) $(X, \vee, \wedge) \longmapsto (X, \leqslant) \longmapsto (X, \vee', \wedge') = (X, \vee, \wedge)$.

Udowodnić te zależności.

30. Dany jest zbiór X wraz z działaniem $\vee : X^2 \to X$ spełniającym postulaty (i), (ii), (iii) z zadania 28, to jest łącznym, przemiennym i idempotentnym; obiekt taki nazywamy *półgrupą przemienną idempotentną*.

Wykazać, że:

(a) Relacja $\leqslant$ w zbiorze X określona wzorem $a \leqslant b \;:\Longleftrightarrow\; a \vee b = b$ jest porządkiem (częściowym), przy którym każdy dubleton $\{a, b\}$ ma kres górny równy $a \vee b$; taki poset $(X, \leqslant)$ nazywamy *półkratą górną*.

(b) Jeżeli w półkracie górnej X określimy działanie $\vee : X^2 \to X$, kładąc $a \vee b = \sup\{a, b\}$, to otrzymamy półgrupę przemienną idempotentną $(X, \vee)$.

(c) Opisane w punktach (a), (b) przejścia są zgodne, to znaczy:

1°) $(X, \leqslant) \longmapsto (X, \vee) \longmapsto (X, \leqslant') = (X, \leqslant)$

2°) $(X, \vee) \longmapsto (X, \leqslant) \longmapsto (X, \vee') = (X, \vee)$.

KOMENTARZ: Dualnie półgrupę przemienną idempotentną można identyfikować z *półkratą dolną* ($a \wedge b = \inf\{a, b\}$, $a \leqslant b \iff a \wedge b = a$), a także z półkratą górną. Takie zależności „strukturalne” zostaną dokładniej opisane w rozdziale 8.

31*. Udowodnić, że zbiór X wraz z działaniami $\vee, \wedge : X^2 \to X$ jest kratą w sensie zadania 29, tzn. spełnione są warunki (i), (ii), (iv) łączności, przemienności i absorpcji wtt, gdy:

(1) $(b \wedge a) \vee a = a$

(2) $(((a \wedge b) \wedge c) \vee d) \vee e = (((b \wedge c) \wedge a) \vee e) \vee ((f \vee d) \wedge d)$, dla wszystkich $a, b, c, d, e, f \in X$.

KOMENTARZ: Wynik ten podał J. A. Kalman w artykule *A two axion definition for lattices*, Rev. Roumaine Math. Pures Appl. 13, 1968, pp. 669–670.

W roku 1970 R. N. McKenzie (Math. Scand 27, pp. 24–38) pokazał, że istnieje jedna identyczność charakteryzująca kraty — ma ona kilka tysięcy zmiennych.

Natomiast A. Tarski (Contributions to Math. Logic, Amsterdam, 1968, pp. 275–288) udowodnił, że dla każdego $n \geqslant 1$ istnieje niezależny n-elementowy zbiór identyczności charakteryzujący kraty (niezależny — tzn. żadna identyczność nie może być opuszczona — dla każdej identyczności z tego zbioru istnieje obiekt $(X, \vee, \wedge)$, w którym są spełnione wszystkie identyczności z danego zbioru, z wyjątkiem tej jednej).

32. Udowodnić, że dla kraty X równoważne są poniższe dwa warunki:

(1) $\forall\, a, b, c \in X : a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

(2) $\forall\, a, b, c \in X : a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Kratę spełniającą te warunki nazywamy *dystrybutywną*.

33. Dla dowolnej kraty X i elementów $a, b \in X$ takich, że $a \leqslant b$, określamy dwa odwzorowania $\alpha, \beta : X \to X$, kładąc dla $x \in X$:

$$\alpha(x) = a \vee (x \wedge b), \qquad \beta(x) = (a \vee x) \wedge b.$$

Udowodnić, że dla $x \in X$:

(1) $a \leqslant \alpha(x) \leqslant \beta(x) \leqslant b$

(2) $a \leqslant x \leqslant b \implies \alpha(x) = \beta(x) = x$.

Odwzorowania α i β nazywamy odpowiednio *rzutowaniem dolnym* i *rzutowaniem górnym* kraty X na przedział $[a, b]$; jeżeli $\alpha = \beta$, to przedział $[a, b]$ nazywamy *reqularnym*. Kratę X nazywamy *modularną*, jeśli w niej każdy niepusty przedział domknięty jest regularny. Tak więc:

$$X \text{ – modularna } \Leftrightarrow \underset{a \leqslant b}{\forall\, a, b, x \in X} : a \vee (x \wedge b) = (a \vee x) \wedge b.$$

34. Udowodnić, że dla kraty X zachodzi równoważność:

$$X \text{ – modularna } \iff \forall\, a, b, x \in X : (a \wedge b) \vee (x \wedge b) = ((a \wedge b) \vee x) \wedge b.$$

35. Narysować diagramy wszystkich n-elementowych krat nieizomorficznych dla $n \leqslant 5$ (por. zadanie 20). Które z tych krat są autodualne?

36. Ile jest nieizomorficznych krat 6-elementowych?
Wskazówka: dodawać elementy 0 (najmniejszy) i 1 (największy) do 4-elementowych posetów z zadania 20.

37. Udowodnić, że krata dystrybutywna jest modularna.
Podać przykłady:

(a) 5-elementowej kraty modularnej i niedystrybutywnej

(b) 5-elementowej kraty niemodularnej.

38. Dla kraty X i elementów $a, b, c \in X$ mówimy, że element $x \in X$ jest (b, c)-*dopełnieniem* elementu a, jeżeli $a \wedge x = b$, $a \vee x = c$.

Udowodnić, że:

(a) W kracie dystrybutywnej X zachodzi *prawo dopełnień*, które mówi, że jeżeli $a, b, c \in X$ i element a ma (b, c)-dopełnienie, to jest ono wyznaczone jednoznacznie.

(b) Jeżeli krata X jest modularna, $a, b, c \in X$, elementy $x, y \in X$ są (b, c)-dopełnieniami elementu a i elementy te są *porównywalne* (tzn. $x \leqslant y \vee y \leqslant x$), to $x = y$.

39. W kracie X elementy zbioru:

$$A = \{a \in X \mid \forall\, x, y \in X\ [a = x \vee y \ \Rightarrow\ a = x \vee a = y]\}$$

nazywamy *nieprzywiedlnymi*.
Wykazać, że dla kraty dystrybutywnej:

$$a \in A \iff \forall\, x, y \in X\ [a \leqslant x \vee y \ \Rightarrow\ a \leqslant x \vee a \leqslant y].$$

40. Jeżeli krata X jest *ograniczona*, tzn. ma element największy $1 = 1_X := \max X$ i element najmniejszy $0 = 0_X := \min_X$, to dla $a \in X$ *dopełnieniem* elementu a nazywamy $(0,1)$-dopełnienie tego elementu (zob. zadanie 39), czyli taki element $x \in X$, że $a \wedge x = 0$ i $a \vee x = 1$; przy dodatkowym założeniu, że krata X jest dystrybutywna, taki element, jeżeli istnieje, to istnieje dokładnie jeden — oznaczamy go $a^{\neg}$; mamy więc: $a \wedge a^{\neg} = 0$, $a \vee a^{\neg} = 1$.

Mówimy, że krata ograniczona X jest *z dopełnieniami*, jeśli każdy element $a \in X$ ma w niej dopełnienie.

Algebrą Boole'a nazywamy kratę ograniczoną X, dystrybutywną i z dopełnieniami. Porządek $\leqslant$ w X nazywamy wówczas *boole'owskim*.

Algebrą Boole'a nazywamy również (analogicznie jak dla krat — por. zadanie 29) zbiór X wraz z działaniami: $\vee, \wedge : X^2 \to X$, $\ ^{\neg} : X \to X$, $0, 1 \in X$, takimi, że dla $a, b, c \in X$:

(1) $(a \vee b) \vee c = a \vee (b \vee c), \quad (a \wedge b) \wedge c = a \wedge (b \wedge c)$

(2) $a \vee b = b \vee a, \quad a \wedge b = b \wedge a$

(3) $a \vee (a \wedge b) = a, \quad a \wedge (a \vee b) = a$

(4) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c), \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

(5) $a \vee 0 = a, \quad a \wedge 1 = a$

(6) $a \vee a^{\neg} = 1, \quad a \wedge a^{\neg} = 0,$

gdyż w tej sytuacji relacja $\leqslant$ w X określona wzorem $a \leqslant b \ :\iff\ a \vee b = b$ (lub $a \leqslant b \ :\iff\ a \wedge b = a$) jest porządkiem boole'owskim i przejścia:

$$(X, \leqslant) \rightleftarrows (X, \vee, \wedge, ^{\neg}, 0, 1)$$

są *zgodne*, w tym sensie, że:

1°) $(X, \leqslant) \longmapsto (X, \vee, \wedge, ^{\neg}, 0, 1) \longmapsto (X, \dot{\leqslant}) = (X, \leqslant)$

2°) $(X, \vee, \wedge, ^{\neg}, 0, 1) \longmapsto (X, \leqslant) \longmapsto (X, \dot{\vee}, \dot{\wedge}, \dot{^{\neg}}, \dot{0}, \dot{1}) = (X, \vee, \wedge, ^{\neg}, 0, 1).$

Udowodnić te zależności.

41. Udowodnić, że w algebrze Boole'a X spełnione są prawa de Morgana:

$$(a \vee b)^{\neg} = a^{\neg} \wedge b^{\neg}, \quad (a \wedge b)^{\neg} = a^{\neg} \vee b^{\neg} \qquad \text{dla } a, b \in X.$$

Ponadto:

(*) $$a^{\neg\neg} = a, \qquad a \leqslant b \iff b^{\neg} \leqslant a^{\neg}.$$

42. Udowodnić, że dla zbioru X relacja inkluzji jest:

(a) porządkiem boole'owskim zupełnym w $\mathcal{P}X$

(b) porządkiem kratowym zupełnym w $\operatorname{Equ} X$

(c) porządkiem kratowym zupełnym w $\mathcal{E} = \mathcal{E}_\Phi = \{E \subset X \mid \forall \varphi \in \Phi : \varphi(E) \subset E\}$, przy ustalonym zbiorze odwzorowań $\Phi \subset \operatorname{Map}(X, X)$.

W każdym z tych trzech przypadków wskazać kres dolny i kres górny podzbioru.

43. *Twierdzenie Tarskiego o punkcie stałym*:

Odwzorowanie rosnące (w sensie słabym) kraty zupełnej w siebie ma punkt stały.

Dokładniej: Jeżeli X jest kratą zupełną, $f : X \to X$, $\forall x, y \in X : x \leqslant y \Rightarrow f(x) \leqslant f(y)$, to $P := \{x \in X \mid f(x) = x\} \neq \varnothing$, przy czym:

(a) $a := \sup\{x \in X \mid x \leqslant f(x)\} = \max P$

(b) $b := \inf\{x \in X \mid f(x) \leqslant x\} = \min P$.

Udowodnić to.

44. Wykorzystując twierdzenie Tarskiego o punkcie stałym (zadanie 43) udowodnić twierdzenie z zadania 3.20* bez żadnych założeń o funkcjach f i g, to jest udowodnić, że:

$$\forall f : X \to Y, g : Y \to X \; \exists A, B, C, D \; [A \cup B = X, A \cap B = \varnothing, \\ C \cup D = Y, C \cap D = \varnothing, f(A) = C, g(D) = B].$$

Wskazówka: Odwzorowanie $\varphi : \mathcal{P}X \longrightarrow \mathcal{P}X$, $\varphi(E) = X \setminus g(Y \setminus f(E))$ ma punkt stały $A \subset \mathcal{P}X$.

W szczególności, jeżeli funkcje f i g są injekcjami, $f : X \hookrightarrow Y$, $g : Y \hookrightarrow X$, to $(f|A) \cup (g|D)^{-1} : X \hookrightarrow\!\!\!\!\rightarrow Y$, a więc $X \sim Y$.

(Twierdzenie Cantora–Bernsteina w wersji Tarskiego — zob. zadanie 3.20*).

45. Dana jest krata zupełna X i zbiory $A \subset B \subset X$. Zbiór B z porządkiem indukowanym $(\leqslant) \cap B^2$ jest posetem (nie musi być kratą).

Oznaczmy $a = \sup A = \sup_X A$.

Udowodnić, że:

(1) $a \in B \implies a = \sup_B A$

(2) $b = \sup_B A \in B \implies a \leqslant b$.

(3) Jeżeli $c \in X$ i $B = [c, \cdot\,] = \{x \in X \mid c \leqslant x\}$, to B jest kratą zupełną,

$$\sup_B A = \begin{cases} a, & \text{gdy } A \neq \varnothing \\ c, & \text{gdy } A = \varnothing. \end{cases}$$

46*. Udowodnić, że zbiór P punktów stałych odwzorowania rosnącego $f : X \to X$ kraty zupełnej X (zob. zadanie 43) z porządkiem indukowanym z X jest kratą zupełną.

47*. Dla posetu X oznaczmy $S^-(X)$ ($S^+(X)$) ogół lewych (prawych) odcinków w X;

$$S^-(X) = \{A \subset X \mid \forall x, y \in X : x \leqslant y \in A \;\Rightarrow\; x \in A\}$$

i dualnie $(\ldots \geqslant \ldots)$ dla $S^+(X)$.

Natychmiast widać, że zbiór $S^-(X)$ (i dualnie $S^+(x)$) jest kratą zupełną; $\mathcal{A} \subset S^-(X) \Rightarrow \sup \mathcal{A} = \bigcup \mathcal{A} \in S^-(X)$.

Ponadto $\forall\, A \subset X : A \in S^-(X) \Leftrightarrow X \setminus A \in S^+(X)$.

Udowodnić poniższe uogólnienie na posety twierdzenia Cantora–Bernsteina (zob. zadania 44 i 3.19; zbiór E możemy utożsamiać z posetem (E, id_E)):

Jeżeli X, Y są posetami, f jest izomorfizmem posetu X na prawy odcinek Y' posetu Y; $f : X \xrightarrow{\sim} Y'$, $Y' \in S^+(Y)$ i analogicznie $g : Y \xrightarrow{\sim} X'$, $X' \in S^-(X)$, to istnieje bijekcja $h : X \hookrightarrow\!\!\!\!\rightarrow Y$ taka, że:

$$(*) \qquad \forall\, x, z \in X : x < z \;\Rightarrow\; \neg h(x) > h(z) \qquad (\textit{quasiizomorfizm}).$$

W szczególności, dla dwóch łańcuchów X, Y (zbiorów liniowo uporządkowanych), jeżeli $X \simeq Y' \in S^+(Y)$ i $Y \simeq X' \in S^-(Y)$, to $X \simeq Y$.

(Uwaga: Dla posetów stwierdzenie takie jest fałszywe; zob. zadanie 5.20*).

48*. Udowodnić poniższe uogólnienie na posety twierdzenia Cantora o zbiorze potęgowym (zob. zadanie 3.20).

Twierdzenie Dilwortha–Gleasera:
Dla posetu X nie istnieje surjekcja rosnąca $F : X \twoheadrightarrow S^-(X)$.
Wskazówka: Rozumując nie wprost wziąć:

$$A := \{x \in X \mid x \notin F_X\} \subset B = \bigcup_{a \in A} [\,\cdot\,, a] \in S^-(X).$$

49. Udowodnić, że jedynym automorfizmem zbioru dobrze uporządkowanego X jest id_X.

50. Udowodnić, że dla dwóch zbiorów dobrze uporządkowanych X, Y istnieje co najwyżej jeden izomorfizm $f : X \xrightarrow{\sim} Y$.

51. Dane są dwa zbiory dobrze uporządkowane X, Y, odwzorowanie rosnące (w sensie słabym) $f : X \to Y$ takie, że $\operatorname{Im} f$ jest odcinkiem (lewym) w Y, oraz odwzorowanie silnie rosnące $g : X \to Y$.

Wykazać, że $\forall\, x \in X : f(x) \leqslant g(x)$.

52*. Dane są dwa zbiory dobrze uporządkowane X, Y i odwzorowanie $f : X \to Y$.

Udowodnić, że relacja R w X określona wzorem:

$$x \, R \, z \iff f(x) < f(z) \vee [f(x) = f(z) \wedge x \leqslant z].$$

jest dobrym porządkiem w X.
Wskazówka: Według kryterium Tarskiego należy wykazać spójność i istnienie elementu minimalnego w każdym niepustym podzbiorze X.

4.3. Odpowiedzi

1. Dowody są bezproblemowe — wykorzystujemy definicje.

Na przykład (20):

$\subset$) HP: $\exists)\, x \in B \setminus S_a(A,R)$; $\neg x < a$, $a \leqslant x$, $a \in B$. Ale, jako R-minimum $A \setminus B$, $a \in A \setminus B$ ↯.

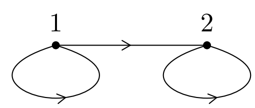
$\supset$) HP: $\exists)\, x \in S_a(A,R) \setminus B$; $x < a$, $x \in A \setminus B$, $a \leqslant x$ ↯.

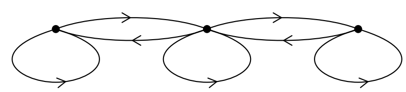
2.

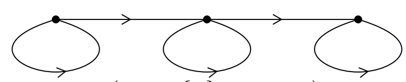
1) HP: $S \not\subset R$. $\exists)\,(x,y) \in S \setminus R$; $(y,x) \in R$, $(y,x) \in S$, $x = y$, $(x,y) \in R$ ↯.
2) HP: $\exists)\,(x,y),(y,z) \in R$, $(x,z) \notin R$. $(z,y) \in R$ $\quad\langle R$ – symetryczna$\rangle$.
   $(y,z),(z,y) \in S$ $\quad\langle R \subset S\rangle$.
   $y = z$ $\quad\langle S$ – antysymetryczna$\rangle$, $(x,z) \in R$ ↯.
3) $\Rightarrow$) $\quad R \subset R^{-1}$ $\quad\langle$z definicji symetryczności relacji$\rangle$.
   HP: $\exists)\,(x,y) \in R^{-1} \setminus R$, $(y,x) \in R$, $(x,y) \in R$ ↯.

3. $\Rightarrow$) $S \circ R = (S \circ R)^{-1} = R^{-1} \circ S^{-1} = R \circ S$.
$\Leftarrow$) $(S \circ R)^{-1} = (R \circ S)^{-1} = S^{-1} \circ R^{-1} = S \circ R$.

4.

1)  $(R = \{(1,1),(2,2),(1,2)\})$

2) 

3) 

4) 5) • $(X = \{1\},\ R = \varnothing)$.

5. Fakt, że relacja równoliczności jest równoważnością, wynika natychmiast z własności bijekcji (bijektywność identyczności, złożenie, odwrotność).

Prawa (a), (b), (c) uzasadniamy, wskazując odpowiednie bijekcje. Na przykład (piszemy fa zamiast $f(a)$):

(a) $\mathrm{Map}(A,B) \times \mathrm{Map}(A,C) \ni (f,g) \longmapsto \{a \mapsto (fa, g\,a) \mid a \in A\}$
(b) $\mathrm{Map}(A, \mathrm{Map}(B,C)) \ni f \longmapsto \{(a,b) \mapsto (fa)b \mid (a,b) \in A \times B\}$
(c) $\mathrm{Map}(A,C) \times \mathrm{Map}(B,C) \ni (f,g) \longmapsto f \cup g$
(d) $\mathrm{Map}^\circ(A,B) \ni f \longmapsto f \cup ((A \setminus \mathrm{Dom}\, f) \times \{B\})$.

6. Przechodniość relacji $\equiv \pmod{\mathcal{I}}$ wynika z inkluzji: $A \dot{-} C \subset (A \dot{-} B) \cup (B \dot{-} A)$, która z kolei jest wnioskiem z dwu oczywistych faktów:
$A \setminus C \subset (A \setminus B) \cup (B \setminus C)$
$C \setminus A \subset (C \setminus B) \cup (B \setminus A)$.

7. Intuicja: zbiory należące do filtru są „duże", „istotne". Na przykład może być $\mathcal{F} = \{A \mid Y \subset A \subset X\}$ dla pewnego $Y \subset X$; mówimy wówczas, że $\mathcal{F}$ jest *filtrem głównym generowanym przez* Y.

Dla filtru $\mathcal{F}$ na zbiorze X określamy w $\mathcal{P}X$ równoważność zwaną *przystawaniem modulo* $\mathcal{F}$:

$$A \equiv B \pmod{\mathcal{F}} \iff (A \mathbin{\dot{-}} B)^{\urcorner} = (A \cap B) \cup (A \cup B)^{\urcorner} \in \mathcal{F}.$$

Łatwo wskazać bijekcję kanoniczną $\varphi : \alpha(X) \hookrightarrow\!\!\!\!\rightarrow \beta(X)$, $\varphi(A) = A^{\urcorner} = X \setminus A$ — bijekcja ta przenosi relację przystawania modulo ideał na relację przystawania modulo filtr.

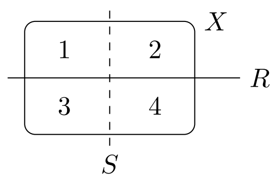
8. Przechodniość relacji $\underset{\mathcal{F}}{\equiv}$ wynika z inkluzji:

$$\mathrm{Ker}(f, g) \cap \mathrm{Ker}(g, h) \subset \mathrm{Ker}(f, h)$$

dla $f, g, h : X \to Y$.

9.

(a) Nie. Zachodzi tylko implikacja „$\Leftarrow$”.
$\langle$HP: $\exists)\ (x, y) \in X^2 \setminus (S \circ R)$. Niech na przykład $R = X^2$. Wówczas $(x, y) \in R$, $(y.y) \in S$, a więc $(x, y) \in S \circ R$ ↯$\rangle$. Implikacja „$\Rightarrow$” na ogół nie zachodzi. $\langle$Weźmy $X = I_4$, $R = \mathrm{id}_X \cup \{(1, 2), (2, 1), (3, 4), (4, 3)\} \subsetneq X^2$, $S = \mathrm{id}_X \cup \{(1, 3), (3, 1), (2, 4), (4, 2)\} \subsetneq X^2$.



Łatwo widać, że $S \circ R = X^2\rangle$.

(b) $\langle$HP: $S \circ R = X^2 \wedge \exists)\ (x, y) \in X^2 \setminus (R \circ S)$. Wówczas $(y, x) \in S \circ R$, $\exists\, z)\ (y, z) \in R$, $(z, x) \in S$; z symetryczności R i S wynika, że $(x, z) \in S$, $(z, y) \in R$, a więc $(x, y) \in R \circ S$ ↯$\rangle$.

10. Mechaniczne przeliczenia w oparciu o definicje.
Na przykład implikacja (b) $\Rightarrow$ (a):
HP: (b)$\wedge\exists)\ (x, y) \in R \setminus S$. $\exists)\ \xi \in X/R : x, y \in \xi$. $\exists)\ \eta \in X/S : \xi \subset \eta$. $x, y \in \eta, (x, y) \in S$ ↯.

11.

(i) Na ogół w tej sytuacji dowodzimy najpierw jednoznaczności, a potem istnienia odwzorowania g.

Jednoznaczność: Przypuśćmy, że takie g już mamy. Wówczas dla $x \in \xi \in X/R : \xi = [x] = \mathrm{nat}\, x$, $g(\xi) = g(\mathrm{nat}\, x) = f(x)$.

Istnienie: Określamy funkcję $g : X/R$ powyższym wzorem; określenie jest poprawne, gdyż dla $x, y \in \xi \in X/R : \mathrm{nat}\, x = [x] = \xi = [y] = \mathrm{nat}\, y$.

(ii) Surjektywność: Dla $y = f(x) \in \mathrm{Im}\, f : y = g([x]) \in \mathrm{Im}\, g$.

Injektywność: Jeżeli dla $x, z \in X : g([x]) = g([z])$, to $f(x) = f(z)$, $(x, z) \in \ker f$, a więc $[x] = [z]$.

12. $\Rightarrow$) $\forall\, x, z \in X\ (x, z) \in R \ \Rightarrow\ f(x) = h(\operatorname{nat} x) = h(\operatorname{nat} z) = f(z)$.
$\Leftarrow$) Określamy $h : X/R \to Y$, kładąc dla $x \in \xi \in X/R : h(\xi) = f(x)$. Określenie to jest poprawne, gdyż dla $x, z \in \xi \in X/R : (x, z) \in R \subset \ker f$, a więc $f(x) = f(z)$.

13. Określimy odwzorowanie:

$$\psi : \operatorname{Equ}(X/R) \longrightarrow \{S \in \operatorname{Equ} X \mid R \subset S\}.$$

Niech $T \in \operatorname{Equ}(X/R)$. Połóżmy $\psi(T) = S = \ker(\operatorname{nat}_T \circ \operatorname{nat}_R)$

$$X \xrightarrow{\operatorname{nat}_R} X/R \xrightarrow{\operatorname{nat}_T} (X/R)/T;$$

wówczas rzeczywiście $R \subset S$ $\langle x\ R\ y \ \Rightarrow\ [x]_R = [y]_R \ \Rightarrow\ (\operatorname{nat}_T \circ \operatorname{nat}_R)(x) = (\operatorname{nat}_T \circ \operatorname{nat}_R)(y) => x\ S\ y\rangle$.

Wystarczy teraz pokazać, że $\psi \circ \varphi \subset \mathrm{id}$ i $\varphi \circ \psi \subset \mathrm{id}$:

1° Dla $R \subset S \in \operatorname{Equ} X : \psi(\varphi(S)) = S$. $\langle$Oznaczmy $T = \varphi(S) = S/R$. Niech $x, y \in X$. Wówczas:
$(x, y) \in \psi(T) \Leftrightarrow (\operatorname{nat}_T \circ \operatorname{nat}_R)(x) = (\operatorname{nat}_T \circ \operatorname{nat}_R)(y)$
$\Leftrightarrow ([x]_R, [y]_R) \in S/R \Leftrightarrow h([x]_R) = h([y]_R) \Leftrightarrow [x]_S = [y]_S \Leftrightarrow (x, y) \in S\rangle$.

2° Dla $T \in \operatorname{Equ}(X/R) : \varphi(\psi(T)) = T$. $\langle$Oznaczmy $S = \psi(T) = \ker(\operatorname{nat}_T \circ \operatorname{nat}_R)$. Wówczas dla $x, y \in X$:
$([x]_R, [y]_R) \in \varphi(S) = S/R \Leftrightarrow h([x]_R) = h([y]_R) \Leftrightarrow [x]_S = [y]_S$
$\Leftrightarrow (x, y) \in S \Leftrightarrow (\operatorname{nat}_T \circ \operatorname{nat}_R)(x) = (\operatorname{nat}_T \circ \operatorname{nat}_R)(y) \Leftrightarrow ([x]_R, [y]_R) \in T\rangle$.

14. Mechaniczne przeliczenia w oparciu o definicje. (por. zadanie 11 z rozdziału 3).

15. Notujmy $RS = S \circ R$, $R^2 = RR$.

(a) $\Rightarrow$)
$\subset$) Niech $x(R \cup S)y$, czyli $x\ R\ y$ lub $x\ S\ y$.
Jeżeli $x\ R\ y$, to $x\ RS\ y$, gdyż $y\ S\ y$.
Jeżeli $x\ S\ y$, to $x\ RS\ y$, gdyż $x\ R\ x$.
$\supset$) Niech $x\ RS\ y$. $\exists\, z) x\ R\ z, z\ S\ y$. Wówczas $X(R \cup S)z$ i $z(R \cup S)y$, a więc $x(R \cup S)y$.

$\Leftarrow$) Zwrotność i symetria relacji $R \cup S$ są oczywiste. Przechodniość:
Niech $x(R \cup S)y$, $y(R \cup S)z$.
1. Jeżeli $x\ R\ y$ i $y\ S\ z$, to $x\ RS\ z$, a więc $x(R \cup S)z$.
2. Jeżeli $x\ S\ y$ i $y\ R\ z$, to $z\ R\ y$ i $y\ S\ x$, a więc $z\ RS\ x$, $z(R \cup S)x$, $x(R \cup S)z$.

(b) Natychmiastowy wniosek z (a).

(c) $\Rightarrow$) $RS = (RS)^{-1} = S^{-1}R^{-1} = SR$.
$\Leftarrow$) $\forall\, x \in X : x\ R\ x, x\ S\ x$, a więc $x\ RS\ x$, $\mathrm{id}_X \subset RS$.
Ponadto $(RS)^2 = RSRS = RRSS = RS$ oraz $(RS)^{-1} = S^{-1}R^{-1} = SR = RS$.

16. Utrzymujemy notację z 15. Niech $R, S \in \operatorname{Equ} X$ oraz $RS = SR$. Według 15(c) $RS \in \operatorname{Equ} X$. Ponadto $R \subset RS$ i $S \subset RS$, a więc $R \cup S \subset RS$.
Także $R \cup S \subset T \in \operatorname{Equ} X \ \Rightarrow\ RS \subset T$. $\langle$Jeżeli $x\ RS\ y$, to $\exists\, z) x\ R\ z, z\ S\ y$, a więc $x(R \cup S)z$, $z(R \cup S)y$, skąd $x\ T\ z, z\ T\ y$ i ostatecznie $x\ T\ y\rangle$. Zatem $RS = (R \cup S)^{-}$.

17. Ogólny schemat postępowania w takiej sytuacji jest następujący (por. punkt (26) ze Wstępu):

1) Określamy $f : \alpha(X) \longrightarrow \beta(X)$, kładąc dla $\varphi \in \alpha(X)$: $f(\varphi) = \{A \subset X \mid \varphi A = A\}$. $\langle$Sprawdzamy, że $\mathcal{F} = f(\varphi) \in \beta(X)$. $X \subset \varphi X \subset X$, a więc $X = \varphi X$, $X \in \mathcal{F}$. Jeżeli $\varnothing \neq \mathcal{A} \subset \mathcal{F}$, to $\forall\, A \in \mathcal{A} : \bigcap \mathcal{A} \subset A$, $\varphi \bigcap \mathcal{A} \subset \varphi A = A$, a więc $\varphi \bigcap \mathcal{A} \subset \bigcap \mathcal{A}$, czyli $\varphi \bigcap \mathcal{A} = \bigcap \mathcal{A}$, $\bigcap \mathcal{A} \in \mathcal{F}\rangle$.

2) Określamy $g : \beta(X) \longrightarrow \alpha(X)$.
Dla $\mathcal{F} \in \beta(X)$ definiujemy $g(\mathcal{F}) = \varphi : \mathcal{P}X \to \mathcal{P}X$, kładąc dla $A \subset X$: $\varphi A = \bigcap\{B \in \mathcal{F} \mid A \subset B\}$. $\langle$Sprawdzamy, że $\varphi \in \alpha(X)$. $\forall\, A, B \subset X : A \subset \varphi A$, gdyż $X \in \mathcal{F}$.
Jeżeli $A \subset B$, to $A \subset \varphi B \in \mathcal{F}$, a więc $\varphi A \subset \varphi B$.
Wreszcie, ponieważ $\varphi A \subset \varphi A \in \mathcal{F}$, więc $\varphi\varphi A \subset \varphi A$, czyli $\varphi\varphi A = \varphi A\rangle$.

3) Sprawdzamy, że $g \circ f \subset \mathrm{id}$. $\langle$Niech $\varphi \in \alpha(X)$, $\mathcal{F} = f(\varphi)$, $\varphi' = g(\varphi)$. Dla $A \subset X$: $\varphi' A = \bigcap\{B \subset X \mid A \subset B \wedge \varphi B = B\}$. Jednak $\bigcap\{B \subset X \mid A \subset B \wedge \varphi B = B\} = \varphi A$, gdyż $\varphi A \in \{B \subset X \mid A \subset B \wedge \varphi B = B\}$ oraz $\forall\, B \subset X : A \subset B \wedge \varphi B = B \;\Rightarrow\; \varphi A \subset B$. Zatem $\varphi' A = \varphi A$. Czyli $\varphi' = \varphi\rangle$.

4) Sprawdzamy, że $f \circ g \subset \mathrm{id}$. $\langle$Niech $\mathcal{F} \in \beta(X)$, $\varphi = g(\mathcal{F})$, $\mathcal{F}' = f(\varphi)$. Dla $A \subset X : A \in \mathcal{F}' \Leftrightarrow \varphi A = A \Leftrightarrow A = \bigcap\{B \in \mathcal{F} \mid A \subset B\} \Leftrightarrow A \in \mathcal{F}$, a więc $\mathcal{F}' = \mathcal{F}\rangle$.

Z 1)–4) wynika, że $f : \alpha(X) \lhook\joinrel\twoheadrightarrow \beta(X)$, $g = f^{-1}$.

18. Jeżeli φ jest operacją domknięcia w X, to oczywiście zachodzi (*) $\langle A \subset \varphi B \;\Rightarrow\; \psi A \subset \varphi A \subset \varphi B\rangle$.

Natomiast jeżeli zachodzi (*) i $A, B \subset X$, to:

1) $A \subset B \;\Rightarrow\; A \subset B \cup \psi B \;\Rightarrow\; \varphi A \subset \varphi B$

2) $A \subset \varphi A = A \cup \psi A$

3) $\varphi A \subset \varphi\varphi A$ wg 1), 2),

ale $\varphi A \subset A \cup \psi A$, więc wg (*) $\psi\varphi A \subset \varphi A$, zatem $\varphi\varphi A = \varphi A \cup \psi\varphi A \subset \varphi A$, czyli $\varphi\varphi A = \varphi A$.

19.
$\Rightarrow$) Natychmiastowy wniosek z przechodniości relacji $\leqslant$.
$\Leftarrow$) Ponieważ $a \in [\,\cdot\,, a] \subset [\,\cdot\,, b]$, więc $a \leqslant b$. Analogicznie $b \leqslant a$, czyli $a = b$.

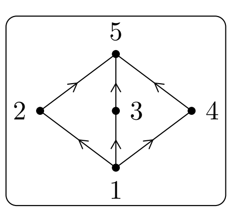
Kresy we wskazanym sensie nie są zachowywane.

Mamy tylko inkluzje:

$a \vee b = c \implies [\,\cdot\,, a] \cup [\,\cdot\,, b] \subset [\,\cdot\,, c]$
$a \wedge b = c \implies [\,\cdot\,, a] \cap [\,\cdot\,, b] \subset [\,\cdot\,, c]$.

Równości nie muszą zachodzić.

Przykład:

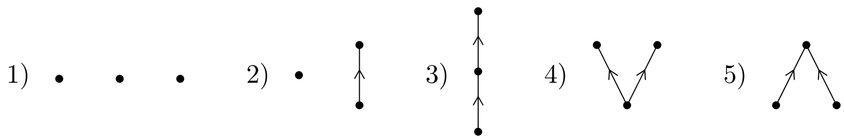


X

$2 \vee 4 = 5$
$[\,\cdot\,, 2] \cup [\,\cdot\,, 4] = \{1, 2\} \cup \{1, 4\} = \{1, 2, 4\}$
$[\,\cdot\,, 5] = X = \{1, 2, 3, 4, 5, \}$.

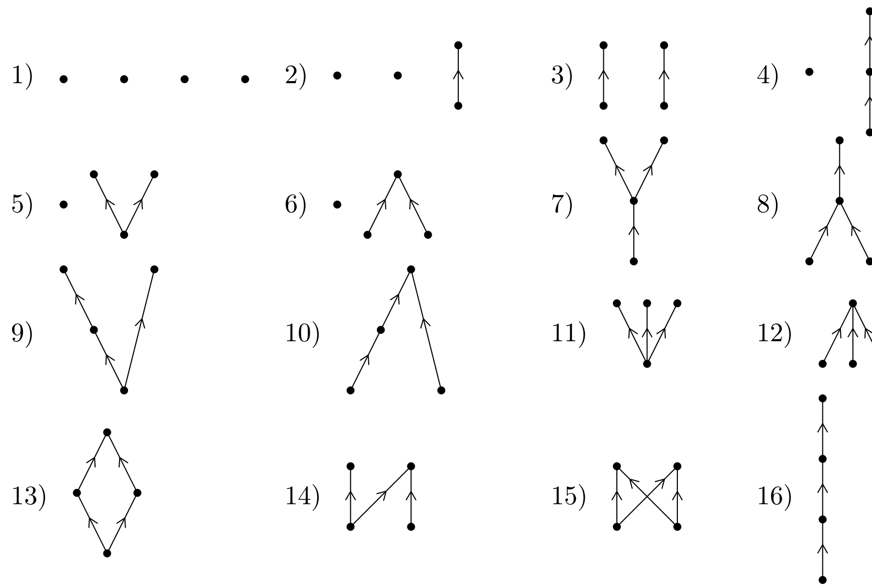
20.

(a)



Autodualne są posety: 1), 2) i 3).

(b)



Autodualne są posety: 1), 2), 3), 4), 13), 14), 15), 16).

Jak widzimy, dla małych liczb n lista tzw. *typów porządkowych* (*order types*) mocy n, czyli liczb nieizomorficznych posetów n-elementowych, wygląda następująco:

n	0	1	2	3	4	...
τ_n	1	1	2	5	16	...

Obszerniejszą listę znajdziemy u Sloane'a: `oeis A000112`.

21.

(i)

$\mathrm{id}_X = \{(1,1),(2,2),(3,3)\}$,

$\mathrm{id}_X \cup \{(1,2)\}$, $\quad \mathrm{id}_X \cup \{(2,1)\}$,
$\mathrm{id}_X \cup \{(1,3)\}$, $\quad \mathrm{id}_X \cup \{(3,1)\}$,
$\mathrm{id}_X \cup \{(2,3)\}$, $\quad \mathrm{id}_X \cup \{(3,2)\}$,

$\mathrm{id}_X \cup \{(1,2),(2,3),(1,3)\}$, $\quad \mathrm{id}_X \cup \{(1,3),(3,2),(1,2)\}$,
$\mathrm{id}_X \cup \{(2,1),(1,3),(2,3)\}$, $\quad \mathrm{id}_X \cup \{(2,3),(3,1),(2,1)\}$,
$\mathrm{id}_X \cup \{(3,1),(1,2),(3,2)\}$, $\quad \mathrm{id}_X \cup \{(3,2),(2,1),(3,1)\}$,

$\mathrm{id}_X \cup \{(1,2),(1,3)\}$, $\quad \mathrm{id}_X \cup \{(2,1),(3,1)\}$,

$\mathrm{id}_X \cup \{(2,1),(2,3)\}$, $\mathrm{id}_X \cup \{(1,2),(3,2)\}$,
$\mathrm{id}_X \cup \{(3,1),(3,2)\}$, $\mathrm{id}_X \cup \{(1,3),(2,3)\}$.

(ii) W zbiorze E porządków częściowych w X $(= I_n)$ określamy równoważność, kładąc dla $R, S \in E$:

$$R \equiv S \iff R = S \vee R = S^{-1}.$$

Wszystkie warstwy tej równoważności, z wyjątkiem warstwy $[\mathrm{id}_X] = \{\mathrm{id}_X\}$, są dwuelementowe; jeżeli tych warstw dwuelementowych jest k, to:

$$\alpha_n = 2k + 1.$$

22.

(i) Wynika natychmiast z definicji rozważanych operacji.

(ii) HP: $A \subset X \wedge \exists)\, a \in A,\ a \notin A^{+-}$.
Ponieważ $A^{+-} = \{x \in X \mid \forall\, b \in A^+ : x\ R\ b\}$, więc $\exists)\, b \in A^+ : \neg a\ R\ b$. Jednak z definicji A^+ wynika, że $a\ R\ b$ ↯.

(iii) Jeżeli $A \subset X$, to według (ii) i (i) $A^{+-+} \subset A^+$; i według (ii) zastosowanego do $B = A^+$: $A^+ \subset A^{+-+}$, a więc $A^{+-+} = A^+$.

Jeżeli klasa $A \subset X$ jest domknięta, to $A = A^{+-} = B^-$ dla $B = A^+ \subset Y$.
Na odwrót, jeżeli $A = B^-$ dla $B \subset Y$, to $A^{+-} = B^{-+-} = B^- = A$, a więc klasa A jest domknięta.
Jedno-jednoznaczność odpowiedniości Galois wynika natychmiast z (iii).

23. Dla $A \subset X$:
$A^+ = \{x \in X \mid \forall\, a \in A : a \leqslant x\} = M(A) =$ majoranty A
$A^- = \{x \in X \mid \forall\, a \in A : x \leqslant a\} = m(A) =$ minoranty A.
Dla $a \in X$:
$\{a\}^+ = [a, \cdot\,]$, $\{a\}^- = [\,\cdot\,, a]$
$[a, \cdot\,]^+ = M([a, \cdot\,]) = \{y \in X \mid \forall\, z \in [a, \cdot\,]\ y \in [z, \cdot\,]\} = \bigcap_{z \in [a, \cdot\,]} [z, \cdot\,] \subset [a, \cdot\,]$
(tak więc $[a, \cdot\,]^+ = \{\max[a, \cdot\,]\}$, jeżeli w przedziale $[a, \cdot\,]$ istnieje element największy oraz $[a, \cdot\,]^+ = \varnothing$ w przeciwnym wypadku)
$[a, \cdot\,]^- = \{x \in X \mid \forall\, z \in [a, \cdot\,] : x \leqslant z\} = [\,\cdot\,, a]$.
Dualnie:
$[\,\cdot\,, a]^+ = [a, \cdot\,]$, $[\,\cdot\,, a]^- = \bigcap_{z \in [\,\cdot\,, a]} [\,\cdot\,, z]$.
Tak więc zbiory $[\,\cdot\,, a]$ są $(+-)$-domknięte, zaś zbiory $[a, \cdot\,]$ są $(-+)$-domknięte; zbiory te pozostają w odpowiedniości Galois.

24*.

(a) Niech $\mathcal{A} \subset \mathcal{F}$. Wówczas $\sup \mathcal{A} = (\bigcup \mathcal{A})^{+-}$, gdyż:
1) $\forall\, A \in \mathcal{A} : A \subset \bigcup \mathcal{A} \subset (\bigcup \mathcal{A})^{+-}$.
2) Jeżeli $B \in \mathcal{F}$ i $\forall\, A \in \mathcal{A} : A \subset B$

to $\bigcup \mathcal{A} \subset B$, a więc $(\bigcup \mathcal{A})^{+-} \subset B^{+-} = B$.

$\left(\text{Analogicznie } \inf \mathcal{A} = \begin{cases} \bigcap \mathcal{A}, & \text{gdy } \mathcal{A} \neq \varnothing \\ X, & \text{gdy } \mathcal{A} = \varnothing \end{cases}\right).$

(b)

Ad 1) Równoważność jest natychmiastowym wnioskiem z definicji (por. zadanie 19).

Ad 2) Jeżeli $a \in A$, to $a \leqslant c$, a więc $\varphi(a) = [\,\cdot\,, a] \subset [\,\cdot\,, c] = \varphi(c)$, czyli $\varphi(c)$ jest majorantą zbioru $\varphi(A)$ w $\mathcal{F}$.

Załóżmy teraz, że $C \in \mathcal{F}$ i $\forall\, a \in A : \varphi(a) \subset C$, czyli $a \in [\,\cdot\,, a] \subset C$. Zatem $A \subset C$, skąd $C^+ \subset A^+$, $\forall\, x \in C^+ : x \in A^+ = M(A)$, a więc $\forall\, x \in C^+ : c \leqslant x$, czyli $c \in C^{+-}$, $\varphi(c) = [\,\cdot\,, c] \subset C^{+-} = C$.

Ad 3) Jeżeli $a \in A$, to $d \leqslant a$, a więc $\varphi(d) = [\,\cdot\,, d] \subset [\,\cdot\,, a] = \varphi(a)$, czyli $\varphi(d)$ jest minorantą zbioru $\varphi(A)$ w $\mathcal{F}$.

Załóżmy teraz, że $D \in \mathcal{F}$ i $\forall\, a \in A : D \subset \varphi(a)$, czyli $D \subset [\,\cdot\,, a]$, $a \in [a, \cdot\,] = [\,\cdot\,, a]^+ \subset D^+$. Zatem $A \subset D^+$, $D = D^{+-} \subset A^-$. Ponieważ $d = \inf A$, więc $\forall\, x \in D : x \in A^-$, $x \leqslant d$. $D \subset [\,\cdot\,, d] = \varphi(d)$.

25. Niech na przykład $\alpha \leqslant \beta$ (symetria sytuacji). Należy wykazać, że $\sup(A \cup B) = \beta$.

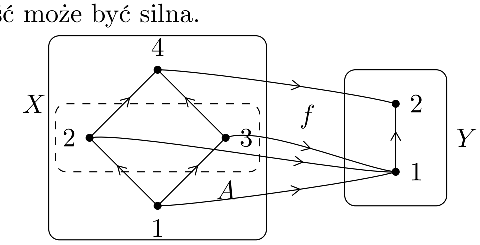
1°) $\beta \in M(A \cup B)$ $\quad \langle \forall x \in A \cup B : x \in A \;\Rightarrow\; x \leqslant \alpha \leqslant \beta,\; x \in B \;\Rightarrow\; x \leqslant \beta \rangle$.

2°) Jeżeli $\beta' \in M(A \cup B)$, to $\beta \leqslant \beta'$ $\quad \langle$HP: $\neg \beta \leqslant \beta'$. Wówczas $\beta' < \beta$ (porządek jest liniowy), a więc $\beta' \notin M(B)$. Zatem $\exists)\, x \in B : \neg x \leqslant \beta'$, $\beta' < x$, ale $x \in A \cup B$, $x \leqslant \beta'$ $\lightning\rangle$.

26. $\sup f(A) \leqslant f(\sup A)$, gdyż oznaczając $\alpha = \sup A$, $\beta = \sup f(A)$, będziemy mieli: $\forall\, x \in A$, $x \leqslant \alpha$, $f(x) \leqslant f(\alpha)$, a więc $f(\alpha) \in M(f(A))$, $\beta \leqslant f(\alpha)$.

Nierówność może być silna.

Przykład:



$X = (I_4, \mathrm{id}_{I_4} \cup \{(1,2), (2,4), (1,3), (3,4), (1,4)\})$, $Y = (I_2, \mathrm{id}_{I_2} \cup \{(1,2)\})$, $A = \{2,3\}$, $f = \{1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 1, 4 \mapsto 2\}$.

Wówczas $f(A) = \{1\}$, $\sup A = 4$, $\sup f(A) = 1$, a więc $\sup f(A) = 1 < f(\sup A) = f(4) = 2$.

27. Należy wykazać, że:

1) $\alpha \in M(\operatorname{Im} g)$

2) $\forall\, \alpha' \in M(\operatorname{Im} g) : \alpha \leqslant \alpha'$.

Ad 1) $\forall\, (a,b) \in A \times B : g(a,b) \leqslant f(a) \leqslant \alpha$

Ad 2) Ponieważ $\forall\, a \in A\ \forall\, b \in B : g(a,b) \leqslant \alpha'$, więc $\forall\, a \in A : \alpha' \in M(\{g(a,b) \mid b \in B\})$, $f(a) \leqslant \alpha'$. Zatem $\alpha' \leqslant M(\operatorname{Im} f)$, $\alpha \leqslant \alpha'$.

Uwaga: W związku z powyższym dowodem punktu 2) nasuwa się spostrzeżenie, iż niekiedy hipoteza dowodu nie wprost nic nie daje, a nawet prowadzi na manowce. W przypadku 2) mielibyśmy HP: $\exists)\, \alpha' \in M(\operatorname{Im} g) : \neg\alpha \leqslant \alpha'$. Stąd, przy dodatkowym założeniu, że porządek w X jest liniowy; $\alpha' < \alpha = \sup(\operatorname{Im} f)$, $\alpha' \notin M(\operatorname{Im} f)$, $\exists)\, a \in A : \alpha' < f(a) = \sup\limits_{b\in B} g(a,b)$, $\exists)\, b \in B : \alpha' < g(a,b) \leqslant \alpha'$ ↯.

Może się pojawić przypuszczenie, że twierdzenie jest prawdziwe tylko dla zbiorów liniowo uporządkowanych, a następnie bezowocne poszukiwanie kontrprzykładu w posecie niebędącym łańcuchem.

28. Zależności te wynikają natychmiast z definicji kraty. Na przykład dowód pierwszej równości w (i) sprowadza się do wykazania, że obie strony są równe $\sup\{a,b,c\}$ $\langle a \leqslant a\vee b \leqslant (a\vee b)\vee c$, $b \leqslant \ldots$, $c \leqslant \ldots$, a więc $(a\vee b)\vee c \in M(a,b,c)$; jeśli $d \in M(a,b,c)$, to $d \in M(a,b)$, $a\vee b \leqslant d$, $d \in M(a\vee b, c)$, $(a\vee b)\vee c \leqslant d$, a więc $(a\vee b)\vee c = \sup\{a,b,c\}\rangle$.

Dla dowodu (v) wystarczy oczywiście pokazać, że $a\wedge(b\vee c) \in M(a\wedge b, a\wedge c)$ $\langle a\wedge b \leqslant a$, $a\wedge b \leqslant b \leqslant b\vee c$, a więc $a\wedge b \in m(a, b\vee c)$, skąd $a\wedge b \leqslant a\wedge(b\vee c)$. Analogicznie $a\wedge c \leqslant a\wedge(b\vee c)\rangle$.

29. Dowód sprowadza się do prostych przekształceń wykorzystujących definicje. Na przykład relacja $a \leqslant b :\Leftrightarrow a\vee b = b$ jest zwrotna, $a \leqslant a$, gdyż według (iv): $a\vee a = a\vee(a\wedge(a\vee a)) = a$.
Podobnie $a \leqslant' b \Leftrightarrow a\vee b = b \Leftrightarrow a \leqslant b$ dla $a, b \in X$.

30. Tak jak w zadaniu poprzednim — przekształcenia bazujące na definicjach. Np. $a \leqslant b \;\wedge\; b \leqslant c \;\Rightarrow\; a \leqslant c$, gdyż $a\vee b = b \;\wedge\; b\vee c = c \implies a\vee c = a\vee(b\vee c) = (a\vee b)\vee c = b\vee c) = c$.

31*. Łatwo widać, że w kracie X spełnione są warunki (1), (2) Kalmana. Trudniejszy jest dowód implikacji w przeciwnym kierunku:

(3) $c\vee e = (((b\wedge c)\wedge a)\vee e)\vee((f\vee c)\wedge c)\ )$ $\quad\langle(1), (2), d\mapsto c\rangle$
(4) $(((a\wedge b)\wedge c)\vee d)\vee a = a\vee((f\vee d)\wedge d)$ $\quad\langle(1), (2), e\mapsto a\rangle$
(5) $c\vee a = a\vee((f\vee c)\wedge c)$ $\quad\langle(1), (4), d\mapsto c\rangle$
(6) $c\vee a = a\vee(c\wedge c)$ $\quad\langle(1), (5), f\mapsto c\wedge c\rangle$
(7) $c\vee(g\wedge(c\wedge c)) = c\wedge c$ $\quad\langle(1), (6), a\mapsto g\wedge(c\wedge c)\rangle$
(8) $a = a\vee((f\vee(a\wedge a))\wedge(a\wedge a))$ $\quad\langle(1), (5), c\mapsto a\wedge a\rangle$
(9) $a = a\vee((a\wedge a)\wedge(a\wedge a))$ $\quad\langle(1), (8), f\mapsto f\wedge(a\wedge a)\rangle$
(10) $a = a\wedge a$ $\quad\langle(7), (9), c\mapsto a, g\mapsto a\wedge a\rangle$
(11) $c\vee a = a\vee c$ – $\vee$-komutatywność! $\quad\langle(6), (10)\rangle$
(12) $a = a\vee a$ $\quad\langle(1), (10)\rangle$
(13) $(a\vee d)\vee e = (a\vee e)\vee((f\vee d)\wedge d)$ $\quad\langle(2), (10), b\mapsto a, c\mapsto a\rangle$
(14) $(a\vee d)\vee e = (a\vee e)\vee d$ $\quad\langle(10), (12), (13), f\mapsto d\rangle$
(15) $(d\vee a)\vee e = d\vee(a\vee e)$ – $\vee$-asocjatywność! $\quad\langle(11), (14)\rangle$
(16) $a\vee(a\wedge b) = a$ – $\vee$-pochłanianie! $\quad\langle(1), (11)\rangle$
(17) $c\vee((f\vee c)\wedge c) = (f\vee c)\wedge c$ $\quad\langle(5), (12), a\mapsto(f\vee c)\wedge c\rangle$
(18) $c = (f\vee c)\wedge c$ $\quad\langle(1), (11), (17)\rangle$

(Odtąd zaczyna się prawdziwe „żyłowanie”!)

(19) $((a \wedge b) \wedge c) \vee d = ((b \wedge c) \wedge a) \vee d$ $\langle(2), (12), (15), (18), e \mapsto d\rangle$
(20) $((a \wedge b) \wedge c) \vee a = a$ $\langle(1), (19), d \mapsto a\rangle$
(21) $(a \wedge c) \vee a = a$ $\langle(10), (20), b \mapsto a\rangle$
(22) $a \wedge b = ((b \wedge c) \wedge a) \vee (a \wedge b)$ $\langle(19), (21), d \mapsto a \wedge b\rangle$
(23) $a \wedge b = (b \wedge a) \vee (a \wedge b)$ $\langle(10), (22), c \mapsto b\rangle$
(24) $b \wedge a = (b \wedge a) \vee (a \wedge b)$ $\langle(11), (23), a \mapsto b, b \mapsto a\rangle$
(25) $a \wedge b = b \wedge a$ – $\wedge$-komutatywność! $\langle(23), (24)\rangle$
(26) $c \wedge (c \vee f) = c$ – $\wedge$-pochłanianie! $\langle(11), (18), (25)\rangle$
(27) $(a \wedge b) \wedge c = ((c \wedge b) \wedge a) \vee ((a \wedge b) \wedge c)$ $\langle(12), (19), (25), d \mapsto (a \wedge b) \wedge c)\rangle$
(28) $(c \wedge b) \wedge a = ((c \wedge b) \wedge a) \vee ((a \wedge b) \wedge c)$ $\langle(11), (27), a \mapsto c, c \mapsto a\rangle$
(29) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ – $\wedge$-asocjatywność! $\langle(25), (27), (28)\rangle$.

Komentarz: Jak widać, uzyskanie sześciu klasycznych aksjomatów teorii krat, wychodząc z aksjomatów Kalmana (1), (2), jest dość kłopotliwe. Ciekawym problemem jest, w jaki sposób dojść do takich równości jak (1) i (2); por.: R. Padmanabhan, *On identities defining lattices*, Algebra Universalis 1, 1972, pp. 359–361.

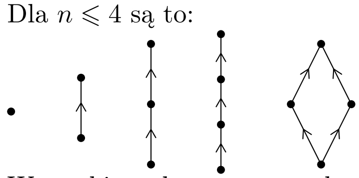
32. Ze względu na dualność wystarczy wykazać, że (1) $\implies$ (2).
$(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = a \vee (a \wedge c) \vee (b \wedge c) = a \vee (b \wedge c)$.

33.

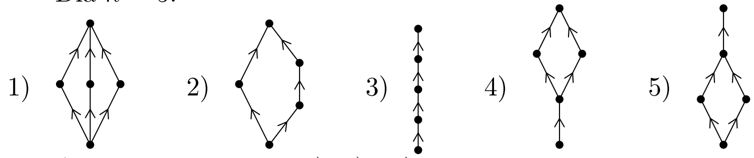
(1) Ponieważ $a \leqslant a \vee (x \wedge b) = \alpha(x)$ i $\beta(x) = (a \vee x) \wedge b \leqslant b$, więc wystarczy udowodnić, że $\alpha(x) \leqslant \beta(x)$.
Otóż $a \leqslant a \vee x$, $x \wedge b \leqslant x \leqslant a \vee x$, a więc $a \vee x \in M(a, x \wedge b)$, skąd $\alpha(x) = a \vee (x \wedge b) \leqslant a \vee x$. Również $a \leqslant b$, $x \wedge b \leqslant b$, więc $b \in M(a, x \wedge b)$, czyli $a \vee (x \wedge b) = \alpha(x) \leqslant b$. Zatem $\alpha(x) \in m(a \vee x, b)$, a więc $\alpha(x) \leqslant (a \vee x) \wedge b = \beta(x)$.
(2) Jeśli $a \leqslant x \leqslant b$, to $\alpha(x) = a \vee (x \wedge b) = a \vee x = x$ oraz $\beta(x) = (a \vee x) \wedge b = x \wedge b = x$.

34. $\Rightarrow$) Ponieważ $a \wedge b \leqslant b$, to $(a \wedge b) \vee (x \wedge b) = ((a \wedge b) \vee x) \wedge b$.
$\Leftarrow$) Jeśli $a, b, x \in X$ i $a \leqslant b$, to $a \wedge b = a$ i równość upraszcza się do $a \wedge (x \vee b) = (a \wedge x) \vee b$.

35. Dla $n \leqslant 4$ są to:

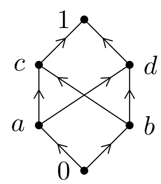


Wszystkie te kraty są autodualne.
Dla $n = 5$:



Autodualne są kraty 1), 2) i 3).

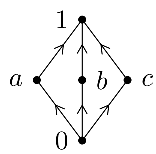
36. Dodając 0 i 1 do szesnastu posetów z zadania 20.(b) otrzymamy piętnaście nieizomorficznych krat 6-elementowych: 1)–14) i 16), (por. `oeis A006966`). Poset otrzymany w ten sposób z posetu 15) ma diagram:



i dalej nie jest kratą, gdyż $M\{a, b\} = \{c, d, 1\}$, $a \vee b = \min\{c, d, 1\} = \mathbb{V}$.

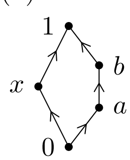
37. Jeżeli krata X jest dystrybutywna i $a, b, x \in X$, przy czym $a \leqslant b$, to $(a \vee x) \wedge b = (a \wedge b) \vee (x \wedge b) = a \vee (x \wedge b)$, a więc krata X jest modularna.

(a) Krata o diagramie:



jest modularna ⟨sprawdzimy np. równość rzutowań α, β na przedział $[a, 1]$:
$\alpha(0) = a \vee (0 \wedge 1) = a \vee 0 = a$ $\beta(0) = (a \vee 0) \wedge 1 = a \wedge 1 = a$
$\alpha(b) = a \vee (b \wedge 1) = a \vee b = 1$ $\beta(b) = (a \vee b) \wedge 1 = 1 \wedge 1 = 1$
i analogicznie $\alpha(c) = \beta(c)$⟩
i nie jest dystrybutywna ⟨$a \wedge (b \vee c) = a \wedge 1 = a$; $(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$⟩.

(b) Krata o diagramie:



nie jest modularna, gdyż dla przedziału $[a, b]$: $\alpha(x) = a \vee (x \wedge b) = a \vee 0 = a < \beta(x) = (a \vee x) \wedge b = 1 \wedge b = b$.

38.
(a) HP: $\exists) \, x, y$ – (b, c)-dopełnienia elementu a, $x \neq y$.
Wówczas $a \wedge x = a \wedge y$, $a \vee x = a \vee y$, a więc $x = x \wedge (a \vee x) = x \wedge (a \vee y) = (x \wedge a) \vee (x \wedge y) = (y \wedge a) \vee (x \wedge y) \leqslant y$, i analogicznie $y \leqslant x$, czyli $x = y$ ↯.
(b) Niech np. $x \leqslant y$. Wówczas $x = x \vee (a \wedge x) = x \vee (a \wedge y) = (x \vee a) \wedge y = (y \vee a) \wedge y = y$.

39.
$\Rightarrow)$ HP: $\exists) \, x, y \in X : a \leqslant x \vee y$, $a \nleqslant x$, $a \nleqslant y$.
$a = a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y)$, $a = a \wedge x \quad \vee \quad a = a \wedge y$, $a \leqslant x \quad \vee \quad a \leqslant y$ ↯.
$\Leftarrow)$ HP: $\exists) \, x, y \in X : a = x \vee y$, $a \neq x$, $a \neq y$.
$a \leqslant x \quad \vee \quad a \leqslant y$. Jeśli np. $a \leqslant x$, to $a \leqslant x \leqslant x \vee y = a$, a więc $a = x$ ↯.

40. Fakty te wynikają wprost z przyjętych definicji. Na przykład relacja $a \leqslant b :\Leftrightarrow a \vee b = b$ jest porządkiem boole'owskim w X, gdyż jest porządkiem kratowym (zadanie 26), a więc $a \vee 0 = a$, $0 \leqslant a$, $0 = \min X$, oraz $a \leqslant b \Leftrightarrow a \wedge b = a$, skąd $a \wedge 1 = a$, $a \leqslant 1$, $1 = \max X$.

41. $(a \vee b) \vee (a^\neg \wedge b^\neg) = (a \vee b \vee a^\neg) \wedge (a \vee b \vee b^\neg) = (b \vee 1) \wedge (a \vee 1) = 1 \wedge 1 = 1$,
$(a \vee b) \wedge (a^\neg \wedge b^\neg) = (a \wedge a^\neg \wedge b) \vee (b \wedge a^\neg \wedge b^\neg) = (b \wedge 0) \vee (a \wedge 0) = 0 \vee 0 = 0$.
Prawa (*) wynikają z praw de Morgana.

42.

(a) Dla $\mathcal{A} \subset \mathcal{P}X : \sup \mathcal{A} = \bigcup \mathcal{A}$, $\inf \mathcal{A} = X \cap \bigcap \mathcal{A}$.

(b) Dla $\mathcal{R} \subset \operatorname{Equ} X : \sup \mathcal{R} = (\bigcup \mathcal{R})^- = \bigcap \{R \in \operatorname{Equ} X \mid \bigcup \mathcal{R} \subset R\}$, $\inf \mathcal{R} = X^2 \cap \bigcap \mathcal{R}$.

(c) Dla $\mathcal{A} \subset \mathcal{E} : \bigcup \mathcal{A} \in \mathcal{E}$ $\quad\langle$HP: $\bigcup \mathcal{A} \notin \mathcal{E}$, $\exists)\, \varphi \in \Phi : \varphi(\bigcup \mathcal{A}) \not\subset \bigcup \mathcal{A}$, $\exists)\, x \in \bigcup \mathcal{A} : \varphi(x) \notin \bigcup \mathcal{A}$, $\exists)\, A \in \mathcal{A} : x \in A$. $A \in \mathcal{E}$, $\varphi(A) \subset A$, $\varphi(x) \in A \subset \bigcup \mathcal{A}$ ↯$\rangle$, a więc $\sup \mathcal{A} = \bigcup \mathcal{A}$.
Analogicznie $\varnothing \neq \mathcal{A} \subset \mathcal{E} \;\Rightarrow\; \bigcap \mathcal{A} \in \mathcal{E}$, a więc $\inf \mathcal{A} = X \cap \bigcap \mathcal{A}$.

43. Wystarczy udowodnić (a) (dualność).
Oznaczmy $A = \{x \in X \mid x \leqslant f(x)\}$, $a = \sup A$. Wówczas $x \in A \;\Rightarrow\; x \leqslant a$, $x \leqslant f(x) \leqslant f(a)$, a więc $f(a) \in M(A)$, $a \leqslant f(a)$, $f(a) \leqslant f(f(a))$, $f(a) \in A$, $f(a) \leqslant a$, czyli $f(a) = a$, $a \in P$.

Ponieważ $P \subset A$, więc $x \in P \;\Rightarrow\; x \leqslant a$, czyli $a = \max P$.

44. Odwzorowanie φ ma punkt stały $A \subset X$, gdyż jest rosnące; $A = \varphi(A) = X \setminus g(Y \setminus f(A))$, i wówczas $B = X \setminus A = g(D)$, gdzie $D = Y \setminus C$, $C = f(A)$.

45.

(1) Jeżeli $a \in B$, to $x \in A \;\Rightarrow\; x \in B$, $x \leqslant a$, a więc $a \in M_B(A) \subset M(A)$.
$\forall\, a' \in M_B(A) : a' \in M(A)$, $a \leqslant a'$, a więc $a = \sup_B A$.

(2) Zakładamy, że $b = \sup_B A \in B$.
Wówczas $\forall\, x \in A : x \leqslant b$, a więc $b \in M(A)$, $a \leqslant b$.

(3) Jeżeli $\varnothing \neq A \subset B$, to $a \in B$ $\quad\langle\exists)\, x \in A$. Wówczas $x \leqslant a$ oraz $x \in B$, czyli $c \leqslant x$, a więc $c \leqslant a$, $a \in [c, \cdot\,] = B\rangle$, zatem wg (1) $a = \sup_B A$.
Oczywiście $\sup_B \varnothing = c$.

46*. HP: $\exists)\, A \subset P : \sup_P A = \mathbb{V}$.
Oznaczmy $a = \sup A = \sup_X A$. Wówczas $a \notin P$ $\quad\langle$wg 45.(1)$\rangle$ oraz

$$f([a, \cdot\,]) \subset [a, \cdot\,]$$

$\langle$HP: $\exists)\, x \in [a, \cdot\,] : f(x) \notin [a, \cdot\,]$.
$a \leqslant x$, $f(a) \leqslant f(x)$.
$y \in A \;\Rightarrow\; y \leqslant a$, $f(y) \leqslant f(a)$, $y = f(y) \leqslant f(x)$. Zatem $f(x) \in M(A)$, $a \leqslant f(x)$, $f(x) \in [a, \cdot\,]$ ↯$\rangle$.

Według 45.(3) przedział $[a, \cdot\,]$ jest kratą zupełną, a więc na podstawie twierdzenia Tarskiego o punkcie stałym $b = \min\{x \in [a, \cdot\,] \mid f(x) = x\} \in [a, \cdot\,]$. Tak więc $b = \min([a, \cdot\,] \cap P)$.

Wówczas $b = \sup_P A$ ↯
$\langle$ 1°) $x \in A \Rightarrow x \leqslant a \leqslant b$, a więc $b \in M_P(A)$.
2°) Niech $b' \in M_P(A)$. Tak więc $b' \in P$ i $x \in A \Rightarrow x \leqslant b'$. Zatem $b' \in M(A)$, $a \leqslant b'$, czyli $b' \in [a, \cdot\,] \cap P$, $b \leqslant b'\rangle$.

47*. Określamy odwzorowanie $\varphi : S^-(X) \to S^-(X)$, kładąc dla $A \in S^-(X) : \varphi(A) = X \setminus g(Y \setminus f(A))$. $\langle$Określenie jest poprawne, gdyż $f(A) \in S^-(Y') \subset S^-(Y)$, a więc $Y \setminus f(A) \in S^+(Y)$, $g(Y \setminus f(A)) \in S^+(X') \subset S^+(X)\rangle$.

Odwzorowanie φ jest rosnące $\langle \dots \rangle$, a więc według twierdzenia Tarskiego (zadanie 43) ma punkt stały $A \in S^-(X)$; $A = \varphi(A)$, $X \setminus A = g(Y \setminus f(A))$.

Określamy $h : X \to Y$, $h(x) = \begin{cases} f(x), & \text{gdy } x \in A \\ g^{-1}(x), & \text{gdy } x \in X \setminus A. \end{cases}$

Wówczas:

1) $h : X \twoheadrightarrow Y$ $\langle$HP: $\exists)\, y \in Y : y \notin h(X)$. Gdyby $y \in f(A)$, to $\exists\, x \in A : y = f(x) = h(x) \in h(X)$ ↯, zatem $y \in Y \setminus f(A)$, $g(y) = x \in X \setminus A$, $y = g^{-1}(x) = h(x) \in h(X)$ ↯$\rangle$.
2) $h : X \hookrightarrow Y$ $\langle$HP: $\exists)\, x, z \in Y : x \neq z$, $h(x) = h(z)$. Ze względu na symetrię sytuacji wystarczy rozważyć przypadek, gdy $x \in A$, $z \in X \setminus A$; wówczas $f(A) \ni f(x) = g^{-1}(z) \in Y \setminus f(A)$ ↯$\rangle$.
3) Bijekcja h spełnia warunek (*).
$\langle$ HP: $\exists)\, x, z \in X : x < z$, $h(x) > h(z)$.

Cztery przypadki:
(i) $x, z \in A$. Wówczas $h(x) = f(x) < f(z) = h(z)$ ↯.
(ii) $x \in A$, $z \notin A$. Wówczas $h(z) = g^{-1}(z) \in g^{-1}(X \setminus A) = Y \setminus f(A) \in S^+(Y)$, a więc $f(x) = h(x) \in Y \setminus f(A)$ ↯.
(iii) $x \notin A$, $z \in A$. Wówczas $x < z \in A \in S^-(x)$, a więc $x \in A$ ↯.
(iv) $x, z \in X \setminus A$. Wówczas $h(x) = g^{-1}(x) < g^{-1}(z) = h(z)$ ↯$\rangle$.

48*. HP: $\exists)\, F : X \twoheadrightarrow S^-(X)$, $\forall\, x, y \in X : x \leqslant y \implies F_x \subset F_y$. Wówczas $A := \{x \in X \mid x \notin F_x\} \subset B := \bigcup_{a \in A} [\,\cdot\,, a] \in S^-(X)$, a więc $\exists)\, x \in X : B = F_x$.
$x \notin A$ $\langle$HP: $x \in A$, wówczas $x \in B = F_x$, a więc $x \notin A$ ↯$\rangle$. Zatem $x \in F_x = B$, a więc $\exists)\, a \in A : x \in [\,\cdot\,, a]$, i wówczas $x \leqslant a$, $B = F_x \subset F_a$, i ponieważ $A \subset B$, więc $a \in B$, $a \in F_a$, $a \notin A$ ↯.

49. HP $\exists)\, f : X \xrightarrow{\sim} X$, $f \neq \mathrm{id}_X$.
$\forall\, x \in X : x \leqslant f(x)$ $\langle$lemat o przesunięciu w prawo$\rangle$.
Ponieważ również $f^- : X \xrightarrow{\sim} X$, więc $\forall\, x \in X : x \leqslant f^{-1}(x)$, $f(x) \leqslant f(f^{-1}(x)) = x$, zatem $\forall\, x \in X : f(x) = x$, $f = \mathrm{id}_X$ ↯.

50. Natychmiastowy wniosek z 49. $\langle$Gdyby jeszcze $g : X \xrightarrow{\sim} Y$, to $g^{-1} \circ f : X \xrightarrow{\sim} X$, a więc $g^{-1} \circ f = \mathrm{id}_X$, $f = g\rangle$.

51. HP: $A = \{x \in X \mid g(x) < f(x)\} \neq \varnothing$.
Niech $a = \min A$.

Wówczas $g(a) < f(a)$, $g(a) \in \operatorname{Im} f$, $\exists)\, x \in A : g(a) = f(x)$, $f(x) < f(a)$, $x < a$, czyli $f(x) \leqslant g(x) < g(a) = f(x)$ ↯.

52*.

1) R spójna w X

$\langle$HP: $\exists)\, x, z \in X : \neg(x \underset{R}{\leqslant} z \vee z \underset{R}{\leqslant} x)$.

Wówczas $f(x) = f(z)$ i, ponieważ $x \leqslant z \vee z \leqslant x$, więc $x \underset{R}{\leqslant} z \vee z \underset{R}{\leqslant} x$ ↯$\rangle$.

2) HP: $\exists)\, \varnothing \neq A \subset X : \neg\exists\, a$ – element R-minimalny A.

$\varnothing \neq f(A) \subset Y$. $\exists)\, b$ – minimum $f(A)$.

$\varnothing \neq A' = \{a \in A \mid f(a) = b\} \subset A$. $\exists)\, a$ – minimum A'.

$a \in A$, $\exists)\, x \in A : x \underset{R}{<} a$, $f(x) < f(a) \vee [f(x) = f(a) \wedge x < a]$.

$x \in A'$ $\langle$HP: $x \notin A'$. $f(x) \neq b = f(a)$, $f(x) < f(a)$, $f(x) < b$, $f(x) \notin f(A)$, $x \notin A$ ↯$\rangle$.

$f(x) = b = f(a)$, $x < a \leqslant x$ ↯.

5

Liczby porządkowe, liczby naturalne

5.1. Wstęp

Wprowadzone w rozdziale 3. liczby naturalne $0, 1, 2, \ldots$, jako zbiory $0 = \varnothing$, $1 = \{0\}$, $2 = \{0, 1\}$, i ogólnie $n + 1 = \operatorname{seq} n = n \cup \{n\} = \{0, 1, \ldots, n\}$ mają następujące dwie własności:

1° są tranzytywne ($x \in n \implies x \subset n$)

2° są spójne ze względu na relację $x \in y \vee x = y$ (przynależność lub równość).

To spostrzeżenie prowadzi do ogólnie przyjętej definicji liczby porządkowej Johna von Neumanna z roku 1928 (samo pojęcie liczby porządkowej wprowadził Georg Cantor w roku 1880).

(1) $\mathbb{E} := \{(x, y) \mid x \in y \vee x = y\}$

(2) A – *liczba porządkowa* $:\iff$ A – tranzytywna $\wedge$ $\mathbb{E}$ – spójna w A.

Tak więc klasa A jest liczbą porządkową wtt, gdy $\forall\, x, y \in A : x \subset A \;\wedge\; (x \in y \vee y \in x \vee x = y)$.

(3) $\mathrm{Ord} := \{\alpha \mid \alpha$ – liczba porządkowa$\}$.

Jest to klasa wszystkich liczb porządkowych będących zbiorami (*Ordinal numbers*). Łatwo widać, że $\alpha \in \mathrm{Ord} \Rightarrow \operatorname{seq} \alpha \in \mathrm{Ord}$, a więc $0, 1, 2, \cdots \in \mathrm{Ord}$.

(4) *Twierdzenie o dobrym porządku*:
A – liczba porządkowa $\Rightarrow$ $\mathbb{E}$ – dobry porządek w $A \wedge \forall\, a \in A : S_a(A, \mathbb{E}) = a$ $\langle$wniosek z kryterium Tarskiego$\rangle$.

W dalszym ciągu będziemy mówili, że $\mathbb{E}$ jest *naturalnym porządkiem* w liczbie porządkowej A i literę $\mathbb{E}$ będziemy opuszczali, pisząc dla $a, b \in A : a \leqslant b, a < b$ zamiast $a \underset{\mathbb{E}}{\leqslant} b, a \underset{\mathbb{E}}{<} b$.

Zbierzmy elementarne własności liczb porządkowych:

(5) A – liczba porządkowa $\wedge$ $B \subsetneq A$ $\wedge$ B – tranzytywna $\implies$ $B \in A$ $\langle B$ – $\mathbb{E}$-odcinek A, $\exists)\, a$ – $\mathbb{E}$-minimum $A \setminus B$, $B = S_a(A, \mathbb{E}) = a\rangle$.

(6) A, B – liczby porządkowe $\Rightarrow$ $(A \subsetneq B \Leftrightarrow A \in B)$ $\langle$wg (5)$\rangle$.

(7) A – liczba porządkowa $\Rightarrow$ $A \subset \mathrm{Ord}$ $\langle \forall\, x \in y \in a \in A : a \subset A$, $x, y \in A$, $x < y < a$, $x < a$, $x \in a\rangle$.

(8) Ord – liczba porządkowa. $\langle$Tranzytywność wg (7). Spójność: $\forall\, \alpha, \beta \in \mathrm{Ord}$: $\alpha \cap \beta \subset \alpha$, $\alpha \cap \beta \subset \beta$, a więc wg (1) $\alpha \cap \beta = \alpha \vee \alpha \cap \beta = \beta$, $\alpha \subset \beta \vee \beta \subset \alpha$ i wg (6) $\alpha \leqslant \beta \vee \beta \leqslant \alpha\rangle$.

(9) $\mathrm{Ord} \notin \mathbb{V}$ $\langle$HP: $\mathrm{Ord} \in \mathbb{V}$; wówczas wg (8): $\mathrm{Ord} \in \mathrm{Ord}$ ↯$\rangle$.

Tak więc nie istnieje zbiór wszystkich liczb porządkowych. Klasa Ord wszystkich liczb porządkowych jest właściwa i jest jedyną liczbą porządkową nie będącą zbiorem (antynomia Burali–Fortiego z 1897r.). W dalszym ciągu zamiast „A – liczba porządkowa” będziemy też pisali: $A \leqslant \mathrm{Ord}$ ($A \leqslant \mathrm{Ord} \Leftrightarrow A \in \mathrm{Ord} \vee A = \mathrm{Ord}$).

(10) $\varnothing \neq C \subset \mathrm{Ord} \;\Rightarrow\; \bigcap C$ – $\mathbb{E}$-minimum C.
$\langle \exists \rangle\, \alpha \in C$, $\bigcap C \subset \alpha$, a więc $\gamma := \bigcap C \in \mathrm{Ord}$. $\forall\, \alpha \in C : \gamma \subset \alpha$, $\exists\, \alpha \in C, \gamma = \alpha$, więc $\gamma \in C$. $\forall\, \alpha \in C : \gamma \subset \alpha, \gamma \leqslant \alpha \rangle$.
Zamiast $\bigcap C$ będziemy też pisać $\min C$.

(11) $C \subset \mathrm{Ord} \;\Rightarrow\; \bigcup C \leqslant \mathrm{Ord}$
$\langle$wg (8) $\bigcup C \subset \bigcup \mathrm{Ord} \subset \mathrm{Ord}$, więc $\mathbb{E}$ – spójna w $\bigcup C$. Tranzytywność klasy $\bigcup C$ wynika wprost z definicji pojęcia liczby porządkowej$\rangle$.

W tym kontekście piszemy też $\sup C := \bigcup C$, gdyż dla $C \in \mathbb{V}$ jest: $\sigma = \bigcup C \in \mathrm{Ord}$ oraz

1° $\forall\, \gamma \in C\;\gamma \leqslant \sigma$
2° $\forall\, \tau \in \mathrm{Ord}\; [(\forall\, \gamma \in C\; \gamma \leqslant \tau) \;\Rightarrow\; \sigma \leqslant \tau]$.

Natomiast jeżeli $C \notin \mathbb{V}$, to $\bigcup C = \mathrm{Ord}$.

Wprowadzamy pojęcie liczby porządkowej granicznej:

(12) A – *liczba porządkowa graniczna* $:\Longleftrightarrow\; O \neq A \leqslant \mathrm{Ord} \;\wedge\; \forall\, \alpha \in \mathrm{Ord}\; A \neq \mathrm{seq}\, \alpha$.
Oczywiście klasa Ord jest liczbą porządkową graniczną.

(13) $\mathrm{Lim} := \{\lambda \mid \lambda$ – liczba porządkowa graniczna$\}$.

(14) $\mathrm{Lim} \neq \varnothing$
$\langle$według aksjomatu nieskończoności klasa Univ wszystkich zbiorów uniwersalnych jest niepusta (tu pierwszy raz korzystamy z aksjomatu nieskończoności) i — jak łatwo sprawdzić — $\forall\, u \in \mathrm{Univ} : u \cap \mathrm{Ord} \in \mathrm{Lim}\rangle$.

Zbiór *liczb naturalnych* określamy jako najmniejszą liczbę porządkowa graniczną. Używamy podwójnego oznaczenia:

(15) $\omega = \mathbb{N} := \bigcap \mathrm{Lim}$ (analogia z $0 = \varnothing$).

Z powyższej definicji wynika, że $0 \in \mathbb{N}$ oraz $\alpha \in \mathbb{N} \;\Rightarrow\; \mathrm{seq}\, \alpha \in \mathbb{N}$, a więc $1 \in \mathbb{N}$, $2 \in \mathbb{N}, \ldots$

W aksjomatyce ZFC_0 (A1 – A8) definicję $\mathbb{N}$ należałoby zmodyfikować: $\mathbb{N} = \mathrm{Ord} \cap \bigcap \mathrm{Lim}$, i wówczas aksjomat nieskończoności byłby równoważny zdaniu $\mathbb{N} \in \mathrm{Ord}$, zaś jego negacja zdaniu $\mathbb{N} = \mathrm{Ord}$.

Natychmiastowym wnioskiem z zasady minimum dla relacji dobrego porządku jest *zasada indukcji*:

(16) $A \leqslant \mathrm{Ord} \;\wedge\; \forall\, \alpha \in A\, (\alpha \subset C \;\Rightarrow\; \alpha \in C) \;\Rightarrow\; A \subset C$.
Drugi człon tej koniunkcji nazywamy *warunkiem indukcyjnym* (C jest dowolną klasą).
$\langle$HP: $\ldots$, $A \not\subset C$; dla $\alpha = \bigcap (A \setminus C) = \min(A \setminus C)$ jest $\alpha \in A \setminus C$ i $\forall\, \xi \in A \setminus C : \alpha \leqslant \xi$. $\forall\, \xi < \alpha : \xi \in A, \xi \in C$, a więc $\alpha \subset C$ i — na mocy warunku indukcyjnego — $\alpha \in C$ ↯$\rangle$.

Zwykle stosuje się zasadę indukcji w tak zwanej *wersji praktycznej*:

(17) $A \leqslant \mathrm{Ord} \ \wedge\ 0 \in C \ \wedge\ \forall\, \alpha \in A\, (\alpha \in C \ \Rightarrow\ \mathrm{seq}\, \alpha \in C)$
$\wedge\ \forall\, \lambda \in A \cap \mathrm{Lim}\, (\lambda \subset C \ \Rightarrow\ \lambda \in C) \,.\!\Rightarrow\ A \subset C.$

W szczególności dla $A = \mathbb{N}$ otrzymujemy:

(18) $0 \in C \wedge \forall\, n \in \mathbb{N}\, (n \in C \ \Rightarrow\ \mathrm{seq}\, n \in C) \,.\!\Rightarrow\ \mathbb{N} \subset C.$
⟨Dla $\alpha \in A$, $\alpha \subset C$ rozpatrujemy trzy przypadki – zerowy, sekwensowy i graniczny – w każdym z nich $\alpha \in C$⟩.

Jest to jeden z najczęściej stosowanych tak zwanych *schematów dowodzenia indukcyjnego*. W dalszym ciągu tego rodzaju schematy będziemy stosowali bez komentarza, gdyż równie łatwo można je sprowadzić do ogólnej zasady indukcji (16).

Z zasadą indukcji związane jest twierdzenie o definiowaniu indukcyjnym ciągów (skrótowo mówiąc jest to twierdzenie o indukcji + twierdzenie o sklejaniu funkcji).

Ciągiem nazywamy każdą funkcję, której dziedzina jest liczbą porządkową. Ciąg $a : \mathbb{N} \to \mathbb{V}$ nazywamy *przeliczalnym*; ciąg $a : n \to \mathbb{V}$, gdzie $n \in \mathbb{N}$, nazywamy *skończonym*. Zwyczajowo ciągami nazywamy też funkcje $a : \mathbb{N}^* \to \mathbb{V}$, $a : I_n \to \mathbb{V}$ $(n \in \mathbb{N})$ itp.

Mówimy, że ciąg f jest *zdefiniowany indukcyjnie przez* H, gdy $\forall\, \alpha \in \mathrm{Ord} : f(\alpha) = H(f|\alpha)$ — jest to tzw. *warunek indukcyjny*. Jeśli tak jest, to dla liczby porządkowej $\alpha \notin A = \mathrm{Dom}\, f$: $A \subset \alpha$, $f|\alpha = f$ i $\mathbb{V} = f(\alpha) = H(f)$ (na ogół $H : \mathbb{V} \multimap \mathbb{V}$).

(19) *Lemat o jednoznaczności*:
f, g – ciągi zdefiniowane indukcyjnie przez $H \ \Rightarrow\ f = g$.
⟨Indukcją na $\alpha \in \mathrm{Ord}$ pokazujemy, że $f(\alpha) = g(\alpha)$⟩.

(20) *Twierdzenie o definiowaniu indukcyjnym*:
$\Phi = \{\varphi \mid \varphi$ – ciąg $\wedge\, \forall\, \alpha \in \mathrm{Dom}\, \varphi : \varphi(\alpha) = H(\varphi|\alpha)\} \wedge f = \bigcup \Phi \,.\!\Rightarrow\ f$ – ciąg określony indukcyjnie przez H.
⟨Z twierdzenia o sklejaniu funkcji i zasady indukcji wynika, że f jest funkcją; f jest ciągiem, gdyż $A = \mathrm{Dom}\, f = \bigcup\{\mathrm{Dom}\, \varphi \mid \varphi \in \Phi\} \leqslant \mathrm{Ord}$. Jeśli $\alpha \in A$, to $\exists)\, \varphi \in \Phi :$ $\alpha \in \mathrm{Dom}\, \varphi$, i wówczas $f(\alpha) = \varphi(\alpha) = H(\varphi|\alpha) = H(f|\alpha)$. Dla $\alpha \in \mathrm{Ord} \setminus A : \neg\, \alpha < A$, $A \subset \alpha$ i $H(f) = \mathbb{V}$, bo gdyby $c = H(f) = \mathbb{V}$, to $c \in \mathbb{V}$, $\varphi = f \cup \{A \mapsto c\} \in \Phi$, a więc $A \in \mathrm{Dom}\, \varphi \subset \mathrm{Dom}\, f = A$ ↯⟩.

Podobnie jak dla zasady indukcji mamy różne – łatwo sprowadzalne do (20) – *schematy definiowania indukcyjnego*.

Najprostszym i najważniejszym jest

(21) *Twierdzenie o definiowaniu indukcyjnym – wersja praktyczna*:

Niech A będzie liczbą porządkową graniczną, $c \in C$, $M : A \times C \to C$, $N : \bigcup\limits_{\lambda \in A \cap \mathrm{Lim}} \mathrm{Map}(\lambda, C) \to C$. W tej sytuacji mówiąc: „określamy indukcyjnie ciąg $f : A \to C$ spełniający warunki (*wstępny*, *sekwensowy*, *graniczny*): $f(0) = c$, $\forall\, \alpha \in A : f(\mathrm{seq}\, \alpha) = M(\alpha, f(\alpha))$, $\forall\, \lambda \in A \cap \mathrm{Lim} : f(\lambda) = N(f|\lambda)$”, mamy na myśli ciąg f zdefiniowany indukcyjnie warunkiem $\forall\, \alpha \in \mathrm{Ord} : f(\alpha) = H(f|\alpha)$, gdzie $H : \bigcup\limits_{\alpha \in A} \mathrm{Map}(\alpha, C) \to \mathbb{V}$, $H(0) = c$, $\alpha \in A \wedge \varphi : \mathrm{seq}\, \alpha \to C \ \Rightarrow\ H(\varphi) = M(\alpha, \varphi(\alpha))$, $\lambda \in A \cap \mathrm{Lim} \ \wedge\ \varphi : \lambda \to C \implies H(\varphi) = N(\varphi)$.

Tak określony ciąg spełnia powyższe warunki $\langle$przeliczenie$\rangle$ i jest przez nie wyznaczony jednoznacznie $\langle$wykazujemy indukcyjnie, że taki ciąg f spełnia warunek $\forall\,\alpha \in \mathrm{Ord} : f(\alpha) = H(f|\alpha)\rangle$.

(22) *Twierdzenie o uniwersalności liczb porządkowych*:
Jeżeli R – dobry porządek w C, f – ciąg określony warunkiem indukcyjnym $\forall\,\alpha \in \mathrm{Ord} : f(\alpha) = \bigcap\{x \mid x - R\text{-minimum } C \setminus \mathrm{Im}(f|\alpha)\}$ i $A = \mathrm{Dom}\, f$, to

(a) $f : A \hookrightarrow\!\!\!\!\rightarrow C \wedge f - \mathbb{E}\text{-}R\text{-rosnąca}$

(b) $B \leqslant \mathrm{Ord} \;\;\wedge\;\; g : B \hookrightarrow\!\!\!\!\rightarrow C \;\;\wedge\;\; g - \mathbb{E}\text{-}R\text{-rosnąca} \implies f = g$.

$\langle$Ad (a): $\forall\,\alpha \in A\;\, f(\alpha) - R$-minimum $C \setminus \mathrm{Im}(f|\alpha)$, a więc $f : A \hookrightarrow C$, f – $\mathbb{E}$-R-rosnąca. Gdyby $\mathrm{Im}\, f \subsetneq C$, to $\mathrm{Im}\, f$ – R-odcinek C, $\exists)\, c$ – R-minimum $C \setminus \mathrm{Im}\, f$, i wówczas $\mathrm{Im}\, f = S_c(C, R) \in \mathbb{V}$, $A \in \mathrm{Ord}$, $\mathbb{V} = f(A) = c \in \mathbb{V}$ ↯.
Ad (b): Wystarczy wykazać, że ciąg g spełnia ten sam warunek indukcyjny co f. Przypuśćmy więc, że $\exists)\, \alpha \in \mathrm{Ord} : g(\alpha) \neq \bigcap\{x \mid x - R\text{-minimum } C \setminus \mathrm{Im}(g|\alpha)\}$. Wówczas $\alpha \in B$, $g(\alpha)$ – R-minimum $C \setminus \mathrm{Im}(g|\alpha)$ ↯$\rangle$.

W sytuacji opisanej przez powyższe twierdzenie będziemy używali następującej notacji i terminologii:
typ porządkowy C względem R $= \mathrm{ord}(C, R) := A$
naturalna numeracja C względem R $= \mathrm{nat}_{C,R} := f$.
Dla $C \subset \mathrm{Ord}$ piszemy $\mathrm{ord}\, C := \mathrm{ord}(C, \mathbb{E})$, $\mathrm{nat}_C := \mathrm{nat}_{C,\mathbb{E}}$; tak więc $\mathrm{ord}\, C \leqslant \mathrm{Ord}$ i $\mathrm{nat}_C : \mathrm{ord}\, C \hookrightarrow\!\!\!\!\rightarrow C$, nat_C – rosnąca. $\alpha \in \mathrm{Ord} \Rightarrow \mathrm{ord}\, \alpha = \alpha$.
Jeżeli $C \subset \alpha \in \mathrm{Ord}$, to $\mathrm{ord}\, C \leqslant \alpha$ $\langle$HP: $\alpha < \gamma = \mathrm{ord}\, C$. Wówczas dla $f = \mathrm{nat}_C : \gamma \to C$, $\alpha \leqslant f(\alpha) \in C \subset \alpha$ ↯$\rangle$.

Arytmetyka porządkowa

Działania *dodawania*, *mnożenia* i *potęgowania* liczb porządkowych $+, \cdot, ^\wedge : \mathrm{Ord}^2 \to \mathrm{Ord}$ określamy indukcją względem drugiego członu pary $(\alpha, \beta) \in \mathrm{Ord}^2$.

(23) $\alpha + 0 = \alpha$, $\alpha + \mathrm{seq}\, \beta = \mathrm{seq}(\alpha + \beta)$, $\beta \in \mathrm{Lim} \;\Rightarrow\; \alpha + \beta = \bigcup\limits_{\eta<\beta} \alpha + \eta$.

Ponieważ $\alpha + 1 = \alpha + \mathrm{seq}\, 0 = \mathrm{seq}(\alpha + 0) = \mathrm{seq}\, \alpha$, więc w dalszym ciągu dla $\alpha \in \mathrm{Ord}$ zamiast $\mathrm{seq}\, \alpha$ będziemy używali tradycyjnego zapisu $\alpha + 1$.

(24) $\alpha \cdot 0 = 0$, $\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha$, $\beta \in \mathrm{Lim} \;\Rightarrow\; \alpha \cdot \beta = \bigcup\limits_{\eta<\beta} \alpha \cdot \eta$.

Przyjmujemy wszystkie powszechnie stosowane konwencje notacyjne: kolejność działań, opuszczanie zbędnych nawiasów i kropki mnożenia (tak więc $\alpha + \beta\gamma$ oznacza $\alpha + (\beta \cdot \gamma)$ itp.).
Dla potęgowania będziemy również używali tradycyjnej notacji $\alpha^\beta := \alpha{}^\wedge\beta$.

(25) $\alpha^0 = 1$, $\alpha^{\beta+1} = \alpha^\beta\alpha$, $\beta \in \mathrm{Lim} \;\Rightarrow\; \alpha^\beta = \bigcup\limits_{\eta<\beta} \alpha^\eta$.

Niech $\alpha, \beta, \gamma, \delta \in \mathrm{Ord}$, $\lambda \in \mathrm{Lim}$, $m, n \in \mathbb{N} = \omega$.

(26) $0 + \alpha = \alpha$. $\langle$Indukcja na α. Podobnie dla dalszych praw arytmetyki porządkowej – indukcja względem ostatniego członu równości (nierówności) lub bezpośrednio z definicji$\rangle$.

(27) $\alpha + \lambda \in \mathrm{Lim}$

(28) $\beta < \gamma \ \Rightarrow \ \alpha + \beta < \alpha + \gamma$

(29) $\beta \leqslant \gamma \ \Rightarrow \ \beta + \alpha \leqslant \gamma + \alpha$ (tu nie można dać nierówności silnej; np. $0 < 1$, ale $0 + \omega = \omega = 1 + \omega$)

(30) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ (prawo przemienności nie jest spełnione; np. $1 + \omega = \omega < \omega + 1$)

(31) $0 \cdot \alpha = 0$, $1 \cdot \alpha = \alpha \cdot 1 = \alpha$

(32) $\alpha \neq 0 \wedge \beta < \gamma \ \Rightarrow \ \alpha\beta < \alpha\gamma$

(33) $\beta \leqslant \gamma \ \Rightarrow \ \beta\alpha \leqslant \gamma\alpha$ (nierówności silnej nie można tu położyć nawet dla $\alpha \neq 0$; np. $1 < 2$, ale $1 \cdot \omega = \omega = 2 \cdot \omega$)

(34) $\alpha \neq 0 \ \Rightarrow \ \alpha\lambda \in \mathrm{Lim}$

(35) $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ (prawo przemienności mnożenia nie jest spełnione; np. $2 \cdot \omega = \omega < \omega \cdot 2 = \omega + \omega$)

(36) $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$ (prawo rozdzielności lewostronnej mnożenia względem dodawania). Prawostronna rozdzielność nie zachodzi. Np. $(1+1)\omega = 2\omega = \omega < 1\cdot\omega + 1\cdot\omega = \omega + \omega$.

(37) $\exists!\, \lambda \in \mathrm{Lim}_0,\ n \in \mathbb{N} : \alpha = \lambda + n$, gdzie $\mathrm{Lim}_0 := \mathrm{Lim} \cup \{0\}$ $\langle$zadanie 10$\rangle$.
Natomiast $\alpha \geqslant \omega \ \Rightarrow \ n + \alpha = \alpha$ $\langle$indukcja na $\alpha\rangle$.

(38) $m + n, mn, m^n \in \mathbb{N}$, $m + n = n + m$, $mn = nm$ $\langle$zadanie 11$\rangle$

(39) $\alpha \leqslant \beta \ \Rightarrow \ \exists!\, \gamma \in \mathrm{Ord} : \alpha + \gamma = \beta$;
określamy *różnicę* $\beta - \alpha = \gamma$, tak więc dla $\alpha \leqslant \beta : \alpha + (\beta - \alpha) = \beta$ $\langle$Zadanie 12*$\rangle$.

(40) Prawa dla odejmowania:

(i) $\alpha - \alpha = 0$, $\alpha - 0 = \alpha$
(ii) $\alpha < \lambda \ \Rightarrow \ \lambda - \alpha \in \mathrm{Lim}$
(iii) $\alpha \leqslant \beta < \gamma \ \Rightarrow \ \beta - \alpha < \gamma - \alpha$
(iv) $\alpha \leqslant \beta \leqslant \gamma \ \Rightarrow \ \gamma - \beta \leqslant \gamma - \alpha$ (ale $0 < 1 < \omega$ i $\omega - 1 = \omega = \omega - 0$)
(v) $\alpha \leqslant \beta \ \Rightarrow \ \gamma(\beta - \alpha) = \gamma\beta - \gamma\alpha$ (ale $(2-1)\omega = \omega$ i $2 \cdot \omega - 1 \cdot \omega = \omega - \omega = 0$)
(vi) $\alpha + \beta - \alpha = \beta$
(vii) $\exists\, \alpha, \beta : \alpha + \beta - \beta < \alpha$ i $\exists\, \alpha, \beta : \alpha + \beta - \beta > \alpha$ $\langle$zadanie 13$\rangle$.

(41) *Twierdzenie o dzieleniu z resztą*:
$\beta \neq 0 \implies \exists!\, q, r \in \mathrm{Ord} : \alpha = \beta q + r \wedge r < \beta$ $\langle$zadanie 14$\rangle$,
jednoznacznie wyznaczone liczby q, r nazywamy odpowiednio *ilorazem* i *resztą* z dzielenia α przez β; oznaczamy $[\frac{\alpha}{\beta}] := q$, $\alpha \pmod{\beta} := r$.

Zauważmy, że $[\frac{\alpha}{\beta}] = q \leqslant \beta q + r = \alpha$, a więc $\alpha, \beta \in \mathbb{N} \wedge \beta \neq 0 \implies [\frac{\alpha}{\beta}]$, $\alpha \pmod{\beta} \in \mathbb{N}$.

Jeżeli $\alpha \pmod{\beta} = 0$, czyli $\alpha = \beta q$, to mówimy, że α jest *podzielne* przez β lub że β jest *dzielnikiem* α, co notujemy: $\beta \mid \alpha$, piszemy wówczas zwyczajowo $\frac{\alpha}{\beta}$ lub $\frac{1}{\beta} \cdot \alpha$ zamiast $[\frac{\alpha}{\beta}]$.

Definicję podzielności formułujemy ogólniej, dla dowolnych $\alpha, \beta \in \mathrm{Ord}$:

(42) $\beta \mid \alpha \ :\Longleftrightarrow \ \exists\, q \in \mathrm{Ord} : \alpha = \beta q$.

Relacja podzielności w klasie Ord ma następujące własności:

(i) $\alpha \mid 0$, $0 \mid \alpha \Leftrightarrow \alpha = 0$

(ii) $1 \mid \alpha$, $\alpha \mid 1 \Leftrightarrow \alpha = 1$

(iii) $\alpha \mid \beta \wedge \beta \neq 0 \ \Rightarrow \ \alpha \leqslant \beta$

(iv) relacja podzielności jest porządkiem (częściowym), tzn. $\alpha \mid \alpha$, $\alpha \mid \beta \wedge \beta \mid \gamma \ \Rightarrow \ \alpha \mid \gamma$, $\alpha \mid \beta \wedge \beta \mid \alpha \ \Rightarrow \ \alpha = \beta$

(v) $\alpha \mid \beta \wedge \alpha \mid \gamma \ \Rightarrow \ \forall\, \xi, \eta \in \mathrm{Ord} : \alpha \mid \beta\xi + \gamma\eta$

(vi) $\alpha \mid \beta \ \Rightarrow \ \alpha \mid \beta\gamma \wedge \gamma\alpha \mid \gamma\beta$

(vii) $\alpha, \beta, \gamma, \delta \in \mathbb{N} \wedge \alpha \mid \beta \wedge \gamma \mid \beta \ \Rightarrow \ \alpha\gamma \mid \beta\delta$

(viii) $\omega \mid \lambda$

$\langle$zadanie 15$\rangle$.

(43) Prawa dla potęgowania liczb porządkowych:

(i) $0^0 = 0^\lambda = 1$, $0^{\alpha+1} = 0$, $\beta > 0 \ \Rightarrow \ \beta^\alpha > 0$

(ii) $\alpha^1 = \alpha$, $1^\alpha = 1$, $\alpha^2 = \alpha\alpha$, $2^\omega = \omega$

(iii) $1 < \alpha \ \Rightarrow \ \alpha^\lambda, \lambda^\alpha \in \mathrm{Lim}$

(iv) $1 < \alpha \wedge \beta < \gamma \ \Rightarrow \ \alpha^\beta < \alpha^\gamma$

(v) $1 < \alpha \ \Rightarrow \ \gamma \leqslant \alpha^\gamma$

(vi) $1 < \alpha \leqslant \beta \ \Rightarrow \ \alpha^\gamma \leqslant \beta^\gamma$

(vii) $\alpha^{\beta+\gamma} = \alpha^\beta \alpha^\gamma$

(viii) $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$

$\langle$zadanie 16$\rangle$.

Działania dodawania i mnożenia liczb porządkowych uogólniamy na większa liczbę wyrazów.
Dla $\alpha \in \mathrm{Ord}$; $f, g : \alpha \longrightarrow \mathrm{Ord}$

$$\sum f = \sum_{\xi<\alpha} f(\xi) \in \mathrm{Ord}, \qquad \prod g = \prod_{\xi<\alpha} g(\xi) \in \mathrm{Ord},$$

indukcja na α:

(I) dla $\alpha = 0$: $\sum f = 0$, $\prod g = 1$

(II) dla $\alpha = \beta + 1$: $\sum f = \sum f|\beta + f(\beta)$
$\prod g = \prod f|\beta \cdot f(\beta)$

(III) dla $\alpha \in \mathrm{Lim}$: $\sum f = \bigcup\limits_{\xi<\alpha} \sum f|\xi$
$\prod g = \bigcup\limits_{\xi<\alpha} \prod g|\xi$.

Zamiast $\sum\limits_{n<\omega} f(n)$ piszemy też zwyczajowo $\sum\limits_{n=0}^{\infty} f(n)$ i analogicznie $\sum\limits_{n=1}^{\infty} f(n)$ itp.

Z powyższej definicji natychmiast widać, że:

$$\alpha = 1 \implies \sum f = f(0), \qquad \prod g = g(0)$$
$$\alpha = 2 \implies \sum f = f(0) + f(1), \qquad \prod g = g(0) \cdot g(1) \qquad \text{itd.}$$

Zamiast sumować po liczbie porządkowej α, sumujemy też po zbiorze A z ustalonym dobrym porządkiem typu α, np. dla $n \in \mathbb{N}$ i $a : I_n \to \mathrm{Ord}$, $\sum\limits_{k=1}^{n} a_k$ oznacza $\sum\limits_{k<n} a_{k+1}$. Często też używamy bardziej sugestywnej notacji wielokropkowej, pisząc np. $1 + 2 + 2^2 + \cdots + 2^{n-1}$ zamiast $\sum\limits_{k<n} 2^k$, $\sum\limits_{k=0}^{n-1} 2^k$.

Ważne jest:

(44) *Twierdzenie o rozwinięciu pozycyjnym*:
$\forall \underset{\gamma \geqslant 2}{\alpha, \gamma \in \mathrm{Ord}}\ \exists!\, k \in \mathbb{N},\ \xi : I_k \to \mathrm{Ord},\ \eta : I_k \to \gamma \setminus 1\ :$
$\xi_1 < \ldots < \xi_k \quad \wedge \quad \alpha = \gamma^{\xi_k}\eta_k + \cdots + \gamma^{\xi_1}\eta_1;$
parę (ξ, η) nazywamy *rozwinięciem pozycyjnym liczby* α *przy podstawie* γ – liczby ξ_i, η_i to odpowiednio *wykładniki* i *cyfry* tego rozwinięcia.

$\langle$zadania 34–37$\rangle$.

Zbiór równoliczny z liczbą naturalną nazywamy *skończonym*. Oznaczmy $\mathrm{Fin} := \{x \mid \exists n \in \mathbb{N} : x \sim n\}$ – klasa wszystkich zbiorów skończonych (*Finite sets*). Elementy klasy $\mathbb{V} \setminus \mathrm{Fin}$ to zbiory *nieskończone*. Oczywiście $\mathbb{N} \subset \mathrm{Fin}$. $\mathbb{N} \notin \mathrm{Fin}$ (zadanie 40).

Zbiór równoliczny z $\mathbb{N}$ nazywamy *przeliczalnym*. W literaturze często termin „przeliczalny” oznacza „skończony lub przeliczalny” – studiując jakiś tekst, trzeba zawsze starannie czytać definicje (i założenia twierdzeń). W dalszym ciągu, mówiąc o zbiorze X że jest *nieprzeliczalny*, będziemy mieli na myśli „nieskończony i nieprzeliczalny”.

Dla liczb naturalnych z równoliczności wynika równość:

(45) $\forall m, n \in \mathbb{N} : m \sim n \implies m = n.$
$\langle$Niech np. $m \leqslant n$. Indukcja na n:
I $\quad n = 0$. Wówczas $m = 0$, $m = n$.
II $\quad n > 0$ i implikacja zachodzi dla $n' < n$. Przypuśćmy, że $m < n$ i $m \sim n$. Wówczas też $m > 0$, a więc $\exists)\, k, l : m = k+1, n = l+1$. $\exists\, f : m \hookrightarrow\!\!\!\!\rightarrow n$, $f(k) = l \quad \langle\exists)\, f : m \hookrightarrow\!\!\!\!\rightarrow n$. Jeśli $f(k) = b \neq l$, to dla $a = f^{-1}(k)$: $\tilde{f} = (f \setminus \{k \mapsto b, a \mapsto l\}) \cup \{k \mapsto l, a \mapsto b\} : m \hookrightarrow\!\!\!\!\rightarrow n$, $\tilde{f}(k) = l\rangle$. Wówczas $f|k : k \hookrightarrow\!\!\!\!\rightarrow l$, czyli $k \sim l$, $k < l < n$ ↯$\rangle$.

Zatem dla zbioru skończonego x istnieje dokładnie jedna liczba naturalna n taka, że $x \sim n$; nazywamy ją *liczbą kardynalną* lub *mocą* zbioru x i oznaczamy $|x|$; dla $x, y \in \mathrm{Fin} : x \sim y \Leftrightarrow |x| = |y|$.

Z (38) wynika natychmiast, że dla zbiorów skończonych x, y:

$$(46) \quad \begin{cases} x \cap y = \varnothing \ \Rightarrow\ x \cup y \in \mathrm{Fin} \ \wedge\ |x \cup y| = |x| + |y| \\ x \times y \in \mathrm{Fin} \ \wedge\ |x \times y| = |x| \cdot |y| \\ \mathrm{Map}(x, y) \in \mathrm{Fin} \ \wedge\ |\mathrm{Map}(x, y)| = |y|^{|x|}. \end{cases}$$

Ponadto:

(47) $x \in \mathrm{Fin} \Rightarrow \mathcal{P}x \in \mathrm{Fin} \;\wedge\; |\mathcal{P}x| = 2^{|x|}$ $\quad\langle \mathcal{P}x \sim \mathrm{Map}(x,2)\rangle$.

Dalsze podstawowe własności zbiorów skończonych:

(48) $x \subset y \in \mathrm{Fin} \Rightarrow x \in \mathrm{Fin} \;\wedge\; |x| \leqslant |y|$, czyli podzbiór zbioru skończonego jest skończony. $\langle (\exists)\, f : y \hookrightarrow\!\!\!\!\!\twoheadrightarrow n = |y|$, $x' = \mathrm{Im}(f|x) \subset n$, $m = \mathrm{ord}\, x' \leqslant n$ $\quad\langle$por. (22)$\rangle$, zatem $x \sim x' \sim m \leqslant n\,\rangle$.

(49) $g : x \hookrightarrow y \wedge y \in \mathrm{Fin} \Rightarrow x \in \mathrm{Fin} \wedge |x| \leqslant |y|$. $\quad\langle$Uogólnienie (48): $x \sim \mathrm{Im}\, g \subset y\rangle$.

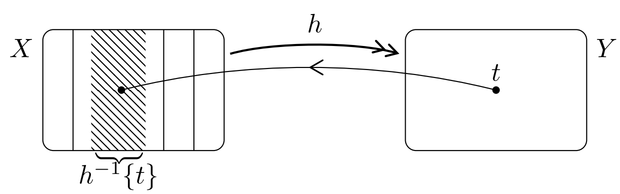
(50) $x, y \in \mathrm{Fin} \Longrightarrow x \cup y \in \mathrm{Fin} \;\wedge\; |x \cup y| \leqslant |x| + |y|$. $\quad\langle$Wniosek z (46)–(49), gdyż $\exists\, g : x \cup y \hookrightarrow (x \times \{0\}) \cup (y \times \{1\})$, np. $g = \{t \mapsto (t,0) \mid t \in x\} \cup \{s \mapsto (s,1) \mid s \in y \setminus x\}\rangle$.

Dla zbiorów skończonych aksjomat wyboru (AC) jest w ZF twierdzeniem, które oznaczamy $\mathrm{AC_{fin}}$:

(51) $\forall\, x \in \mathrm{Fin}\, [\varnothing \notin x \Longrightarrow \exists\, f : x \to \bigcup x\; \forall\, y \in x : f(y) \in y]$
$\langle$indukcja na $|x|\rangle$.

Z (51) wynika natychmiast dualny odpowiednik (49):

(52) $h : x \twoheadrightarrow y \wedge x \in \mathrm{Fin} \Rightarrow y \in \mathrm{Fin} \;\wedge\; |y| \leqslant |x|$
$\langle \varnothing \notin z = \{h^{-1}\{t\} \mid t \in y\} \subset \mathcal{P}x \in \mathrm{Fin}$, a więc $z \in \mathrm{Fin}$, i według $\mathrm{AC_{fin}}$ $\exists)\, f : z \to \bigcup z \subset x\; \forall\, t \in y : f(h^{-1}\{t\}) \in h^{-1}\{t\}$



i wówczas $\{t \mapsto f(h^{-1}\{t\}) \mid t \in y\} : y \hookrightarrow x$, a więc $y \in \mathrm{Fin}$ i $|y| \leqslant |x|\rangle$.

Dział matematyki zajmujący się szacowaniem i wyznaczaniem mocy zbiorów skończonych nazywamy *kombinatoryką*.

Jednym z podstawowych narzędzi kombinatoryki jest *zasada szufladkowa Dirichleta*:

(53) $x, y \in \mathrm{Fin} \wedge |x| > |y| \wedge f : x \twoheadrightarrow y \Rightarrow \exists\, t \in y\; |f^{-1}\{t\}| \geqslant 2$
(x – przedmioty, y – szufladki, f – wkładanie przedmiotów do szufladek)
$\langle$HP: $\forall\, t \in y\; |f^{-1}\{t\}| \leqslant 1$. Wówczas $f : x \hookrightarrow\!\!\!\!\!\twoheadrightarrow y$, $|x| = |y|$ $\lightning\rangle$.

Zasadę tę można wzmocnić, kładąc w następniku implikacji zamiast 2 pewną liczbę zależną od $|x|$, $|y|$ (zadanie 39). W angielskich szkołach wzmocnienie to nosi nazwę *pigeon hole principle*: jeżeli do trzech dziupli ($|y| = 3$) wskakuje siedem gołębi, to w co najmniej jednej dziupli będą siedzieć co najmniej trzy gołębie $\quad\langle$bo gdyby w każdej dziupli siedziały co najwyżej dwa, to byłoby ich co najwyżej sześć$\rangle$.

Drugim podstawowym narzędziem kombinatoryki jest *zasada klasyfikacji*:

(54) $\mathcal{A} \in \mathrm{Fin} \ \wedge \ \mathcal{A} \subset \mathrm{Fin} \implies \bigcup\mathcal{A} \in \mathrm{Fin} \ \wedge \ |\bigcup\mathcal{A}| \leqslant \sum\limits_{A\in\mathcal{A}} |A|$
$\wedge \ \big[(\forall\, A, B \in \mathcal{A} : A \neq B \ \Rightarrow \ A \cap B = \varnothing) \implies |\bigcup\mathcal{A}| = \sum\limits_{A\in\mathcal{A}} |A|\big]$ $\langle$indukcja na $|\mathcal{A}|\rangle$.

W szczególności:

(55) $X \in \mathrm{Fin} \ \wedge \ R \in \mathrm{Equ}\, X \wedge n \in \mathbb{N} \wedge \forall\, x \in X : \big|[x]_R\big| = n \implies |X| = |X/R| \cdot n$ (*teoriomnogościowa formuła Lagrange'a*).

W sytuacji (54), jeżeli znane są moce iloczynów zbiorów z $\mathcal{A}$, to można podać dokładny wzór na $|\bigcup\mathcal{A}|$. Jest to tzw. *formuła włączania-wyłączania*:

(56) $A, B \in \mathrm{Fin} \ \Rightarrow \ |A \cup B| = |A| + |B| - |A \cap B|$
$\langle A \cup B = A \cup (B \setminus A),\ B = (B \setminus A) \cup (A \cap B)\rangle$.

(57) $A, B, C \in \mathrm{Fin} \ \Rightarrow \ |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$
$\langle$wg (56), $A \cup B \cup C = (A \cup B) \cup C \ldots\rangle$.

Ogólnie:

(58) $n \in \mathbb{N} \wedge A : I_n \to \mathrm{Fin} \implies \Big|\bigcup\limits_{k=1}^{n} A_k\Big| = \sum\limits_{k=1}^{n} (-1)^{k+1} \sum\limits_{\alpha : I_k \nearrow I_n} \Big|\bigcap\limits_{l=1}^{k} A_{\alpha_l}\Big|$,

gdzie zapis $\alpha : I_k \nearrow I_n$ oznacza, że α jest injekcją rosnącą z I_k do I_n $\langle$indukcja na n. I. $n = 0, 1, 2$, OK II. Jeśli $n \geqslant 3$ i OK dla $n - 1$, to $\ldots$ $\langle$zadanie 55$\rangle\rangle$.

Częstym w kombinatoryce problemem jest wyznaczanie mocy pewnych zbiorów funkcji lub relacji. Niech $k, n \in \mathbb{N}$.
Według (46), (47): $|k \times n| = kn$, $|\operatorname{Map}(k, n)| = n^k$, $|\mathcal{P}n| = 2^n$.
Oznaczmy $n^{\underline{k}} = \operatorname{Inj}(k, n)$.
Oczywiście $k > n \ \Rightarrow \ n^{\underline{k}} = 0$, $n^{\underline{0}} = 1$.

(59) $k \leqslant n \ \Rightarrow \ n^{\underline{k}} = \prod\limits_{i=1}^{k} (n - i + 1) = n(n-1)\ldots(n-k+1)$
$\langle$indukcja na $k\rangle$.

Funkcję $n^{\underline{k}}$ nazywamy *potęgą kroczącą* (*dolną*) o podstawie n i wykładniku k.
W szczególności dla $k = n$ oznaczamy $n! = n^{\underline{n}}$ (*silnia*, *faktoriał*). Tak więc

(60) $n! = |\operatorname{Perm}(n)|$; $0! = 1$, $(n+1)! = n!(n+1)$.

Ważną funkcją w kombinatoryce jest *symbol Newtona* zwany też *współczynnikiem dwumianowym*:

$\binom{n}{k} := |\mathcal{P}_k(n)|$ (czyt. „n po k”), gdzie dla dowolnej klasy A: $\mathcal{P}_k(A) := \{X \subset A \mid |X| = k\}$.
Zachodzi równość:

(61) $n^{\underline{k}} = \binom{n}{k} \cdot k!$ $\langle \operatorname{Inj}(k, n) = \bigcup\limits_{X \in \mathcal{P}_k(n)} \operatorname{Bij}(k, X)\rangle$, a więc $\binom{n}{k} = \frac{n^{\underline{k}}}{k!}$.

Zauważmy, że:

(62) $k \leqslant n \ \Rightarrow \ \binom{n}{k} = \frac{n!}{k!(n-k)!}$, $k > n \ \Rightarrow \ \binom{n}{k} = 0$ $\langle$wg (61)$\rangle$

(63) $0 < k \leqslant n \;\Rightarrow\; \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
$\langle \exists)\, a \in n.\ \mathcal{P}_k(n) = \{X \in \mathcal{P}_k(n) \mid a \in X\} \cup \{X \in \mathcal{P}_k(n) \mid a \notin X\}\rangle$.

Korzystając z (69), tworzymy *trójkąt Pascala*:

$$\begin{array}{ccccccccccc}
 & & & & & 1\ (=\binom{0}{0}) & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots
\end{array}$$

(64) $\sum_{k=0}^{n} \binom{n}{k} = 2^n \quad \langle \mathcal{P}(n) = \bigcup_{k=0}^{n} \mathcal{P}_k(n)\rangle$.

Równość (64) można też otrzymać z poniższej *formuły dwumianowej* (stąd druga nazwa symbolu Newtona), kładąc $a = b = 1$:

(65) $\forall\, a, b, n \in \mathbb{N} : (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \quad \langle$indukcja na n, lub kombinatorycznie: $(a+b)^n = \sum_{X \subset I_n} a^{|X|} b^{|X^\urcorner|} = \ldots\rangle$.

Wśród liczb naturalnych podstawowe znaczenie mają *liczby pierwsze* $\mathbb{P} := \{p \in \mathbb{N} \mid p > 1 \wedge \forall\, d \in \mathbb{N}\ (d \mid p \;\Rightarrow\; d = 1 \vee d = p)\} = \{2, 3, 5, 7, 11, \ldots\}$.

Liczby złożone $:= \mathbb{N}_2 \setminus \mathbb{P} = \{4, 6, 8, 9, 10, \ldots\}$.

Każda liczba naturalna $n \geqslant 2$ ma dzielnik pierwszy; $\forall\, n \in \mathbb{N}_2\ \exists\, p \in \mathcal{P} : p \mid n$ $\langle$indukcja na $n\rangle$; skąd wynika, że zbiór $\mathbb{P}$ liczb pierwszych jest nieskończony $\langle$HP: $\mathbb{P} \in \mathrm{Fin}.\ \exists)\, q \in \mathbb{P} : q \mid \prod \mathbb{P} + 1$. Ale $q \mid \prod \mathbb{P}$, a więc $q \mid 1$ ↯$\rangle$.

Jeżeli $n \in \mathbb{N}_2 \setminus \mathbb{P}$ i p jest najmniejszym dzielnikiem pierwszym liczby n, to $p^2 \leqslant n$ $\langle$HP: $n < p^2$. $\exists)\, x \in \mathbb{N} : n = px$, $px < p^2$, $x < p$. Ale $x \geqslant 2$ $\langle$bo $n \notin \mathbb{P}\rangle$, a więc $\exists)\, q \in \mathbb{P} : q \mid x$, i wówczas $q \mid n$, $p \leqslant q$, jednak $q \leqslant x < p$ ↯$\rangle$.

Tak więc:

(66) $\forall\, n \in \mathbb{N}_2\ [n \in \mathbb{P} \Leftrightarrow \forall\, p \in \mathbb{P}(p^2 \leqslant n \;\Rightarrow\; p \nmid n)]$.

Jest to najprostsze kryterium pierwszości. Naprawdę dużych liczb pierwszych szuka się wśród tzw. *liczb Mersenne'a*, to jest liczb ze zbioru $\{2^p - 1 \mid p \in \mathbb{P}\} \cap \mathbb{P}$. Największą znaną obecnie (grudzień 2018) liczbą pierwszą jest $2^{82\,589\,933} - 1$; jej zapis dziesiętny ma 24 862 048 cyfr.

Tak zwane *zasadnicze twierdzenie arytmetyki* mówi o istnieniu jednoznacznego z dokładnością do porządku rozkładu niezerowej liczby naturalnej na czynniki pierwsze.

Dowód istnienia rozkładu jest bezproblemowy $\langle$indukcja$\rangle$.

Nieco trudniejszy jest dowód jednoznaczności — można go przeprowadzić indukcyjnie.

(67) $\forall\, n \in \mathbb{N}^*\ \exists!\, k \in \mathbb{N}, p : I_k \to \mathbb{P}\ (n = p_1 \ldots p_k \wedge p_1 \leqslant \ldots \leqslant p_k)$.
$\langle$Przypuśćmy, że n jest najmniejszą niezerową liczbą naturalną, która ma dwa różne

rozkłady na czynniki pierwsze: $n = p_1 \dots p_k = q_1 \dots q_l$; $p_1 \leqslant \dots \leqslant p_k$, $q_1 \leqslant \dots \leqslant q_l$; $(p_1, \dots, p_k) \neq (q_1, \dots, q_l)$. Wówczas $p_k \neq q_l$ $\langle$wniosek z minimalności $n\rangle$, np. $p_k < q_l$. Niech $n' = n - q_1 \dots q_{l-1} p_k = q_1 \dots q_{l-1}(q_l - p_k)$. Ponieważ $0 < n' < n$, więc n' ma jednoznaczny rozkład. Jednak $n' = p_1 \dots p_k - q_1 \dots q_{l-1} p_k = (p_1 \dots p_{k-1} - q_1 \dots q_{l-1}) p_k$, czyli $p_k \mid n'$, i ponieważ $p_k \not| q_l - p_k$ $\langle$HP: $p_k \mid q_l - p_k$. Wówczas $p_k \mid q_l$, $p_k = q_l$ ↯$\rangle$, więc $\exists) \, i \in I_{l-1} : q_i = p_k$.

Po uproszczeniu: $p_1 \dots p_{k-1} = q_1 \dots q_{i-1} q_{i+1} \dots q_{l-1} q_l < n$, a więc, znów na mocy minimalności n: $(p_1, \dots, p_{k-1}) = (q_1, \dots, q_{i-1}, q_{i+1}, \dots, q_l)$, skąd $q_l = p_{k-1} \leqslant p_k$ ↯$\rangle$.

Oznaczając dla $n \in \mathbb{N}^*$ i $p \in \mathbb{P}$: $\nu_p(n) =$ *stopień podzielności* n przez $p :=$ największe $k \in \mathbb{N}$ takie, że $p^k \mid n$, możemy, na mocy (67), liczbę n zapisać w *postaci kanonicznej*: $n = \prod\limits_{p \in \mathbb{P}} p^{\nu_p(n)}$, iloczyn ten jest tylko pozornie nieskończony, gdyż $\nu_p(n) = 0$ dla prawie wszystkich $p \in \mathbb{P}$.

Na przykład $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$, i ogólnie (*formuła Legendre'a*): $\nu_p(n!) = \sum\limits_{k \in \mathbb{N}^*} [\frac{n}{p^k}]$ $\langle$sumujemy jednokrotne, dwukrotne itd. wystąpienia liczby p w iloczynie $n! = 1 \cdot 2 \cdot \ldots \cdot n\rangle$.

Dla $a, b, c \in \mathbb{N}^*$:

(68) $a \mid b \Leftrightarrow \forall\, p \in \mathbb{P} : \nu_p(a) \leqslant \nu_p(b)$

(69) $(a, b) =$ największy wspólny dzielnik a i $b = \prod\limits_{p \in \mathbb{P}} p^{\nu_p(a) \cap \nu_p(b)}$,

$(a, b, c) = \prod\limits_{p \in \mathbb{P}} p^{\nu_p(a) \cap \nu_p(b) \cap \nu_p(c)}$ itd.

Analogicznie:

(70) $[a, b] =$ najmniejsza wspólna wielokrotność a i $b = \prod\limits_{p \in \mathbb{P}} p^{\nu_p(a) \cup \nu_p(b)}, \dots$

Jeżeli oznaczymy przez $\mathcal{D}(a)$ ogół dzielników liczby a: $\mathcal{D}(a) = \{d \in \mathbb{N} \mid d|a\}$, to

(71) $|\mathcal{D}(a)| = \prod\limits_{p \in \mathbb{P}} (\nu_p(a) + 1)$

$(a, b) = 1 \Leftrightarrow \forall\, p \in \mathbb{P} : \neg(p \mid a \wedge p \mid b) \Leftrightarrow \sum\limits_{p \in \mathbb{P}} \nu_p(a) \cdot \nu_p(b) = 0$ (a, b *pierwsze względem siebie*).

Ostatni człon tej równości usprawiedliwia (odwołanie do iloczynu skalarnego) wygodną notację:
$a \perp b \;:\Leftrightarrow\; (a, b) = 1$ ([**Graham... 02**, s. 139]).

Dla uzupełnienia można by położyć:
$a \parallel b \;:\Leftrightarrow\; \forall\, p \in \mathbb{P} : (p \mid a \Leftrightarrow p \mid b)$.

Relacja $\parallel$ jest równoważnością w $\mathbb{N}^*$ i spełnia warunek

$$\forall\, a, b, c \in \mathbb{N}^* : a \parallel b \;\;\wedge\;\; a \perp c \;\Rightarrow\; b \perp c.$$

Z zasadniczego twierdzenia arytmetyki (67) natychmiast wynika ważny fakt:

(72) $\forall\, a, b, c, \in \mathbb{N}^* : a \mid bc \wedge a \perp b \;\Rightarrow\; a \mid c$.

P. Fermat przypuszczał, że liczby $F_n = 2^{2^n} + 1$, nazwane później *liczbami Fermata*, są pierwsze — pięć początkowych liczb Fermata to liczby pierwsze: $F = \{0 \mapsto 3, 1 \mapsto$

$5, 2 \mapsto 17, 3 \mapsto 257, 4 \mapsto 65597, \dots\}$. Jednak, jak pokazał Euler – $F_5 \notin \mathbb{P}$ $\langle F_5 = 2^{32}+1 = 2^{32}+2^{28}\cdot 5^4 - (2^{28}\cdot 5^4 - 1) = 2^{28}\cdot 641 - (2^{14}\cdot 5^2+1)(2^7\cdot 5-1)\cdot 641\rangle$.

Obecnie przypuszcza się, że $n \geqslant 5 \;\Rightarrow\; F_n \notin \mathbb{P}$.

Indukcyjnie łatwo udowodnić wzór rekurencyjny:

(73) $n \geqslant 1 \;\Rightarrow\; F_n = F_0F_1\dots F_{n-1}+2$.

Z powyższej formuły wynika, że liczby Fermata są pierwsze względem siebie:

(74) $k \neq n \;\Rightarrow\; F_k \perp F_n$.

Wnioskiem z (74) jest nieskończoność zbioru $\mathbb{P}$, jak również oszacowanie od góry liczb pierwszych przez liczby Fermata:
Oznaczając $p = \mathrm{nat}_{\mathbb{P}} = \{0 \mapsto 2, 1 \mapsto 3, 2 \mapsto 5, \dots\}$, będziemy mieli:

(75) $n \geqslant 1 \;\Rightarrow\; p_n \leqslant F_{n-1}$.

5.2. Tematy

1. Zredagować dowody podstawowych własności liczb porządkowych (twierdzenie o dobrym uporządkowaniu (4), prawa (5)–(11)).

2. Oznaczmy przez T klasę wszystkich zbiorów tranzytywnych; $T = \{x \mid x \subset \mathcal{P}x\} = \{x \mid \bigcup x \subset x\}$.

(i) Czy prawdziwe jest twierdzenie:

$$C \subset T \;\Rightarrow\; \bigcup C\text{– klasa tranzytywna?}$$

(ii) Dla ustalonego zbioru x określamy indukcyjnie ciąg $s : \mathbb{N} \to \mathbb{V}$; $s_0 = x$, $\forall\, n \in \mathbb{N} : s_{n+1} = \bigcup s_n$. Niech $\bar{x} = \bigcup_{n\in\mathbb{N}} s_n$.

Wykazać, że $\bar{x}$ jest najmniejszym zbiorem tranzytywnym zawierającym zbiór x, tzn. $x \subset \bar{x}$, $\bar{x} \in T$, $\forall\, y \in T : x \subset y \implies \bar{x} \subset y$.

Zbiór $\bar{x}$ nazywamy *domknięciem tranzytywnym* zbioru x i oznaczamy też $\mathrm{TC}(x)$ (*Transitive Closure*); zachodzi równoważność: $x \in T \Leftrightarrow x = \bar{x}$.

(iii) Wykazać, że:

$$\forall\, x, y : x \subset \bar{x},\ \bar{\bar{x}} = \bar{x},\ x \subset y \;\Rightarrow\; \bar{x} \subset \bar{y}.$$

Powyższe trzy własności oznaczają, że funkcja

$$TC = \{x \mapsto \bar{x} \mid x \in \mathbb{V}\} : \mathbb{V} \to \mathbb{V}$$

jest operacją *domknięcia* w klasie $\mathbb{V}$ wszystkich zbiorów.

(iv) Udowodnić *Zasadę regularności* (analogon Zasady minimum; por. rozdz. 4 (37)):

$$A \neq \varnothing \;\Rightarrow\; \exists\, a \in A : a \cap A = \varnothing \qquad (A \text{ – dowolna klasa}).$$

Wskazówka: Rozumując nie wprost, dla ustalonego $a \in A$ wziąć zbiór $\bar{a} \cap A \neq \varnothing$, wówczas ...

3. Klasę A nazywamy *sekwensowo domkniętą*, gdy spełnia warunek:

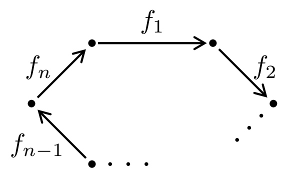
$$\varnothing \in A \quad\wedge\quad \forall\, x \in A : \operatorname{seq} x \in A.$$

Oznaczmy przez H ogół zbiorów sekwensowo domkniętych. Wykazać, że $\mathbb{N} = \bigcap H$.

4. Dane są ciągi zbiorów $A, B : \mathbb{N} \to \mathbb{V}$. Zbadać zależność między zbiorami $\bigcap\limits_{n\in\mathbb{N}} (A_n \setminus B_n)$ i $\bigcap\limits_{n\in\mathbb{N}} A_n \setminus \bigcap\limits_{n\in\mathbb{N}} B_n$. Kiedy zachodzi równość? Podać możliwie najprostszy przykład inkluzji silnej. (por. zadanie 3.8).

5. Wykazać, że jeżeli A jest liczbą porządkową i $f : A \hookrightarrow A$ oraz $\forall\ \alpha \in A : f(\alpha) \leqslant \alpha$, to $f = \mathrm{id}_A$.

6*. Uogólnić twierdzenie z zadania 3.21 w przypadku łańcucha zamkniętego n funkcji, $n \in \mathbb{N}^*$:



7. Wykazać, że $\forall\ A, B\ (A \subset B \subset \mathrm{Ord}\ \Rightarrow\ \mathrm{ord}\, A \leqslant \mathrm{ord}\, B)$.

8. Oznaczmy $\mathrm{Lim}_0 := \mathrm{Lim} \cup \{0\} = \{\alpha \in \mathrm{Ord} \mid \forall\ \beta \in \mathrm{Ord} : \alpha \neq \mathrm{seq}\,\beta\}$ – *liczby graniczne w szerszym sensie*.

Udowodnić, że:

$$\forall\,\alpha \in \mathrm{Ord} \begin{bmatrix} \alpha \in \mathrm{Lim}_0 \Leftrightarrow \alpha = \bigcup \alpha, \\ \alpha \notin \mathrm{Lim}_0 \Leftrightarrow \alpha = \mathrm{seq} \bigcup \alpha \end{bmatrix}.$$

Tak więc dla $\alpha \in \mathrm{Seq} := \mathrm{Ord} \setminus \mathrm{Lim}_0$ – *liczby sekwensowe*, $\bigcup \alpha$ jest *poprzednikiem* liczby α.

9. Naszkicować dowody praw (26)–(36) arytmetyki porządkowej.

10. Udowodnić prawo (37) (dla $\alpha \in \mathrm{Ord}$ liczby $\lambda \in \mathrm{Lim}_0$ i $n \in \mathbb{N}$ takie, że $\alpha = \lambda + n$, nazywamy odpowiednio *częścią graniczną* i *częścią naturalną* liczby porządkowej α).

11. Udowodnić (38), to jest własności działań na liczbach naturalnych.

12*. Podać ścisłą definicję różnicy $\beta - \alpha$ ($\alpha, \beta \in \mathrm{Ord}$) i uzasadnić ją (por. (39)).

13. Udowodnić własności (i)–(vii) odejmowania z (40).

14. Udowodnić twierdzenie o dzieleniu z resztą (41).

15. Udowodnić własności (i)–(viii) relacji podzielności z (42).

16. Udowodnić własności (i)–(viii) potęgowania z (43).

17*. Udowodnić, że dla dowolnych liczb porządkowych α, β, γ, jeżeli $\omega^\alpha = \beta + \gamma$, to $\beta = \omega^\alpha$ lub $\gamma = \omega^\alpha$.

18. Opisać bardziej formalnie i uzasadnić *algorytm Euklidesa* wyznaczania największego wspólnego dzielnika (α, β) dwu niezerowych liczb porządkowych α i β. Polega on na dzieleniu jednej liczby przez drugą, i jeżeli otrzymujemy niezerową resztę, to dzielimy drugą liczbę przez tę resztę, uzyskując kolejną mniejszą resztę itd. Ostatnia niezerowa reszta będzie n.w.d. danych dwu liczb. $(22\ 533, 42\ 439) = ?$

19. Czy jest prawdą, że dla zbioru dobrze uporządkowanego Y i odwzorowania f : Ord $\to Y$ relacja R określona w klasie Ord tak jak w zadaniu 4.52*, a mianowicie

$$\alpha R \beta \;:\Longleftrightarrow\; f(\alpha) < f(\beta) \vee [f(\alpha) = f(\beta) \wedge \alpha \leqslant \beta],$$

jest dobrym porządkiem w Ord?

20*. Podać przykład nieizomorficznych (niepodobnych) posetów X i Y, z których pierwszy jest podobny do prawego odcinka drugiego, zaś drugi do lewego odcinka pierwszego (por. zadanie 4.47*).

Wskazówka: w posecie $P = (\mathbb{N}^2, R)$, gdzie dla a, b, c, $d \in \mathbb{N}$: $(a, b) \underset{R}{\leqslant} (c, d) \Leftrightarrow a = c \wedge b \leqslant d$, ustalić dwa podzbiory $X, Y \subset \mathbb{N}^2$ i potraktować je jako posety z porządkiem indukowanym z P.

21. Ograniczając się do liczb naturalnych, można w definicji indukcyjnej potęgowania przestawić czynniki w kroku sekwensowym (mnożenie w $\mathbb{N}$ jest przemienne).
Tak więc dla $a, b \in \mathbb{N}$ możemy napisać:

$$a^0 = 1, \quad a^{b+1} = a \cdot a^b.$$

Nazywając mnożenie liczb naturalnych *potęgowaniem rzędu 0*, $a \overset{0}{\wedge} b = ab$, zaś zwykłe potęgowanie – *potęgowaniem rzędu 1*, $a \overset{1}{\wedge} b = a \wedge b = a^b$, otrzymamy zapis

$$a \overset{1}{\wedge} 0 = 1, \quad a \overset{1}{\wedge} (b+1) = a \overset{0}{\wedge} (a \overset{1}{\wedge} b).$$

Według tego schematu możemy dla $n \in \mathbb{N}$ określić indukcyjnie potęgowanie rzędu n, kładąc dla $a, b \in \mathbb{N}$:

$$a \overset{0}{\wedge} b = ab$$

$$a \overset{n+1}{\wedge} 0 = 1, \quad a \overset{n+1}{\wedge} (b+1) = a \overset{n}{\wedge} (a \overset{n+1}{\wedge} b). \qquad \text{([**Conway... 99**, s. 71]).}$$

(i) Wyjaśnić, dlaczego bez przestawienia czynników w kroku sekwensowym otrzymalibyśmy dla $n \geqslant 2$ działanie trywialne.

(ii) Udowodnić, że dla $a, b, n \in \mathbb{N}$:

1) $b \geqslant 1 \;\Rightarrow\; a \overset{2}{\wedge} b = \underbrace{a^{a^{\cdot^{\cdot^{a}}}}}_{b}$

2) $a \overset{n}{\wedge} 1 = a$

3) $n \geqslant 1, b \geqslant 2 \;\Rightarrow\; a \overset{n}{\wedge} b = \underbrace{a \overset{n-1}{\wedge} (a \overset{n-1}{\wedge} (\dots (a \overset{n-1}{\wedge} a) \dots))}_{b \text{ wystąpień litery } a}$

4) $2 \overset{n}{\wedge} 2 = 4$

5) $n \geqslant 1 \;\Rightarrow\; 1 \overset{n}{\wedge} b = 1$

6) $n \geqslant 2 \;\Rightarrow\; 0 \overset{n}{\wedge} b = \begin{cases} 1, & \text{gdy } 2 \mid b \\ 0, & \text{gdy } 2 \nmid b. \end{cases}$

(iii) Kładąc dla $n \in \mathbb{N}$: $A_n = n \overset{n}{\wedge} n$, otrzymamy *ciąg Ackermanna*, który jest *rekurencyjny* (obliczalny w intuicyjnym sensie według tzw. *tezy Churcha* – ścisła definicja np. z wykorzystaniem zasady minimum), ale nie jest *pierwotnie rekurencyjny* (*primitive recursive* – zamiast zasady minimum przyjmujemy tzw. *schemat rekursji prostej*, czyli definiowanie indukcyjne z przejściem $n \mapsto n+1$), gdyż „za szybko rośnie" (można wykazać, że w pewnym sensie majoryzuje wszystkie funkcje $f : \mathbb{N} \to \mathbb{N}$ pierwotnie rekurencyjne).

Podać wartości A_n dla $n \leqslant 4$.

22. Udowodnić, że dla $n \in \mathbb{N}$:

(a) $4 \mid 5^{2^n} + 7$, $8 \mid 5^{2^{n+1}} + 7$
(b) $8 \mid 5^{n+1} + 2^{3^n} + 1$
(c) $13 \mid 4^{2n+1} + 3^{n+2}$
(d) $25 \mid 4 \cdot 6^n + 5n - 4$
(e) $a \in \mathbb{N}^* \;\Rightarrow\; a^2 \mid 1 + (a+1)^n(na-1)$.

23*. Określamy indukcyjnie ciąg $a : \mathbb{N} \to \mathbb{N}$, $a_0 = 2$, $a_{n+1} = 2^{a_n}$.
Wykazać, że $n \geqslant 2 \;\Rightarrow\; 7 \mid a_n - 2$.

24*. Wykazać, że dla liczby naturalnej $n \geqslant 3$:

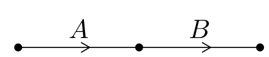
$$\overbrace{n^{n^{\cdot^{\cdot^{n}}}}}^{n+1} > (n+1)^{\underbrace{(n+1)^{\cdot^{\cdot^{(n+1)}}}}_{n}}.$$

Wskazówka: sformułować temat bardziej formalnie, a następnie znaleźć ogólniejszą formułę, z której nasza nierówność będzie natychmiastowym wnioskiem i której indukcyjny dowód nie sprawi większej trudności.

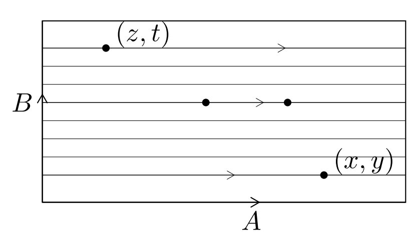
25. Niech $A, B \in \mathbb{V}$, R – dobry porządek w A, S – dobry porządek w B, $\alpha = \mathrm{ord}(A, R)$, $\beta = \mathrm{ord}(B, S)$.

Wykazać, że:

1) jeżeli $A \cap B = \varnothing$, to relacja $T = R \cup (A \times B) \cup S$ jest dobrym porządkiem w $A \cup B$ i $\alpha + \beta = \mathrm{ord}(A \cup B, T)$

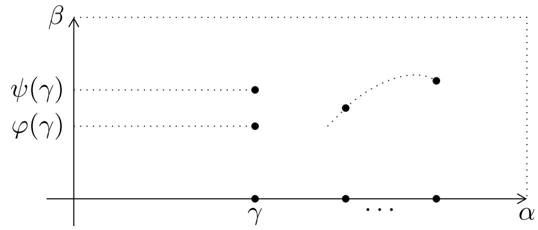


2) relacja $T = \{((x,y),(z,t)) \in (A \times B)^2 \mid y \underset{S}{<} t \vee (y = t \wedge x \underset{R}{\leqslant} z)\}$ (*porządek leksykograficzny prawostronny* indukowany przez porządki R i S) jest dobrym porządkiem w $A \times B$ i $\alpha\beta = \mathrm{ord}(A \times B, T)$.



26*. Niech $\alpha, \beta \in \mathrm{Ord}$, $\Phi = \{\varphi : \alpha \to \beta \mid \exists\, n < \omega, s : n \hookrightarrow \alpha\ \forall\, \xi < \alpha : \varphi(\xi) \neq 0 \Leftrightarrow \xi \in \mathrm{Im}\, s\}$; mówimy w tej sytuacji, że funkcja $\varphi : \alpha \to \beta$ znika prawie wszędzie; zbiór skończony $\mathrm{Im}\, s \subset \alpha$ nazywamy jej *suportem* albo *nośnikiem* i oznaczamy $\mathrm{supp}\, \varphi$).

W zbiorze Φ określamy relację $T = \{(\varphi, \psi) \in \Phi^2 \mid \varphi = \psi \vee \exists\, \gamma < \alpha : \varphi(\gamma) < \psi(\gamma) \wedge \forall_{\gamma < \xi < \alpha}\, \varphi(\xi) = \psi(\xi)\}$.



Wykazać, że T jest dobrym porządkiem w Ψ i $\beta^\alpha = \mathrm{ord}(\Phi, T)$.

27. Udowodnić, że dla $\alpha, \beta \in \mathrm{Ord}$:

(i) $\alpha\beta = \sum\limits_{\eta<\beta} \alpha$

(ii) $\alpha \neq 0 \implies \alpha^\beta = \prod\limits_{\eta<\beta} \alpha$.

28. Dla ciągu $a : \lambda \to \mathrm{Ord}$, gdzie $\lambda \in \mathrm{Lim}$, określamy *granicę* $\lim a = \lim\limits_{\xi<\lambda} a_\xi :=$

$$\bigcap\{\alpha \in \mathrm{Ord}^* \mid \forall\, \beta < \alpha\ \exists\, \mu < \lambda\ \forall\, \mu < \xi < \lambda : \beta < a_\xi < \alpha\} \qquad (\mathrm{Ord}^* = \mathrm{Ord} \setminus 1).$$

Wykazać, że:

(i) granica ciągu, jeżeli istnieje (to znaczy $\lim a \neq \mathbb{V}$), jest wyznaczona jednoznacznie, a więc $\forall\, \alpha \in \mathrm{Ord}^* : \lim a = \alpha \iff \forall\, \beta < \alpha\ \exists\, \mu < \lambda\ \forall\, \mu < \xi < \lambda : \beta < a_\xi < \alpha$.

(ii) Jeżeli ciąg $a : \lambda \to \mathrm{Ord}$ jest silnie rosnący, $a : \lambda \nearrow \mathrm{Ord}$, to $\lim a = \sup\limits_{\xi<\lambda} a_\xi = \bigcup\limits_{\xi<\lambda} a_\xi \in \mathrm{Lim}$.

(iii) $\lambda \in \mathrm{Lim}$, $a : \lambda \nearrow \mathrm{Ord}$, $\lim a = \alpha$, $f : \alpha \nearrow \mathrm{Ord} \implies \lim f = \lim(f \circ a)$.

29. Dla liczby porządkowej granicznej A ($A = \mathrm{Ord}\ \vee\ A \in \mathrm{Lim}$) ciąg $f : A \to \mathrm{Ord}$ nazywamy *normalnym*, gdy:

(i) jest silnie rosnący, co będziemy oznaczać $f : A \nearrow \mathrm{Ord}$

(ii) $\forall\, \lambda \in A \cap \mathrm{Lim} : \lim\limits_{\xi<\lambda} f(\xi) = f(\lambda)$ (mówimy w tej sytuacji, że funkcja f jest *ciągła*).

Wykazać, że ciąg normalny $f : \mathrm{Ord} \to \mathrm{Ord}$ ma dowolnie duże punkty stałe, zwane też *krytycznymi*. Dokładniej, jeżeli $\alpha \in \mathrm{Ord}$ i $f(\alpha) \neq \alpha$ (a więc $\alpha < f(\alpha)$ na mocy lematu o przesunięciu w prawo), to najmniejszy punkt stały $\beta > \alpha$ otrzymujemy jako granicę ciągu silnie rosnącego $\alpha < f(\alpha) < f(f(\alpha)) < \dots$

Czy twierdzenie powyższe pozostaje w mocy dla ciągu normalnego $f : \lambda \to \lambda$, $\lambda \in \mathrm{Lim}$?

30. Udowodnić, że ciągi $\omega+\xi$, $\omega\xi$, ω^ξ ($\xi \in \mathrm{Ord}$) są normalne. Ciągi te mają więc dowolnie duże punkty stałe – dla każdego z nich naturalna numeracja punktów stałych jest określona na klasie Ord wszystkich liczb porządkowych. W szczególności numeracja klasy punktów stałych ciągu $\xi \mapsto \omega^\xi$ oznaczana jest tradycyjnie literą ε — liczby ε_α ($\alpha \in \mathrm{Ord}$) nazywamy *epsilonowymi*.
Wyznaczyć najmniejszy punkt stały każdego z tych ciągów.

31. Udowodnić, że dla ciągu normalnego $f : \mathrm{Ord} \to \mathrm{Ord}$ naturalna numeracja $g = \mathrm{nat}_C\, \mathrm{Ord} \to \mathrm{Ord}$ klasy C punktów stałych ciągu f jest ciągiem normalnym.

32. Dany jest ciąg normalny f spełniający warunek:

$$f(0) = 1 \quad \wedge \quad \forall\ \alpha, \beta \in \mathrm{Ord} : f(\alpha + \beta) = f(\alpha) \cdot f(\beta).$$

Wykazać, że istnieje jednoznacznie wyznaczona liczba porządkowa γ taka, że $\forall\ \alpha \in \mathrm{Ord} : f(\alpha) = \gamma^\alpha$; przy czym $\gamma > 1$.

33. Dla $n < \omega$:

(i) $1 + 2 + 2^2 + \ldots + 2^n = ?$

(ii) $1 + \omega + \omega^2 + \ldots + \omega^n = ?$

(iii) $1 \cdot 1 + 2 \cdot 2 + 3 \cdot 2^2 + \ldots + (n+1)2^n = \sum\limits_{k=0}^{n} (k+1)2^k = ?$

(iv) $1 + 2 + 3 + \ldots + n = \sum\limits_{k=1}^{n} k = ?$

Wskazówka: Oznaczyć $S_n = \sum\limits_{k=1}^{n} k$ i sumować obustronnie równość $(k+1)^2 = k^2+2k+1$ dla $k = 1, \ldots, n$.

(v) $1 + 2^2 + 3^2 + \ldots + n^2 = \sum\limits_{k=1}^{n} k^2 = ?$

Wskazówka: Postępować jak w (iv), wykorzystując równość $(k+1)^3 = k^3+3k^2+3k+1$.

(vi) $1 + 2^2 + 3^2 + \ldots + n^2 = \sum\limits_{k=1}^{n} k^3 = ?$

W każdym z powyższych przypadków należy uzyskać tak zwaną zwartą postać (por. [**Graham... 02**, s. 17]).

34. Udowodnić, że dla danego rozwinięcia pozycyjnego niezerowej liczby porządkowej α

$$\alpha = \gamma^{\xi_k}\eta_k + \ldots + \gamma^{\xi_1}\eta_1 \qquad (\gamma \geqslant 2, \xi_1 < \ldots < \xi_k, 0 < \eta_i < \gamma,\ \text{zob. (44)})$$

zachodzi nierówność:

$$\gamma^{\xi_k} > \gamma^{\xi_{k-1}} \cdot \eta_{k-1} + \ldots + \gamma^{\xi_1} \cdot \eta_1.$$

Wskazówka: zastosować indukcję względem $k = 1, 2, \ldots$

35. Dana jest liczba porządkowa $\gamma \geqslant 2$. Dla dowolnej liczby porządkowej α oznaczamy przez $\tau(\alpha)$ najmniejszą liczbę porządkową τ taką, że $\alpha < \gamma^\tau$; $\tau(\alpha) = \bigcap\{\tau \in \mathrm{Ord} \mid \alpha < \gamma^\tau\}$ $\langle$liczby takie istnieją, gdyż $\alpha \leqslant \gamma^\alpha < \gamma^{\alpha+1}\rangle$.

Liczbę $\tau(\alpha)$ nazywamy *rzędem wielkości* liczby α przy podstawie γ. Wykazać, że jeżeli $\alpha \neq 0$, to $\tau(\alpha) \in \mathrm{Seq}$, czyli $\tau(\alpha) = \xi + 1$, gdzie $\xi = \bigcup \tau(\alpha)$.

Wykazać, że jeżeli dane jest rozwinięcie pozycyjne (ξ, η) niezerowej liczby α przy podstawie γ,

$$\alpha = \gamma^{\xi_k}\eta_k + \ldots + \gamma^{\xi_1}\eta_1 \quad \text{(zob. (44))},$$

to $\tau(\alpha) = \xi_k + 1$.

36. W zastosowaniach ważne są rozwinięcia przy podstawach 2 i ω. Przejście od jednej z tych podstaw do drugiej jest łatwe, gdyż zachodzi równość $2^\omega = \omega$.

a) Rozwinąć przy podstawie 2 liczbę:
$\alpha = \omega^\omega \cdot 3 + \omega^2 \cdot 2 + \omega$.

b) Rozwinąć przy podstawie ω liczbę:
$\beta = 2^{\omega\cdot 2+1} + 2^{\omega+2} + 2^\omega + 2^2 + 2^1 + 2^0$.

37. Udowodnić twierdzenie o rozwinięciu pozycyjnym (44). Wskazówka: zastosować indukcję względem $\tau = \tau(\alpha) = \bigcap\{\tau \in \mathrm{Ord} \mid \alpha < \gamma^\tau\}$ (por. zadanie 35).

38*. Dla $m \in \mathbb{N}$ określamy indukcyjnie *ciąg Goodsteina* o początku m, $a = \overset{m}{a} : \mathbb{N} \to \mathbb{N}$,

I $\quad a_0 = m$

II jeśli $n \geqslant 1$, to chcąc obliczyć a_n, bierzemy tzw. *pełne rozwinięcie* a_{n-1} *przy podstawie* $n + 1$. Polega ono na tym, że w zwykłym rozwinięciu rozwijamy wykładniki większe od $n+1$, z uzyskanymi rozwinięciami postępujemy analogicznie itd., aż otrzymamy zapis, w którym nie występują liczby większe od podstawy. Następnie każde wystąpienie podstawy, czyli $n + 1$, zamieniamy na $n + 2$. Wreszcie od wyniku odejmujemy 1, przy czym odejmowanie traktujemy w sensie zredukowanym, np. $0 - 1 = 0$ (por. zadanie 7*).

Na przykład siedem pierwszych wyrazów ciągu Goodsteina o początku 4. ($a = \overset{4}{a}$), to:
$a_0 = \underline{4} = 2^2$
$a_1 = 3^3 - 1 = \underline{26} = 3^2 \cdot 2 + 3 \cdot 2 + 2$
$a_2 = 4^2 \cdot 2 + 4 \cdot 2 + 2 - 1 = \underline{41} = 4^2 \cdot 2 + 4 \cdot 2 + 1$
$a_3 = 5^2 \cdot 2 + 5 \cdot 2 = \underline{60}$
$a_4 = 6^2 \cdot 2 + 6 \cdot 2 - 1 = \underline{83} = 6^2 \cdot 2 + 6 + 5$
$a_5 = 7^2 \cdot 2 + 7 + 5 - 1 = \underline{109} = 7^2 \cdot 2 + 7 + 4$
$a_6 = 8^2 \cdot 2 + 8 + 3 = \underline{139}$.

a) Wyznaczyć siedem pierwszych wyrazów ciągu $\overset{8}{a}$.

b) Podać ścisłą i bardziej formalną definicję ciągu Goodsteina o danym początku.

Wskazówka: Określić najpierw indukcyjnie funkcje $S : \mathbb{N} \times \mathbb{N}_2 \to \mathbb{N}$, $S(x, n) =$ wynik zastąpienia w pełnym rozwinięciu x przy podstawie n wszędzie $n \mapsto n + 1$.

c) Naśladując definicję funkcji S z punktu b), określamy dla ustalonej liczby naturalnej $n \geqslant 2$ ciąg $f_n : \mathbb{N} \to \mathrm{Ord}$

(I) $f_n(0) = 0$

(II) jeżeli $1 \leqslant x = n^{\xi_k} \cdot \eta_k + \ldots + n^{\xi_1} \cdot \eta_1$, gdzie $\xi_1 < \ldots < \xi_k < \omega$, $0 < \eta_i < n$ dla $i \in I_k$, to $f_n(x) = \omega^{f_n(\xi_k)} \cdot \eta_k + \ldots + \omega^{f_n(\xi_1)} \cdot \eta_1$.
Wykazać, że:

$$\forall\ n \in \mathbb{N}_2, x \in \mathbb{N} : f_n(x) = f_{n+1}(S(x,n)).$$

d) Udowodnić, że dla każdej liczby naturalnej $n \geqslant 2$ ciąg $f_n : \mathbb{N} \to \mathrm{Ord}$ określony w punkcie c) jest silnie rosnący.
Wskazówka: W rozwinięciu pozycyjnym liczby $x \in \mathbb{N}_1$ przy podstawie n dopuścić cyfry zerowe: $x = n^r \cdot \alpha_r + \ldots + n \cdot \alpha_1 + \alpha_0$, gdzie $\forall\ i \leqslant r : \alpha_i < n$, $\alpha_r \neq 0$, i wówczas $f_n(x) = \omega^{f_n(r)} \cdot \alpha_r + \ldots + \omega^{f_n(1)} \cdot \alpha_1 + \alpha_0$.

e) Udowodnić *twierdzenie Goodsteina*:

$\forall\ m \in \mathbb{N}\ \exists n \in \mathbb{N}\ \overset{m}{a}_n = 0$, gdzie $\overset{m}{a} = a : \mathbb{N} \to \mathbb{N}$ jest ciągiem Goodsteina o początku m.
Wskazówka: Dowodzić nie wprost. Zbadać monotoniczność ciągu $b : \mathbb{N} \to \mathrm{Ord}$, $b_n = f_{n+2}(\overset{m}{a}_n)$.
Komentarz: Twierdzenie to udowodnił R.L. Goodstein w roku 1944 (J. Symb. Logic 9, 33–41), używając rozwinięć pozycyjnych przy podstawie ω. W roku 1982 J. Paris i L. Kirby udowodnili jego niezależność od arytmetyki Peana — wykazali, że istnieje niestandardowy model arytmetyki PA, w którym twierdzenie Goodsteina nie jest prawdziwe.

f) Na mocy e) uzyskujemy ciąg $c : \mathbb{N} \to \mathbb{N}$, $c_m = \min\{n \in \mathbb{N} \mid \overset{m}{a}_n = 0\}$; jego początkowe wyrazy to: 0, 1, 3, 5. Wyznaczyć c_4.
Wskazówka: Dla $a = \overset{4}{a}$ wyznaczyć $k > 0$ takie, że $a_k = (k+2)^2$, a następnie $l > k$ takie, że $a_l = l + 2$.
Komentarz: Można dowieść, że ciąg c, podobnie jak ciąg Ackermanna (zadanie 21), jest rekurencyjny, ale nie pierwotnie rekurencyjny.

39. Udowodnić następujące wzmocnienie zasady szufladkowej Dirichleta:
Jeżeli $x, y \in \mathrm{Fin}$, $|x| = m > n = |y|$, oraz $f : x \twoheadrightarrow y$, to istnieje $t \in y$ takie, że:

$$|f^{-1}\{t\}| \geqslant \varphi(m,n) = \begin{cases} \frac{m}{n}, & \text{gdy } n \mid m \\ \left[\frac{m}{n}\right] + 1, & \text{gdy } n \nmid m. \end{cases}$$

Inaczej, $\varphi(m,n) = \left\lceil \frac{m}{n} \right\rceil := \min\{k \in \mathbb{N} \mid m \leqslant nk\}$ (*część całkowita górna*).
Na przykład (*Pigeon Hole Principle*); $\varphi(7,3) = 3$.

40. Wykazać, że $x \in \mathrm{Fin} \Rightarrow \forall\ y \subset x\ (y \sim x \Rightarrow y = x)$.
Implikacja w przeciwnym kierunku zachodzi w ZFC, to jest po przyjęciu aksjomatu wyboru (AC). W ZF zbiory spełniające warunek z następnika nazywamy *skończonymi w sensie Dedekinda*. Każdy zbiór skończony jest skończony w sensie Dedekinda. Zbiór $\mathbb{N}$ nie jest skończony (jest nieskończony), gdyż nie jest skończony w sensie Dedekinda. $\langle 2\mathbb{N} := \{2n \mid n \in \mathbb{N}\} = \{0, 2, 4, \ldots\} \subsetneq \mathbb{N},\ 2\mathbb{N} \sim \mathbb{N} \rangle$.

41. Oznaczmy $\mathcal{D} = \{x \mid \forall\ y \subset x\ (y \sim x \Rightarrow y = x)\}$ – zbiory skończone w sensie Dedekinda (zadanie 40) $\mathrm{Fin} \subset \mathcal{D}$.
Wykazać, że dla dowolnego zbioru x:

(i) $x \in \mathcal{D} \Rightarrow \neg\exists\, s : \omega \hookrightarrow x$
(ii) $x \in \mathcal{D} \Rightarrow \mathcal{P}x \subset \mathcal{D}$
(iii) $\mathcal{P}x \in \mathcal{D} \Rightarrow x \in \mathcal{D}$.

42. Warunek, aby zbiór x był skończony w sensie Dedekinda, można zapisać w postaci równoważnej:

$$(*) \qquad \forall\, f : x \hookrightarrow x \ (f : x \twoheadrightarrow x).$$

Warunek dualny do (*):

$$(\circ) \qquad \forall\, g : x \twoheadrightarrow x \ (g : x \hookrightarrow x)$$

jest również warunkiem koniecznym skończoności zbioru x (zbiór x spełniający warunek ($\circ$) nazywamy *skończonym dualnie w sensie Dedekinda*). Udowodnić ten fakt.

43. Dla $k \in \mathbb{N}^*$, $n \in \mathbb{N}$ znaleźć liczbę rozwiązań w liczbach naturalnych:
a) nierówności $x_1 + \ldots + x_k \leqslant n$
b) równania $x_1 + \ldots + x_k = n$.

Wskazówka:

oznaczając $\alpha_{k,n} = |A_{k,n}|$, $A_{k,n} = \{x : I_k \to \mathbb{N} \mid \sum_{i=1}^{k} x_i \leqslant n\}$

$\beta_{k,n} = |B_{k,n}|$, $B_{k,n} = \{x : I_k \to \mathbb{N} \mid \sum_{i=1}^{k} x_i = n\}$

zbadać odwzorowanie

$$f = \left\{ x \mapsto \Big\{ \sum_{i=1}^{j} x_i + j \mid j \in I_k \Big\} \ldots \right\} : A_{k,n} \to \mathcal{P}I_{n+k}.$$

44. Wykorzystując poprzednie zadanie 43, wykazać, że:

$$\forall\, m, n \in \mathbb{N} : \sum_{i=0}^{n} \binom{m+i}{m} = \binom{m+n+1}{m+1}.$$

Udowodnić powyższą równość indukcyjnie. (Jest to tzw. *wzór na równoległe sumowanie*, por. [**Graham... 02**, s. 202]).

45. Liczbę relacji równoważnościowych w I_n $(n = 0, 1, \ldots)$ nazywamy n-tą *liczbą Bella*; $B_n := |\operatorname{Equ} I_n|$. Oczywiście $B_0 = 1$. Znaleźć wzór rekurencyjny na B_n $(n \geqslant 1)$ i obliczyć B_n dla $1 \leqslant n \leqslant 5$.
Wskazówka: $B_n = |\operatorname{Part} I_n|$. Jeżeli $n \geqslant 1$, to $n \in I_n$; klasyfikujemy podziały zbioru I_n ze względu na moc różnicy $\xi \setminus \{n\}$, gdzie ξ jest warstwą podziału taką, że $n \in \xi$.

46. Dla $k, n \in \mathbb{N}$ *liczbą Sterlinga drugiego rodzaju* nazywamy liczbę podziałów zbioru n-elementowego na k części; $\left\{ {n \atop k} \right\} := |\operatorname{Part}_k I_n|$, gdzie dla zbioru X, $\operatorname{Part}_k X := \{\mathcal{A} \in PartX \mid |\mathcal{A}| = k\}$ (*liczba Sterlinga pierwszego rodzaju* $\left[{n \atop k} \right]$ to liczba permutacji zbioru n-elementowego mających rozkład na k permutacji cyklicznych).

Oczywiście $\left\{ {n \atop n} \right\} = 1$, $n \geqslant 1 \Rightarrow \left\{ {n \atop 0} \right\} = 0 \wedge \left\{ {n \atop 1} \right\} = 1$, $k > n \Rightarrow \left\{ {n \atop k} \right\} = 0$.

(a) Wykazać, że $n \geqslant 2 \Rightarrow \left\{ {n \atop 2} \right\} = 2^{n-1} - 1$.

(b) Dla $k, n \geqslant 1$ znaleźć dwa wzory rekurencyjne na $\left\{ {n \atop k} \right\}$, dzieląc zbiór k-elementowych podziałów $\mathcal{A}$ zbioru I_n na dwa różne sposoby:

1°) ze względu na moc zbioru $A \in \mathcal{A}$ takiego, że $n \in A$

2°) $\operatorname{Part}_k I_n = \{\mathcal{A} \mid \{n\} \in \mathcal{A}\} \cup \{\mathcal{A} \mid \{n\} \notin \mathcal{A}\}$.

Narysować odpowiednik trójkąta Pascale dla $\left\{ {n \atop k} \right\}$; $n, k \leqslant 5$.

47. Liczba wszystkich relacji w zbiorze I_n $(n = 0, 1, 2, \dots)$ równa jest $|\mathcal{P} I_n^2| = 2^{n^2}$. Ile jest w I_n relacji:

a) zwrotnych?
b) symetrycznych?
c) zwrotnych i symetrycznych?
d) antysymetrycznych?
e) zwrotnych i antysymetrycznych?
f) spójnych?
g) spójnych i antysymetrycznych?
h) liniowo porządkujących?
i) przechodnich, dla $n = 2$? (Nie znamy zwartej formuły dla liczby τ_n relacji przechodnich w zbiorze n-elementowym; wartości τ_n dla małych n znajdziemy, np. w `oeis.org//A006905`).

48. Porównując punkty g) i h) w poprzednim zadaniu otrzymujemy nierówność:

$$\forall\ n \in \mathbb{N} : n! \leqslant 2^{\frac{n^2 - n}{2}}.$$

Udowodnić ją indukcyjnie.

49. Dla $n \in \mathbb{N}$ obliczyć:

$$\alpha_n = \sum_{X \subset I_n} |X|, \quad \beta_n = \sum_{X, Y \subset I_n} |X \cap Y|, \quad \gamma_n = \sum_{\substack{X, Y \subset I_n \\ X \neq Y}} |X \cap Y|.$$

50. Wykazać, że dla $n \in N^*$:

$$f(n) := \min\{k \in \mathbb{N} \mid \underset{|\mathcal{A}| = k}{\forall\, \mathcal{A} \subset \mathcal{P} I_n}\ \underset{A \neq B}{\exists\, A, B \in \mathcal{A}} : A \cap B = \varnothing\} = 2^{n-1} + 1.$$

Wskazówka: Wykorzystać zasadę szufladkową Dirichleta.

51. Dla naturalnego n określamy $n!!$ (i analogicznie $n!!!$, $n!^4$,$\dots$), kładąc $0!! = 1!! = 1$, $n \geqslant 2 \;\Rightarrow\; n!! = (n-2)!! \cdot n$.

a) Wykazać, że:

$2 \mid n \;\Rightarrow\; n!! = 2^{\frac{n}{2}} \cdot \left(\dfrac{n}{2}\right)!$

$2 \nmid n \;\Rightarrow\; n!! = \dfrac{(n+1)!}{(n+1)!!} = \dfrac{(n+1)!}{2^{\frac{n+1}{2}} \cdot \left(\frac{n+1}{2}\right)!}$

b) Wykazać, że dla n, $k \in \mathbb{N}^*$:

$$\prod_{i=1}^{k}\sum_{j=1}^{n}(i+j-1) = \frac{n^k(n+2k-1)!!}{2^k(n-1)!!}$$

(por. zadanie D1.24 z [**Marek... 75**, s. 133]).

52. Dla $n \in \mathbb{N}^*$ ile jest liczb n-cyfrowych (w dziesiętnym systemie pozycyjnym) o wszystkich cyfrach różnych?

53. Dla $n \in \mathbb{N}^*$ wypisujemy liczby 1, 2, 3, …, $\underbrace{55\ldots5}_{n}$. Niech α_n oznacza liczbę wystąpień cyfry 9 w powyższym ciągu.
$\alpha_n = ?$
Wypisać wartości α_n dla $n \leqslant 5$.

54. Warunek z zadania 40 nie określa klasy Fin zbiorów skończonych w ZF — jest to tylko warunek konieczny (zob. np. [**Herrlich 06**]). Warunek konieczny i wystarczający (w ZF), nie angażujący liczb naturalnych, podał w roku 1924 A. Tarski:

$$\forall\ X\ (X \in \mathrm{Fin} \Leftrightarrow \forall\ \varnothing \neq \mathcal{A} \subset \mathcal{P}X\ \exists\, M - \text{element maksymalny } \mathcal{A}).$$

Udowodnić tę równoważność.

55. Zredagować rachunek z kroku indukcyjnego dowodu formuły włączania–wyłączania w postaci ogólnej (59). (Potrzebna jest tu umiejętność operowania sumami skończonymi — polecić można np. [**Graham... 02**, rozdział 2.3.]).

56. Dla $k, n \in \mathbb{N}$ wyznaczyć $a_{k,n} = |\operatorname{Sur}(k,n)|$; $a_{4,3} = ?$
Wskazówka: $a_{k,n} = |\operatorname{Sur}(I_k, I_n)|$, $\operatorname{Sur}(I_k, I_n) = \operatorname{Map}(I_k, I_n) \setminus \bigcup\limits_{i=1}^{n} A_i$, gdzie $A_i = \{f : I_k \to I_n \mid i \notin \operatorname{Im} f\}$. Zastosować ogólną formułę włączania–wyłączania (59).

Dla kontroli można policzyć $a_{4,3}$ (ogólniej $a_{n+1,n}$), stosując zasadę szufladkową Dirichleta (53).

57. Udowodnić własności (66)–(68) liczb Fermata: $F_n = 2^{2^n} + 1$.

58. Udowodnić, że dla $p \in \mathbb{P}$ funkcja $\nu_p : \mathbb{N}^* \to \mathbb{N}$ spełnia warunki:

(a) $\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b)$, $a \mid b \Rightarrow \nu_p(\frac{b}{a}) = \nu_p(b) - \nu_p(a)$
(b) $\nu_p((a,b)) = \nu_p(a) \cap \nu_p(b)$
(c) $\nu_p([a,b]) = \nu_p(a) \cup \nu_p(b)$
(d) $\nu_p(a+b) \geqslant \nu_p(a) \cap \nu_p(b)$.

59. Udowodnić, że jeżeli funkcja $\nu : \mathbb{N}^* \to \mathbb{N}$ ma własności (a) i (b) z zadania 58, to $\nu = 0$ lub $\nu = k \cdot \nu_p$ dla pewnych $k \in \mathbb{N}^*$, $p \in \mathbb{P}$.

60*. Niech $p \in \mathbb{P}$; $k, n \in \mathbb{N}$, $1 \leqslant k \leqslant p^n - 1$ (a więc $\nu_p(k) < n$).
Wykazać, że $\nu_p\left(\binom{p^n}{k}\right) = n - \nu_p(k)$.

Wskazówka: Wykorzystać formułę Legendre'a: $\nu_p(n!) = \sum\limits_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$ $\quad \langle \nu_p(n!) = \sum\limits_{i=1}^{\infty} \alpha_i$, gdzie $\alpha_i = |\{i \in I_n \mid p^k \cdot i \leqslant n\}| = \left[\frac{n}{p^i}\right] \rangle$.

61. Niech p, q będą kolejnymi liczbami pierwszymi; $p, q \in \mathbb{P}$, $p < q$, $\forall\, n \in \mathbb{N}$ ($p < n < q \;\Rightarrow\; n \notin \mathbb{P}$). Wykazać dla liczby naturalnej n takiej, że $p < n < q^2$ zachodzi równoważność:

$$n \in \mathbb{P} \iff \exists\, a, b \in \mathbb{N}\, (n = a - b,\ a \perp b,\ \prod_{\substack{r \in \mathbb{P} \\ r \leqslant p}} r \mid ab).$$

62. Udowodnić poniższe kryterium skończoności zbioru X (por. zadanie 54):

$$X \in \mathrm{Fin} \iff \exists\, f : X \to X\ \forall\, \varnothing \neq A \subsetneq X : f(A) \not\subset A.$$

Wykazać, że funkcja f w prawej stronie tej równoważności jest permutacją cykliczną zbioru X.

63. Udowodnić (w ZF), że:

(a) W łańcuchu (zbiorze liniowo uporządkowanym) X skończonym i niepustym istnieje element największy (najmniejszy).

(b) W posecie X skończonym i niepustym istnieje element maksymalny (minimalny).

(c) Jeżeli w posecie skończonym X element a jest jedynym elementem maksymalnym, to jest on elementem największym w X. (Założenie skończoności zbioru X jest istotne — por. zadanie 8).

64. Na mocy 63(a) (poprzednie zadanie)

$$\mathrm{Fin} \subset \mathcal{T} = \{X \mid \forall\, R\, (R - \text{porządek liniowy w } X \;\Rightarrow\; R - \text{dobry porządek w } X)\}.$$

Zbiory należące do klasy $\mathcal{T}$ nazywamy *skończonymi w sensie Tarskiego*.

Wykazać (w ZF), że:

$$\mathrm{Fin} = \mathcal{T} \iff \forall\, X\, \exists\, R - \text{porządek liniowy w } X.$$

(por. zadanie 6.6).

65. Udowodnić, że jeżeli w posecie X podzbiory A i B są dwoma różnymi łańcuchami maksymalnymi, to

$$\exists\, a \in A, b \in B : a \perp b,$$

gdzie dla $a, b \in X$ zapis $a \perp b$ oznacza, że elementy a, b są *nieporównywalne*;

$$a \perp b \;:\!\iff\; \neg(a \leqslant b \vee b \leqslant a).$$

66*. W zbiorze $\mathcal{F}$ podzbiorów skończonych zbioru $\mathbb{N} = \{0, 1, 2, \dots\}$ ($\mathcal{F} = \mathrm{Fin} \cap \mathcal{P}\mathbb{N}$) określamy relację

$$A \leqslant B \;:\!\iff\; A = B \vee \max(A \dot{-} B) \in B.$$

(i) Wykazać, że tak określona relacja jest dobrym porządkiem w $\mathcal{F}$ i ustawić w tym porządku wszystkie elementy zbioru $\mathcal{P}3$ (jest ich $2^3 = 8$).

(ii) Wykazać, że $\mathrm{ord}(\mathcal{F}, \leqslant) = \omega$.

Wskazówka: Zauważyć, że dla $A, B \in \mathcal{F}$: $\varnothing \leqslant A$ oraz $\varnothing \neq A < B \Rightarrow \max A \leqslant \max B$.

67. *Ciąg kumulacyjny* $V : \mathrm{Ord} \to \mathbb{V}$ określamy indukcyjnie: $V_0 = \varnothing$, $V_{\alpha+1} = \mathcal{P}V_\alpha$, $\lambda \in \mathrm{Lim} \Rightarrow V_\lambda = \bigcup_{\xi<\lambda} V_\xi$.

Wykazać, że dla $\alpha, \beta \in \mathrm{Ord}$, $\lambda \in \mathrm{Lim}$:

(a) $V_\alpha \in T =$ klasa wszystkich zbiorów tranzytywnych (zadanie 2)

(b) $\alpha < \beta \Rightarrow V_\alpha \in V_\beta$

(c) $\alpha \leqslant \beta \Rightarrow V_\alpha \subset V_\beta$

(d) $\alpha \in V_{\alpha+1} \setminus V_\alpha$

(e) $V_\omega \in \mathrm{Univ}$, $V_\omega = \bigcap \mathrm{Univ}$

(f) $V_\alpha^2 \subset V_{\alpha+2}$, $V_\lambda^2 \subset V_\lambda$.

68. Udowodnić *twierdzenie o wypełnieniu*:

$$\bigcup_{\alpha\in\mathrm{Ord}} V_\alpha = \mathbb{V}, \text{ gdzie } V \text{ jest ciągiem kumulacyjnym z poprzedniego zadania.}$$

Wskazówka: W dowodzie nie wprost wykorzystać zasadę regularności (zadanie 2).

69. Na mocy twierdzenia o wypełnieniu (zadanie 68) każdej klasie A można przyporządkować *indeks*:

$$\rho(A) := \bigcap\{\alpha \in \mathrm{Ord} \mid A \cap V_\alpha \neq \varnothing\}.$$

Wówczas:
$A \neq \varnothing \Rightarrow \rho(A) \in \mathrm{Ord} \ \wedge\ A \cap V_{\rho(A)} \neq \varnothing \ \wedge\ \forall\, \beta \in \mathrm{Ord} : A \cap V_\beta \neq \varnothing \Rightarrow \rho(A) \leqslant \beta$; tak więc niepustej klasie A przyporządkowaliśmy kanonicznie niepusty podzbiór $A^\square := A \cap V_{\rho(A)}$.

Możemy teraz określić funkcję $m : \mathbb{V} \to \mathbb{V}$, która każdemu zbiorowi x przyporządkowuje jego *moc*, inaczej *liczbę kardynalną*

$$m(x) := \{y \mid x \sim y\}^\square,$$

gdzie $\sim$ jest relacją równoliczności w klasie $\mathbb{V}$ (zadanie 4.5), a następnie klasę liczb kardynalnych $\mathcal{C} := \mathrm{Im}(m)$. (Uwaga: Cały czas pracujemy w ZF — nie korzystamy z AC).

(a) Wykazać, że $\forall\, x, y : x \sim y \Rightarrow m(x) = m(y)$.

(b) Określić w klasie $\mathcal{C}$ relacje porządku (częściowego) „$\leqslant$” tak, żeby $\forall\, x, y : x \subset y \Rightarrow m(x) \leqslant m(y)$.

(c) Określić w naturalny sposób w klasie $\mathcal{C}$ działania arytmetyczne: dodawanie, mnożenie, potęgowanie. Ich własności?

70. Po odpowiednim utożsamieniu można przyjąć, że $\mathbb{N} \subset \mathcal{C}$, gdzie $\mathcal{C}$ jest klasą liczb kardynalnych w sensie zadania 69. Dlaczego?

71. Korzystając z twierdzenia o wypełnieniu (zadanie 68) określa się też *funkcję rangi* (*rank function*) $\mathrm{rk} : \mathbb{V} \to \mathrm{Ord}$,

$$\mathrm{rk}\, x = \bigcap\{\alpha \in \mathrm{Ord} \mid x \subset V_\alpha\}.$$

Dla niepustej klasy A wyrazić $\rho(A)$ za pomocą funkcji rk.

72. Wykazać, że dla $\alpha \in \mathrm{Ord}$ i dowolnych zbiorów x, y:

(a) $x \subset V_{\mathrm{rk}\, x}$, $x \subset V_\alpha \;\Rightarrow\; \mathrm{rk}\, x \leqslant \alpha$

(b) $x \subset y \;\Rightarrow\; \mathrm{rk}\, x \leqslant \mathrm{rk}\, y$

(c) $V_\alpha = \{x \mid \mathrm{rk}\, x < \alpha\}$

(d) $x \in y \;\Rightarrow\; \mathrm{rk}\, x < \mathrm{rk}\, y$

(e) $\mathrm{rk}\, V_\alpha = \alpha$

(f) $V_{\alpha+1} \setminus V_\alpha = \{x \mid \mathrm{rk}\, x = \alpha\}$

(g) $\mathrm{rk}\, \alpha = \alpha$

(h) $\mathrm{rk}\, x = 0 \Leftrightarrow x = \varnothing$, $\quad \mathrm{rk}\, x = 1 \Leftrightarrow x = 1$

(i) $\mathrm{rk}\, \mathcal{P}x = \mathrm{rk}\{x\} = \mathrm{rk}\, x + 1$

(j) $\mathrm{rk}\, x = \bigcup\{\mathrm{rk}\, y + 1 \mid y \in x\} = \bigcap\{\alpha \in \mathrm{Ord} \mid \forall\, y \in x : \mathrm{rk}\, y < \alpha\}$

(k) $x \neq \varnothing \;\Rightarrow\; \mathrm{rk} \bigcap x < \mathrm{rk}\, x$

(l) $\mathrm{rk} \bigcup x = \bigcup \mathrm{rk}\, x$.

73. Wykorzystując funkcję rangi (zadania 71, 72) udowodnić, że:

$$\mathrm{Ord} = T \cap \mathcal{P}T,$$

gdzie T jest klasą wszystkich zbiorów tranzytywnych (zadanie 2).

74. Uogólnieniem pojęcia dobrego porządku jest pojęcie relacji ufundowanej (w kryterium Tarskiego pomijamy warunek spójności).
R – *ufundowana* w A $:\Leftrightarrow$ $\forall\, Z\ (\varnothing \neq Z \subset A \implies \exists\, x$ – element R-minimalny $Z)$ $\wedge$ $\forall\, a \in A : S_a(A, R) \in \mathbb{V}$.

Na przykład relacja $\mathbb{E} = \{(x, y) \mid x \in y \vee x = y\}$ jest ufundowana w A (A – dowolna klasa).

Udowodnić dla relacji ufundowanej poniższy odpowiednik zasady minimum z rozdziału 4:

Zasada elementu minimalnego:
R – ufundowana w $A \wedge \varnothing \neq B \subset A \implies \exists\, b$ – element R-minimalny B (por. zadanie 2.(iv)).

75. Sformułować i udowodnić dla relacji R ufundowanej w klasie A (zadanie 74) poniższy odpowiednik lematu o przesunięciu w prawo dla relacji dobrego porządku (rozdział 4): *Lemat o niecofaniu*:

R – ufundowana w A, B – R-odcinek A, $f : B \to A$, f – R-R-silnie rosnąca $\implies$ $\forall\, x \in B : \neg f(x) \underset{R}{<} x$.

76. Udowodnić *twierdzenie o indukcji dla relacji ufundowanej*:

R – ufundowana w A, $\forall\, a \in A\ [S_a(A, R) \subset B \;\Rightarrow\; a \in B] \implies A \subset B$.

W szczególności dla relacji $\mathbb{E}$ otrzymujemy tzw. *twierdzenie o indukcji ze względu na przynależność*:
$\forall\, a \in A\ (a \cap A \subset B \;\Rightarrow\; a \in B) \implies A \subset B$.

77*. Udowodnić *twierdzenie o definiowaniu indukcyjnym dla relacji ufundowanej*:
Jeżeli R jest relacją ufundowaną w klasie A,
$H : A \times \mathrm{Map}^0(A, B) \to B$
$f = \bigcup \Phi$, gdzie
$\Phi = \{\varphi : A \multimap\!\!\to B \mid \mathrm{Dom}\,\varphi$ – R-odcinek $A \ \wedge \ \forall\, x \in \mathrm{Dom}\,\varphi : \varphi(x) = H(x, \varphi|_{S_x(A,R)})\}$,
to:
1°) $f : A \to B \wedge \forall\, x \in A : f(x) = H(x, f|_{S_x(A,R)})$
2°) $g : A \to B \wedge \forall\, x \in A : g(x) = H(x, g|_{S_x(A,R)})$
$\implies f = g$.
O funkcji f mówimy, że jest określona R-indukcyjnie warunkiem:

$$\forall\, x \in A : f(x) = H(x, f|_{S_x(A,R)}),$$

z którego funkcję H można odtworzyć.

Wskazówka: Naśladować dowód twierdzenia o definiowaniu indukcyjnym.

78*. Twierdzenie o definiowanie indukcyjnym (zadanie 77*) zastosowane do relacji $\mathbb{E}$ (przynależność lub równość) prowadzi do ważnego w teorii modeli teoriomnogościowych *twierdzenia Mostowskiego o kolapsie*:

Jeżeli A jest klasą *ekstensjonalną*, tzn. taką, w której jest spełniony aksjomat ekstensjonalności (A1 z rozdziału 3.):

$$\forall\, x, y \in A\ [\forall\, z \in A\ (z \in x \Leftrightarrow z \in y) \ \Rightarrow \ x = y],$$

funkcja $f : A \to \mathbb{V}$ określona jest warunkiem $\mathbb{E}$-indukcyjnym $\forall\, x \in A : f(x) = \mathrm{Im}(f|_{x \cap A})$, to:
(i) Klasa $B := \mathrm{Im}\, f$ jest tranzytywna, $f : A \hookrightarrow\!\!\!\!\to B$, $\forall\, x, y \in A\ [x \in y \Leftrightarrow f(x) \in f(y)]$.
(ii) Jeżeli klasa C jest tranzytywna, $g : A \hookrightarrow\!\!\!\!\to C$ i $\forall\, x, y \in A\ [x \in y \Leftrightarrow g(x) \in g(y)]$, to $f = g$.
(iii) Jeżeli klasa T jest tranzytywna, $T \subset A$, to $f|_{T \cup (A \cap \mathcal{P}T))} \subset \mathrm{id}$.

5.3. Odpowiedzi

1. Dowody są bezproblemowe.
Należy tylko zachować kolejność. Na przykład dla liczby porządkowej A i elementu $a \in A$

$$S_a(A, \mathbb{E}) = \{x \in A \mid x \in a\} = A \cap a = a.$$

2.
(i) Tak. $\langle$Jeżeli $x \in y \in \bigcup C$, to $\exists)\, z \in C$; $y \in z$, i wówczas $z \in T$, $y \subset z$, $x \in z$, $x \in \bigcup C\rangle$.
(ii) Oczywiście $x \subset \bar{x}$.
$\bar{x} \in T$, gdyż dla $y \in z \in \bar{x}\ \exists)\, n \in \mathbb{N}$; $z \in s_n$, a więc $y \in \bigcup s_n = s_{n+1} \subset \bar{x}$.
Jeżeli $x \subset y \in T$, to $s_0 \subset y$, i jeżeli dla $n \in \mathbb{N}$ $s_n \subset y$, to $s_{n+1} = \bigcup s_n \subset \bigcup y \subset y$, a więc na mocy zasady indukcji $\bar{x} \subset y$.

Wreszcie, jeżeli $x \in T$, to $\bar{x} \subset x$, a więc $x = \bar{x}$; na odwrót, jeżeli $x = \bar{x}$, to $x \in T$, gdyż $\bar{x} \in T$.

(iii) Według (2): $x \subset \bar{x}$ oraz $\bar{x} \in T$, a więc $\bar{\bar{x}} = \bar{x}$. Jeżeli $x \subset y$, to $x \subset y \subset \bar{y}$, $x \subset \bar{y} \in T$, a więc $\bar{x} \subset \bar{y}$.

(iv) HP: $A \neq \varnothing \wedge \forall\, a \in A : a \cap A \neq \varnothing$. $\exists)\, a \in A$. $\varnothing \neq a \cap A \subset \bar{a} \cap A$. $\mathbb{V} \ni \bar{a} \cap A \neq \varnothing$, a więc $\exists)\, x \in \bar{a} \cap A : x \cap \bar{a} \cap A = \varnothing$. Ponieważ $x \cap A \neq \varnothing$, więc $\exists)\, y \in x \cap A$. Ale $y \in x \in \bar{a}$, skąd $y \in \bar{a}$, czyli $y \in \bar{a} \cap x \cap A = \varnothing$ ↯.

3. Ponieważ $\mathbb{N} \in H$, więc $\bigcap H \subset \mathbb{N}$.

Na mocy zasady indukcji: $\mathbb{N} \subset \bigcap H \quad \langle 0 \in \bigcap H$. Jeżeli $x \in \bigcap H$, to $\forall\, z \in H : x \in z$, $\operatorname{seq} x \in z$, a więc $\operatorname{seq} x \in \bigcap H\rangle$.

4. Stosując uproszczoną notację z zadania 2.2

$$(XY = X \cap Y,\ X^{\neg} = \mathbb{V} \setminus X,\ \text{gdzie } \mathbb{V} = \bigcup_{n\in\mathbb{N}} (A_n \cap B_n)),$$

możemy zapisać:

$$\begin{aligned} L &= \bigcap_{n\in\mathbb{N}} (A_n \setminus B_n) = \bigcap_{n\in\mathbb{N}} A_n B_n^{\neg} \\ R &= \bigcap_{n\in\mathbb{N}} A_n \cap (\bigcap_{n\in\mathbb{N}} B_n)^{\neg} = \bigcap_{n\in\mathbb{N}} A_n \bigcup_{m\in\mathbb{N}} B_m^{\neg} \\ &= \bigcup_{m\in\mathbb{N}} \bigcap_{n\in\mathbb{N}} A_n B_m^{\neg} \supset \bigcap_{m\in\mathbb{N}} \bigcap_{n\in\mathbb{N}} A_n B_m^{\neg} = \bigcap_{n\in\mathbb{N}} A_n B_n^{\neg} = L. \end{aligned}$$

Tak więc $L \subset R$.

Analogicznie jak w zadaniu 3.8 łatwo sprawdzić, że:

$$\bigcap_{n\in\mathbb{N}} (A_n \setminus B_n) = \bigcap_{n\in\mathbb{N}} A_n \setminus \bigcup_{n\in\mathbb{N}} B_n,$$

skąd natychmiast wynika inkluzja $L \subset R \quad \langle$gdyż $\bigcap_{n\in\mathbb{N}} B_n \subset \bigcup_{n\in\mathbb{N}} B_n\rangle$.

Ponadto, oznaczając $X = \bigcap_{n\in\mathbb{N}} A_n$, $Y = \bigcup_{n\in\mathbb{N}} B_n$, $Z = \bigcap_{n\in\mathbb{N}} B_n$, i korzystając z zależności:

$$Z \subset Y \ \Rightarrow\ [X \setminus Y = X \setminus Z \Leftrightarrow X \cap (Y \setminus Z) = \varnothing]$$

otrzymujemy równoważność

$$L = R \iff \bigcap_{n\in\mathbb{N}} A_n \cap (\bigcup_{n\in\mathbb{N}} B_n \setminus \bigcap_{n\in\mathbb{N}} B_n) = \varnothing.$$

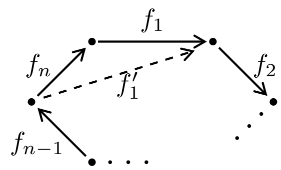
Jako najprostszy przykład na inkluzję silną $L \subsetneq R$ można wziąć:

$$A_n = \{0\} = B_0, \quad B_k = \varnothing \text{ dla } k > 0.$$

Wówczas $L = \varnothing \subsetneq R = \{0\}$.

5. HP: $f \neq \mathrm{id}_A$. Niech $\alpha = \bigcap\{\xi \in A \mid f(\xi) < \xi\}$. Wówczas $\alpha \in A$, $f(\alpha) < \alpha$, i z minimalności α wynika, że $f(f(\alpha)) = f(\alpha)$; czyli $f(\alpha) = \alpha \quad \langle f$ jest injekcją$\rangle$ ↯.

6*. Przyjmując oznaczenia z rozwiązania zadania 3.21 (w szczególności: $fg = g \circ f$), należy udowodnić, że dla danych funkcji



takich, że wszystkie złożenia

$$f_1 f_2 \dots f_{n-1} f_n, \quad f_2 f_3 \dots f_n f_1, \quad \dots, \quad f_n f_1 \dots f_{n-2} f_{n-1}$$

są injekcjami lub surjekcjami, przy czym co najmniej jedno z nich jest injekcją i co najmniej jedno z nich jest surjekcją, wszystkie funkcje $f_1, \dots, f_n$ są bijekcjami.

Dowód indukcją na n. Według zadań z rozdziału 3 twierdzenie jest prawdziwe dla $n \leqslant 3$. Załóżmy więc, że $n \geqslant 4$ i twierdzenie jest prawdziwe dla $n-1$ funkcji. Bez straty ogólności można przyjąć, że:

(*) $$f_1 f_2 \dots f_{n-1} f_n : \hookrightarrow, \ f_2 f_3 \dots f_n f_1 : \twoheadrightarrow \quad \langle\text{przenumerowanie}\rangle.$$

Wówczas $f_1 : \hookrightarrow$, $f_1 : \twoheadrightarrow$, a więc $f_1 : \hookrightarrow\!\!\!\!\!\twoheadrightarrow$. Traktując bijekcję f_1 jako identyfikację i korzystając z założenia indukcyjnego łatwo uzyskamy tezę.

Dokładniej, rozważmy dwa przypadki:

1) Wśród funkcji:

(**) $$f_3 f_4 \dots f_n f_1 f_2, \quad \dots, \quad f_n f_1 \dots f_{n-2} f_{n-1}$$

przynajmniej jedna jest injekcją. Oznaczmy: $f_1' = f_n f_1$, $f_i' = f_i$ dla $i = 2, \dots, n-1$. Wówczas

$$\begin{cases} f_1' f_2' \dots f_{n-2}' f_{n-1}' & = f_n f_1 f_2 \dots f_{n-2} f_{n-1} \\ f_2' f_3' \dots f_{n-1}' f_1' & = f_2 f_3 \dots f_{n-1} f_n f_1 \\ f_3' f_4' \dots f_1' f_2' & = f_3 f_4 \dots f_n f_1 f_2 \\ \dots & \dots \\ f_{n-1}' f_1' \dots f_{n-3}' f_{n-2}' & = f_{n-1} f_n f_1 \dots f_{n-3} f_{n-2} \end{cases}$$

i druga z tych funkcji jest surjekcją (według (*)), natomiast pozostałe są injekcjami lub surjekcjami, przy czym (według (**)) przynajmniej jedna z nich jest injekcją.

Zatem, na mocy założenia indukcyjnego, wszystkie funkcje $f_1', \dots, f_{n-1}'$ są bijekcjami, skąd wynika teza.

2) Wszystkie funkcje (**) są surjekcjami.

Indukcją na $k = 1, 2, \dots, n$ wykażemy, że $f_k : \hookrightarrow\!\!\!\!\!\twoheadrightarrow$. Należy wykonać krok indukcyjny. Załóżmy więc, że $k \geqslant 2$ i wszystkie funkcje $f_1, \dots, f_{k-1}$ są bijekcjami.

Jeśli $k < n$, to według (*): $f_k \dots f_{n-1} f_n : \hookrightarrow$. Ponieważ $f_{k+1} f_{k+2} \dots f_{k-1} f_k : \twoheadrightarrow$, więc $f_k : \twoheadrightarrow$, i ostatecznie $f_k : \hookrightarrow\!\!\!\!\!\twoheadrightarrow$.

Dla $k = n$ bijektywność f_n wynika z (*) i z założenia indukcyjnego: $f_1, \dots, f_{n-1} : \hookrightarrow\!\!\!\!\!\twoheadrightarrow$.

7. HP: $\operatorname{ord} B = \beta < \alpha = \operatorname{ord} A$.

Oznaczmy $f = \mathrm{nat}_A$, $g = \mathrm{nat}_B$; tak więc $f : \alpha \xrightarrow{\sim} A$, $g : \beta \xrightarrow{\sim} B$, czyli $g^{-1} \circ f : \alpha \hookrightarrow \beta$ – rosnąca, i wg lematu o przesunięciu w prawo: $\beta \leqslant g^{-1}(f(\beta)) < \beta$ ↯.

8. Wniosek z opisanej w (11) charakteryzacji $\bigcup C$ dla $C \subset \mathrm{Ord}$. Bezpośredni rachunek też szybko prowadzi do celu.

9. Dowody indukcją ze względu na ostatni człon lub nie wprost.
Na przykład (26): $0 + \alpha = \alpha$.

1) $\alpha = 0$. $0 + 0 = 0$

2) $\alpha = \beta + 1$. $0 + (\beta + 1) = (0 + \beta) + 1 = \beta + 1$

3) $\alpha = \lambda \in \mathrm{Lim}$. $0 + \lambda = \bigcup\{0 + \xi \mid \xi < \lambda\} = \bigcup\{\xi \mid \xi < \lambda\} = \bigcup \lambda = \lambda$.

Analogicznie dla (27)–(36) (we wskazanej kolejności). Pewne trudności może sprawiać, „krok graniczny”, gdy $\alpha = \lambda \in \mathrm{Lim}$.
Na przykład w dowodzie prawa (30) (łączność dodawania).
Zakładamy, że $\forall\ \xi < \lambda : (\alpha+\beta)+\xi = \alpha+(\beta+\xi)$; chcemy dowieść, że $L = (\alpha+\beta)+\lambda = \alpha + (\beta + \lambda) = R$.
HP: $L \neq R$. Możliwe są dwa przypadki:

1) $L < R$.
Według (27) $\beta+\lambda \in \mathrm{Lim}$, więc $R = \bigcup\{\alpha+\eta \mid \eta < \beta+\lambda\}$, czyli $\exists)\, \eta < \beta+\lambda : L < \alpha+\eta$. Ale $\beta + \lambda = \bigcup\{\beta + \xi \mid \xi < \lambda\}$, a więc $\exists)\, \xi < \lambda : \eta < \beta + \xi$, skąd, według (28), $\alpha + \eta < \alpha + (\beta + \xi) = (\alpha + \beta) + \xi < (\alpha + \beta) + \lambda = L$ ↯.

2) $R < L$. Znów skorzystamy z (28), $\exists)\, \xi < \lambda : R < (\alpha + \beta) + \xi = \alpha + (\beta + \xi) < \alpha + (\beta + \lambda) = R$ ↯.

10.

1) Istnienie: Indukcja na α.

2) Jednoznaczność:

Należy udowodnić, że dla $\lambda, \mu \in \mathrm{Lim}_0 = \mathrm{Lim} \cup \{0\}$ i $n, m \in \mathbb{N} : \lambda + n = \mu + m \Rightarrow \lambda = \mu \wedge n = m$.
Zastosujemy indukcję na n:
Dla $n = 0$: $\lambda+0 = \lambda$ i gdyby $m = k+1$, to $\lambda = n+m = \mu+(k+1) = (\mu+k)+1 \notin \mathrm{Lim}_0$ ↯.
Dla $n = k + 1$: $\lambda + n = (\lambda + k) + 1 \in \mathrm{Seq}$, a więc $\mu + m \in \mathrm{Seq}$, $m \in \mathrm{Seq}$, $m = l + 1$, $(\lambda + k) + 1 = (\mu + l) + 1$, $\lambda + k = \mu + l$, $\lambda = \mu$, $k = l$, $n = m$.

11. Indukcja.
Na przykład przemienność dodawania w $\mathbb{N}$:

Wstępnie dowodzimy indukcją na $n \in \mathbb{N}$, że $n + 1 = 1 + n$.
$\langle$1) Według (26) $0 + 1 = 1 = 1 + 0$.
2) Jeżeli $n = k + 1$ i $k + 1 = 1 + k$, to korzystając z (30): $n + 1 = (k + 1) + 1 = (1 + k) + 1 = 1 + (k + 1) = 1 + n\rangle$.

Następnie dla $n, m \in \mathbb{N}$ indukcją na m dowodzimy, że $n + m = m + n$.

1) Według (26) $0 + n = n = n + 0$.

2) Jeżeli $m = k+1$ i $n+k = k+n$, to $n+m = n+(k+1) = (n+k)+1 = (k+n)+1 = k + (n + 1) = k + (1 + n) = (k + 1) + n = m + n$.

12*. $\beta - \alpha := \bigcap\{\gamma \in \mathrm{Ord} \mid \alpha \leqslant \beta \ \Rightarrow\ \alpha + \gamma = \beta\}$.
Jeżeli $\beta < \alpha$, to $\beta - \alpha = \bigcap \mathrm{Ord} = 0$. Tak więc określiliśmy w gruncie rzeczy tak zwaną *różnicę zredukowaną*.

Załóżmy teraz, że $\alpha \leqslant \beta$.
Wówczas $\beta - \alpha = \bigcap\{\gamma \in \mathrm{Ord} \mid \alpha + \gamma = \beta\}$, i dla wykazania poprawności naszej definicji należy udowodnić dwie rzeczy:

1°) $\exists\gamma \ \in \mathrm{Ord} : \alpha + \gamma = \beta$

2°) $\forall\ \gamma, \delta \in \mathrm{Ord} : \alpha + \gamma = \alpha + \delta = \beta \ \Rightarrow\ \gamma = \delta$.

Punkt 2°) jest wnioskiem z (28).
Dla dowodu punktu 1°), czyli istnienia, zastosujemy indukcję względem β:

i) Jeśli $\beta = \alpha$, to dla $\gamma = 0$ mamy $\alpha + 0 = \beta$.

ii) Jeśli $\alpha < \beta = \beta' + 1$ i 1°) zachodzi dla β', wówczas $\alpha < \beta'$ lub $\alpha = \beta'$.
Jeżeli $\alpha < \beta'$, to według założenia indukcyjnego $\exists\gamma' \in \mathrm{Ord})\beta' = \alpha + \gamma'$ i wówczas $\beta = (\alpha + \gamma') + 1 = \alpha + (\gamma' + 1)$, i bierzemy $\gamma = \gamma' + 1$.
Jeżeli zaś $\alpha = \beta'$, to $\beta = \alpha + 1$, i bierzemy $\gamma = 1$.

iii) Jeśli $\alpha < \beta = \lambda \in \mathrm{Lim}$ oraz $\forall\ \alpha \leqslant \eta < \lambda\ \exists\xi \in \mathrm{Ord} : \eta = \alpha + \xi$, wówczas $\exists) f : \lambda \setminus \alpha \to \mathrm{Ord}\ \forall\ \eta \in \lambda \setminus \alpha : \eta = \alpha + f(\eta) \quad \langle f(\eta) = \eta - \alpha\rangle$, i bierzemy $\gamma = \bigcup \mathrm{Im}\, f$.
Wówczas $\gamma \in \mathrm{Lim} \quad \langle$gdyż $\lambda \in \mathrm{Lim}\rangle$ oraz $\alpha + \gamma = \lambda \quad \langle$nie wprost$\rangle$.

13. Jeżeli $\alpha \leqslant \beta$, to $\alpha + (\beta - \alpha) = \beta$, i tak wyznaczona liczba $(\beta - \alpha)$ istnieje dokładnie jedna.
Tak więc korzystając z (23)–(36):

(i) $\alpha \leqslant \alpha$ i $\alpha + 0 = \alpha$, a więc $0 = \alpha - \alpha$; oraz $0 \leqslant \alpha$ i $0 + \alpha = \alpha$, a więc $\alpha = \alpha - 0$.

(ii) HP: $\beta := \lambda - \alpha \notin \mathrm{Lim}$. $\lambda = \alpha + \beta$, $\beta \neq 0 \quad \langle$HP: $\beta = 0$, $\lambda = \alpha < \lambda$ ϟ$\rangle$. Zatem $\exists)\,\gamma \in \mathrm{Ord} : \beta = \gamma + 1$, $\lambda = \alpha + (\gamma + 1) = (\alpha + \gamma) + 1 \notin \mathrm{Lim}$ ϟ.

(iii) Oznaczmy $\xi = \beta - \alpha$, $\eta = \gamma - \alpha$. HP: $\neg\xi < \eta$; wówczas $\eta \leqslant \xi$, $\gamma = \alpha + \eta \leqslant \alpha + \xi = \beta < \gamma$ ϟ.

(iv) Oznaczmy $\zeta = \gamma - \beta$, $\xi = \gamma - \alpha$. HP: $\neg\zeta \leqslant \xi$; wówczas $\xi < \zeta$, $\gamma = \alpha + \xi < \alpha + \zeta \leqslant \beta + \zeta = \gamma$ ϟ.

(v) Jeśli $\alpha \leqslant \beta$, to $\gamma\alpha \leqslant \gamma\beta$.
Oznaczmy: $\xi = \beta - \alpha$, $\eta = \gamma\beta - \gamma\alpha$; wówczas $\beta = \alpha + \xi$, $\gamma\beta = \gamma\alpha + \eta$. $\gamma\beta = \gamma(\alpha + \xi) = \gamma\alpha + \gamma\xi$, a więc $\gamma\beta - \gamma\alpha = \gamma\xi = \gamma(\beta - \alpha)$.

(vi) Oznaczmy $\xi = (\alpha + \beta) - \alpha$; tak więc $\alpha + \xi = \alpha + \beta$, skąd, na mocy (28), $\xi = \beta$.

(vii) Niech $\xi = (0 + 1) - 1$. Wówczas $1 + \xi = \omega + 1$.
Ponieważ $\omega + 1 = (1 + \omega) + 1 = 1 + (\omega + 1)$, więc $\xi = \omega + 1$. Tak więc $(\omega + 1) - 1 = \omega + 1 > \omega$.
Jako przykład na pierwszy człon koniunkcji może służyć nierówność: $(1 + \omega) - \omega = \omega - \omega = 0 < 1$.

14. Zakładamy, że α, $\beta \in \mathrm{Ord}$ i $\beta \neq 0$.

1) Jednoznaczność.
Niech $\alpha = \beta q + r = \beta q' + r'$, gdzie $r, r' < \beta$.

Gdyby $q \neq q'$, na przykład $q < q'$, to $q + 1 \leqslant q'$, a więc $\alpha = \beta q + r < \beta q + \beta = \beta(q + 1) \leqslant \beta q' \leqslant \beta q' + r' = \alpha$ ↯, zatem $q = q'$, a stąd, według (28), $r = r'$.

2) Istnienie.

Indukcja na α.

Krok wstępny ($\alpha = 0$) i krok sekwensowy ($\alpha = \alpha' + 1$) są bezproblemowe.

W kroku granicznym załóżmy, że dla każdego $\alpha < \lambda \in \mathrm{Lim}$ istnieją liczby q, r takie, że $\alpha = \beta q + r$ i $r < \beta$.

Ponieważ $1 \leqslant \beta$, więc według (31)–(33): $\lambda = 1 \cdot \lambda \leqslant \beta\lambda < \beta(\lambda + 1)$.

Niech $Q = \bigcap\{\gamma \in \mathrm{Ord} \mid \lambda < \beta\gamma\}$.

Wówczas $\lambda < \beta Q$ i $\forall\, \gamma \in \mathrm{Ord} : \lambda < \beta\gamma \;\Rightarrow\; Q \leqslant \gamma$. $Q \notin \mathrm{Lim}$ $\quad\langle$HP: $Q \in \mathrm{Lim}$. Wówczas $\lambda < \beta Q = \bigcup\limits_{\gamma<Q} \beta\gamma$, a więc $\exists)\, \gamma < Q : \lambda < \beta\gamma$, skąd $Q \leqslant \gamma$ ↯$\rangle$.

Ponieważ $Q \neq 0$ $\quad\langle\lambda < \beta Q\rangle$, więc $\exists)\, q \in \mathrm{Ord} : Q = q + 1$, $\lambda < \beta(q + 1)$. Wówczas $\beta q \leqslant \lambda$ $\quad\langle$HP: $\lambda < \beta q$. $Q \leqslant q < q+1 = Q$ ↯$\rangle$. Niech $r = \lambda - \beta q$. Wówczas $\lambda = \beta q + r$ oraz $r < \beta$ $\quad\langle$HP: $\beta \leqslant r$. $\lambda < \beta(q + 1) = \beta q + \beta \leqslant \beta q + r = \lambda$ ↯$\rangle$.

15.

(i) $0 = \alpha \cdot 0$, a więc $\alpha \mid 0$, w szczególności $0 \mid 0$. Jeśli $0 \mid \alpha$, to $\exists\, q : \alpha = 0 \cdot q = 0$.

(ii) $\alpha = 1 \cdot \alpha$. Jeśli $\alpha \mid 1$, to $\exists\, q)1 = \alpha q$, $q \neq 0$, $\alpha \neq 0$, gdyby $q > 1$, to $1 = \alpha q > \alpha \cdot 1 = \alpha$ ↯, a więc $q = 1$, $\alpha = 1$.

(iii) $\exists\, q)\beta = \alpha q$, $q \geqslant 1$, a więc $\beta = \alpha q \geqslant \alpha \cdot 1 = \alpha$.

(iv) Zwrotność: $\alpha \mid \alpha$, gdyż $\alpha = \alpha \cdot 1$.

Przechodniość: jeżeli $\alpha \mid \beta$ i $\beta \mid \gamma$, to $\exists)\, p, q : \beta = \alpha p$, $\gamma = \beta q$, a więc $\gamma = \alpha pq$, $\alpha \mid \gamma$.

Antysymetria: jeżeli $\alpha \mid \beta$ i $\beta \mid \alpha$, to $\exists)\ p, q : \beta = \alpha p$, $\alpha = \beta q$; HP: $\alpha \neq \beta$; wówczas $\alpha \neq 0 \neq \beta$, $p > 1$, $q > 1$, $pq > 1$, $\alpha = \alpha pq > \alpha$ ↯.

(v) $\exists)\, p, q : \beta = \alpha p$, $\gamma = \alpha q$, i wówczas $\beta\xi + \gamma\eta = \alpha(p\xi + q\eta)$, a więc $\alpha \mid \beta\xi + \gamma\eta$.

(vi) $\beta = \alpha p \;\Rightarrow\; \beta\gamma = \alpha p\gamma \wedge \gamma\beta = \gamma\alpha p$.

(vii) Wynika z przemienności mnożenia w $\mathbb{N}$.

(viii) Według twierdzenia o dzieleniu z resztą $\exists)\, q, r : \lambda = \omega q + r$, $r < \omega$; gdyby $r \neq 0$, to $r = s + 1$, $\lambda = \omega q + s + 1 \notin \mathrm{Lim}$, zatem $r = 0, \lambda = \omega q$, czyli $\omega \mid \lambda$.

16.

(i), (ii) Według definicji. Równość $1^\alpha = 1$ indukcją na α.

(iii) Według (i) $\alpha^\lambda \neq 0$. Gdyby $\alpha^\lambda = \beta + 1$, to $\beta < \alpha^\lambda$, a więc $\exists)\, \xi < \lambda : \beta < \alpha^\xi$, $\alpha^\lambda = \beta+1 \leqslant \alpha^\xi < \alpha^\xi \cdot \alpha = \alpha^{\xi+1} \leqslant \alpha^\lambda$ ↯. Teraz $\lambda^\alpha \in \mathrm{Lim}$, gdyż $\lambda^\alpha \neq 0$ i dla $\alpha = \beta+1$, $\lambda^\alpha = \lambda^\beta \cdot \lambda \in \mathrm{Lim}$.

(iv) Indukcja na γ:

I $\gamma = 0$. $\neg\beta < 0$

II $\gamma = \delta + 1$. $\beta \leqslant \delta$. Dwa przypadki:

1) $\beta = \delta$. Wówczas $\alpha^\beta = \alpha^\delta < \alpha^\delta \cdot \alpha = \alpha^{\delta+1} = \alpha^\gamma$.

2) $\beta < \delta$. Wówczas na mocy założenia indukcyjnego
$\alpha^\beta < \alpha^\delta < \alpha^\delta \cdot \alpha = \alpha^{\delta+1} = \alpha^\gamma$.

III $\gamma \in \mathrm{Lim}$. Wówczas $\beta < \beta+1 < \gamma$, a więc $\alpha^\beta < \alpha^\beta \cdot \alpha = \alpha^{\beta+1} \leqslant \bigcup_{\xi<\gamma} \alpha^\xi = \alpha^\gamma$.

(v)–(viii) Indukcja na γ.

17*. HP: $\omega^\alpha = \beta + \gamma$, $\beta \neq \omega^\alpha \neq \gamma$.
Wówczas $\beta \leqslant \beta+\gamma = \omega^\alpha$, $\gamma \leqslant \beta+\gamma = \omega^\alpha$, a więc $0 < \beta < \omega^\alpha$, $0 < \gamma < \omega^\alpha$.
Rozważmy dla α trzy przypadki: zerowy, sekwensowy i graniczny.

I $\alpha = 0$.
Wówczas $1 = \beta+\gamma$, a więc $\beta = 0$ lub $\gamma = 0$ ↯.

II $\alpha = \delta + 1$.
Z twierdzenia o dzieleniu z resztą (41) otrzymujemy: $\exists)\, q, r \in \mathrm{Ord} : \beta = \omega^\delta \cdot q + r \wedge r < \omega^\delta$.
$q < \omega$ $\langle$HP: $q \leqslant \omega$. Wówczas $\beta < \omega^\alpha = \omega^\delta + 1 = \omega^\delta \cdot \omega \leqslant \omega^\delta \cdot q + r = \beta$ ↯$\rangle$, a więc $q+1 < \omega$, $\omega - (q+1) = \omega$,

$$\gamma < \omega^\alpha = \omega^{\delta+1} = \omega^\delta\omega = \omega^\delta(\omega-(q+1)) = \omega^\alpha - \omega^\delta(q+1),$$

i ponieważ $\beta < \omega^\delta \cdot q + \omega^\delta = \omega^\delta(q+1)$, więc według (40) (iv): $\gamma < \omega^\alpha - \omega^\delta(q+1) \leqslant \omega^\alpha - \beta = \gamma$ ↯.

III $\alpha \in \mathrm{Lim}$.
Ponieważ $\beta < \omega^\alpha = \bigcup_{\xi<\alpha} \omega^\xi$, więc $\exists)\ \xi < \alpha : \beta < \omega^\xi$, i analogicznie $\exists)\ \xi' < \alpha : \gamma < \omega^{\xi'}$.
Wówczas dla $\eta = \xi \cup \xi' < \alpha$: $\beta < \omega^\eta$, $\gamma < \omega^\eta$, a więc $\omega^\alpha = \beta+\gamma < \omega^\eta + \omega^\eta = \omega^\eta \cdot 2 < \omega^\eta \cdot \omega = \omega^{\eta+1} < \omega^\alpha$ ↯.

18. Z twierdzenia (40) o dzieleniu z resztą wyprowadzamy
algorytm Euklidesa:

$$\begin{aligned}
&\forall\ \alpha,\beta \in \mathrm{Ord}^* := \mathrm{Ord}\setminus\{0\}\ \exists\, n \in \mathbb{N}^*; q, r : n+1 \to \mathrm{Ord}\\
&r_0 = \alpha, \quad r_1 = \beta\\
&\begin{cases}
r_0 = r_1 q_1 + r_2, & 0 < r_2 < r_1\\
r_1 = r_2 q_2 + r_3, & 0 < r_3 < r_2\\
\cdots\cdots & \cdots\\
r_{n-2} = r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1}\\
r_{n-1} = r_n q_n.
\end{cases}
\end{aligned}$$

$\langle$Gdyż nie istnieje silnie malejący i nieskończony ciąg liczb porządkowych. Formalna prezentacja musi oczywiście korzystać z twierdzenia o definiowaniu indukcyjnym ciągów $q, r : \mathbb{N} \to \mathrm{Ord}\rangle$.
W powyższej sytuacji $r_n \mid r_{n-1}$, $r_n \mid r_{n-2}$ $\langle r_{n-2} = r_n q_n q_{n-1} + r_n = r_n(q_n q_{n-1} + 1)\rangle$ itd., aż wreszcie $r_n \mid \alpha$, $r_n \mid \beta$.
Jeżeli teraz dla pewnego $d \in \mathrm{Ord}$ mamy podzielności: $d \mid \alpha$, $d \mid \beta$, to $d \mid r_2$ $\langle \alpha = dq'$, $\beta = dq''$, $dq' = dq'' q_1 + r_2$, $r_2 = dq' - dq'' q_1 = d(q' - q'' q_1)\rangle$ itd., aż otrzymujemy, że $d \mid r_n$, $d \leqslant r_n$.

Tak więc liczba r_n jest *największym wspólnym dzielnikiem* α i β; tę jednoznacznie wyznaczoną liczbę oznaczamy $(\alpha, \beta) := r_n$. Jeśli $(\alpha, \beta) = 1$, to mówimy, że liczby α, β są *względnie pierwsze*, co notujemy $\alpha \perp \beta$ ([**Graham... 02**, s. 139]).

$? = 37$
$\langle 42\,439 = 22\,533 \cdot 1 + 19\,906$
$22\,533 = 19\,906 \cdot 1 + 2\,627$
$19\,906 = 2\,627 \cdot 7 + 1\,517$
$\ldots$
$111 = 74 \cdot 1 + 37$
$74 = 37 \cdot 2\rangle$.

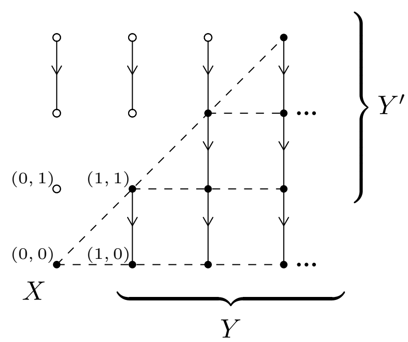
19. Nie. $\langle$Dla $Y = 2$ określamy $f : \mathrm{Ord} \to 2$, kładąc dla $\lambda \in \mathrm{Lim}_0$ i $n \in \mathbb{N}$:

$$f(\lambda + 2n) = 0, \quad f(\lambda + 2n + 1) = 1.$$

Wówczas $S_1(\mathrm{Ord}, R) = \{\alpha \in \mathrm{Ord} \mid \alpha \underset{R}{<} 1\} = \{\alpha \in \mathrm{Ord} \mid f(\alpha) < 1 \vee [f(\alpha) = 1 \wedge \alpha < 1]\} = \{\alpha \in \mathrm{Ord} \mid f(\alpha) = 0\} = \{\lambda + 2n \mid \lambda \in \mathrm{Lim}_0, n \in \mathbb{N}\} \notin \mathbb{V}\rangle$.

20*. Określamy:

$$X = \{(a, b) \in \mathbb{N}^2 \mid a \geqslant b\}, \quad Y = X \setminus \{(0, 0)\}.$$



Posety X i Y nie są izomorficzne, gdyż $(0, 0)$ jest jednocześnie elementem minimalnym i maksymalnym w X, zaś w Y elementu o tej własności nie ma.

Jednakże

$$X \simeq Y' := \{(a, b) \in Y \mid b \geqslant 1\} \in \mathcal{S}^+(Y)$$
$$Y \simeq X' := Y \in \mathcal{S}^-(X).$$

21.

(i) Wynika to z nieprzemienności potęgowania (np. $1 \wedge 2 \neq 2 \wedge 1$) – bez przestawienia czynników w kroku indukcyjnym mielibyśmy dla $n \geqslant 2$ i $a, b \in \mathbb{N}$: $a \overset{n}{\wedge} b = 1$ $\langle a \overset{2}{\wedge} 0 = 1$, i jeżeli $a \overset{2}{\wedge} b = 1$, to $a \overset{2}{\wedge} (b+1) = (a \overset{2}{\wedge} b) \overset{1}{\wedge} a = 1^a = 1$. Dalej indukcja na $n \geqslant 2$; jeżeli $a \overset{n}{\wedge} b = 1$, to $a \overset{n+1}{\wedge} 0 = 1$, i jeśli $a \overset{n+1}{\wedge} b = 1$, to $a \overset{n+1}{\wedge} (b+1) = (a \overset{n+1}{\wedge} b) \overset{n}{\wedge} a = 1 \overset{n}{\wedge} b = 1\rangle$.

(ii)

1) $a \overset{2}{\wedge} 1 = a \overset{1}{\wedge} (a \overset{2}{\wedge} 0) = a \overset{1}{\wedge} 1 = a^1 = a$, i jeżeli $a \overset{2}{\wedge} b = \left. a^{a^{\cdot^{\cdot^{a}}}} \right\} b$, to $a \overset{2}{\wedge} (b+1) = a \overset{1}{\wedge} (a \overset{2}{\wedge} b) = a^{a \overset{2}{\wedge} b} = \left. a^{a^{\cdot^{\cdot^{a}}}} \right\} b+1$.

2) $a \overset{0}{\wedge} 1 = a$, i jeżeli $a \overset{n}{\wedge} 1 = a$, to $a \overset{n+1}{\wedge} 1 = a \overset{n}{\wedge} (a \overset{n+1}{\wedge} 0) = a \overset{n}{\wedge} 1 = a$.

3) $a \overset{n}{\wedge} 2 = a \overset{n-1}{\wedge} (a \overset{n}{\wedge} 1) = a \overset{n-1}{\wedge} a \quad \langle$wg 2)$\rangle$, i jeżeli dla $b \geqslant 2$:
$a \overset{n}{\wedge} b = \underbrace{a \overset{n-1}{\wedge} (a \overset{n-1}{\wedge} \ldots (a \overset{n-1}{\wedge} a) \ldots)}_{b \text{ wystąpień } a}$, to $a \overset{n}{\wedge} (b+1) = a \overset{n-1}{\wedge} (a \overset{n}{\wedge} b) = \ldots$

4) $2 \overset{0}{\wedge} 2 = 2 \overset{1}{\wedge} 2 = 4$ i wg 2), 3) dla $n \geqslant 2$, jeżeli $2 \overset{n-1}{\wedge} 2 = 4$, to $2 \overset{n}{\wedge} 2 = 2 \overset{n-1}{\wedge} (2 \overset{n}{\wedge} 1) = 2 \overset{n-1}{\wedge} 2 = 4$.

5) $1 \overset{n}{\wedge} 0 = 1$, i jeżeli $1 \overset{n}{\wedge} b = 1$, to wg 2) $1 \overset{n}{\wedge} (b+1) = 1 \overset{n-1}{\wedge} (1 \overset{n}{\wedge} b) = 1 \overset{n-1}{\wedge} 1 = 1$.

6) Dla $n = 2$: $0 \overset{2}{\wedge} 0 = 1$ i dla $b \geqslant 1$, jeśli dla $b-1$ jest OK, to
$2 \mid b \ \Rightarrow\ 0 \overset{2}{\wedge} b = 0 \overset{1}{\wedge} (0 \overset{2}{\wedge} (b-1)) = 0 \overset{1}{\wedge} 0 = 0^0 = 1$,
$2 \nmid b \ \Rightarrow\ 0 \overset{2}{\wedge} b = 0 \overset{1}{\wedge} 1 = 0^1 = 0$.

Jeżeli teraz dla $n \geqslant 2$ jest OK, to $0 \overset{n+1}{\wedge} 0 = 1$, i dla $b \geqslant 1$, jeśli dla $b-1$ jest OK, to
$2 \mid b \ \Rightarrow\ 0 \overset{n+1}{\wedge} b = 0 \overset{n}{\wedge} (0 \overset{n+1}{\wedge} (b-1)) = 0 \overset{n}{\wedge} 0 = 1$,
$2 \nmid b \ \Rightarrow\ 0 \overset{n+1}{\wedge} b = 0 \overset{n}{\wedge} 1 = 0$.

(iii) $A_0 = 0,\ A_1 = 1,\ A_2 = 4$,
$A_3 = 3 \overset{3}{\wedge} 3 = 3 \overset{2}{\wedge} (3 \overset{2}{\wedge} 3) = 3 \overset{2}{\wedge} 3^{3^3} = 3 \overset{2}{\wedge} 3^{27} = \left. 3^{3^{\cdot^{\cdot^{3}}}} \right\} 3^{27} = \left. 3^{3^{\cdot^{\cdot^{3}}}} \right\} 7\,625\,597\,484\,987$.
$A_4 = 4 \overset{4}{\wedge} 4 = 4 \overset{3}{\wedge} (4 \overset{3}{\wedge} (4 \overset{3}{\wedge} 4)) = 4 \overset{3}{\wedge} (4 \overset{3}{\wedge} [4 \overset{2}{\wedge} (4 \overset{2}{\wedge} 4^{4^{4^4}})]) = \ldots$

22. Dowody są indukcyjne.

I Dla $n = 0$ podzielności zachodzą.

II Przejście od n do $n+1$:

(a) Jeżeli $5^{2^n} + 7 = 4k$, to $5^{2^{n+1}} + 7 = \left(5^{2^n}\right)^2 + 7 = (4k-7)^2 + 7 = 8(2k^2 - 7k + 7)$; zatem, jeżeli $5^{2^{n+1}} + 7 = 8k$, to $5^{2^{n+2}} + 7 = 8(8k^2 - 14k + 2)$.
(b) Jeżeli $5^{n+1} + 2 \cdot 3^n + 1 = 8k$, to $5^{n+2} + 2 \cdot 3^{n+1} + 1 = 5(8k - 2 \cdot 3^n - 1) + 6 \cdot 3^n + 1 = \ldots = 40k - 4(3^n + 1)$, i ponieważ $2 \mid 3^n + 1 \quad \langle \ldots \rangle$, więc …
(c) Jeżeli $4^{2n+1} + 3^{n+2} = 13k$, to $4^{2(n+1)+1} + 3^{n+3} = 4^{2n+1} \cdot 16 + 3^{n+3} = (13k - 3^{n+2})16 + 3^{n+3} = \ldots = 13(16k - 3^{n+2})$.
(d), (e) – Analogicznie.

23*. Tu prymitywna indukcja nie prowadzi do celu; trzeba delikatniej:

1) $n \geqslant 1 \ \Rightarrow\ \exists\, k \in \mathbb{N} : a_n = 4^k \quad \langle \ldots \rangle$.
2) Jeśli $n \geqslant 2$, to $a_n = 2^{a_{n-1}}$, i według 1) $\exists)\, k \in \mathbb{N} : a_{n-1} = 4^k$.
Ponieważ $3 \mid 4^k - 1 \quad \langle \ldots \rangle$, więc $\exists)\ l \in \mathbb{N} : 4^k - 1 = 3l,\ a_{n-1} = 3l + 1,\ a_n - 2 = 2^{3l+1} - 2 = 2(8^l - 1)$.
Ponieważ $7 \mid 8^l - 1 \quad \langle \ldots \rangle$, więc $7 \mid a_n - 2$.

24*. Określmy funkcję $f : \mathbb{N}^2 \to \mathbb{N}$ indukcyjnie:

$$f(n,0) = 1, \quad f(n,k+1) = n^{f(n,k)}.$$

(Wówczas $\overbrace{n^{n^{\cdot^{\cdot^{\cdot^{n}}}}}}^{k} = f(n,k)$).

Należy wykazać, że:

$$n \geqslant 3 \;\Rightarrow\; f(n,n+1) > f(n+1,n).$$

Wystarczy wykazać, że $n \geqslant 3$, $k \geqslant 1 \;\Rightarrow\; f(n,k+1) > nf(n+1,k)$.

Dowód indukcyjny (ustalamy $n \geqslant 3$).

I $\quad k = 1$.
Wówczas $f(n,k+1) = n^n$, $nf(n+1,k) = n(n+1)$.
Nierówność

$$(*) \qquad n^n > n(n+1)$$

zachodzi, gdyż $n^{n-1} \geqslant n^2 > 2n > n+1$.

II $\;$ Zakładamy, że dla $k \geqslant 1$:

$$f(n,k+1) > nf(n+1,k).$$

Należy wykazać, że

$$f(n,k+2) > nf(n+1,k+1).$$

Na mocy założenia indukcyjnego

$$f(n,k+2) = n^{f(n,k+1)} > n^{nf(n+1,k)} = (n^n)^{f(n+1,k)},$$

a więc według nierówności (*):

$$f(n,k+2) > n^{f(n+1,k)}(n+1)^{f(n+1,k)} \geqslant nf(n+1,k+1).$$

25. Oznaczmy $f = \mathrm{nat}_{A,R}$, $g = \mathrm{nat}_{B,S}$.

W obydwu przypadkach łatwo sprawdzić, że T jest dobrym porządkiem $\langle$spójność i istnienie elementów minimalnych$\rangle$. Należy jeszcze wskazać odpowiednie bijekcje rosnące.

1°) Określamy $h : \alpha + \beta \to A \cup B$; dla $\xi < \alpha + \beta$:

$$h(\xi) = \begin{cases} f(\xi), & \text{gdy } \xi < \alpha \\ g(\xi - \alpha), & \text{gdy } \alpha \leqslant \xi < \alpha + \beta. \end{cases}$$

Określenie jest poprawne, gdyż $\alpha \leqslant \xi < \alpha + \beta \;\Rightarrow\; \xi - \alpha < (\alpha + \beta) - \alpha = \beta$ (por. (40)).

$$h : \alpha + \beta \hookrightarrow\!\!\!\!\twoheadrightarrow A \cup B, \quad h - \mathbb{E}\text{-}T - \text{silnie rosnące.}$$

$\langle$ 1) Surjektywność: Niech $x \in A \cup B$.

Dwa przypadki:

1.1) $x \in A$. Wówczas $\xi := f^{-1}(x) < \alpha$, $x = f(\xi) = h(\xi)$

1.2) $x \in B$. Wówczas dla $\eta := g^{-1}(x) < \beta$: $\alpha \leqslant \alpha + \eta < \alpha + \beta$, i wówczas dla $\xi = \alpha + \eta$

$$\xi - \alpha = (\alpha + \eta) - \alpha = \eta < \beta, \quad x = g(\eta) = g(\xi - \alpha) = h(\xi).$$

2) h – silnie rosnąca, a więc injektywna; dla $\xi < \eta < \alpha + \beta$ rozpatrujemy przypadki:
2.1) $\xi < \eta < \alpha$.
Wówczas $h(\xi) = f(\xi) \underset{R}{<} f(\eta) = h(\eta)$, czyli $h(\xi) \underset{T}{<} h(\eta)$.
2.2) $\xi < \alpha \leqslant \eta < \alpha + \beta$.
Wówczas $h(\xi) \in A$, $h(\eta) \in B$, a więc $h(\xi) \underset{T}{<} h(\eta)$.
2.3) $\alpha \leqslant \xi < \eta < \alpha + \beta$.
Wówczas $\xi - \alpha < \eta - \alpha$, $h(\xi) = g(\xi - \alpha) \underset{S}{<} g(\eta - \alpha) = h(\eta)$, a więc $h(\xi) \underset{T}{<} h(\eta)\rangle$.

2°) Określamy bijekcję rosnącą $h : \alpha\beta \hookrightarrow\!\!\!\rightarrow A \times B$.
Jeśli $\alpha = 0$, to $h = \varnothing$; można więc przyjąć, że $\alpha \neq 0$.
Dla $\xi < \alpha\beta$: $\xi = \alpha q + r$, gdzie $q = \left[\frac{\xi}{\alpha}\right]$, $r = \xi \pmod{\alpha} < \alpha$ oraz $q < \beta$ $\quad\langle$HP: $\beta \leqslant q$.
Wówczas $\alpha\beta \leqslant \alpha q \leqslant \alpha q + r = \xi$ ↯$\rangle$; kładziemy: $h(\xi) = (f(r), g(q))$. Łatwo sprawdzić (jak w 1°)), że h jest bijekcją rosnącą $\alpha\beta$ na $A \times B$.

26*. Do porządnego zredagowania dowodu potrzebny jest pewien fakt z teorii zbiorów skończonych, to jest takich zbiorów X, że $\exists\, n < \omega : X \sim n$, a mianowicie, jeżeli X jest takim zbiorem niepustym i R jest porządkiem w X, to istnieje w X element R-maksymalny. $\quad\langle$Indukcja na $n\rangle$.
(Φ to ogół funkcji $\varphi : \alpha \to \beta$ o suporcie skończonym).
Relacja T jest dobrym porządkiem w Φ.
$\langle$ 1°) Spójność:
Jeżeli $\varphi, \psi \in \Phi$ i $\varphi \neq \psi$, to zbiór $\{\gamma < \alpha \mid \varphi(\gamma) \neq \psi(\gamma)\}$ jest skończony i niepusty; jeżeli γ jest jego największym elementem i na przykład $\varphi(\gamma) < \psi(\gamma)$, to $\varphi \underset{T}{<} \psi$.
2°) Elementy minimalne:
Jeżeli $\varnothing \neq \Psi \subset \Phi$, to ustalamy $\psi \in \Psi$, $\operatorname{supp}\psi \sim n < \omega$ dla pewnego $0 < n < \omega$. Indukcją na n pokazujemy, że w zbiorze $\{\varphi \in \Psi \mid \varphi \underset{T}{\leqslant} \psi\}$ istnieje element najmniejszy; jest on elementem minimalnym w $\Psi\rangle$.
Bijekcję rosnącą $h : \beta^\alpha \hookrightarrow\!\!\!\rightarrow \Phi$ określamy indukcją na α ($h = h_\alpha$), rozpatrując kolejno przypadki: zerowy, sekwensowy i graniczny.

27. Prosta indukcja na β. Udowodnimy np. (ii):
(I) $\beta = 0$. $L = 1 = P$
(II) $\beta = \gamma + 1$ i $\alpha^\gamma = \prod_{\eta<\gamma} \alpha$
$$L = \alpha^{\gamma+1} = \alpha^\gamma\alpha, \quad P = \prod_{\eta<\gamma+1} \alpha = \prod_{\gamma<\alpha} \alpha \cdot \alpha = \alpha^\gamma \cdot \alpha = L.$$
(III) $\beta \in \mathrm{Lim}$ i $\forall\, \gamma < \beta : \alpha^\gamma = \prod_{\eta<\gamma} \alpha$
$$L = \bigcup_{\gamma<\beta} \alpha^\gamma, \quad P = \bigcup_{\gamma<\beta} \prod_{\eta<\gamma} \alpha = \bigcup_{\gamma<\eta} \alpha^\gamma = L.$$

28.

(i) HP: warunek $\forall\, \beta < \alpha\ \exists\, \mu < \lambda\ \forall\, \mu < \xi < \lambda : \beta < a_\xi < \alpha$ oprócz liczby α spełnia jeszcze liczba $0 < \alpha' < \alpha$. Wówczas: $\exists)\, \mu < \lambda\ \forall\, \mu < \xi < \lambda : \alpha' < a_\xi < \alpha$, $\exists)\, \mu' < \lambda\ \forall\, \mu' < \xi < \lambda : 0 < a_\xi < \alpha'$ i dla $\xi = (\mu \cup \mu') + 1$ uzyskujemy sprzeczność.

(ii) Oznaczmy $\alpha = \bigcup_{\xi<\alpha} a_\xi$. HP: $\exists)\, \beta < \alpha\ \forall\, \mu < \lambda\ \exists\, \mu < \xi < \lambda : \neg\ \beta < a_\xi < \alpha$. $\exists)\, \mu < \lambda : \beta < a_\mu$. $\exists)\, \mu < \xi < \lambda : \neg\ \beta < a_\xi < \alpha$. Ale $\beta < a_\mu < a_\xi < a_{\xi+1} \leqslant \alpha$ ↯.
Zatem $\alpha = \lim a$. $\alpha \in \mathrm{Lim}$, gdyż $\alpha \neq 0$ $\quad\langle a_0 < a_1 \leqslant \alpha\rangle$, i gdyby $\alpha = \beta + 1$, to $\exists)\, \mu < \lambda\, \forall \mu < \xi < \lambda : \beta < a_\xi < \alpha$, w szczególności $\beta < a_{\mu+1} < a_{\mu+2} \leqslant \alpha$ ↯.

(iii) Wykorzystujemy (ii) i sprawdzamy, że granica ciągu f jest najmniejszą majorantą ciągu $f \circ a : \lambda \nearrow \mathrm{Ord}$, a więc jego granicą.

29. Zakładamy, że $\alpha < f(\alpha)$ i określamy indukcyjnie ciąg $a : \omega \to \mathrm{Ord}$; $a_0 = \alpha$, $a_{n+1} = f(a_n)$. Wówczas $a : \omega \nearrow \mathrm{Ord}$, a więc $\beta := \lim_{n<\omega} a_n = \bigcup_{n<\omega} a_n > \alpha$ oraz $f(\beta) = f\big(\lim_{n<\omega} a_n\big) = \lim_{n<\omega} f(a_n) = \lim_{n<\omega} a_{n+1} = \beta$.

Gdyby dla jakiegoś $\alpha < \gamma < \beta$ było $f(\gamma) = \gamma$, to $\exists)\, n < \omega : a_n < \gamma < a_{n+1}$, a więc $a_{n+1} = f(a_n) < f(\gamma) = \gamma$ ↯.

Twierdzenie nie zachodzi dla $A = \lambda \in \mathrm{Lim}$; na przykład ciąg normalny $f : \omega \to \omega$, $f(n) = n + 1$ nie ma punktu stałego.

30. Normalność tych trzech ciągów wynika natychmiast z ich definicji i odpowiednich praw arytmetyki porządkowej.

Najmniejszymi punktami stałymi są odpowiednio: ω^2 $\quad\langle \omega+\omega^2 = \omega(1+\omega) = \omega^2\rangle$, ω^ω $\quad\langle \omega\cdot\omega^\omega = \omega^{1+\omega} = \omega^\omega\rangle$, $\varepsilon_0 = \lim_{n<\omega} a_n$, gdzie $a_0 = 0$, $a_{n+1} = \omega^{a_n}$; tę ostatnią liczbę oznacza się zwyczajowo $\omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}$.

31. $g : \mathrm{Ord} \nearrow \mathrm{Ord}$. Pozostaje udowodnić ciągłość.
HP: $\exists)\, \lambda \in \mathrm{Lim} : g(\lambda) \neq \sigma := \bigcup_{\xi<\lambda} g(\xi)$.

Ponieważ $\forall\, \xi < \lambda : g(\xi) < g(\lambda)$, więc $\sigma < g(\lambda)$.
$\sigma \in C$ $\quad\langle$HP: $\sigma \notin C$, a więc $\sigma < f(\sigma) = \bigcup_{\eta<\sigma} f(\eta)$, skąd $\exists)\, \eta < \sigma : \sigma < f(\eta)$, i dalej $\exists)\, \xi < \lambda : \eta < g(\xi)$; $f(\eta) < f(g(\xi)) = g(\xi) < \sigma$ ↯$\rangle$.
$\exists)\, \tau \in \mathrm{Ord} : \sigma = g(\tau) < g(\lambda)$, $\tau < \lambda$.
Jednak $\forall\, \xi < \lambda : g(\xi) < \sigma = g(\tau)$, w szczególności $g(\tau) < g(\tau)$ ↯.

32. Jednoznaczność: jeżeli γ jest taką liczbą, to $\gamma = f(1)$.
Istnienie: Niech $\gamma = f(1)$, $1 = f(0) < f(1) = \gamma$.
Teraz prostą indukcją na $\alpha \in \mathrm{Ord}$ pokazujemy, że $f(\alpha) = \gamma^\alpha$.

33.

(i) Oznaczmy $S = 1 + 2 + \ldots + 2^n$, wówczas
$$\begin{aligned} 2S &= 2 + 2^2 + \ldots + 2^{n+1}, \\ 1 + 2S &= S + 2^{n+1}, \text{ a więc} \\ S &= 2^{n+1} - 1. \end{aligned}$$

(ii) $1 + \omega = \omega$
$1 + \omega + \omega^2 = \omega + \omega^2 = \omega(1 + \omega) = \omega^2$
$\dots$
i ogólnie:
$1 + \omega + \ldots + \omega^n = \omega^n$

W obydwu przypadkach (i) i (ii) można oczywiście zastosować notację „Σ" i zredagować dowód indukcyjny.

(iii) Oznaczmy $S_n = \sum_{k=0}^{n} (k+1)2^k$.

$$
\begin{aligned}
S_3 &= 2^0 + 2 \cdot 2^1 + 3 \cdot 2^2 + 4 \cdot 2^3 \\
&= \begin{array}{ccccccc} 2^0 + & 2^1 & + & 2^2 & + & 2^3 & + \\ & 2^1 & + & 2^2 & + & 2^3 & + \\ & & & 2^2 & + & 2^3 & + \\ & & & & & 2^3 & \end{array} \\
&= 2^4 - 1 + 2(2^3 - 1) + 2^2(2^2 - 1) + 2^3(2 - 1) \\
&= 2^4 - 1 + 2^4 - 2 + 2^4 - 2^2 + 2^4 - 2^3 \\
&= 4 \cdot 2^4 - (1 + 2 + 2^2 + 2^3) = 4 \cdot 2^4 - (2^4 - 1) = 3 \cdot 2^4 + 1
\end{aligned}
$$

i ogólnie $S_n = n2^{n+1} + 1$.

Dowód indukcyjny:

I $n = 0$. $S_0 = 1$, OK

II OK dla n; dla $n + 1$?

$$
\begin{aligned}
S_{n+1} &= S_n + (k+1) \cdot 2^k|_{k=n+1} = S_n + (n+2) \cdot 2^{n+1} \\
&= n \cdot 2^{n+1} + 1 + (n+2)2^{n+1} = n \cdot 2^{n+1} + 1 + n \cdot 2^{n+1} + 2^{n+2} \\
&= n \cdot 2^{n+2} + 1 + 2^{n+2} = (n+1) \cdot 2^{n+2} + 1.
\end{aligned}
$$

(iv) $\displaystyle\sum_{k=1}^{n} (k+1)^2 = \sum_{k=1}^{n} k^2 + 2\sum_{k=1}^{n} k + \sum_{k=1}^{n} 1$, czyli

$$\sum_{i=1}^{n} i^2 - 1 + (n+1)^2 = \sum_{k=1}^{n} k^2 + 2S_n + n,$$

$$n^2 + 2n = 2S_n + n, \quad 2S_n = n^2 + n = n(n+1), \quad S_n = \frac{n(n+1)}{2}.$$

(v) $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

(vi) $\displaystyle\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

34.

I $k = 1$. Wówczas $\gamma_k^{\xi_k} > 0$.

II Załóżmy, że $k \geqslant 2$ i teza zachodzi dla $k-1$.

Ponieważ $\eta_{k-1} < \gamma$, więc $\gamma = \eta_{k-1} + \rho$, gdzie $\rho = \gamma - \eta_{k-1} \geqslant 1$.
Zatem $\gamma^{\xi_k} \geqslant \gamma^{\xi_{k-1}+1} = \gamma^{\xi_{k-1}} \cdot \gamma = \gamma^{\xi_{k-1}}(\eta_{k-1} + \rho) = \gamma^{\xi_{k-1}}\eta_{k-1} + \gamma^{\xi_{k-1}} \cdot \rho \geqslant \gamma^{\xi_{k-1}}\eta_{k-1} + \gamma^{\xi_{k-1}}$
i stosując do $\gamma^{\xi_{k-1}}$ założenie indukcyjne:
$\gamma^{\xi_{k-1}} > \gamma^{\xi_{k-2}} \cdot \eta_{k-2} + \ldots + \gamma^{\xi_1}\eta_1$ otrzymujemy nierówność $\gamma^{\xi_k} > \gamma^{\xi_{k-1}} \cdot \eta_{k-1} + \gamma^{\xi_{k-2}} \cdot \eta_{k-2} + \ldots + \gamma^{\xi_1}\eta_1$.

35. Jeśli $\alpha \neq 0$, to $\tau(\alpha) \neq 0$ $\quad\langle \gamma^0 = 1 \rangle$.
Gdyby $\tau(\alpha) = \tau \in \mathrm{Lim}$, to $\alpha < \gamma^\tau = \bigcup\limits_{\xi<\tau} \gamma^\xi$, a więc $\exists\, \xi < \tau : \alpha < \gamma^\xi$ ↯.

Na mocy nierówności z zadania 34:
$\alpha < \gamma^{\xi_k} \cdot \eta_k + \gamma^{\xi_k} = \gamma^{\xi_k}(\eta_k + 1) \leqslant \gamma^{\xi_k} \cdot \gamma = \gamma^{\xi_k+1}$, a więc $\tau(\alpha) \leqslant \xi_k + 1$.
Gdyby $\tau(\alpha) < \xi_k+1$, to $\tau(\alpha) \leqslant \xi_k$, a więc $\alpha < \gamma^{\tau(\alpha)} \leqslant \gamma^{\xi_k} \leqslant \gamma^{\xi_k} \cdot \eta_k + \ldots \gamma^{\xi_1} \cdot \eta_1 = \alpha$ ↯.

36.

a) $\alpha = (2^\omega)^\omega \cdot (2+1) + (2^\omega)^2 \cdot 2 + 2^\omega = 2^{\omega^2+1} + 2^{\omega^2} + 2^{\omega\cdot 2+1} + 2^\omega$

b) $\beta = (2^\omega)^2 \cdot 2 + 2^\omega \cdot 4 + 2^\omega + 7 = \omega^2 \cdot 2 + \omega \cdot 4 + \omega + 7 = \omega^2 \cdot 2 + \omega^1 \cdot 5 + \omega^0 \cdot 7$.

37. Przypuśćmy, że twierdzenie nie zachodzi dla liczby $\tau = \tau(\alpha)$, natomiast zachodzi dla wszystkich $\tau' < \tau$.
Wówczas $0 < \alpha < \gamma^\tau$ $\quad\langle$gdyż dla $\alpha = 0$ mamy jednoznaczne rozwinięcie z $k = 0\rangle$, $\tau \neq 0$, $\tau \notin \mathrm{Lim}$ $\quad\langle$HP: $\tau \in \mathrm{Lim}$. Wówczas $\alpha < \bigcup\limits_{\xi<\tau} \gamma^\xi$, a więc $\exists\, \xi < \tau : \alpha < \gamma^\xi$ ↯. (por. zadanie 27)$\rangle$.
Zatem $\tau = \xi+1$ i dzieląc α przez γ^ξ otrzymujemy: $\exists)\, \eta, \rho \in \mathrm{Ord} : \alpha = \gamma^\xi \cdot \eta + \rho \ \wedge\ \rho < \gamma^\xi$; przy czym $\xi < \tau$ i $0 < \eta < \gamma$. $\quad\langle$Gdyby $\eta = 0$, to $\alpha = \rho < \gamma^\xi$ ↯. Gdyby $\eta \geqslant \gamma$, to $\alpha \geqslant \gamma^\xi \cdot \eta \geqslant \gamma^\xi \cdot \gamma = \gamma^{\xi+1} = \gamma^\tau$ ↯$\rangle$.
Teraz na mocy założenia indukcyjnego istnieje rozwinięcie

$$\rho = \gamma^{\xi_k}\eta_k + \ldots + \gamma^{\xi_1}\eta_1, \qquad \xi_1 < \cdots < \xi_k, \qquad \eta_i \neq 0.$$

Zauważmy przy tym, że $\xi_k < \xi$ $\quad\langle$HP: $\xi_k \geqslant \xi$, wówczas $\rho \geqslant \gamma^{\xi_k}\eta_k \geqslant \gamma^{\xi_k} \geqslant \gamma^\xi$ ↯$\rangle$, a więc otrzymaliśmy rozwinięcie $\alpha = \gamma^\xi\eta + \gamma^{\xi_k}\eta_k + \ldots + \gamma^{\xi_1}\eta_1$.

W takim razie nie zachodzi jednoznaczność rozwinięcia; liczba α ma dwa różne rozwinięcia: $(\xi, \eta) \neq (\xi', \eta')$,

$$\alpha = \gamma^{\xi_k}\eta_k + \ldots + \gamma^{\xi_1}\eta_1 = \gamma^{\xi'_{k'}}\eta'_{k'} + \ldots + \gamma^{\xi'_1}\eta'_1.$$

Ponieważ $\tau(\alpha) = \xi_k + 1 = \xi'_{k'} + 1$ (zob. zadanie 27), więc $\xi_k = \xi'_{k'}$. Również $\eta_k = \eta'_{k'}$ $\langle$HP: $\eta_k \neq \eta'_{k'}$, na przykład $\eta_k < \eta'_{k'}$; wówczas $\eta_k + 1 \leqslant \eta'_{k'}$, a więc, wykorzystując zadanie 23, $\alpha \geqslant \gamma^{\xi_k}(\eta_k+1) + \gamma^{\xi'_{k'-1}}\eta'_{k'-1} + \ldots + \gamma^{\xi'_1}\eta'_1 \geqslant \gamma^{\xi_k}(\eta_k+1) = \gamma^{\xi_k}\eta_k + \gamma^{\xi_k} > \gamma^{\xi_k}\eta_k + \gamma^{\xi_{k-1}}\eta_{k-1} + \ldots + \gamma^{\xi_1}\eta_1 = \alpha$ ↯$\rangle$. Zatem liczba

$$\alpha' := \gamma^{\xi_{k-1}}\eta_{k-1} + \ldots + \gamma^{\xi_1}\eta_1 = \gamma^{\xi'_{k'-1}}\eta'_{k'-1} + \ldots + \gamma^{\xi'_1}\eta'_1$$

ma dwa różne rozwinięcia, przy czym

$$\tau(\alpha') = \xi_{k-1} + 1 < \xi_k + 1 = \tau(\alpha)\ ↯.$$

38*.

a) 8, 80, 553, 6 310, 93 451, 1 647 195, 33 554 571.

b) Określamy funkcję $(x, n) \mapsto S(x, n)$ indukcją na $x \in \mathbb{N}$ przy ustalonym $n \in \mathbb{N}$; $n \geqslant 2$:

(I) $S(0, n) = 0$.

(II) Jeżeli $1 \leqslant x = n^{\xi_k} \cdot \eta_k + \ldots + n^{\xi_1} \cdot \eta_1$, gdzie $\xi_1 < \cdots < \xi_k < \omega$, $0 < \eta_i < n$ dla $i \in I_k$, to

$$S(x, n) = (n+1)^{S(\xi_k, n)} \cdot \eta_k + \ldots + (n+1)^{S(\xi_1, n)} \cdot \eta_1.$$

Definicja jest poprawna, gdyż dla $i \in I_k$: $\xi_i < x$. $\langle$Ponieważ $\forall\ \alpha \in \mathbb{N} : \alpha < 2^\alpha$ $\langle$indukcja na $\alpha\rangle$, więc $\xi_i < 2^{\xi_i} \leqslant n^{\xi_i} \leqslant x\rangle$.

Mając funkcję S możemy już dla ustalonego $m \in \mathbb{N}$ określić indukcyjnie ciąg Goodsteina $a = \overset{m}{a} : \mathbb{N} \to \mathbb{N}$:

I $a_0 = m$

II $n > 0 \Rightarrow a_n = S(a_{n-1}, n+1) - 1$.

c) Indukcja na x:

(I) $f_n(0) = 0 = f_{n+1}(S(0, n))$.

(II) Załóżmy, że $1 \leqslant x = n^{\xi_k}\eta_k + \ldots + n^{\xi_1}\eta_1 \in \mathbb{N}$ (oznaczenia jak w temacie), i równość zachodzi dla wszystkich $x' < x$.

Wówczas

$$f_{n+1}(S(x, n)) = \omega^{f_{n+1}(S(\xi_k, n))} \cdot \eta_k + \ldots + \omega^{f_{n+1}(S(\xi_1, n))} \cdot \eta_1.$$

Ale $\forall\ i \in I_k : \xi_i < x$, a więc na mocy założenia indukcyjnego $f_{n+1}(S(\xi_i, n)) = f_n(\xi_i)$, czyli $f_{n+1}(S(x, n)) = \omega^{f_n(\xi_k)} \cdot \eta_k + \ldots + \omega^{f_n(\xi_1)} \cdot \eta_1 = f_n(x)$.

d) Indukcją na $x \in \mathbb{N}$ pokażemy, że $f_n(x) < f_n(x+1)$.

(I) $x = 0$.

Wówczas $x + 1 = 1 = n^0 \cdot 1$, a więc

$$f_n(x+1) = \omega^{f_n(0)} \cdot 1 = \omega^0 \cdot 1 = 1 > 0 = f_n(x).$$

(II) Załóżmy, że $1 \leqslant x = n^r\alpha_r + \ldots + \alpha_0$, $\alpha_i < n$, $\alpha_r \neq 0$, i $\forall\ x' < x : f_n(x') < f_n(x'+1)$.

Rozważmy trzy przypadki:

1) $\alpha_0 < n - 1$.

Wówczas $x + 1 = n^r \cdot \alpha_r + \ldots + \alpha_0 + 1$, a więc

$$f_n(x+1) = \omega^{f_n(r)} \cdot \alpha_r + \ldots + \alpha_0 + 1 = f_n(x) + 1 > f_n(x).$$

2) $\exists)\, 0 < s \leqslant r : \alpha_s < n - 1 \ \wedge\ \forall\ i < s : \alpha_i = n - i$, czyli

$$x = n^r\alpha_r + \ldots + n^s\alpha_s + n^{s-1}(n-1) + \ldots + n - 1.$$

Wówczas $x + 1 = n^r\alpha_r + \ldots + n^s\alpha_s + n^s = n^r\alpha_r + \ldots + n^s(\alpha_s + 1)$, gdyż

(*) $$\forall\ k \in \mathbb{N} : \sum_{i<k} n^i(n-1) + 1 = n^k. \quad \langle\text{Indukcja na } k\rangle.$$

Zatem $f_n(x+1) = \omega^{f_n(r)}\alpha_r + \ldots + \omega^{f_n(s)}(\alpha_s+1) = \omega^{f_n(r)}\alpha_r + \ldots + \omega^{f_n(s)}\alpha_s + \omega^{f_n(s)}$. Ale $n^s > n^{s-1}\alpha_{s-1} + \ldots + \alpha_0$ $\langle$zadanie 34$\rangle$ oraz $n^s < x$ $\langle n_s \leqslant n^r\alpha_r \leqslant n^r\alpha_r + \ldots + n^s\alpha_s < n^r\alpha_r + \ldots + n^s\alpha_s + n^{s-1}(n-1) + \ldots + n - 1 = x\rangle$, a więc na mocy założenia indukcyjnego

$$f_n(n^s) = \omega^{f_n(s)} > f_n(n^{s-1}\alpha_{s-1} + \ldots + \alpha_0) = \omega^{f_n(s-1)} \cdot \alpha_{s-1} + \ldots + \alpha_0,$$

skąd $f_n(x+1) > \omega^{f_n(r)}\alpha_r + \ldots + \omega^{f_n(s)}\alpha_s + \omega^{f_n(s-1)}\alpha_{s-1} + \ldots + \alpha_0 = f_n(x)$.
3) $\forall\, s \leqslant r : \alpha_s = s - 1$, czyli $x = n^r(n-1) + \ldots + n - 1$.
Wówczas $x + 1 = n^{r+1}$ $\langle$(*)$\rangle$, a więc $f_n(x+1) = \omega^{f_n(r+1)}$, natomiast $f_n(x) = \omega^{f_n(r)} \cdot (n-1) + \ldots + (n-1)$.
Ponieważ $r < 2^r \leqslant n^r \leqslant x$, więc $f_n(r+1) > f_n(r)$, czyli $f_n(r+1) \geqslant f_n(r) + 1$, zatem, znów na mocy nierówności z zadania 34,

$$f_n(x+1) = \omega^{f_n(r+1)} \geqslant \omega^{f_n(r)+1} > \omega^{f_n(r)} \cdot (n-1) + \ldots + (n-1) = f_n(x).$$

e) HP: $\exists)\, m \in \mathbb{N}\, \forall\, n \in \mathbb{N} : a_n = \overset{m}{a}_n > 0$. Rozważmy ciąg $b_n = f_{n+2}(a_n)$.

$$b_{n+1} = f_{n+3}(a_{n+1}) = f_{n+3}(S(a_n, n+2) - 1).$$

Ponieważ $a_{n+1} > 0$, więc $S(a_n, n+2) > 1$, i według c) i b): $b_{n+1} < f_{n+3}(S(a_n, n+2)) = f_{n+2}(a_n) = b_n$.
Uzyskaliśmy więc silnie malejący ciąg $b : \mathbb{N} \to \mathrm{Ord}$ $\lightning$.

f) Policzmy kilka kolejnych, poczynając od szóstego, wyrazów ciągu $a = \overset{4}{a} : \mathbb{N} \to \mathbb{N}$:

$$\begin{array}{rl}
 & a_6 = 8^2 \cdot 2 + 8 \cdot 1 + 3 \\
 & a_7 = 9^2 \cdot 2 + 9 + 2 \\
 & a_8 = 10^2 \cdot 2 + 10 + 1 \\
 & a_9 = 11^2 \cdot 2 + 11 \\
\begin{array}{c}12\\ \text{wyrazów}\end{array} & \left\{\begin{array}{l} a_{10} = 12^2 \cdot 2 + 12 - 1 = 12^2 \cdot 2 + 11 \\ a_{11} = 13^2 \cdot 2 + 10 \\ \ldots\ldots \quad \ldots \\ a_{21} = 23^2 \cdot 2 \end{array}\right. \\
\begin{array}{c}24\\ \text{wyrazy}\end{array} & \left\{\begin{array}{l} a_{22} = 24^2 \cdot 2 - 1 = 24^2 + 24 \cdot 23 + 23 \\ a_{23} = 25^2 + 25 \cdot 23 + 22 \\ \ldots\ldots \quad \ldots \\ a_{45} = 47^2 \cdot 2 + 47 \cdot 23 \end{array}\right. \\
\begin{array}{c}48\\ \text{wyrazów}\end{array} & \left\{\begin{array}{l} a_{46} = 48^2 + 48 \cdot 23 - 1 = 48^2 + 48 \cdot 22 + 47 \\ a_{47} = 49^2 + 49 \cdot 22 + 46 \\ \ldots\ldots \quad \ldots \\ a_{93} = 95^2 + 95 \cdot 22 \end{array}\right. \\
 & \ldots\ldots
\end{array}$$

Wyraz o numerze k, takim, że $a_k = (k+2)^2$ otrzymamy po wyrazie a_{21} w dwudziestu czterech „dużych krokach", których długości rosną w postępie geometrycznym;

$$k = 21 + (24 + 24 \cdot 2 + 24 \cdot 2^2 + \ldots + 24 \cdot 2^{23}) = 21 + 24(2^{24} - 1) = 3 \cdot 2^{27} - 3.$$

Szukamy teraz $l > k$ takiego, że $a_l = l + 2$. Dla takiego l:

$$a_{l+1} = l + 3 - 1 = l + 2,\ a_{l+2} = l + 1,\ \ldots,\ a_{2l+2} = 1,\ a_{2l+3} = 0,$$

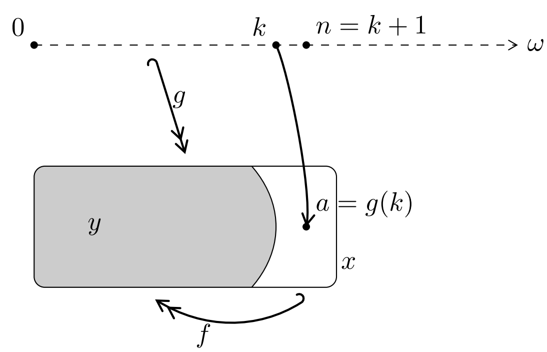
czyli $c_4 = 2l + 3$.
Teraz $a_{k+1} = (k+3)^2 - 1 = (k+3)(k+2) + k + 2$, $a_{k+2} = (k+4)(k+2) + (k+1)$, $\ldots$, $a_{2k+3} = (2k+5)(k+2)$ ($k+3$ kroki), i dalej $a_{2k+4} = (2k+6)(k+2) - 1 = (2k+6)(k+1) + 2k + 5$, $\ldots$, $a_{4k+9} = (4k+11)(k+1)$ ($(k+3) \cdot 2$ kroki). Po $k+2$ „dużych krokach" otrzymamy $a_l = l + 2$. Tak więc $l = k + (k+3) + (k+3) \cdot 2 + \ldots + (k+3) \cdot 2^{k+1} = k + (k+3)(2^{k+2} - 1) = (k+3) \cdot 2^{k+2} - 3$, i ostatecznie $c_4 = 2l + 3 = (k+3)2^{k+3} - 3 = 3 \cdot (2^{27+3 \cdot 2^{27}} - 1) = 3(2^{402\,653\,211} - 1)$.

39. HP: $\forall\ t \in y : |f^{-1}\{t\}| < \varphi(m,n)$. Wówczas $m = |x| = \Big|\bigcup\limits_{t \in y} f^{-1}\{t\}\Big| = \sum\limits_{t \in y} |f^{-1}\{t\}|$.

Dwa przypadki:

I $\quad n \mid m$.
Wówczas $\varphi(m,n) = \frac{m}{n}$, a więc $\forall\ t \in y\ \ |f^{-1}\{t\}| < \frac{m}{n}$, czyli $m < |y| \cdot \frac{m}{n} = n \cdot \frac{m}{n} = m$ ↯.
II $\quad n \nmid m$.
Wówczas $m = nq + r$, gdzie $q, r < \omega$, $0 < r < n$. W tym przypadku $\varphi(m,n) = q + 1$, a więc $\forall\ t \in y\ \ |f^{-1}\{t\}| < q + 1$, czyli $|f^{-1}\{t\}| \leqslant q$, skąd $m \leqslant nq < nq + r = m$ ↯.

40. HP: $x \in \mathrm{Fin}$ i $\exists)\, y \subsetneq x,\ y \sim x$. $\exists)\ f : x \hookrightarrow\!\!\!\!\rightarrow y$, $a \in x \setminus y$. Niech $n = |x|$; $x \neq \varnothing$, $n > 0$, $\exists)\, k < n : n = k + 1$. $\exists)\, g : n \hookrightarrow\!\!\!\!\rightarrow x$, $g(k) = a$.



Wówczas $h = g^{-1} \circ f \circ g : n \hookrightarrow k$, a więc $n \sim \mathrm{Im}\, h \subset k$, i wg (48) $n = |\mathrm{Im}\, h| \leqslant k < n$ ↯.

41.

(i) HP: $\exists)\, s : \omega \hookrightarrow x$. Wówczas $y = x \setminus \{s_0\} \subsetneq x$ i $\{s_k \mapsto s_{k+1} \mid k < \omega\} \cup \mathrm{id}_{x \setminus \mathrm{im}\, s} : x \hookrightarrow\!\!\!\!\rightarrow y$ ↯.
(ii) HP: $\exists)\, y \subsetneq z \subset x$, $f : z \hookrightarrow\!\!\!\!\rightarrow y$. Wówczas $y \cup (x \setminus z) \subsetneq x$ i $f \cup \mathrm{id}_{x \setminus z} : x \hookrightarrow\!\!\!\!\rightarrow y \cup (x \setminus z)$ ↯.

(iii) HP: $\exists)\, y \subsetneq x,\ f : x \lhook\joinrel\longrightarrow\!\!\!\!\rightarrow y$. Wówczas $g = \{\{t\} \mapsto \{f(t)\} \mid t \in x\} \cup \mathrm{id}_{\mathcal{P}x \setminus \{\{t\} \mid t \in x\}} : \mathcal{P}x \lhook\joinrel\longrightarrow \mathcal{P}x$ i $\neg g : \mathcal{P}x \longrightarrow\!\!\!\!\rightarrow \mathcal{P}x$ ↯.

42. HP: $\exists)\, x \in \mathrm{Fin},\ g : x \longrightarrow\!\!\!\!\rightarrow x,\ \neg\, g : x \lhook\joinrel\longrightarrow x$. Na mocy $\mathrm{AC_{fin}}$ (zob. (51)) istnieje funkcja wyboru $\tau : \mathcal{P}x \setminus \{\varnothing\} \to x$.

Injekcja $f = \{t \mapsto \tau(g^{-1}\{t\}) \mid t \in x\} : x \hookrightarrow x$ nie jest surjekcją $\langle \exists)\, a, b \in x,\ a \neq b,\ g(a) = g(b)$. Wówczas $\{a, b\} \subset g^{-1}(a),\ \tau(g^{-1}\{a\}) \neq a \ \Rightarrow\ a \notin \mathrm{Im}\, f$, $\tau(g^{-1}\{a\}) \neq b \ \Rightarrow\ b \notin \mathrm{Im}\, f\rangle$. Zatem $\neg \forall\ f : x \hookrightarrow x\ (f : x \twoheadrightarrow x)$, a więc $x \notin \mathrm{Fin}$ ↯.

43. $f : A_{k,n} \lhook\joinrel\longrightarrow\!\!\!\!\rightarrow \mathcal{P}_k I_{n+k}$, a więc $\alpha_{k,n} = \binom{n+k}{k}$

$\langle$ 1°) f jest injekcją, gdyż $\forall\ j \in I_{k-1} : \sum\limits_{i=1}^{j+1} x_i + j + 1 > \sum\limits_{i=1}^{j} x_i + j$

2°) f jest surjekcją, gdyż dla $E = \{y_1, \ldots, y_k\} \in \mathcal{P}_k I_{n+1},\ i < j \ \Rightarrow\ y_i < y_j$ określamy ciąg $x \in A_{k,n}$, kładąc $x_1 = y_1 - 1,\ \forall\ j \in I_{k-1} : x_{j+1} = y_{j+1} - y_j - 1$, i wówczas $E = f(x)\rangle$.

$\alpha_{k,n} = \beta_{k+1,n}$, gdyż dla $x : I_k \to \mathbb{N}$

$$x \in A_{k,n} \iff \big(x_1, \ldots, x_k, n - \sum_{i=1}^{k} x_i \bigcap\big) \in B_{k+1,n}.$$

Zatem dla $k \geqslant 2$: $\beta_{k,n} = \alpha_{k-1,n} = \binom{n+k-1}{k-1}$. Równość ta utrzymuje się dla $k = 1$ $\langle \beta_{1,n} = 1\rangle$. Tak więc $\beta_{k,n} = \binom{n+k-1}{k-1}$, $\alpha_{k,n} = \binom{n+k}{k}$.

44. Przyjmując oznaczenia z poprzedniego zadania otrzymamy $x \in A_{k,n} \Leftrightarrow \exists i \leqslant n : x \in B_{k,i}$, a więc $\alpha_{k,n} = \sum\limits_{i=0}^{n} \beta_{k,i}$, czyli $\binom{n+k}{k} = \sum\limits_{i=0}^{n} \binom{i+k-1}{k-1}$; kładąc $m = k - 1$ otrzymamy równość: $\sum\limits_{i=0}^{n} \binom{m+i}{m} = \binom{m+n+1}{m+1}$. Dowód tej równości indukcją na n jest bezproblemowy.

45. $B_n = \sum\limits_{k=0}^{n-1} \binom{n-1}{k} B_{n-k-1} = \sum\limits_{i=0}^{n-1} \binom{n-1}{i} B_i \quad \langle \binom{n-1}{n-1-k} = \binom{n-1}{k}\rangle$. Tak więc $B_1 = 1$, $B_2 = 2$, $B_3 = 5$, $B_4 = 15$, $B_5 = 52$.

46.

(a) $|\,\mathrm{Part}_2\, I_n| = |\{A \subset I_n \mid n \in A \subsetneq I_n\} = |\mathcal{P}I_{n-1} \setminus \{I_{n-1}\}|$.

(b) 1°) $\left\{ {n \atop k} \right\} = \sum\limits_{i=0}^{n-1} \binom{n-1}{i} \left\{ {n-i-1 \atop k-1} \right\}$.

2°) $|\{\mathcal{A} \in \mathrm{Part}_k\, I_n \mid \{n\} \in \mathcal{A}\}| = \left\{ {n-1 \atop k-1} \right\}$.

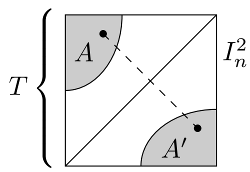
Oznaczmy $S = \{\mathcal{A} \in \mathrm{Part}_k\, I_n \mid \{n\} \notin \mathcal{A}\}$, i dla $\mathcal{A} \in S$: $F(\mathcal{A}) =$ jedyne takie $A \in \mathcal{A}$, że $n \in A$, $\mathcal{A}' = \mathcal{A} \setminus \{F(\mathcal{A})\} \cup \{F(\mathcal{A}) \setminus \{n\}\}$.

Wówczas $\{\mathcal{A} \mapsto (\mathcal{A}', F(\mathcal{A})) \mid \mathcal{A} \in S\} : S \lhook\joinrel\longrightarrow\!\!\!\!\rightarrow \bigcup\limits_{\mathcal{B} \in \mathrm{Part}_k\, I_{n-1}} \{\mathcal{B}\} \times \mathcal{B}$, a więc $|S| = \sum\limits_{\mathcal{B} \in \mathrm{Part}_k\, I_{n-1}} |\{\mathcal{B}\} \times \mathcal{B}| = k\left\{ {n-1 \atop k} \right\}$.

Zatem $\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k\left\{ {n-1 \atop k} \right\}$.

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 0 & & 1 & & & & \\
 & & & 0 & & 1 & & 1 & & & \\
 & & 0 & & 1 & & 3 & & 1 & & \\
 & 0 & & 1 & & 7 & & 6 & & 1 & \\
0 & & 1 & & 15 & & 25 & & 10 & & 1 \\
\cdots & & & & & & & & & & \cdots
\end{array}
$$

47.



$$T = \{(x,y) \in I_n^2 \mid x < y\}, \quad |T| = 2^{\frac{n^2-n}{2}}.$$

a) 2^{n^2-n}

b) $2^n \cdot 2^{\frac{n^2-n}{2}} = 2^{\frac{n^2+n}{2}}$

c) $2^{\frac{n^2-n}{2}}$

d) $2^n \cdot \sum\limits_{A \subset T} 2^{\frac{n^2-n}{2}-|A|} = 2^n \cdot \sum\limits_{k=0}^{\frac{n^2-n}{2}} \binom{\frac{n^2-n}{2}}{k} 2^{\frac{n^2-n}{2}-k} = 2^n \cdot (1+2)^{\frac{n^2-n}{2}} = 2^n \cdot 3^{\frac{n^2-n}{2}}$

e) $3^{\frac{n^2-n}{2}}$

f) $\sum\limits_{A \subset T} |\mathcal{P}A| = \sum\limits_{k=0}^{\frac{n^2-n}{2}} \binom{\frac{n^2-n}{2}}{k} 2^k = (2+1)^{\frac{n^2-n}{2}} = 3^{\frac{n^2-n}{2}}$

g) $|\mathcal{P}T| = 2^{\frac{n^2-n}{2}}$

h) $n!$

i) 13 $\langle$są trzy relacje nieprzechodnie: $\{(0,1),\ (1,0)\}$, $\{(0,1),\ (1,0),\ (0,0)\}$, $\{(0,1),\ (1,0),\ (1,1)\}\rangle$.

48.

I $n = 0$ OK

II $n \geqslant 1$, OK dla $n-1$

$$n! = (n-1)!n \leqslant 2^{\frac{(n-1)^2-(n-1)}{2}} \cdot n = 2^{\frac{n^2-3n+2}{2}} \cdot n = \leqslant 2^{\frac{n^2-n}{2}},$$

gdyż $\forall\ n \in \mathbb{N}^* : n \leqslant 2^{n-1}$. $\langle$Indukcja na $n\rangle$.

49. $\gamma_n = \beta_n - \alpha_n$, $\alpha_0 = \beta_0 = 0$.

Dla $n \geqslant 1$:

$$\alpha_n = \sum_{k=0}^{n} \sum_{\substack{X \subset I_n \\ |X|=k}} k = \sum_{k=0}^{n} k\binom{n}{k} = n\sum_{k=1}^{n} \frac{(n-1)!}{(k-1)!(n-k)!} = n\sum_{i=0}^{n-1}\binom{n-1}{i} = n2^{n-1}$$

$$\beta_n = \sum_{X \subset I_n} \sum_{Y \subset I_n} |X \cap Y| = \sum_{k=1}^{n} \sum_{\substack{X \subset I_n \\ |X|=k}} \sum_{Y \subset I_n} |X \cap Y|.$$

Dla ustalonych $k \in I_n$, $X \subset I_n$, $|X| = k$:
$\sum\limits_{Y \subset I_n} |X \cap Y| = \sum\limits_{i=1}^{k} \binom{k}{i} \cdot i \cdot 2^{n-k} = 2^{n-k} \sum\limits_{i=1}^{k} \frac{k!}{(i-1)!(k-i)!} = 2^{n-k} \cdot k \sum\limits_{i=1}^{k} \binom{k-1}{i-1} = 2^{n-k} \cdot k \sum\limits_{j=0}^{k-1} \binom{k-1}{j} = 2^{n-k} \cdot k \cdot 2^{k-1} = k \cdot 2^{n-1}$,
a więc
$\beta_n = \sum\limits_{k=1}^{n} \binom{n}{k} \cdot k2^{n-1} = 2^{n-1} \cdot n \sum\limits_{k=1}^{n} \binom{n-1}{k-1} = 2^{n-1} \cdot n \cdot 2^{n-1} = n \cdot 2^{2n-2}$.
$\gamma_n = n2^{2n-2} - n2^{n-1} = n2^{n-1}(2^{n-1} - 1)$.

50. Łatwo widać, że $f(n) \geqslant 2^{n-1} + 1$. $\langle$Dla $\mathcal{A} := \{X \cup \{n\} \mid X \subset I_{n-1}\} \subset \mathcal{P}I_n$: $|\mathcal{A}| = 2^{n-1}$, i $\forall_{\substack{A,B \in \mathcal{A} \\ A \neq B}} : n \in A \cap B\rangle$.
Niech $A \subset \mathcal{P}I_n$, $|\mathcal{A}| = 2^{n-1} + 1$.
Równoważność $A \equiv B \;:\Leftrightarrow\; A = B \;\vee\; A = B^{\neg}$ w $\mathcal{P}I_n$ ma warstwy dwuelementowe, i jest tych warstw $|\mathcal{P}I_n/_{\equiv}| = 2^{n-1}$, a więc według zasady szufladkowej Dirichleta $\exists\, A, B \in \mathcal{A} : A \neq B, A \equiv B$, czyli $B = A^{\neg}$, $A \cap B = \varnothing$.

51.

a) Indukcja na n.

b) Indukcja na k lub bezpośrednim rachunkiem:

$$\begin{aligned} L = \prod_{i=1}^{k} \frac{(2i+n-1) \cdot n}{2} &= \frac{n^k}{2^k} \prod_{i=1}^{k} (2i+n-1) \\ &= \frac{n^k}{2^k}(n+1)(n+3)\dots(n+2k-1) = \frac{n^k}{2^k} \frac{(n+2k-1)!!}{(n-1)!!}. \end{aligned}$$

52. $9 \cdot |\operatorname{Inj}(n-1, 9)| = 9 \cdot 9^{\underline{n-1}} = 9 \cdot \binom{9}{n-1}(n-1)!$.

53. $\alpha_1 = 0$, $\alpha_2 = 5$, $\alpha_3 = 105$.
Ogólnie $\{1, 2, \dots, \underbrace{55\dots5}_{n}\} \ni \sum\limits_{k=0}^{n-1} c_k 10^k$

gdzie $c_k \in \{0, 1, \dots, 9\}$, $\sum\limits_{k=0}^{n-1} c_k > 0$, $c_{n-1} \leqslant 4$ lub: $c_{n-1} = 5$ i $\sum\limits_{k=1}^{n-2} c_k 10^k \leqslant \underbrace{55\dots5}_{n-1}$.
Zatem dla $n \geqslant 2$: $\alpha_n = \alpha_{n-1} + 5\beta_{n-1}$, gdzie $\beta_n =$ (liczba wystąpień cyfry 9 w ciągu

$1, 2, \ldots, \underbrace{99\ldots9}_{n}) = \sum_{k=1}^{n} \binom{n}{k} \cdot k \cdot 9^{n-k} = n \sum_{k=1}^{n} \binom{n-1}{k-1} \cdot 9^{n-k} = n \sum_{i=0}^{n-1} \binom{n-1}{i} \cdot 9^{n-i-1} = n10^{n-1}$.

Tak więc dla $n \geqslant 2$: $\alpha_n = \alpha_{n-1} + 5(n-1) \cdot 10^{n-2} = 5 + 5 \cdot 2 \cdot 10 + 5 \cdot 3 \cdot 10^2 + \cdots + 5 \cdot (n-1)10^{n-2} = 5 \cdot \sum_{k=1}^{n-1} k10^{k-1} = 5 \cdot \frac{(n-1)10^n - n10^{n-1} + 1}{81}$. $\alpha_4 = 1605$, $\alpha_5 = 21\,605$.

54. $\Rightarrow$) W niepustym posecie skończonym $(\mathcal{A}, \subset)$ istnieje element maksymalny. $\langle$Indukcja na $|\mathcal{A}|\rangle$.
$\Leftarrow$) HP: $X \notin \mathrm{Fin}$.
$\mathcal{A} := \mathcal{P}X \cap \mathrm{Fin} \neq \varnothing \quad \langle \varnothing \in \mathcal{A} \rangle$.
$\exists$) M – element maksymalny $\mathcal{A}$.
$M \subsetneq X \quad \langle M \in \mathrm{Fin} \rangle$. $\exists$) $a \in X \setminus M$. $M \subsetneq M \cup \{a\} \in \mathcal{A}$ ↯.

55.

$$\begin{aligned}
\left|\bigcup_{k=1}^{n} A_k\right| &= \left|\bigcup_{k=1}^{n-1} A_k\right| + |A_n| - \left|\bigcup_{k=1}^{n-1} A_k \cap A_n\right| \\
&= \sum_{k=1}^{n-1} (-1)^{k+1} \sum_{\alpha: I_k \nearrow I_{n-1}} \left|\bigcap_{i=1}^{k} A_{\alpha_i}\right| + |A_n| - \sum_{k=1}^{n-1} (-1)^{k+1} \sum_{\alpha: I_k \nearrow I_{n-1}} \left|\bigcap_{i=1}^{k} A_{\alpha_i} \cap A_n\right| \\
&= \sum_{k=2}^{n-1} (-1)^{k+1} \sum_{\alpha: I_k \nearrow I_{n-1}} \left|\bigcap_{i=1}^{k} A_{\alpha_i}\right| + \sum_{k=1}^{n} |A_k| - \sum_{l=2}^{n} (-1)^{l} \sum_{\alpha: I_{l-1} \nearrow I_{n-1}} \left|\bigcap_{i=1}^{l-1} A_{\alpha_i} \cap A_n\right| \\
&= \sum_{k=1}^{n} |A_k| + \sum_{k=2}^{n} (-1)^{k+1} \sum_{\alpha: I_k \nearrow I_{n-1}} \left|\bigcap_{i=1}^{k} A_{\alpha_i}\right| + \sum_{k=2}^{n} (-1)^{k+1} \sum_{\alpha: I_{k-1} \nearrow I_{n-1}} \left|\bigcap_{i=1}^{k-1} A_{\alpha_i} \cap A_n\right| \\
&= \sum_{k=1}^{n} |A_k| + \sum_{k=2}^{n} (-1)^{k+1} \sum_{\alpha: I_k \nearrow I_n} \left|\bigcap_{i=1}^{k} A_{\alpha_i}\right| \\
&= \sum_{k=1}^{n} (-1)^{k+1} \sum_{\alpha: I_k \nearrow I_n} \left|\bigcap_{i=1}^{k} A_{\alpha_i}\right|.
\end{aligned}$$

56. $a_{k,n} = n^k - b$, gdzie

$$b = \left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} (-1)^{i+1} \sum_{\alpha: I_i \nearrow I_n} \left|\bigcap_{j=1}^{i} A_{\alpha_j}\right|.$$

Dla $i \in I_n$: $\left| \bigcap\limits_{j=1}^{i} A_{\alpha_j} \right| = |\operatorname{Map}(I_k, I_n \setminus \operatorname{im}\alpha)| = (n-i)^k$.

Zatem $b = \sum\limits_{i=1}^{n} (-1)^{i+1}(n-i)^k \cdot |\{\alpha \mid \alpha : I_i \nearrow I_n\}| = \sum\limits_{i=1}^{n} (-1)^{i+1}\binom{n}{i}(n-i)^k$.

Po zmianie indeksu sumacyjnego $j = n - i \in \{n-1, \ldots, 1, 0\}$ $(i = n - j)$:

$$b = -(-1)^n \sum_{j=0}^{n-1} (-1)^j \binom{n}{j} j^k, \text{ a więc } a_{k,n} = n^k + (-1)^n \sum_{j=0}^{n-1} (-1)^j \binom{n}{j} j^k$$

i ostatecznie $\boxed{a_{k,n} = (-1)^n \sum\limits_{j=0}^{n} (-1)^j \binom{n}{j} j^k}$.

Teraz $a_{4,3} = (-1)^3 \sum\limits_{j=0}^{3} (-1)^j \binom{3}{j} j^4 = -[-\binom{3}{1} + \binom{3}{2} \cdot 2^4 - \binom{3}{3} \cdot 3^4] = 3 - 3 \cdot 16 + 81 = 36$.

Ten sam wynik uzyskamy, licząc $a_{n+1,n}$ z wykorzystaniem zasady szufladkowej Dirichleta:

$$a_{n+1,1} = n \cdot \binom{n+1}{2} \cdot (n-1)! = \frac{(n+1)^2 \cdot n^2 \cdot (n-1)!}{2} = \frac{(n+1)! \cdot n}{2},$$

$$a_{4,3} = \frac{4! \cdot 3}{2} = 36.$$

57. Ad (66). Wykażemy indukcją na $n \in \mathbb{N}^*$, że $F_n = F_0 F_1 \ldots F_{n-1} + 2$.

I $\quad n = 1$ OK $\quad \langle F_1 = 5 = F_0 + 2 = 3 + 2 \rangle$.

II $\quad$ OK dla n. Dla $n+1$?

$$F_0 F_1 \ldots F_n + 2 = (F_n - 2)F_n + 2 = (F_n - 1)^2 + 1 = \left(2^{2^n}\right)^2 + 1 = F_{n+1}.$$

Ad (67). HP: $\exists)\, k < n\ \exists)\, p \in \mathbb{P} : p \mid F_k \ \wedge\ p | F_n$.
Wówczas według (66) $p \mid 2$, a więc $p = 2$, $2 \mid F_n$ ↯.

Ad (68). HP: $\exists)\ n \in \mathbb{N}^* : F_{n-1} < p_n$.
Według (67): $\exists)\, q : n \hookrightarrow \mathbb{P}\ \forall\ i < n : q_i \mid F_i$.
Ponieważ $\{q_0, \ldots, q_{n-1}\} \not\subset \{p_1, \ldots, p_{n-1}\}$, $\quad \langle$bo gdyby, to $n \leqslant n-1$ ↯$\rangle$, więc $\exists)\ i < n : q_i \notin \{p_1, \ldots, p_{n-1}\}$. Ale $q_i \leqslant F_i \leqslant F_{n-1} < p_n$, a więc $q_i = p_0 = 2$, $2 \mid F_i$ ↯.

58. Dowody sa bezproblemowe – w oparciu o definicję funkcji ν_p i zasadnicze twierdzenie arytmetyki (65).

Udowodnimy np. własność (d): Niech $\alpha = \nu_p(a)$, $\beta = \nu_p(b)$ i $\alpha \leqslant \beta$. Wówczas $a = p^\alpha c$, $b = p^\beta d$, a więc $a + b = p^\alpha(c + p^{\beta-\alpha} d)$, $\nu_p(a+b) = \nu_p(p^\alpha) + \nu_p(c + p^{\beta-\alpha} d) \geqslant \nu_p(p^\alpha) = \alpha = \alpha \cap \beta$.

59. $\nu(1) = 0 \quad \langle \nu(1) = \nu(1) + \nu(1) \rangle$.
Jeżeli $\forall\ p \in \mathbb{P} : \nu(p) = 0$, to wg (65) $f = 0$.
W przeciwnym wypadku $\exists)\, p \in \mathbb{P} : k = \nu(p) > 0$, i wówczas $\forall\ n \in \mathbb{N}^* : \nu(p^n) = \nu(p) \cdot n = k \cdot \nu_p(p^n)$.
Ponieważ $\forall\ q \in \mathbb{P} \setminus \{p\} : \nu(q) = 0 \quad \langle$HP: $\nu(q) > 0$. $0 = \nu((p,q)) = \nu(p) \cap \nu(q) > 0$ ↯$\rangle$, więc – znów na mocy (65) – $\forall\ a \in \mathbb{N}^* : \nu(a) = k \cdot \nu_p(a)$.

60*. $\nu_p\left(\binom{p^n}{k}\right) = \nu_p\left(\dfrac{p^n!}{k!(p^n-k)!}\right) = \nu_p(p^n!) - \nu_p(k!) - \nu_p((p^n-k)!) = \sum\limits_{i=1}^{\infty}\left[\dfrac{p^n}{p^i}\right] - \sum\limits_{i=1}^{\infty}\left[\dfrac{k}{p^i}\right] - \sum\limits_{i=1}^{\infty}\left[\dfrac{p^n-k}{p^i}\right] = \sum\limits_{i=1}^{\infty}\left(p^{n-i} - \left[\dfrac{k}{p^i}\right] - \left[\dfrac{p^n-k}{p^i}\right]\right).$

Dla ustalonego $i \in I_n$:

$$\alpha_i = p^{n-i} - \left[\frac{k}{p^i}\right] - \left[\frac{p^n-k}{p^i}\right] = \begin{cases} 0 & \text{gdy } p^i \mid k, \text{ to jest } \nu_p(k) \geqslant i \\ 1 & \text{gdy } p^i \nmid k, \text{ to jest } \nu_p(k) < i. \end{cases}$$

$\langle$Jeśli $p^i \mid k$, to $p^i \mid p^n - k$, a więc $\alpha_i = 0$.
Jeżeli zaś $p^i \nmid k$, to $p^i \nmid p^n - k$, a więc $\exists)\ q, r, q', r' \in \mathbb{N} : k = p^i \cdot q + r$, $p^n - k = p^i \cdot q' + r'$, $0 < r < p^i$, $0 < r' < p^i$, czyli $0 < r + r' < 2p^i$. Ale $p^i \mid r + r'$, a więc $r + r' = p^i$, $p^n = p^i(q + q') - p^i$, $p^{n-i} - q - q' = 1$ $\rangle$.
Zatem $\nu_p\left(\binom{p^n}{k}\right) = \sum\limits_{\substack{i=1 \\ p^i \nmid k}}^{n} 1 = \sum\limits_{\substack{i=1 \\ \nu_p(k) < i}}^{n} 1 = n - \nu_p(k)$.

61.

$\Rightarrow$) Niech $b = \prod\limits_{\substack{r \in \mathbb{P} \\ r \leqslant p}} r$, $a = n + b$; wówczas

1° $n = a - b$

2° $a \perp b$ $\quad\langle$HP: $\exists)\ r \in \mathbb{P} : r \mid a$, $r \mid b$. Wówczas $r \mid n$, a więc $n \notin \mathbb{P}$ ↯$\rangle$

3° $b \mid ab$

$\Leftarrow$) HP: $n \notin \mathbb{P}$. $\exists)\, r \in \mathbb{P} : r \mid n$, $r^2 \leqslant n$. Wówczas $q \leqslant r$ $\quad\langle$HP: $r < q$. Wówczas $r \leqslant p$, a więc $r \mid a$, $r \mid b$, $a \not\perp b$ ↯$\rangle$. Zatem $q^2 \leqslant r^2 \leqslant n < q^2$ ↯.

62.

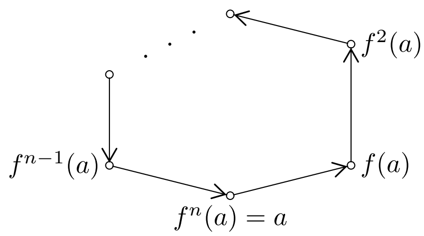
$\Rightarrow$) Dla $X = I_n$ wystarczy wziąć

$$f = \{1 \mapsto 2, 2 \mapsto 3, \ldots, n-1 \mapsto n, n \mapsto 1\}.$$

$\Leftarrow$) HP: $\exists)\, f : X \to X\ \forall\ \varnothing \neq A \subsetneq X : f(A) \not\subset A$ i $X \notin \mathrm{Fin}$. Dla $n \in \mathbb{N}$ niech f^n będzie n-tą iteracją funkcji f; $f^0 = \mathrm{id}_X$, $f^{n+1} = f \circ f^n$.

Oznaczmy dla $a \in X$: $B_a = \{f^n(a) \mid n \in \mathbb{N}\}$; wówczas $\forall\ a \in X : B_a = X$ $\quad\langle a \in B_a \neq \varnothing$, $f(B_a) \subset B_a\rangle$.
$\exists)\, a \in X$ $\quad\langle X \neq \varnothing$, gdyż $X \notin \mathrm{Fin}\rangle$.
$\exists\, n \in \mathbb{N} : f^{n+1}(a) = a$ $\quad\langle a \in B_{f(a)} = X\rangle$.

Weźmy najmniejsze $n \in \mathbb{N}^*$ takie, że $f^n(a) = a$.



Wówczas $X = \{f^k(a) \mid k < n\}$ $\langle$HP: $\exists) \, x \in X \ \forall k < n : x \neq f^k(a)$. Weźmy najmniejsze $m \in \mathbb{N}$ takie, że $x = f^m(a)$, $n \leqslant m$. Wówczas $\exists) \, q, r \in \mathbb{N} : m = nq + r$, $r < n$, a więc $x = f^r(f^{nq}(a))$, ale $f^{nq}(a) = a$, $\langle$indukcja na $q\rangle$, czyli $x = f^r(a)$ ↯$\rangle$.
Zatem $\{k \mapsto f^k(a) \mid k < n\} : n \longrightarrow\!\!\!\!\!\rightarrow X$, czyli, według kryterium (52) ze Wstępu, $X \in \mathrm{Fin}$ ↯.

Funkcja f jest permutacją cykliczną zbioru X, gdyż dla $a \in X$: $f = \{a \mapsto f(a), f(a) \mapsto f^2(a), \ldots, f^{n-1}(a) \mapsto a\}$.

63.

(a) Indukcja na $|X|$.

(b) Indukcja na $|X|$. HP: $\forall a \in X \ \exists x \in X : a < x$, $\exists) \, a \in X$. $A := \{x \in X \mid a < x\} \neq \varnothing$.
$|A| < |X|$ $\langle a \notin A\rangle$, więc według założenia indukcyjnego $\exists) \, b$ – element maksymalny A. $b \in X$, $\exists) \, x \in X : b < x$. Ale $a < b < x$, więc $x \in B$, $\neg \, b < x$ ↯.

(c) HP: $\exists) \, x \in X : \neg \, x \leqslant a$. $A = \{x \in X \mid \neg \, x \leqslant a\} \neq \varnothing$, a więc według (b) $\exists) \, b$ – element maksymalny A. Ponieważ $a \notin A$, więc $a \neq b$, $\exists) \, x \in X : b < x$. Wówczas $x \notin A$, $x \leqslant a$, $b < a$, ale $b \in A$, $\neg \, b \leqslant a$ ↯.

64.

$\Rightarrow)$ HP: $\neg \exists R$ – porządek liniowy w X. Wówczas $X \in \mathcal{T} \setminus \mathrm{Fin}$ ↯.

$\Leftarrow)$ HP: $\exists) \, X \in \mathcal{T} \setminus \mathrm{Fin}$. $\exists) \, R$ – porządek liniowy w X. Wówczas R jest dobrym porządkiem w X, a więc dla $\alpha = \mathrm{ord}(X, R)$ $f = \mathrm{nat}_{X,R} : \alpha \hookrightarrow\!\!\!\!\!\rightarrow X$, $\omega \leqslant \alpha$, $f|_\omega : \omega \hookrightarrow X$, $X \notin \mathrm{Fin}$ ↯.

65. $A \subsetneq A \cup B$, $\langle$bo gdyby $A = A \cup B$ to $B \subset A$, a więc $A = B$ ↯$\rangle$.
Zatem $A \cup B$ nie jest łańcuchem; $\exists x, y \in A \cup B : x \perp y$. Ponieważ $\{x, y\} \not\subset A$ i $\{x, y\} \not\subset B$, więc $x \in A$, $y \in B$ lub $x \in B$, $y \in A$.

66*.

(i) Natychmiast widać, że relacja $\leqslant$ jest zwrotna, antysymetryczna i spójna.
Ustawienie w tej relacji wszystkich elementów zbioru $\mathcal{P}3$ wygląda następująco:

$$\varnothing < \{0\} < \{1\} < \{0,1\} < \{2\} < \{0,2\} < \{1,2\} < \{0,1,2\}.$$

Aby udowodnić, że relacja $\leqslant$ jest dobrym porządkiem w $\mathcal{F}$, wystarczy jeszcze wykazać, że w każdym $\varnothing \neq \mathcal{A} \subset \mathcal{F}$ istnieje element minimalny $\langle$kryterium Tarskiego$\rangle$.

Jeżeli $\varnothing \in \mathcal{A}$, to $\varnothing$ jest elementem minimalnym $\mathcal{A}$.

Załóżmy, że $\varnothing \notin \mathcal{A} \neq \varnothing$. Wówczas wybieramy w $\mathcal{A}$ taki element $A = \{a_0, a_1, \ldots, a_m\}$, $a_0 < a_1 < \ldots < a_m$, że dla każdego $\mathcal{A} \ni B = \{b_0, b_1, \ldots, b_n\}$, $b_0 < b_1 < \ldots < b_n$ jest $a_m = b_n$, $a_{m-1} = b_{n-1}$, …, $a_{m-k} = b_{n-k}$ i $k = m$ lub $a_{m-k-1} < b_{n-k-1}$.

Łatwo sprawdzić, że A jest elementem minimalnym $\mathcal{A}$.

(ii) Ponieważ dla $A, B \in \mathcal{F}$ takich, że $\varnothing \neq A < B$ jest $\max A \leqslant \max B$, czyli $A \subset \{0, 1, \ldots, \max B\}$, więc dla każdego $B \in \mathcal{F}$ zbiór $\{A \in \mathcal{F} \mid A < B\}$ jest skończony, skąd wynika, że $\operatorname{ord}(\mathcal{F}, \leqslant) = \omega$.

67.

(a) Indukcją na α pokazujemy, że $V_\alpha \subset \mathcal{P}V_\alpha$:

(I) $V_0 = \varnothing \subset \mathcal{P}V_0$.

(II) Jeżeli $V_\alpha \subset \mathcal{P}V_\alpha = V_{\alpha+1}$, to $V_{\alpha+1} = \mathcal{P}V_\alpha \subset \mathcal{P}V_{\alpha+1}$.

(III) Jeżeli $\lambda \in \mathrm{Lim}$ i $\forall \xi < \lambda : V_\xi \subset \mathcal{P}V_\xi$, to dla $x \in V_\lambda$ $\exists \xi < \lambda : x \in V_\xi$, $x \subset V_\xi \subset \bigcup_{\xi<\lambda} V_\xi = V_\lambda$, a więc $V_\lambda \subset \mathcal{P}V_\lambda$.

(b) Indukcja na β:

(I) $\beta = 0$ OK.

(II) OK dla β. Jeżeli $\alpha < \beta + 1$, to $\alpha \leqslant \beta$, i mamy dwa przypadki:

1) $\alpha < \beta$. Wówczas $V_\alpha \in V_\beta$, więc (według a)) $V_\alpha \subset V_\beta$, czyli $V_\alpha \in \mathcal{P}V_\beta = V_{\beta+1}$.

2) $\alpha = \beta$, i wtedy $V_\alpha = V_\beta \in \mathcal{P}V_\beta = V_{\beta+1}$.

(III) $\beta \in \mathrm{Lim}$ i OK dla wszystkich $\xi < \beta$.
Jeśli $\alpha < \beta$, to $\exists)\, \xi < \beta : \alpha < \xi$, $V_\alpha \in V_\xi \subset V_\beta$.

(c) Wniosek z b) i a).

(d) Indukcja na α:

(I) $0 \in V_1 \setminus V_0 = \{0\}$.

(II) Jeżeli $\alpha \in V_{\alpha+1} \setminus V_\alpha$, to $\{\alpha\} \subset V_{\alpha+1}$ i $\alpha \subset V_{\alpha+1}$, a więc $\alpha + 1 = \alpha \cup \{\alpha\} \subset V_{\alpha+1}$, $\alpha + 1 \in \mathcal{P}V_{\alpha+1} = V_{\alpha+2}$. $\alpha + 1 \notin V_{\alpha+1}$ $\quad\langle$HP: $\alpha + 1 = \alpha \cup \{\alpha\} \in V_{\alpha+1}$, $\alpha \in \alpha \cup \{\alpha\} \subset V_\alpha$, a więc $\alpha \in V_\alpha$ $\lightning\rangle$.

(e) Sprawdzamy, że:

1) Zbiór V_ω spełnia wszystkie postulaty zbioru uniwersalnego, a więc $V_\alpha \in \mathrm{Univ}$.

2) Dla dowolnego $U \in \mathrm{Univ}$ indukcją na $n < \omega$ sprawdzamy, że $V_n \subset U$, a więc $V_\omega = \bigcup_{n<\omega} V_n \subset U$.

(f) Proste wykorzystanie własności ciągu V i definicji pary.

68. HP: $\mathbb{V} \setminus \bigcup_{\alpha\in\mathrm{Ord}} V_\alpha \neq \varnothing$. Na mocy zasady regularności:

$$\exists)\, a \in \mathbb{V} \setminus \bigcup_{\alpha\in\mathrm{Ord}} V_\alpha : a \cap \left(\mathbb{V} \setminus \bigcup_{\alpha\in\mathrm{Ord}} V_\alpha\right) = \varnothing.$$

Wówczas $a \subset \bigcup_{\alpha\in\mathrm{Ord}} V_\alpha$, $\quad\langle$bo gdyby $\exists\, x \ldots\rangle$,

$f := \{x \mapsto \bigcap\{\alpha \in \mathrm{Ord} \mid x \in V_\alpha\} \mid x \in a\} : a \to \mathrm{Ord}$, $\forall x \in a : x \in V_{f(x)}$.

$\beta := \bigcup\{f(x) \mid x \in a\} \in \mathrm{Ord}$, $\forall\, x \in a : f(x) \leqslant \beta$, $V_{f(x)} \subset V_\beta$, $x \in V_\beta$.
Zatem $a \subset V_\beta$, $a \in V_{\beta+1} \subset \bigcup\limits_{\alpha \in \mathrm{Ord}} V_\alpha$ ↯.

69.

(a) Równoważność wynika z faktu, że $\varnothing \neq m(x) \subset \{y \mid x \sim y\}$, (relacja $\sim$ jest równoważnością w klasie wszystkich zbiorów);
(b) Dla $a, b \in \mathcal{C}$ określamy:

$$a \leqslant b \;:\Longleftrightarrow\; \exists\, x, y : a = m(x) \;\;\wedge\;\; b = m(y) \;\;\wedge\;\; x \subset y.$$

Zwrotność i przechodniość tej relacji łatwo wynika z powyższej definicji; antysymetria jest natychmiastowym wnioskiem z twierdzenia Cantora–Bernsteina.
(c) Dla $a, b \in \mathcal{C}$:

$$\begin{aligned} a + b &:= \bigcap\{m(x \cup y) \mid m(x) = a, m(y) = b, x \cap y = \varnothing\} \in \mathcal{C} \\ a \cdot b &:= \bigcap\{m(x \times y) \mid m(x) = a, m(y) = b\} \in \mathcal{C} \\ b^a &:= \bigcap\{m(\mathrm{Map}(x, y)) \mid m(x) = a, m(y) = b\} \in \mathcal{C}. \end{aligned}$$

Poprawność tych definicji, na przykład dodawania, wynika stąd, że $\forall\, x, y, x', y' :$ $m(x) = m(x') = a \;\;\wedge\;\; m(y) = m(y') = b \;\;\wedge\;\; x \cap y = \varnothing = x' \cap y' \;\Rightarrow\; m(x \cup y) = m(x' \cup y')$, i wówczas $\forall\, z, t : z \cap t = \varnothing \wedge m(z) = a \wedge m(t) = b \;\Rightarrow\; \{m(x \cup y) \mid m(x) = a, m(y) = b, x \cap y = \varnothing\} = \{m(z \cup t)\}$.
Analogicznie jest dla mnożenia i potęgowania.

Własności wyżej określonych działań, takie jak np. łączność i przemienność dodawania i mnożenia, rozdzielność mnożenia względem dodawania, elementarne prawa potęgowania itp., uzasadniamy mechanicznym rachunkiem.

70. Z łatwego do udowodnienia faktu:

$$\forall\, k, n \in \mathbb{N} : k \leqslant n \wedge k \sim n \;\Rightarrow\; k = n \quad \langle\text{indukcja na } n\rangle$$

wynika, że $m|_{\mathbb{N}} : \mathbb{N} \hookrightarrow \mathcal{C}$, a więc liczby kardynalne zbiorów skończonych możemy utożsamiać z liczbami naturalnymi.

71. $\forall\, x \in A : x \subset V_{\mathrm{rk}\, x}$, $x \in V_{\mathrm{rk}\, x+1}$, $A \cap V_{\mathrm{rk}\, x+1} \neq \varnothing$.
Zatem $\rho(A) = \bigcap\{\mathrm{rk}\, x + 1 \mid x \in A\} = \bigcap\{\mathrm{rk}\, x \mid x \in A\} + 1$.

72.

(a), (b) wynikają natychmiast z definicji.
(c) Indukcja na α.
(d) Rozpatrujemy oddzielnie trzy przypadki dla $\beta = \mathrm{rk}\, y$: $\beta = 0$, $\beta \in \mathrm{Seq}$, $\beta \in \mathrm{Lim}$.
(e) Ponieważ $V_\alpha \subset V_\alpha$, więc $\mathrm{rk}\, V_\alpha \leqslant \alpha$. HP: $\mathrm{rk}\, V_\alpha = \beta < \alpha$; wówczas $V_\alpha \subset V_\beta \subset V_\alpha$, a więc $V_\alpha = V_\beta$, $\alpha = \beta$ ↯.
(f) $\subset$) Jeśli $x \in V_{\alpha+1} \setminus V_\alpha$, to $x \subset V_\alpha$, $\mathrm{rk}\, x \leqslant \alpha$.
HP: $\mathrm{rk}\, x = \beta < \alpha$; wówczas $x \subset V_\beta$, $x \in V_{\beta+1} \subset V_\alpha$ ↯.

$\supset$) Jeśli $\operatorname{rk} x = \alpha$, to $x \subset V_\alpha$, $x \in V_{\alpha+1}$.
HP: $x \in V_\alpha$. Wówczas $\operatorname{rk} x < \alpha$ $\langle$wg (c)$\rangle$ $\lightning$.

(g) Ponieważ $\alpha \in V_{\alpha+1} \setminus V_\alpha$ $\langle$zadanie 28.(d)$\rangle$, więc $\operatorname{rk} \alpha = \alpha$ $\langle$wg (f)$\rangle$.

(h) Natychmiastowy wniosek z definicji.

(i) Oznaczmy $\alpha = \operatorname{rk} x$. Ponieważ $x \subset V_\alpha$, więc $\mathcal{P}x \subset \mathcal{P}V_\alpha = V_{\alpha+1}$, $\operatorname{rk} \mathcal{P}x \leqslant \alpha + 1$.
HP: $\operatorname{rk} \mathcal{P}x < \alpha + 1$; wówczas $\operatorname{rk} \mathcal{P}x \leqslant \alpha$, $\mathcal{P}x \subset V_\alpha$, $x \in V_\alpha$, $\operatorname{rk} x < \alpha$ $\langle$wg (c)$\rangle$ $\lightning$.
Podobnie $x \in V_{\alpha+1}$, $\{x\} \subset V_{\alpha+1}$, $\operatorname{rk}\{x\} \leqslant \alpha + 1, \ldots$

(j) Pierwsza równość: Sprawdzamy, że:

1°) $\forall y \in x : \operatorname{rk} y + 1 \leqslant \operatorname{rk} x$ $\langle$wg (d)$\rangle$.

2°) Jeśli $\beta \in \mathrm{Ord}$ i $\forall y \in x : \operatorname{rk} y + 1 \leqslant \beta$, to $\forall y \in x : \operatorname{rk} y < \beta$, $y \in V_\beta$ $\langle$wg (c)$\rangle$, a więc $y \subset V_\beta$, $x \in V_\beta$, $\operatorname{rk} x \leqslant \beta$.

Druga równość:

1°) $\operatorname{rk} x \in \{\alpha \in \mathrm{Ord} \mid \forall y \in x : \operatorname{rk} y < \alpha\}$ $\langle$wg (d)$\rangle$.

2°) Jeśli dla $\alpha \in \mathrm{Ord}$ zachodzi warunek $\forall y \in x : \operatorname{rk} y < \alpha$, to $x \subset V_\alpha$, a więc $\operatorname{rk} x \leqslant \alpha$.

(k) $\exists y \in x$. $\bigcap x \subset y$. $\operatorname{rk} \bigcap x \leqslant \operatorname{rk} y < \operatorname{rk} x$ $\langle$wg (b), (d)$\rangle$.

(l) Podobnie jak w punkcie (d) rozpatrujemy trzy przypadki dla $\alpha = \operatorname{rk} x$.

73.

$\subset$) $\mathrm{Ord} \subset T$ $\langle$z definicji$\rangle$.
Jeżeli $\alpha \in \mathrm{Ord}$, to $\alpha \subset \mathrm{Ord}$, a więc $\alpha \subset T$, $\alpha \in \mathcal{P}T$, czyli $\mathrm{Ord} \subset \mathcal{P}T$, $\mathrm{Ord} \subset T \cap \mathcal{P}T$.

$\supset$) HP: $\mathrm{Ord} \subsetneq T \cap \mathcal{P}T$.

Weźmy najmniejszej rangi element a taki, że $a \in (T \cap \mathcal{P}T) \setminus \mathrm{Ord}$.
Tak więc $\forall x \in (T \cap \mathcal{P}T) \setminus \mathrm{Ord} : \operatorname{rk} a \leqslant \operatorname{rk} x$.
Ponieważ $a \in T$ i $a \notin \mathrm{Ord}$, więc $\exists)\, x, y \in a : x \neq y \wedge x \notin y \wedge y \notin x$;
$\operatorname{rk} x < \operatorname{rk} a$ $\langle$zadanie 72.(d)$\rangle$.
$x \in T$ $\langle a \in \mathcal{P}T$, a więc $a \subset T\rangle$.
$x \subset T$ $\langle$HP: $\exists)\, z \in x : z \notin T$. Ponieważ $a \in T$, więc $a \subset \mathcal{P}a$, $x \in \mathcal{P}a$, $x \subset a$, zatem $z \in a$. Ale $a \in \mathcal{P}T$, więc $a \subset T$, $z \in T$ $\lightning\rangle$.
Tak więc $x \in T \cap \mathcal{P}T$, a więc $x \in \mathrm{Ord}$ $\langle$HP: $x \notin \mathrm{Ord}$. Wówczas $x \in (T \cap \mathcal{P}T) \setminus \mathrm{Ord}$, a więc $\operatorname{rk} a \leqslant \operatorname{rk} x < \operatorname{rk} a$ $\lightning\rangle$.
Analogicznie $y \in \mathrm{Ord}$.
Zatem $x = y \vee x \in y \vee y \in x$ $\lightning$.

74. Notujmy $\leqslant$, $<$ zamiast $\underset{R}{\leqslant}$, $\underset{R}{<}$ i dla $a \in A$: S_a zamiast $S_a(A, R)$; $S_a = \{x \in A \mid x < a\} \in \mathcal{P}A$.
HP: $\neg \exists b \in B\ \forall x \in B\ (x \leqslant b \Rightarrow x = b)$, a więc $\forall b \in B\ \exists x \in B : x < b$, czyli $\forall b \in B : S_b \cap B \neq \varnothing$. $\exists)\, b \in B$.
Określamy ciąg $F : \mathbb{N} \to \mathcal{P}B \setminus \{\varnothing\}$: $F_0 = S_b \cap B$, $F_{n+1} = \bigcup\limits_{x \in F_n} F_x \cap B$.
$E := \bigcup\limits_{n \in \mathbb{N}} F_n \in \mathcal{P}B \setminus \{\varnothing\}$. $\exists)\, e$ – element R-minimalny E.
$\exists)\, n \in \mathbb{N} : e \in F_n$, $\exists)\, x \in S_e \cap B \subset F_{n+1} \subset E$; $x < e$ $\lightning$.

75. Przyjmijmy oznaczenia z poprzedniego zadania 74.
Przypuśćmy, że $\exists\, x \in B : f(x) < x$.
Zatem $C = \{x \in B \mid f(x) < x\} \neq \varnothing$. Na mocy zasady elementu minimalnego (zadanie 74) $\exists)\, c$ – element R-minimalny C. $f(c) < c$, $f(c) \in B$ $\quad\langle C \subset B$ i B jest R-odcinkiem w $A\rangle$, $f(c) \notin C$.

Ale $f(f(c)) < f(c)$, czyli $f(c) \in C$ ↯.

76. HP: $A \not\subset B$.
Zatem $\varnothing \neq A \setminus B \subset A$, i według zasady elementu minimalnego (zadanie 74):

$$\exists)\, a \text{ – element } R\text{-minimalny } A \setminus B.$$

Wówczas $S_a(A, R) \subset B$, a więc $a \in B$ ↯.

77*. Przyjmijmy oznaczenia jak w rozwiązaniach zadań 74–76.

1) $f : A \multimap B$ $\quad\langle$Sprawdzamy warunek sklejenia:
Niech $\varphi, \psi \in \Phi$, $A' := \{x \in A \mid x \in \operatorname{Dom}\varphi \cap \operatorname{Dom}\psi \;\Rightarrow\; \varphi(x) = \psi(x)\}$. Jeżeli dla $x \in A$, $S_x \subset A'$, to $x \in A'$ $\quad\langle$HP: $x \notin A'$. $x \in \operatorname{Dom}\varphi \cap \operatorname{Dom}\psi$ i $\varphi(x) \neq \psi(x)$. Jednak $S_x \subset \operatorname{Dom}\varphi \cap \operatorname{Dom}\psi$, $\varphi|_{S_x} = \psi|_{S_x}$, a więc $\varphi(x) = H(x, \varphi|_{S_x}) = H(x, \psi|_{S_x}) = \psi(x)$ ↯$\rangle$. Zatem na mocy twierdzenia o indukcji (zadanie 76) $A' = A\rangle$.

2) $f : A \to B$ $\quad\langle$HP: $\operatorname{Dom} f \subsetneq A$. Na mocy zasady elementu minimalnego (zadanie 74) $\exists)\, a$ – element R-minimalny $A \setminus \operatorname{Dom} f$. Jednak $\operatorname{Dom} f = \bigcup\{\operatorname{Dom}\varphi \mid \varphi \in \Phi\}$ – R-odcinek A, a więc $\varphi := f \cup \{a \mapsto H(a, f)\} \in \Phi$ $\quad\langle\operatorname{Dom}\varphi = \operatorname{Dom} f \cup \{a\}$, $S_a \subset \operatorname{Dom}\varphi\rangle$, czyli $a \in \operatorname{Dom}\varphi \subset \operatorname{Dom} f$ ↯$\rangle$.

3) Jeżeli $x \in A$, to $\exists)\, \varphi \in \Phi : x \in \operatorname{Dom}\varphi$, $\varphi \subset f$, $f(x) = \varphi(x) = H(x, \varphi|_{S_x}) = H(x, f|_{S_x})$.

4) Jeżeli $g : A \to B$ i $\forall\, x \in A : g(x) = H(x, g|_{S_x})$, to zastosujmy twierdzenie o indukcji (zadanie 76) do klasy $A' = \{x \in A \mid fx = g(x)\}$.
Niech $x \in A$, $S_x \subset A'$. Wówczas $f|_{S_x} = g|_{S_x}$, a więc $f(x) = H(x, f|_{S_x}) = H(x, g|_{S_x}) = g(x)$.
Zatem $A' = A$, czyli $f = g$.

78*.

Ad (i).

1°) Klasa B jest tranzytywna $\quad\langle$HP: $\exists)\, y \in B : y \not\subset B$ $\exists)\, z \in y \setminus B$. $\exists)\, x \in A : y = f(x) = \operatorname{Im}(f|_{x \cap A})$. $z \in \operatorname{Im}(f|_{x \cap A})$. $\exists)\, t \in x \cap A : z = f(t) \in B$ ↯$\rangle$.

2°) Jeżeli $x, y \in A$ i $x \in y$, to $f(x) \in f(y)$ $\quad\langle f(y) = \operatorname{Im}(f|_{y \cap A})$, $x \in y \cap A\rangle$.

3°) $f : A \hookrightarrow\!\!\!\!\rightarrow B$ $\quad\langle$HP: $\neg\, f : A \hookrightarrow B$. Wówczas $A' := \{x \in A \mid \forall\, y \in A : x \neq y \;\Rightarrow\; f(x) \neq f(y)\} \subsetneq A$.
Według twierdzenia o indukcji dla relacji $\mathbb{E}$ (zadanie 76):
$\exists)\, x \in A : x \cap A \subset A' \;\wedge\; x \notin A'$, a więc $\exists)\, y \in A : x \neq y \;\wedge\; f(x) = f(y)$.
$x \cap A \neq y \cap A$ $\quad\langle$bo klasa A jest ekstensjonalna$\rangle$.
Możliwe są dwa przypadki:

(I) $\exists)\, z \in x \cap A$, $z \notin y$.
Wówczas $z \in A'$, $f(z) \in \operatorname{Im}(f|_{x \cap A}) = f(x) = f(y) = \operatorname{Im}(f|_{x \cap A})$, $\exists)\, t \in y \cap A : f(z) = f(t)$, a więc $z = t \in y$ ↯.

(II) $\exists)\, z \in y \cap A,\ z \notin x$.

Wówczas $f(z) \in \operatorname{Im}(f|_{y\cap A}) = f(y) = f(x) = \operatorname{Im}(f|_{x\cap A})$, $\exists)\, t \in x \cap A : f(z) = f(t)$, $t \in A'$, $z = t \in x$ ↯$\rangle$.

4°) Jeżeli $x, y \in A$ i $f(x) \in f(y)$, to $\exists)\, z \in A \cap y : f(x) = f(z)$, $x = z$, a więc $x \in y$.

Ad (ii). Oznaczmy $A' = \{x \in A \mid f(x) = g(x)\}$.

Jeżeli $x \in A$ i $x \cap A \subset A'$, to $f|_{x\cap A} = g|_{x\cap A}$, a więc $f(x) = \operatorname{Im}(f|_{x\cap A}) = \operatorname{Im}(g|_{x\cap A}) = g(x)$, czyli $x \in A'$.

Na mocy twierdzenia o indukcji ze względu na przynależność (zadanie 76) $A' = A$, $f = g$.

Ad (iii).

1°) Oznaczmy $A' = \{x \in A \mid x \in T \Rightarrow f(x) = x\}$.

Jeżeli $x \in A$ i $x \cap A \subset A'$, to $x \in A'$ $\langle$HP: $x \notin A'$, a więc $x \in T$ i $f(x) \neq x$.

Mamy dwa przypadki:

(I) $\exists)\, y \in f(x) \setminus x$. Ponieważ $y \in f(x) = \operatorname{Im}(f|_{x\cap A})$, więc $\exists)\, z \in x \cap A : y = f(z)$. Ale $z \in A'$ i $z \in T$ $\langle$bo $x \subset T\rangle$, więc $f(z) = z$, $y = z \in x$ ↯.

(II) $\exists)\, y \in x \setminus f(x)$. Wówczas $y \in x \subset T \subset A$, czyli $y \in x \cap A \subset A'$, $y = f(y) \in f(x)$ ↯$\rangle$.

Zatem $A' = A$, czyli $f|_T \subset \mathrm{id}$.

2°) Klasa $A \cap \mathcal{P}T$ jest tranzytywna. $\langle$Jeżeli $x \in A \cap \mathcal{P}T$, to $x \subset T \subset A \cap \mathcal{P}T\rangle$, a więc, według 1°), $f|_{A\cap\mathcal{P}T} \subset \mathrm{id}$.

6

Aksjomat wyboru

6.1. Wstęp

Równoważnikiem aksjomatu wyboru (AC) jest poniższe *twierdzenie o dobrym uporządkowaniu* (WO, *Well-ordering theorem*, 1904, E. Zermelo) mówiące, że każdy zbiór można dobrze uporządkować;

symbolicznie

$$\text{(WO)} \qquad \forall\, A\, \exists\, R : R - \text{dobry porządek w } A.$$

W postaci równoważnej:

$$\text{(WO}'\text{)} \qquad \forall\, A\, \exists\, \alpha \in \mathrm{Ord} : A \sim \alpha.$$

$\langle$(WO)$\Rightarrow$(WO$'$). Dla $\alpha = \mathrm{ord}(A,R)$, $f = \mathrm{nat}_{A,R}$, $f : \alpha \lhook\joinrel\twoheadrightarrow A$.

(WO$'$)$\Rightarrow$(WO). $\exists)\, f : \alpha \lhook\joinrel\twoheadrightarrow A$. Bijekcja f przenosi naturalny dobry porządek w α na zbiór $A\rangle$.

$\langle$(AC)$\Rightarrow$(WO$'$). $\exists)\, \tau : \mathcal{P}A \setminus \{\varnothing\} \to A\ \forall \varnothing \neq X \subset A : \tau(X) \in X$ (τ jest funkcją wyboru dla zbioru $\mathcal{P}A \setminus \{\varnothing\}$).

Określamy indukcyjnie ciąg f:

$$\forall\, \xi \in \mathrm{Ord} : f(\xi) = \tau(A \setminus \mathrm{Im}(f|\xi)).$$

Niech $\alpha = \mathrm{Dom}\, f$.

Z warunku określającego f wynika, że $\forall\, \eta < \xi \in \alpha : f(\eta) \neq f(\xi) \quad \langle f(\eta) \in \mathrm{Im}(f|\xi)\rangle$, a więc $f : \alpha \lhook\joinrel\longrightarrow A$, skąd $\alpha \in \mathrm{Ord}$.

Ponieważ $\alpha \notin \alpha$, więc $\mathbb{V} = f(\alpha) = \tau(A \setminus \mathrm{Im}\, f)$, czyli $A \setminus \mathrm{Im}\, f = \varnothing$, $f : \alpha \lhook\joinrel\twoheadrightarrow A$, $A \sim \alpha$.

(WO$'$)$\Rightarrow$(AC).
Niech $\varnothing \notin x$. $\exists)\, \alpha \in \mathrm{Ord}$, $f : \alpha \lhook\joinrel\twoheadrightarrow \bigcup x$. Funkcję wyboru $\tau : x \to \bigcup x$ określamy, kładąc dla $y \in x$: $\tau(y) = f(\bigcap \mathrm{Im}(f^{-1}|y)))\rangle$.

Drugim często wykorzystywanym równoważnikiem aksjomatu wyboru jest *lemat Zorna* (ZL, *Zorn Lemma*, 1935 M. Zorn) mówiący, że w posecie, w którym każdy łańcuch posiada majorantę, istnieje element maksymalny;

symbolicznie:

$$\forall\, A, R - \text{porządek w } A\ \big[\forall\, B \subset A (R - \text{porządek liniowy w } B$$
$$\Rightarrow\ \exists\, x \in A\, \forall\, y \in B\ y \underset{R}{\leqslant} x) \implies \exists\, x - \text{element } R\text{-maksymalny } A\big].$$

$\langle$(AC) $\Rightarrow$ (ZL). HP: $\neg \ldots$
Wówczas $\forall\, B \in \mathcal{B} :=$ ogół łańcuchów w A: $M^*(B) =$ *silne majoranty* $B := \{z \in A \mid \forall\, y \in B : y \underset{R}{<} z\} \neq \varnothing$. $\exists)\, \tau : \mathcal{P}A \setminus \{\varnothing\} \to A$ – funkcja wyboru.

Określamy indukcyjnie ciąg $f : \forall\, \xi \in \mathrm{Ord} : f(\xi) = \tau(M^*(\mathrm{Im}(f|\xi)))$.

Niech $\alpha \in \mathrm{Dom}\, f$.
Wówczas $\forall\, \xi \in \alpha : f(\xi) \in M^*(\mathrm{Im}(f|\xi))$, $\mathrm{Im}(f|\xi) \in \mathcal{B}$; $f : \alpha \hookrightarrow A$, $\alpha \in \mathrm{Ord}$, $\forall\, \eta < \xi \in \alpha : f(\eta) \underset{R}{<} f(\xi)$, $\mathrm{Im}\, f \in \mathcal{B}$.

Ponieważ $\alpha \notin \alpha$, więc $\mathbb{V} = f(\alpha) = \tau(M^*(\mathrm{Im}(f))$, skąd $M^*(\mathrm{Im}\, f) = \varnothing$ ↯.

(ZL) $\Rightarrow$ (AC). Niech $\varnothing \notin x$.
Zbiór $F = \{f : x \multimap \bigcup x \mid \forall\, y \in \mathrm{Dom}\, f : f(y) \in y\}$ częściowych funkcji wyboru w x spełnia założenia lematu Zorna. $\langle$Dla $\subset$-łańcucha $G \subset F$ majorantą G jest $\bigcup G \in F\rangle$. Element maksymalny τ posetu F jest pełna funkcja wyboru $\tau : x \to \bigcup x$ $\langle$HP: $\mathrm{Dom}\, \tau \subsetneq x$. $\exists)\, y \in x \setminus \mathrm{Dom}\, \tau$; $y \neq \varnothing$, $\exists)\, z \in y$, $\tau \subsetneq \tau \cup \{y \mapsto z\} \in F$ ↯$\rangle\rangle$.

Niektóre inne równoważniki aksjomatu wyboru znajdziemy w zadaniach.

6.2. Tematy

1. Wykazać, że poniższa *zasada maksimum Hausdorffa* (Hausdorff Maximal Principle) – w dwóch równoważnych wersjach:

(HMP) w posecie X każdy łańcuch można rozszerzyć do łańcucha maksymalnego,

(HMP$'$) w każdym posecie istnieje łańcuch maksymalny,

jest równoważna aksjomatowi wyboru.
Wskazówka: Oczywiście (HMP)$\Rightarrow$(HMP$'$). $\langle$Łańcuch pusty $\varnothing$ rozszerzamy do łańcucha maksymalnego$\rangle$. Wystarczy więc wykazać, że (ZL)$\Rightarrow$(HMP) i (HMP$'$)$\Rightarrow$(ZL).

2. Dla danego zbioru X oznaczmy:

$$\begin{aligned} F(X) &= \{R \subset X^2 \mid R\text{-porządek w } X\} \\ &= \text{ ogół porządków (częściowych) w } X \end{aligned}$$

i analogicznie:

$$L(X) = \text{ogół porządków liniowych w } X$$

$$\begin{aligned} M(X) &= \text{ogół porządków maksymalnych w } X \\ &= \{R \in F(X) \mid \forall\, S \in F(X) : R \subset S \;\Rightarrow\; R = S\}. \end{aligned}$$

Wykazać (w ZFC), że:
(i) $\forall\, R \in F(X)\; \exists\, R' \in M(X) : R \subset R'$
(ii) $L(X) = M(X)$
(iii) $\forall\, R \in F(X)\; \exists\, R' \in L(X) : R \subset R'$.

Tak więc każdy porządek w danym zbiorze można rozszerzyć do porządku liniowego. Porządki liniowe w zbiorze X są dokładnie porządkami maksymalnymi w zbiorze $F(X)$ wszystkich porządków w X.

Wskazówka: Jeżeli $R \in F(X) \setminus L(X)$, to dla pewnych $x, y \in X$ $(x,y), (y,x) \notin R$ i wówczas $R \subsetneq R' = R \cup \{(a,b) \in X^2 \mid (a,x), (y,b) \in R\} \in F(x)$.

3.

(a) Dla ustalonego $n \in N$ określić *naturalny* porządek liniowy $\leqslant$ w zbiorze $\mathcal{P}I_n$ (= ogół podzbiorów zbioru $I_n = \{1, ..., n\}$) będący rozszerzeniem relacji inkluzji, to jest spełniający warunek:

$$\forall\, A, B \subset I_n : A \subset B \;\Rightarrow\; A \leqslant B.$$

Wskazówka: wykorzystać rozkłady pozycyjne.
Narysować odpowiedni diagram dla $n = 3$.

(b) Wykorzystując konstrukcję z punktu (a), zdefiniować *naturalny* dobry porządek R w zbiorze $\mathrm{Fin} \cap \mathcal{P}\mathbb{N}^*$ wszystkich podzbiorów skończonych zbioru $\mathbb{N}^* = \{1, 2, 3, \ldots\}$.

Wypisać w tym uporządkowaniu szesnaście pierwszych podzbiorów skończonych zbioru $\mathbb{N}^*$.

Oznaczając $E = \mathrm{nat}_{\mathrm{Fin} \cap \mathcal{P}\mathbb{N}^*, R}$, sformułować podstawowe własności porządku R.

Porównać otrzymane wyniki z zadaniem 5.66^*.

Na mocy twierdzenia o dobrym uporządkowaniu (WO) istnieje dobry porządek w zbiorze $\mathcal{P}\mathbb{N}^*$, nie znamy jednak żadnego przykładu ani konstrukcji takiego porządku.

4. Dla zbioru X, zachowując notację z zadania 2, oznaczmy $W(X) =$ ogół dobrych porządków w X.

Wykazać, że:

$$\forall\, R \in L(X)\; \exists\, Y \subset X \;\left[R \cap Y^2 \in W(Y) \wedge \forall\, x \in X\; \exists\, y \in Y : x \underset{R}{\leqslant} y \right].$$

Dla posetu X i zbioru $A \subset X$ mówimy, że A jest *współkońcowy* z X, gdy $\forall\, x \in X\; \exists\, a \in A : x \leqslant a$.

Powyższe twierdzenie mówi, że każdy zbiór liniowo uporządkowany zawiera współkońcowy z nim podzbiór dobrze uporządkowany.

Wskazówka: Rodzinę $\mathcal{A} = \{A \subset X \mid R \cap A^2 \in W(A)\}$ uporządkować, kładąc dla $A, B \in \mathcal{A}$: $A \leqslant B \iff A$ – R-odcinek B.

5.

a) Zachowujemy notację z zadań 2 i 4.
Udowodnić (w ZF), że $\forall\, X \in \mathrm{Fin} : W(X) = L(X)$, tzn. w zbiorze skończonym każdy porządek liniowy jest dobrym porządkiem.

b) Podać przykład zbioru nieskończonego X i porządku liniowego R w X nie będącego dobrym porządkiem w X.
Tak więc nie każdy porządek w zbiorze nieskończonym X można rozszerzyć do dobrego porządku (por. zadanie 2.(c)).

6. W ZF mamy równoważność: AC $\iff \forall\, x : W(x) \neq \varnothing$.

Symbolicznie: $\mathrm{ZF} \vdash \mathrm{AC} \iff \forall\, x : W(x) \neq \varnothing$ (oznaczenia z poprzednich zadań). Rozważmy słabszy warunek, że każdy zbiór można liniowo uporządkować:

(OP) $\forall\, x : L(x) \neq \varnothing$ *(Ordering principle).*

Wykazać, że $\mathrm{ZF} \vdash \mathrm{OP} \Rightarrow \mathrm{ACF}$, gdzie

(ACF) $\forall\, x \subset \mathrm{Fin}\, [\varnothing \notin x \Rightarrow \exists\, f : x \to \mathbb{V}\ \forall\, y \in x\ f(y) \in y]$.

(Dla każdej rodziny zbiorów skończonych i niepustych istnieje funkcja wyboru – *Axiom of choice for finite sets*).

Fraenkel udowodnił (J. Symb. Log. 2, 1937), że implikacji tej nie da się odwrócić, tj.

$$\neg(\mathrm{ZF} \vdash \mathrm{ACF} \implies \mathrm{OP}) \qquad \text{(por. zadanie 5.64).}$$

W 1939 roku A. Mostowski (Fund. Math. 32, 1939) udowodnił, że $\neg(\mathrm{ZF} \vdash \mathrm{ACF} \implies \mathrm{AC})$.

Również implikacji $\mathrm{OP} \implies \mathrm{AC}$ nie da się w ZF udowodnić; zob. [**Herrlich 06**] lub [**Jech 03**].

7. Zbiór $\mathcal{A}$ nazywamy *induktywnym*, gdy

$$\forall\, \mathcal{B} \subset \mathcal{A}\, (\mathcal{B} - \subset\text{-łańcuch} \Rightarrow \bigcup \mathcal{B} \in \mathcal{A}).$$

Wykazać, że poniższa *zasada maksimum Kuratowskiego*:

(KMP) Każdy zbiór induktywny ma element $\subset$-maksymalny,

jest równoważna aksjomatowi wyboru.

8. Zbiór $\mathcal{A}$ nazywamy *finitarnym* (lub mówimy, że ma *charakter skończony*,gdy

$$\varnothing \in \mathcal{A} \ \wedge\ \forall\, A\, (A \in \mathcal{A} \iff \mathrm{Fin} \cap \mathcal{P}A \subset \mathcal{A}).$$

Wykazać, że:

(i) Zbiór finitarny jest induktywny

(ii) Poniższy *lemat Teichmüllera–Tukey'ego*:

(TTL) Każdy zbiór finitarny ma element $\subset$-maksymalny

jest równoważny aksjomatowi wyboru.

9. Wszystkie definicje skończoności w systemie ZF są równoważne na gruncie ZFC. Udowodnić na przykład (w ZFC), że:

(i) $X \notin \mathrm{Fin} \iff \exists\, f : \mathbb{N} \hookrightarrow X$

(ii) $\mathrm{Fin} = \mathcal{D}$, gdzie $\mathcal{D} = \{x \mid \forall\, y \subset x\ (y \sim x \Rightarrow y = x)\}$ zbiory *skończone w sensie Dedekinda*.

10*. W zadaniu 5.69 określiliśmy (w ZF) klasę $\mathcal{C}$ liczb kardynalnych i funkcję „moc zbioru" $m : \mathbb{V} \twoheadrightarrow \mathcal{C}$ taką, że $X \sim Y \iff m(X) = m(Y)$, a następnie w naturalny sposób porządek (częściowy) w $\mathcal{C}$:

$$a \leqslant b \iff \exists\, X, Y : a = m(X) \wedge b = m(Y) \wedge X \subset Y.$$

Wykazać (w ZF), że:

$$\mathrm{AC} \iff \forall\, a, b \in \mathcal{C} : a \leqslant b \vee b \leqslant a.$$

Warunek spójności relacji $\leqslant$ w klasie $\mathcal{C}$ notuje się też:

$$\forall\, a, b \in \mathcal{C} : a < b \vee a = b \vee a > b$$

i nazywa *warunkiem trichotomii*. Bez użycia liczba kardynalnych można go zapisać:

$$\forall\, X, Y\ (\exists\, f : X \hookrightarrow Y \vee \exists\, g : Y \hookrightarrow X).$$

Wskazówka: w dowodzie implikacji „$\Leftarrow$” wykorzystać poniższy *lemat Hartogsa* (1916):

$$\neg\, \exists\, X\ \forall\, \alpha \in \mathrm{Ord}\ \exists\, f : \alpha \hookrightarrow X.$$

W dowodzie nie wprost lematu Hartogsa rozważyć zbiór $Y = \{(Z, R) \mid Z \subset X,\ R \subset Z^2,\ R$ – dobry porządek w $Z\}$.

11*. Zbiór $\mathcal{F}$ nazywamy *rozproszonym*, gdy

$$\forall\, X, Y \in \mathcal{F} : X \neq Y \ \Rightarrow\ X \cap Y \in \mathrm{Fin}\,.$$

Wykazać, że istnieje nieprzeliczalna i rozproszona rodzina podzbiorów przeliczalnych zbioru $\mathbb{N}$.

Symbolicznie:

$$\exists\, \mathcal{A} \subset \mathcal{P}\mathbb{N}\ [\mathcal{A} \notin \mathrm{Fin} \ \wedge\ A \not\sim \mathbb{N} \ \wedge\ \forall\, A, B \in \mathcal{A}$$
$$(A \sim \mathbb{N} \wedge B \sim \mathbb{N} \wedge (A \neq B \ \Rightarrow\ A \cap B \in \mathrm{Fin}))].$$

Wskazówka:
Po ustaleniu numeracji $p : \mathbb{N}^* \hookrightarrow\!\!\!\!\rightarrow \mathcal{P}$ wziąć rodzinę zbiorów $A_n = \{p_n^k \mid k \in \mathbb{N}^*\}$, $n \in \mathbb{N}^*$.

Komentarz: Wykorzystujący jeden z równoważników aksjomatu wyboru (AC) dowód istnienia takiej rodziny $\mathcal{A} \subset \mathcal{P}\mathbb{N}$ jest – jak mówimy – niekonstruktywny. Nie można „wyobrazić sobie” takiej rodziny podzbiorów zbioru $\mathbb{N}$, podobnie jak dobrego porządku w $\mathcal{P}\mathbb{N}$ (czy w $\mathbb{R}$).

Zderzamy się tutaj z filozoficznym problemem natury prawdy i natury matematyki.

Rozważmy zdania:

(1) $\exists\, R$ – dobry porządek w $\mathcal{P}\mathbb{N}$
(Wniosek z AC).

(2) $\forall\, \mathcal{A} \subset \mathcal{P}\mathbb{N}\ (\mathcal{A} \in \mathrm{Fin} \ \vee\ \mathcal{A} \sim \mathbb{N} \ \vee\ \mathcal{A} \sim \mathcal{P}\mathbb{N})$
(*Hipoteza continuum*. Znak „$\sim$” oznacza równoliczność).

(3) $\forall\, n \in \mathbb{N}\ \exists\, p, q \in \mathbb{P} : 4 + 2n = p + q$
(*Hipoteza Goldbacha*).

(4) $\forall_{\substack{n \in \mathbb{N} \\ n \geqslant 2}}\ \exists\, k \in \mathbb{N} : \overset{n}{g}(k) = 0$, gdzie $\overset{n}{g} : \mathbb{N} \to \mathbb{N}$ jest ciągiem Goodsteina o początku n
(*Twierdzenie Goodsteina* – zadanie 5.38*).

(5) Teoria PA jest niesprzeczna (i podobnie dla ZFC, ZF, ZF_0 itp.).

Zdanie (1) jest twierdzeniem ZFC. Zdanie (4) jest twierdzeniem ZF. Zdanie (2) jest niezależne od ZF (Gödel 1940 – Cohen 1963).

Zdanie (3) jest „prawdopodobnie" prawdziwe, ale dotychczas tego nie udowodniono. Zdanie (4) jest twierdzeniem ZF, ale nie jest twierdzeniem arytmetyki Peana, PA (Paris–Kirby 1994).

Zdanie (5) jest intuicyjnie prawdziwe. Dowód?

Widzimy, że status zdania (3) jest istotnie różny od statusu zdania (2). Zdanie (3) jest prawdziwe lub fałszywe – nie wiadomo. O zdaniu (2) nie można tego powiedzieć. Co to jest „dowolny podzbiór zbioru liczb naturalnych"? $\mathcal{P}\mathbb{N} = ?$

Matematyka to coś więcej niż systemy aksjomatyczne i dedukcja w ich ramach.

12*. Wykazać, że każda permutacja zbioru X jest złożeniem dwu inwolucji.

Symbolicznie

$$\forall f : X \hookrightarrow\!\!\!\!\rightarrow X \; \exists g, h : X \to X \; (g \circ g = h \circ h = \mathrm{id}_X \wedge f = h \circ g).$$

Wskazówka: Wystarczy wykazać, że istnieje taka inwolucja g zbioru X, iż $f \circ g$ jest też inwolucją. Należy przejść do funkcji częściowych i zastosować lemat Zorna.

13*. Wykazać, że poset w którym wszystkie łańcuchy i antyłańcuchy są skończone, jest skończony.

Wskazówka: Prowadząc dowód nie wprost wykazać wpierw, że nad każdym elementem danego posetu znajduje się element maksymalny.

6.3. Odpowiedzi

1. (ZL)$\Rightarrow$(HMP). Uporządkowany przez inkluzję zbiór łańcuchów w X zawierających dany łańcuch spełnia założenia lematu Zorna, a więc istnieje w nim element maksymalny.

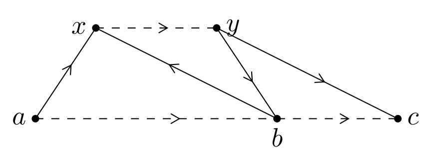
(HMP$'$)$\Rightarrow$(ZL) Przypuśćmy, że w spełniającym założenia lematu Zorna posecie X nie istnieje element maksymalny. $\exists)\, B$ – łańcuch maksymalny w X, $\exists)\, x \in M(B) =$ majoranty B w X, $\exists)\, y \in X : x < y$; wówczas $B \subsetneq B \cup \{y\}$ – łańcuch w X $\lightning$.

2.

(i) Zbiór $\mathcal{R}$ wszystkich porządków w X zawierających dany porządek R spełnia założenia lematu Zorna. $\langle$Dla łańcucha $\varnothing \neq \mathcal{C} \subset R$ majorantą jest $\bigcup \mathcal{C}$; dla łańcucha $\varnothing$ majorantą jest $R\rangle$, a więc istnieje w $\mathcal{R}$ element maksymalny.

(ii) Inkluzja $L(X) \subset M(X)$ jest oczywista.

HP: $L(X) \subsetneq M(X)$. $\exists)\, R \in M(X) \setminus L(X)$. $\exists)\, x, y \in X : (x, y), (y, x) \notin R$



Niech $R' = R \cup \{(a, b) \mid (a, x), (y, b) \in R\}$;

wówczas $R' \in F(X)$ $\quad\langle$Sprawdzamy warunki definicji porządku:

1) Zwrotność zachodzi, gdyż $R \subset R'$.

2) Przechodniość. HP: $\exists)\, a, b, c \in X : (a, b), (b, c) \in R', (a, c) \notin R'$. Możliwe są trzy przypadki:

2.1) $(a, b) \notin R$, $(b, c) \in R$.
Wówczas $(a, x), (y, b) \in R$, a więc $(y, c) \in R$, $(a, c) \in R'$ ↯.

2.2) $(a, b) \in R$, $(b, c) \notin R$.
Wówczas $(b, x), (y, c) \in R$, a więc $(a, x) \in R$, $(a, c) \in R'$ ↯.

2.3) $(a, b), (b, c) \notin R$.
Wówczas $(a, x), (y, b), (b, x), (y, c) \in R$, a więc $(y, x) \in R$ ↯.

3) Antysymetria. HP: $\exists)\, a, b \in X : (a, b), (b, a) \in R'$, $a \neq b$.
Analogicznie jak w punkcie 2) rozpatrujemy trzy przypadki dla par (a, b) i (b, a) – za każdym razem dochodzimy do sprzeczności$\rangle$.

Ponieważ $(x, y) \in R' \quad \langle (x, x), (y, y) \in R \rangle$, więc $R \subsetneq R'$ ↯.

(iii) Natychmiastowy wniosek z (i) i (ii).

3.

(a) Określamy $f : \mathcal{P}I_n \hookrightarrow \mathbb{N}$, kładąc dla $A \subset I_n$, $k = \mathrm{ord}_A$:

$$f(A) = \sum_{i<k} (n+1)^{n-i-1} \cdot \mathrm{nat}_A(k - i - 1),$$

a następnie dla $A, B \subset I_n$:

$$A \leqslant B \ :\Longleftrightarrow\ f(A) \leqslant f(B).$$

(Można by ten porządek nazwać *leksykograficznym*).

W przypadku, gdy $n = 3$:

$$\begin{tikzcd}
 & \varnothing \arrow[dl] \arrow[d, dashed] \arrow[dr, dashed] & \\
\{1\} \arrow[r] \arrow[d, dashed] \arrow[dr, dashed] & \{2\} \arrow[r, dashed] \arrow[dl] \arrow[dr, dashed] & \{3\} \arrow[d, dashed] \arrow[dl] \\
\{1,2\} \arrow[urr] \arrow[r, dashed] \arrow[dr, dashed] & \{1,3\} \arrow[r] \arrow[d, dashed] & \{2,3\} \arrow[dl] \\
 & \{1,2,3\} &
\end{tikzcd}$$

(b) Oznaczając przez R_n porządek w $\mathcal{P}I_n$ określony w punkcie (a), kładziemy:

$$R = \bigcup_{n \in \mathbb{N}} R_n.$$

Sprawdzenie, że R jest dobrym porządkiem typu $\mathbb{N}$ w zbiorze $\mathcal{P}\mathbb{N}^* \cap \mathrm{Fin}$, nie nastręcza trudności.

Szesnaście pierwszych wyrazów ciągu E:

k	0	1	2	3	4	5	6	7	8
E_k	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$	$\{3\}$	$\{1,3\}$	$\{2,3\}$	$\{1,2,3\}$	$\{4\}$

9	10	11	12	13	14	15	16
$\{1,4\}$	$\{2,4\}$	$\{3,4\}$	$\{1,2,4\}$	$\{1,3,4\}$	$\{2,3,4\}$	$\{1,2,3,4\}$	$\{5\}$

Porządek R jest rozszerzeniem relacji inkluzji w $\mathcal{P}\mathbb{N}^* \cap \mathrm{Fin}$;

$$\forall\, i,j \in \mathbb{N} : E_i \subset E_j \;\Rightarrow\; i \leqslant j.$$

Ponadto, dla $n \in \mathbb{N}$: $E_{2^n-1} = I_n$, $E_{2^n} = \{n+1\}$, $\{E_0,\dots,E_{2^n-1}\} = \mathcal{P}I_n$.

Łatwo widać, że porządek R jest identyczny z dokładnością do przesunięcia $n \mapsto n+1$ z porządkiem z zadania 5.66*.

4. Natychmiast widać, że tak określona relacja jest porządkiem (częściowym) w $\mathcal{A}$.

Poset $(\mathcal{A},\leqslant)$ spełnia założenia lematu Zorna, gdyż majorantą łańcucha $\mathcal{B} \subset \mathcal{A}$ jest $C := \bigcup\mathcal{B}$ $(\in \mathcal{A})$. $\langle$Łatwo widać, że R jest porządkiem liniowym w C. Należy jeszcze wykazać, że w każdym $\varnothing \neq Z \subset C$ istnieje R-minimum.
$\exists)\, z \in Z$. $\exists)\, A \in \mathcal{B} : z \in A$. $\varnothing \neq Z \cap A \subset A$. $\exists)\, x$ – R-minimum $Z \cap A$.
Wówczas x – R-minimum Z $\langle$HP: $\exists)\, y \in Z : y \underset{R}{<} x$. $y \in C$. $\exists)\, B \in \mathcal{B} : y \in B$.
Dwa przypadki:
(i) $A \leqslant B$. Ponieważ $x \in A$, więc $y \in A$, $y \in Z \cap A$ $\lightning$.
(ii) $B < A$. Wówczas $B \subset A$, $y \in A$, $y \in Z \cap A$ $\lightning$.$\rangle\rangle$.

Zatem $\exists)\, Y$ – element $\leqslant$-maksymalny $\mathcal{A}$. Zbiór Y jest współkońcowy z X.
$\langle$HP: $\exists)\, x \in X \forall\, y \in Y : y < x$; wówczas $Y < Y \cup \{x\} \in \mathcal{A}$ $\lightning\rangle$.

5.
(a) Indukcja na $n = |X|$
I. $n = 0$, OK.
II. $n \geqslant 1$, OK dla $n-1$.
HP: $\exists\, X, R)$ $X \in \mathrm{Fin}$, $|X| = n$, $R \in L(X) \setminus W(X)$. $\exists)\, a$ – R-maksimum w X $\langle$zob. zadanie 5.63$\rangle$.
Dla $Y = X \setminus \{a\} : W(Y) = L(Y)$, a więc $R \cap Y^2 \in W(Y)$. Ponieważ $R \notin W(X)$, więc $\exists)\, \varnothing \neq Z \subset X\ \forall\, z \in Z\ \exists\, t \in Z : t < z$ (tzn. $t \underset{R}{<} z$ itd.).
$Z \neq \{a\}$. $Z \setminus \{a\} \subset Y$. $\exists)\, z$ – R-minimum $Z \setminus \{a\}$.
Ponieważ $z \in Z$, więc $\exists)\, t \in Z : t < z$. $t \neq a$ $\langle t = a \;\Rightarrow\; a < z \leqslant a$ $\lightning\rangle$, a więc $t \in Z \setminus \{a\}$, czyli $z \leqslant t$ $\lightning$.
(b) Na przykład $(\mathbb{N},\geqslant)$.

6. HP: OP $\wedge$ $\neg$ ACF
$\exists)\, x \subset \mathrm{Fin} : \varnothing \notin x \;\wedge\; \neg\,\exists\, f$ – funkcja wyboru dla x.
Według OP $\exists)\, R \in L(\bigcup x)$.
$\forall\, y \in x : y \in \mathrm{Fin}$, a więc $L(y) = W(y)$.
Możemy teraz określić funkcję wyboru $f : x \to \bigcup x$, kładąc dla $y \in x$: $f(y) = R$-minimum y.

7. ZL $\Rightarrow$ KMP

Poset $(\mathcal{A}, \subset)$ spełnia założenia lematu Zorna, a więc istnieje w nim element maksymalny.

KMP $\Rightarrow$ AC.

Dla zbioru x o elementach niepustych ($\varnothing \notin x$) rodzina $\mathcal{A}$ częściowych funkcji wyboru

$$(\mathcal{A} = \{f : x \multimap \bigcup x \mid \forall\, y \in \operatorname{Dom} f : f(y) \in y\})$$

jest induktywna, a więc istnieje w niej element maksymalny τ. Gdyby $\operatorname{Dom} \tau \subsetneq x$, to $\exists)\, y \in x \setminus \operatorname{Dom} \tau$, i wówczas $\exists)\, z \in y$, $\tau \subsetneq \tau \cup \{y \mapsto z\} \in \mathcal{A}$ ↯.

8.

(i) HP: $\exists)\, \mathcal{A}$ – finitarny, $\mathcal{B} \subset \mathcal{A}$
$\forall\, B, C \in \mathcal{B}\ (B \subset C \vee C \subset B)$ i $A = \bigcup \mathcal{B} \notin \mathcal{A}$.
Dla $E \in \mathrm{Fin} \cap \mathcal{P}A$ indukcją na $n = |E|$ dowodzimy, że $\exists)\, B \in \mathcal{B} : E \subset B$; ponieważ $B \in \mathcal{A}$, więc $E \in \mathcal{A}$. Zatem $\mathrm{Fin} \cap \mathcal{P}A \subset \mathcal{A}$, skąd $A \in \mathcal{A}$ ↯.

(ii) AC $\Rightarrow$ TTL. Wniosek z (i) i twierdzenia z zadania 7.

TTL $\Rightarrow$ AC.
Dla zbioru x o elementach niepustych rodzina $\mathcal{A}$ częściowych funkcji wyboru jest finitarna, a więc ma element maksymalny $\tau : x \to \bigcup x$.

9.

(i) Należy udowodnić implikację „$\Rightarrow$”
$\exists)\, \alpha \in \mathrm{Ord}$, $f : \alpha \hookrightarrow\!\!\!\rightarrow X$; wówczas $\omega \leqslant \alpha$, a więc $f|\omega : \omega \hookrightarrow X$.

(ii) Należy udowodnić inkluzję $\mathcal{D} \subset \mathrm{Fin}$.
HP: $\exists)\, X \in \mathcal{D} \setminus \mathrm{Fin}$. Według (i) $\exists)\, f : \mathbb{N} \hookrightarrow X$. Określamy $g : X \hookrightarrow X$,

$$g(x) = \begin{cases} x, & \text{gdy } x \notin \operatorname{Im} f \\ f(n+1), & \text{gdy } x = f(n) \in \operatorname{Im} f \end{cases},$$

wówczas $X \sim X \setminus \{f(0)\} \subsetneq X$, a więc $X \notin \mathcal{D}$ ↯.

10*. $\Rightarrow$) $\exists)\, X, Y : a = m(X), b = m(Y)$. $\exists)\, \alpha, \beta \in \mathrm{Ord}, f : \alpha \hookrightarrow\!\!\!\rightarrow X$, $g : \beta \hookrightarrow\!\!\!\rightarrow Y$. Jeśli np. $\alpha \leqslant \beta$, to $g \circ f^{-1} : X \hookrightarrow Y$, a więc $a \leqslant b$.
$\Leftarrow$)

(1°) Dowód lematu Hartogsa (w ZF): HP: $\exists\, X\ \forall\, \alpha \in \mathrm{Ord}\ \exists\, f : \alpha \hookrightarrow X$. Weźmy zbiór Y jak we wskazówce. Określamy funkcję $g : Y \to \mathrm{Ord}$, $g((Z, R)) = \mathrm{ord}(Z, R)$. Wówczas $\alpha = \operatorname{Im} g \in \mathrm{Ord}$. $\langle$Należy udowodnić tranzytywność zbioru α. Jeżeli $\gamma \in \beta \in \alpha$, to $\exists)\, (Z, R) \in Y : \beta = \mathrm{ord}(Z, R)$, i wówczas $h = \mathrm{nat}_{Z,R} : \beta \hookrightarrow\!\!\!\rightarrow Z$, h – $\mathbb{E}$-R-rosnąca, a więc $Z' = \mathrm{Im}(h|\gamma) \subset Z$, i dla $R' = \{(h(\xi), h(\eta)) \mid \xi < \eta < \gamma\}$ $(Z', R') \in Y$, $\gamma = \mathrm{ord}(Z', R') \in \alpha\rangle$.
Teraz $\exists)\, f : \alpha \hookrightarrow X$, a więc $\exists)\, (Z, R) \in Y$: $\alpha = \mathrm{ord}(Z, R) = g(Z, R)$, czyli $\alpha \in \alpha$ ↯.

(2°) Dowód implikacji:
HP: $\exists\, X)\ \neg\, \exists\, R$ – dobry porządek w X.

Wówczas $\forall\,\alpha \in \mathrm{Ord}\,\neg\,\exists\, f : X \hookrightarrow \alpha$, a więc $\forall\,\alpha \in \mathrm{Ord}\ \exists\, f : \alpha \hookrightarrow X$ w sprzeczności z lematem Hartogsa.

11*. Ustalmy bijekcję

$$p = \{1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 5, \dots\} : \mathbb{N}^* \hookrightarrow\!\!\!\!\to \mathbb{P}$$

i niech dla $n \in \mathbb{N}^*$: $A_n := \{p_n^k \mid k \in \mathbb{N}^*\}$; $A_1 = \{2, 4, 8, \dots\}$, $A_2 = \{3, 9, 27, \dots\}$, $\dots$ Niech $A_0 := \mathbb{N} \setminus (A_1 \cup A_2 \cup A_3 \cup \dots\}$. Rodzina $\mathcal{A} = \{A_n \mid n \in \mathbb{N}\} \subset \mathcal{P}\mathbb{N}$ jest przeliczalna, rozproszona i jej elementy są przeliczalne.

Na mocy zasady maksimum Kuratowskiego (KMP, zadanie 7) istnieje maksymalna rodzina rozproszona o elementach przeliczalnych $\mathcal{A} \subset \mathcal{B} \subset \mathcal{P}\mathbb{N}$.
Rodzina $\mathcal{B}$ jest nieprzeliczalna, $\mathcal{B} \not\sim \mathbb{N}$.
$\langle$HP: $\mathcal{B} \sim \mathbb{N}$. $\exists)\, B : \mathbb{N} \hookrightarrow\!\!\!\!\to \mathcal{B}$. $\exists)\, x : \mathbb{N} \hookrightarrow \mathbb{N}\ \forall n \in \mathbb{N} : x_n \in B_n \setminus \bigcup\limits_{k<n} (B_k \cap B_n)$.

Niech $X = \{x_n \mid n \in \mathbb{N}\}$. Wówczas $X \sim \mathbb{N}$ i $\forall n \in \mathbb{N} : X \cap B_n \in \mathrm{Fin}$. $\langle X \cap B_n \subset \bigcup\limits_{k<n} (B_k \cap B_n) \cup \{x_n\} \in \mathrm{Fin}\rangle$. Zatem rodzina $\mathcal{B} \cup \{X\}$ jest rozproszona, jej elementy są przeliczalne i $\mathcal{B} \subsetneq \mathcal{B} \cup \{X\}$ ↯$\rangle$.

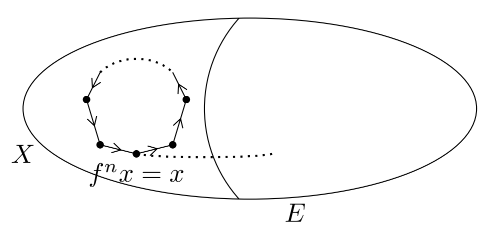
12*. Dla dowolnych f, X oznaczmy

$$f : X \xrightarrow{\mathrm{inv}} X \ :\Longleftrightarrow\ f : X \to X \quad \wedge \quad f \circ f = \mathrm{id}_X\,.$$

Oczywiście $f : X \xrightarrow{\mathrm{inv}} X \implies f : X \hookrightarrow\!\!\!\!\to X \wedge f^{-1} = f$. Niech $f : X \hookrightarrow\!\!\!\!\to X$. Oznaczmy:

$$G = \{g : X \multimap\!\!\to X \mid g, f \circ g : \mathrm{Dom}\, g \xrightarrow{\mathrm{inv}} \mathrm{Dom}\, g\}.$$

Poset $(G, \subset)$ spełnia założenia lematu Zorna $\langle \forall\, C \subset G$: C – łańcuch $\Rightarrow \bigcup C \in G\rangle$, a więc $\exists\, g)$ g – element maksymalny G. Wówczas $\mathrm{Dom}\, g = X$. $\langle$HP: $\mathrm{Dom}\, g = E \subsetneq X$. $\exists)\, x \in X \setminus E$.



Wówczas $fx = f(x) \in X \setminus E$ $\langle$HP: $fx \in E$. Ponieważ $f \circ g : E \xrightarrow{\mathrm{inv}} E$, więc $\exists)\, t \in E : fx = fg\,t$, skąd $x = g\,t \in E$ ↯$\rangle$.
Również $f^{-1}x \in X \setminus E$ $\langle$HP: $t = f^{-1}x \in E$. $\exists)\, s \in E : t = g\,s$, a więc $E \ni fg\,s = ft = ff^{-1}x = x$ ↯$\rangle$.
Zatem $D = \{f^n x, f^{-n} x \mid x \in \mathbb{N}\} \subset X \setminus E$, gdzie $f^n = \underbrace{f \circ \dots \circ f}_{n}$, $f^{-n} = (f^{-1})^n$ $\langle$Indukcja na $n\rangle$.
$\exists n \in \mathbb{N}^* : f^n x = x$ $\langle$HP: $\forall n \in \mathbb{N}^* : f^n x \neq x$. Wówczas dla $E' = E \cup D$,

$g' = g \cup \{f^n x \mapsto f^{-n}x, f^{-n}x \mapsto f^n x \mid n \in \mathbb{N}\}$. $g' : E' \xrightarrow{\text{inv}} E'$, $f \circ g' : E' \xrightarrow{\text{inv}} E'$ oraz $g \subsetneq g'$ ↯⟩.

$\exists) \, n \in \mathbb{N}^*$ najmniejsze takie, że $f^n x = x$. $D = \{x, fx, f^2x, \ldots, f^{n-1}x\}$.
Dla $E' = E \cup D$, $g' = g \cup \{x \mapsto f^{n-1}x, fx \mapsto f^{n-2}x, \ldots, f^{n-1}x \mapsto x\} = g \cup \{f^{k-1}x \mapsto f^{n-k}x \mid k \in I_n\} : E' \to E'$ będziemy mieli: $g' : E' \xrightarrow{\text{inv}} E'$, $f \circ g' : E' \xrightarrow{\text{inv}} E'$ oraz $g \subsetneq g'$ ↯⟩.

Tak więc g, $f \circ g : X \xrightarrow{\text{inv}} X$.

13*. Dla dowolnego posetu P oznaczmy przez $M(P)$ ogół elementów maksymalnych w P;

$$M(P) = \{a \in P \mid \forall\, p \in P : \neg\, a < p\}.$$

Przypuśćmy, że P jest posetem nieskończonym, w którym wszystkie łańcuchy i antyłańcuchy są skończone.

Wówczas $M(P) \in \text{Fin}$ $\quad\langle M(P)$ jest antyłańcuchem⟩.

$$(*) \qquad \forall\, x \in P \;\exists\, a \in M(P) : x \leqslant a.$$

⟨HP: $\exists) \, p \in P \; \forall\, a \in M(P) : \neg\, p \leqslant a$. Każdy niepusty łańcuch w posecie $X = [p, \cdot\,] = \{x \in X \mid p \leqslant x\}$ jest skończony, a więc ma element największy, który jest jego majorantą. Ponadto $X \neq \varnothing$ $\quad\langle p \in X\rangle$.

Zatem, na mocy tematu Zorna w posecie X istnieje element maksymalny a, i wówczas $a \in M(P)$; $p \leqslant a$ ↯⟩.
Z (*) wynika, że $P = \bigcup_{a \in M(P)} F(a)$, gdzie dla $a \in P$:

$$F(a) = [\,\cdot\,, a] = \{x \in P \mid x \leqslant a\}.$$

Wówczas
$\exists) \, a_0 \in M(P) : F(a_0) \notin \text{Fin}$, a więc również $F^*(a_0) = F(a_0) \setminus \{a_0\} = [\cdot, a_0) \in \text{Fin}$.

Powtarzając tę procedurę otrzymamy element $a_1 < a_0 \in M(F^*(a_0))$ itd.; a więc, korzystając z aksjomatu wyboru, otrzymamy w posecie P zbiór $a_0 > a_1 > a_2 > \ldots$, który jest łańcuchem nieskończonym $\quad$⟨nie ma w nim elementu najmniejszego⟩ ↯.

7

Liczby kardynalne

7.1. Wstęp

Na mocy aksjomatu wyboru każdy zbiór jest równoliczny z jakąś liczbą porządkową. Możemy więc określić funkcję card : $\mathbb{V} \to$ Ord, $\operatorname{card} x = |x| = \min\{\alpha \in \text{Ord} \mid x \sim \alpha\}$; liczbę $|x|$ nazywamy *mocą* lub *liczbą kardynalną* zbioru x. Oznaczmy Card := Im(card), jest to klasa wszystkich liczb kardynalnych.

Z powyższych definicji natychmiast wynika, że

(1) $\forall\, x, y : x \sim y \iff |x| = |y|$

(2) $\forall\, \alpha \in \text{Ord} : |\alpha| \leqslant \alpha \wedge (|\alpha| = \alpha \Leftrightarrow \alpha \in \text{Card})$

(3) $\mathbb{N} = \omega \subset \text{Card} \subset \text{Ord}$ $\quad\langle$gdyż $\forall\, m, n \in \mathbb{N} : m \sim n \Leftrightarrow m = n\rangle$.

Tak więc rozszerzyliśmy pojęcie mocy zbioru skończonego (rozdział 5) na dowolne zbiory.

Twierdzenie o monotoniczności:

(4) $\forall\, x, y : x \subset y \;\Rightarrow\; |x| \leqslant |y|$

$\langle$Dowód wystarczy przeprowadzić w przypadku, gdy $y = \beta \in \text{Card}$; wówczas $|x| \leqslant \operatorname{ord} x \leqslant \beta = |y|\rangle$.

Twierdzenie Cantora–Bernsteina:

(5) $x \sim y' \subset y \;\wedge\; y \sim x' \subset x \implies x \sim y$

jest natychmiastowym wnioskiem z (4) $\quad\langle |x| = |y'| \leqslant |y| = |x'| \leqslant |x| \rangle$.

Innym ważnym wnioskiem z (4) jest twierdzenie o kardynalności kresu górnego zbioru liczb kardynalnych:

(6) $\forall\, z \subset \text{Card} : \sup z = \bigcup z \in \text{Card}$

$\langle \sigma := \sup z = \bigcup z$. HP: $\sigma \notin \text{Card}$. Zatem $|\sigma| < \sigma$. $\exists)\, \alpha \in z : |\sigma| < \alpha$. Wówczas $\alpha \subset \sigma$, więc $\alpha = |\alpha| \leqslant |\sigma|$ ↯$\rangle$.

Drugim podstawowym twierdzeniem o liczbach kardynalnych jest *twierdzenie Cantora*:

(7) $\forall\, x : |x| < |\mathcal{P}x|$

$\langle |x| \leqslant |\mathcal{P}x|$, gdyż $\{t \mapsto \{t\} \mid t \in x\} : x \hookrightarrow \mathcal{P}x$. HP: $|x| = |\mathcal{P}x|$. Wówczas $\exists)\, f : x \longrightarrow\!\!\!\!\rightarrow \mathcal{P}x$, a więc $\exists)\, s \in X : f(s) = \{t \in x \mid t \notin f(t)\}$, $\forall\, t \in x : t \in f(s) \Leftrightarrow t \notin f(t)$, w szczególności $s \in f(s) \Leftrightarrow s \notin f(s)$ ↯$\rangle$.

Działania *arytmetyki kardynalnej*: *dodawanie*, *mnożenie* i *potęgowanie*: $\widetilde{+}$, $\widetilde{\cdot}$ i $\widetilde{\wedge}$: $\mathrm{Card}^2 \to \mathrm{Card}$ określamy w sposób naturalny, przy czym tyldę ($\widetilde{\ }$) odróżniającą je od odpowiednich działań arytmetyki porządkowej będziemy na ogół opuszczali, zdając się na kontekst. Dla $\alpha, \beta \in \mathrm{Card}$ kładziemy:

$$(8)\quad \begin{cases} \alpha + \beta := |(\alpha \times \{0\}) \cup (\beta \times \{1\})| \\ \alpha \cdot \beta = \alpha\beta := |\alpha \times \beta| \\ \alpha^\wedge \beta = \alpha^\beta := |\operatorname{Map}(\beta, \alpha)|. \end{cases}$$

Elementarne prawa arytmetyki kardynalnej różnią się od praw arytmetyki porządkowej. Mnożenie i dodawanie są łączne i przemienne. Mnożenie jest rozdzielne względem dodawania. Potęgowanie spełnia trzy standardowe prawa:

(9) $\forall\, \alpha, \beta, \gamma \in \mathrm{Card} : \alpha^\beta \alpha^\gamma = \alpha^{\beta+\gamma},\ \alpha^\gamma \beta^\gamma = (\alpha\beta)^\gamma,\ (\alpha^\beta)^\gamma = \alpha^{\beta\gamma}.$

Prawa monotoniczności zachodzą w wersji słabej, $\alpha \leqslant \beta \ \Rightarrow\ \alpha + \gamma \leqslant \beta + \gamma$, itp.

Jedynym elementarnym prawem, w którym występuje nierówność silna, jest *nierówność Cantora*:

(10) $\forall\, \alpha \in \mathrm{Card} : \alpha < 2^\alpha$.

Jest to wniosek z (7) i faktu, że:

(11) $\forall\, A : \chi_A = \{X \mapsto (X \times \{1\}) \cup ((A \setminus X) \times \{0\}) \mid X \subset A\} : \mathcal{P}A \hookrightarrow\!\!\!\!\rightarrow \operatorname{Map}(A, 2)$; dla $X \subset A$ funkcję $\chi_{A,X} = \chi_A(X) : A \to 2$ nazywamy *funkcją charakterystyczną* zbioru X (jako podzbioru zbioru A).

Dowody elementarnych praw arytmetyki kardynalnej są mechaniczne i sprowadzają się do wskazania odpowiedniej bijekcji lub injekcji. Obszerniejszy przegląd tych praw znajdziemy w zadaniu 1.

Według (10):

(12) $\forall\, \alpha \in \mathrm{Ord} : \alpha < 2^{|\alpha|} \in \mathrm{Card}$

$\langle$HP: $2^{|\alpha|} \leqslant \alpha$. Wówczas $2^{|\alpha|} \subset \alpha$, a więc $2^{|\alpha|} \leqslant |\alpha| < 2^{|\alpha|}$ $\lightning\rangle$.

Wynika stąd że $\mathrm{Ord} = \bigcup \mathrm{Card}$, a więc klasa Card wszystkich liczb kardynalnych jest właściwa (nie jest zbiorem).

(13) $\mathrm{Card} \notin \mathbb{V}$.

Indukcyjnie łatwo pokazać, że w zakresie liczb naturalnych arytmetyka kardynalna pokrywa się z arytmetyką porządkową:

(14) $\forall\, n, k \in \omega : n \,\widetilde{+}\, k = n + k,\ n \,\widetilde{\cdot}\, k = n \cdot k,\ n \widetilde{\wedge} k = n^\wedge k = n^k$.

Według (13) $\mathrm{Card}\setminus\omega \notin \mathbb{V}$, a więc $\operatorname{ord}(\mathrm{Card}\setminus\omega) = \mathrm{Ord}$; naturalną numerację klasy $\mathrm{Card}\setminus\omega$ oznaczamy za Cantorem literą hebrajską *alef*: $\aleph := \mathrm{nat}_{\mathrm{Card}\setminus\omega}$.

Funkcja alef jest w pełni określona warunkiem:

(15) $\aleph : \mathrm{Ord} \hookrightarrow\!\!\!\!\rightarrow \mathrm{Card}\setminus\omega \ \ \wedge\ \ \forall\, \alpha, \beta \in \mathrm{Ord}(\alpha < \beta \ \Rightarrow\ \aleph_\alpha < \aleph_\beta)$.

Tak więc $\aleph_0 = \omega < \aleph_1 < \aleph_2 < \ldots < \aleph_\omega < \aleph_{\omega+1} < \ldots$; liczby kardynalne nieskończone, czyli elementy klasy $\mathrm{Card}\setminus\omega$ nazywamy zwyczajowo *alefami*; o funkcji $\aleph$ mówimy też, że jest *skalą alefów*.

Według (10) $\forall\,\alpha \in \mathrm{Ord} : \aleph_\alpha < 2^{\aleph_\alpha}$, a więc $\aleph_{\alpha+1} \leqslant 2^{\aleph_\alpha}$, w szczególności $\aleph_1 \leqslant 2^{\aleph_0}$.
Łatwo widać, że dla $\lambda \in \mathrm{Lim} : \aleph_\lambda = \sup\limits_{\alpha<\lambda} \aleph_\alpha = \bigcup\limits_{\alpha<\lambda} \aleph_\alpha$ (por. zadanie 7).

Liczbę $2^{\aleph_0}$ nazywamy *continuum* (gdyż jest to nie tylko moc zbioru $\mathcal{P}\mathbb{N}$, lecz także – jak się później okaże – moc zbioru $\mathbb{R}$ wszystkich liczb rzeczywistych) i oznaczamy zwyczajowo literą $\mathfrak{c}$ (gotyckie c). *Hipoteza continuum*, w skrócie CH, to zdanie $\mathfrak{c} = \aleph_1$. Jej uogólnieniem jest zdanie $\forall\,\alpha \in \mathrm{Ord} : 2^{\aleph_\alpha} = \aleph_{\alpha+1}$ oznaczane jako GCH (*Generalized Continuum Hypothesis*).

Zdania CH i GCH są niezależne od ZFC (K. Gödel 1940, P. Cohen 1963). Udowodnienie tego faktu jest ważnym osiągnięciem matematyki XX wieku – potwierdza intuicję względności i nieokreśloności pojęcia nieskończoności aktualnej ($\mathcal{P}\mathbb{N} = ?$).

Arytmetyka alefów jest trywialna w zakresie dodawania i mnożenia – sprowadza się do ich porównywania:

(16) $\alpha, \beta \in \mathrm{Card},\ \beta \geqslant \omega,\ \alpha \leqslant \beta \implies (\alpha + \beta = \beta,\ \alpha \neq 0 \ \Rightarrow\ \alpha \cdot \beta = \beta)$
(G. Hessenberg, 1906).

Twierdzenie (16) jest natychmiastowym wnioskiem z lematu: $\forall\,\alpha \in \mathrm{Card}\backslash\omega : \alpha^2 = \alpha$.

W dowodzie lematu wykorzystujemy relację R w klasie $\mathrm{Ord}^2 = \mathrm{Ord} \times \mathrm{Ord}$ określoną wzorem:

$$(\alpha,\beta)\,R\,(\gamma,\delta) \;:\!\iff\; \alpha \cup \beta < \gamma \cup \delta \ \vee\ [\alpha \cup \beta = \gamma \cup \delta \wedge (\alpha < \gamma \vee (\alpha = \gamma \wedge \beta \leqslant \delta))],$$

która jest dobrym porządkiem w Ord^2 na mocy kryterium Tarskiego (zadanie 3.(a)).

$\langle$Dowód lematu prowadzimy nie wprost. Przypuśćmy, że $\alpha \in \mathrm{Card}\backslash\omega$ jest najmniejszym alefem, dla którego $\alpha < \alpha^2$.
Niech $\beta = \mathrm{ord}(\alpha \times \alpha, R)$, $f = \mathrm{nat}_{\alpha\times\alpha,R}$. Tak więc $\beta \in \mathrm{Ord}$, $f : \beta \lhook\joinrel\twoheadrightarrow \alpha \times \alpha$, $\forall\,\xi < \eta < \beta : f(\xi) R f(\eta)$.
Jest $\alpha < \beta$ $\quad\langle$HP: $\beta \leqslant \alpha$. Wówczas $\alpha^2 = |\beta| \leqslant \beta \leqslant \alpha < \alpha^2$ ↯$\rangle$.
Oznaczmy $(\gamma,\delta) = f(\alpha)$
Wówczas $f|\alpha : \alpha \lhook\joinrel\twoheadrightarrow S_{(\gamma,\delta)} = S_{(\gamma,\delta)}(\mathrm{Ord}, R) = \{(\xi,\eta) \in \mathrm{Ord}^2 \mid (\xi,\eta) < (\gamma,\delta)\}$.
Jeśli $(\xi,\eta) \in S_{(\gamma,\delta)}$, to $\xi \leqslant \xi \cup \eta \leqslant \gamma \cup \delta < \varepsilon := (\gamma \cup \delta) + 1 < \alpha$ $\quad\langle$gdyż $\alpha \in \mathrm{Card}\backslash\omega \subset \mathrm{Lim}$ – zadanie 2$\rangle$, i analogicznie $\eta < \alpha$. Zatem $S_{(\gamma,\delta)} \subset \varepsilon \times \varepsilon$, $f|\alpha : \alpha \lhook\joinrel\longrightarrow \varepsilon \times \varepsilon$, $\alpha \leqslant |\varepsilon|^2$, $\omega \leqslant |\varepsilon| \leqslant \varepsilon < \alpha$, czyli $\alpha \leqslant |\varepsilon|^2 = |\varepsilon| < \alpha$ ↯$\rangle$.

Arytmetyka alefów w zakresie potęgowania nie jest trywialna. Z (16) wynika jedynie nieistotność nietrywialnej (tj. $\geqslant 2$) podstawy, jeżeli tylko nie przekracza ona nieskończonego wykładnika, czyli:

(17) $\alpha, \beta \in \mathrm{Card},\ 2 \leqslant \alpha \leqslant \beta,\ \omega \leqslant \beta \implies \alpha^\beta = 2^\beta$.

$\langle\alpha < 2^\alpha$, a więc $\alpha^\beta \leqslant 2^{\alpha\beta} = 2^\beta \leqslant \alpha^\beta\rangle$ (por. zadanie 4).

Na przykład $2^\omega = \mathfrak{c} = \omega^\omega$, $2^\mathfrak{c} = \omega^\mathfrak{c} = \mathfrak{c}^\mathfrak{c}$. Natomiast $\mathfrak{c}^\omega = (2^\omega)^\omega = 2^{\omega^2} = 2^\omega = \mathfrak{c}$.

Suma i *iloczyn* rodziny $f : I \to \mathrm{Card}$, $I \in \mathbb{V}$, liczb kardynalnych określamy w naturalny sposób:

$$\tilde{\sum} f = \tilde{\sum_{i\in I}} f(i) := \Big|\bigsqcup f\Big|, \qquad \tilde{\prod} f = \tilde{\prod_{i\in I}} f(i) := \Big|\prod f\Big|,$$

gdzie dla dowolnej rodziny zbiorów $A : I \to \mathbb{V}$

$$\bigsqcup A = \bigsqcup_{i\in I} A_i := \bigcup_{i\in I} A_i \times \{i\} \qquad (\textit{suma kartezjańska}),$$
$$\prod A = \prod_{i\in I} A_i := \{x : I \to \bigcup_{i\in I} A_i \mid \forall\, i \in I : x_i \in A_i\} \qquad (\textit{iloczyn kartezjański}).$$

Tak jak poprzednio odróżniającą tyldę „$\tilde{}$" będziemy na ogół opuszczali, kierując się kontekstem. Działania te uogólniają zwykłe dodawanie i mnożenie; $\alpha, \beta \in \mathrm{Card} \Rightarrow \alpha + \beta = \sum\{1 \mapsto \alpha, 2 \mapsto \beta\}$, i analogiczne dla mnożenia, ponadto $\alpha\beta = \sum\{i \to \alpha \mid i < \beta\}$, $\alpha^\beta = \prod\{i \mapsto \alpha \mid \alpha < \beta\}$.

Elementarne prawa dotyczące działań $\sum$ i $\prod$ nie różnią się w sposób istotny od odpowiednich praw dla dodawania i mnożenia (zadanie 5). Zanotujmy jedynie:

(18) $\forall\, A : I \to \mathbb{V} \quad \big|\bigcup_{i\in I} A_i\big| \leqslant \sum_{i\in I} |A_i|$

$\langle \exists)\, \tau : \mathcal{P}I \setminus \{\varnothing\} \to I$ – funkcja wyboru. $\{x \to (x, \tau(\{i \in I \mid x \in A_i\})) \mid \ldots\} : \bigcup_{i\in I} A_i \hookrightarrow \bigsqcup_{i\in I} A_i\rangle$.

Sumowanie nieskończonej rodziny niezerowych liczb kardynalnych również sprowadza się do wyznaczania kresów górnych:

(19) $\alpha \in \mathrm{Card}\setminus\omega, f : \alpha \to \mathrm{Card}\setminus 1 \implies \sum f = \alpha \cup \bigcup_{\xi<\alpha} f(\xi)$

$\langle \sigma := \bigcup_{\xi<\alpha} f(\xi) \in \mathrm{Card}$, $\xi < \alpha \Rightarrow f(\xi) \leqslant \sigma$, a więc $\sum f \leqslant \sum_{\xi<\alpha} \sigma = \alpha \cdot \sigma = \alpha \cup \sigma$.
Gdyby $\sum f < \alpha \cup \sigma$, to możliwe są dwa przypadki:
1) $\sum f < \alpha$. Wówczas $\alpha = \sum_{\xi<\alpha} 1 \leqslant \sum f < \alpha$ ↯
2) $\sum f < \sigma$. Wówczas $\exists)\, \eta < \alpha : \sum f < f(\eta) < \sum f$ ↯$\rangle$.

Na przykład:

(20) $\lambda \in \mathrm{Lim} \implies \aleph_\lambda = \bigcup_{\xi<\lambda} \aleph_\xi = \sum_{\xi<\lambda} \aleph_\xi$.

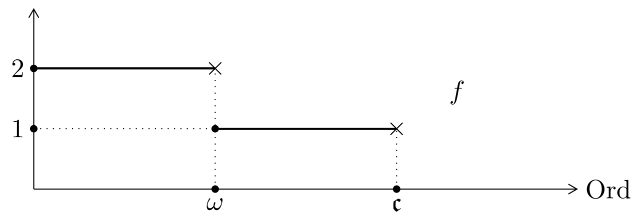
$\langle \sum_{\xi<\lambda} \aleph_\xi = |\lambda| \cup \bigcup_{\xi<\lambda} \aleph_\xi = |\lambda| \cup \aleph_\lambda$, gdyż na mocy tematu o przesunięciu w prawo $|\lambda| \leqslant \lambda \leqslant \aleph_\lambda\rangle$.

Dla iloczynu, w ogólnym przypadku, zachodzi jedynie nierówność:

(21) $\alpha \in \mathrm{Card}\setminus\omega,\ f : \alpha \to \mathrm{Card}\setminus 1 \implies \prod f \leqslant \big(\bigcup_{\xi<\alpha} f(\xi)\big)^\alpha$.

$\langle \forall\, \xi < \alpha : f(\xi) \leqslant \sigma$, gdzie $\sigma = \bigcup\limits_{\xi<\alpha} f(\xi) \in \mathrm{Card}$, a więc $\prod f \leqslant \prod\limits_{\xi<\alpha} \sigma = \sigma^\alpha \rangle$.

Równość zachodzi, gdy funkcja f jest rosnąca (słabo: $\xi < \eta < \alpha \Rightarrow f(\xi) \leqslant f(\eta)$), zob. zadanie 10*; przy czym warunek ten jest istotny, jak wskazuje przykład:



$f = (\omega \times \{2\}) \cup ((\mathfrak{c} \setminus \omega) \times \{1\}) : \mathfrak{c} \to \mathrm{Card}\setminus 1, \qquad \prod f = 2^\omega = \mathfrak{c} < 2^{\mathfrak{c}} = (\bigcup\limits_{\xi<\mathfrak{c}} f(\xi))^{\mathfrak{c}}.$

Silną nierówność z twierdzenia Cantora ($\alpha < 2^\alpha$ dla $\alpha \in \mathrm{Card}$) uogólnia *twierdzenie Königa*:

(22) $I \in \mathbb{V} \ \wedge\ f, g : I \to \mathrm{Card} \ \wedge\ \forall\, i \in I\ f(i) < g(i) \implies \sum f < \prod g$.
(Jeśli $|I| = \alpha$, $f = I \times \{1\}$, $g = I \times \{2\}$, to $\sum f = \alpha$, $\prod g = 2^\alpha$)

$\langle \sum f \leqslant \prod g$, gdyż $\varphi : \bigsqcup f \hookrightarrow \prod g$, gdzie dla $(\xi, i) \in \bigsqcup f$ (tj. $i \in I$, $\xi < f(i)$) $\varphi(\xi, i) = \{i \mapsto \xi\} \cup \{j \mapsto f(j) \mid j \in I \setminus \{i\}\}$. HP: $\sum f = \prod g$. $\exists)\, \psi : \bigsqcup f \twoheadrightarrow \prod g$. Dla ustalonego $i \in I$ oznaczmy przez p_i i-tą projekcję, $p_i : \prod g \mapsto g(i)$, $p_i(x) = x_i$, zaś przez q_i i-tą injekcją, $q_i : f(i) \to \bigsqcup f$, $q_i(\xi) = (\xi, i)$;

$$\begin{tikzcd} \bigsqcup f \arrow[r, hook, two heads, "\psi"] & \prod g \arrow[d, "p_i"] \\ f(i) \arrow[u, "q_i"] \arrow[r, dashed, "\psi_i"] & g(i) \end{tikzcd} .$$

wówczas $\psi_i := p_i \circ \psi \circ q_i : f(i) \to g(i)$, $\mathrm{Im}\,\psi_i \subsetneq g(i)$ $\quad\langle$bo gdyby $\psi_i : f(i) \twoheadrightarrow g(i)$, to $g(i) \leqslant f(i)\rangle$. Zatem $\exists)\, x \in \prod g\ \forall\, i \in I : x_i \in g(i) \setminus \mathrm{Im}\,\psi_i$. Niech $(\xi, j) = \psi^{-1}(x)$, czyli $j \in I$, $\xi \in f(j)$, $\psi(\xi, j) = \alpha$; wówczas $x_j = p_j(\psi(q_j(\xi))) = \psi_j(\xi) \in \mathrm{Im}\,\psi_j$ ↯$\rangle$.

Wyznaczanie mocy zbiorów nieskończonych nazywa się też *kombinatoryką nieskończoną*. Można na przykład rozszerzyć pojęcie symbolu Newtona, kładąc dla dowolnych $\alpha, \beta \in \mathrm{Card}$

$$\binom{\alpha}{\beta} := |\mathcal{P}_\beta(\alpha)|, \qquad \text{gdzie } \forall\, X : \mathcal{P}_\beta(X) := \{Y \subset X \mid |Y| = \beta\}.$$

Łatwo wykazać, że:

(23) $\alpha \in \mathrm{Card}\setminus\omega$, $\beta \in \mathrm{Card}$, $\beta \leqslant \alpha \implies \binom{\alpha}{\beta} = |\,\mathrm{Inj}(\beta, \alpha)| = \alpha^\beta$.

$\langle \binom{\alpha}{\beta} \leqslant |\,\mathrm{Inj}(\beta, \alpha)| \leqslant |\,\mathrm{Map}(\beta, \alpha)| = \alpha^\beta$. W druga stronę: $\alpha^\beta \leqslant |\mathcal{P}_\beta(\alpha \times \beta)| = \binom{\alpha\beta}{\beta}$. Dla $\beta = 0$ prawo (23) jest oczywiste; jeśli $\beta \neq 0$, to $\alpha\beta = \alpha$, a więc $\alpha^\beta \leqslant \binom{\alpha}{\beta}\rangle$.

Z równości (23) wynika na przykład, że w zbiorze nieskończonym mocy α jest dokładnie α podzbiorów skończonych (zadanie 12).

7.2. Tematy

1. Udowodnić, że dla $\alpha, \beta, \gamma \in \mathrm{Card}$; $A, B \in \mathbb{V}$:

(a) $A \cap B = \varnothing \implies |A \cup B| = |A| + |B|$
(b) $|A \times B| = |A| \cdot |B|$
(c) $|\operatorname{Map}(A, B)| = |B|^{|A|}$
(d) $|\mathcal{P}A| = 2^{|A|}$, $\alpha < 2^\alpha$
(e) $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$
(f) $\alpha+\beta = \beta+\alpha$, $\alpha\beta = \beta\alpha$
(g) $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$
(h) $\alpha+0 = \alpha$, $\alpha \cdot 0 = 0$, $\alpha \cdot 1 = \alpha$
(i) $\alpha \leqslant \beta \implies \alpha+\gamma \leqslant \beta+\gamma \;\;\wedge\;\; \alpha\gamma \leqslant \beta\gamma$
(j) $\alpha\beta = 0 \implies \alpha = 0 \;\;\vee\;\; \beta = 0$
(k) $\alpha^{\beta+\gamma} = \alpha^\beta\alpha^\gamma$, $(\alpha\beta)^\gamma = \alpha^\gamma\beta^\gamma$
(l) $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$
(m) $\alpha^0 = 1 = 1^\alpha$, $\alpha^1 = \alpha$, $\alpha \neq 0 \implies 0^\alpha = 0$, $\alpha^2 = \alpha \cdot \alpha$, ...
(n) $\alpha \leqslant \beta \implies \alpha^\gamma \leqslant \beta^\gamma$
(o) $\alpha \neq 0 \wedge \beta \leqslant \gamma \implies \alpha^\beta \leqslant \alpha^\gamma$.

2. Wykazać, że alefy są liczbami granicznymi w sensie porządkowym, to jest że $\mathrm{Card}\backslash\omega \subset \mathrm{Lim}$.

3. W klasie $\mathrm{Ord} \times \mathrm{Ord}$ określamy relację R wzorem:

$$(\alpha, \beta)\, R\, (\gamma, \delta) \iff \alpha \cup \beta < \gamma \cup \delta \;\;\vee\;\; [\alpha \cup \beta = \gamma \cup \delta \wedge (\alpha < \gamma \vee (\alpha = \gamma \wedge \beta \leqslant \delta))].$$

Wykazać, że:

(a) R jest dobrym porządkiem w $\mathrm{Ord} \times \mathrm{Ord}$
(b) $\alpha \in \mathrm{Card}\backslash\omega \implies \mathrm{ord}(\alpha \times \alpha, R) = \alpha$
(c) $\mathrm{ord}(\mathrm{Ord} \times \mathrm{Ord}, R) = \mathrm{Ord}$.

4. Arytmetyka alefów upraszcza się, jeżeli przyjmiemy GCH jako dodatkowy aksjomat.

Scharakteryzować w systemie ZFC + GCH potęgę $\aleph_\alpha^{\aleph_\beta}$ dla $\alpha, \beta \in \mathrm{Ord}$.

5. Wykazać, że jeżeli $X, Y \in \mathbb{V}$, $A : X \to \mathbb{V}$; $f, g : X \to \mathrm{Card}$, $h : X \times Y \to \mathrm{Card}$; $\alpha, \beta \in \mathrm{Card}$, to:

(a) $(\forall\, x, z \in X\; [x \neq z \;\Rightarrow\; A(x) \cap A(z) \neq \varnothing]) \implies \big|\bigcup_{x \in X} A(x)\big| = \sum_{x \in X} |A(x)|$
(b) $|\prod A| = \prod_{x \in X} |A(x)|$
(c) $\sum h = \sum_{x \in X} \sum_{y \in Y} h(x, y)$ i analogicznie dla $\prod$
(d) $\varphi : Y \hookrightarrow\!\!\!\!\rightarrow X \implies \sum f = \sum f \circ \varphi$ i analogicznie dla $\prod$

(e) $(\forall x \in X\ f(x) \leqslant g(x)) \implies \sum f \leqslant \sum g \ \wedge\ \prod f \leqslant \prod g$
(f) $Y \subset X \implies \sum f|Y \leqslant \sum f$
(g) $Y \subset X \ \wedge\ 0 \notin \operatorname{Im} f \implies \prod f|Y \leqslant \prod f$
(h) $\sum\limits_{\xi<\alpha} \beta = \alpha\beta,\ \prod\limits_{\xi<\alpha} \beta = \beta^\alpha$
(i) $(\sum f)\alpha = \sum\limits_{x\in X} f(x)\alpha,\ (\prod f)^\alpha = \prod\limits_{x\in X} f(x)^\alpha$
(j) $\alpha^{\sum f} = \prod\limits_{x\in X} \alpha^{f(x)}$.

6. Dany jest przeliczalny ciąg niezerowych liczb kardynalnych $\tau : \omega \to \mathrm{Card}\backslash 1$.
Wykazać, że:

(i) $\sum \tau = \bigcup\limits_{n<\omega} \sum \tau|n$
(ii) $\prod \tau \geqslant \bigcup\limits_{n<\omega} \prod \tau|n$.

Pokazać na przykładzie, że nierówność w (ii) może być silna.

7. Funkcja alef $\aleph : \mathrm{Ord} \to \mathrm{Ord}$ jest normalna, to znaczy silnie rosnąca i ciągła ($\forall \lambda \in \mathrm{Lim} : \aleph_\lambda = \bigcup\limits_{\xi<\lambda} \aleph_\xi$), i jako taka ma dowolnie duże punkty stałe (rozdział 5, zadania 29–31) – są to tak zwane *alefy krytyczne*.

Ich klasa $\mathcal{A}' := \{\aleph_\alpha \mid \alpha \in \mathrm{Ord}, \aleph_\alpha = \alpha\}$ ($\mathcal{A} := \mathrm{Card}\backslash\omega$ = alefy) jest więc właściwa; $\mathcal{A}' \notin \mathbb{V} \quad \langle \bigcup \mathcal{A} = \mathrm{Ord}\rangle$, zatem $\mathrm{ord}_{\mathcal{A}'} = \mathrm{Ord}$. Oznaczmy $\aleph' = \mathrm{nat}_{\mathcal{A}'}$, tak więc $\aleph' : \mathrm{Ord} \hookrightarrow\!\!\!\!\rightarrow \mathcal{A}'$, $\forall \alpha, \beta \in \mathrm{Ord} : \alpha < \beta \Rightarrow \aleph'_\alpha < \aleph'_\beta$ (skala alefów krytycznych).
Wykazać, że funkcja $\aleph'$ też jest normalna.
Wnioski ($\aleph''$, $\aleph'''$, ...)?

8*. Znaleźć liczby kardynalne $0 < \alpha < \beta$, $0 < \gamma < \delta$ takie, że $\alpha^\gamma = \beta^\delta$.
Wskazówka: Wziąć $\alpha = \bigcup\limits_{n<\omega} \tau_n$, gdzie $\tau_0 = \omega$, $\tau_{n+1} = 2^{\tau_n}$. $\alpha^\omega = ?$

9. Wykazać (w ZFC), że:

$$\mathrm{GCH} \iff \forall\, a \in \mathrm{Card}\backslash\omega : a = \sum_{b \in \mathrm{Card} \cap a} 2^b.$$

10*. Wykazać, że jeżeli $\alpha \in \mathrm{Card}\backslash\omega$, $f : \alpha \to \mathrm{Card}\backslash 1$, $\forall \xi < \eta < \alpha : f(\xi) \leqslant f(\eta)$, to $\prod f = \big(\bigcup\limits_{\xi<\alpha} f(\xi)\big)^\alpha$.
Wskazówka: Wykorzystać dobry porządek R w klasie $\mathrm{Ord} \times \mathrm{Ord}$ opisany w zadaniu 3.

11. Wykazać, że jeżeli $\alpha \in \mathrm{Card}$, $\tau : \omega \to \mathrm{Card}$ i $\forall n < m < \omega : \tau_n < \tau_m$, to $2^\alpha \neq \sum\limits_{n<\omega} \tau_n$. (W szczególności $\mathfrak{c} = 2^\omega \neq \aleph_\omega = \sum\limits_{n<\omega} \aleph_n$).

12. Wykazać, że $\alpha \in \mathrm{Card}\backslash\omega \implies |\mathcal{P}\alpha \bigcap \mathrm{Fin}\,| = \alpha$.

13. Wykazać, że $\alpha \in \mathrm{Card}\backslash\omega \implies \alpha! = 2^\alpha$, gdzie $\alpha! = |\,\mathrm{Perm}(\alpha)|$, $\mathrm{Perm}(\alpha) = \{f \mid f : \alpha \hookrightarrow\!\!\!\!\rightarrow \alpha\}$.

14*. Udowodnić, że jeżeli σ-*algebra* $\mathfrak{m}$ podzbiorów zbioru X (tzn. $\mathfrak{m} \subset \mathcal{P}X$, $X \in \mathfrak{m}$, $\forall\, A : \mathbb{N}^* \to \mathfrak{m}$ $(\bigcup_{i=1}^{\infty} A_i \in \mathfrak{m})$ i $\forall\, B \in \mathfrak{m} : B^{\neg} = X \setminus B \in \mathfrak{m})$ jest nieskończona, to jest ona mocy co najmniej continuum ($|\mathfrak{m}| \geqslant \omega \;\Rightarrow\; |\mathfrak{m}| \geqslant 2^{\omega}$).

Wskazówka: $\exists)\, A : \mathbb{N}^* \hookrightarrow \mathfrak{m}$. Dla ciągu $\alpha : \mathbb{N}^* \to \{0,1\} = 2$ oznaczmy $S_\alpha = \bigcap_{i=1}^{\infty} A_i^{\alpha_i}$, gdzie dla $B \subset X : B^0 = B, B^1 = B^{\neg}$, i dalej $\mathcal{A} = \{\alpha : \mathbb{N}^* \to 2 \mid S_\alpha \neq \varnothing\}$. Udowodnić, że $|\mathcal{A}| \geqslant \omega$ i wskazać injekcję $\mathcal{P}\mathcal{A} \hookrightarrow \mathfrak{m}$.

15. Dla liczby porządkowej granicznej λ ($\lambda \in \mathrm{Lim} = \{\alpha \in \mathrm{Ord} \mid \alpha \neq 0 \wedge \bigcup \alpha = \alpha\}$) oznaczmy:

1) $\mathrm{Cf}\,\lambda = \{X \subset \lambda \mid \bigcup X = \lambda\}$ – podzbiory *współkońcowe* (nieograniczone) liczby λ,
2) $\mathrm{cf}\,\lambda = \bigcap\{|X| \mid X \in \mathrm{Cf}\,\lambda\}$ – *współkońcowość* λ.

Wykazać, że dla $X \subset \lambda \in \mathrm{Lim}$:

(a) $X \in \mathrm{Cf}\,\lambda \iff \forall\,\eta < \lambda\, \exists\,\xi \in X : \eta < \xi$
(b) $\lambda \in \mathrm{Cf}\,\lambda$
(c) $X \in \mathrm{Cf}\,\lambda \implies |X| \geqslant \omega$
(d) $\mathrm{cf}\,\lambda \in \mathrm{Card}$, $\omega \leqslant \mathrm{cf}\,\lambda \leqslant |\lambda|$
(e) $\alpha \in \mathrm{Ord}$, $f : \alpha \to \lambda$, $\bigcup \mathrm{Im}\, f = \lambda \implies \mathrm{cf}\,\lambda \leqslant |\alpha|$.

16. Udowodnić, że:

$$\lambda \in \mathrm{Lim} \implies \exists\, Y \in \mathrm{Cf}\,\lambda : |Y| = \mathrm{ord}\, Y = \mathrm{cf}\,\lambda.$$

17*. Wykazać, że dla liczb granicznych $\lambda, \mu \in \mathrm{Lim}$:

$$f : \mu \to \lambda \;\;\wedge\;\; \forall\,\xi < \eta < \mu : f(\xi) \leqslant f(\eta) \;\;\wedge\;\; \bigcup \mathrm{Im}\, f = \lambda \;.\!\Rightarrow\; \mathrm{cf}\,\mu = \mathrm{cf}\,\lambda.$$

Czy założenie monotoniczności (słabej!) funkcji f jest konieczne?

18. Dla liczb granicznych $\lambda, \mu \in \mathrm{Lim}$ oznaczmy:

(i) $f : \mu \nearrow \lambda \;:\!\iff\; f : \mu \to \lambda, \forall\,\xi < \eta < \mu\; f(\xi) < f(\mu) \wedge \bigcup \mathrm{Im}\, f = \lambda$
(ii) $\mu \nearrow \lambda \;:\!\iff\; \exists\, f : \mu \nearrow \lambda$.

Wykazać, że dla $\lambda, \mu, \nu \in \mathrm{Lim}$:

(a) $\mathrm{cf}\,\lambda \nearrow \lambda$
(b) $\mu \nearrow \lambda \implies \mathrm{cf}\,\mu = \mathrm{cf}\,\lambda$
(c) $\mathrm{cf}\,\mathrm{cf}\,\lambda = \mathrm{cf}\,\lambda$
(d) $\lambda \nearrow \lambda$, $\nu \nearrow \mu \wedge \mu \nearrow \lambda \implies \nu \nearrow \lambda$
(e) $\lambda = \aleph_{\alpha+1}$, $\alpha \in \mathrm{Ord} \implies \mathrm{cf}\,\lambda = \lambda$.

19. Wykazać, że dla $\varkappa \in \mathrm{Card}\setminus\omega$, $\alpha \in \mathrm{Ord}$:

(a) $\exists\,\varphi : \alpha \to \varkappa \cap \mathrm{Card}$ $(\sum \varphi = \varkappa) \iff \mathrm{cf}\,\varkappa \leqslant \alpha$
(b) jeżeli α jest najmniejszą liczbą porządkową, dla której istnieje ciąg $\varphi : \alpha \to \varkappa \cap \mathrm{Card}$ taki, że $\sum \varphi = \varkappa$, to $\alpha = \mathrm{cf}\,\varkappa$
(c) $\varkappa < \varkappa^{\mathrm{cf}\,\varkappa}$
(d) $2 \leqslant \alpha \in \mathrm{Card} \implies \varkappa < \mathrm{cf}\,\alpha^{\varkappa}$.

20. Liczbę kardynalną nieskończoną $\varkappa$ nazywamy *regularną*, gdy $\operatorname{cf}\varkappa = \varkappa$; w przeciwnym wypadku, to jest gdy $\operatorname{cf}\varkappa < \varkappa$, mówimy, że liczba $\varkappa$ jest *syngularna*. Regularne są wszystkie *alefy sekwensowe*, to jest liczby postaci $\aleph_{\alpha+1}$, gdzie $\alpha \in \mathrm{Ord}$ (zadanie 18.(e)) oraz liczba $\omega = \aleph_0$. Jeżeli liczba $\varkappa$ jest syngularna, to jest alefem *granicznym*, tzn. $\varkappa = \aleph_\lambda$, gdzie $\lambda \in \mathrm{Lim}$.

Mówimy, że liczba $\varkappa$ jest *nieosiągalna*, jeżeli jest ona alefem granicznym regularnym.

Wykazać, że:

(a) Każda liczba nieosiągalna jest alefem krytycznym.
(b) Wszystkie alefy graniczne postaci $\aleph_{\alpha+\omega}$, gdzie $\alpha \in \mathrm{Ord}$, $\alpha \neq 0$, są syngularne; $\operatorname{cf}\aleph_{\alpha+\omega} = \omega$.
(c) $\forall\, \lambda \in \mathrm{Lim} : \operatorname{cf}\aleph_\lambda = \omega \implies \aleph_\lambda \neq 2^\omega$.

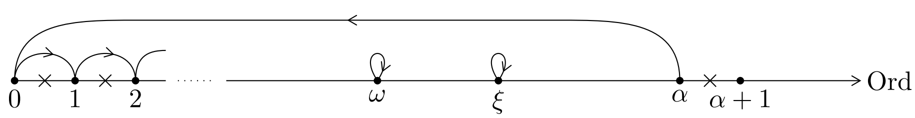
7.3. Odpowiedzi

1. Dowody sprowadzają się do wskazania odpowiedniej bijekcji lub injekcji (dla nierówności). Na przykład, dla dowodu prawa (l) bierzemy $f : \mathrm{Map}(\gamma, \mathrm{Map}(\beta,\alpha)) \hookrightarrow\!\!\!\rightarrow \mathrm{Map}(\beta\times\gamma,\alpha)$, kładąc dla $\varphi : \gamma \to \mathrm{Map}(\beta,\alpha)$

$$f\varphi = \{(y,z) \mapsto (\varphi z)y \mid (y,z) \in \beta\times\gamma\}$$

(piszemy $fx = f(x)$ itp.).

2. HP: $\exists)\, \alpha \in \mathrm{Ord} : \alpha + 1 \in \mathrm{Card}\setminus\omega$. Wówczas:

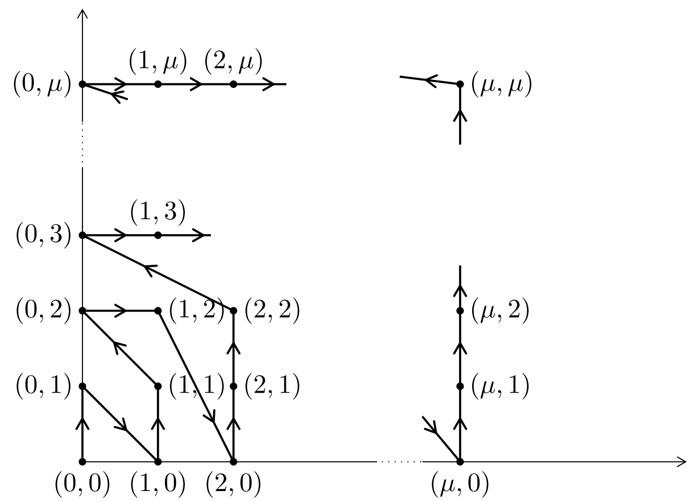


$f = \{\alpha \mapsto 0\} \cup \{n \mapsto n+1 \mid n < \omega\} \cup \{\xi \mapsto \xi \mid \omega \leqslant \xi < \alpha\} : \alpha + 1 \hookrightarrow\!\!\!\rightarrow \alpha$, a więc $\alpha + 1 = |\alpha| \leqslant \alpha < \alpha + 1$ ↯.

3.

(a) Korzystamy z kryterium Tarskiego:
1°) Spójność relacji R wynika ze spójności relacji naturalnego porządku w klasie Ord.
2°) Odcinki $S_{(\gamma,\delta)} = \{(\alpha,\beta) \in \mathrm{Ord}^2 \mid (\alpha,\beta) \underset{R}{<} (\gamma,\delta)\}$ są zbiorami, gdyż dla $(\alpha,\beta) \in S_{(\gamma,\delta)}$: $\alpha \leqslant \alpha\cup\beta < \varepsilon := (\alpha\cup\beta)+1$, i analogicznie $\beta < \varepsilon$, a więc $S_{(\gamma,\delta)} \subset \varepsilon\times\varepsilon$.
3°) W każdym zbiorze $\varnothing \neq X \subset \mathrm{Ord}\times\mathrm{Ord}$ istnieje element R-minimalny.

⟨Naszkicujmy diagram relacji R:



Niech $\mu = \min\{\alpha \cup \beta \mid (\alpha, \beta) \in X\}$.
„Ramka" $A = \{(\alpha, \beta \in \mathrm{Ord}^2 \mid \alpha \cup \beta = \mu\}$ rozpada się na dwa zbiory, $A = B \cup C$, gdzie $B = \{(\alpha, \mu) \mid \alpha < \mu\}$, $C = \{(\mu, \beta) \mid \beta \leqslant \mu\}$.
$\varnothing \neq A \cap X = (B \cap X) \cup (C \cap X)$.
Jeżeli $B \cap X \neq \varnothing$, to – jak łatwo widać – elementem R-minimalnym zbioru X jest (δ, μ), gdzie $\delta = \min\{\alpha \mid (\alpha, \mu) \in B \cap X\}$.
Jeżeli zaś $B \cap X = \varnothing$, to $C \cap X \neq \varnothing$, i element minimalnym jest (μ, δ), gdzie $\delta = \min\{\beta \mid (\mu, \beta) \in C \cap X\}$⟩.

(b) Niech $\beta = \mathrm{ord}(\alpha \times \alpha, R)$, $f = \mathrm{nat}_{\alpha\times\alpha,R} : \beta \lhook\joinrel\twoheadrightarrow \alpha \times \alpha$. Wówczas $|\beta| = \alpha^2 = \alpha$, a więc $\alpha \leqslant \beta$.
HP: $\alpha < \beta$. Wówczas $f(\alpha) = (\gamma, \delta) \in \alpha \times \alpha$, a więc $\gamma \leqslant \gamma \cup \delta < \varepsilon := (\gamma \cup \delta) + 1 < \alpha$, i analogicznie $\delta < \varepsilon < \alpha$, czyli $(\gamma, \delta) \in \varepsilon \times \varepsilon$, $f|\alpha : \alpha \hookrightarrow \varepsilon \times \varepsilon$, $\alpha \leqslant |\varepsilon|^2$, $\varepsilon \geqslant \omega$, $|\varepsilon|^2 = |\varepsilon|$, $\alpha \leqslant |\varepsilon| \leqslant \varepsilon < \alpha$ ↯.
(c) $\mathrm{Ord}^2 = \mathrm{Ord} \times \mathrm{Ord} \notin \mathbb{V}$, gdyż $\mathrm{Ord} \notin \mathbb{V}$ i $\{\alpha \mapsto (\alpha, 0) \mid \alpha \in \mathrm{Ord}\} : \mathrm{Ord} \hookrightarrow \mathrm{Ord}^2$.
Jeśli $A = \mathrm{ord}(\mathrm{Ord}^2, R)$, to $A \leqslant \mathrm{Ord}$ i $F = \mathrm{nat}_{\mathrm{Ord}^2,R} : A \lhook\joinrel\twoheadrightarrow \mathrm{Ord}^2$, a więc $A = \mathrm{Ord}$.

4. W ZFC + GCH:
1°) Jeżeli $\alpha \leqslant \beta$, to $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta} = \aleph_{\beta+1}$.
2°) Jeżeli $\beta < \alpha + 1$, to $\aleph_{\alpha+1}^{\aleph_\beta} = 2^{\aleph_\alpha \aleph_\beta} = 2^{\aleph_\alpha} = \aleph_{\alpha+1}$.
3°) Jeżeli $\beta < \lambda \in \mathrm{Lim}$, to $\aleph_\lambda \leqslant \aleph_\lambda^{\aleph_\alpha} \leqslant \aleph_{\lambda+1}^{\aleph_\alpha} = \aleph_{\lambda+1}$, a więc $\aleph_\lambda^{\aleph_\alpha} \in \{\aleph_\lambda, \aleph_{\lambda+1}\}$.

5. Podobnie jak w zadaniu 1 wystarczy wskazać odpowiednią bijekcję lub injekcję. Na przykład
ad(j): $\alpha^{\sum f} = |\,\mathrm{Map}(\sum f, \alpha) = |\,\mathrm{Map}(\bigsqcup f, \alpha)|$, $\prod\limits_{x \in X} \alpha^{f(x)} = \Big|\prod\limits_{x \in X} \mathrm{Map}(f(x), \alpha)\Big|$.

Oznaczmy dla $x \in X$:

$$\pi_x = \{\xi \mapsto (\xi, x) \mid \xi < f(x)\}; \quad \pi_x : f(x) \hookrightarrow\!\!\!\!\rightarrow f(x) \times \{x\} \subset \bigsqcup f.$$

Określamy bijekcję

$$F : \mathrm{Map}\left(\bigsqcup f, \alpha\right) \hookrightarrow\!\!\!\!\rightarrow \prod_{x \in X} \mathrm{Map}(f(x), \alpha),$$

kładąc dla $\varphi : \bigsqcup f \to \alpha$:

$$F(\varphi) = \{x \mapsto \varphi \circ \pi_x \mid x \in X\}.$$

6.

(i) $\forall\, n < \omega \ \sum \tau|n \leqslant \sum \tau$, a więc $\sigma := \bigcup\limits_{n<\omega} \sum \tau|n \leqslant \sum \tau$.

HP: $\sigma < \sum \tau = \omega \cup \bigcup\limits_{n<\omega} \tau_n$.

Dwa przypadki:

1) $\sigma < \omega$.
Wówczas $\forall\, n < \omega : \sum \tau|n \leqslant \sigma$. Jednak $\sum \tau|n = \sum\limits_{k<n} \tau_k \geqslant \sum\limits_{k<n} 1 = n$, a więc dla $n = \sigma + 1$: $\sigma + 1 \leqslant \sigma$ ↯.

2) $\sigma < \bigcup\limits_{n<\omega} \tau_n$.
$\exists)\, n < \omega : \sigma < \tau_n < \sum \tau|(n+1) \leqslant \sigma$ ↯.

(ii) Nierówność wykazujemy analogicznie jak w (i).
Jeżeli $\tau = \omega \times \{2\}$, to

$$\prod \tau = \prod_{n<\omega} 2 = 2^\omega = \mathfrak{c}, \quad \text{natomiast}$$
$$\bigcup_{n<\omega} \prod \tau|n = \bigcup_{n<\omega} \prod_{k<n} 2 = \bigcup_{n<\omega} 2^n = \omega < \mathfrak{c}.$$

7. Jest to ogólna prawidłowość.
Jeżeli ciąg $f : \mathrm{Ord} \to \mathrm{Ord}$ jest normalny, tzn.

1°) $\forall\, \xi, \eta \in \mathrm{Ord} : \xi < \eta \implies f(\xi) < f(\eta)$ i

2°) $\forall\, \lambda \in \mathrm{Lim} : f(\lambda) = \bigcup\limits_{\xi<\lambda} f(\xi)$,

to ma dowolnie duże punkty krytyczne (rozdział 5. zadanie 29), a więc ich ogół $K = \{\alpha \in \mathrm{Ord} \mid f(\alpha) = \alpha\}$ jest klasą właściwą i jej naturalna numeracja $f' = \mathrm{nat}_K : \mathrm{Ord} \hookrightarrow\!\!\!\!\rightarrow K$ też jest ciągiem normalnym $\langle$Należy wykazać, że $\forall\, \lambda \in \mathrm{Lim} : f'(\lambda) = \bigcup\limits_{\xi<\lambda} f'(\xi)$. HP: $\exists)\, \mu \in \mathrm{Lim} : f'(\mu) \neq \bigcup\limits_{\xi<\mu} f'(\xi)$.
Oznaczmy $\sigma = \bigcup\limits_{\xi<\mu} f'(\xi)$. Wówczas $\forall\, \xi < \mu : f'(\xi) < f'(\mu)$, a więc $\sigma \leqslant f'(\mu)$, czyli $\sigma < f'(\mu)$.
$\sigma \in \mathrm{Lim}$ $\langle$HP: $\exists)\, \alpha \in \mathrm{Ord} : \sigma = \alpha + 1$. Wówczas $\alpha < \sigma$, $\exists)\, \xi < \mu : \alpha < f'(\xi)$;
$\alpha \leqslant f(\alpha) < f(f'(\xi)) = f'(\xi) < f'(\xi + 1) \leqslant \sigma = \alpha + 1$ ↯$\rangle$.

$\sigma = f(\sigma)$ $\langle$HP: $\sigma < f(\sigma) = \bigcup_{\xi<\sigma} f(\xi)$. $\exists)\, \xi < \sigma : \sigma < f(\xi)$. $\exists)\, \eta < \mu : \xi < f'(\eta)$, i wówczas $\sigma < f(\xi) < f(f'(\eta)) = f'(\eta) \leqslant \sigma$ $\lightning\rangle$.
Zatem $\exists)\, \alpha \in \mathrm{Ord} : \sigma = f'(\alpha)$.
$\alpha < \mu$ $\langle$HP: $\mu \leqslant \alpha$. Wówczas $f'(\mu) < f'(\alpha) = \sigma < f'(\mu)$ $\lightning\rangle$,
a więc $\sigma = f'(\alpha) < f'(\alpha+1) \leqslant \sigma$ $\lightning\rangle$.

Tak więc funkcja $\aleph' : \mathrm{Ord} \to \mathrm{Ord}$ jest normalna, klasa $\mathcal{A}''$ jej punktów krytycznych jest właściwa; jej numeracja $\aleph'' : \mathrm{Ord} \to \mathrm{Ord}$ jest normalna itd.

Zauważmy, że wszystko to dzieje się w ZFC.

8*. Określamy ciąg $\tau : \omega \to \mathrm{Card}$; $\tau_0 = \omega$, $\tau_{n+1} = 2^{\tau_n}$

Liczba $\alpha := \bigcup_{n<\omega} \tau_n \in \mathrm{Card}$ $\langle$według (6)$\rangle$. $\tau_0 < \tau_1 < \ldots < \alpha$.

Z aksjomatu wyboru wynika, że istnieje ciąg bijekcji $\varphi_n : \mathcal{P}\tau_n \hookrightarrow\!\!\!\!\rightarrow \tau_{n+1}$, $n < \omega$. Określmy injekcię $f : \mathcal{P}\alpha \hookrightarrow \mathrm{Map}(\omega, \alpha)$, kładąc dla $X \subset \alpha$: $f_X = \{n \mapsto \varphi_n(X \cap \tau_n) \mid n < \omega\}$ $\langle$Jest to iniekcja, gdyż $X \subset \alpha \implies X = \bigcup_{n<\omega} X \cap \tau_n\rangle$.
Zatem $2^\alpha \leqslant \alpha^\omega$.
Jednak $\alpha < 2^\alpha$, a więc $\alpha^\omega \leqslant 2^{\alpha\cdot\omega} = 2^\alpha$. Tak więc $\alpha^\omega = 2^\alpha = 2^{\alpha^2} = (2^\alpha)^\alpha$, czyli $\alpha < 2^\alpha$, $\omega < \alpha$, i $\alpha^\omega = (2^\alpha)^\alpha$.

(Uwaga: określając ciąg τ, możemy jako τ_0 wziąć dowolną liczbę kardynalną nieskończoną).

9. $S := \sum_{b\in \mathrm{Card}\cap a} 2^b = |\,\mathrm{Card} \cap a| \cup \sigma$, gdzie $\sigma = \bigcup_{b\in\mathrm{Card}\cap a} 2^b$ $(\in \mathrm{Card})$.

$\Rightarrow)$ Trzy przypadki:

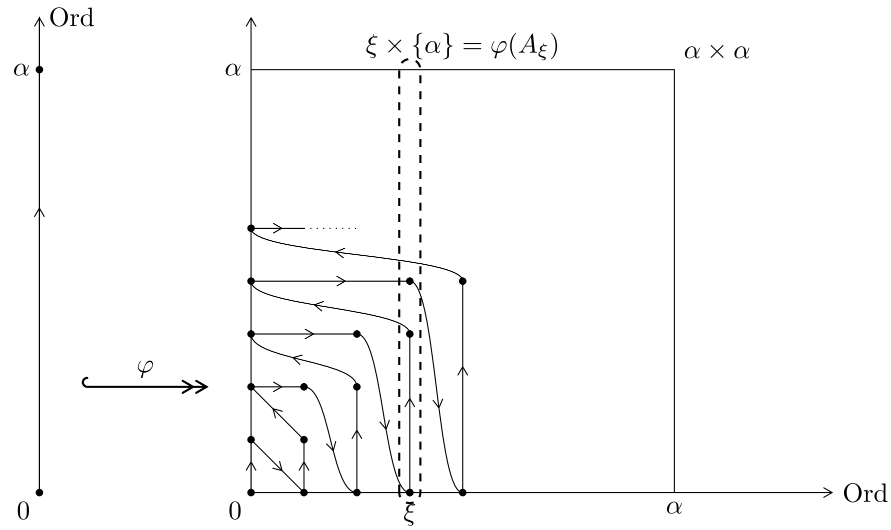
1) $a = \aleph_0$ $(= \omega)$.
Wówczas $\sigma = \bigcup_{b<\omega} 2^b = \omega$, $\mathrm{Card} \cap a = \omega$, a więc $S = \omega \cup \omega = \omega = a$.
2) $a = \aleph_{\alpha+1}$, $\alpha \in \mathrm{Ord}$.
Wówczas $\sigma = \bigcup_{\beta\leqslant\alpha} 2^{\aleph_\beta} = 2^{\aleph_\alpha} = \aleph_{\alpha+1}$, $|\,\mathrm{Card} \cap a| \leqslant a = \aleph_{\alpha+1}$, a więc $S = \aleph_{\alpha+1}$.
3) $a = \aleph_\lambda$, $\lambda \in \mathrm{Lim}$.
Wówczas $\sigma = \bigcup_{\beta<\lambda} 2^{\aleph_\beta} = \bigcup_{\beta<\lambda} \aleph_{\beta+1} = \aleph_\lambda$, $|\,\mathrm{Card} \cap a| \leqslant \aleph_\lambda$, a więc $S = \aleph_\lambda$.

$\Leftarrow)$ Niech $\alpha \in \mathrm{Ord}$. Weźmy $a = \aleph_{\alpha+1}$. Wówczas $S = |\,\mathrm{Card} \cap \aleph_{\alpha+1}| \cup \bigcup_{\beta\leqslant\alpha} 2^{\aleph_\beta} = |\,\mathrm{Card} \cap \aleph_{\alpha+1}| \cup 2^{\aleph_\alpha}$; ale $|\,\mathrm{Card} \cap \aleph_{\alpha+1}| \leqslant \aleph_{\alpha+1} \leqslant 2^{\aleph_\alpha}$, a więc $S = 2^{\aleph_\alpha}$, czyli $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$.

10*. Wystarczy udowodnić, że $\prod f \geqslant \sigma^\alpha$, gdzie $\sigma := \bigcup_{\xi<\alpha} f(\xi)$.

Niech R będzie dobrym porządkiem w $\mathrm{Ord} \times \mathrm{Ord}$ (zadanie 3.(a)); $\mathrm{ord}(\alpha \times \alpha, R) = \alpha$ (zadanie 3.(b)), a więc $\varphi = \mathrm{nat}_{\alpha\times\alpha,R} : \alpha \hookrightarrow\!\!\!\!\rightarrow \alpha \times \alpha$, $\forall\, \xi < \eta < \alpha : \varphi(\xi) \underset{R}{<} \varphi(\eta)$.

Rozważmy podział $\{A_\xi \mid \xi < \alpha\}$ zbioru α, gdzie dla $\xi < \alpha$: $A_\xi = \varphi^{-1}(\{\xi\} \times \alpha)$.



Tak więc $\prod f = \prod\limits_{\xi<\alpha} \prod\limits_{\zeta \in A_\xi} f(\zeta)$.

Zauważmy, że $\forall\, \xi < \alpha : \bigcup f(A_\xi) = \sigma$ (zob. rysunek) $\langle$HP: $\exists)\, \xi < \alpha : \sigma' := \bigcup f(A_\xi) < \sigma$. Wówczas $\exists)\, \beta < \alpha : \sigma' < f(\beta)$, a więc $\forall\, \zeta \in A_\xi : f(\zeta) < f(\beta)$, $\zeta < \beta$ czyli $A_\xi \subset \beta$ $\langle$bo gdyby $\beta \leqslant \zeta$, to $f(\beta) \leqslant f(\zeta)$ ↯$\rangle$.
Tak więc $\forall\, \eta < \alpha : \varphi^{-1}(\xi,\eta) < \beta$, $(\xi,\eta) \underset{R}{<} (\gamma,\delta) := \varphi(\beta)$, i dla $\eta = (\gamma \cup \delta) + 1 < \alpha$: $\eta \leqslant \xi \cup \eta \leqslant \gamma \cup \delta < (\gamma \cup \delta) + 1 = \eta$ ↯$\rangle$.
Ponieważ dla $\xi < \alpha$, $\forall\, \zeta' \in A_\xi : f(\zeta') \leqslant \prod\limits_{\zeta \in A_\xi} f(\zeta)$, więc $\sigma \leqslant \prod\limits_{\zeta \in A_\xi} f(\zeta)$, skąd $\prod f \geqslant \prod\limits_{\xi<\alpha} \sigma = \sigma^\alpha$.

11. HP: $2^\alpha = \sum\limits_{n<\omega} \tau_n$.
Wówczas $\alpha \geqslant \omega$ $\langle 2^\alpha \geqslant \sum\limits_{n<\omega} 1 = \omega \rangle$, a więc $2^\alpha < \prod\limits_{n<\omega} \tau_{n+1} \leqslant \prod\limits_{n<\omega} 2^\alpha = \left(2^\alpha\right)^\omega = 2^{\alpha\cdot\omega} = 2^\alpha$ ↯.

12. $|\mathcal{P}\alpha \cap \mathrm{Fin}\,| = \sum\limits_{n<\omega} \binom{\alpha}{n} = \sum\limits_{n<\omega} \alpha^n = \sum\limits_{0<n<\omega} \alpha = \alpha \cdot \omega = \alpha$.

13. $\mathrm{Perm}(\alpha) \subset \mathrm{Map}(\alpha,\alpha)$, a więc $\alpha! \leqslant \alpha^\alpha = 2^\alpha$.
Dla dowodu nierówności w drugą stronę zauważmy, że każdy zbiór nietrywialny (tj. mocy $\geqslant 2$) ma permutację bez punktów stałych. $\langle$Jeżeli $2 \leqslant n < \omega$, to można wziąć permutację cykliczną $\{0 \mapsto 1, 1 \mapsto 2, \ldots, n-2 \mapsto n-1, n-1 \mapsto 0\} : n \hookrightarrow\!\!\!\!\!\rightarrow n$.
Dla $\alpha \in \mathrm{Card}\backslash\omega$ można wziąć na przykład $\bigcup\limits_{\substack{\lambda \in \mathrm{Lim}_0 \cap \alpha \\ n<\omega}} \{\lambda+2n \mapsto \lambda+2n+1, \lambda+2n+1 \mapsto \lambda+2n\} : \alpha \hookrightarrow\!\!\!\!\!\rightarrow \alpha\rangle$.

Zbiór $\mathcal{A} = \{A \subset \alpha \mid |A| \geqslant 2\}$ jest mocy 2^α. Dla $A \in \mathcal{A}$ niech φ_A będzie permutacją bez punktów stałych zbioru A $\langle$AC$\rangle$.

Określamy injekcję $f : \mathcal{A} \hookrightarrow\!\!\!\!\rightarrow \operatorname{Perm}(\alpha)$, kładąc dla $A \in \mathcal{A} : f_A = \varphi_A \cup \mathrm{id}_{\alpha \setminus A}$ $\langle$jeśli $f_A = f_B$ dla $A, B \in \mathcal{A}$, to $A = \{\xi < \alpha \mid f_A(\xi) \neq \xi\} = \{\xi < \alpha \mid f_B(\xi) \neq \xi\} = B\rangle$.

Zatem $2^\alpha = |\mathcal{A}| \leqslant |\operatorname{Perm}(\alpha)| = \alpha!$.

14*. Rodzina $\{S_\alpha \mid \alpha \in \mathcal{A}\}$ jest podziałem zbioru X.
Określamy injekcję $F : \mathbb{N}^* \hookrightarrow \mathcal{P}\mathcal{A}$, kładąc dla $i \in \mathbb{N}^*$, $F(i) = \{\alpha \in \mathcal{A} \mid S_\alpha \subset A_i\}$ $\langle$HP: $\exists)\, i, j \in \mathbb{N}^*$, $i \neq j$, $x \in A_i \setminus A_j$, $F(i) = F(j)$. Wówczas $\exists)\, \alpha \in \mathcal{A} : x \in S_\alpha = \bigcap_{k=1}^{\infty} A_k^{\alpha_k} \subset A_i$. Zatem $\alpha \in F(i) = F(j)$, $S_\alpha \subset A_j$, $x \in A_j$ ↯$\rangle$.

Zatem $|\mathcal{P}\mathcal{A}| \geqslant \omega$, a więc $|\mathcal{A}| \geqslant \omega$, $|\mathcal{P}\mathcal{A}| \geqslant 2^\omega$.
Następnie określamy injekcję $G : \mathcal{P}\mathcal{A} \hookrightarrow \mathfrak{m}$, kładąc dla $\mathcal{B} \subset \mathcal{A}$, $G(\mathcal{B}) = \bigcup_{\beta \in \mathcal{B}} S_\beta$ $\langle$HP: $\exists)\, \mathcal{B}, \mathcal{C} \subset \mathcal{A}$, $\beta \in \mathcal{B} \setminus \mathcal{C}$, $G(\mathcal{B}) = G(\mathcal{C})$. Wówczas $\exists)\, x \in S_\beta \subset G(\mathcal{B})$, $x \in G(\mathcal{C})$, $\exists)\, \gamma \in \mathcal{C} : x \in S_\gamma$; $\beta \neq \gamma$, $x \in S_\beta \cap S_\gamma = \varnothing$ ↯$\rangle$.
Zatem $|\mathfrak{m}| \geqslant |\mathcal{P}\mathcal{A}| \geqslant 2^\omega$.

15. (a)–(d) to natychmiastowe wnioski z przyjętych definicji.
(e): $\operatorname{Im} f \in \operatorname{Cf} \lambda$, a więc $\operatorname{cf} \lambda \leqslant |\operatorname{Im} f| \leqslant |\alpha|$.

16. $\exists)\, X \in \operatorname{Cf} \lambda : |X| = \alpha = \operatorname{cf} \lambda$. $\exists)\, f : \alpha \hookrightarrow\!\!\!\!\rightarrow X$.
Określamy indukcyjnie ciąg g, kładąc dla $\xi \in \mathrm{Ord}$:

$$g(\xi) = \bigcap \{\eta \in \mathrm{Ord} \mid f(\xi) < \eta < \lambda \ \ \wedge \ \ \operatorname{Im}(g|\xi) \subset \eta\}.$$

Niech $\beta = \operatorname{Dom} g$.
Wówczas $\forall\, \xi < \beta : f(\xi) < g(\xi) < \lambda \ \ \wedge \ \ \operatorname{Im}(g|\xi) \subset g(\xi)$.
Zatem $\beta \leqslant \alpha \ \ \wedge \ \ \forall\, \zeta < \xi < \beta : g(\zeta) < g(\xi)$.
Jest $\beta = \alpha$ $\langle$HP: $\beta < \alpha$. Wówczas $g(\beta) = \mathbb{V}$, a więc

$$\{\eta \in \mathrm{Ord} \mid f(\beta) < \eta < \lambda \ \ \wedge \ \ \operatorname{Im} g \subset \eta\} = \varnothing.$$

Zatem $\forall\, \eta \in \mathrm{Ord} : f(\beta) < \eta < \lambda \implies \exists\, \xi < \alpha : \eta \leqslant g(\xi)$, a więc $\bigcup \operatorname{Im} g = \lambda$, czyli $\operatorname{Im} g \in \operatorname{Cf} \lambda$, $\alpha \leqslant |\operatorname{Im} g| = |\beta| \leqslant \beta$ ↯$\rangle$.

Tak więc dla $Y = \operatorname{Im} g : \mathrm{nat}_Y = g$, $|Y| = \operatorname{ord} Y = \operatorname{cf} \lambda$.

17*. Oznaczmy $\alpha = \operatorname{cf} \lambda$, $\beta = \operatorname{cf} \mu$. Z faktu udowodnionego w zadaniu 16 wynika, że istnieją injekcje rosnące $\varphi : \alpha \to \lambda$, $\psi : \beta \to \mu$ takie, że $\bigcup \operatorname{Im} \varphi = \lambda$, $\bigcup \operatorname{Im} \psi = \mu$.

Wówczas $f \circ \psi : \beta \to \lambda$ oraz $\bigcup \operatorname{Im}(f \circ \psi) = \lambda$ $\langle$Niech $\eta < \lambda$. $\exists)\, \zeta < \mu : \eta < f(\zeta)$. $\exists)\, \xi < \beta : \zeta < \psi(\xi)$, a więc $f(\zeta) \leqslant f(\psi(\xi))$. Zatem $\eta < (f \circ \psi)(\xi)\rangle$.
Tak więc $\alpha = \operatorname{cf} \lambda \leqslant |\operatorname{Im}(f \circ \psi)| \leqslant \beta$.

Wykażemy, że $\beta \leqslant \alpha$, a więc $\alpha = \beta$. Określamy indukcyjnie ciąg g, kładąc

$$\forall\, \xi \in \mathrm{Ord} : g(\xi) = \bigcap \{\zeta < \mu \mid \operatorname{Im}(g|\xi) \subset \zeta \ \ \wedge \ \ \varphi(\xi) < f(\zeta)\}.$$

Oznaczmy $\alpha' = \operatorname{Dom} g$. Wówczas

$$\forall\, \xi < \alpha' : g(\xi) < \mu, \ \operatorname{Im}(g|\xi) \subset g(\xi), \ \varphi(\xi) < f(g(\xi)).$$

Zatem $\alpha' \leqslant \alpha$ $\langle$gdyż $\xi < \alpha' \ \Rightarrow \ \xi \in \operatorname{Dom} \varphi = \alpha\rangle$, oraz $g : \alpha' \hookrightarrow \mu$, g – rosnąca.

$\bigcup \operatorname{Im} g = \mu \quad \langle$HP: $\sigma = \bigcup \operatorname{Im} g < \mu$. Wówczas $f(\sigma) < \lambda$, $\exists)\, \xi < \alpha : f(\sigma) < \varphi(\xi) < \lambda = \bigcup \operatorname{Im} f$, $\exists)\, \zeta < \mu : \varphi(\xi) < f(\zeta)$, a więc $f(\sigma) < f(\xi)$, skąd $\sigma < \zeta \quad \langle$HP: $\xi \leqslant \sigma$. Wówczas $f(\zeta) < f(\sigma) < f(\zeta)$ ↯$\rangle$.

$\operatorname{Im} g \subset \zeta \quad \langle \forall\, \xi' < \alpha' : g(\xi') \leqslant \sigma < \zeta \rangle$, i tym bardziej $\operatorname{Im}(g|\xi) \subset \xi$, a więc $\zeta \in \{\zeta < \mu \mid \operatorname{Im}(g|\xi) \subset \zeta \ \wedge \ \varphi(\xi) < f(\zeta)\}$, skąd wynika, że $g(\xi) \leqslant \zeta$, $\xi < \alpha'$, $\varphi(\xi) < f(g(\xi))$, $f(\sigma) < f(g(\xi))$, $\sigma < g(\xi) \leqslant \sigma$ ↯$\rangle$.

Zatem $\beta = \operatorname{cf} \mu \leqslant \alpha' \leqslant \alpha$.

Założenie monotoniczności funkcji f jest konieczne.

Przykład:
$\{n \mapsto \aleph_{\omega+n} \mid n < \omega\} : \omega \to \aleph_\omega$, a więc $\operatorname{cf} \aleph_\omega = \omega = \operatorname{cf} \omega$ $(\omega = \aleph_0)$, oraz $\operatorname{cf} \aleph_1 = \aleph_1$ (zob. zadanie 18.(c)).

1°) $\exists)\, f : \aleph_\omega \to \aleph_1$ $[f|\aleph_1 \subset \mathrm{id}]$, i wówczas $\bigcup \operatorname{Im} f = \aleph_1$ i $\aleph_0 = \operatorname{cf} \aleph_\omega < \aleph_1 = \operatorname{cf} \aleph_1$

2°) $\exists)\, f : \aleph_1 \to \omega = \aleph_0$ $[f(\omega) \subset \omega]$, $\bigcup \operatorname{Im} f = \omega : \omega = \operatorname{cf} \aleph_0 < \aleph_1 = \operatorname{cf} \aleph_1$.

18. Dowody praw (a)–(d) są bezproblemowe.
(e): Jest $\operatorname{cf} \lambda \leqslant \lambda$. HP: $\gamma = \operatorname{cf} \lambda < \lambda = \aleph_{\alpha+1}$. Wówczas $\gamma \leqslant \aleph_\alpha$.
$\exists)\, X \subset \lambda : \bigcup X = \lambda$. $|X| = \gamma$.
Wówczas $\lambda = |\bigcup X| \leqslant \sum\limits_{\xi \leqslant X} |\xi| \leqslant |X| \cdot \aleph_\alpha = \gamma \cdot \aleph_\alpha = \aleph_\alpha < \lambda$ ↯.

19.

(a)
$\Rightarrow)$ Hp: $\alpha < \operatorname{cf} \varkappa$. $\exists)\, \varphi : \alpha \to \varkappa \cap \mathrm{Card}$ $(\sum \varphi = \varkappa)$.
Wówczas $\sigma = \bigcup \operatorname{Im} \varphi < \varkappa \quad \langle$HP: $\varkappa \leqslant \sigma$. Jednak $\operatorname{Im} \varphi \subset \varkappa$, a więc $\sigma = \bigcup \operatorname{Im} \varphi \leqslant \varkappa$, czyli $\varkappa = \sigma$. Zatem $\operatorname{cf} \varkappa \leqslant |\operatorname{Im} \varphi| \leqslant |\alpha| < \alpha$ ↯$\rangle$.
$\Leftarrow)$ $\exists)\, f : \operatorname{cf} \varkappa \nearrow \varkappa \quad \langle$zadanie 18.(a)$\rangle$.
Niech $\varphi = \mathrm{card} \circ f$. Wówczas $\varphi : \operatorname{cf} \varkappa \to \varkappa \cap \mathrm{Card}$, $\forall\, \xi < \operatorname{cf} \varkappa : \varphi(\xi) = |f(\xi)|$.
Zatem $\varkappa = \bigcup \operatorname{Im} f = \bigcup\limits_{\xi < \operatorname{cf} \varkappa} f(\xi) \leqslant \sum\limits_{\xi < \operatorname{cf} \varkappa} \varphi(\xi) \leqslant \varkappa \cdot \operatorname{cf} \varkappa = \varkappa$, a więc $\sum\limits_{\xi < \operatorname{cf} \varkappa} \varphi(\xi) = \sum \varphi = \varkappa$.

Dla $\alpha \geqslant \operatorname{cf} \varkappa$ bierzemy $\varphi' = \varphi \cup \{\xi \mapsto 0 \mid \operatorname{cf} \varkappa \leqslant \xi < \alpha\}$ i wówczas $\sum \varphi' = \sum \varphi = \varkappa$.

(b) Jest to wniosek z (a).
(c) $\exists)\, \varphi : \operatorname{cf} \varkappa \to \varkappa \cap \mathrm{Card}$, $\sum \varphi = \varkappa \quad \langle$wg. (a)$\rangle$. Na mocy twierdzenia Königa $\varkappa < \prod\limits_{\xi < \operatorname{cf} \varkappa} \varkappa = \varkappa^{\operatorname{cf} \varkappa}$.
(d) HP: $\operatorname{cf} \alpha^\varkappa \leqslant \varkappa$.
Wówczas $\exists)\, \varphi : \varkappa \to \alpha^\varkappa \cap \mathrm{Card}$, $\sum \varphi = \alpha^\varkappa$. Zatem $\alpha^\varkappa = \sum\limits_{\xi < \varkappa} \varphi(\xi) < \prod\limits_{\xi < \varkappa} \alpha^\varkappa = \left(\alpha^\varkappa\right)^\varkappa = \alpha^{\varkappa^2} = \alpha^\varkappa$ ↯.

20.

(a) Niech $\lambda \in \mathrm{Lim}$ i $\operatorname{cf} \aleph_\lambda = \aleph_\lambda$.
$\aleph|\lambda : \lambda \nearrow \aleph_\lambda$, a więc $\aleph_\lambda = \operatorname{cf} \aleph_\lambda = \operatorname{cf} \lambda \leqslant \lambda \leqslant \aleph_\lambda$.
(b) $\{n \mapsto \aleph_{\alpha+n} \mid n < \omega\} : \omega \nearrow \aleph_{\alpha+\omega}$, a więc $\operatorname{cf} \aleph_{\alpha+\omega} = \operatorname{cf} \omega = \omega$.

(c) HP: $\aleph_\lambda = 2^\omega$.
Wówczas na mocy 19(d): $\omega < \operatorname{cf} 2^\omega = \operatorname{cf} \aleph_\lambda = \omega$ $\lightning$.

8

Kategorie i struktury

8.1. Wstęp

8.1.1. *Kategoria zwyczajna* $\mathcal{T} = (T, \sigma)$ jest określona przez dwa odwzorowania: $T : \mathbb{V} \to \mathbb{V}$, $\sigma : (\operatorname{Ob} T)^2 \to \mathbb{V}$, gdzie $\operatorname{Ob} T = \{(A, \alpha) \mid A \in \mathbb{V}, \alpha \in T(A)\}$ – klasa obiektów kategorii $\mathcal{T}$; dla dwóch takich obiektów $X = (A, \alpha)$, $Y = (B, \beta)$ zachodzi inkluzja: $\sigma(X, Y) \subset \operatorname{Map}(A, B)$.

Postulujemy:

1° $X, Y, Z \in \operatorname{Ob} T \ \wedge \ f \in \sigma(X, Y) \ \wedge \ g \in \sigma(Y, Z) \implies g \circ f \in \sigma(X, Z)$ (*postulat złożenia*)
2° $X = (A, \alpha) \in \operatorname{Ob} T \ \wedge \ f : A \hookrightarrow\!\!\!\!\rightarrow B \implies \exists!\, Y = (B, \beta) \in \operatorname{Ob} T : f \in \sigma(X, Y)$, $f^{-1} \in \sigma(Y, X)$ (*postulat przeniesienia*).

8.1.2. Odwzorowania należące do $\sigma(X, Y)$ nazywamy *morfizmami* z X do Y; dla poszczególnych kategorii zwyczajnych, np. grup czy przestrzeni topologicznych, morfizmy mają specjalne nazwy – odpowiednio: homomorfizmy, odwzorowania ciągłe itp.

Dla $X = (A, \alpha) \in \operatorname{Ob} T$ zbiór A nazywamy *zbiorem podkładowym* obiektu X; notacja: $\operatorname{set} X = \underline{X} := A$; element α to *struktura* X; $\operatorname{str} X = \alpha$. Zwykle dla $X \in \operatorname{Ob} T$ piszemy X zamiast $\underline{X}$ lub $\operatorname{set} X$, zdając się na kontekst; np. zapis $x \in X$ rozumiemy jako $x \in \underline{X}$ itp.

Dla morfizmu $f \in \sigma(X, Y)$ piszemy też $f : X \stackrel{.}{\longrightarrow} Y$ lub $f : X \xrightarrow[\mathcal{T}]{} Y$; zapis $f : X \to Y$ może już prowadzić do nieporozumień.

Zauważmy, że dla $X = (A, \alpha) \in \operatorname{Ob} T$; $\operatorname{id}_A : X \stackrel{.}{\longrightarrow} X$ – jest to tzw. *morfizm identycznościowy* obiektu X. $\langle$Wg 2° $\exists!)\, \beta \in T(A) : \operatorname{id}_A : X \stackrel{.}{\longrightarrow} Y$, $\operatorname{id}_A^{-1} = \operatorname{id}_A : Y \stackrel{.}{\longrightarrow} X$, gdzie $Y = (A, \beta)$. Teraz wg 1°, $\operatorname{id}_A : X \stackrel{.}{\longrightarrow} X$ (i $X = Y$, znów według 2°)$\rangle$.

8.1.3. Przykłady:

1) Kategoria systemów relacyjnych.
$T(A) = \mathcal{P}A^2$; dla $X = (A, \alpha)$, $Y = (B, \beta) \in \operatorname{Ob} T$: $\alpha \subset A^2$, $\beta \subset B^2$, $\sigma(X, Y) = \{f : A \to B \mid \forall\, x, t \in A : x \underset{\alpha}{\leqslant} t \ \Rightarrow \ f(x) \underset{\beta}{\leqslant} f(t)\}$.

Tak więc morfizmami w tej kategorii są *odwzorowania rosnące* (w sensie słabym).

2) Kategoria Pretop *przestrzeni pretopologicznych*.
$T(A) = \mathcal{P}^2 A = \mathcal{P}\mathcal{P}A$; dla $X = (A,\alpha)$, $Y = (B,\beta) \in \mathrm{Ob}\, T : \alpha \subset \mathcal{P}A$, $\beta \subset \mathcal{P}B$, $\sigma(X,Y) = \{f : A \to B \mid \forall\, U \in \beta : f^{-1}(U) \in \alpha\}$.

Morfizmy tej kategorii nazywamy *odwzorowaniami ciągłymi*.

3) *Kategoria grupoidów*.
$T(A) = Map(A^2, A) \times A$; dla $X = (A,(\varphi,a))$, $Y = (B,(\psi,b)) \in \mathrm{Ob}\, T$: $\varphi : A^2 \to A$, $a \in A$, $\psi : B^2 \to B$, $b \in B$, $\sigma(X,Y) = \{f : A \to B \mid \forall\, x,t \in A\ [f(\varphi(x,t)) = \psi(f(x), f(t)) \wedge f(a) = b]\}$.

Dla grupoidów morfizmy nazywamy *homomorfizmami*.

4) Kategoria Set wszystkich zbiorów (i ich odwzorowań dowolnych).
$T(A) = 1 = \{\varnothing\}$. Tak więc $\mathrm{Ob}\, T = \{(A,\varnothing) \mid A \in \mathbb{V}\}$ i możemy utożsamiać: $\mathrm{Ob}\, T = \mathbb{V}$. Po tym utożsamieniu $\sigma(A,B) = \mathrm{Map}(A,B)$ dla dowolnych zbiorów A i B.

Sprawdzenie postulatów złożenia i przeniesienia (1°, 2°) we wszystkich tych czterech przypadkach sprowadza się do mechanicznych przeliczeń.

8.1.4. W definicji kategorii zwyczajnej kluczowe znaczenie ma postulat przeniesienia stwierdzający „nieistotność” zbioru podkładowego (nie materia, tylko forma!).

Jeżeli $X = (A,\alpha) \in \mathrm{Ob}\, T$, $f : A \hookrightarrow\!\!\!\!\rightarrow B$ i $Y = (B,\beta)$ jest jedynym takim obiektem kategorii $\mathcal{T}$, że

$$f : X \xrightarrow{\ .\ } Y \quad \text{i} \quad f^{-1} : Y \xrightarrow{\ .\ } X,$$

to bijekcję f nazywamy *izomorfizmem* X na Y i mówimy, że obiekty X i Y są *izomorficzne*; zapis: $f : X \xrightarrow{\sim} Y$, $f : X \xrightarrow[\mathcal{T}]{\sim} Y$, $X \simeq Y \ :\Longleftrightarrow\ \exists\, f : X \xrightarrow{\sim} Y$.

Tak więc

$$f : X \xrightarrow{\sim} Y \iff f : X \xrightarrow{\ .\ } Y \wedge f : \underline{X} \hookrightarrow\!\!\!\!\rightarrow \underline{Y} \wedge f^{-1} : Y \xrightarrow{\ .\ } X.$$

Łatwo widać, że relacja izomorfizmu „$\simeq$” jest równoważnością w klasie $\mathrm{Ob}\, T$ wszystkich obiektów kategorii $\mathcal{T}$.

8.1.5. W klasie $\mathrm{Ob}\, T$ wszystkich obiektów kategorii $\mathcal{T}$ określamy porządek (częściowy):

$$X \prec Y \ :\Longleftrightarrow\ \underline{X} = \underline{Y} = E \ \ \wedge\ \ \mathrm{id}_E : Y \xrightarrow{\ .\ } X;$$

mówimy, że X jest *słabszy* od Y, Y jest *silniejszy* od X.

Na przykład dla systemów relacyjnych $X = (E,\alpha)$, $Y = (E,\beta)$: $X \prec Y \iff [\forall\, x,z \in E : (x,z) \in \beta \ \Rightarrow\ (x,z) \in \alpha] \iff \alpha \supset \beta$.

Dla przestrzeni pretopologicznych $X = (E,\alpha)$, $Y = (E,\beta)$: $X \prec Y \iff \alpha \subset \beta$.

8.1.6. Dla dwu kategorii zwyczajnych $\mathcal{T} = (T,\sigma)$, $\mathcal{T}' = (T',\sigma')$ mówimy, że $\mathcal{T}'$ jest *podkategorią* kategorii $\mathcal{T}$, co notujemy: $\mathcal{T}' \underset{\cdot}{\subset} \mathcal{T}$, gdy

1° $\mathrm{Ob}\, T' \subset \mathrm{Ob}\, T$ (równoważnie: $\forall\, A : T'(A) \subset T(A)$)

2° $\forall\, X,Y \in \mathrm{Ob}\, T' : \sigma'(X,Y) \subset \sigma(X,Y)$.

Mówimy, że $\mathcal{T}'$ jest *podkategorią pełną* kategorii $\mathcal{T}$, notujemy: $\mathcal{T}' \underset{\circ}{\subset} \mathcal{T}$, gdy warunek 2° zastąpimy mocniejszym:

$2^{\circ\circ}$ $\forall\, X,Y \in \mathrm{Ob}\, T' : \sigma'(X,Y) = \sigma(X,Y)$.

Podkategoria pełna $\mathcal{T}'$ kategorii $\mathcal{T}$ może być utożsamiana z klasą $K \subset \operatorname{Ob} T$ zamkniętą ze względu na izomorfizmy, to jest spełniającą warunek:

$$\forall\, X \in K, Y \in \operatorname{Ob} T : X \simeq Y \;\Rightarrow\; Y \in K,$$

i wówczas $K = \operatorname{Ob} \mathcal{T}'$. Klasę taką nazywamy też *niezmiennikiem* kategorii $\mathcal{T}$.

Na przykład, jeżeli $\mathcal{T}$ jest kategorią systemów relacyjnych, to

$$\mathrm{WOS} \underset{\circ}{\subset} \mathrm{LOS} \underset{\circ}{\subset} \mathrm{POS} \underset{\circ}{\subset} \mathcal{T},$$

gdzie odpowiednio POS, LOS i WOS są kategoriami posetów, zbiorów liniowo uporządkowanych (łańcuchów); zbiorów dobrze uporządkowanych i ich odwzorowań rosnących (w sensie słabym); również $\mathrm{Set} \underset{\circ}{\subset} \mathcal{T}$, $\mathrm{Set} \underset{\circ}{\subset} \mathrm{Pretop}$.

Jeżeli $\mathcal{T}$ jest kategorią grupoidów, to określamy podkategorie pełne:

$$\mathrm{Ab} \underset{\circ}{\subset} \mathrm{Gr} \underset{\circ}{\subset} \mathrm{Sgr}_1 \underset{\circ}{\subset} \mathcal{T}.$$

Kategoria Sgr_1 to kategoria *półgrup z jedynką*, czyli takich grupoidów $G = (A, (\varphi, a))$, w których działanie jest *łączne*, tzn. $\forall\, x, y, z \in A : \varphi(x, \varphi(y, z)) = \varphi(\varphi(x, y), z)$, oraz element wyróżniony $a \in A$ jest *neutralny* względem działania φ, tzn. $\forall\, x \in A : \varphi(a, x) = \varphi(x, a) = x$.

W dalszym ciągu termin *półgrupa* będzie oznaczał półgrupę z jedynką, chyba że postanowimy inaczej.

Zwyczajowo dla półgrup przyjmujemy *notację multyplikatywną*; dla półgrupy $G = (A, (\varphi, a))$ działanie φ oznaczamy jako mnożenie, $xy = x \cdot y = x \underset{G}{\cdot} y := \varphi(x, y)$, zaś element neutralny nazywamy jedynką, $1 = 1_G := a$.

Przykładowo, dla zbioru A mamy półgrupę odwzorowań A w siebie, $\operatorname{Map} A = (\operatorname{Map}(A, A), (\circ, \mathrm{id}_A))$.

Gr to ważna *kategoria grup*; półgrupę $G \in \mathrm{Sgr}_1$ nazywamy *grupą*, gdy każdy element jest w niej *odwracalny*, $\forall\, x \in G\; \exists\, y \in G : xy = yx = 1$.

Dla zbioru A mamy *grupę permutacji* A:

$$\operatorname{Perm} A := (\{\sigma \mid \sigma : A \hookrightarrow\!\!\!\!\twoheadrightarrow A\}, (\circ, \mathrm{id}_A)).$$

Ogólniej dla obiektu X ustalonej kategorii zwyczajnej mamy grupę *automorfizmów* $\operatorname{Aut} X = \{f : f : X \xrightarrow{\sim} X\}$ i półgrupę *endomorfizmów* $\operatorname{End} X = \{f \mid f : X \underset{\cdot}{\longrightarrow} X\}$.

Jeżeli dodatkowo zażądamy, żeby działanie w półgrupie było przemienne, to otrzymamy kategorię *półgrup przemiennych* lub *komutatywnych* Sgrc_1.

Opuszczając element neutralny, otrzymamy kategorię półgrup (bez jedynki) Sgr.

Grupę przemienną nazywamy też abelową (od nazwiska norweskiego matematyka N. H. Abela); ich kategorię oznaczamy Ab.

Tak więc $\mathrm{Ab} \underset{\circ}{\subset} \mathrm{Sgrc}_1 \underset{\circ}{\subset} \mathrm{Sgr}_1$, $\mathrm{Ab} \underset{\circ}{\subset} \mathrm{Gr}$.

Dla grup abelowych (i tylko dla takich) najczęściej używamy *notacji addytywnej*, oznaczając wynik działania jako $x + y$; zaś element neutralny jako 0.

8.1.7. Dla dwu kategorii zwyczajnych $\mathcal{T} = (T, \sigma)$ i $\mathcal{T}' = (T', \sigma')$ określamy ich *zestawienie* $\mathcal{T} \vartriangle \mathcal{T}'$ jako kategorię zwyczajną $\mathcal{T}'' = (T'', \sigma'')$ taką, że

1° $\forall\, A : T''(A) = T(A) \times T'(A)$

2° $\forall\, X = (A, (\alpha, \alpha')),\ Y = (B, (\beta, \beta')) \in \operatorname{Ob} T'' : \sigma''(X, Y) = \sigma((A, \alpha), (B, \beta)) \cap \sigma'((A, \alpha'), (B, \beta'))$.

Dla kategorii zwyczajnych łączenie operacji zestawiania i przechodzenia do podkategorii (na ogół pełnej) jest typowym sposobem otrzymywania złożonych struktur matematycznych.

Przykłady:

1. *Kategoria grup uporządkowanych* $\mathrm{OrdGr} \underset{\circ}{\subset} \mathrm{Ab} \vartriangle \mathrm{POS}$. Dla $G \in \mathrm{Ab} \vartriangle \mathrm{POS} : G \in \mathrm{OrdGr} :\Longleftrightarrow \forall\, x, y, z \in G : x \leqslant y \ \Rightarrow\ x + z \leqslant y + z.$
2. *Kategoria pierścieni (z jedynką)*: $\mathrm{Rin}_1 \underset{\circ}{\subset} \mathrm{Ab} \vartriangle \mathrm{Sgr}_1$; dla $R \in \mathrm{Ab} \vartriangle \mathrm{Sgr}_1$: $R \in \mathrm{Rin}_1 :\Longleftrightarrow \forall\, x, y, z \in R : (x + y)z = xz + yz \ \wedge\ z(x + y) = zx + zy.$

Dołączając postulat przemienności mnożenia, otrzymamy kategorię Rinc_1 *pierścieni przemiennych*.

8.1.8. *Funktorem zwyczajnym* z kategorii $\mathcal{T} = (T, \sigma)$ do kategorii $\mathcal{T}' = (T', \sigma')$ nazywany funkcję $F : \operatorname{Ob} T \to \operatorname{Ob} T'$ taką, że:

1° $\forall\, X \in \operatorname{Ob} T : \operatorname{set} F(X) = \operatorname{set} X$

2° $\forall\, X, Y \operatorname{Ob} T : \sigma(X, Y) \subset \sigma'(F(X), F(Y))$;

zapisujemy: $F : \mathcal{T} \xrightarrow[\cdot]{} \mathcal{T}'$.

Jeżeli w punkcie 2° zachodzi zawsze równość zamiast inkluzji, to mówimy, że funktor F jest *pełny*, co notujemy: $F : \mathcal{T} \xrightarrow[\circ]{} \mathcal{T}'$.

Na przykład, jeżeli $\mathcal{T}'' = \mathcal{T} \vartriangle \mathcal{T}'$, to mamy tzw. *funktory zapominające* $F : \mathcal{T}'' \xrightarrow[\cdot]{} \mathcal{T}$, $F' : \mathcal{T}'' \xrightarrow[\cdot]{} \mathcal{T}'$; $\forall\, X = (A, (\alpha, \alpha')) \in \mathcal{T}'' : F(X) = (A, \alpha),\ F'(X) = (A, \alpha')$.

Oczywiście, jeżeli $\mathcal{T}' \underset{\cdot}{\subset} \mathcal{T}$, to $\mathrm{id}_{\operatorname{Ob} T'} : \mathcal{T}' \xrightarrow[\cdot]{} \mathcal{T}$ ($\mathrm{id}_{\operatorname{Ob} T'} : \mathcal{T}' \xrightarrow[\circ]{} \mathcal{T}$, jeśli $\mathcal{T}' \underset{\circ}{\subset} \mathcal{T}$).

8.1.9. Dla dwu kategorii zwyczajnych $\mathcal{T}$ i $\mathcal{T}'$ mówimy, że funktor zwyczajny $F : \mathcal{T} \xrightarrow[\cdot]{} \mathcal{T}'$ ustala ich *równoważność*, co notujemy: $F : \mathcal{T} \xrightarrow{\sim} \mathcal{T}'$, gdy $F : \operatorname{Ob} T \hookrightarrow\!\!\!\!\rightarrow \operatorname{Ob} T'$ i $F^{-1} : \mathcal{T}' \xrightarrow[\cdot]{} \mathcal{T}$.

Kategorie takie możemy identyfikować, uwzględniając oczywiście odpowiedni funktor ustalający ich równoważność. Na przykład, piszemy $\mathcal{T} \vartriangle \mathcal{T}' \simeq \mathcal{T}' \vartriangle \mathcal{T}$, mając na myśli funktor F określony wzorem $F((A, (\alpha, \alpha')) = (A, (\alpha', \alpha))$.

Równoważność kategorii zwyczajnych $\mathcal{T}$ i $\mathcal{T}'$ ustala się zwykle przez wskazanie dwóch funktorów $F : \mathcal{T} \xrightarrow[\cdot]{} \mathcal{T}'$ i $G : \mathcal{T}' \xrightarrow[\cdot]{} \mathcal{T}$ takich, że $G \circ F \subset \mathrm{id}$ i $F \circ G \subset \mathrm{id}$, gdyż wówczas $F : \mathcal{T} \xrightarrow{\sim} \mathcal{T}'$ i $G = F^{-1}$.

Na przykład w rozdziale 4 w zadaniach 4.28 i 4.29 podano dwie równoważne definicje pojęcia kraty. W gruncie rzeczy uzyskaliśmy dwie równoważne kategorie zwyczajne krat i ich (homo)morfizmów:

1° Kategoria Latt (*lattices*) systemów algebraicznych $(X, \vee, \wedge)$ takich, że działania $\vee, \wedge : X^2 \to X$ są łączne, przemienne i spełniają postulat absorpcji:

$$\forall\, a, b \in X : a \vee (a \wedge b) = a \wedge (a \vee b) = a.$$

Morfizmami są homomorfizmy, czyli odwzorowania $f : X \to Y$ $(X, Y \in \mathrm{Latt})$ zgodne z działaniami, to jest takie, że:

$$(*) \qquad \forall\, a, b \in X : f(a \vee b) = f(a) \vee f(b),\ f(a \wedge b) = f(a) \wedge f(b).$$

2° Kategoria $\mathrm{Latt}' \underset{\cdot}{\subsetneq} \mathrm{POS}$; w kategorii tej obiektami są posety X, w których każdy dubleton $\{a, b\} \subset X$ ma kresy: $a \vee b = \sup\{a, b\}$, $a \wedge b = \inf\{a, b\}$, zaś morfizmami są odwzorowania rosnące (w sensie słabym) $f : X \to Y$ zachowujące kresy, czyli spełniające warunek (*).

Funktory ustalające równoważność $\mathrm{Latt} \underset{\overset{\cdot}{\longleftarrow}}{\overset{\cdot}{\longrightarrow}} \mathrm{Latt}'$ przedstawiono w zadaniu 4.29 (1°), 2°)). Mając na uwadze te funktory, kategorie Latt i Latt′ możemy identyfikować.

Zauważmy, że odwzorowanie rosnące na ogół nie zachowuje kresów (zadanie 4.26); zachodzą tylko nierówności $f(a \vee b) \geqslant f(a) \vee f(b)$, $f(a \wedge b) \leqslant f(a) \wedge f(b)$.
Tak więc $\neg\, \mathrm{Latt} \underset{\circ}{\subset} \mathrm{POS}$.

Podobnie w zadaniu 4.40 znajdziemy dwie równoważne wersje kategorii Bool *algebr Boole'a*.
Zwykle rozważamy kategorię Bool jako kategorię zwyczajną systemów algebraicznych postaci $(X, \vee, \wedge, ^\neg, 0, 1)$ takich, że działania $\vee, \wedge : X^2 \to X$ są łączne, przemienne, spełniające postulat absorpcji i wzajemnie rozdzielne (postulaty (1)–(4)), stałe $0, 1 \in X$ są elementami neutralnymi odpowiednio dla działań $\vee$, $\wedge$ ($a \vee 0 = a = a \wedge 1$, postulat (5)), zaś działanie $^\neg : X \to X$ jest tak zwanym dopełnieniem, to znaczy $a \vee a^\neg = 1$, $a \wedge a^\neg = 0$ (postulat (6)).

Morfizmami są odwzorowania $f : X \to Y$ $(X, Y \in \mathrm{Bool})$ zgodne ze wszystkimi działaniami, czyli tak zwane homomorfizmy.

Typowym przykładem algebry Boole'a jest algebra wszystkich podzbiorów ustalonego zbioru wraz ze zwykłymi działaniami teoriomnogościowymi.

Dowodzi się, że kategoria algebra Boole'a jest równoważna kategorii pierścieni przemiennych z idempotentnym mnożeniem (warunek $a^2 = a$), $\mathcal{R} \underset{\circ}{\subset} \mathrm{Rinc}_1$.
(Zadanie 2 – zakładamy znajomość elementarnych praw dla pierścieni i ich homomorfizmów).

8.1.10. Pojęcie kategorii zwyczajnej prowadzi do bardziej ogólnego pojęcia *kategorii* (abstrakcyjnej) jako klasy C, której elementy nazywamy *morfizmami* lub *strzałkami*, z działaniem częściowym $\cdot : C^2 \multimap\!\!\to C$ takim, że:

(C1) Oznaczając $\mathrm{Ob}\, C =$ *obiekty* kategorii $C :=$

$$\{a \in C \mid \forall\, x \in C : (ax \in C \ \Rightarrow\ ax = x) \wedge (xa \in C \ \Rightarrow\ xa = x)\}$$

mamy: $\forall\, x \in C\ \exists!\, a, b \in \mathrm{Ob}\, C : ax, xb \in C$.
Dla $x \in C$ jednoznacznie wyznaczone obiekty a, b takie, że $ax = x = xb$, nazywamy odpowiednio *dziedziną* i *kodziedziną* morfizmu x; notacja: $\mathrm{dom}\, x = a$, $\mathrm{cod}\, x = b$.

Dla $a, b \in \operatorname{Ob} C$ oznaczamy $\operatorname{Mor}(a,b) = \{x \in C \mid \operatorname{dom} x = a, \operatorname{cod} x = b\}$; piszemy też $x : a \to b$ lub $a \xrightarrow{x} b$, gdy $x \in \operatorname{Mor}(a,b)$.
(C2) $\forall\, x, y \in C : xy \in C \;\Rightarrow\; \operatorname{dom}(xy) = \operatorname{dom} x \wedge \operatorname{cod}(xy) = \operatorname{cod} y \wedge \operatorname{cod} x = \operatorname{dom} y$
(C3) $\forall\, x, y \in C : \operatorname{cod} x = \operatorname{dom} y \;\Rightarrow\; xy \in C$
(C4) $\forall\, x, y, z \in C : (xy)z = x(yz)$.

Dla kategorii zwyczajnej $\mathcal{T} = (T, \sigma)$, kładąc

$$\mathcal{C} = \{(X, f, Y) \mid X, Y \in \operatorname{Ob} T, f \in \sigma(X,Y)\}$$

i określając działanie częściowe $\cdot : \mathcal{C}^2 \xrightarrow{\circ} \mathcal{C}$ wzorem:

$$(X, f, Y) \cdot (Y, g, Z) = \begin{cases} (X, g \circ f, Z), & \text{gdy } Y = Y' \\ \mathbb{V}, & \text{w przeciwnym wypadku} \end{cases}$$

otrzymamy kategorię w powyższym sensie; klasę $\operatorname{Ob} \mathcal{C} = \{(X, \mathrm{id}_X, X) \mid X \in \operatorname{Ob} T\}$ możemy identyfikować z klasą $\operatorname{Ob} T$ obiektów kategorii $\mathcal{T}$.

W praktyce $\mathcal{T}$ i $\mathcal{C}$ identyfikujemy, używając tego samego symbolu, na przykład Gr dla kategorii grup.

8.1.11. Jeżeli dla klasy C i działania $\cdot : C^2 \xrightarrow{\circ} C$ przyjmiemy tylko postulaty (C1) i (C2), to otrzymamy pojęcie *grafu* (*multyplikatywnego*).

Dla dwu grafów C i C' odwzorowanie $f : C \to C'$ nazywamy *funktorem*, jeżeli

$$f(\operatorname{Ob} C) \subset \operatorname{Ob} C' \;\;\wedge\;\; \forall\, x, y \in C\; [xy \in C \;\Rightarrow\; f(xy) = f(x) f(y)];$$

notacja: $f : C \underset{\cdot}{\longrightarrow} C'$. Jeżeli $f : C \underset{\cdot}{\longrightarrow} C'$ i $x \in C$, to $f(\operatorname{dom} x) = \operatorname{dom} f(x)$ i $f(\operatorname{cod} x) = \operatorname{cod} f(x)$ $\langle$jeżeli np. $a = \operatorname{dom} x$, to $ax = x$, a więc $f(a)f(x) = f(x)$, i ponieważ $f(a) \in \operatorname{Ob} C'$, więc $f(a) = \operatorname{dom} f(x)\rangle$.

Graf C (i odpowiednio kategorię) nazywamy:
(1°) *lokalnie małym*, gdy $\forall\, a, b \in \operatorname{Ob} C : \operatorname{Mor}(a,b) \in \mathbb{V}$,
(2°) *małym*, gdy $C \in \mathbb{V}$.

Tak na przykład kategoria zwyczajna $\mathcal{C}$ jest lokalnie mała.

Możemy więc mówić o kategoriach zwyczajnych Graph grafów małych i Cat $\underset{\circ}{\subset}$ Graph kategorii małych i ich funktorów. Zauważmy, że Gr $\underset{\circ}{\subset}$ Sgr_1 $\underset{\circ}{\subset}$ Cat.

Graf mały S nazywamy też *schematem diagramowym* i w tej sytuacji, dla danej kategorii C, funktor $D : S \underset{\cdot}{\longrightarrow} C$ nazywamy też *diagramem* w C o schemacie S.

8.1.12. W dalszym ciągu tego rozdziału ustalamy kategorię zwyczajną $\mathcal{T} = (T, \sigma)$. Pojęcia, które można sformułować w odpowiadającej jej kategorii (abstrakcyjnej) $\mathcal{C}$, a więc bez korzystania z pojęcia przynależności elementu do zbioru, nazywamy *ogólnokategorialnymi*. Najważniejsze z nich jest pojęcie *uniwersalności*.

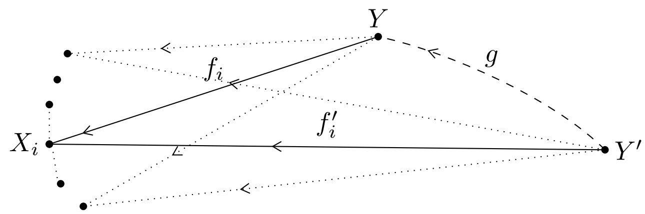
Dla rodziny $X : I \to \operatorname{Ob} T$, $I \in \mathbb{V}$ obiektów kategorii $\mathcal{T}$ *stożkiem projektywnym* nad X nazywamy parę (Y, f) taką, że:

$$Y \in \operatorname{Ob} X,\; f : I \to \mathbb{V},\; \forall\, i \in I\; (f_i : Y \underset{\cdot}{\longrightarrow} X_i);$$

obiekt Y nazywamy *wierzchołkiem* stożka – morfizm f_i to jego i-ta *projekcja*.
Ogół takich stożków oznaczamy $\operatorname{Con} X$.

Stożek $(Y, f) \in \operatorname{Con} X$ nazywany *produktem* rodziny X, gdy spełnia poniższy *warunek uniwersalności*:

(*) $$\forall\, (Y', f') \in \operatorname{Con} X\ \exists!\, g : Y' \longrightarrow Y\ \forall\, i \in I\ (f'_i = f_i \circ g).$$



Z warunku uniwersalności (*) wynika, że produkt rodziny X, jeżeli istnieje, to jest wyznaczony jednoznacznie z dokładnością do izomorfizmu; dokładniej, jeżeli (Y, f) i (Y', f') są dwoma produktami nad X i $g : Y' \to Y$ jest wyznaczonym jednoznacznie morfizmem takim, że $\forall\, i \in I : f'_i = f_i \circ g$, to $g : Y' \xrightarrow{\sim} Y$. $\langle (\exists!)\, h : Y \longrightarrow Y'\ \forall\, i \in I : f_i = f'_i \circ h$, a więc $f_i = f_i \circ g \circ h$, i z warunku (*) wynika, że $g \circ h = \mathrm{id}_Y$. Analogicznie $h \circ g = \mathrm{id}_{Y'}$, a więc $g : Y' \longrightarrow Y$, $h = g^{-1} \rangle$.

Jeżeli dla liczby kardynalnej α istnieje produkt każdej rodziny $X : I \to \operatorname{Ob} T$, gdzie $\operatorname{card} I = \alpha$, to mówimy, że kategoria $\mathcal{T}$ jest *z produktami w mocy* α. Mówimy, że kategoria $\mathcal{T}$ jest *z produktami*, jeżeli jest z produktami w każdej mocy, tzn. istnieje w niej produkt każdej rodziny obiektów.

8.1.13. Kategorii (abstrakcyjnej) $(C, \cdot)$ odpowiada *kategoria dualna* $(C, \circ)$, $\circ : C^2 \xrightarrow{\circ} C$, $x \circ y = yx$. Na mocy *zasady dualności* każdemu pojęciu i twierdzeniu ogólnokategorialnemu odpowiada twierdzenie i pojęcie dualne otrzymane przez mechaniczne „odwrócenie strzałek”, i wprowadzając takie pojęcia, wystarczy ograniczyć się do przedstawienia terminologii i oznaczeń.

I tak dla rodziny $X : I \to \operatorname{Ob} T$, $I \in \mathbb{V}$ obiektów kategorii $\mathcal{T}$ *stożkiem induktywnym* nad X będzie para (Y, f) taka, że $Y \in \operatorname{Ob} X$, $f : I \to \mathbb{V}$, $\forall\, i \in I\ (f_i : X_i \longrightarrow Y)$; stożek taki nazywamy *koproduktem* rodziny X, gdy spełnia (dualny) warunek uniwersalności.

8.1.14. Kategoria Set wszystkich zbiorów i ich odwzorowań dowolnych (zob. 8.1.3) jest z produktami i koproduktami. Dla rodziny zbiorów $X : I \to \mathbb{V}$, $I \in \mathbb{V}$ produktem jest para (Y, f), gdzie $Y = \{x : I \to \bigcup_{i \in I} X_i \mid \forall\, i \in I : x_i \in X_i\}$, oraz dla $i \in I$, $f_i : Y \to X_i$, $f_i(x) = x_i$; produkt taki nazywamy *iloczynem kartezjańskim* rodziny X, oznaczamy: $\prod X = \prod_{i \in I} X_i := Y$, $\mathrm{pr}_i = f_i$ (i-ta projekcja).

Koproduktem rodziny X jest para (Y, f), gdzie $Y = \{(x, i) \mid i \in I,\ x \in X_i\}$, oraz dla $i \in I$, $f_i : X_i \to Y$, $f_i(x) = (x, i)$; koprodukt ten nazywamy *sumą kartezjańską* rodziny X, oznaczamy: $\bigsqcup X = \bigsqcup_{i \in I} X_i := Y$, $\mathrm{in}_i = f_i$ (i-ta iniekcja).

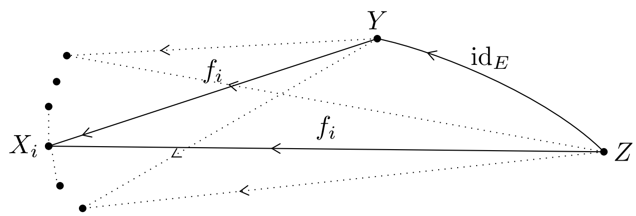
W przypadku rodziny skończonej, np. gdy $I = \{1, 2\}$ używamy standardowej notacji $X_1 \times X_2$, $X_1 \sqcup X_2$. $\langle$Sprawdzenie warunku uniwersalności w obu dualnych przypadkach sprowadza się do mechanicznego przeliczenia$\rangle$.

8.1.15. Dla rodziny obiektów $X : I \to \mathrm{Ob}\, T$, $I \in \mathbb{V}$ stożek projektywny (Y, f) nazywamy *początkowym* (pojęcie dualne: stożek induktywny *końcowy*), gdy jest spełniony poniższy *warunek początkowości*:

$$\forall\, Z \in \mathrm{Ob}\, T,\ g : \underline{Z} \to \underline{Y}\ [(\forall\, i \in I\ f_i \circ g : Z \underset{\cdot}{\longrightarrow} X_i)\ \Rightarrow\ g : Z \underset{\cdot}{\longrightarrow} Y]$$

(oczywiście pojęcia początkowości i końcowości nie są już ogólnokategorialne).

Jeżeli tak jest, to obiekt Y jest najsłabszy ze wszystkich obiektów $Z \in \mathrm{Ob}\, T$ o tym samym zbiorze podkładowym co Y; $\underline{Z} = \underline{Y} = E$ i takich, że $\forall\, i \in I : f_i : Z \underset{\cdot}{\longrightarrow} X_i$



$\langle$Istotnie, wówczas $f_i = f_i \circ \mathrm{id}_E : Z \underset{\cdot}{\longrightarrow} X_i$, $\forall\, i \in I$, a więc $\mathrm{id}_E : Z \underset{\cdot}{\longrightarrow} Y$, czyli $Y \prec Z\rangle$.

Tak więc, jeżeli na zbiorze E istnieje struktura $Y \in \mathrm{Ob}\, T$, $\underline{Y} = E$ taka, że stożek (Y, f) jest początkowy, to jest ona wyznaczona jednoznacznie – nazywamy ją *strukturą początkową indukowaną* na zbiorze E przez X i f.

8.1.16. Twierdzenie: Jeżeli $X : I \to \mathrm{Ob}\, T$, $I \in \mathbb{V}$, $E = \prod_{i \in I} \underline{X_i}$, $f : I \to \mathbb{V}$, $\forall\, i \in I$ $(f_i = \mathrm{pr}_i : E \to \underline{X_i})$, $Y \in \mathrm{Ob}\, T$, $\underline{Y} = E$ i (Y, f) jest stożkiem projektywnym początkowym nad X, to (Y, f) jest produktem rodziny X w kategorii $\mathcal{T}$.

$\langle$Jeżeli (Y', f') jest stożkiem projektywnym nad X i $g : Y' \to Y$ jest jedynym odwzorowaniem takim, że $\forall\, i \in I : f'_i = f_i \circ g$, to z warunku początkowości wynika, iż $g : Y' \underset{\cdot}{\longrightarrow} Y\rangle$.

Tak określony produkt nazywamy *zwyczajnym* i oznaczamy $\prod X$, $\prod_{\mathcal{T}} X$, $\prod_{i \in I} X_i$, $X_1 \times X_2$.
(Koprodukt *zwyczajny*, $\coprod X$, $\ldots$).

Tak więc, chcąc znaleźć produkt zwyczajny rodziny obiektów $X : I \to \mathrm{Ob}\, T$, należy:

1° W zbiorze wszystkich struktur na $\prod_{i \in I} \underline{X_i}$ takich, że wszystkie projekcje pr_i są morfizmami, znaleźć odpowiednią strukturę (najsłabszą).

2° Sprawdzić, czy struktura znaleziona w punkcie 1° jest początkowa.

8.1.17. Obiekt Y kategorii $\mathcal{T}$ nazywany *końcowym*, gdy jest produktem rodziny pustej, a więc spełnia warunek:

$$\forall\, Y' \in \mathrm{Ob}\, T\ \exists!\, f : Y' \underset{\cdot}{\longrightarrow} Y.$$

W kategorii Set produktem zwyczajnym rodziny pustej jest zbiór $\prod \varnothing = \{\varnothing\} = 1$; każdy zbiór jednoelementowy (singleton) jest obiektem końcowym. Koproduktem zwyczajnym rodziny pustej i jedynym obiektem początkowym jest zbiór pusty.

Jeżeli w jakiejś kategorii istnieje obiekt, który jest jednocześnie obiektem początkowym i końcowym, to nazywamy go *obiektem zerowym*; w kategorii grup Gr takim obiektem jest każda grupa jednoelementowa (trywialna).

8.1.18. Stożek projektywny jednoelementowy możemy identyfikować z morfizmem $f : X \underset{\cdot}{\longrightarrow} Y$ $(X, Y \in \operatorname{Ob} T)$. Warunek początkowości oznacza w tym przypadku, że:

$$\forall\, Z \in \operatorname{Ob} T,\ g : Z \to X\ [f \circ g : Z \underset{\cdot}{\longrightarrow} Y \ \Rightarrow\ g : Z \underset{\cdot}{\longrightarrow} X];$$

nasz morfizm nazywamy wówczas *początkowym* (pojęcie dualne: morfizm *końcowy*).

8.1.19. Dla $X, Y \in \operatorname{Ob} T$ mówimy, że Y jest *podobiektem* X, co notujemy: $Y \underset{\cdot}{\subset} X$, $Y \underset{\mathcal{T}}{\subset} X$, gdy $Y \subset X$ oraz id_Y jest morfizmem początkowym Y w X, to jest $\mathrm{id}_Y : Y \underset{\cdot}{\longrightarrow} X$ i $\forall\, Z \in \operatorname{Ob} T,\ f : Z \to Y\ [f : Z \underset{\cdot}{\longrightarrow} X \ \Rightarrow\ f : Z \underset{\cdot}{\longrightarrow} Y]$.

Podzbiór $E \subset X$ nazywany *zgodnym* z X, notacja: $E \underset{\cdot}{\subset} X$, gdy istnieje podobiekt $Y \underset{\cdot}{\subset} X$ o zbiorze podkładowym $\underline{Y} = E$; podobiekt taki istnieje wówczas dokładnie jeden – nazywamy go podobiektem indukowany na E przez X (w kategorii $\mathcal{T}$) i oznaczamy $X|E$ lub po prostu E. Dopuszczamy też dwuznaczność (zdając się na kontekst), gdy oznaczamy symbolem $\operatorname{Sub}(X)$ ogół podobiektów obiektu X i ogół podzbiorów zbioru $\underline{X}$ zgodnych z X.

Dla injekcji $f : X \hookrightarrow Y$ $(X, Y \in \operatorname{Ob} T)$ równoważne są warunki:

(i) $\operatorname{Im} f \underset{\cdot}{\subset} Y \ \wedge\ f : X \xrightarrow{\sim} Y|\operatorname{Im} f$

(ii) f – morfizm początkowy X w Y.

Morfizm injektywny spełniający któryś z tych warunków nazywany *zanurzeniem* lub *immersją* X w Y; notacja: $f : X \overset{\sim}{\hookrightarrow} Y$.

8.1.20. Pojęciem dualnym do pojęcia podobiektu jest pojęcie obiektu ilorazowego. Dla $X, Y \in \operatorname{Ob} T$ mówimy, że Y jest *obiektem ilorazowym* lub *faktorobiektem* obiektu X (konkretnie – grupą ilorazową, przestrzenią ilorazową, itp.), gdy $\underline{Y} = \underline{X}/R$ dla pewnej (jednoznacznie wyzaczonej) równoważności R w zbiorze $\underline{X}$ i surjekcja naturalna $\mathrm{nat}_R : \underline{X} \twoheadrightarrow \underline{Y}$ jest morfizmem końcowym X w Y.

Mówimy, że równoważność R w zbiorze $\underline{X}$ jest *zgodna* z X lub że jest *kongruencją* w X, gdy istnieje obiekt ilorazowy Y obiektu X, dla którego: $\underline{Y} = \underline{X}/R$; obiekt taki istnieje wówczas dokładnie jeden – nazywamy go *ilorazem* lub *obiektem ilorazowym* X przez R (w kategorii $\mathcal{T}$) i oznaczamy X/R.

Ogół kongruencji w X oznaczamy $\operatorname{Congr}(X)$, dokładniej $\operatorname{Congr}_{\mathcal{T}}(X)$.

Jeżeli f jest surjektywnym morfizmem końcowym X na Y $(X, Y \in \operatorname{Ob} T)$, to $\ker f \in \operatorname{Congr}(X)$, gdyż w rozkładzie kanonicznym funkcji f (zadanie 4.5)

$$\begin{tikzcd} X \arrow[r, two heads, "f", "\cdot"'] \arrow[d, two heads, "\mathrm{nat}"'] & Y \\ Z = X/\ker f \arrow[ur, hook, two heads, "g"'] & \end{tikzcd}$$

bijekcja odwrotna do bijekcji kanonicznej g przenosi jednoznacznie strukturę z obiektu Y na zbiór $X/\ker f$; otrzymujemy więc $Z \in \operatorname{Ob} T$ taki, że $\underline{Z} = \underline{X}/\ker f$ oraz $g : Z \xrightarrow{\sim} Y$, i wówczas $Z = X/\ker f$ $\quad\langle$gdyż $\mathrm{nat} = g^{-1} \circ f$ jest morfizmem końcowym jako złożenie dwóch morfizmów końcowych (izomorfizm jest morfizmem końcowym)$\rangle$.

Tak więc w kategorii zwyczajnej *z końcowością surjekcji* (morfizmy surjektywne są końcowe) obrazami danego obiektu przez morfizmy surjektywne są – z dokładnością do naturalnego izomorfizmu – obiekty ilorazowe tego obiektu.

8.1.21. Dla obiektu X kategorii zwyczajnej $\mathcal{T} = (T, \sigma)$ podzbiór $A \subset X$ nazywamy *generującym*, gdy $\forall\, Y \underset{\cdot}{\subset} X$ $(A \subset Y \;\Rightarrow\; Y = X)$; ogół takich podzbiorów oznaczamy $\mathcal{G}(X)$. Oczywiście $\underline{X} \in \mathcal{G}(X)$ i $\mathcal{G}(X) \ni A \subset B \subset X \;\Rightarrow\; B \in \mathcal{G}(X)$.

Mówimy, że obiekt X jest *skończenie generowany*, gdy $\mathcal{G}(X) \cap \mathrm{Fin} \neq \varnothing$. Elementy zbioru generującego (ustalonego) nazywamy zwyczajowo *generatorami* obiektu X.

8.1.22. O kategorii zwyczajnej $\mathcal{T}$ mówimy, że jest *z multyplikatywnością podobiektów*, gdy

$$\forall\, X \in \operatorname{Ob} T,\ \varnothing \neq \mathcal{A} \subset \operatorname{Sub}(X) : \bigcap \mathcal{A} \underset{\cdot}{\subset} X;$$

jeżeli tak jest, to dla $X \in \operatorname{Ob} T$ i $A \subset X$ oznaczamy przez A^- lub $\langle A \rangle$, dokładniej $\langle A \rangle_{X, \mathcal{T}}$, podobiekt $\bigcap \{B \in \operatorname{Sub}(X) \mid A \subset B\}$. A^- jest najmniejszym podobiektem X zawierającym zbiór A; $A \in \mathcal{G}(A^-)$; mówimy, że A^- jest *podobiektem generowanym przez* A.

Operacja przejścia od A do A^- jest operacją domknięcia w X (tzn. $\forall\, A, B \underset{\cdot}{\subset} X$: $A \subset A^-$, $A^{--} = A^-$, $A \subset B \;\Rightarrow\; A^- \subset B^-$, zob. zadania 4.17 i 4.18).

Jeżeli jeszcze kategoria $\mathcal{T}$ jest *z obrazami* i *z przeciwobrazami*, tzn.

$$\forall\, X, Y \in \operatorname{Ob} T,\ f : X \xrightarrow{\cdot} Y,\ A \underset{\cdot}{\subset} X,\ B \underset{\cdot}{\subset} Y\ [f(A) \underset{\cdot}{\subset} Y,\ f^{-1}(B) \underset{\cdot}{\subset} X],$$

to dla $f : X \xrightarrow{\cdot} Y$ i $A \subset X$:

$$f(A)^- = f(A^-)$$

$\langle\subset)$ $A \subset A^-$, a więc $f(A) \subset f(A^-) \underset{\cdot}{\subset} Y$, skąd $f(A)^- \subset f(A^-)$.
$\supset)$ $f(A) \subset f(A)^-$, a więc $A \subset f^{-1}(f(A)) \subset f^{-1}(f(A)^-)$, $A^- \subset f^{-1}(f(A)^-)$, $f(A^-) \subset f(f^{-1}(f(A)^-)) \subset f(A)^-\rangle$.

8.1.23. Podzbiór A obiektu X nazywamy *bazowym* lub *bazą* X, gdy

$$\forall\, Y \in \operatorname{Ob} T,\ \varphi : A \to Y\ \exists!\, \varphi \subset f : X \underset{\cdot}{\longrightarrow} Y$$

(każde odwzorowanie tego zbioru w dowolny obiekt naszej kategorii ma dokładnie jedno rozszerzenie do morfizmu); ogół takich podzbiorów oznaczamy $\mathcal{B}(X)$. Obiekt X nazywamy *wolnym*, gdy $\mathcal{B}(X) \neq \varnothing$.

Obiekt wolny jest wyznaczony przez swoją bazę jednoznacznie z dokładnością do izomorfizmu identycznościowego na bazie. Dokładniej, jeżeli $X, Y \in \operatorname{Ob} T$, $A \in \mathcal{B}(X)$, $B \in \mathcal{B}(Y)$, $\varphi : A \hookrightarrow\!\!\!\!\rightarrow B$, $\varphi \subset f : X \underset{\cdot}{\longrightarrow} Y$, to $f : X \xrightarrow{\sim} Y$.

$\langle \exists!)\, \varphi^{-1} \subset g : Y \underset{\cdot}{\longrightarrow} X$, $\varphi^{-1} \circ \varphi = \mathrm{id}_A \subset g \circ f : X \underset{\cdot}{\longrightarrow} X$; ale również $\mathrm{id}_A \subset \mathrm{id}_X : X \underset{\cdot}{\longrightarrow} X$, a więc $g \circ f = \mathrm{id}_X$. Analogicznie $f \circ g = \mathrm{id}_Y$. Zatem $f : X \xrightarrow{\sim} Y$, $g = f^{-1} \rangle$.

Mówimy, że kategoria $\mathcal{T}$ jest *z obiektami wolnymi*, jeśli $\forall\, A\ \exists\, X \in \operatorname{Ob} T : A \in \mathcal{B}(X)$.

8.1.24. Oddzielając istnienie od jednoznaczności, otrzymamy dla $X \in \operatorname{Ob} T$:

$$\mathcal{B}(X) = \mathcal{I}(X) \cap \mathcal{D}(X), \quad \text{gdzie}$$

$\mathcal{I}(X) := \{A \subset X \mid \forall\, Y \in \operatorname{Ob} T,\ \varphi : A \to Y\ \exists \varphi \subset f : X \underset{\cdot}{\longrightarrow} Y\}$ = podzbiory *niezależne* w X,
$\mathcal{D}(X) := \{A \subset X \mid \forall\, Y \in \operatorname{Ob} T,\ f, g : X \underset{\cdot}{\longrightarrow} Y\ (f|A = g|A \ \Rightarrow\ f = g\}$ = podzbiory *gęste* w X.

Z definicji wynika wprost, że nadzbiór zbioru gęstego jest gęsty i niepusty, podzbiór zbioru niezależnego jest niezależny.

8.1.25. Powyższe definicje (8.1.23–24) można sformułować ogólniej, mówiąc, zamiast o podzbiorach, o rodzinach elementów obiektu X.

Na przykład dla $X \in \operatorname{Ob} T$, $a : I \to X$, $I \in \mathbb{V}$ mówimy, że rodzina a jest *niezależna w* X, gdy

$$\forall\, Y \in \operatorname{Ob} T,\ \varphi : I \to Y\ \exists\, f : X \underset{\cdot}{\longrightarrow} Y\ (\varphi = f \circ a)$$

$$\begin{tikzcd} I \arrow[r, "a"] \arrow[d, "\varphi"'] & X \arrow[dl, "f"] \\ Y & \end{tikzcd}$$

Uogólnienie to jest pozorne, gdyż jeżeli kategoria $\mathcal{T}$ jest *nietrywialna*, tzn. $\exists\, Y \in \operatorname{Ob} T : \operatorname{card} Y \geqslant 2$, to rodzina niezależna $a : I \to X$ elementów obiektu $X \in \operatorname{Ob} T$ jest injektywna; $a : I \hookrightarrow X$.

$\langle$HP: $\exists)\, i, j \in I : i \neq j, a_i = a_j$. $\exists)\, Y \in \operatorname{Ob} T : \operatorname{card} Y \geqslant 2$. $\exists)\, \varphi : I \to Y$, $\varphi(i) \neq \varphi(j)$. $\exists)\, f : X \underset{\cdot}{\longrightarrow} Y$, $\varphi = f \circ a$. Wówczas $\varphi(i) = f(a_i) = f(a_j) = \varphi(j) \lightning \rangle$.

Zatem dla nietrywialnej kategorii zwyczajnej $\mathcal{T}$ niezależność (gęstość, bazowość) rodziny $a : I \to X$ ($I \in \mathbb{V}$) elementów obiektu X jest równoważna niezależności (gęstości, bazowości) podzbioru $\operatorname{Im} a = a(I)$ zbioru X.

8.1.26. Jeżeli kategoria $\mathcal{T}$ jest nietrywialna, to baza obiektu wolnego X jest maksymalnym podzbiorem niezależnym i minimalnym podzbiorem gęstym, to znaczy:

$$A \subset B \subset C \subset X,\ B \in \mathcal{B}(X),\ A \in \mathcal{D}(X),\ C \in \mathcal{I}(X) \implies A = B = C.$$

$\langle \exists)\, Y \in \operatorname{Ob} T : \operatorname{card} Y \geqslant 2.$
HP: $A \subsetneq C$.
$\exists)\, \varphi, \psi : C \to Y,\ \varphi|A = \psi|A.\ \varphi \neq \psi.$
$\exists)\, \varphi \subset f : X \longrightarrow Y,\ \exists)\, \psi \subset g : X \longrightarrow Y.$
Wówczas $f \neq g$, ale $f|A = \varphi|A = \psi|A = g|A$, a więc $f = g$ ↯$\rangle$.

8.1.27. W dowolnej kategorii zwyczajnej $\mathcal{T} = (T, \sigma)$ baza obiektu wolnego jest podzbiorem generującym:

$$\forall\, X \in \operatorname{Ob} T : \mathcal{B}(X) \subset \mathcal{G}(X).$$

$\langle$HP: $\exists)\, X \in \operatorname{Ob} T,\ B \in \mathcal{B}(X) \setminus \mathcal{G}(X)$.
$\exists)\, B \subset Y \subset X,\ Y \subsetneq X,\ \exists!)\, \mathrm{id}_B \subset f : X \longrightarrow Y$. Wówczas $f : X \longrightarrow X$. Ale również $\mathrm{id}_B \subset \mathrm{id}_X : X \longrightarrow X$, a więc $f = \mathrm{id}_X$, skąd $\operatorname{Im} f = X \subset Y$ ↯$\rangle$.

8.1.28. Będziemy mówili, że kategoria $\mathcal{T}$ jest *z jądrami par morfizmów*, gdy dla dowolnych $X, Y \in \operatorname{Ob} T$ i dwóch morfizmów $f, g : X \longrightarrow Y$

$$\operatorname{Ker}(f, g) := \{x \in X \mid f(x) = g(x)\} \subset X.$$

W kategorii z jądrami par morfizmów podzbiór generujący jest gęsty;

$$\forall\, X \in \operatorname{Ob} T : \mathcal{G}(X) \subset \mathcal{D}(X)$$

$\langle$HP: $\exists)\, A \in \mathcal{G}(X) \setminus \mathcal{D}(X)$.
Wówczas $\exists)\, Y \in \operatorname{Ob} T;\ f, g : X \longrightarrow Y,\ f|A = g|A,\ f \neq g.$
$A \subset \operatorname{Ker}(f, g) \subset X,\ \operatorname{Ker}(f, g) = X,\ f = g$ ↯$\rangle$.

Zatem w kategorii z jądrami par morfizmów

$$\forall\, X \in \operatorname{Ob} T : \mathcal{B}(X) = \mathcal{I}(X) \cap \mathcal{G}(X)$$

$\langle \mathcal{B}(X) \subset \mathcal{I}(X) \cap \mathcal{D}(X) \cap \mathcal{G}(X) \subset \mathcal{I}(X) \cap \mathcal{D}(X) = \mathcal{B}(X) \rangle$.

W związku z tym w takiej kategorii bazę obiektu wolnego nazywamy też zbiorem *wolnych* (lub *niezależnych*) generatorów.

8.1.29. Jeżeli kategoria z jądrami par morfizmów jest nietrywialna, to baza obiektu wolnego jest minimalnym zbiorem generującym.

$\langle$HP: $\exists)\, A \in \mathcal{G}(X),\ A \subsetneq B \in \mathcal{B}(X)$. Wówczas $B \in \mathcal{G}(X)$ $\langle$8.1.27$\rangle$ i $A \in \mathcal{D}(X)$ $\langle$8.1.28$\rangle$, a więc według 8.1.26 $A = B$ ↯$\rangle$.

8.1.30. Przez analogię do algebry uniwersalnej (zob. rozdz. 9) teorię kategorii zwyczajnych, czyli ogólną teorię struktur matematycznych, można by nazwać *matematyką uniwersalną*. Pozwala ona uwolnić się od rozpatrywania w konkretnych przypadkach (grupy, pierścienie, przestrzenie topologiczne itp.) różnych podstawowych prawidłowości, które zazwyczaj są w takim ogólnym ujęciu dosyć proste i łatwe do udowodnienia (np. zgodność obrazu z generowaniem podobiektu lub zgodność produktu z podobiektami – por. komentarz do zadania 17), umożliwiając skupienie się na tym, co jest istotne w danej teorii. Dochodzi do tego uporządkowanie i usystematyzowanie podstawowego aparatu pojęciowego.

Niektóre z wyżej wspomnianych prawidłowości są jednak trudniejsze do udowodnienia.

Na przykład operację domknięcia $\{A \mapsto A^- \mid A \subset X\}$ w zbiorze X nazywamy *algebraiczną*, gdy spełnia warunek:

$$\forall\, A \subset X,\ x \in A^-\ \exists\, B \subset A : |B| < \omega \quad \wedge \quad x \in B^-.$$

(Nazwę tę usprawiedliwia twierdzenie Schmidta mówiące, że operacja domknięcia $\varphi : \mathcal{P}X \to \mathcal{P}X$ w zbiorze X jest algebraiczna wtedy i tylko wtedy, gdy istnieje algebra ogólna (X, α) o podkładzie X, dla której φ jest operacją przejścia od podzbioru do podalgebry generowanej – zob. rozdział 9, zadanie 3).

Kategorię zwyczajną $\mathcal{T}$ nazwijmy *algebraiczną*, gdy jest nietrywialna, z jądrami par morfizmów, z multyplikatywnością podobiektów i taka, że dla dowolnego obiektu X operacja przejścia od podzbioru $A \subset X$ do podobiektu generowanego $A^- \underset{\cdot}{\subset} X$ jest algebraiczna.

Ważne twierdzenie głosi, że w takiej kategorii obiekt z bazą nieskończoną ma wszystkie bazy równoliczne:

$$X \in \operatorname{Ob} T,\ B \in \mathcal{B}(X),\ |B| \geqslant \omega \implies \forall\, A \in \mathcal{B}(X) : |A| = |B|.$$

$\langle$Zadanie 22$\rangle$.

Jeżeli dodatkowo założymy, że w kategorii algebraicznej $\mathcal{T} = (T, \sigma)$ istnieje obiekt Z skończony i nietrywialny; $2 \leqslant |Z| = n < \omega$, to wszystkie bazy obiektu wolnego X kategorii $\mathcal{T}$ są równoliczne – ich wspólną moc nazywamy *rangą* X.

Istotnie, jeżeli obiekt X ma bazę skończoną A, to na mocy powyższego twierdzenia każda inna baza $B \in \mathcal{B}(X)$ jest skończona, i wówczas $|\operatorname{Map}(B, Z)| = |\sigma(X, Z)|$ $\langle \{f \mapsto f|B \dots\} : \sigma(X, Z) \hookrightarrow\!\!\!\!\rightarrow \operatorname{Map}(B, Z) \rangle$.

Analogicznie $|\operatorname{Map}(A, Z)| = |\sigma(X, Z)|$, a więc $|\operatorname{Map}(A, Z)| = |\operatorname{Map}(B, Z)|$, $n^{|A|} = n^{|B|}$, $|A| = |B|$.

Sytuacja taka ma miejsce dla kategorii algebraicznych: Sgr_1, Gr, Ab, Rin_1, Rinc_1 itp. (ale np. nie dla kategorii Vect_K przestrzeni wektorowych nad ciałem nieskończonym K; teza o równoliczności baz też jest w tym wypadku prawdziwa, ale w dowodzie trzeba zastosować np. tzw. mechanizm wymiany).

Na tego rodzaju prawidłowościach zasadza się głównie „siła redukująca” matematyki uniwersalnej.

8.2. Tematy

1. Udowodnić, że dla kategorii zwyczajnej $\mathcal{T} = (T, \sigma)$ poniższe dwa warunki są równoważne:

(i) morfizmy bijektywne są izomorfizmami
(ii) $\forall\, X, Y \in \operatorname{Ob} T : X \prec Y \;\Rightarrow\; X = Y$.

Podać przykłady.

2. Określamy kategorię pierścieni boolowskich $\mathcal{R} \underset{\circ}{\subset} \mathrm{Rinc}_1$; dla $X \in \mathrm{Rinc}_1$:

$$X \in \mathcal{R} \iff \forall\, a \in X : a^2 = a.$$

Następnie określamy funkctory zwyczajne:

$$\mathrm{Bool} \underset{G\,\cdot}{\overset{F}{\underset{\longleftarrow}{\overset{\cdot}{\longrightarrow}}}} \mathcal{R}.$$

(i) Dla $\tilde{X} = (X, \vee, \wedge, {}^\neg, 0, 1)$

$$F(\tilde{X}) = (X, +, \cdot, 0, 1),$$

gdzie dla $a, b \in X$:

$$a + b = (a \wedge b^\neg) \vee (a^\neg \wedge b), \qquad a \cdot b = a \wedge b.$$

(ii) Dla $\tilde{X} = (X, +, \cdot, 0, 1) \in \mathcal{R}$

$$G(\tilde{X}) = (X, \vee, \wedge, {}^\neg, 0, 1),$$

gdzie dla $a, b \in X$:

$$a \vee b = a + b + ab, \qquad a \wedge b = ab, \qquad a^\neg = a + 1.$$

Udowodnić, że funktory F i G są dobrze określone i ustalają równoważność kategorii Bool i $\mathcal{R}$.

3. Wykazać, że klasa $\mathcal{C}$ z działaniem częściowym $\cdot : C^2 \multimap C$, jest kategorią wtt, gdy dla każdych $x, y, z \in C$, oznaczając

$$U_l = \{a \in C \mid \forall\, x \in C : ax \in C \;\Rightarrow\; ax = x\} \qquad (\textit{jedności lewostronne}),$$
$$U_r = \{b \in C \mid \forall\, x \in C : xb \in C \;\Rightarrow\; xb = x\} \qquad (\textit{jedności prawostronne}),$$

zachodzi:

(C1') $\exists\, a \in U_l,\ b \in U_r : ax, xb \in C$
(C2') $xy, yz \in C \;\Rightarrow\; (xy)z = x(yz) \in C$
(C3') $(xy)z \in C \;\Rightarrow\; yz \in C$
(C4') $x(yz) \in C \;\Rightarrow\; xy \in C$.

4. Morfizm $x : a \to b$ w kategorii C nazywamy:

(i) *monomorfizmem* lub *morfizmem końcowo skracalnym*, gdy

$$\forall\, y, z \in C : yx = zx \in C \;\Rightarrow\; y = z;$$

ich ogół oznaczamy $\operatorname{Mono} C = \operatorname{Mono}$ (literę C tu i w innych oznaczeniach tego rodzaju opuszczamy, gdy wiadomo, o jaką kategorię chodzi),

(ii) *epimorfizmem* lub *morfizmem początkowo skracalnym*, gdy

$$\forall\, y, z \in C : xy = xz \in C \;\Rightarrow\; y = z; \qquad \text{ich ogół: Epi},$$

(iii) *morfizmem regularnym* lub *skracalnym*, gdy

$$x \in \operatorname{Reg} := \operatorname{Mono} \cap \operatorname{Epi};$$

(iv) *sekcją* lub *morfizmem końcowo odwracalnym*, gdy

$$\exists\, u \in C : xu = a; \qquad \text{ich ogół: Sect},$$

(v) *retrakcją* lub *morfizmem początkowo odwracalnym*, gdy

$$\exists\, v \in C : vx = b; \qquad \text{ich ogół: Retr},$$

(vi) *izomorfizmem* lub *morfizmem odwracalnym*, gdy

$$\exists\, w \in C : xw = a, wx = b; \qquad \text{ich ogół: Iso}\,.$$

Wykazać, że (formuły dualne opuszczamy):

1) $\displaystyle\mathop{\forall\, x, y \in C}_{\operatorname{cod} x = \operatorname{dom} y} \quad (x, y \in \operatorname{Mono} \Rightarrow xy \in \operatorname{Mono} \Rightarrow x \in \operatorname{Mono})$
2) $\operatorname{Sect} \subset \operatorname{Mono}$, $\displaystyle\mathop{\forall\, x, y \in C}_{\operatorname{cod} x = \operatorname{dom} y} \quad (x, y \in \operatorname{Sect} \Rightarrow xy \in \operatorname{Sect} \Rightarrow y \in \operatorname{Sect})$
3) Jeżeli dla $u, v \in C : xu = a$, $vx = b$, to $u = v$, a więc $\operatorname{Iso} = \operatorname{Sect} \cap \operatorname{Retr}$. Dla $x \in \operatorname{Iso}$ jedyny izomorfizm $w \in C$ taki, że $xw = a$ i $wx = b$ nazywamy *odwrotnym* do x i oznaczamy $x^{-1} = w$; wówczas $(x^{-1})^{-1} = x$ i $\displaystyle\mathop{\forall\, x, y \in \operatorname{Iso}}_{\operatorname{cod} x = \operatorname{dom} y} (xy)^{-1} = y^{-1}x^{-1}$
4) $\operatorname{Mono} \cap \operatorname{Retr} = \operatorname{Iso}$.

5. Oznaczmy dla kategorii zwyczajnej $\mathcal{T} = (T, \sigma)$ symbolami Inj, Sur, Bij klasy morfizmów odpowiednio injektywnych, surjektywnych i bijektywnych. Wykazać, że:

(i) $\operatorname{Sect} \subset \operatorname{Inj} \subset \operatorname{Mono}$
(ii) $\operatorname{Retr} \subset \operatorname{Sur} \subset \operatorname{Epi}$
(iii) $\operatorname{Iso} \subset \operatorname{Bij} \subset \operatorname{Reg}$.

6. Zachowując oznaczenia z zadania 5 wykazać, że dla kategorii Set wszystkich zbiorów i ich odwzorowań dowolnych:

(i) $\operatorname{Sect} \subsetneq \operatorname{Inj} = \operatorname{Mono}$
(ii) $\operatorname{Retr} = \operatorname{Sur} = \operatorname{Epi}$
(iii) $\operatorname{Iso} = \operatorname{Bij} = \operatorname{Reg}$.

7. Niech C będzie kategorią z obiektem zerowym 0 (8.1.17).
Dla $a, b \in \operatorname{Ob} C$ niech $\omega_{ab} = uv$, gdzie $u : a \to 0$, $v : 0 \to b$. Udowodnić, że morfizm ω_{ab} nie zależy od wyboru obiektu zerowego – nazywamy go *morfizmem zerowym* z a do b.

8. Udowodnić, że w kategorii C z obiektem zerowym każda projekcja w produkcie jest retrakcją (morfizmem początkowo odwracalnym).

9*. Typowym przykładem kategorii z obiektem zerowym jest kategoria grup Gr. Każda grupa trywialna (jednoelementowa) jest takim obiektem. W tym zadaniu zakładamy znajomość podstawowych faktów z kategorii grup i kategorii $\mathrm{Top} \underset{\circ}{\subsetneq} \mathrm{Pretop}$ przestrzeni topologicznych. Zakładamy, że dysponujemy funktorem $H : \mathrm{Top} \underset{\cdot}{\longrightarrow} \mathrm{Gr}$ takim, że dla kuli $K = \{x \in \mathbb{R}^3 \mid |x| = 1\}$ i jej brzegu (sfery) $S = \{x \in \mathbb{R}^3 \mid |x| = 1\}$ grupa $H(K)$ jest trywialna, natomiast grupa $H(S)$ jest nietrywialna (H to *funktor homologii*, może on wychodzić z jakiejś podkategorii $\mathcal{T} \underset{\cdot}{\subsetneq} \mathrm{Top}$ i takiej, że $K, S \in \mathcal{T}$). Wykazać, że:

(i) Nie istnieje retrakcja (ciągła) $r : K \to S$.

(ii) Każde odwzorowanie ciągłe $f : K \to K$ ma punkt stały (*Twierdzenie Brouwera o punkcie stałym* – ogólnie w $\mathbb{R}^n$).

10*. W tym zadaniu będziemy konsekwentnie oznaczać przez af wartość f na argumencie a; $af := f(a)$. Tak np. dla

$$f : A \to \mathrm{Map}(B, C),\ a \in A,\ b \in B : b(af) = (f(a))(b) \in C.$$

Jeżeli G jest grafem, C – kategorią, to dla funktorów $f, g : G \underset{\cdot}{\longrightarrow} C$ *transformacją naturalną* f w g nazywamy odwzorowanie $\varphi : \operatorname{Ob} G \to C$ takie, że dla obiektu $a \in \operatorname{Ob} G$; $a\varphi : af \to ag$ oraz dla $G \ni x : a \to b$ kwadrat

$$\begin{tikzcd} af \arrow[r, "a\varphi"] \arrow[d, "xf"'] & ag \arrow[d, "xg"] \\ bf \arrow[r, "b\varphi"'] & bg \end{tikzcd}$$

jest przemienny, tzn. $a\varphi \cdot xg = xf \cdot b\varphi$.

Notacja: $\varphi : f \underset{\cdot}{\longrightarrow} g$.

Ustalmy kategorię lokalnie małą C ($\forall\, a, b \in \operatorname{Ob} C : \mathrm{Mor}(a, b) \in \mathbb{V}$):

(i) Każdemu obiektowi $p \in \operatorname{Ob} C$ przyporządkowujemy odwzorowanie $\overrightarrow{p} : C \to \mathrm{Set}$, kładąc dla $C \ni x : a \to b$

$$x\overrightarrow{p} : \mathrm{Mor}(p, a) \to \mathrm{Mor}(p, b), \quad \forall\, y \in \mathrm{Mor}(p, a) : y(x\overrightarrow{p}) = yx.$$

Wykazać, że $\overrightarrow{p}$ jest funktorem, $\overrightarrow{p} : C \underset{\cdot}{\longrightarrow} \mathrm{Set}$ (dla $a \in \operatorname{Ob} C : a\overrightarrow{p} = \mathrm{Mor}(p, a)$). Nazywamy go *funktorem głównym* C w Set indukowanym przez obiekt p.

(ii) Jeśli mamy dany obiekt $p \in \operatorname{Ob} C$, funktor $f : C \to \mathrm{Set}$ i punkt $t \in pf$, określamy odwzorowanie $\widehat{t} : \operatorname{Ob} C \to \mathrm{Set}$, kładąc dla $a \in \operatorname{Ob} C$,

$$a\widehat{t} : a\overrightarrow{p} \to af, \quad \forall\, y \in a\overrightarrow{p} = \mathrm{Mor}(p, a) : y(a\widehat{t}) = t(yf) \in af.$$

Sprawdzić, że otrzymaliśmy w ten sposób transformację naturalną $\widehat{t} : \overrightarrow{p} \underset{\cdot}{\longrightarrow} f$.

(iii) Udowodnić *Lemat Yonedy*:

$$p \in \mathrm{Ob}\, C,\ f : C \underset{\cdot}{\longrightarrow} \mathrm{Set},\ \varphi : \overrightarrow{p} \underset{\cdot}{\longrightarrow} f \ \Rightarrow\ \exists!\, t \in pf : \varphi = \widehat{t}.$$

Tak więc dla obiektu $p \in \mathrm{Ob}\, C$ i funktora $f : C \to \mathrm{Set}$ transformacje naturalne $\varphi : \overrightarrow{p} \underset{\cdot}{\longrightarrow} f$ można identyfikować z elementami zbioru $pf = f(p)$.
(iv) Niech $p, q \in \mathrm{Ob}\, C$. Korzystając z lematu Yonedy ((iii)) scharakteryzować transformacje naturalne $\varphi : \overrightarrow{p} \underset{\cdot}{\longrightarrow} \overrightarrow{q}$.

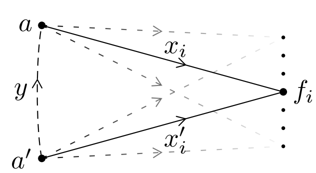
11*. Pojęcie *granicy projektywnej* (*induktywnej*) diagramu jest uogólnieniem pojęcia produktu (koproduktu).
Niech będą dane: schemat diagramowy S ($S \in \mathrm{Graph}$), kategoria C i diagram $f : S \underset{\cdot}{\longrightarrow} C$. Oznaczmy $I = \mathrm{Ob}\, S$.

Stożkiem projektywnym nad diagramem f nazywamy parę (a, x) taką, że $a \in \mathrm{Ob}\, C$, $x : I \to C$, $\forall\, i \in I : x_i : a \underset{C}{\longrightarrow} f_i$ oraz $\forall\, s : i \underset{G}{\longrightarrow} j$ $(x_i \cdot f_s = x_j)$. Ogół takich stożków oznaczmy $\mathrm{Con}(f)$. Dla $(a, x) \in \mathrm{Con}(f)$, a to *wierzchołek* x_i – projekcje.

Jeśli $S = I$, to nasz schemat możemy identyfikować ze zbiorem, f jest rodziną obiektów kategorii C i otrzymujemy pojęcie produktu rodziny f.

Stożek $(a, x) \in \mathrm{Con}(f)$ nazywamy *granicą projektywną* diagramu f, gdy spełnia *warunek uniwersalności*:

$$\forall\, (a', x') \in \mathrm{Con}(f)\ \exists!\, y : a' \underset{C}{\longrightarrow} a\ \forall\, i \in I : x'_i = y x_i.$$



Jednoznacznie wyznaczony morfizm y to sprowadzenie stożka (a', x') do stożka (granicy) (a, x).

Oznaczmy $\mathrm{Lim\,pr}(f)$:= klasa wszystkich granic projektywnych diagramu f. W przypadku gdy f jest rodziną obiektów kategorii C ($S = I$), granice projektywne to produkty – ich ogół oznaczamy $\mathrm{Prod}(f)$ – dla rodziny skończonej np. dwuelementowej, $b, c \in \mathrm{Ob}\, C$, notujemy: $\mathrm{Prod}(a, b)$.

Granica projektywna $(a, x) \in \mathrm{Lim\,pr}(f)$, jeżeli istnieje, jest wyznaczona jednoznacznie z dokładnością do komutującego izomorfizmu, tzn. jeżeli jeszcze $(a', x') \in \mathrm{Lim\,pr}\, f$, to morfizm sprowadzający y jest izomorfizmem $y : a' \xrightarrow{\sim} a$.

Kategorię C nazywamy *projektywnie zupełną* (*induktywnie zupełną*), jeżeli dla każdego schematu S i diagramu $f : S \to C$ istnieje granica projektywna (induktywna) – $\mathrm{Lim\,pr}(f) \neq \varnothing$ ($\mathrm{Lim\,ind}(f) \neq \varnothing$).

Przykładowo parę morfizmów $(u, v) \in C^2$ taką, że $\mathrm{dom}\, u = \mathrm{dom}\, v$ i $\mathrm{cod}\, u = \mathrm{cod}\, v$ możemy traktować jako diagram o schemacie

$$\bullet \rightrightarrows \bullet \quad .$$

Stożek projektywny nad tym diagramem może być identyfikowany z morfizmem $x \in C$ takim, że $xu = xv \in C$.

$$\begin{tikzcd}
\bullet \arrow[r, "x"] & \bullet \arrow[r, bend left, "u"] \arrow[r, bend right, "v"'] & \bullet \\
\bullet \arrow[u, dashed, "y"] \arrow[ur, bend right, "x'"'] & &
\end{tikzcd}$$

.

Każdy taki morfizm x nazywamy *ekwalizatorem* pary (u, v); granicę projektywną nazywamy też *uniwersalnym ekwalizatorem* lub *jądrem* pary (u, v); oznaczamy:

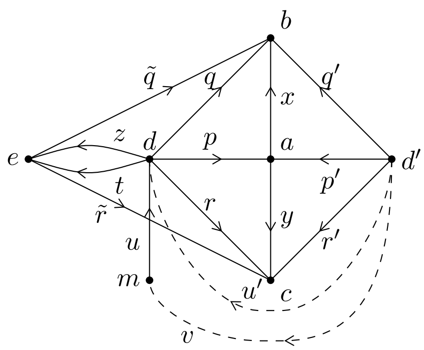
$$\mathrm{Ker}(u, v) = \{x \in C \mid xu = xv \in C \wedge \forall\, x' \in C\ [x'u = x'v \in C \ \Rightarrow\ \exists!\, z \in C\ (x' = yx)]\}.$$

(i) Udowodnić, że (zob. zadanie 4)

$$\forall\, u, v \in C\ [\mathrm{dom}\, u = \mathrm{dom}\, v \wedge \mathrm{cod}\, u = \mathrm{cod}\, v \ \Rightarrow\ \mathrm{Ker}(u, v) \subset \mathrm{Mono}].$$

(ii) Scharakteryzować jądra par morfizmów w kategorii zbiorów Set (por. rozdział 4, zadanie 8) – będą to tzw. *jądra zwyczajne*.

(iii) Udowodnić, że jeżeli kategoria C jest z produktami i jądrami par morfizmów (tzn. $\forall\, u, v \in C : \mathrm{dom}\, u = \mathrm{dom}\, v \wedge \mathrm{cod}\, u = \mathrm{cod}\, v \ \Rightarrow\ \mathrm{Ker}(u, v) \neq \varnothing$), to granicę projektywną diagramu $b \xleftarrow{x} a \xrightarrow{y} c$ w kategorii C można uzyskać w następujący sposób:



Bierzemy $(d, (p, q, r)) \in \mathrm{Prod}(a, b, c)$, $(e, (\tilde{q}, \tilde{r})) \in \mathrm{Prod}(b, c)$, $z =$ morfizm sprowadzający stożek $(d, (q, r))$ do stożka $(e, (\tilde{q}, \tilde{r}))$, $t =$ morfizm sprowadzający stożek $(d, (px, py))$ do stożka $(e, (\tilde{q}, \tilde{r}))$, $u \in \mathrm{Ker}(z, t)$, $m = \mathrm{dom}\, u$. Stożek $(m, (up, uq, ur))$ jest szukaną granicą projektywną naszego diagramu.

(iv) Stosując metodę z (iii) udowodnić, że kategoria C z produktami i jądrami par morfizmów jest projektywnie zupełna.

(v) Udowodnić, że kategoria zbiorów Set jest z jądrami i kojądrami par morfizmów; dla odwzorowań $f, g : X \to Y$ $(X, Y \in \mathbb{V})$:

1°) jądrem jest zbiór $K = \mathrm{Ker}(f, g) = \{x \in X \mid f(x) = g(x)\}$, dokładniej morfizm (K, id_K, K)

2°) kojądrem jest zbiór $\mathrm{Coker}(f, g) = Y/\bar{R}$, dokładniej surekcja naturalna $\mathrm{nat}_{\bar{R}} : Y \twoheadrightarrow Y/\bar{R}$, gdzie $\bar{R}$ jest domknięciem równoważnościowym relacji $R = \{(f(x), g(x)) \mid x \in X\}$,

$$\bar{R} = \bigcap \{S \in \mathrm{Equ}(Y) \mid R \subset S\}.$$

Tak określone jądra i kojądra w kategorii Set nazywamy *zwyczajnymi*. Dla diagramu w kategorii Set jego granicę projektywną, określoną przez produkty zwyczajne i jądra zwyczajne, tak jak pokazano w punkcie (iv), nazywamy *zwyczajną*. Mówimy, że kategoria Set jest projektywnie i induktywnie zupełna *w sposób zwyczajny*.

Pojęcia te przenosi się w sposób naturalny na (niektóre) kategorie zwyczajne – należy jedynie zamiast o podzbiorach i równoważnościach mówić o podobiektach i kongruencjach.

12*. Granica projektywna diagramu $\bullet \xrightarrow{x} \bullet \xleftarrow{y} \bullet$ w kategorii C jest wyznaczona przez parę morfizmów $u, v \in C$ taką, że przemienny jest kwadrat (x, y, u, v)

$$\begin{tikzcd}
& \bullet \arrow[r, "x"] & \bullet \\
& \bullet \arrow[u, "u"] \arrow[r, "v"'] & \bullet \arrow[u, "y"'] \\
\bullet \arrow[uur, bend left, "u'"] \arrow[ur, dashed, "w"] \arrow[urr, bend right, "v'"'] & &
\end{tikzcd}$$

to znaczy $ux = vy \in C$ i spełniony jest *warunek uniwersalności*

$$\forall\, u', v' \in C\ [u'x = v'y \in C \ \Rightarrow\ \exists!\, w \in C : u' = wu,\ v' = wv];$$

kwadrat taki nazywamy *produktem włóknistym* pary x, y lub *pullbackiem* (pojęcie dualne: *pushout*), mówimy że morfizm w (wyznaczony jednoznacznie) *sprowadza* kwadrat przemienny (x, y, u', v') do pullbacku (x, y, u, v).

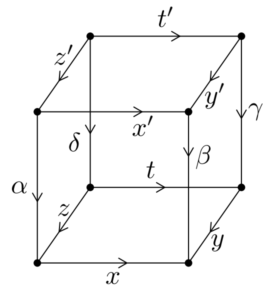
Wykazać, że:

(i) Jeżeli kwadrat (x, y, u, v) jest pullbackiem, i $x \in$ Mono, to $y \in$ Mono.
(ii) Pullbacki możemy zestawiać, jak pokazuje poniższy rysunek,

$$\begin{tikzcd}
\bullet \arrow[r, "w"] & \bullet \arrow[r, "x"] & \bullet \\
\bullet \arrow[u, "z"] \arrow[r, "t"'] & \bullet \arrow[u, "u"] \arrow[r, "v"'] & \bullet \arrow[u, "y"']
\end{tikzcd}$$

to znaczy, jeżeli kwadraty (x, y, u, v) i (w, u, z, t) są pullbackami, to kwadrat (wx, y, z, tv) też jest pullbackiem.
(iii) Jeżeli w sytuacji (ii) kwadraty (wx, y, z, tv) i (x, y, u, v) są pullbackami, zaś kwadrat (w, u, z, t) jest przemienny, to kwadrat ten też jest pullbackiem.

(iv) Jeżeli w sześcianie przemiennym (tzn. wszystkie ściany są kwadratami przemiennymi) podłoga i ściany boczne są pullbackami, to sufit (x', y', z', t') też jest pullbackiem.



13*. Przyjmijmy notację i terminologię jak w zadaniu 10*.
Dana jest kategoria C i schemat diagramowy (graf mały) $S \neq \varnothing$, $I = \operatorname{Ob} S$. Transformacje naturalne diaqramów (funktorów) z S do C możemy składać, jeżeli $f, g, h : S \xrightarrow[\cdot]{} C$, $\varphi : f \xrightarrow[\cdot]{} g$, $\psi : g \xrightarrow[\cdot]{} h$, to określamy transformację naturalną $\varphi\psi : f \xrightarrow[\cdot]{} h$, kładąc dla $i \in I$: $i(\varphi\psi) = i\varphi \cdot i\psi$.

(i) Wykazać, że określiliśmy w ten sposób kategorię $D = \operatorname{Diag}(S, C)$ diagramów w C o schemacie S i ich transformacji naturalnych. Sformułować ścisłą definicją kategorii D; jakie będą jej obiekty? izomorfizmy? ($\operatorname{Iso} D =$?).

(ii) Określamy odwzorowanie $\lambda : C \to D$, przyporządkowując każdemu morfizmowi $C \ni x : a \to b$ transformację naturalną $x\lambda : a\lambda \xrightarrow[\cdot]{} b\lambda$, gdzie dla $a \in \operatorname{Ob} C$ $a\lambda$ jest diagramem stałym, $a\lambda : S \xrightarrow[\cdot]{} C$, $\forall\, s \in S : s(a\lambda) = a$; zaś $x\lambda : I \to C$; $\forall\, i \in I : i(x\lambda) = x$, $i(a\lambda) \xrightarrow[C]{} i(b\lambda)$ $(i(a\lambda) = a,\ i(b\lambda) = b)$.

Wykazać, że określiliśmy w ten sposób funktor injektywny $\lambda : C \overset{\cdot}{\hookrightarrow} D$, który możemy traktować jako utożsamienie, $C \subset D$.

Czym będzie w kategorii D granica projektywna diagramu $f : S \xrightarrow[\cdot]{} C$ (zadanie 11*)?

14. Wykazać, że dla izomorfizm $f : X \xrightarrow{\sim} Y$ obiektów kategorii zwyczajnej $\mathcal{T}$ i podobiektu $Z \underset{\cdot}{\subsetneq} X$ jego obraz $f(Z)$ jest podobiektem obiektu Y; $f(Z) \underset{\cdot}{\subsetneq} Y$.

Jest to ilustracja ogólnego faktu, że „izomorfizm zachowuje wszystko” – można go traktować jako „zmianę nazw”, „utożsamienie”, czyli odwzorowanie identycznościowe – oczywiście w ramach ustalonej kategorii zwyczajnej.

15. Posetowi P przyporządkujmy kategorię małą

$$C = F(P) := \{(a, b) \in P^2 \mid a \leqslant b\}, \qquad \cdot : C^2 \multimap C;$$

$$(a, b) \cdot (c, d) = \begin{cases} (a, d), & \text{gdy b=c} \\ \mathbb{V}, & \text{w przeciwnym wypadku.} \end{cases}$$

Pokazać, że w ten sposób rzeczywiście określiliśmy kategorię małą C z obiektami $\operatorname{Ob} C = \{(a, b) \in P^2 \mid a = b\}$, które możemy identyfikować z punktami posetu P, oraz że F można traktować jako funktor $F : \mathrm{POS} \xrightarrow[\cdot]{} \mathrm{Cat}$.

Scharakteryzować produkty i koprodukty rodziny $a : I \to P$, $I \in \mathbb{V}$, obiektów kategorii $C = F(P)$.

16. Oznaczmy przez Fltr podkategorię pełną kategorii Pretop przestrzeni pretopologicznych i ich odwzorowań ciągłych; obiekty kategorii Fltr, zwane *przestrzeniami filtrowymi*, są postaci $X = (A, \alpha)$, gdzie α jest filtrem na zbiorze A (zadania 7 i 8 z rozdziału 4.), to jest:

$$A \in \alpha \subset \mathcal{P}A \ \wedge \ \forall U, V \in \alpha : U \cap W \in \alpha \ \wedge \ \forall U \in \alpha, W \subset A : U \subset W \Rightarrow W \in \alpha.$$

Wykazać, że kategoria Fltr jest z produktami zwyczajnymi; dokładniej dla rodziny $X : I \to$ Fltr przestrzeni filtrowych, gdzie $X_i = (A_i, \alpha_i)$ dla $i \in I$, jej produktem zwyczajnym jest przestrzeń filtrowa $Y = (B, \beta)$, gdzie $B = \prod_{i \in I} A_i$,

$$\beta = \{U \subset B \mid \exists V : I \to \mathbb{V}\ [(\forall i \in I : V_i \in \alpha_i) \wedge \{i \in I \mid V_i \neq A_i\} \in \mathrm{Fin} \wedge \prod_{i \in I} V_i \subset U]\}.$$

Filtr β na produkcie B nazywamy *filtrem Tichonowa* indukowanym przez rodzinę X przestrzeni filtrowych.

17. Wykazać, że jeżeli kategoria $\mathcal{T}$ jest z produktami zwyczajnymi oraz $X : I \to \mathrm{Ob}\,T$, $I \in \mathbb{V}$, $A : I \to \mathbb{V}$ oraz $\forall i \in I : A_i \subsetneq X_i$ (tzn. zbiór A_i jest zgodny ze strukturą X_i), to

1°) $\prod A \subsetneq \prod X$
2°) $\prod X | \prod A = \prod_{i \in I} X_i | A_i$.

W szczególności dla $X, Y \in \mathrm{Ob}\,T$, $A \subsetneq X$, $B \subsetneq Y$ będziemy mieli:

$$A \times B \subsetneq X \times Y \ \wedge \ (X \times Y)|(A \times B) = (X|A) \times (Y|B)$$

(zgodność podobiektów z produktem).

18. Udowodnić, że jeżeli kategoria zwyczajna $\mathcal{T} = (T, \sigma)$ jest z przeciwobrazami (podobiektów), z przeciwobrazami kongruencji (tzn. $\forall X, Y \in \mathrm{Ob}\,T$, $f : X \longrightarrow Y$, $R \in \mathrm{Congr}(Y) : f^{-1}(R) = \{(x,t) \in X^2 \mid (f(x), f(t)) \in R\} \in \mathrm{Congr}(X)$) oraz morfizmy bijektywne są w niej izomorfizmami (por. zadanie 1), to podobiekt obiektu ilorazowego danego obiektu X kategorii $\mathcal{T}$ jest obiektem ilorazowym pewnego podobiektu obiektu X. (Natomiast obiekt ilorazowy podobiektu obiektu X nie musi być izomorficzny z jakimś podobiektem obiektu ilorazowego X. Kontrprzykład można podać dla kategorii grup).

19*. Udowodnić, że operacja domknięcia $\{A \mapsto A^- \mid A \subset X\}$ w zbiorze X jest algebraiczna (tzn. $\forall A \subset X$, $x \in A^- \ \exists B \subset A : |B| < \omega \wedge x \in B^-$)

wtedy i tylko wtedy,

gdy suma każdego niepustego łańcucha zbiorów domkniętych jest zbiorem domkniętym, tzn. oznaczając przez Cl rodzinę podzbiorów domkniętych w X, $\mathrm{Cl} = \{A \subset X \mid A = A^-\}$, gdy jest spełniony *warunek sumy łańcucha*:

$$\forall \varnothing \neq \mathcal{A} \subset \mathrm{Cl} : (\forall A, B \in \mathcal{A} : A \subset B \vee B \subset A) \Rightarrow \bigcup \mathcal{A} \in \mathrm{Cl}\,.$$

Wskazówka: W dowodzie nie wprost implikacji „warunek sumy łańcucha $\Rightarrow$ algebraiczność" wziąć najmniejszej mocy α podzbiór A zbioru X realizujący niealgebraiczność oraz numerację $a : \alpha \hookrightarrow\!\!\!\!\twoheadrightarrow A$ zbioru A. Rozpatrzyć zbiory $H_\xi = \{a_\eta \mid \eta < \xi\}$ dla $\xi < \alpha$ (oczywiście $A = \bigcup\limits_{\xi<\alpha} H_\xi$).

20. Trzy twierdzenia Emmy Nöther o izomorfizmach struktur algebraicznych (wynikające z odpowiednich twierdzeń dla zbiorów – por. zadania 4.11–13) można sformułować – przy pewnych dodatkowych założeniach – dla kategorii zwyczajnej $\mathcal{T}$.

Oto te twierdzenia w kolejności takiej, jak w monografii [**Cohn 65**, II, 3].

Należy sformułować dla kategorii $\mathcal{T}$ założenia, przy których wszystkie trzy twierdzenia są prawdziwe i naszkicować dowody.

(I) Morfizm $f : X \xrightarrow{\cdot} Y$ ma rozkład kanoniczny

$$\begin{tikzcd} X \arrow[r, "f", "\cdot"'] \arrow[d, two heads, "\mathrm{nat}"', "\cdot"] & Y \\ X/\ker f \arrow[r, "\sim", "\tilde{f}"'] & \mathrm{Im}\, f \arrow[u, hook, "\cdot"', "\mathrm{id}"] \end{tikzcd}$$

Jeżeli ponadto $R \in \mathrm{Congr}\, X$, to zachodzi równoważność:

$$\exists\, g : X/R \xrightarrow{\cdot} Y \ (f = g \circ \mathrm{nat}_R) \iff R \subset \ker f$$

$$\begin{tikzcd} X \arrow[r, "f", "\cdot"'] \arrow[d, two heads, "\mathrm{nat}"', "\cdot"] & Y \\ X/R \arrow[ur, "\cdot", "g"'] & \end{tikzcd}$$

Inkluzja $R \subset \ker f$ zwana jest *warunkiem faktoryzacji* f przez R; jeżeli warunek ten jest spełniony, to komutujący morfizm g istnieje dokładnie jeden.

(II) Jeżeli $Y \underset{\cdot}{\subset} X$, $R \in \mathrm{Congr}\, X$, to $R \cap Y^2 \in \mathrm{Congr}\, Y$, $\{[y]_R \mid y \in Y\} \underset{\cdot}{\subset} X/R$ i $Y/R \bigcap Y^2 \simeq \{[y]_R \mid y \in Y\}$.

(III) Jeżeli $R, S \in \mathrm{Congr}\, X$ i $R \subset S$, to według (I) istnieje dokładnie jeden morfizm $h : X/R \xrightarrow{\cdot}\!\!\!\!\twoheadrightarrow X/S$ taki, że $\mathrm{nat}_S = g \circ \mathrm{nat}_R$.

$$\begin{tikzcd} X \arrow[r, two heads, "\mathrm{nat}_S", "\cdot"'] \arrow[d, two heads, "\mathrm{nat}_R"', "\cdot"] & X/S \\ X/R \arrow[ur, two heads, "h"] \arrow[d, two heads, "\mathrm{nat}_{\ker h}"'] & \\ (X/R)/\ker h \arrow[uur, "\sim", "\tilde{h}"'] & \end{tikzcd}$$

Wówczas $S/R := \ker h \in \mathrm{Congr}(X/R)$, i w rozkładzie kanonicznym morfizm h indukuje izomorfizm

$$\tilde{h} : (X/R)/(S/R) \xrightarrow{\sim} X/S.$$

Dla ustalonej kongruencji $R \in \operatorname{Congr} X$ otrzymujemy bijekcję kanoniczną

$$\{S \mapsto S/R \mid R \subset S \in \operatorname{Congr} X\} : \{S \in \operatorname{Congr} X \mid R \subset S\} \hookrightarrow\!\!\!\rightarrow \operatorname{Congr}(X/R).$$

21. Określamy kategorię zwyczajną $\mathcal{T} = (T, \sigma)$ *przestrzeni z operacją domknięcia* (por. zadania 4.17 i 4.18):

1°) $\operatorname{Ob} T = \{(x, \varphi) \mid \varphi$ – operacja domkniącia w $X\}$; przy ustalonym (znanym) φ notujemy: $A^- = \varphi(A)$, dla $A \subset X$.
2°) $\forall\, X, Y \in \operatorname{Ob} T : \sigma(X, Y) = \{f : X \to Y \mid \forall\, A \subset X : f(A^-) \subset (f(A))^-\}$.

O punktach zbioru X, które należą do A^-, gdzie $A \subset X$, mówimy, że są *przyległe* do A.

Warunek określający $\sigma(X, Y)$ mówi, że morfizm f „nie odrywa" od A punktów przyległych do zbioru $A \subset X$; jeżeli x przylega do A, to $f(x)$ przylega do $f(A)$. W związku z tym morfizmy obiektów kategorii $\mathcal{T}$ nazywamy też *odwzorowaniami ciągłymi* – okaże się (zob. (4)), że kategorię $\mathcal{T}$ można utożsamiać z pewną podkategorią pełną przestrzeni pretopologicznych.

Jeżeli zażądamy, żeby operacja domknięcia spełniała dodatkowo dwa postulaty:

(i) $\varnothing^- = \varnothing$,
(ii) $\forall\, A, B \subset X : (A \cup B)^- = A^- \cup B^-$,

to przejdziemy do jeszcze węższej podkategorii pełnej Top *przestrzeni topologicznych*.

(1) Udowodnić poprawność powyższej definicji.
(2) Podzbiór A przestrzeni z operacją domknięcia X nazywamy *domkniętym*, gdy $A^- = A$; ich ogół oznaczamy $\mathcal{F} = \mathcal{F}_X$; $\mathcal{F} = \{A \subset X \mid A^- = A\}$.
Wykazać, że:
(a) cała przestrzeń jest zbiorem domkniętym; $X \in \mathcal{F}$,
(b) przecięcie niepustej rodziny zbiorów domkniętych jest zbiorem domkniętym; $\varnothing \neq \mathcal{A} \subset \mathcal{F} \;\Rightarrow\; \bigcap \mathcal{A} \in \mathcal{F}$.
(3) Przeciwobraz zbioru domkniętego przez odwzorowanie ciągłe jest zbiorem domkniętym;

$$\forall\, X, Y \in \operatorname{Ob} T,\; f : X \xrightarrow{\cdot} Y,\; B \in \mathcal{F}_Y \;\Rightarrow\; f^{-1}(B) \in \mathcal{F}_X.$$

(4) Określamy kategorię zwyczajną $\mathcal{T}' = (T', \sigma')$:
1° $\operatorname{Ob} T' = \{(X, \mathcal{F}) \mid \mathcal{F} \subset \mathcal{P}X \;\wedge\; X \in \mathcal{F} \;\wedge\; \forall \varnothing \neq \mathcal{A} \subset \mathcal{F} : \bigcap \mathcal{A} \in \mathcal{F}\}$
2° $\forall \left.\begin{smallmatrix} X=(|X|,\mathcal{F}) \\ Y=(|Y|,\mathcal{H}) \end{smallmatrix}\right\} \in \operatorname{Ob} T' : \sigma'(X, Y) = \{f : X \to Y \mid \forall\, B \in \mathcal{H} : f^{-1}(B) \in \mathcal{F}\}$.

Na mocy (2) i (3) odwzorowanie $F : \operatorname{Ob} T \to \operatorname{Ob} T'$, $F(x, \varphi) = (X, \mathcal{F}_X)$ jest funktorem zwyczajnym; $F : \mathcal{T} \xrightarrow{\cdot} \mathcal{T}'$.
Udowodnić, że funktor F ustala równoważność kategorii $\mathcal{T}$ i $\mathcal{T}'$; $F : \mathcal{T} \xrightarrow{\sim} \mathcal{T}'$. Kategorie $\mathcal{T}$ i $\mathcal{T}'$ możemy więc utożsamiać.
(5) Udowodnić, że dla przestrzeni z operacją domknięcia X, Y odwzorowanie $f : X \to Y$ jest ciągłe wtt, gdy

$$\forall\, B \subset Y : (f^{-1}(B))^- \subset f^{-1}(B^-).$$

(6) Podzbiór A przestrzeni z operacją domknięcia X nazywamy *otwartym*, gdy jego dopełnienie $A^\neg = X \setminus A$ jest podzbiorem domkniętym; ogół takich podzbiorów oznaczamy przez $\mathcal{G}_X$.
Udowodnić, że dla przestrzeni z operacją domknięcia X, Y odwzorowanie $f : X \to Y$ jest ciągłe wtt, gdy $\forall\, B \in \mathcal{G}_Y : f^{-1}(B) \in \mathcal{G}_X$.

22. Wykazać, że jeżeli kategoria zwyczajna $\mathcal{T} = (T, \sigma)$ jest algebraiczna (tzn. nietrywialna, z jądrami par morfizmów, z multyplikatywnością podobiektów i taka, że operacja przejścia od podzbioru do podobiektu generowanego jest algebraiczna), oraz

$$X \in \operatorname{Ob} T,\ B \in \mathcal{B}(X),\ |B| \geqslant \omega,\ G \in \mathcal{G}(X),$$

to $|B| \leqslant |G|$.

Wynika stąd, że dla dowolnej innej bazy $A \in \mathcal{B}(X)$ zachodzi równość: $|A| = |B|$ $\langle$gdyż baza A jest zbiorem generującym (8.1.27), a więc $|B| \leqslant |A|$, skąd $|A| \geqslant \omega$ i, zamieniając rolami A i B, otrzymujemy nierówność $|A| \leqslant |B|\rangle$.

Wskazówka: Z przyjętych założeń o kategorii $\mathcal{T}$ wynika, że baza B jest minimalnym zbiorem generującym (1.8.29), $B^- = X$, $\exists)\, F : X \to \mathcal{P}B \cap \mathrm{Fin}\ \forall\, x \in X : x \in F(x)^-$. Zbadać zbiór $B' := \bigcup\limits_{x \in G} F(x) \subset B$.

8.3. Odpowiedzi

1.
(i) $\Rightarrow$ (ii)) Jeżeli $X = (A, \alpha) \prec Y = (B, \beta)$, to $A = B$ i $\mathrm{id}_A : X \xrightarrow{\sim} Y$, a więc, na mocy postulatu przeniesienia, $X = Y$.
(ii) $\Rightarrow$ (i)) Jeżeli dla $X = (A, \alpha)$, $Y = (B, \beta)$, $f : A \hookrightarrow\!\!\!\!\rightarrow B$ jest $f : X \xrightarrow{.} Y$, to istnieje dokładnie jeden obiekt $Z = (B, \gamma)$ taki, że $f : X \xrightarrow{\sim} Z$ (postulat przeniesienia), czyli $f : X \xrightarrow{.} Z$ i $f^{-1} : Z \xrightarrow{.} X$. Zatem, na mocy postulatu złożenia, $\mathrm{id}_B = f \circ f^{-1} : Z \xrightarrow{.} Y$, a więc $Y \prec Z$, $Y = Z$, $f : X \xrightarrow{\sim} Y$.
W kategorii systemów relacyjnych $X = (\mathbb{N}, \leqslant) \prec Y = (\mathbb{N}, =)$ i $X \neq Y$, a więc obydwa warunki (i) i (ii) nie są spełnione.
Podobnie jest w kategorii przestrzeni pretopologicznych.

W kategorii grupoidów dla dwu obiektów $X = (A, (\varphi, a))$, $Y = (B, (\psi, b))$, jeżeli $f : A \hookrightarrow\!\!\!\!\rightarrow B$ i $f : X \xrightarrow{.} Y$, to $f^{-1}(b) = f^{-1}(f(a)) = a$, oraz dla $y, t \in B$, oznaczając $x = f^{-1}(y)$, $z = f^{-1}(t)$, będziemy mieli $f^{-1}(\psi(y, t)) = f^{-1}(\psi(f(x), f(z))) = f^{-1}(f(\varphi(x, z))) = \varphi(x, z) = \varphi(f^{-1}(y), f^{-1}(t))$, a więc $f^{-1} : Y \xrightarrow{.} X$, czyli $f : X \xrightarrow{\sim} Y$.

Tak więc w kategorii tej obydwa warunki (i) i (ii) są spełnione.

2.
1°) $F : \mathrm{Bool} \xrightarrow{.} \mathcal{R}$ $\langle$mechaniczny rachunek$\rangle$.
2°) $G : \mathcal{R} \xrightarrow{.} \mathrm{Bool}$ $\langle$jak w 1°$\rangle\rangle$.
3°) $G \circ F \subset \mathrm{id}$

$\langle$Niech $X \in \mathrm{Bool}$, $X' = (\underline{X}', \vee', \wedge', {}^{\neg'}, 0', 1') = G(F(X))$.
$X' = X$, gdyż dla $a, b \in X$: $a \vee' b = a + b + ab = [(a \wedge b^\neg) \vee (a^\neg \wedge b)] + (a \wedge b) =$

$([(a\wedge b^\neg)\vee(a^\neg\wedge b)]\wedge(a^\neg\wedge b^\neg))\vee((a^\neg\vee b)\wedge(a\vee b^\neg)\wedge(a\wedge b)) = (a^\neg\wedge b)\vee(a\wedge b^\neg)\vee(a\wedge b) = a\vee b$,
$a \wedge' b = ab = a \wedge b$,
$a^{\neg\prime} = a + 1 = (a \wedge 1^\neg) \vee (a^\neg \wedge 1) = (a \wedge 0) \vee a^\neg = 0 \vee a^\neg = a^\neg\rangle$.

4°) $F \circ G \subset \mathrm{id}$ $\quad\langle$Analogiczne przeliczenia jak w 3°)$\rangle$.

3. Sprawdzenie, że kategoria $(C, \cdot)$ spełnia warunki (C1')–(C4'), jest natychmiastowe ($\mathrm{Ob}\, C = U_l \cap U_r$).

Załóżmy teraz, że dla mnożenia $\cdot : C^2 \multimap\!\!\to C$ zachodzi (C1')–(C4').

Wówczas:

Dla $a \in U_l$ istnieje $b \in U_r : ab \in C$, a więc $a = ab = b$, czyli $a \in U_r$. Zatem $U_l \subset U_r$. Analogicznie $U_r \subset U_l$, a więc $U_l = U_r = \mathrm{Ob}\, C$.

Jeżeli $x \in C$ oraz $a, c \in \mathrm{Ob}\, C : ax, cx \in C$, to $ax = cx = x$, a więc $x = ax = a(cx)$, i według (C4') $ac \in C$, czyli $a = ac = c$.

Podobnie dla mnożenia prawostronnego. Tak więc punkt (C1) został udowodniony, i dla morfizmu $x : a \to b$ możemy wprowadzić oznaczenia: $\mathrm{dom}\, x = a$, $\mathrm{cod}\, x = b$.

Dowód punktów (C2), (C3) i (C4) nie sprawi już większych trudności.

4.

1) Jeżeli $x, y \in \mathrm{Mono}$ i dla $z, t \in C$ $zxy = txy \in C$, to $zx = tx$, $z = t$, a więc $xy \in \mathrm{Mono}$.

Jeżeli $xy \in \mathrm{Mono}$ i dla $z, t \in C$ $zx = tx \in C$, to $zxy = txy$, $z = t$, czyli $x \in \mathrm{Mono}$.

2) Jeżeli $x \in \mathrm{Sect}$, to $\exists)\, u \in C : xu = a$. Teraz jeżeli dla $z, t \in C$ $zx = tx \in C$, to $zxu = txu$, $za = ta$, $z = t$, a więc $x \in \mathrm{Mono}$.

Załóżmy teraz, że $\mathrm{cod}\, x = \mathrm{dom}\, y = b$.

Jeżeli $x, y \in \mathrm{Sect}$ to $\exists)\, u, v \in C : xu = a$, $yv = b$ $\quad a \underset{u}{\overset{x}{\rightleftarrows}} b \underset{v}{\overset{y}{\rightleftarrows}} c$, a więc $xyvu = xbu = xu = a$, czyli $xy \in \mathrm{Sect}$.

Jeżeli $xy \in \mathrm{Sect}$ to $\exists)\, w \in C : xyw = a$, a więc $x \in \mathrm{Sect}$.

3) Jest $\begin{tikzcd} a \arrow[r, "x"] & b \arrow[l, bend right, "u"'] \arrow[l, bend left, "v"] \end{tikzcd}$, $u = bu = vxu = va = v$.

Zatem $\mathrm{Sect} \cap \mathrm{Retr} = \mathrm{Iso}$ i morfizm odwrotny do x jest wyznaczony jednoznacznie.
Jeżeli $x, y \in \mathrm{Iso}$ i $\mathrm{cod}\, x = \mathrm{dom}\, y$, to $xyy^{-1}x^{-1} = xbx^{-1} = xx^{-1} = a$, a więc $(xy)^{-1} = y^{-1}x^{-1}$.

4) $\mathrm{Iso} = \mathrm{Sect} \cap \mathrm{Retr} \subset \mathrm{Mono} \cap \mathrm{Retr}$.

Teraz jeżeli $x \in \mathrm{Mono} \cap \mathrm{Retr}$, to $\exists)\, v \in C : vx = b = \mathrm{cod}\, x$. $\quad a \underset{v}{\overset{x}{\rightleftarrows}} b$. Wówczas $xvx = xb = x = ax$, a więc $xv = a$, czyli $x \in \mathrm{Iso}$.

5. Niech $X, Y \in \mathrm{Ob}\, T$, $f \in \sigma(X, Y)$.

Ad (i):

1°) HP: $f \in \mathrm{Sect} \setminus \mathrm{Inj}$.
$\exists)\, g \in \sigma(Y, X) : g \circ f = \mathrm{id}_X$, $\exists)\, x, z \in X : x \neq z$, $f(x) = f(z)$.
Wówczas $x = g(f(x)) = g(f(z)) = z$ ↯.

2°) HP: $f \in \mathrm{Inj} \setminus \mathrm{Mono}$.
$\exists)\, Z \in \mathrm{Ob}\, T;\ g, h \in \sigma(Z, X) : f \circ g = f \circ h,\ g \neq h$.
$\exists)\, z \in Z : g(z) \neq h(z)$.
Wówczas $f(g(z)) \neq f(h(z))$, a więc $f \circ g \neq f \circ h$ $\lightning$.

Ad (ii):

1°) HP: $f \in \mathrm{Retr} \setminus \mathrm{Sur}$.
$\exists)\, g \in \sigma(Y, X) : f \circ g = \mathrm{id}_Y,\ \exists)\, y \in Y \setminus \mathrm{Im}\, f$.
Wówczas $y = f(g(y)) \in \mathrm{Im}\, f$ $\lightning$.
2°) HP: $f \in \mathrm{Sur} \setminus \mathrm{Epi}$.
$\exists)\, Z \in \mathrm{Ob}\, T;\ g, h \in \sigma(Y, Z) : g \circ f = h \circ f,\ g \neq h$.
$\exists)\, y \in Y : g(y) \neq h(y)$.
Wówczas $\exists)\, x \in X : y = f(x)$, a więc $g(y) = g(f(x)) = h(f(x)) = h(y)$ $\lightning$.

(iii) Jest wnioskiem z (i) i (ii).

6. W kategorii Set: Sect $\subsetneq$ Inj, gdyż dla $f = \varnothing : \varnothing \hookrightarrow Y$, gdzie $Y \neq \varnothing$ jest $f \in \mathrm{Inj} \setminus \mathrm{Sect}$.

Dowody pozostałych równości są bezproblemowe.

7. Niech $0'$ będzie innym obiektem zerowym kategorii C, $u' : a \to 0'$, $v' : 0' \to b$, $f : 0 \xrightarrow{\sim} 0'$.

$$\begin{tikzcd} & 0 \arrow[dr, "v"] \arrow[dd, "f"] & \\ a \arrow[ur, "u"] \arrow[dr, "u'"'] & & b \\ & 0' \arrow[ur, "v'"'] & \end{tikzcd}$$

Wówczas $u'v' = uff^{-1}v = uv$.

8. Niech (b, f) będzie produktem rodziny $a : I \to \mathrm{Ob}\, C$ o wierzchołku $b \in \mathrm{Ob}\, C$ i projekcjach $f_i : b \to a_i$. Ustalmy $i \in I$. Należy wykazać, że istnieje morfizm $g : a_i \to b$ taki, że $gf_i = a_i$.

Rozważmy stożek projektywny (a_i, f') nad rodziną a taki, że dla $j \in I$:

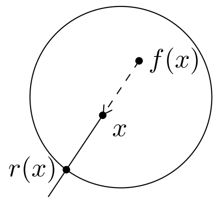
$$f'_j = \begin{cases} a_i, & \text{gdy } j = i \\ \omega_{a_i a_j}, & \text{gdy } j \neq i \end{cases} \quad \text{(zadanie 7).}$$

Wówczas $\exists)\, g : a_i \to b\ \forall\, j \in I : f'_j = gf_j$; w szczególności dla $j = i$ otrzymujemy: $a_i = gf_i$.

9*.

(i) HP: $\exists)\, r : K \to S$ retrakcja. Wówczas $\exists)\, f : S \to K;\ r \circ f = \mathrm{id}_S$, $H(r) \circ H(f) = H(\mathrm{id}_S) = \mathrm{id}_{H(S)}$ – homomorfizm zerowy $\lightning$ (gdyż grupa $H(S)$ jest nietrywialna).
(ii) Przypuśćmy, że istnieje odwzorowanie ciągłe $f : K \to K$ bez punktów stałych. Oznaczając przez $r(x)$ punkt przecięcia sfery S półprostą o początku $x \in K$ i wektorze

kierującym $x - f(x)$ otrzymamy retrakcję ciągłą $f : K \to S$ $\lightning$.



10*.

(i) Dla $a \in \operatorname{Ob} C$, $a\overrightarrow{p} : \operatorname{Mor}(p,a) \to \operatorname{Mor}(p,a)$, $\forall\, y \in \operatorname{Mor}(p,a) : y(a\overrightarrow{p}) = ya = y$, czyli $a\overrightarrow{p} = \mathrm{id}_{\operatorname{Mor}(p,a)}$ – utożsamiane ze zbiorem $\operatorname{Mor}(p,a)$.

Dla $C \ni a \xrightarrow{x} b \xrightarrow{y} c$, $(xy)\overrightarrow{p} : \operatorname{Mor}(p,a) \to \operatorname{Mor}(p,c)$, $\forall\, z \in \operatorname{Mor}(p,a) : z((xy)\overrightarrow{p}) = z(xy)$, $z(x\overrightarrow{p})(y\overrightarrow{p}) = (zx)(y\overrightarrow{p}) = (zx)y = z(xy)$, czyli $(xy)\overrightarrow{p} = x\overrightarrow{p} \cdot y\overrightarrow{p}$.

(ii) Należy wykazać, że dla morfizmu $C \ni x : a \to b$ przemienny jest kwadrat:

$$\begin{tikzcd} a\overrightarrow{p} \arrow[r, "\widehat{at}"] \arrow[d, "x\overrightarrow{p}"'] & af \arrow[d, "xf"] \\ b\overrightarrow{p} \arrow[r, "\widehat{bt}"] & bf. \end{tikzcd}$$

Dla $y \in a\overrightarrow{p} = \operatorname{Mor}(p,a)$:
$y(\widehat{at})(xf) = t(yf)(xf)$,
$y(x\overrightarrow{p})(\widehat{bt}) = (yx)(\widehat{bt}) = t(yx)f = t(yf)(xf)$.

(iii)

1°) <u>Jednoznaczność:</u>

Jeżeli $\varphi = \widehat{t}$ dla pewnego $t \in pf$, to $\forall\, a \in \operatorname{Ob} C : a\varphi = \widehat{at} : a\overrightarrow{p} \to af$, w szczególności $p\varphi = \widehat{pt} : \operatorname{Mor}(p,p) \to pf$, i biorąc $p \in \operatorname{Mor}(p,p)$, otrzymamy: $p(p\varphi) = p(\widehat{pt}) = t(pf) = t$.

2°) <u>Istnienie:</u>

Niech $t = p(p\varphi)$ $(p\varphi : p\overrightarrow{p} = \operatorname{Mor}(p,p) \to pf)$.
Wykażemy, że $\varphi = \widehat{t}$, czyli że

$$\forall\, a \in \operatorname{Ob} C : a\varphi a = \widehat{at} \quad (: a\overrightarrow{p} \to af).$$

Ustalmy $a \in \operatorname{Ob} C$, i niech $y \in \operatorname{Mor}(p,a)$, tj. $C \ni y : p \to a$.
Wykażemy, że $y(a\varphi) = y(\widehat{at})$.
Zachodzi równość $y(\widehat{at}) = t(yf) = p(p\varphi)(yf)$, a więc, korzystając z komutatywności kwadratu

$$\begin{tikzcd} p \in \operatorname{Mor}(p,p) = p\overrightarrow{p} \arrow[r, "p\varphi"] \arrow[d, "y\overrightarrow{p}"'] & pf \arrow[d, "yf"] \\ \operatorname{Mor}(p,a) = a\overrightarrow{p} \arrow[r, "a\varphi"'] & af, \end{tikzcd}$$

otrzymujemy

$$y(\widehat{at}) = p(y\overrightarrow{p})(a\varphi) = (py)(a\varphi) = y(a\varphi).$$

(iv) Niech $p, q \in \operatorname{Ob} C$ i $\varphi : \overrightarrow{p} \overset{\cdot}{\longrightarrow} \overrightarrow{q}$.
Według (iii) $\varphi = \widehat{t}$ dla jednoznacznie wyznaczonego $t \in p\overrightarrow{q} = \operatorname{Mor}(q, p)$.
Tak więc dla $a \in \operatorname{Ob} C$:

$$a\varphi = a\widehat{t} : a\overrightarrow{p} \to a\overrightarrow{q}.$$

Zatem $a\varphi : \operatorname{Mor}(p, a) \to \operatorname{Mor}(q, a)$, i dla $y \in \operatorname{Mor}(p, a)$ zachodzi równość:

$$y(a\varphi) = y(a\widehat{t}) = t(y\overrightarrow{q}) = ty \qquad (t = p(p\varphi) \in \operatorname{Mor}(q, p)).$$

11*.

(i) Natychmiastowy wniosek z definicji monomorfizmu jako morfizmu końcowo skracalnego.
(ii) Dla odwzorowań $f, g : X \to Y$ $(X, Y \in \mathbb{V})$ jądrem jest zbiór $\operatorname{Ker}(f, g) = \{x \in X \mid f(x) = g(x)\}$; dokładniej w kategorii Set morfizm (K, id_K, X), gdzie $K = \operatorname{Ker}(f, g)$.
(iii)
1°) $(m, (up, uq, ur))$ jest stożkiem projektywnym nad diagramem $b \xleftarrow{x} a \xrightarrow{y} c$, gdyż $px = t\tilde{q}$, $py = t\tilde{r}$, a więc $upx = ut\tilde{q} = uz\tilde{q} = uq$, i analogicznie $upy = ur$.
2°) Stożek $(m, (up, uq, ur))$ jest uniwersalny.

$\langle$Niech $(d', (p', q', r'))$ będzie jakimś innym stożkiem projektywnym nad naszym diagramem, tj. $p'x = q'$ i $p'y = r'$.
$\exists!)\, u' \in C : p' = u'p,\ g' = u'q,\ r' = u'r$.

Morfizm $u'z$ przeprowadza stożek projektywny $(d', (q', r'))$ nad rodziną (b, c) przez produkt $(e, (\tilde{q}, \tilde{r}))$ tej rodziny, gdyż $u'z\tilde{q} = u'q = q'$ i $u'z\tilde{r} = u'r = r'$.

Podobnie zachowuje się morfizm $u't$;

$$u't\tilde{q} = u'px = p'x = q', \quad u't\tilde{r} = u'py = p'y = r'.$$

Zatem $u'z = u't$, a więc $\exists!)\, v \in C : u' = vu$.

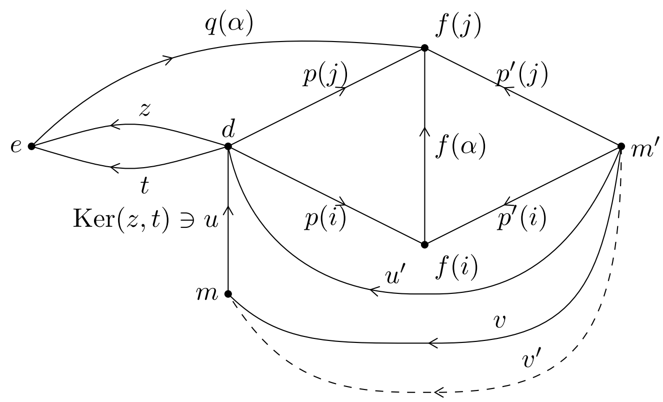
Morfizm $v : d' \to m$ sprowadza stożek $(d', (p', q', r'))$ nad naszym diagramem do stożka $(m, (up, uq, ur))$, to jest $vup = u'p = p'$, $vuq = u'q = q'$, $vur = u'r = r'$, i jeżeli jeszcze $v' : d' \to m$, $v'up = p'$, $v'uq = q'$, $v'ur = r'$, to morfizmy vu i $v'u$ sprowadzają stożek $(d', (p', q', r'))$ nad rodziną (a, b, c) do produktu $(d, (p, q, r))$, a więc $vu = v'u$, skąd wynika, że $v = v'$, gdyż $u \in \operatorname{Ker}(z, t) \subset \mathrm{Mono}\rangle$.

(iv) Mając diagram $f : S \to C$ ustalamy produkty $(d, p) \in \operatorname{Prod}(f|I)$, $(e, q) \in \operatorname{Prod}(\{\alpha \mapsto f(\operatorname{cod} \alpha) \mid \alpha \in S\})$. Następnie bierzemy morfizmy $z, t : d \to e$ sprowadzające odpowiednio stożki $(d, \{\alpha \mapsto p(\operatorname{cod} \alpha) \mid \alpha \in S\})$ i $(d, \{\alpha \mapsto p(\operatorname{dom} \alpha) \cdot f(\alpha) \mid \alpha \in S\})$ nad rodziną $\{\alpha \mapsto f(\operatorname{cod} \alpha) \mid \alpha \in S\}$ do produktu (e, q).
$\exists)\, u \in \operatorname{Ker}(z, t)$, $u : m \to d$ (zob. rysunek poniżej).

Stożek $\sigma = (m, \{i \mapsto u \cdot p(i) \mid i \in I\})$ jest granicą projektywną diagramu f.

Dowód tego faktu jest niemal wierną kopią dowodu punktu (iii).

Dla $S \ni \alpha : i \to j$ mamy: $C \ni f(\alpha) : f(i) \to f(j)$, $\operatorname{cod} f(\alpha) = f(\operatorname{cod}\alpha) = f(j)$, $\operatorname{dom} f(\alpha) = f(\operatorname{dom}(\alpha) = f(i)$.



$$\forall\, \alpha \in S\ [z \cdot q(\alpha) = p(\operatorname{cod}\alpha),\ t \cdot q(\alpha) = p(\operatorname{dom}\alpha) \cdot f(\alpha)]$$

1°) σ jest stożkiem projektywnym nad diagramem f, tzn.

$$\forall\, S \ni \alpha : i \to j\ [u \cdot p(i) \cdot f(\alpha) = u \cdot p(j)].$$

Istotnie $p(i) \cdot f(\alpha) = t \cdot q(\alpha)$, $p(j) = z \cdot q(\alpha)$, a więc $up(i)f(\alpha) = utq(\alpha) = uzq(\alpha) = u \cdot p(j)$.

2°) Stożek σ spełnia warunek uniwersalności.

$\langle$Niech (m', p') będzie jakimś innym stożkiem projektywnym nad diagramem f, tzn. $m' \in \operatorname{Ob} C$, $\forall\, i \in I : p'(i) : m' \to f(i)$ i $\forall\, S \ni \alpha : i \to j\ [p'(i) \cdot f(\alpha) = p'(j)]$.
$\exists!\, u' : m' \to d\ \forall\, i \in I : u' \cdot p(i) = p'(i)$ $\quad\langle(m', p')$ jest stożkiem projektywnym nad rodziną $f|I$, zaś $(d, p) \in \operatorname{Prod}(f|I)\rangle$.
Wówczas $u'z = u't$, gdyż obydwa te morfizmy sprowadzają stożek $(m', \{\alpha \mapsto p'(\operatorname{cod}\alpha) \mid \alpha \in S\})$ nad rodziną $\{\alpha \mapsto f(\operatorname{cod}\alpha) \mid \alpha \in S\}$ do produktu (e, q) tej rodziny $\langle\forall\, S \ni \alpha : i \to j\ [u'zq(\alpha) = u'p(j) = p'(j) = p'(\operatorname{cod}\alpha) \wedge u'tq(\alpha) = u'p(i)f(\alpha) = p'(i) \cdot f(\alpha) = p'(j) = p'(\operatorname{cod}\alpha)]\rangle$, i ponieważ morfizm u jest uniwersalnym ekwalizatorem pary (z, t), więc $\exists!)\, v : m' \to m\ (u' = vu)$.
Morfizm v jest sprowadzeniem stożka (m', p') nad diagramem f do stożka σ.

$\langle$ 2°1) $\forall\, i \in I : vup(i) = u'p(i) = p'(i)$.
2°2) Jeżeli jeszcze morfizm $v'; m' \to m$ ma tę własność, że $\forall\, i \in I : v'up(i) = p'(i)$, to $vu = v'u$ $\quad\langle$morfizmy vu, $v'u$ sprowadzają stożek (d', p') nad rodziną $f|I$ do produktu (d, p) tej rodziny$\rangle$, a więc $v = v'$ $\quad\langle$gdyż wg (i) $u \in \operatorname{Ker}(z, t) \subset \mathrm{Mono}\rangle\rangle\rangle$.

(v) Dowód punktu 1°) jest bezproblemowy. Udowodnimy 2°). koekw(a/i)lizator?
Łatwo widać, że odwzorowanie $\varphi = \operatorname{nat}_{\bar{R}} : Y \to Y/\bar{R}$ jest koekwalizatorem pary (f, g) definicja?
$\langle\forall\, x \in X : (f(x), g(x)) \in R \subset \bar{R}$, a więc $\varphi(f(x)) = [f(x)]_R = [g(x)]_R = \varphi(g(x))$, czyli $\varphi \circ f = \varphi \circ g\rangle$.

Dla dowodu uniwersalności weźmy jeszcze odwzorowanie $h : Y \to Z$ takie, że $h \circ f = h \circ g$.

$$\begin{tikzcd} X \arrow[r, bend left, "f"] \arrow[r, bend right, "g"'] & Y \arrow[r, "\varphi"] \arrow[dr, "h"'] & Y/\bar{R} \arrow[d, dashed, "h'"] \\ & & Z \end{tikzcd}$$

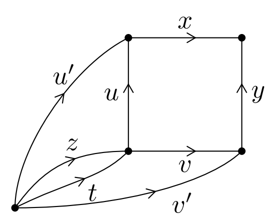
Jeżeli $h' : Y/\bar{R} \to Z$ i $h' \circ \varphi = h$, to dla $\eta = [y]_R$, $y \in Y$: $h'(\eta) = h'(\varphi(y) = h(y)$, a więc odwzorowanie h' jest wyznaczone jednoznacznie wzorem: $\eta = [y]_R$, $y \in Y \;\Rightarrow\; h'(\eta) = h(y)$.
Powyższe określenie jest poprawne, tzn. nie zależy od wyboru reprezentanta y warstwy η.

$\langle$ Niech $y, t \in \eta \in Y/\bar{R}$; wówczas $(y,t) \in \bar{R}$.
Zauważmy, że:

$$(u,v) \in R \;\Rightarrow\; \exists\, x \in X : (u,v) = (f(x), g(x)),\; h(u) = h(f(x)) = h(g(x)) = h(v).$$

Zatem $R \subset \ker h \in \mathrm{Equ}(Y)$, a więc $\bar{R} \subset \ker h$, skąd wynika, że $h(y) = h(t)\rangle$.

12*.
(i) Niech $z, t \in C$ i $zv = tv = v' \in C$.



Wówczas $zux = zvy = tvy = tux$, i ponieważ $x \in$ Mono, więc $zu = tu = u' \in C$. Kwadrat (x, y, u', v') jest przemienny $\langle u'x = zux = zvy = v'y\rangle$ i obydwa morfizmy z, t sprowadzają go do pullbacku (x, y, u, v), a więc $z = t$. Zatem $v \in$ Mono.
(ii) Kwadrat (wx, y, z, tv) jest przemienny, gdyż $zwx = tux = tvy$. Dla sprawdzenia uniwersalności weźmy morfizmy $p, q \in C$ takie, że $pwx = qy \in C$.
$\exists!)\, r \in C : ru = pw$, $rv = y$, gdyż (x, y, u, v) jest pullbackiem.
Lewy kwadrat też jest pullbackiem, a więc
$\exists!)\, s \in C : sz = p$, $st = r$. Zatem $stv = rv = q$.
Jeżeli jeszcze morfizm $s' \in C$ jest taki, że $s'z = p$, $s'tv = q$, to $s = s'$ $\langle$morfizm $s't$ podobnie jak morfizm r sprowadza kwadrat (x, y, pw, q) do pullbacku (x, y, u, v), gdyż $s'tu = s'zw = pw$, a więc $s't = r\rangle$.
(iii) Weźmy morfizmy $p, q \in C$ takie, że $pw = qu \in C$.
Wówczas $pwx = qux = qvy$, i ponieważ kwadrat (wx, y, z, tv) jest pullbackiem, zatem $\exists!)\, r \in C : rz = p$, $rtv = qv$.
Oba morfizmy q i rt sprowadzają kwadrat przemienny (x, y, pw, qv) do pullbacku (x, y, u, v), a więc $rt = q$.

Jeżeli jeszcze $r'z = p$ i $r't = q$, to $r'tv = qv$, a więc $r = r'$.
(iv) Postępujemy podobnie jak w (ii) i (iii) — jest to tzw. chodzenie po diagramie. Koniecznie trzeba wykorzystać założenie, że wszystkie pięć wymienianych ścian są pullbackami.

13*.

(i) Definicja złożenia $\varphi\psi$ transformacji naturalnych $\varphi : f \underset{\cdot}{\longrightarrow} g$ i $\psi : g \underset{\cdot}{\longrightarrow} h$ jest poprawna, gdyż dla $S \ni x : a \to b$ mamy dwa kwadraty przemienne

$$\begin{tikzcd}
af \arrow[r, "a\varphi"] \arrow[d, "xf"'] & ag \arrow[r, "a\psi"] \arrow[d, "xg"] & ah \arrow[d, "xh"] \\
bf \arrow[r, "b\varphi"'] & bg \arrow[r, "b\psi"'] & bh,
\end{tikzcd}$$

a więc kwadrat zewnętrzny też jest przemienny.
Łączność składania transformacji naturalnych wynika natychmiast z łączności mnożenia morfizmów kategorii C.

W ścisłym sformułowaniu kategoria $D = \mathrm{Diag}(S, C)$ to klasa wszystkich trójek (f, φ, g), gdzie $f, g : S \underset{\cdot}{\longrightarrow} C$, $\varphi : f \underset{\cdot}{\longrightarrow} g$, z mnożeniem częściowym:

$$(f, \varphi, g) \cdot (g, \psi, h) = (f, \varphi\psi, h).$$

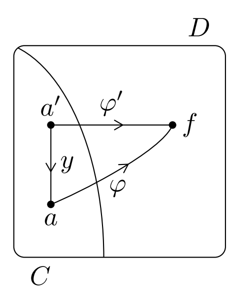
$\mathrm{Ob}\, D = \{(f, \mathrm{id}_f, f) \mid f : S \underset{\cdot}{\longrightarrow} C\}$, gdzie $\mathrm{id}_f : f \underset{\cdot}{\longrightarrow} f$, $\mathrm{id}_f = \{a \mapsto af \mid a \in \mathrm{Ob}\, S\}$. Klasę obiektów kategorii D w naturalny sposób identyfikujemy z klasą wszystkich diagramów $f : S \underset{\cdot}{\longrightarrow} C$, którą zwykle oznaczamy tym samym symbolem $\mathrm{Diag}(S, C)$, zdając się na kontekst.

$$\mathrm{Iso}\, D = \{(f, \varphi, g) \in D \mid \forall\, a \in \mathrm{Ob}\, S : a\varphi : af \xrightarrow{\sim} ag\}.$$

(ii) Z przyjętych określeń wynika natychmiast, że λ jest funktorem, $\lambda : C \underset{\cdot}{\longrightarrow} D$. Funktor ten jest injektywny $\langle$HP: $\exists)\, x, x' \in C : x \neq x'$, $x\lambda = x'\lambda$, czyli $\forall\, i \in I : x = i(x\lambda) = i(x'\lambda) = x'$. Ale $I \neq \varnothing$ $\langle$gdyż $S \neq \varnothing\rangle$, a więc $\exists)\, i \in I$, czyli $x = x'$ ↯$\rangle$.

Granicy projektywnej (a, x) diagramu $f : S \underset{\cdot}{\longrightarrow} C$ odpowiada transformacja naturalna $\varphi : a\lambda \underset{\cdot}{\longrightarrow} f$ taka, że $\forall\, i \in I : i\varphi = ix : a(= i(a\lambda)) \xrightarrow[C]{} if$ spełniające warunek uniwersalności:

$$\forall\, a' \in C,\ \varphi' : a'\lambda \underset{\cdot}{\longrightarrow} f\ \exists!\, y : a' \xrightarrow[C]{} a\ (y\lambda \cdot \varphi = \varphi').$$



14. Mechaniczny dowód wykorzystujący tylko definicje. Dla ułatwienia można narysować odpowiedni diagram.

15. Sprawdzenie warunków definicji kategorii i funktora jest w tym przypadku mechaniczne. Produktem rodziny $a : I \to P$ jest największy element (jeśli takowy istnieje) zbioru $\{p \in P \mid \forall i \in I : p \leqslant a_i\}$, czyli kres dolny zbioru $\{a_i \mid i \in I\}$; dualnie koproduktem będzie kres górny tego zbioru.

16.

1) β jest filtrem na B.

$\langle$ 1°$B \in \beta$, gdyż $\forall\, i \in I : A_1 \in \alpha_i$.
2°Jeżeli $U, U' \in \beta$ i $V, V' : I \to \mathbb{V}$ są takie jak w opisie β, to $U \cap U' \supset (\prod_i V_i) \cap (\prod_i V_i') = \prod_i (V_i \cap V_i')$, $V_i \cap V_i' \in \alpha_i$, $\{i \in I \mid V_i \cap V_i' \neq A_i\} \subset \{i \mid V_i \neq A_i\} \cup \{i \mid V_i' \neq A_i\} \in \mathrm{Fin}$, a więc $U \cap U' \in \beta$.
3°Jeżeli $\beta \ni U \subset W \subset B$, to $W \in \beta$, co wynika wprost z definicji $\beta\rangle$.

2) Dla $i \in I$ projekcja $\mathrm{pr}_i : B \to A_i$ jest ciągła, $\mathrm{pr}_i : Y \xrightarrow[\cdot]{} X_i$, gdyż dla $W \in \alpha_i$: $\mathrm{pr}^{-1}(W) = \{x \in B \mid x_i \in W\} = \prod_{j \in I} V_j$, gdzie $V_j = \begin{cases} W & \text{gdy } j = i \\ A_j & \text{gdy } j \neq i \end{cases}$, a więc $\mathrm{pr}^{-1}(W) \in \beta$.
3) Warunek początkowości jest spełniany.

$\langle$Niech $Z = (C, \gamma)$ będzie przestrzenią filtrową, $g : C \to B$ i $\forall\, i \in I : \mathrm{pr}_i \circ g : Z \xrightarrow[\cdot]{} X_i$. Wówczas $g : Z \xrightarrow[\cdot]{} Y$, gdyż dla $U \in \beta$ i $V : I \to \mathbb{V}$ takiego jak w opisie β:
$g^{-1}(U) \supset g^{-1}(\prod_i V_i) = \{z \in C \mid g(z) \in \prod_i V_i\} = \{z \in C \mid \forall\, i \in I : \mathrm{pr}_i(g(z)) \in V_i\} = \bigcap_{i \in I} (\mathrm{pr}_i \circ g)^{-1}(V_i)$, $(\mathrm{pr}_i \circ g)^{-1}(V_i) \in \gamma$, i jeżeli $V_i = A_i$, to $(\mathrm{pr}_i \circ g)^{-1}(V_i) = C$, a więc w naszym iloczynie mnogościowym tylko skończona liczba czynników jest różna od C (w tym miejscu interweniuje warunek skończoności: $\{i \in I \mid V_i \neq A_i\} \in \mathrm{Fin}$ z definicji β), zatem $g^{-1}(\prod_{i \in I} V_i) \in \gamma$, skąd $g^{-1}(U) \in \gamma\rangle$.

17. Dowód metodą „chodzenia po diagramie":
Oznaczmy $\varphi_i = \mathrm{id}_{A_i}$ dla $i \in I$, $\psi = \mathrm{id}_{\prod A}$:

$$\begin{array}{ccccc}
\prod X & \xleftarrow{\psi} & \prod_{i \in I} X_i | A_i & \xleftarrow{f} & Z \\
\Big\downarrow{\scriptstyle p_i} & & \Big\downarrow{\scriptstyle q_i} & & \\
X_i & \xleftarrow[\cdot]{\varphi_i} & X_i | A_i & &
\end{array}$$

(p_1, q_i – projekcje kanoniczne).

Należy wykazać, że ψ jest morfizmem początkowym:

1°) Ponieważ dla każdego $i \in I$ odwzorowanie $p_i \circ \psi = \varphi_i \circ q_i$ jest morfizmem, więc z warunku początkowości dla produktu zwyczajnego $\prod X$ wynika, że ψ jest morfizmem;

2°) Dla sprawdzenia początkowości morfizmu ψ weźmy $Z \in \operatorname{Ob} T$, odwzorowanie $f : Z \to \prod A$ i załóżmy, że $f \in \sigma(Z, \prod X)$. Wówczas dla ustalonego $i \in I$, $p_i \circ f = p_i \circ \psi \circ f = \varphi_i \circ q_i \circ f$ jest morfizmem Z w X_i, a więc – z warunku początkowości dla podobiektu $X_i|A_i$ – wynika, że $q_i \circ f$ jest morfizmem. Teraz z warunku początkowości dla produktu $\prod\limits_{i\in I} X_i|A_i$ wynika, że $f \in \sigma(Z, \prod\limits_{i\in I} X_i|A_i)$.

Komentarz. Udowodnione elementarne twierdzenie mówiące o przemienności produktowania i przechodzenia do podstruktur należy do *matematyki uniwersalnej* – jednym z jej zadań jest ustalenie pojęć i faktów ogólnostrukturalnych, co uwalnia nas od konieczności dowodzenia tego rodzaju podstawowych prawd w konkretnych przypadkach grup, pierścieni, przestrzeni topologicznych itp.

18. Niech $X \in \operatorname{Ob} T$, $R \in \operatorname{Congr}(X)$, $Y \underset{\cdot}{\subset} X/R$.
Wówczas $Z := \operatorname{nat}_R^{-1}(Y) \underset{\cdot}{\subset} X$,
$S := \operatorname{id}_Z^{-1}(R) = R \cap Z^2 \in \operatorname{Congr}(Z)$.
$\underline{Z/S} = \operatorname{set}(Z/S) = \operatorname{set} Y = \underline{Y}$,
$\operatorname{nat}_R |Z = \operatorname{id}_Y \circ \operatorname{nat}_S$.

Tak więc mamy diagram przemienny:

$$\begin{tikzcd}
 & Z \arrow[r, "\mathrm{id}_Z"] \arrow[dl, "\mathrm{nat}_S"'] \arrow[dd, "\mathrm{nat}_R|Z"] & X \arrow[dd, "\mathrm{nat}_R"] \\
Z/S \arrow[dr, leftrightarrow, "\mathrm{id}_Y"'] & & \\
 & Y \arrow[r, "\mathrm{id}_Y"'] & X/R.
\end{tikzcd}$$

Zatem $\operatorname{id}_Y : Z/S \underset{\cdot}{\longrightarrow} Y$, i ponieważ $\operatorname{id}_Y : Z/S \lhook\joinrel\twoheadrightarrow Y$, więc $\operatorname{id}_Y : Z/S \xrightarrow{\sim} Y$, skąd $Z/S = Y$.

19*. Algebraiczność $\implies$ warunek sumy łańcucha.

HP: $\exists)\, \varnothing \neq \mathcal{A} \subset \mathrm{Cl}$, $\forall\, A, B \in \mathcal{A}\ (A \subset B \vee B \subset A)$, $\bigcup \mathcal{A} \notin \mathrm{Cl}$.
$\exists)\, x \in (\bigcup \mathcal{A})^- \setminus (\bigcup \mathcal{A})$. $\exists)\, B \subset \bigcup \mathcal{A} : |B| < \omega \wedge x \in B^-$.
Indukcją na $|B|$ dowodzimy, że $\exists)\, A \in \mathcal{A} : B \subset A$. Wówczas $B^- \subset A^- = A$, a więc $x \in A \subset \bigcup \mathcal{A}$ ↯.

Warunek sumy łańcucha $\implies$ algebraiczność.

Oznaczmy $\mathrm{Alg} = \{A \subset X \mid \forall\, x \in A^-\ \exists\, B \subset A : |B| < \omega \wedge x \in B^-\}$.
HP: $\mathrm{Alg} \neq \mathcal{P}X$.
$\exists)\, A \subset X : A \notin \mathrm{Alg}\ \wedge\ \forall\, B \in X : |B| < |A| \ \Rightarrow\ B \in \mathrm{Alg}$.
Niech $\alpha = |A|$. Oczywiście $\alpha \geqslant \omega$.
$\exists)\, x \in A^-\ \forall\, B \subset A\ (|B| < \omega \ \Rightarrow\ x \notin B^-)$.
$\exists)\, a : \alpha \lhook\joinrel\twoheadrightarrow A$.
Oznaczmy dla $\xi < \alpha$: $H_\xi = \{a_\eta \mid \eta < \xi\}$;
wówczas $|H_\xi| = |\xi| \leqslant \xi < \alpha$, a więc $H_\xi \in \mathrm{Alg}$.

Oczywiście $A = \bigcup\limits_{\xi<\alpha} H_\xi \subset \bigcup\limits_{\xi<\alpha} H_\xi^-$.

Rodzina $\{H_\xi^- \mid \xi < \alpha\}$ jest niepustym łańcuchem zbiorów domkniętych, a więc $\bigcup\limits_{\xi<\alpha} H_\xi^- \in \mathrm{Cl}$.

Zatem $x \in A^- \subset (\bigcup\limits_{\xi<\alpha} H_\xi^-)^- = \bigcup\limits_{\xi<\alpha} H_\xi^-$, $\exists)\, \xi < \alpha : x \in H_\xi^-$, a więc $\exists)\, B \subset H_\xi : |B| < \omega \wedge x \in B^-$. Jednak $H_\xi \subset A$ zatem $B \subset A$, $|B| < \omega$, a więc $x \notin B^-$ ↯.

20. Można przyjąć następujące założenia:

(1) jeżeli $f : X \dot{\longrightarrow} Y$, to $\ker f \in \mathrm{Congr}\, X$, $\mathrm{Im}\, f \mathrel{\dot{\subset}} Y$,
(2) jeżeli $f : X \dot{\hookrightarrow\!\!\!\rightarrow} Y$, to $f : X \xrightarrow{\sim} Y$; tzn. morfizmy bijektywne są izomorfizmami,

lub

(1') jeżeli $f : X \dot{\longrightarrow} Y$, to $\mathrm{Im}\, f \mathrel{\dot{\subset}} Y$,
(2') morfizmy surjektywne są końcowe (wówczas $f : X \dot{\twoheadrightarrow} Y \;\Rightarrow\; \ker f \in \mathrm{Congr}\, X$ oraz $f : X \dot{\hookrightarrow\!\!\!\rightarrow} Y \;\Rightarrow\; f : X \xrightarrow{\sim} Y$).

Szkice dowodów:

(I) Dowód jest taki sam jak dla zbiorów (por. zadania 4.11 i 4.12).
(II) Wystarczy zastosować (I) do morfizmu $f = \mathrm{nat}_R \circ \mathrm{id}_Y : Y \dot{\longrightarrow} X/R$.
(III) Jak dla zbiorów.

21.

(1) Sprawdzenie postulatów definicji kategorii zwyczajnej sprowadza się do mechanicznych rachunków. Na przykład złożenie odwzorowań ciągłych $f : X \dot{\longrightarrow} Y$ i $g : Y \dot{\longrightarrow} Z$ jest ciągłe, gdyż dla $A \subset X$, $fA^- \subset (fA)^-$ (opuszczamy zbędne nawiasy), a więc $gfA^- \subset g(fA)^- \subset (gfA)^-$.

(2)
Ad (a): $X^- \subset X \subset X^-$, więc $X^- = X$, $X \in \mathcal{F}_X$.
Ad (b): $\forall\, A \in \mathcal{A} : \bigcap \mathcal{A} \subset A$, $(\bigcap \mathcal{A})^- \subset A^- = A$, a więc $(\bigcap \mathcal{A})^- \subset \bigcap \mathcal{A}$, $\bigcap \mathcal{A} \in \mathcal{F}_X$.

(3) Tu i dalej opuszczamy zbędne nawiasy.
$A := f^{-1}B \subset X$, $fA^- \subset (fA)^- = (ff^{-1}B)^-$, ale $ff^{-1}B \subset B$, więc $(ff^{-1}B)^- \subset B^- = B$, czyli $fA^- \subset B$, skąd $A^- \subset f^{-1}fA^- \subset f^{-1}B = A$, a więc $A = f^{-1}B \in \mathcal{F}$.

(4) Określamy funktor zwyczajny $G : \mathcal{T}' \dot{\longrightarrow} \mathcal{T}$ $\forall\,(X, \mathcal{F}) \in \mathrm{Ob}\, \mathcal{T}' : G(X, \mathcal{F}) = (X, \varphi)$, gdzie $\varphi : \mathcal{P}X \to \mathcal{P}X$, $\forall\, A \subset X : \varphi A = A^- := \bigcap \{B \in \mathcal{F} \mid A \subset B\}$ ($\in \mathcal{F}$, gdyż $A \subset X \in \mathcal{F}$); operacja φ spełnia wszystkie trzy postulaty nałożone na operację domknięcia.

1° $A \subset A^-$, gdyż $A \subset X \in \mathcal{F}$,
2° jeżeli $A \subset B$, to $A \subset B^- \in \mathcal{F}$, więc $A^- \subset B^-$,
3° $\forall\, B \in \mathcal{F} : B^- \subset B$ $\quad\langle$gdyż $B \subset B\rangle$, a więc $B^- = B$. Ponieważ $A^- \in \mathcal{F}$, więc $A^{--} = A^-$.

Należy jeszcze wykazać, że:

(a) $G \circ F \subset \mathrm{id}$,
(b) $F \circ G \subset \mathrm{id}$.

Ad (a). Niech $(X, \varphi) \in \operatorname{Ob} T$, $F(X, \varphi) = (X, \mathcal{F})$, $G(X, \mathcal{F}) = (X, \varphi')$.
Wówczas $\varphi = \varphi'$, to jest $\forall\, A \subset X : \varphi A = \varphi' A$.

$\langle$Niech $A \subset X$. $\varphi' A = \bigcap\{B \in \mathcal{F} \mid A \subset B\}$, $A \subset \varphi A \in \mathcal{F}$, a więc $\varphi' A \subset \varphi A$.
Jednakże $A \subset \varphi' A \in \mathcal{F}$, więc $\varphi A \subset \varphi\varphi' A = \varphi' A\rangle$.

Ad (b). Niech $(x, \mathcal{F}) \in \operatorname{Ob} T'$, $G(X, \mathcal{F}) = (X, \varphi)$, $F(X, \varphi) = (X, \mathcal{F}')$. Wówczas $\mathcal{F} = \mathcal{F}' \quad \langle A \in \mathcal{F} \iff \varphi A = A \iff A \in \mathcal{F}'\rangle$.

(5)

$\Rightarrow$) Jeżeli $f : X \xrightarrow{\cdot} Y$ i $B \subset Y$, to dla $A = f^{-1}B$ będziemy mieli: $fA^- \subset (fA)^- \in \mathcal{F}_Y$, a więc $A \subset f^{-1}(fA)^- \in \mathcal{F}_X$, skąd $A^- \subset f^{-1}(fA)^-$, i ponieważ $fA = ff^{-1}B \subset B$, więc $(f^{-1}B)^- \subset f^{-1}B^-$.

$\Leftarrow$) Zakładamy, że odwzorowanie $f : X \xrightarrow{\cdot} Y$ spełnia podany warunek. Wówczas dla $A \subset X$, $A^- \subset (f^{-1}fA)^- \subset f^{-1}(fA)^-$, a więc $fA^- \subset ff^{-1}(fA)^- \subset (fA)^-$.

(6)

$\Rightarrow$) Jeżeli $f : X \xrightarrow{\cdot} Y$ i $B \in \mathcal{G}_Y$, to $B^\neg \in \mathcal{F}_Y$, a więc $f^{-1}B^\neg = (f^{-1}B)^\neg \in \mathcal{F}_X$, skąd $f^{-1}B \in \mathcal{G}_X$.

$\Leftarrow$) Jeżeli odwzorowanie $f : X \xrightarrow{\cdot} Y$ spełnia podany w temacie warunek i $B \in \mathcal{F}_Y$, to $B^\neg \in \mathcal{G}_Y$, $f^{-1}B^\neg = (f^{-1}B)^\neg \in \mathcal{G}_X$, a więc $f^{-1}B \in \mathcal{F}_X$.

22. $B' \in \mathcal{G}(X) \quad \langle \forall\, x \in G : x \in F(x)^- \subset B'^-$, a więc $G \subset B'^-$, $X = G^- \subset B'^-$, czyli $B'^- = X\rangle$, zatem $B' = B$, $|B| = |B'| \leqslant \sum\limits_{x \in G} |F(x)|$.

Z ostatniej nierówności wynika, że $|G| \geqslant \omega$, a więc $|B| \leqslant |G| \cdot \omega = |G|$.

9

Podstawowe struktury matematyczne

9.1. Wstęp

9.1.1. Algebry ogólne. Dla ustalonej funkcji $\nu : \Omega \to \mathbb{N}$ zwanej *sygnaturą algebr ogólnych* (*uniwersalnych*), gdzie Ω jest zbiorem, którego elementy nazywamy *symbolami funkcyjnymi* lub *operatorami*, określamy kategorię zwyczajną $\mathcal{A}_\nu = (T, \sigma)$ *algebr o sygnaturze* ν:

1° $\forall\, A : T(A) = \{\alpha : \Omega \to \bigcup_{n\in\mathbb{N}} \mathrm{Map}(A^n, A) \mid \forall\, \omega \in \Omega : \alpha(\omega) : A^{\nu(\omega)} \to A\}$.

Tak więc obiekty kategorii $\mathcal{A}_\nu$ są postaci $X = (A, \alpha)$, gdzie $\alpha : \Omega \to \mathbb{V}$ i dla $\omega \in \Omega$, $n = \nu(\omega)$, $\alpha(\omega) : A^n \to A$; *działanie n-argumentowe* $\alpha(\omega)$ w zbiorze podkładowym $A = \underline{X}$ algebry X oznaczamy też ω_X. Liczbę naturalną $n = \nu(\omega)$ nazywamy *argumentowością* symbolu funkcyjnego ω.

Oznaczmy $\Omega(n) := \{\omega \in \Omega \mid \alpha(\omega) = n\}$.

W przypadku gdy $n = 0$ mamy $A^0 = 1 = \{0\}$, a więc działanie 0-argumentowe $\omega_X : 1 \to A$ możemy utożsamiać z elementem zbioru A – mówimy wówczas, że ω_X jest *stałą* algebry X odpowiadającą operatorowi ω; $\omega_X \in A$.

2° Dla dwu algebr $X, Y \in \mathcal{A}_\nu$ morfizmy X w Y zwane *homomorfizmami*, to odwzorowania $f : X \to Y$ zgodne ze wszystkimi działaniami, to jest spełniające warunek: $\forall_{\substack{\omega\in\Omega, n=\nu(\omega)\\ a_1,\dots,a_n\in X}} [f(\omega_X(a_1, \dots, a_n)) = \omega_Y(f(a_1), \dots, f(a_n))]$.

Zbiór $\sigma(X, Y)$ wszystkich homomorfizmów X w Y oznaczamy tradycyjnie $\mathrm{Hom}(X, Y)$.

9.1.2. Grupoidy. Dla dwuelementowego zbioru $\Omega = \{m, e\}$ i sygnatury $\nu = \{m \mapsto 2, e \mapsto 0\}$ algebry kategorii $\mathcal{G}_1 = \mathcal{A}_\nu$ nazywamy *grupoidami* (por. 8.1.3) (z *elementem wyróżnionym*). Symbolem $\mathcal{G}$ oznaczamy kategorię algebr o sygnaturze $\{m \mapsto 2\}$; jej obiekty też będziemy nazywać *grupoidami* – znaczenie słowa uzależniamy od kontekstu – na ogół, mówiąc „grupoid" będziemy mieli na myśli grupoid z elementem wyróżnionym. Zwyczajowo dla $X \in \mathcal{G}_1$ działanie $m_X : X^2 \to X$ nazywamy *mnożeniem* i dla $a, b \in X$ notujemy $ab = a \cdot b = m_X(a, b)$ (*notacja multyplikatywna*); stałą e_X oznaczamy zwykle 1 lub 1_X i nazywamy *jedynką* grupoidu X.

Tak więc dla dwóch grupoidów X, Y i odwzorowania $f : X \to Y$ zachodzi równoważność

$$f \in \mathrm{Hom}(X, Y) \iff \forall\, a, b \in X : f(ab) = f(a)f(b) \quad\wedge\quad f(1_X) = 1_Y.$$

Mnożenie w grupoidzie X nazywamy

(i) *łącznym* lub *asocjatywnym*, gdy

$$\forall\, a, b, c \in X : (ab)c = a(bc),$$

(ii) *przemiennym* lub *komutatywnym*, gdy

$$\forall\, a, b \in X : ab = ba.$$

Element $e = 1_X$ jest *elementem neutralnym* dla działania $\cdot : X^2 \to X$, gdy $\forall\, a \in X : ea = a = ae$; element taki, jeśli istnieje, to istnieje dokładnie jeden $\langle$bo gdyby jeszcze e' było takie, to $e = e'e = e'\rangle$. Dla działania przemiennego używamy chętniej *notacji addytywnej* $(a + b)$ i wówczas element wyróżniony nazywamy *zerem* i oznaczamy $0 = 0_X$.

9.1.3. Własności algebr ogólnych. Łatwo sprawdzić, że kategoria $\mathcal{A}_\nu$ algebr o sygnaturze $\nu : \Omega \to \mathbb{N}$ ma niżej wymienione własności (1)–(9). Wystarczy to wykazać dla kategorii $\mathcal{G}_1$ grupoidów – w sytuacji ogólnej dowody będą analogiczne (zadanie 2).

(1) Homomorfizmy injektywne – zwane też zwyczajowo *monomorfizmami* – są początkowe. Homomorfizmy surjektywne – inaczej *epimorfizmy* – są końcowe.

UWAGA: Homomorfizmy injektywne (surjektywne) są monomorfizmami (epimorfizmami) w sensie ogólnokategorialnym, ale pojęcia te nie pokrywają się.

???
nieczytelne

(2) Homomorfizmy bijektywne są izomorfizmami, a więc relacja $\prec$ porównywania algebr jest relacją identyczności (zob. zadanie 1 z rozdziału 8).

(3) Kategoria A_ν jest z produktami zwyczajnymi; działania w produkcie określamy „po współrzędnych". W przypadku grupoidów dla $X : I \to \mathcal{G}_1$, $1_{\prod X} = \{i \mapsto 1_{X_i} \mid i \in I\}$ oraz $\forall\, x, y \in \prod X : xy = \{i \mapsto x_i y_i \mid i \in I\}$.

Produktami w mocy 0, czyli obiektami końcowymi kategorii $\mathcal{A}_\nu$, są algebry jednoelementowe zwane też *trywialnymi*.

(4) Podzbiór E algebry X jest zgodny z X, jest – jak mówimy – *podalgebrą* X, gdy jest zamknięty ze względu na wszystkie działania; jeżeli tak jest, to podalgebrę indukowaną $X|E$ utożsamiamy w zapisie z E.
Ogół takich podzbiorów – i ogół podalgebr, w zależności od kontekstu – oznaczamy $\operatorname{Sub} X$.

Dla grupoidu G i zbioru $E \subset G$: $E \underset{\cdot}{\subset} G \iff 1 \in E \;\wedge\; \forall\, x, y \in E : xy \in E$.

Zauważmy, że $X \in \operatorname{Sub} X$ oraz $\varnothing \in \operatorname{Sub} X \iff \forall\, \omega \in \Omega : \nu(\omega) > 0$.

(5) Kategoria $\mathcal{A}_\nu$ jest z obrazami i z przeciwobrazami.

(6) Równoważność R w algebrze X jest zgodna z X – jest *kongruencją* w X – wtt, gdy jest zgodna ze wszystkimi działaniami o dodatniej argumentowości. Ogół takich równoważności oznaczamy $\operatorname{Congr} X$.

Tak więc dla grupoidu X i równoważności R w zbiorze X:

$$R \in \operatorname{Congr} X \iff \forall\, x, y, z, t \in X : x\,R\,z \wedge y\,R\,t \;\Rightarrow\; xy\,R\,zt.$$

(7) Kategoria $\mathcal{A}_\nu$ jest z multyplikatywnością podobiektów. Operacja domknięcia w algebrze X polegająca na przejściu od podzbioru $E \subset X$ do generowanej przez niego podalgebry $E^- = \langle E\rangle = \langle E\rangle_X$ jest algebraiczna.

Na przykład dla grupoidu X i podzbioru $E \subset X$:

$$E^- = \bigcup_{n=0}^{\infty} F_n, \text{ gdzie } F_0 = E,\ F_{n+1} = F_n \cup \{1_X\} \cup \{xy \mid x, y \in F_n\}$$

i analogicznie w przypadku ogólnym.

(8) Kategoria $\mathcal{A}_\nu$ jest z jądrami par morfizmów.
(9) Baza algebry wolnej X (w $\mathcal{A}_\nu$) jest maksymalnym podzbiorem niezależnym i minimalnym podzbiorem generującym; dwie bazy takiej algebry są równoliczne $\langle$gdyż w $\mathcal{A}_\nu$ istnieje algebra skończona i nietrywialna; np. $X = 2$, $\forall\,\omega \in \Omega$, $\nu(\omega) = n$, $x \in 2^n : \omega_X(x) = 0\rangle$.

Dla dowolnej algebry X: $\mathcal{G}(X) \subset \mathcal{D}(X)$ i $\mathcal{B}(X) = \mathcal{G}(X) \cap \mathcal{I}(X)$ (oznaczenia z rozdziału 8.).

9.1.4. Półgrupy. Kategorię Sgr_1 *półgrup* (z jedynką) określiliśmy jako podkategorię pełną kategorii grupoidów $(X, (\cdot, e)) \in \mathcal{G}_1$ takich, że

$$\forall\, x, y, z \in X : (xy)z = x(yz) \quad \wedge \quad ex = x = xe \quad (8.1.6);$$

element wyróżniony e nazywamy *elementem neutralnym* lub – w notacji multyplikatywnej – *jedynką* i oznaczamy 1_X lub krótko 1.

W notacji addytywnej (preferowanej, gdy działanie w półgrupie X jest przemienne) mówimy o *dodawaniu* i piszemy $x + y$, $0_X = 0 = e$.

Łatwo sprawdzić, że kategoria półgrup ma wszystkie własności (1)–(9).

Dla $X \in \mathrm{Sgr}_1$ i $A \subset X$ podgrupa generowana przez A ma postać:

$$A^- = \Big\{ \prod_{k=1}^{n} a_k^{\alpha_k} \mid n \in \mathbb{N},\ a : I_n \to A,\ \alpha : I_n \to \mathbb{N} \Big\}$$

gdzie
dla $x \in X, k \in \mathbb{N} : x^0 = 1,\ x^{k+1} = x^k x$
oraz dla $n \in \mathbb{N}$, $b : I_n \to X$, element $\prod b = \prod\limits_{k=1}^{n} b_k \in X$ zwany *iloczynem* układu b określamy indukcją na n:

$$\prod \varnothing = 1$$

$$n > 0 \ \Rightarrow\ \prod b = \prod_{k=1}^{n-1} b_k \cdot b_n.$$

Stosując dla półgrupy przemiennej $X \in \mathrm{Sgrc}_1$ notację addytywną, mówimy o *sumie*: $\sum b$, $\sum\limits_{k=1}^{n} b_k$; możemy wówczas dla dowolnej rodziny $b : T \to X$ takiej, że prawie wszystkie b_t są równe zeru (tzn. $\{t \in T \mid b_t \neq 0\} \in \mathrm{Fin}$) określić $\sum b = \sum\limits_{t \in T} b_t \in X$.

9.1.5. Półgrupy wolne. Kategoria Sgr_1 półgrup jest z obiektami wolnymi. Dla zbioru A, który nazywamy w tym kontekście *alfabetem*, określamy *półgrupę słów* nad A; $\mathrm{W}(A) \in \mathrm{Sgr}_1$, oraz injekcję kanoniczną $\iota : A \hookrightarrow \mathrm{W}(A)$.

$$\mathrm{W}(A) = \bigcup_{n \in \mathbb{N}} \mathrm{Map}(I_n, A), \quad \mathrm{Map}(I_n, A) = \ \textit{słowa o długości } n.$$

Działanie $* : \mathrm{W}(A)^2 \to \mathrm{W}(A)$ zwane *(kon)katenacją* lub *składaniem* określamy następująco:

dla $a : I_n \to A$, $b : I_m \to A$, $n, m \in \mathbb{N}$

$$a * b = a \cup \{k \mapsto b_{n-k} \mid n \leqslant k \leqslant n+m\} : I_{n+m} \to A.$$

Elementem neutralnym jest słowo puste $\varnothing : I_0 \to A$; $\iota = \{a \mapsto \{1 \mapsto a\} \mid a \in A\}$.

Po utożsamieniu $A = \iota(A)$ łatwo sprawdzić, że $\mathrm{W}(A)$ jest półgrupą wolną (obiektem wolnym w kategorii Sgr_1) o bazie A. Tak więc otrzymaliśmy funktor $\mathrm{W} : \mathrm{Set} \to \mathrm{Sgr}_1$, który na każdym zbiorze A rozpina półgrupę wolną $\mathrm{W}(A)$.

9.1.6. Algebry wolne. Termy. Dla dowolnej sygnatury $\nu : \Omega \to \mathbb{N}$, $\Omega \in \mathbb{V}$ kategoria A_ν algebr o sygnaturze ν jest z obiektami wolnymi. Mając dany zbiór V, którego elementy zwyczajowo nazywamy *zmiennymi* (*formalnymi*), określamy *algebrę termów o sygnaturze ν nad V*, $\mathrm{Term} = \mathrm{Term}_\nu(V) \in \mathcal{A}_\nu$, w następujący sposób:

1° Dla uproszczenia zapisu zakładamy, że $V \cap \Omega = \varnothing$ – bez tego założenia trzeba by sumę $V \cup \Omega$ zastąpić sumą rozłączną $V \sqcup \Omega = (V \times \{0\}) \cup (\Omega \times \{1\})$ – i jako zbiór podkładowy algebry Term przyjmujemy zbiór: $\bigcup_{n \in \mathbb{N}} T_n \subset W(V \cup \Omega)$, gdzie $T_0 = V$ (po identyfikacji: $V \subset W(V \cup \Omega)$),

$$T_{n+1} = T_n \cup \{\omega\, t_1 \dots t_k \mid \omega \in \Omega,\ k = \nu(\omega); t_1, \dots, t_k \in T_n\}.$$

Najmniejsze n takie, że $t \in T_n$ nazywamy *stopniem złożenia* lub *złożonością* termu. Indukcją na złożoność termu t niebędącego zmienną łatwo wykazać jednoznaczność jego przedstawienia w postaci $t = \omega\, t_1 \dots t_k$. Wygodnie jest przedtem udowodnić lemat: $t \in \mathrm{Term}$, $w \in W(V \cup \Omega)$, $t\,w \in \mathrm{Term} \implies w = \varnothing$ ⟨dowód lematu indukcją na długość termu t⟩.

2° Jeżeli $w \in \Omega$, $k = \nu(\omega)$; $t_1, \dots t_k \in \mathrm{Term}$, to $\omega_{\mathrm{Term}}(t_1, \dots t_k) = \omega\, t_1 \dots t_k$.

Algebra Term jest obiektem wolnym o bazie V w kategorii Alg_ν, to znaczy $\forall_{\substack{X \in \mathcal{A}_\nu \\ \varphi : V \to X}} \exists!\, \varphi \subset f : \mathrm{Term} \overset{\cdot}{\longrightarrow} X$; w tej sytuacji odwzorowanie φ nazywamy *wartościowaniem* zmiennych w algebrze X, i dla $t \in \mathrm{Term}$ element $t[\varphi]_X \overset{\mathrm{df}}{=} f(t) \in X$ nazywamy *wartością* termu t w algebrze X przy wartościowaniu φ ⟨Jednoznaczność f … Istnienie f …⟩.

Symbolem $\mathrm{Fr}\, t$ oznaczamy ogół zmiennych występujących w termie t; ścisła definicja jest indukcyjna:

1° $t \in V \implies \mathrm{Fr}\, t = \{t\}$

2° $\mathrm{Fr}(\omega\, t_1 \dots t_k) = \mathrm{Fr}\, t_1 \cup \ldots \cup \mathrm{Fr}\, t_k$.

Indukcją na złożoność termu t dowodzimy, że

$$X \in \mathcal{A}_\nu,\ \varphi, \psi : V \to X,\ \varphi|\,\mathrm{Fr}\, t = \psi|\,\mathrm{Fr}\, t \implies t[\varphi]_X = t[\psi]_X;$$

w szczególności jeżeli $\mathrm{Fr}\, t \subset \{v_1, \dots, v_n\}$, $n \in \mathbb{N}$, $v : I_n \hookrightarrow X$, to notujemy $t = t(v_1, \dots, v_n)$ i dla $a_1, \dots, a_n \in X$ $t[a_1, \dots, a_n]_X := t[\varphi]_X$, gdzie $\{v_1 \mapsto a_1, \dots, v_n \mapsto a_n\} \subset \varphi : V \to X$. W szczególności dla $s_1, \dots, s_n \in \mathrm{Term}$ określamy *podstawienie*: $t(s_1, \dots, s_n) \overset{\mathrm{df}}{=} t[s_1, \dots, s_n]_{\mathrm{Term}} \in \mathrm{Term}$.

Term c ($\in \mathrm{Term}$) nazywamy *stałym*, gdy $\mathrm{Fr}\, t = \varnothing$; jego wartość w dowolnej algebrze X nie zależy od wartościowania – oznaczamy ją c_X.

O funkcji $\{a \mapsto t[a_1, \dots, a_n]_X \mid a = (a_1, \dots, a_n) \in X^n\} : X^n \to X$ mówimy, że

jest to funkcja *algebraiczna* wyznaczona przez term t i zmienne $v_1, \dots, v_n$ ($\operatorname{Fr} t \subset \{v_1, \dots, v_n\}$). Funkcje algebraiczne tworzą podzbiór $\operatorname{Alg}(X^n, X) \subset \operatorname{Map}(X^n, X)$; dla $X \in \mathcal{A}_\nu$.
Zbiór $E \subset X^n$ nazywamy *algebraicznym*, gdy $E = \operatorname{Ker}(f, g)$ ($= \{x \in X \mid f(x) = g(x)\}$) dla pewnych $f, g \in \operatorname{Alg}(X^n, X)$.

Poniższy *lemat o zgodności homomorfizmu z wartościowaniem* jest często stosowany:

$$X, Y \in \mathcal{A}_\nu,\ h : X \xrightarrow{\cdot} Y,\ \varphi : V \to X,\ t \in \operatorname{Term} \implies h(t[\varphi]_X) = t[h \circ \varphi]_Y.$$

W szczególności w wyżej opisanej sytuacji:

$$h(t[a_1, \dots, a_n]_X) = t[h(a_1), \dots, h(a_n)]_Y,$$
$$h(c_X) = c_Y.$$

$\langle$Indukcja na złożoność termu t $\dots\rangle$.

9.1.7. Algebry definiowalne równościowo. Ustalmy sygnaturę $\nu : \Omega \to \mathbb{N}$, przeliczalny zbiór „zmiennych formalnych" $V = \{v_0, v_1, v_2, \dots\}$ rozłączny ze zbiorem Ω, $V \cap \Omega = \varnothing$ i relację ρ (*tożsamości formalne*) w algebrze $T = \operatorname{Term}_\nu(V)$; $\rho \subset T^2$.

Łatwo sprawdzić, że klasa

$$\mathcal{C} = \{X \in \mathcal{A}_\nu \mid \forall\, (t, s) \in \rho\ \forall\, \varphi : V \to X\ [t[\varphi]_X = s[\varphi]_X]\}$$

jest zamknięta ze względu na izomorfizmy oraz że

$$\mathcal{C} = \{X \in \mathcal{A}_\nu \mid \forall\, (t, s) \in \rho\ \forall\, f : T \xrightarrow{\cdot} X\ [f(t) = f(s)]\}.$$

$\langle$Wpierw sprawdzamy powyższą równość, a następnie implikację: $X \in \mathcal{C}$, $Y \in \mathcal{A}_\nu$, $g : X \xrightarrow{\sim} Y \implies Y \in \mathcal{C}\rangle$.

Klasa $\mathcal{C}$ wyznacza więc podkategorię pełną $\mathcal{A}_{\nu\rho}$ kategorii $\mathcal{A}_\nu$. Mówimy, że jest to *kategoria definiowalna równościowo* (*rozmaitość*, *warieta*) algebr o sygnaturze ν wyznaczona przez relacje ρ.

Mechanicznym rachunkiem sprawdzamy, że kategoria $\mathcal{A}_{\nu\rho}$ ma wszystkie własności (1)–(9) przysługujące kategorii $\mathcal{A}_\nu$, przy czym:

Ad (3). $(\prod X)_{\mathcal{A}_{\nu\rho}} = (\prod X)_{\mathcal{A}_\nu}$ dla $I \in \mathbb{V}$, $X : I \to \mathcal{A}_{\nu\rho}$.

$\langle$Wystarczy sprawdzić, że $(\prod X)_{\mathcal{A}_\nu} \in \mathcal{A}_{\nu\rho}\rangle$.

Ad (4). $\operatorname{Sub}_{\mathcal{A}_{\nu\rho}} X = \operatorname{Sub}_{\mathcal{A}_\nu} X$ dla $X \in \mathcal{A}_{\nu\rho}$ oraz $(X|A)_{\mathcal{A}_{\nu\rho}} = (X|A)_{\mathcal{A}_\nu}$ dla $A \in \operatorname{Sub}_{\mathcal{A}_\nu} X$.
Ad (6). $\operatorname{Congr}_{\mathcal{A}_{\nu\rho}} X = \operatorname{Congr}_{\mathcal{A}_\nu}$ dla $X \in \mathcal{A}_{\nu\rho}$ oraz $(X/R)_{\mathcal{A}_{\nu\rho}} = (X/R)_{\mathcal{A}_\nu}$ dla $R \in \operatorname{Congr}_{\mathcal{A}_\nu} X$.
Ad (7). $\langle E\rangle_{\mathcal{A}_{\nu\rho}} = \langle E\rangle_{\mathcal{A}_\nu}$ dla $X \in \mathcal{A}_{\nu\rho}$, $E \subset X$ oraz $\mathcal{G}_{\mathcal{A}_{\nu\rho}}(X) = \mathcal{G}_{\mathcal{A}_\nu}(X)$ (te same podzbiory generujące).
Ad (9). Dla $X \in \mathcal{A}_{\nu\rho} : \mathcal{I}_{\mathcal{A}_{\nu\rho}}(X) = \mathcal{I}_{\mathcal{A}_\nu}(X) =: \mathcal{I}(X)$ i analogicznie dla podzbiorów gęstych i bazowych; $\mathcal{B}(X) \subset D(X) \subset \mathcal{G}(X)$, $\mathcal{B}(X) = \mathcal{I}(X) \cap \mathcal{G}(X)$.

Jeżeli kategoria $\mathcal{A}_{\nu\rho}$ jest nietrywialna, tzn. $\operatorname{card} Z \geqslant 2$ dla pewnego $Z \in \mathcal{A}_{\nu\rho}$, to baza obiektu wolnego w $\mathcal{A}_{\nu\rho}$ jest maksymalnym podzbiorem niezależnym i minimalnym podzbiorem generującym; jeżeli przy tym nietrywialna algebra Z jest skończona, to dowolne dwie bazy algebry wolnej w $\mathcal{A}_{\nu\rho}$ są równoliczne i można mówić o *randze* takiej algebry.

9.1.8. Algebry wolno definiowalne równościowo. Na dowolnym zbiorze E można rozpiąć algebrę wolną w kategorii $\mathcal{A}_{\nu\rho}$ w następujący sposób:

W algebrze termów $S = \operatorname{Term}_\nu(E)$ określamy kongruencję:

$$\sigma = \{(u,v) \in S^2 \mid \forall\, X \in \mathcal{A}_{\nu\rho},\ h : S \xrightarrow{\cdot} X\ [h(u) = h(v)]\}.$$

Wówczas $S/\sigma \in \mathcal{A}_{\nu\rho}$, $\iota = \{a \mapsto [a]_\sigma \mid a \in E\} : E \hookrightarrow S/\sigma$ i S/σ jest algebrą wolną w $\mathcal{A}_{\nu\rho}$ o bazie $\iota : E \hookrightarrow S/\sigma$. $\langle$Dowód ogólny nie różni się istotnie od bezproblemowego dowodu dla grupoidów$\rangle$.

Łatwo sprawdzić, że kategorie $\mathcal{A}_\nu$ i $\mathcal{A}_{\nu\rho}$ są z multyplikatywnością kongruencji, tzn. dla dowolnej algebry X:

$$\varnothing \neq \mathcal{F} \subset \operatorname{Congr} X \implies \bigcap \mathcal{F} \in \operatorname{Congr} X.$$

Algebrę $X \in \mathcal{A}_{\nu\rho}$ można określić, podając jej tak zwaną *reprezentację van Dycka* (E, R), czyli zbiór E traktowany jako baza algebry wolnej Y w kategorii $\mathcal{A}_{\nu\rho}$, oraz relację $R \subset Y^2$ taką, że $X \simeq Y/\bar{R}$, gdzie $\bar{R} = \bigcap\{S \in \operatorname{Congr} Y \mid R \subset S\}$ – *domknięcie kongruencyjne* relacji S.

9.1.9. Elementy odwracalne i regularne w półgrupie. Grupy. Dla półgrupy $G \in \mathrm{Sgr}_1$ określamy dwa podzbiory:

1) $\mathcal{U}(G) := \{a \in G \mid \exists\, b \in G : ab = ba = 1\}$ – *elementy odwracalne*, *jedności*.
2) $\mathcal{R}(G) := \{a \in G \mid \forall\, b,c \in G : (ab = ac \ \Rightarrow\ b = c) \ \wedge\ (ba = ca \ \Rightarrow\ b = c)\}$ – *elementy regularne*, *elementy skracalne*.

Podstawowe fakty:

(1) Dla $a \in \mathcal{U}(G)$ element $b \in G$ taki, że $ab = ba = 1$ istnieje dokładnie jeden $\langle$jeżeli jeszcze $ac = ca = 1$, to $c = c \cdot 1 = c(ab) = (ca)b = 1 \cdot b = b\rangle$; nazywamy go *elementem odwrotnym* do a i oznaczamy a^{-1}. W przypadku notacji addytywnej używamy terminu *element przeciwny* i oznaczenie: $-a$.
(2) $1 \in \mathcal{U}(G)$, $\forall\, a,b \in \mathcal{U}(G) : ab, a^{-1} \in \mathcal{U}(G)$, $(ab)^{-1} = b^{-1}a^{-1}$, $(a^{-1})^{-1} = a$.
(3) $\mathcal{U}(G) \subset \mathcal{R}(G)$.
(4) $\forall\, a,b \in \mathcal{R}(G) : ab \in \mathcal{R}(G)$, a więc $\mathcal{U}(G) \subsetneq \mathcal{R}(G) \subsetneq G$.
(5) Jeżeli jeszcze $H \in \mathrm{Sgr}_1$ i $f : G \xrightarrow{\cdot} H$, to

$$\forall\, a \in \mathcal{U}(G) : f(a) \in \mathcal{U}(H) \ \ \wedge\ \ f(a)^{-1} = f(a^{-1}).$$

$\langle$Dowody praw (2)–(5) sprowadzają się do mechanicznych przeliczeń$\rangle$.

Grupą nazywamy półgrupę $G \in \mathrm{Sgr}_1$, w której każdy element jest odwracalny; $\mathcal{U}(G) = G$.

9.1.10. Własności grup. Klasa Gr wszystkich grup tworzy podkategorię pełną kategorii Sgr_1; $\mathrm{Gr} \underset{\circ}{\subset} \mathrm{Sgr}_1$.

Chcąc traktować kategorię Gr jako rozmaitość (czyli kategorię algebr definiowalną równościowo), określamy ją w sposób równoważny jako podkategorię pełną kategorii Alg_ν algebr o sygnaturze $\nu = \{e \mapsto 0, \lambda \mapsto 1, \omega \mapsto 2\}$ zdefiniowaną przez równości (oznaczamy $x^{-1} = \lambda x$, $xy = \omega\, xy$):

(i) $(xy)z = x(yz)$ – łączność
(ii) $ex = xe = x$ – element neutralny
(iii) $xx^{-1} = x^{-1}x = e$ – elementy odwrotne.

Dołączając jeszcze postulat przemienności: $xy = yx$, otrzymujemy, też definiowalną równościowo, kategorię Ab *grup przemiennych* lub *abelowych.*

Ponieważ element neutralny jest wyznaczony jednoznacznie, więc określając grupę G podaje się zwykle tylko działanie $\cdot : G^2 \to G$.
Jeżeli dla $G, G' \in \mathrm{Gr}$ odwzorowanie $f : G \to G'$ spełnia warunek $\forall\, a, b \in G : f(ab) = f(a)f(b)$, to $f(1_G) = 1_{G'} = 1'$ $\quad \langle 1 = 1 \cdot 1,\ f(1) = f(1) \cdot f(1),\ f(1)f(1)^{-1} = 1'$, skąd $1' = f(1)\rangle$, a więc f jest homomorfizmem grupy G w grupę G', $f : G \xrightarrow{\cdot} G'$.

9.1.11. Podgrupy, podgrupy normalne. Dla grupy G i zbioru $H \subset G$:

$$H \underset{\cdot}{\subset} G \iff 1 \in H \ \wedge\ \forall\, a, b \in H : ab, a^{-1} \in H.$$

$\langle$Kategoria grup jest definiowalna równościowo$\rangle$.

Kongruencje w grupie G są to dokładnie rownoważności $R \in \mathrm{Equ}\, G$ spełniające warunek

$$\forall\, a, b, c, d \in G\ (a\ R\ c \ \wedge\ b\ R\ d \ \Rightarrow\ ab\ R\ cd \ \wedge\ a^{-1}\ R\ c^{-1}).$$

Jeżeli $f : G \xrightarrow{\cdot} G'$ jest homomorfizmem grup, to $\mathrm{Ker}\, f := \{a \in G \mid f(a) = 1\} \underset{\cdot}{\subset} G$. Homomorfizm f jest injektywny wtt, gdy $\mathrm{Ker}\, f = \{1\}$ $\quad \langle f(a) = f(b) \Leftrightarrow f(ab^{-1}) = 1 \Leftrightarrow \ldots\rangle$. Jądro $H = \mathrm{Ker}\, f$ homomorfizmu f spełnia warunek:

$$(*) \qquad \forall\, a, b \in G : b \in H \ \Rightarrow\ aba^{-1} \in H$$

lub, w postaci równoważnej:

$$(**) \qquad \forall\, a, b \in G : aH = Ha \quad (aH := \{ax \mid x \in H\} \text{ itp.}).$$

Podgrupy o tej własności nazywamy *normalnymi*; ich ogół oznaczamy $\mathrm{NSub}\, G$. Zwyczajowo notujemy: $H < G \ :\Leftrightarrow\ H \underset{\cdot}{\subset} G$, $H \lhd G \ :\Leftrightarrow\ H \in \mathrm{NSub}\, G$.
Oczywiście $\{1\}, G \in \mathrm{NSub}\, G$, $G \in \mathrm{Ab} \ \Rightarrow\ \mathrm{NSub}\, G = \mathrm{Sub}\, G$.

Kongruencje w grupie G możemy utożsamiać z jej podgrupami normalnymi, gdyż mamy bijekcje kanoniczne:

$$\varphi = \{H \mapsto \{(a, b) \in G^2 \mid a^{-1}b \in H\} \ldots\} : \mathrm{NSub}\, G \hookrightarrow\!\!\!\!\rightarrow \mathrm{Congr}\, G,$$
$$\psi = \{R \mapsto \{a \in G \mid a\ R\ 1\} \ldots\} : \mathrm{Congr}\, G \hookrightarrow\!\!\!\!\rightarrow \mathrm{NSub}\, G; \qquad \varphi^{-1} = \psi.$$

$\langle$Sprawdzamy, że $\varphi : \mathrm{NSub} \to \mathrm{Congr}\, G$, $\psi : \mathrm{Congr}\, G \to \mathrm{NSub}\, G$, $\psi \circ \varphi \subset \mathrm{id}$, $\varphi \circ \psi \subset \mathrm{id}$, $\ldots\rangle$; dla $H \lhd G$ oznaczamy $G/H := G/\varphi(H)$.

9.1.12. Warstwy podgrupy w grupie. Twierdzenie Lagrange'a. Dla dowolnej podgrupy H grupy G możemy utworzyć zbiory: $(G/H)_l := \{aH \mid a \in G\}$ – *warstwy lewostronne* H w G, $(G/H)_r := \{Ha \mid a \in G\}$ – *warstwy prawostronne* H w G. Oczywiście $H \lhd G \Rightarrow (G/H)_l = (G/H)_r = G/H$.

W przypadku ogólnym zbiory te są równoliczne $\langle\{aH \mapsto Ha \mid a \in G\} : (G/H)_l \hookrightarrow\!\!\!\!\rightarrow (G/H)_r \ldots\rangle$; ich wspólną moc nazywamy *indeksem* podgrupy H w grupie G i oznaczamy $[G : H]$.

Ze względu na dualność, w dalszym ciągu mówiąc „warstwa", będziemy mieli na myśli warstwy lewostronne i będziemy notować $G/H := (G/H)_l$.

Warstwy są parami rozłączne $\langle aH \neq bH \Rightarrow aH \cap bH = \varnothing \ldots\rangle$ oraz równoliczne z H $\langle\{x \mapsto ax \mid x \in H\} : H \hookrightarrow\!\!\!\!\rightarrow aH \ldots\rangle$. Ponadto $G = \bigcup_{a \in G} aH$ $\langle a \in G \Rightarrow a = a \cdot 1 \in aH\rangle$.

Z powyższego wynika ważne *twierdzenie Lagrange'a*

$$G \in \mathrm{Gr} \ \wedge \ H < G \Rightarrow |G| = |H| \cdot [G : H].$$

Zwyczajowo dla grupy skończonej G jej moc nazywamy *rzędem* i oznaczamy $\operatorname{rk} G$; jeśli G jest nieskończona, notujemy: $\operatorname{rk} G = \infty$. Tak więc dla grupy skończonej rząd podgrupy jest dzielnikiem rzędu grupy; ilorazem jest indeks podgrupy w grupie.

9.1.13. Półgrupa ułamków półgrupy G. Dla danej półgrupy przemiennej $G \in \mathrm{Sgrc}_1$ określamy w półgrupie $G \times \mathcal{R}(G)$ (zob. 9.1.9) *relację proporcjonalności*

$$(a, b) \equiv (c, d) \ :\Longleftrightarrow \ ad = bc.$$

(i) Relacja $\equiv$ jest kongruencją w $G \times \mathcal{R}(G)$; możemy więc określić półgrupę ilorazową $\widehat{G} := (G \times \mathcal{R}(G))/_{\equiv}$ zwaną *półgrupą ułamków półgrupy* G. Dla $a \in G$, $b \in \mathcal{R}(G)$. Oznaczamy $\frac{a}{b} := [(a, b)]_R$. Mówiąc zwyczajowo, że $\frac{a}{b}$ jest ułamkiem o *liczniku* a i *mianowniku* b, należy zachować ostrożność, gdyż w istocie rzeczy terminy te odnoszą się do pary (a, b) reprezentującej element $\frac{a}{b}$. Tak więc

$$\forall\,(a, b), (c, d) \in G \times \mathcal{R}(G) : \frac{a}{b} = \frac{c}{d} \iff ad = bc, \ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \ 1_{\widehat{G}} = \frac{1}{1}.$$

(ii) *Injekcja kanoniczna* $\iota = \{a \mapsto \frac{a}{1} \ldots\} : G \hookrightarrow \widehat{G}$ jest homomorfizmem, a więc włożeniem; traktujemy ją jako utożsamienie $G \subset \widehat{G}$.
(iii) $\mathcal{R}(G) \subset \mathcal{U}(\widehat{G})$,

$$\forall\,(a, b) \in G \times \mathcal{R}(G) : \frac{a}{b} \in \mathcal{U}(\widehat{G}) \iff a \in \mathcal{R}(G) \ \wedge \ \left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

(iv) Injekcja kanoniczna ι jest w kategorii Sgrc_1 uniwersalnym homomorfizmem przeprowadzającym elementy regularne w elementy odwracalne, tzn.

$$\forall\, H \in \mathrm{Sgrc}_1, \ f : G \longrightarrow H \ \{f(\mathcal{R}(G)) \subset \mathcal{U}(H) \implies \exists!\, g : \widehat{G} \longrightarrow H \ [f = g \circ \iota]\}.$$

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\iota"'] & H \\ \widehat{G} \arrow[ur, "g"'] & \end{tikzcd}$$

Dowody faktów (i)–(iv) nie przedstawiają większych trudności (zadanie 14).

9.1.14. Pierścień $\mathbb{Z}$ liczb całkowitych. Jeżeli półgrupa przemienna G jest *regularna*, tzn. $\mathcal{R}(G) = G$, to $\widehat{G}$ jest grupą. W szczególności, biorąc półgrupę addytywną $(\mathbb{N}, +, 0)$ liczb naturalnych, otrzymamy grupę addytywną $\mathbb{Z}$ *liczb całkowitych*. Ze względu na notację addytywną zamiast o ułamkach mówimy w tym przypadku o różnicach.

Po utożsamieniu $\mathbb{N} \subset \mathbb{Z}$ $\quad\langle n = n - 0\rangle$ łatwo widać, że $\mathbb{Z} = \mathbb{N} \cup \{-n \mid n \in \mathbb{N}^*\}$. $\langle$Dla $k \in \mathbb{Z} \setminus \mathbb{N}$: $k = m - n$, gdzie $m, n \in \mathbb{N}^*$, i wówczas $k = 0 - (n - m) = -(n - m)$, $n - m \in \mathbb{N}^*\rangle$.
W zbiorze $\mathbb{Z}$ wprowadzamy w naturalny sposób porządek liniowy: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, otrzymując w ten sposób grupę uporządkowaną $(\mathbb{Z}, +, 0, \leqslant)$.

Oznaczamy $\mathbb{Z}_+ = \mathbb{N}$, $\mathbb{Z}_+^* = \mathbb{N}^*$, $\mathbb{Z}_- = \{-n \mid n \in \mathbb{N}\}$, $\mathbb{Z}_-^* = \mathbb{Z}_- \setminus \{0\}$, $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$. Analogiczne oznaczenia przyjmiemy dla wprowadzonych później ciał liczbowych $\mathbb{Q}$ i $\mathbb{R}$.

W $\mathbb{Z}$ określamy też w naturalny sposób mnożenie będące rozszerzeniem mnożenia w $\mathbb{N}$, kładąc dla $a, b \in \mathbb{N}^*$, $c \in \mathbb{N}$: $(-a)c = c(-a) = -ac$, $(-a)(-b) = ab$.
Otrzymujemy w ten sposób pierścień $\mathbb{Z}$ $(\in \mathrm{Rinc}_1)$ – *pierścień liczb całkowitych* $\quad\langle \dots \rangle$.

Zachowujemy dla $a, b, c \in \mathbb{Z}$ standardową notację, np. $a + bc = a + (b \cdot c)$, $a \mid b \Leftrightarrow \exists\, c \in \mathbb{Z} : b = ac$, $a \perp b \Leftrightarrow \neg\exists\, p \in \mathbb{P} : p \mid a \ \wedge\ p \mid b$ itp.

Podstawowe prawa też w sposób naturalny przenoszą się na $\mathbb{Z}$. Tak na przykład mamy *twierdzenie o dzieleniu z resztą*:

$$\forall\, a \in \mathbb{Z},\ b \in \mathbb{N}^*\ \exists!\, q, r \in \mathbb{Z} : a = bq + r \ \wedge\ 0 \leqslant r < b;$$

oznaczamy $[\frac{a}{b}] = q$ (iloraz), $a \pmod b = r$ (reszta). $\quad\langle$Rozpatrujemy przypadki $\dots\rangle$.

Wykorzystując algorytm Euklidesa (rozdział 5) łatwo udowodnić poniższe kryterium pierwszości względem siebie dwu liczb naturalnych:

$$\forall\, a, b \in \mathbb{N}^*\ (a \perp b \iff \exists\, \alpha, \beta \in \mathbb{Z} : \alpha a + \beta b = 1).$$

9.1.15. Ciało ułamków pierścienia całkowitego $\mathbb{Z} \subset \mathbb{Q}$. Pierścień przemienny R $(\in \mathrm{Rinc}_1)$ nietrywialny $(0 \neq 1)$ nazywamy:

a) *ciałem*, gdy $\mathcal{U}(R^*) = R^*$, tj. każdy element niezerowy jest odwracalny $(\forall\, a \in R^* = R \setminus \{0\}\ \exists\, b \in R^* : ab = 1, b = a^{-1})$;

b) *pierścieniem całkowitym*, gdy $\mathcal{R}(R^*) = R^*$, tj. każdy element niezerowy jest regularny (warunek równoważny: $\forall\, a, b \in R^* : ab \in R^*$); element $a \in R^*$ nazywamy zwyczajowo *dzielnikiem zera*, gdy $\exists\, b \in R^* : ab = 0$. Tak więc pierścień całkowity to pierścień przemienny, nietrywialny, bez dzielników zera). Typowym przykładem takiego pierścienia jest pierścień $\mathbb{Z}$ liczb całkowitych.

Traktując dany pierścień całkowity Z jako półgrupę multyplikatywną $(Z, \cdot, 1)$ możemy utworzyć dla niego półgrupę ułamków Q (9.1.10, $Q = \{\frac{a}{b} \mid a \in Z,\ b \in Z^*\}$). W Q określamy dodawanie: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, otrzymując w ten sposób ciało – *ciało ułamków pierścienia Z* $\quad\langle \dots \rangle$

Iniekcja kanoniczna $\iota = \{a \mapsto \frac{a}{1} \dots\} : Z \hookrightarrow Q$ daje utożsamienie $Z \subset Q$. Jest ona uniwersalnym homomorfizmem injektywnym pierścienia Z w ciało. Oznaczając przez Fld (od *Fields*) kategorię ciał możemy ten fakt zapisać symbolicznie:

$$\forall\, K \in \mathrm{Fld},\ f : Z \hookrightarrow K\ \exists!\, g : Q \longrightarrow K : f = g \circ \iota.$$

(Homomorfizm ciał jest zawsze injektywny, $g : Q \hookrightarrow K$ $\langle$HP: $g(x) = 0$, $x \neq 0$. Wówczas $1 = g(1) = g(xx^{-1}) = g(x) \cdot g(x^{-1}) = 0$ ↯$\rangle$).
Tak więc Q jest minimalnym rozszerzeniem Z do ciała. $\langle$Mechanicznym rachunkiem sprawdzamy zgodność odwzorowania g z 9.1.19 z dodawaniem $\ldots\rangle$.

Stosując tę konstrukcję do pierścienia $\mathbb{Z}$ liczb całkowitych otrzymujemy ciało $\mathbb{Q}$ *liczb wymiernych*.

9.1.16. Podpierścienie i ideały. Kategoria Rin_1 pierścieni (z jedynką) jest definiowalna równościowo (9.1.7), a więc stosuje się do niej cała teoria algebr tego rodzaju. W szczególności, dla $R \in \mathrm{Rin}_1$ podpierścienie R stanowią zbiór:

$$\mathrm{Sub}(R) = \{A \subset R \mid (A + A) \cup (A - A) \cup AA \subset A,\ 1 \in A\}$$

$(A + A = \{a + b \mid a, b \in A\}$ itp., $0 = 1 - 1 \in A)$.

Natomiast każdej kongruencji w R odpowiada podgrupa $\mathcal{I}$ grupy addytywnej $(R, +)$ pierścienia R; podgrupa ta spełnia dodatkowo warunek:

(*) $$\forall\, a, b, c, d \in R : a - b, c - d \in \mathcal{I} \;\Rightarrow\; ac - bd \in \mathcal{I},$$

który jest równoważny warunkowi:

(**) $$\mathcal{I}R \cup R\mathcal{I} \subset \mathcal{I}.$$

$\langle(**) \Rightarrow (*)$ $\langle$Jeżeli $a-b, c-d \in \mathcal{I}$, to $ac-bd = ac-ad+ad-bd = a(c-d)+(a-b)d \in \mathcal{I}\rangle$. $(*) \Rightarrow (**)$ $\langle$Jeżeli $a \in \mathcal{I}$, $x \in R$, to $ax, xa \in \mathcal{I}$, gdyż $a - 0, x - x \in \mathcal{I}\rangle\rangle$.

Podgrupy o tej własności nazywamy *ideałami* w pierścieniu R; oznaczamy $\mathcal{I}(R) := \{\mathcal{I} \subset R \mid 0 \in \mathcal{I}, \mathcal{I} + \mathcal{I} \subset \mathcal{I}, \mathcal{I}R \cup R\mathcal{I} \subset R\}$ (jeśli $a \in \mathcal{I}$, to $-a = (-1)a \in \mathcal{I}$, czyli $-\mathcal{I} \subset \mathcal{I}$).

Zauważmy, że dla $\mathcal{I} \in \mathcal{I}(R) : 1 \in \mathcal{I} \Leftrightarrow \mathcal{I} = R$, a więc $\mathcal{I}(R) \cap \mathrm{Sub}(R) = \{R\}$. Mówimy, że R jest *ideałem niewłaściwym* i *podpierścieniem niewłaściwym* pierścienia R; wszystkie pozostałe ideały i podpierścienie R są *właściwe*.

Tak więc kongruencje w pierścieniu R możemy identyfikować z ideałami w tym pierścieniu (podobnie jak kongruencje w grupie identyfikujemy z podgrupami normalnymi tej grupy – por. 1.9.11), dla ideału $\mathcal{I} \in \mathcal{I}(R)$ odpowiadający mu pierścień ilorazowy oznaczamy $R/\mathcal{I}$.

Kategoria Fld ($\underset{\circ}{\subset}$ Rin_1) ciał już nie jest definiowalna równościowo; np. $\mathbb{Q} \in \mathrm{Fld}$, $\mathbb{Q}^2 = \mathbb{Q} \times \mathbb{Q} \in \mathrm{Rin}_1 \setminus \mathrm{Fld}$.

9.1.17. Kongruencje w pierścieniu $\mathbb{Z}$. W szczególności dla pierścienia $\mathbb{Z}$ liczb całkowitych: $\mathrm{Sub}(\mathbb{Z}) = \{\mathbb{Z}\}$, $\mathcal{I}(\mathbb{Z}) = \{m\mathbb{Z} \mid m \in \mathbb{N}\}$ $\langle \ldots \rangle$; w przypadku gdy $m \geqslant 2$ otrzymujemy *pierścień reszt modulo* m, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. Kongruencję odpowiadającą ideałowi $m\mathbb{Z}$ ($m \geqslant 1$) nazywamy *przystawaniem modulo* m, i oznaczamy tradycyjnie $\equiv \pmod{m}$.

Tak więc dla $a, b \in \mathbb{Z}$:

$$a \equiv b \pmod{m} \iff a - b \in m\mathbb{Z} \iff a \ (\mathrm{mod}\ m) = b \ (\mathrm{mod}\ m);$$

kongruencje takie możemy dodawać i mnożyć stronami. Dzielić stronami możemy tylko przez liczbę $d \in \mathbb{Z}^*$ taką, że $d \mid a$, $d \mid b$ i $d \perp m$ $\langle$jeśli $a = kd$, $b = ld$ i $m \mid a - b$, to $m \mid (k - l)d$, a więc $m \mid (k - l)$, czyli $k \equiv l \pmod{m}\rangle$.

Dla dowolnego pierścienia R ($\in \mathrm{Rin}_1$) grupę *jedności*, czyli ogół elementów odwracalnych półgrupy multyplikatywnej $(R, \cdot, 1)$, oznaczamy $\mathcal{U}(R) = \{a \in R \mid \exists\, b \in R : ab = ba = 1\}$. W szczególności dla pierścienia $\mathbb{Z}_m = (\{0, 1, \ldots, m-1\}, +, \cdot)$ $(m \geqslant 2)$ $\mathcal{U}(\mathbb{Z}_m) = \{a \in \{1, \ldots, m-1\} \mid a \perp m\}$. Rząd grupy $\mathcal{U}(\mathbb{Z}_m)$ oznaczamy za Eulerem $\varphi(m)$ (*funkcja Eulera*).

Na przykład $\varphi(12) = |\{1, 5, 7, 11\}| = 4$, $p \in \mathbb{P} \;\Rightarrow\; \varphi(p) = p - 1$.

Z funkcją tą wiąże się ważne *twierdzenie Eulera*:

$$\forall\, m \in \mathbb{N}_2 = \{2, 3, \ldots\},\ a \in \mathbb{Z}\ [a \perp m \;\Rightarrow\; a^{\varphi(m)} \equiv 1 \pmod{m}].$$

$\langle$Wniosek z twierdzenia Lagrange'a: w grupie skończonej $\mathcal{U}(\mathbb{Z}_m)$ rząd elementu jest dzielnikiem rzędu grupy$\rangle$.

Jako szczególny przypadek twierdzenia Eulera otrzymujemy *małe twierdzenie Fermata*:

$$\forall\, p \in \mathbb{P},\ a \in \mathbb{Z}\ [p \nmid a \;\Rightarrow\; a^{p-1} \equiv 1 \pmod{p}].$$

9.1.18. $\mathbb{Q}$ jako ciało uporządkowane. Liczba wymierna $a \in \mathbb{Q}$ ma jednoznacznie wyróżnioną *postać kanoniczną* $a = \frac{p}{q}$, gdzie $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ i $p \perp q$. W $\mathbb{Q}$ określamy naturalny porządek liniowy, kładąc dla liczb $a, b \in \mathbb{Q}$ w postaci kanonicznej $a = \frac{p}{q}$, $b = \frac{r}{s}$:

$$a \leqslant b \;:\Longleftrightarrow\; ps \leqslant qr.$$

Porządek ten jest zgodny z dodawaniem; $(\mathbb{Q}, +, \leqslant) \in \mathrm{OrdGr}$ (zob. 8.1.7. — spełniony jest warunek: $\forall\, x, y, z \in \mathbb{Q} : x \leqslant y \;\Rightarrow\; x + z \leqslant y + z$). Jest on również zgodny z mnożeniem, w tym sensie, że $\forall\, x, y \in \mathbb{Q} : x > 0 \;\wedge\; y > 0 \;\Rightarrow\; xy > 0$. Ciała i ogólniej pierścienie zaopatrzone w tego rodzaju porządek nazywamy *uporządkowanymi* – kategorie: OrdFld i OrdRin.

Ciało $\mathbb{Q}$ jest przeliczalne ($|\mathbb{Q}| = \aleph_0$), gdyż np. $\mathbb{N} \subset \mathbb{Q}$ i $\{\frac{p}{q} \mapsto (p, q) \mid p \in \mathbb{Z},\ q \in \mathbb{N}^*,\ p \perp q\} : \mathbb{Q} \hookrightarrow \mathbb{Z} \times \mathbb{N}^*$.

Jako zbiór liniowo uporządkowany ciało $\mathbb{Q}$ jest gęste, tzn. $\forall_{\substack{a,b \in \mathbb{Q} \\ a<b}}\ \exists\, c \in \mathbb{Q} : a < c < b$ $\quad\langle$np. $c = \frac{a+b}{2}\rangle$, i nie ma elementów ekstremalnych; $\forall\, a \in \mathbb{Q}\ \exists\, b, c \in \mathbb{Q} : b < a < c$.

Zbiór liniowo uporządkowany X nazywamy *ciągłym*, gdy każdy jego niepusty i ograniczony od góry podzbiór ma kres górny ($\forall\, \varnothing \neq A \subset X$ $[M(A) =$ majoranty $A \neq \varnothing \;\Rightarrow\; \sup A \in X]$); równoważnie (dualnie): gdy każdy jego niepusty i ograniczony od dołu podzbiór na kres dolny $\quad\langle$jeśli $\varnothing \neq B \subset X$ i $m(B) =$ minoranty $B \neq \varnothing$, to zbiór $A = m(B)$ jest niepusty i $M(A) \neq \varnothing$ gdyż $B \subset M(A)$, i jak łatwo sprawdzić $\inf B = \sup A$. Analogicznie uzasadniamy implikację w przeciwnym kierunku$\rangle$.

Mówiąc o ciągłości grupy uporządkowanej lub ciała uporządkowanego mamy na myśli ciągłość odpowiedniego zbioru liniowo uporządkowanego.

Ciało uporządkowane $\mathbb{Q}$ nie jest ciągłe, gdyż np. zbiór $A = \{a \in \mathbb{Q} \mid 0 < a \;\wedge\; a^2 < 2\}$ nie posiada kresu górnego w $\mathbb{Q}$ (zadanie 22).

9.1.19. Ciało $\mathbb{R}$ liczb rzeczywistych. Rozszerzamy ciało $\mathbb{Q}$ liczb wymiernych do ciągłego ciała $\mathbb{R}$ *liczb rzeczywistych* (konstrukcja Dedekinda):

$$\mathbb{R} := \{\alpha \mid \varnothing \neq \alpha \subsetneq \mathbb{Q},\ \forall\, x, y \in \mathbb{Q}\ (x < y \;\wedge\; y \in \alpha \;\Rightarrow\; x \in \alpha), \forall\, x \in \alpha\ \exists\, z \in \alpha\ x < z\}$$

(są to tzw. przekroje zbioru $\mathbb{Q}$ – niepuste i niepełne podzbiory $\mathbb{Q}$, lewostronnie porządkowo wysycone i bez elementów największych).

Strukturę ciała uporządkowanego wprowadzamy w $\mathbb{R}$, kładąc dla $\alpha, \beta \in \mathbb{R}$:

1°) $\alpha \leqslant \beta \iff \alpha \subset \beta$
2°) $\alpha + \beta = \{x + y \mid x \in \alpha,\ y \in \beta\}$, $0 = \{x \in \mathbb{Q} \mid x < 0\}$
3°) dla $\alpha, \beta \geqslant 0 \ \Rightarrow\ \alpha\beta = \{xy \mid 0 < x \in \alpha,\ 0 < y \in \beta\} \cup \mathbb{Q}_-$,
w pozostałych przypadkach
$\alpha < 0 \ \wedge\ \beta \geqslant 0 \ \Rightarrow\ \alpha\beta = -(-\alpha)\beta$,
$\alpha \geqslant 0 \ \wedge\ \beta < 0 \ \Rightarrow\ \alpha\beta = -\alpha(-\beta)$,
$\alpha < 0 \ \wedge\ \beta < 0 \ \Rightarrow\ \alpha\beta = (-\alpha)(-\beta)$.

Określamy również *injekcję kanoniczną* $\iota : \mathbb{Q} \hookrightarrow \mathbb{R}$, $\forall\, x \in \mathbb{Q} : \iota(x) = \{y \in \mathbb{Q} \mid y < x\} = (-\infty, x)_{\mathbb{Q}}$.

W ten sposób otrzymujemy ciało uporządkowane ciągłe $\mathbb{R}$, przy czym injekcja ι jest homomorfizmem w kategorii OrdFld – traktujemy ją jako identyfikację: $\mathbb{Q} \subset \mathbb{R}$ (zadanie 23).

9.1.20. Potęgowanie. Funkcje $\exp_a$ i $\log_a$ $(1 \neq a > 0)$. W ciele $\mathbb{R}$, wykorzystując jego ciągłość, określamy funkcje elementarne: *funkcję wykładniczą* i *funkcję logarytmiczną*.

I tak:

1) $\forall\, n \in \mathbb{N}^*,\ a \in \mathbb{R}_+^* = \{x \in \mathbb{R} \mid x > 0\}\ \exists!\, b \in \mathbb{R}_+^* : b^n = a$.

Dowód tego faktu znajdziemy w zadaniu 24.

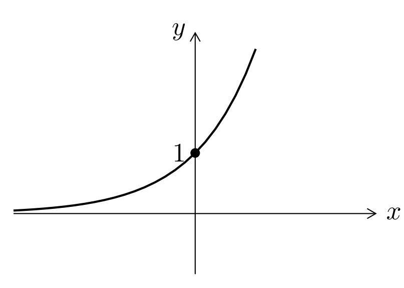
Dowody stwierdzeń z następnych punktów 2)–4) są analogiczne.
Jednoznacznie określoną liczbę $b > 0$ nazywamy *pierwiastkiem n-tego stopnia* z liczby a, oznaczamy: $\sqrt[n]{a}$. Dla $n = 2$ mówimy po prostu o *pierwiastku* – notacja: $\sqrt{a}$.

2) Po ustaleniu praw pierwiastkowania definiujemy potęgę o dowolnym wykładniku wymiernym, kładąc dla $a \in \mathbb{R}_+^*$, $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$: $a^{\frac{p}{q}} = \sqrt[q]{a^p}$. Przy takim określeniu spełnione są standardowe prawa potęgowania: *potęga potęgi*, *iloczyn potęg o równych podstawach*, *potęga iloczynu*.

3) Teraz możemy już zdefiniować potęgę o dowolnym wykładniku rzeczywistym x. Dla $a > 1$ kładziemy: $a^x = \sup\{a^w \mid w \in \mathbb{Q}, w < x\}$. Jeżeli $0 < a < 1$, to $a^x = ((a^{-1})^x)^{-1}$, $1^x = 1$.

Standardowe prawa potęgowania są zachowane. Dla $a \in \mathbb{R}_+^* \setminus \{1\}$ funkcję $\exp_a = \{x \mapsto a^x \mid x \in \mathbb{R}\}$ nazywamy *wykładniczą* (a – *podstawa*, x – *wykładnik*).

4) Dla $1 < a \in \mathbb{R}$ funkcja $\exp_a : \mathbb{R} \to \mathbb{R}_+^*$ jest silnie rosnąca.



Ponadto $\forall\, y \in \mathbb{R}_+^* \ \exists\, x \in \mathbb{R} : y = a^x \quad \langle x = \sup\{w \in \mathbb{Q} \mid a^w < y\}\rangle$.

Tak więc w tym przypadku $\exp_a : \mathbb{R} \hookrightarrow\!\!\!\!\rightarrow \mathbb{R}_+^*$; jest to izomorfizm grupy uporządkowanej $(R, +, \leqslant)$ na grupę uporządkowaną $(\mathbb{R}_+^*, \cdot, \leqslant)$.

Jeżeli $0 < a < 1$, to funkcja $\exp_a : R \to \mathbb{R}_+^*$ jest silnie malejąca i również odwracalna. $\langle$Dla $y \in \mathbb{R}_+^* : y = a^x$, gdzie $x = -z$, $(a^{-1})^z = y\rangle$.

Zatem dla $a \in \mathbb{R}_+^* \setminus \{1\}$, $\exp_a : \mathbb{R} \hookrightarrow\!\!\!\!\rightarrow \mathbb{R}_+^*$. Bijekcja odwrotna $\log_a = (\exp_a)^{-1}$, to *funkcja logarytmiczna* (*logarytm*) *o podstawie* a.

9.1.21. Działanie grupy na zbiorze. Dla ustalonej grupy G (ogólniej, półgrupy $G \in \mathrm{Sgr}_1$) określamy kategorię zwyczajną $\mathcal{T} = \mathcal{T}_G$ *zbiorów, na których działa* grupa G, krótko – *G-przestrzeni*:

1°) obiekty kategorii $\mathcal{T}$ są postaci $(X, \cdot)$, gdzie $\cdot : G \times X \to X$ (dla $\alpha \in G$, $x \in X$ notujemy $\alpha x = \alpha \cdot x$) i

$$\forall\, \alpha, \beta \in G,\ x \in X : \alpha(\beta x) = (\alpha\beta)x, \quad 1x = x \text{ (tu } 1 = 1_G),$$

2°) morfizmami są odwzorowania $f : X \to X'$ takie, że $\forall\, \alpha \in G,\ x \in X : f(\alpha x) = \alpha f(x)$.

Natychmiast widać, że kategoria $\mathcal{T}_G$ jest definiowalną równościowo kategorią algebr ogólnych o sygnaturze $\nu : G \to \{1\}$.

9.1.22. Moduły i przestrzenie wektorowe. Przy ustalonym pierścieniu $R \in \mathrm{Rin}_1$ określamy kategorię zwyczajną Mod_R *modułów* (*lewostronnych*) nad R jako podkategorię pełną zestawienia $\mathrm{Ab} \vartriangle \mathcal{T}$, gdzie $\mathcal{T}$ jest kategorią $(R, \cdot, 1)$-przestrzeni.

Obiekty kategorii Mod_R postaci $(X, +, \cdot)$ $((X, +) \in \mathrm{Ab},\ (X, \cdot) \in \mathcal{T})$ spełniają warunek:

$$\forall\, \alpha, \beta \in R,\ x, y \in X : (\alpha + \beta)x = \alpha x + \beta x,\ \alpha(x + y) = \alpha x + \alpha y.$$

Tak więc:
$(X, +, \cdot) \in \mathrm{Mod}_R \iff [(X, +)$ – grupa abelowa, $\cdot : R \times X \to X,\ \forall\, \alpha, \beta \in R,\ x, y \in X : \alpha(\beta x) = (\alpha\beta)x,\ 1x = x,\ (\alpha + \beta)x = \alpha x + \beta x,\ \alpha(x + y) = \alpha x + \alpha y]$.

Kategoria Mod_R jest definiowalną równościowo kategorią algebr ogólnych i homomorfizmami w tej kategorii są odwzorowania $f : X \to X'$ $(X, X' \in \mathrm{Mod}_R)$ spełniające warunek:

$$\forall\, x, y \in X,\ \alpha \in R\, [f(x + y) = f(x) + f(y),\ f(\alpha x) = \alpha f(x)].$$

Sam pierścień R możemy traktować jako moduł nad sobą samym; mamy więc moduły produktowe $R^2, R^3, \ldots \in \mathrm{Mod}_R$.

W przypadku gdy R jest ciałem, moduły nazywamy *przestrzeniami wektorowymi* nad R i kategorię Mod_R oznaczamy Vect_R; dla $X \in \mathrm{Vect}_R$ elementy zbioru X nazywamy *wektorami*; elementy ciała R to *skalary*.

Jeśli R jest ciałem liczb rzeczywistych i $n \in \mathbb{N}$, to $\mathbb{R}^n$ nazywamy *przestrzenią kartezjańską n-wymiarową*; $\mathbb{R}^1 = \mathbb{R}$ – *prosta kartezjańska*, $\mathbb{R}^2$ – *płaszczyzna kartezjańska*.

9.1.23. Liniowa niezależność. Baza przestrzeni wektorowej. Jeżeli K jest ciałem, $X \in \mathrm{Vect}_K$ i $A \subset X$, to $\langle A \rangle = \{\sum_{i=1}^{n} \alpha_i a_i \mid n \in \mathbb{N},\ a : I_n \to A,\ \alpha : I_n \to K\}$ jest podprzestrzenią X generowaną przez A. Zbiór A nazywamy *liniowo niezależnym*, gdy $\forall\, a \in A : a \notin \langle A \setminus \{a\} \rangle$.

Łatwo widać, że (zadanie 26):

(i) Zbiór $A \subset X$ jest liniowo niezależny wtt, gdy

$$\forall\, n \in \mathbb{N}^*,\ a : I_n \hookrightarrow A,\ \alpha : I_n \to K \left[\sum_{i=1}^{n} \alpha_i a_i = 0 \implies \forall\, i \in I_n : \alpha_i = 0 \right].$$

(ii) Z lematu Zorna wynika, że zbiór liniowo niezależny można rozszerzyć do maksymalnego zbioru liniowo niezależnego.

(iii) Maksymalny zbiór liniowo niezależny $A \subset X$ jest *generujący* (tzn. $\langle A \rangle = X$).

(iv) Zbiór liniowo niezależny i generujący jest niezależny (w sensie strukturalnym – rozdział 8), a więc jest bazą przestrzeni X.

Z (i)–(iv) wynika, że każda przestrzeń wektorowa $X \in \mathrm{Vect}_K$ jest wolna i każdy jej podzbiór liniowo niezależny można rozszerzyć do bazy.

9.1.24. Równania liniowe, macierze, wyznaczniki. Przy ustalonym ciele (ogólniej – pierścieniu przemiennym) R jednym z typowych problemów jest rozwiązywanie układów równań liniowych:

$$(*) \qquad \begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ \ldots \qquad\qquad\qquad \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m, \end{cases}$$

gdzie $n, m \in \mathbb{N}^*$; $a_{ij}, b_j \in R$.

Funkcję $a : I_m \times I_n \to R$ nazywamy *macierzą* o m wierszach i n kolumnach i tradycyjnie notujemy w postaci tabeli:

$$A = \begin{bmatrix} a_{11}, & \ldots, & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{m1}, & \ldots, & a_{mn} \end{bmatrix}.$$

W przypadku $m = n$ macierz nazywamy *kwadratową*; odpowiedni układ (*) n równań o n niewiadomych rozwiązujemy metodą „przeciwnych współczynników", starając się – w przypadku ogólnym – nie wyróżniać żadnej niewiadomej. Dla $n = 3$ otrzymujemy np. $(-a_{11}a_{23}a_{32} + a_{13}a_{21}a_{32} + a_{11}a_{22}a_{33} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31})x_1 = -b_1a_{23}a_{32} + b_2a_{13}a_{32} + b_1a_{22}a_{33} - b_3a_{13}a_{22} - b_2a_{12}a_{33} + b_3a_{12}a_{23}$, itd.

Prowadzi to w przypadku ogólnym do definicji *wyznacznika* macierzy kwadratowej $a : I_n^2 \to R$;

$$\det a = \begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & & \ldots \\ a_{n1} & \ldots & a_{nn} \end{vmatrix} = \sum_{\alpha \in S_n} \operatorname{sgn} \alpha \cdot a_{1\alpha_1} \ldots a_{n\alpha_n},$$

gdzie $S_n = \operatorname{Perm} I_n$, i dla permutacji $\alpha \in S_n$, jej *znak* $\operatorname{sgn}\alpha = (-1)^{\operatorname{inv}\alpha}$, $\operatorname{inv}\alpha =$ liczba inwersji w $\alpha := \operatorname{card}\{(i,j) \in I_n^2 \mid i<j,\ \alpha_i > \alpha_j\} = \prod\limits_{1\leqslant i<j\leqslant n} \frac{\alpha_j-\alpha_i}{j-i}$.

Z powyższego wzoru natychmiast wynika, że dla $\alpha, \beta \in S_n : \operatorname{sgn}(\beta\circ\alpha) = \operatorname{sgn}\beta \cdot \operatorname{sgn}\alpha$, a więc $\operatorname{sgn}\alpha^{-1} = \operatorname{sgn}\alpha$ ($\operatorname{sgn} : S_n \longrightarrow (\{-1,1\},\ \cdot\ )$ – homomorfizm grup).

Dla dowolnej macierzy $a : I_m \times I_n \to R$ określamy *macierz transponowaną* $a^T : I_n \times I_m \to R$; $a^T_{ji} = a_{ij}$.
W przypadku macierzy kwadratowej ($m = n$): $\det a^T = \det a$ $\langle \det a^T = \sum\limits_{\alpha\in S_n} \operatorname{sgn}\alpha \cdot a_{\alpha_1 1}\dots a_{\alpha_n n} = \sum\limits_{\alpha\in S_n} \operatorname{sgn}\alpha^{-1}\cdot a_{1\alpha_1^{-1}}\dots a_{n\alpha_n^{-1}} = \sum\limits_{\beta\in S_n} \operatorname{sgn}\beta\cdot a_{1\beta_1}\dots a_{n\beta_n} = \det a\rangle$.

Bezpośrednio z definicji wynika liniowość wyznacznika ze względu na każdy wiersz (*wieloliniowość*), a więc także ze względu na każdą kolumnę.

Poniższe *twierdzenie Laplace'a* mówi *o rozwinięciu* wyznacznika względem wiersza lub kolumny.
Minorem dowolnej macierzy nazywamy macierz kwadratową lub jej wyznacznik – zależnie od kontekstu – otrzymaną z danej macierzy przez opuszczenie pewnej liczby wierszy i kolumn. W szczególności dla macierzy kwadratowej $a : I_n^2 \to R$ i wskaźników $i, j \in I_n$ oznaczamy przez M_{ij} minor otrzymany z danej macierzy po opuszczeniu i-tego wiersza i j-tej kolumny; wówczas

$$\det a = \sum_{j=1}^{n} a_{ij}(-1)^{i+j}M_{ij} = \sum_{i=1}^{n} a_{ij}(-1)^{i+j}M_{ij}.$$

$\langle$Wykorzystując wieloliniowość wyznacznika wystarczy dla dowodu na przykład pierwszej równości wykazać, że jeżeli i-ty wiersz danej macierzy ma postać $a_{i\cdot} = (0,\dots,0,1,0,\dots,0)$ – z jedynką na j-tym miejscu, to $\det a = (-1)^{i+j}M_{ij}$.

Istotnie $\det a = \sum\limits_{\alpha\in S_n'} \operatorname{sgn}\alpha\cdot a_{1\alpha_1}\dots a_{i-1\,\alpha_{i-1}}a_{i+1\,\alpha_{i+1}}\dots a_{n\alpha_n}$, gdzie $S_n' = \{\alpha \in S_n \mid \alpha_i = j\}$. Permutacji $\alpha \in S_n'$ odpowiada jednoznacznie bijekcja

$$\alpha' = \{1 \mapsto \alpha_1, \dots, i-1 \mapsto \alpha_{i-1}, i+1 \mapsto \alpha_{i+1}, \dots, n \mapsto \alpha_n\} : I_n \setminus \{i\} \lhook\joinrel\twoheadrightarrow I_n \setminus \{j\},$$

tej zaś odpowiada kanonicznie permutacja $\beta \in S_{n-1}$, i – jak łatwo przeliczyć – $\operatorname{inv}\alpha \equiv \operatorname{inv}\beta + i + j \pmod 2$, a więc $\operatorname{sgn}\alpha = (-1)^{i+j}\operatorname{sgn}\beta\rangle$.

Z twierdzenia Laplace'a otrzymujemy dalsze własności wyznaczników:

– Przestawienie w wyznaczniku dwóch wierszy (lub kolumn) zmienia jego znak na przeciwny $\langle$Indukcja$\rangle$.
– Wyznacznik o dwóch wierszach (kolumnach) identycznych jest zerowy.
– Wyznacznik nie zmieni wartości, gdy do elementów jednego wiersza (kolumny) dodamy odpowiednie elementy innego wiersza (kolumny) pomnożone przez skalar z R.

9.1.25. Rząd macierzy. Lemat o minorze bazowym. Niech $a : I_m \times I_n \to R$, gdzie $m, n \in \mathbb{N}^*$ zaś R jest ciałem. *Rzędem* macierzy a, $\operatorname{rk} a$ nazywamy najwyższy stopień niezerowego minora tej macierzy – każdy taki minor nazywamy *bazowym*.

Lemat o minorze bazowym: Wiersze (kolumny) macierzy $a : I_m \times I_n \to R$ wchodzące w minor bazowy stanowią bazę przestrzeni wektorowej rozpiętej na wszystkich wierszach (kolumnach) danej macierzy.

⟨ 1° Liniowa niezależność wierszy wchodzących w minor bazowy wynika z jego niezerowania się.
2° Dla udowodnienia generowania wystarczy wykazać, że każdy wiersz macierzy a jest kombinacją liniową wierszy wchodzących w dany minor bazowy. Dla uproszczenia notacji przyjmijmy, że minor bazowy jest stopnia $r < m$ i leży w lewym górnym rogu naszej macierzy. Wówczas np. m-ty wiersz jest kombinacją liniową wierszy wchodzących w minor bazowy, gdyż dla $j \in I_n$ minor stopnia $r+1$ otrzymany przez dopisanie do minora bazowego wiersza $(a_{m1}, \dots, a_{mr}, a_{mj})$ i kolumny $(a_{1j}, \dots, a_{rj}, a_{mj})$ jest zerowy, a więc, rozwijając go według ostatniej kolumny, otrzymujemy: $0 = \sum_{i=1}^{r} \alpha_{ij} a_{ij} + \beta a_{mj}$, gdzie współczynniki α_{ij} nie zależą od j, zaś $\beta = \det(a|I_r^2) \neq 0$, czyli $a_{mj} = \sum_{i=1}^{r} (-\alpha_{ij}\beta^{-1}) a_{ij}$⟩.

9.1.26. Rozwiązywanie układów równań liniowych. Natychmiastowym wnioskiem z lematu o minorze bazowym jest poniższe *twierdzenie Kroneckera–Capellego*:

Jeżeli $m, n \in \mathbb{N}^*$, R jest ciałem, $a : I_m \times I_n \to R$, $b : I_m \to R$, to układ $(*)$ z 9.1.24 ma rozwiązanie wtt, gdy rząd macierzy a (tzw. *macierzy współczynników*) jest równy rzędowi macierzy otrzymanej z macierzy a przez dopisanie kolumny $(b_1, \dots, b_m)$ wyrazów wolnych (tzw. *macierzy uzupełnionej*).

⟨ ⇐) Jeżeli warunek równości rzędów jest spełniony, to minor bazowy macierzy współczynników jest jednocześnie minorem bazowym macierzy uzupełnionej, i z lematu w wersji dla kolumn wynika istnienie rozwiązania układu $(*)$
⇒) HP: Układ $(*)$ ma rozwiązanie i $r = \operatorname{rk} a < \operatorname{rk} a'$, gdzie a' jest macierzą uzupełnioną. Kolumna wyrazów wolnych jest kombinacją liniową kolumn macierzy a. Ustalmy minor bazowy macierzy uzupełnionej, niech np. będzie on usytuowany w prawym górnym rogu macierzy a'. Jeden z jego minorów stopnia r będzie minorem bazowym macierzy a – ustalmy ów minor. ⟨Wniosek z twierdzenia Laplace'a o rozwinięciu wyznacznika⟩. Z lematu o minorze bazowym wynika, że każda z $n - r$ początkowych kolumn macierzy a jest kombinacją liniową ustalonego minora bazowego, a więc kolumna wyrazów wolnych też jest kombinacją liniową tych r kolumn, co pociąga zerowanie się naszego minora bazowego macierzy uzupełnionej ↯⟩.

W przypadku, gdy $m = n$ i $\det a \neq 0$ układ równań $(*)$ z 9.1.24 nazywany *cramerowskim*; jeżeli taki układ ma rozwiązanie $(x_1, \dots, x_n) \in R^n$, również w przypadku, gdy R jest pierścieniem ($R \in \mathrm{Rinc}_1$), to spełnia ono poniższe *wzory Cramera*:

$$(**) \qquad x_i \cdot \det a = \det a^{(i)}, \quad i = 1, \dots, n,$$

gdzie $a^{(i)}$ jest macierzą otrzymaną z macierzy a przez zastąpienie i-tej kolumny kolumną wyrazów wolnych. ⟨Na przykład dla $i = 1$ równość $(**)$ otrzymamy mnożąc stronami równości $(*)$ z 9.1.24. odpowiednio przez $(-1)^{j+i}M_{j1}$, $j=1,\dots,n$, i dodając je stronami$\rangle$.

Jeżeli R jest ciałem i układ jest cramerowski, to posiada on dokładnie jedno rozwiązanie spełniające $(**)$. $\langle$Warunek równości rzędów z twierdzenia Kroneckera–Capellego jest spełniony$\rangle$.

Tak więc chcąc rozwiązać układ $(*)$ z 9.1.24 należy:

1° Sprawdzić warunek równości rzędów.

2° W przypadku pozytywnym ustalić minor bazowy macierzy współczynników i opuścić równania nie wchodzące w ten minor.

3° Niewiadome ze współczynnikami niewchodzącymi w minor z 2° przenieść na prawą stronę, traktując je jako parametry, i rozwiązać otrzymany układ cramerowski.

9.1.27. Wymiar przestrzeni wektorowej. Niech R będzie ciałem. Mówimy, że przestrzeń wektorowa X nad R jest *skończenie wymiarowa*, jeżeli ma bazę skończoną; jeżeli tak jest, to wszystkie inne bazy tej przestrzeni są skończone, a przy tym równoliczne, co wynika niemal natychmiast z lematu o minorze bazowym – ich wspólną moc nazywamy *wymiarem* przestrzeni X i oznaczamy $\dim X$ (por. zadanie 33).

Można udowodnić więcej:

Jeżeli $n,m\in\mathbb{N}$, $e:I_n\to X$ jest układem liniowo niezależnym i $v:I_m\to X$ układem generującym przestrzeń wektorową X, to $n\leqslant m$.

$\langle$HP: $m<n$, a więc $n\geqslant m+1$.
Wówczas dla $i\in I_{m+1}$, $e_i=\sum\limits_{j=1}^{m}a_{ij}v_j$ dla pewnych $a_{ij}\in R$.

Mamy więc macierz $a:I_{m+1}\times I_m\to R$, i oczywiście $\operatorname{rk}a\leqslant m$. Z lematu o minorze bazowym wynika, że wiersze macierzy a są liniowo zależne. Istnieje więc niezerowy układ skalarów $\alpha_1,\dots,\alpha_{m+1}\in R$ taki, że $\sum\limits_{i=1}^{m+1}\alpha_i a_{i\cdot}=0$, gdzie $a_{i\cdot}=(a_{i1},\dots,a_{im})\in R^m$ jest i-tym wierszem macierzy a, czyli

$$\forall\, j\in I_m:\sum_{i=1}^{m+1}\alpha_i a_{ij}=0,$$

skąd natychmiast wynika, że $\sum\limits_{i=1}^{m+1}\alpha_i e_i=\sum\limits_{j=1}^{m}v_j\big(\sum\limits_{i=1}^{m+1}\alpha_i a_{ij}\big)=0$, a więc liniowa zależność wektorów $e_1,\dots,e_{m+1}$ $\lightning\rangle$.

9.1.28. Liczby zespolone. *Jednostka urojona* i taka, że $i^2=-1$, oraz liczby zespolone $a+bi$, $a,b\in\mathbb{R}$ pojawiły się w szesnastowiecznej Italii (Cardano, Tartaglia) przy badaniu równania trzeciego stopnia:

(*) $$ax^3+bx^2+cx+d=0,\quad \text{gdzie } a,b,c,d\in\mathbb{R} \text{ i } a\neq 0.$$

Dzieląc obustronnie $(*)$ przez *współczynnik kierunkowy* a oraz stosując podstawienie $x=y+\alpha$ z odpowiednio dobranym α uzyskujemy równanie typu:

(**) $$x^3+px+q=0,\quad \text{gdzie } p,q\in\mathbb{R},$$

przy czym można założyć, że $p \neq 0 \neq q$.

Teraz kluczowe jest podstawienie $x = y + \frac{\beta}{y}$, które, jak łatwo sprawdzić, dla $\beta = -\frac{p}{3}$ daje równanie

$$y^3 + \frac{\beta^3}{y^3} + q = 0,$$

to zaś z kolei po przemnożeniu przez $z = y^3$ daje równanie drugiego stopnia: (równanie kwadratowe):

$$z^2 + qz + \beta^3 = 0.$$

Jeżeli wyróżnik tego ostatniego równania $\Delta = q^2 - 4\beta^3 = 4\left[(\frac{p}{3})^3 + (\frac{q}{2})^2\right]$ jest nieujemny, to potrafimy je, a więc i wyjściowe równanie $(*)$, rozwiązać w ciele $\mathbb{R}$ liczb rzeczywistych.

Jednak dla $\Delta < 0$ bez wprowadzenia liczb zespolonych (a później funkcji trygonometrycznych i cyklometrycznych) jesteśmy zablokowani, pomimo że równanie $(*)$ ma zawsze rozwiązanie w $\mathbb{R}$.

Ściśle definiujemy *liczby zespolone* jako punkty grupy addytywnej $\mathbb{R}^2$ (dodawanie po współrzędnych $(a,b)+(c,d) = (a+c, b+d)$) z mnożeniem uzyskanym z formalnego rachunku

$$(a + bi)(c + di) = ac - bd + (ad + bc)i, \quad (i^2 = -1),$$

czyli $(a,b)\cdot(c,d) = (ac-bd, ad+bc)$. Otrzymujemy w ten sposób ciało $\mathbb{C} = (\mathbb{R}^2, +, \cdot)$, które po identyfikacji przez *injekcję kanoniczną*

$$\{x \mapsto (x, 0) \mid x \in \mathbb{R}\} : R \hookrightarrow \mathbb{C}$$

jest rozszerzeniem ciała $\mathbb{R}$, $1_{\mathbb{C}} = (1,0) = 1$. Oznaczając $i := (0,1)$ otrzymamy $i^2 = -1$ oraz $(a,b) = a + bi$, przy czym oznaczając dla $z = a + bi$ $\bar{z} = a - bi$ (*liczba sprzężona*) będziemy mieli: $z\bar{z} = a^2 + b^2 = |z|^2$, a więc $z \neq 0 \Rightarrow z^{-1} = \frac{\bar{z}}{|z|^2}$. $\langle$Przeliczenie$\rangle$. Łatwo sprawdzić, że dla $z, w \in \mathbb{C}$ $\overline{zw} = \bar{z} \cdot \bar{w}$, a więc $|zw| = |z| \cdot |w|$.

Pełniejszy wgląd w strukturę ciała $\mathbb{C}$ daje wprowadzenie wspomnianych już funkcji trygonometrycznych (zadanie 35). Podstawowa jego własność to tzw. *algebraiczna domkniętość*: Każdy wielomian stopnia $n \geqslant 1$ o współczynnikach z $\mathbb{C}$ ma w $\mathbb{C}$ miejsce zerowe (pierwiastek).

9.1.29. Przestrzenie afiniczne. Przy ustalonym ciele K *przestrzeń afiniczna nad* K jest to obiekt postaci $X = (E, V)$, gdzie $V : E \to \{Y \in \mathrm{Vect}_K \mid \underline{Y} = E\}$, przy czym dla $a, b \in E$:

1°) $0_a = a$

2°) $\tau_{a,b} := \{x \mapsto x \underset{a}{+} b \mid x \in E\} : V_a \xrightarrow[\mathrm{Vect}_K]{\sim} V_b$,

gdzie 0_a jest wektorem zerowym, zaś $\underset{a}{+} : E^2 \to E$ dodawaniem wektorów w przestrzeni wektorowej V_a, oznaczanej też X_a; $\tau_{a,b}$ to *translacja* w tej przestrzeni o wektor b.

Przestrzeń afiniczna jest więc jakby przestrzenią wektorową, w której zapomniano o położeniu punktu zerowego.

Kategorię Af_K przestrzeni afinicznych nad K określamy przyjmując dla dwu przestrzeni afinicznych X, Y jako morfizmy odwzorowania $f : X \to Y$ takie, że $\forall\, a \in X\ [f : X_a \xrightarrow[\mathrm{Vect}_K]{} Y_{f(a)}]$; mówimy, że są to *odwzorowania afiniczne* z X do Y.

Przestrzeń wektorową $X \in \mathrm{Vect}_K$ można w naturalny sposób uważać za przestrzeń afiniczną i mówić o pojęciach afinicznych w x, na przykład w $\mathbb{R}^2$, $\mathbb{R}^3$, itp.

Dokładniej mówiąc mamy naturalny funktor zwyczajny $F : \mathrm{Vect}_K \xrightarrow{\cdot} \mathrm{Af}_K$, który przestrzeni wektorowej $X = (E, +, \cdot)$ przyporządkowuje przestrzeń afiniczną $F(X) = (E, V)$ taką, że

$$\forall\, a \in X : \tau_a = \{x \mapsto x + a \mid x \in E\} : X \xrightarrow[\mathrm{Vect}_K]{\sim} V_a.$$

Fakt ten, jak również poniższe własności przestrzeni afinicznych, łatwo sprawdzić bezpośrednim rachunkiem (zadanie 36):

(i) Jeżeli w przestrzeni afinicznej X ustalimy punkt p (np. $p = 0$ w przypadku przestrzeni wektorowej), to dla $a, x, y \in X$, $\alpha \in K$; notując $x+y = x \underset{p}{+} y$ i $\alpha x = \alpha \underset{p}{\cdot} x$, będziemy mieli:

$$x \underset{a}{+} y = x + y - a, \qquad \alpha \underset{a}{\cdot} x = \alpha x + (1-\alpha)a.$$

(ii) Dla przestrzeni $X \in \mathrm{Af}_K$ oznaczmy $T(X) = \{\tau_{a,b} \mid a, b \in X\}$ = ogół translacji przestrzeni X. Przy ustalonym $p \in X$ many bijekcję $\{x \mapsto \tau_{p,x} \mid x \in X\} : X \hookrightarrow\!\!\!\!\rightarrow T(X)$, która przenosi strukturę przestrzeni wektorowej z X_p na $T(X)$. Łatwo sprawdzić, że otrzymana w ten sposób przestrzeń wektorowa nie zależy od wyboru punktu p, przy czym

$$\forall\, a, b, c, d \in X,\ \alpha \in X : \tau_{a,b} + \tau_{c,d} = \tau_{a,b} \circ \tau_{c,d},$$
$$\tau_{a,b} = \tau_{c,d} \iff a + d = b + c,\ \ \alpha\, \tau_{a,b} = \tau_{a, a+\alpha(b-a)},$$

gdzie znak $+$ oznacza $\underset{p}{+}$ dla pewnego ustalonego $p \in X$.

(iii) Jeżeli $X \in \mathrm{Vect}$ i $\varnothing \neq U \subset X$, to

$$U \underset{\mathrm{Af}}{\subset} X \iff \exists\, V \underset{\mathrm{Vect}}{\subset} X,\ a \in X : U = V + a \quad (= \{v + a \mid v \in V\}),$$

przy czym podprzestrzeń wektorowa V jest wyznaczona jednoznacznie – nazywamy ją *kierunkiem* podprzestrzeni afinicznej U.

9.1.30. Kwaterniony. Odkryte w 1843 r. przez Williama Hamiltona *kwaterniony* można określić na podobieństwo liczb zespolonych jako wyrażenia postaci $z + wj$, gdzie $z, w \in \mathbb{C}$, zaś j jest nową „jednostką urojoną”, $j^2 = -1$. Dodawanie określamy w sposób naturalny, $z+wj+u+vj = z+u+(w+v)j$. Natomiast przy określeniu mnożenia rezygnujemy z przemienności, kładąc $jw = \bar{w}j$, gdzie dla $w = c + di \in \mathbb{C}$ $\bar{w} = c - di \in \mathbb{C}$ jest liczbą zespoloną sprzężoną z w. Zachowana zostaje wówczas, jak łatwo sprawdzić, łączność mnożenia oraz obustronna rozdzielność mnożenia względem dodawania.

Tak więc dla $z, w, u, v \in \mathbb{C}$:

$$(z + wj)(u + vj) = zu - w\bar{v} + (zv + w\bar{u})j,$$

lub bardziej formalnie:

$$(z, w) \cdot (u, v) := (zu - w\bar{v}, zv + w\bar{u}).$$

Dla kwaternionu $q = z + wj$ określamy *kwaternion sprzężony* $\bar{q} := \bar{z} - wj$ i wówczas, jeżeli jeszcze $r = u + vj \in \mathbb{K}$, to $\overline{q+r} = \bar{q} + \bar{r}$, $\overline{qr} = \bar{r}\bar{q}$, $\bar{\bar{q}} = q$, $q\bar{q} = \bar{q}q = |q|^2$, gdzie $|q| = \sqrt{|z|^2 + |w|^2}$.

Łatwo sprawdzić, że otrzymana struktura $(\mathbb{K}, +, \cdot\,)$ jest pierścieniem z dzieleniem; jeżeli $q \in \mathbb{K}^* = \mathbb{K} \setminus \{0\}$, to $q^{-1} = \frac{\bar{q}}{|q|^2}$.

Pierścień kwaternionów przy naturalnym zanurzeniu (identyfikacja) $\{z \mapsto (z, 0) \mid \ldots\} : \mathbb{C} \hookrightarrow \mathbb{K}$ jest rozszerzeniem ciała $\mathbb{C}$, przy czym dla $j = (0, 1) \in \mathbb{C}^2$, $j^2 = -1$, i dla $z, w \in \mathbb{C} : jw = \bar{w}j$, $(z, w) = z + wj$.

Oznaczmy $k := ij$. Wówczas $k^2 = ijij = -i^2j^2 = -1$ oraz dla $a, b, c, d \in \mathbb{R}$, $z = a+bi$, $w = c+di : q = z+wj = a+bi+cj+dk$. Jeżeli jeszcze $q' = x+yi+zj+tk$, gdzie $x, y, z, t \in \mathbb{R}$, to $qq' = ax-by-cz-dt+(ay+bx+ct-dz)i+(az-bt+cx+dy)j+(at+bz-cy-dx)k$. Wstawiając ten wynik do równości $|qq'|^2 = |q|^2|q'|^2$ otrzymamy formułę czterokwadratową Eulera prawdziwą w każdym pierścieniu przemiennym.

Kwaterniony mają ważne zastosowanie w geometrii przestrzeni R^3 (zadanie 38^*).

9.1.31. Przestrzenie filtrowe. Ogólne pojęcie granicy. Obiekty kategorii Fltr *przestrzeni filtrowych* (rozdział 8, zadanie 16) są postaci $(X, \mathcal{F})$, gdzie $\mathcal{F}$ jest *filtrem* na zbiorze X, tzn. $\mathcal{F} \subset \mathcal{P}X$, $X \in \mathcal{F}$

$$\text{i} \qquad \forall\, A, B \subset X : (A, B \in \mathcal{F} \;\Rightarrow\; A \cap B \in \mathcal{F}) \;\;\wedge\;\; (\mathcal{F} \ni A \subset B \;\Rightarrow\; B \in \mathcal{F}).$$

Dla dwu przestrzeni filtrowych $(X, \mathcal{F})$ i $(Y, \mathcal{G})$ morfizmami pierwszej w drugą są *odwzorowania ciągłe*, to jest odwzorowania $f : X \to Y$ spełniające warunek $\forall\, B \in \mathcal{G} : f^{-1}(B) \in \mathcal{F}$, lub równoważnie: $\forall\, B \in \mathcal{G}\; \exists\, A \in \mathcal{F} : f(A) \subset B$; w tej sytuacji mówimy też, że funkcja f zmierza (jest zbieżna) do granicy $\mathcal{G}$, gdy jej argument zmierza do $\mathcal{F}$, co notujemy: $\underset{x \to \mathcal{F}}{f(x)} \longrightarrow \mathcal{G}$.

Ogół filtrów na zbiorze X oznaczamy $\mathrm{Fil}(X)$. Injekcję $\iota : \mathcal{P}X \hookrightarrow \mathrm{Fil}(X)$, $\iota(A) = \{B \mid A \subset B \subset X\}$ nazywamy *kanoniczną*; filtry postaci $\iota(A)$, gdzie $A \subset X$, nazywamy *głównymi*. Pozostałe filtry to filtry *niegłówne* – można je traktować jako własności „nieostre” elementów zbioru X. Natychmiast widać, że na zbiorze skończonym X każdy filtr $\mathcal{F}$ jest główny; $\mathcal{F} = \iota(\bigcap \mathcal{F})$.

W zbiorze $\mathrm{Fil}(X)$ wszystkich filtrów na zbiorze X wyróżniamy *filtry właściwe*:

$$\mathrm{Fil}^*(X) = \{\mathcal{F} \in \mathrm{Fil}(X) \mid \varnothing \notin \mathcal{F}\} = \mathrm{Fil}(X) \setminus \{\mathcal{P}X\};$$

jedynym filtrem *niewłaściwym* na X jest więc filtr główny $\iota(\varnothing) = \mathcal{P}X$.

Jeżeli dane są zbiory X, Y, funkcja $f : X \to Y$ i filtr $\mathcal{G}$ na zbiorze Y, to oczywiście

$$\underset{x \to \mathcal{P}X}{f(x)} \longrightarrow \mathcal{G}.$$

W związku z tym w dalszym ciągu, mówiąc o granicach, będziemy zakładali (często milcząco), że odpowiednie filtry są właściwe. Każdy filtr niegłówny jest właściwy.

Ważnymi przykładami filtrów niegłównych (por. zadanie 39) są:

1) *Filtr Frécheta* na zbiorze nieskończonym X:
$\{A \subset X \mid X \setminus A \in \mathrm{Fin}\}$, czyli filtr dopełnień zbiorów skończonych w X (dla $X = \mathbb{N}$ jest to nieostra własność „bycia dużą liczbą naturalną”).

2) Filtr *otoczeń* punktu $a \in \mathbb{R}$:

$$\varPhi_a = \{U \subset \mathbb{R} \mid \exists\, r > 0 : (a - r; a + r) \subset U\}$$

(własność „bycia blisko” punktu a), oraz

$$\varPhi_a^* = \{U \setminus \{a\} \mid U \in \varPhi_a\} \text{ – filtr } \textit{sąsiedztw} \text{ punktu } a.$$

Analogicznie dla $a \in \mathbb{C}$ mamy:

$$\varPhi_a = \{U \subset \mathbb{C} \mid \exists\, r > 0\, \forall\, z \in \mathbb{C}\ (|z - a| < r \ \Rightarrow\ z \in U)\},$$
$$\varPhi_a^* = \{U \setminus \{a\} \mid U \in \varPhi_a\}$$

3)

$$\varPhi_{\pm\infty} = \{U \subset \mathbb{R} \mid \exists\, a, b \in \mathbb{R} : (-\infty, a) \cup (b, \infty) \subset U\}$$

– filtr sąsiedztw nieskończoności w $\mathbb{R}$,

$$\varPhi_\infty = \varPhi_{+\infty} = \{U \subset \mathbb{R} \mid \exists\, a \in \mathbb{R} : (a, \infty) \subset U\}$$

– filtr sąsiedztw plus nieskończoności w $\mathbb{R}$,
i analogicznie $\varPhi_{-\infty}$.

Dla funkcji liczbowej $f : X \to \mathbb{R}$ (i analogicznie $f : X \to \mathbb{C}$), punktu $a \in \mathbb{R}$ i filtru $\mathcal{F}$ na X piszemy $\underset{x \to \mathcal{F}}{f(x)} \longrightarrow a$, gdy $\underset{x \to \mathcal{F}}{f(x)} \longrightarrow \varPhi_a$; jeśli tak jest, to mówimy, że $f(x)$ *zmierza do punktu* a, gdy $x \to \mathcal{F}$; tak więc

$$\underset{x \to \mathcal{F}}{f(x)} \longrightarrow a \iff \forall\, \varepsilon > 0\, \exists\, A \in \mathcal{F}\, \forall\, x \in A : |f(x) - a| < \varepsilon.$$

Analogiczny sens mają zapisy: $\underset{x \to \mathcal{F}}{f(x)} \longrightarrow \infty$, $\underset{x \to \mathcal{F}}{f(x)} \longrightarrow -\infty$, itp.

9.1.32. Granica ciągu. Jeżeli $\mathcal{G}$ jest filtrem na zbiorze Y i $x : \mathbb{N} \to Y$, to zapis $\underset{n \to \infty}{x(n)} \longrightarrow \mathcal{G}$ oznaczać będzie, że $\underset{n \to \mathcal{F}}{x(n)} \longrightarrow \mathcal{G}$, gdzie $\mathcal{F}$ jest filtrem Frécheta na $\mathbb{N}$; natychmiast widać, że

$$\underset{n \to \infty}{x(n)} \longrightarrow \mathcal{G} \iff \forall\, G \in \mathcal{G}\, \exists\, k \in \mathbb{N}\, \forall\, n \in \mathbb{N}\ (n \geqslant k \ \Rightarrow\ x_n \in G).$$

W szczególności dla $a \in \mathbb{R}$ notujemy $\underset{n \to \infty}{x_n} \longrightarrow a$, gdy $\underset{n \to \infty}{x_n} \longrightarrow \varPhi_a$, i analogicznie dla $a = \infty$ lub $a = -\infty$; tak więc dla a skończonego:

$$\underset{n \to \infty}{x(n)} \longrightarrow a \iff \forall\, \varepsilon > 0\, \exists\, k \in \mathbb{N}\, \forall\, n \in \mathbb{N}\ (n \geqslant k \ \Rightarrow\ |x_n - a| < \varepsilon).$$

9.1.33. Generowanie filtrów. Bazy filtrowe. Dla zbioru X i rodziny $\mathcal{A} \subset \mathcal{P}X$ oznaczmy $\langle \mathcal{A} \rangle := \bigcap\{\mathcal{F} \in \mathrm{Fil}(X) \mid \mathcal{A} \subset \mathcal{F}\}$ = najmniejszy filtr na X zawierający $\mathcal{A}$; mówimy że jest to *filtr generowany* przez $\mathcal{A}$; łatwo widać, że

$$\langle \mathcal{A} \rangle = \{X\} \cup \{B \subset X \mid \exists\, n \in \mathbb{N}^*, A : I_n \to \mathcal{A} \quad (\bigcap_{i=1}^{n} A_i \subset B)\}.$$

Łatwo też widać, że filtr $\langle \mathcal{A} \rangle$ jest właściwy wtt, gdy $X \neq \varnothing \ \wedge\ \forall\, n \in \mathbb{N}^*, A : I_n \to \mathcal{A}\ \big(\bigcap_{i=1}^{n} A_i \neq \varnothing\big)$; rodzinę $\mathcal{A}$ podzbiorów zbioru X spełniającą powyższy warunek nazywamy *scentrowaną*.

Bazą filtru $\mathcal{F}$ na zbiorze X nazywamy podzbiór $\mathcal{B} \subset \mathcal{F}$ taki, że $\forall\, A \in \mathcal{F}\ \exists\, B \in \mathcal{B} : B \subset A$; wówczas $\mathcal{F} = \langle \mathcal{B} \rangle = \{A \subset X \mid \exists\, B \in \mathcal{B} : B \subset A\}$.

Rodzinę $\mathcal{B} \subset \mathcal{P}X$ nazywamy *bazą filtrową* na X, gdy jest bazą jakiegoś filtru właściwego na X; jest tak wtt, gdy

$$\mathcal{B} \neq \varnothing \quad\wedge\quad \varnothing \notin \mathcal{B} \quad\wedge\quad \forall\, A, B \in \mathcal{B}\ \exists\, C \in \mathcal{B} : C \subset A \cap B.$$

Jeżeli $\mathcal{A}$ i $\mathcal{B}$ są bazami filtrów właściwych $\mathcal{F}$ i $\mathcal{G}$ odpowiednio na zbiorach X i Y oraz $f : X \to Y$, to $\underset{x \to \mathcal{F}}{f(x)} \longrightarrow \mathcal{G} \iff \forall\, B \in \mathcal{B}\ \exists\, A \in \mathcal{A} : f(A) \subset B$.

Dwie bazy filtrowe $\mathcal{A}$ i $\mathcal{B}$ na zbiorze X nazywany *równoważnymi*, gdy generują ten sam filtr na X, jest tak wtt, gdy

$$(\forall\, A \in \mathcal{A}\ \exists\, B \in \mathcal{B} : B \subset A) \quad\wedge\quad (\forall\, B \in \mathcal{B}\ \exists\, A \in \mathcal{A} : A \subset B).$$

Tak na przykład:

1) Bazą filtrów Frécheta na $\mathbb{N}$ jest rodzina $\{\mathbb{N}_k \mid k \in \mathbb{N}\}$, gdzie dla $k \in \mathbb{N} : \mathbb{N}_k = \{n \in \mathbb{N} \mid n \geqslant k\}$.

2) Bazą filtru $\varPhi_a$ otoczeń punktu $a \in \mathbb{R}$ jest rodzina przedziałów $\{(a - \frac{1}{n}, a + \frac{1}{n}) \mid n \in \mathbb{N}^*\}$.

3) Bazą filtru $\varPhi_\infty$ sąsiedztw nieskończoności w $\mathbb{R}$ jest rodzina $\{(n, \infty) \mid n \in \mathbb{N}\}$, i podobnie dla filtrów $\varPhi_{-\infty}$, $\varPhi_{\pm\infty}$.

9.1.34. Filtry typu przeliczalnego. Warunek Heinego. Mówimy, że filtr właściwy $\mathcal{F}$ na zbiorze X jest *typu przeliczalnego*, jeżeli ma bazę przeliczalną $\mathcal{B}$; $\operatorname{card} \mathcal{B} = \aleph_0$; istnieje wówczas ciąg $B : \mathbb{N} \to \mathcal{F}$ taki, że rodzina $\{B_n \mid n \in \mathbb{N}\}$ jest bazą filtru $\mathcal{F}$ oraz $\forall\, n \in \mathbb{N} : B_{n+1} \subset B_n \quad \langle \exists \rangle\ A : \mathbb{N} \hookrightarrow\!\!\!\!\rightarrow \mathcal{B}$; dla $n \in \mathbb{N}$ bierzemy $B_n = A_0 \cap \ldots \cap A_n \rangle$. Ciąg taki będziemy nazywać *bazą monotoniczną* filtru.
Wszystkie filtry z poprzedniego ustępu są tego rodzaju.

Natychmiast widać, że $\forall\, X,\ Y,\ \mathcal{F} \in \operatorname{Fil}^*(X),\ \mathcal{G} \in \operatorname{Fil}^*(Y),\ f : X \to Y$

$$\Big[\underset{x \to \mathcal{F}}{f(x)} \longrightarrow \mathcal{G} \ \Rightarrow\ \forall\, u : \mathbb{N} \to X\ \big(\underset{n \to \infty}{u_n} \longrightarrow \mathcal{F} \ \Rightarrow\ \underset{n \to \infty}{f(u_n)} \longrightarrow \mathcal{G}\big)\Big].$$

Warunek konieczny zbieżności, stanowiący następnik powyższej implikacji, zwany *warunkiem Heinego*, jest również warunkiem wystarczającym w przypadku, gdy filtr $\mathcal{F}$ jest typu przeliczalnego (zadanie 45).

9.1.35. Przestrzenie topologiczne. Obiekty kategorii zwyczajnej Top *przestrzeni topologicznych* są postaci $(X, \varPhi)$, gdzie $\varPhi : X \to \operatorname{Fil}(X)$, przy czym

$$\forall\, a \in X,\ U \in \varPhi_a\ [a \in U \quad\wedge\quad \exists\, V \in \varPhi_a\ \forall\, b \in V : U \in \varPhi_b].$$

W powyższej sytuacji mówimy, że $\varPhi_a$ jest *filtrem otoczeń* punktu a w przestrzeni X; oczywiście $\varPhi_a \in \operatorname{Fil}^*(X)$.

Dla dwu przestrzeni topologicznych $(X, \varPhi)$, $(Y, \varPsi)$ i punktu $a \in X$ mówimy, że odwzorowanie $f : X \to Y$ jest *ciągłe w punkcie* a, gdy f jest odwzorowaniem ciągłym przestrzeni filtrowej $(X, \varPhi_a)$ w przestrzeń filtrową $(Y, \varPsi_{f(a)})$, tzn.

$$\forall\, V \in \varPsi_{f(a)}\ \exists\, U \in \varPhi_a : f(U) \subset V.$$

Morfizmami w kategorii Top są odwzorowania *ciągłe* w tym sensie, że są ciągłe w każdym punkcie $x \in X$.

Zbiory $\mathbb{R}$ i $\mathbb{C}$ mogą być w naturalny sposób traktowane jako przestrzenie topologiczne (por. 9.1.31.).

Dla przestrzeni topologicznej (X, Φ), punktu $a \in X$, zbioru T z filtrem $\mathcal{F}$ i funkcji $f : T \to X$ piszemy $\underset{t\to\mathcal{F}}{f(t)} \longrightarrow a$, gdy $\underset{t\to\mathcal{F}}{f(t)} \longrightarrow \Phi_a$, to jest, gdy $\forall U \in \Phi_a\ \exists A \in \mathcal{F} : f(A) \subset U$. Oznaczamy $\operatorname*{Lim}_{t\to\mathcal{F}} f(t) := \{a \in X \mid \underset{t\to\mathcal{F}}{f(t)} \longrightarrow \Phi_a\}$ – *granice* funkcji f według filtru $\mathcal{F}$.

Rozważamy też szerszy zbiór *punktów skupienia* f według filtru $\mathcal{F}$:

$$\operatorname*{Adh}_{t\to\mathcal{F}} f(t) = \{a \in X \mid \forall U \in \Phi_a,\ A \in \mathcal{F} : f(A) \cap U \neq \varnothing\} \supset \operatorname*{Lim}_{t\to\mathcal{F}} f(t).$$

W kategorii Top, podobnie jak w kategorii Fltr, każdy podzbiór $A \subset X$ ($\in$ Top) jest zgodny z X; dla $a \in A$ filtrem otoczeń punktu a w podprzestrzeni $X|A$ jest $\{U \cap A \mid U \in \Phi_a\}$.

Kategoria Top jest też z produktami zwyczajnymi. Dla rodziny $X : I \to$ Top przestrzeni topologicznych i punktu $a \in \prod_{i\in I} X_i$ filtr otoczeń:

$$\Phi_a = \Big\{ V \subset \prod X \mid \exists U : I \to \mathbb{V}\ \forall i \in I\ \big[U_i \in \Phi_i(a_i) \\ \wedge\ \ \{i \in I \mid U_i \neq X_i\} \in \mathrm{Fin}\ \ \wedge\ \prod_{i\in I} U_i \subset V\big] \Big\} \quad (\textit{produkt Tichonowa}),$$

gdzie dla $i \in I$, $\Phi_i(a_i)$ jest filtrem otoczeń a_i w X_i.

9.1.36. Przestrzenie Hausdorffa. Przestrzeń topologiczną (X, Φ) nazywamy *przestrzenią Hausdorffa* lub *przestrzenią rozdzielczą* albo też *przestrzenią typu* T_2 – ich podkategoria to Top(T_2) – gdy

$$\forall_{\substack{a,b,\in X\\ a\neq b}} \exists U \in \Phi_a, V \in \Phi_b : U \cap V = \varnothing.$$

Formułowane są też dwa słabsze warunki rozdzielczości:

(T_0) $\quad \forall_{\substack{a,b,\in X\\ a\neq b}} \big[(\exists U \in \Phi_a : b \notin U)\ \vee\ (\exists V \in \Phi_b : a \notin V)\big]$,

(T_1) $\quad \forall_{\substack{a,b,\in X\\ a\neq b}} \exists U \in \Phi_a : b \notin U$.

Jeżeli $X \in \mathrm{Top}(T_2)$, $a \in X$, $f : T \to X$, $\mathcal{F} \in \mathrm{Fil}^*(X)$ oraz $\underset{t\to\mathcal{F}}{f(t)} \longrightarrow a$, to punkt a jest wyznaczony jednoznacznie; notacja: $\lim_{t\to\mathcal{F}} f(t) = a$ $\quad\langle$HP: $\exists)_{\substack{b\in X\\ b\neq a}} : \underset{t\to\mathcal{F}}{f(t)} \longrightarrow b$. $\exists)\, U \in \Phi_a,\ V \in \Phi_b : U \cap V = \varnothing$. $\exists)\, A, B \in \mathcal{F} : f(A) \subset U,\ f(B) \subset V$. Wówczas $\varnothing = A \cap B \in \mathcal{F}$ ↯$\rangle$; tak więc $|\operatorname*{Lim}_{t\to\mathcal{F}} f(t)| \leqslant 1$, $\lim_{t\to\mathcal{F}} f(t) = \bigcap \operatorname*{Lim}_{t\to\mathcal{F}} f(t)$.

Własność jednoznaczności granicy w pełni charakteryzuje przestrzenie topologiczne rozdzielcze (zadanie 46).

Podstawowe własności granic funkcji liczbowych zostały zebrane w zadaniu 47.

Najważniejsze pojęcia topologiczne (domknięcie i wnętrze zbioru, zbiory domknięte, zbiory otwarte) i zależności między nimi zebrano w zadaniu 48.

9.1.37. Zwartość. Mówimy, że przestrzeń topologiczna X jest *zwarta* albo że jest *kompaktem*, gdy z każdego jej pokrycia zbiorami otwartymi można wyjąć pokrycie skończone; lub równoważnie każda rodzina scentrowana podzbiorów domkniętych ma niepuste przecięcie.
Symbolicznie, oznaczając przez τ ogół podzbiorów otwartych przestrzeni X:

$$X - \text{zwarta} \quad :\Longleftrightarrow \ \forall\, \mathcal{A} \subset \tau\ \big(X = \bigcup \mathcal{A} \ \Rightarrow\ \exists\, \mathcal{B} \subset \mathcal{A} : X = \bigcup \mathcal{B} \ \ \wedge\ \ \mathcal{B} \in \mathrm{Fin}\big).$$

Mówimy, że podzbiór $E \subset X$ jest *zwarty*, jeżeli jest przestrzenią zwartą w topologii indukowanej.
Podstawowym faktem jest zwartość przedziału domkniętego i ograniczonego $[a, b]$ w $\mathbb{R}$. $\langle$Dla $C := \{c \in [a, b] \mid [a, c]$ ma pokrycie skończone$\}$ mamy: $s = \sup C \in C$ i $s = b\rangle$.

Comp ($\underset{\circ}{\subset}$ Top) := kategoria przestrzeni topologicznych zwartych; $\mathrm{Comp}(T_2) := \mathrm{Comp} \cap \mathrm{Top}(T_2)$.

Można łatwo wykazać, że przestrzeń topologiczna jest zwarta wtt, gdy każda funkcja wchodząca do tej przestrzeni i określona na zbiorze z filtrem ma punkt skupienia, oraz wtt, gdy każda funkcja wchodząca do tej przestrzeni i określona na zbiorze z ultrafiltrem ma granicę (zadanie 50).

Wnioskiem z powyższej charakteryzacji jest podstawowe w topologii *twierdzenie Tichonowa* o zwartości iloczynu kartezjańskiego rodziny przestrzeni zwartych (zadanie 51).

Wprost z definicji wynika, że podzbiór domknięty przestrzeni zwartej jest zwarty. Natomiast podzbiór zwarty C przestrzeni topologicznej Hausdorffa X jest domknięty $\langle$HP: $\exists)\, x \in C^- \setminus C$. $\exists)\, U, V : C \to \tau =$ podzbiory otwarte w X $\ \forall\, y \in C : x \in U_y$, $y \in V_y$, $U_y \cap V_y = \varnothing$. $\exists)\, A \subset C : A \in \mathrm{Fin}$. $C \subset \bigcup_{a \in A} V_a$. Wówczas $W = \bigcap_{a \in C} U_a \in \Phi_a$, a więc $C \cap W = \varnothing$, $x \notin C^-$ $\lightning\rangle$.

Wnioskiem z powyższego jest stwierdzenie, że podzbiór $A \subset \mathbb{R}$ jest zwarty wtt, gdy jest domknięty i *ograniczony*, tzn. zawarty w pewnym przedziale $[-a, a]$, $a \in \mathbb{R}^+$. $\langle$Zbiór nieograniczony nie może być zwarty, gdyż jego pokrycie $\{(-a, a) \mid a \in \mathbb{R}_+\}$ nie ma podpokrycia skończonego$\rangle$.

Dalsze własności przestrzeni topologicznych zwartych zebrane zostały w zadaniu 52.

9.1.38. Przestrzenie jednostajne, metryczne, unormowane. Bliska kategorii Top przestrzeni topologicznych jest kategoria Unif *przestrzeni jednostajnych*; jej obiekty są postaci $(X, \mathcal{U})$, gdzie $\mathcal{U}$ jest filtrem na X^2 ($\mathcal{U} \in \mathrm{Fil}(X^2)$) spełniającym poniższe trzy warunki:

(1) $\forall\, R \in \mathcal{U} : \mathrm{id}_X \subset R$
(2) $\forall\, R \in \mathcal{U} : R^{-1} \in \mathcal{U}$
(3) $\forall\, R \in \mathcal{U}\ \exists\, S \in \mathcal{U} : S \circ S \subset R$.

Dla dwu takich przestrzeni $(X, \mathcal{U})$, $(X', \mathcal{U}')$ morfizmami są odwzorowania $f : X \to X'$ spełniające warunek $\forall\, R \in \mathcal{U}'\ \exists\, S \in \mathcal{U} : f(S) \subset R$, gdzie $f(S) = \{(f(x), f(z)) \mid (x, z) \in S\}$; mówimy, że są to *odwzorowania jednostajnie ciągłe*.

Dla przestrzeni jednostajnej $(X,\mathcal{U})$ elementy filtru $\mathcal{U}$ nazywamy *otoczeniami przekątnej*; jeżeli przestrzeń taką oznaczamy jedną literą, np. X, to jej filtr otoczeń przekątnej notujemy jako $\mathcal{U}_X$; symbolem $\operatorname{Sym} X$ oznaczamy ogół symetrycznych otoczeń przekątnej – $\operatorname{Sym} X = \{S \in \mathcal{U}_X \mid S^{-1} = S\}$ – zbiór ten jest bazą filtru $\mathcal{U}_X$. $\langle$Dla $R \in \mathcal{U}_X : \operatorname{Sym} X \ni R \cap R^{-1} \subset R\rangle$. Dla $X \in \mathrm{Unif}$ wygodnie jest ograniczać się do symetrycznych otoczeń przekątnej.

W przestrzeni jednostajnej X określamy topologię: dla $x \in X$ jako bazę filtru otoczeń punktu x przyjmujemy zbiór $\{K(x,R) \mid R \in \operatorname{Sym} X\}$, gdzie $K(X,R) = \{y \in X \mid (x,y) \in R\}$. W ten sposób otrzymujemy naturalny funktor zwyczajny

$$F : \mathrm{Unif} \stackrel{\cdot}{\longrightarrow} \mathrm{Top}\,.$$

O przestrzeni topologicznej, którą można uzyskać w ten sposób (tj. należącej do $\operatorname{Im} F$), mówimy, że jest *uniformizowalna*.

Ważne kategorie zwyczajne podporządkowane kategorii Unif – w tym sensie, że z każdej z nich mamy naturalny funktor zwyczajny do kategorii Unif – to:

– Metr – kategoria przestrzeni metrycznych i ich kontrakcji (przestrzeń metryczna (X,ρ), $\rho : X^2 \to \mathbb{R}_+$ ma przeliczalną bazę otoczeń przekątnej: $\{S_n \mid n \in \mathbb{N}^*\}$, gdzie $S_n = \{(x,y) \in X^2 \mid \rho(x,y) \leqslant \frac{1}{n}\}$).
– $\mathrm{TVS} = \mathrm{TVS}_{\mathbb{R}}$ – kategoria przestrzeni wektorowych topologicznych (Topological Vector Spaces) nad ciałem $\mathbb{R}$ i ich odwzorowań liniowych ciągłych (i analogicznie $\mathrm{TVS}_{\mathbb{C}}$).
– $\mathrm{NVS} = \mathrm{NVS}_{\mathbb{R}}$ – kategoria przestrzeni wektorowych unormowanych i ich kontrakcji liniowych.
– Unit – kategoria przestrzeni unitarnych, to jest przestrzeni wektorowych z iloczynem skalarnym, i ich odwzorowań liniowych zachowujących iloczyn skalarny.

Poniższy diagram przedstawia odpowiednie funktory zwyczajne:

$$\begin{tikzcd}
 & & \mathrm{Metr} \arrow[dl] & & \\
\mathrm{Top} & \mathrm{Unif} \arrow[l] & \mathrm{TVS} \arrow[l] & \mathrm{NVS} \arrow[l] \arrow[ul] & \mathrm{Unit}\,. \arrow[l]
\end{tikzcd}$$

9.2. Tematy

1. Niech $n \in \mathbb{N}$. Przez „działanie” rozumieć będziemy działanie dwuargumentowe.

(1) Ile jest działań w zbiorze n-elementowym?

(2) Ile jest działań przemiennych w zbiorze n-elementowym?

(3) Ile jest w zbiorze n-elementowym działań posiadających element neutralny?

(4) Ile jest w zbiorze n-elementowym działań przemiennych i posiadających element neutralny?

(5) Mając dany grupoid $X \in \mathcal{G}$ (tylko mnożenie) określamy $A(X) = \{a \in X \mid \forall\, x,y \in X : (xa)y = x(ay)\} =$ *centrum asocjatywności* X.

Mnożenie w X jest łączne wtt, gdy $A(X) = X$. Wykazać, że zbiór $A(X)$ jest zamknięty ze względu na mnożenie, tzn. $\forall\, a,b \in A(X) : ab \in A(X)$.

(6) Niech $n \in \mathbb{N}$, X – grupoid n-elementowy ($X \in \mathcal{G}$). Jak sprawdzić, mając do dyspozycji tabelkę mnożenia w gropoidzie X (jest to macierz $a : I_n^2 \to X$ taka, że — uprzednio porządkujemy nasz grupoid, $X : I_n \hookrightarrow\!\!\!\!\twoheadrightarrow X$ — $a_{ij} = x_i x_j$), czy mnożenie to jest łączne?

(7) Ile jest działań łącznych w zbiorze 2-elementowym? Podać ich tabelki.

2. Udowodnić własności (1)–(9) kategorii algebr $\mathcal{A}_\nu$ o danej sygnaturze ν.

3*. (J. Schmidt, zob. np. **[Cohn 65]**)
W zbiorze E dana jest algebraiczna operacja domknięcia $\{A \mapsto A^- \mid A \subset E\}$ (zob. 8.1.).

Niech $\Omega = \{(n, a, b) \mid n \in \mathbb{N},\ a = (a_1, \dots, a_n) \in E^n,\ b \in \{a_1, \dots, a_n\}^-\}$, $\nu = \{(n, a, b) \mapsto n \mid (n, a, b) \in \Omega\}$.

Na zbiorze E określamy strukturę algebry X o sygnaturze ν, kładąc dla $\omega = (n, a, b) \in \Omega$, $\omega_X : E^n \to E$, $\forall\, x = (x_1, \dots, x_n) \in E^n : \omega_X(x) = \begin{cases} b, & \text{gdy } x = a \\ x_1, & \text{gdy } x \neq a \end{cases}$.

Wykazać, że operacja przejścia od podzbioru $A \subset E$ do podalgebry $\langle A \rangle$ generowanej przez A pokrywa się z wyjściową operacją domknięcia w E, to jest $\forall\, A \subset E : A^- = \langle A \rangle$.

Tak więc algebraiczna operacja domknięcia w zbiorze E jest zawsze operacją przejścia od podzbioru do podalgebry generowanej w pewnej algebrze ogólnej o podkładzie E.

4. Rozważamy algebry o ustalonej sygnaturze $\nu : \Omega \to \mathbb{N}$. Niech $X, Y, Z \in \mathcal{A}_\nu$, $A \underset{\cdot}{\subset} X$, $R \in \operatorname{Equ} X$ = równoważności w X, $F \underset{\cdot}{\subset} X \times Y$, $G \underset{\cdot}{\subset} Y \times Z$, $f : X \to Y$.

Wykazać, że:

(i) $\operatorname{Im}(F|A)$ $(= \{y \in Y \mid \exists\, a \in A : (a, y) \in F\})$ $\underset{\cdot}{\subset} Y$
(ii) $R \in \operatorname{Congr} X \iff R \underset{\cdot}{\subset} X^2$
(iii) $F^{-1} \underset{\cdot}{\subset} Y \times X$
(iv) $G \circ F \underset{\cdot}{\subset} X \times Z$
(v) $f : X \underset{\cdot}{\longrightarrow} Y \iff f \underset{\cdot}{\subset} X \times Y$.

5. Udowodnić, że dla $X \in \operatorname{Sgr}_1$ (= kategoria półgrup z jedynką), $n, m \in \mathbb{N}$, $a : I_n \to X$, $b : I_m \to X$ zachodzi równość $\prod(a * b) = (\prod a)(\prod b)$ (tu $a * b = a \cup \{b_{n-k} \mid n + 1 \leqslant k \leqslant n + m\}$ — katenacja).

6*. (**[Cohn 65]**, II 5, ex.2)
Dla algebry $X \in \mathcal{A}_\nu$ (= kategoria algebr o sygnaturze ν) niech $F(X) = \{a \in X \mid \forall\, A \subset X : (A \cup \{a\})^- = X \ \Rightarrow\ A^- = X\}$ = elementy *niegenerujące* X (A^- to podalgebra generowana przez $A \subset X$).
Wykazać, że:

(1) $F(X) = \{a \in X \mid \forall\, Y \underset{\cdot}{\subset} X : (Y \cup \{a\})^- = X \ \Rightarrow\ Y = X\}$.
(2) $F(X) \underset{\cdot}{\subset} X$.
$F(X)$ – podalgebra *Frattiniego* algebry X.
(3) $f : X \xrightarrow{\sim} Y \in \mathcal{A}_\nu \ \Rightarrow\ f(F(X)) = F(Y)$.

(4) Jeżeli w algebrze X nie ma podalgebr właściwych maksymalnych ($\forall\, Y \subsetneq X\ \exists\, Y \subsetneq Z \subsetneq X$), to $F(X) = X$.
(5) Jeżeli rodzina $\mathcal{M}$ podalgebr X właściwych maksymalnych jest niepusta, to $F(X) = \bigcap \mathcal{M}$.
Wskazówka:
W dowodzie nie wprost punktów (4) i (5) zastosować lemat Zorna do rodziny

$$\mathcal{N} = \mathcal{N}_a = \{Y \subsetneq X \mid (Y \cup \{a\})^- = X \quad \wedge \quad Y \neq X\},$$

gdzie $a \in X$ (właściwie, do posetu $(\mathcal{N}, \subset)$).

7*. Udowodnić, że w algebrze skończenie generowanej X ($\in \mathcal{A}_\nu$):
(1) każda podalgebra właściwa może być rozszerzana do podalgebry właściwej maksymalnej,
(2) każdy podzbiór generujący zawiera podzbiór generujący skończony.
Wskazówka: Jeżeli $\{a_1, \ldots, a_n\}^- = X$ i Y jest podalgebrą właściwą X, to $a_i \notin Y$ dla pewnego $i \in I_n$.

8. Wykazać, że jeżeli w algebrze X ($\in \mathcal{A}_\nu$) zbiór $B \subset X$ jest minimalnym zbiorem generującym i $|B| \geqslant \omega$, to dla każdego podzbioru generującego G zachodzi nierówność: $|B| \leqslant |G|$.

9*. Dany jest grupoid $X \in \mathcal{G}$ (tylko mnożenie).
(i) Dla $a, b, c \in X$ elementy $(ab)c$ i $a(bc)$ mogą być różne. Podobnie dla czterech elementów $a, b, c, d \in X$ elementy $((ab)c)d$, $(a(bc))d$, $(ab)(cd)$, $a((bc)d)$, $a(b(cd))$ mogą być parami różne.
Podać przykłady.
(ii) Niech α_n oznacza maksymalną liczbę elementów grupoidu X, które można uzyskać przy różnych rozstawieniach nawiasów w iloczynie $a_1 \ldots a_n$.
Tak więc $\alpha_1 = \alpha_2 = 1$, $\alpha_3 = 2$, $\alpha_4 = 5$.
Podać ścisłe określenie ciągu α.
Jak obliczyć α_n?
$\alpha_7 = ?$

10. Udowodnić następujące uogólnienie twierdzenia Lagrange'a (9.1.11):
Dla grup $K < H < G$: $[G : K] = [G : H] \cdot [H : K]$.
(Jeśli $K = \{1\}$, to $[G : K] = [G/K] = |G|$).

11. Rzędem elementu a grupy G nazywamy rząd podgrupy $\langle a \rangle$; $\operatorname{rk} a := \operatorname{rk}\langle a \rangle$.
Niech G będzie grupą skończoną i $a \in G$.
(i) Wykazać, że $\langle a \rangle = \{1, a, \ldots, a^{r-1}\}$, gdzie $r \in \mathbb{N}^*$ jest najmniejszą liczbą taką, że $a^r = 1$, i wówczas $\operatorname{rk} a = r$.
(ii) Wykazać, że jeśli $\operatorname{rk} G = 2n + 1$ ($n \in \mathbb{N}$), to $\forall\, a \in G\ \exists\, b \in G : a = b^2$.
(iii) Wykorzystując *twierdzenie Cauchy'ego* mówiące, że w grupie skończonej, której rząd jest podzielny przez liczbę pierwszą p, istnieje podgrupa rzędu p (zob. np. [**Hungerford 74**, s. 93]), wykazać, że jeśli $\operatorname{rk} G = 2n$ ($n \in \mathbb{N}^*$), to $\exists\, a \in G \setminus \{1\} : a^2 = 1$.

(iv) Udowodnić, że grupa G spełniająca warunek: $\forall\, a \in G : a^2 = 1$ jest abelowa. Podać nietrywialny przykład takiej grupy. Wykazać, że nietrywialna grupa skończona spełniająca powyższy warunek jest rzędu parzystego. (Ze wspomnianego w (iii) twierdzenia Cauchy'ego wynika, że skończona grupa G spełniająca ten warunek jest rzędu 2^k, $k \in \mathbb{N}$).

12. Niech G będzie grupoidem łącznym ($\forall\, a, b, c \in G : (ab)c = a(bc)$) z elementem wyróżnionym $e \in G$. Wykazać, że jeżeli

1°) $\forall\, a \in G : ea = a$ (e jest jedynką lewostronną),
2°) $\forall\, a \in G\ \exists\, b \in G : ba = e$ (dla każdego $a \in G$ istnieje element $b \in G$ lewostronnie odwrotny do a),

to G jest grupą.

13. Dana jest grupa G.

(i) Wykazać, że dla $a \in G$:

$$\sigma_a := \{x \mapsto axa^{-1} \ldots\} : G \xrightarrow{\sim} G.$$

Automorfizmy postaci σ_a nazywamy *wewnętrznymi*.

$$\mathrm{NSub}\, G = \{H \in \mathrm{Sub}\, G \mid \forall\, a \in G : \sigma_a(H) \subset H\}.$$

(ii) $\sigma : G \xrightarrow{\cdot} \mathrm{Aut}\, G$.
(iii) *Centrum* grupy $G = Z(G) := \{a \in G \mid \forall\, x \in G : ax = xa\} = \mathrm{Ker}\, \sigma$; w rozkładzie kanonicznym otrzymujemy więc izomorfizm $\tilde{\sigma} : G/Z(G) \xrightarrow{\sim} \mathrm{Inn}\, G := \mathrm{Im}\, \sigma < \mathrm{Aut}\, G$.
(iv) Centrum $Z(G)$ grupy G jest zamknięte ze względu na wszystkie automorfizmy;

$$\forall\, f \in \mathrm{Aut}\, G : f(Z(G)) \subset Z(G).$$

Podgrupy o tej własności nazywamy *charakterystycznymi*; tak więc każda podgrupa charakterystyczna jest normalna.

14. Udowodnić własności (i)–(iv) półgrupy ułamków danej półgrupy G (9.1.13).

15. Rozważmy grupę addytywną $\mathbb{Z}$ liczb całkowitych,

(i) Wykazać, że $\mathrm{Sub}\, Z = \{n\mathbb{Z} \mid n \in \mathbb{N}\}$.
(ii) Oznaczmy dla $m \in \mathbb{N}_2 = \{2, 3, \ldots\}$: $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ – *grupa reszt modulo m*. Jest to grupa rzędu m – jej elementy można w naturalny sposób utożsamiać z liczbami $0, 1, \ldots, m-1$. Działanie w grupie $\mathbb{Z}_m$ nazywamy *dodawaniem modulo m*. $\mathbb{Z}_m$ jest grupą *cykliczną* (grupa skończona generowana przez jeden element) – jej generatorem jest liczba 1.

Wykazać, że wszystkie liczby $k \in \{1, \ldots, m-1\}$ pierwsze względem m ($k \perp m$) są generatorami grupy $\mathbb{Z}_m$.
(iii) Wykazać, że dla $m, n \in \mathbb{N}_2$ pierwszych względem siebie ($m \perp n$):

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

(Symbol $\cong$ oznacza tu izomorficzność w kategorii grup abelowych).

16. Dana jest grupa G i element $a \in G$. Określić na zbiorze G działanie $*$ tak, aby obiekt $G^* = (G, *)$ był grupą i $f = \{x \mapsto xa^{-1} \mid x \in G\} : G \xrightarrow{\sim} G^*$.
Jaki będzie element neutralny grupy G^*?

17. Udowodnić, że grupa addytywna $\mathbb{Q}$ liczb wymiernych nie jest skończenie generowana.

18*. Wykazać, że grupa addytywna $\mathbb{Q}$ liczb wymiernych:
(1) Nie posiada maksymalnej podgrupy właściwej.
(2) Nie posiada minimalnego zbioru generującego.

19. Wspomagając się prostym kalkulatorem (8 cyfr) wyznaczyć ostatnią cyfrę największej znanej aktualnie (2020) liczby pierwszej $p = 2^{82\,589\,933} - 1$ (rozdz. 5);
$p (\operatorname{mod} 10) = ?$

20. Udowodnić, że dwa zbiory liniowo uporządkowane X, Y przeliczalne, *gęste* (tzn. spełniające warunek: $a < b \;\Rightarrow\; \exists\, c : a < c < b$) i bez elementów ekstremalnych (bez minimum i maksimum) są izomorficzne (podobne).

Wskazówka: Po ustaleniu numeracji tych zbiorów skonstruować ich izomorfizm, dobierając na przemian do elementów jednego z nich odpowiedni element drugiego.

21. Grupę uporządkowaną G nazywany *archimedesową*, gdy
$$\forall_{\substack{a \in G \\ a > 0}} \forall\, x \in G\; \exists\, n \in \mathbb{N} : x \leqslant na.$$
Na przykład grupa $\mathbb{Q}$ jest archimedesowa. $\langle$Dla $p, q, r, s \in \mathbb{N}^*$: $\frac{r}{s} \leqslant n\frac{p}{q} \Leftrightarrow qr \leqslant nps$, co zachodzi np. dla $n = qr\rangle$.

Udowodnić, że grupa ciągła jest archimedesowa.

22. Udowodnić, że zbiór $A = \{a \in \mathbb{Q} \mid 0 < a,\; a^2 < 2\}$ niepusty $\langle 1 \in A\rangle$ i ograniczony od góry $\langle 2 \in M(A)\rangle$ nie ma kresu górnego w $\mathbb{Q}$.

23. Udowodnić własności ciała $\mathbb{R}$ zebrane w zakończeniu Wstępu 9.1.19.

24. Udowodnić 9.1.20 (poprawność definicji pierwiastka; $\sqrt[n]{a}$, dla $a \in R^*_+$, $n \in \mathbb{N}^*$). Naszkicować dowody punktów 2)–4).

25. Dana jest grupa G oraz G-przestrzeń X.
(i) Dla $x \in X$ zbiór $Gx = \{\alpha x \mid \alpha \in G\}$ nazywamy *orbitą* elementu x w przestrzeni X.
Wykazać, że $\{Gx \mid x \in X\}$ jest podziałem X.
(ii) Wykazać, że dla $x \in X$ zbiór $S_x = \{\alpha \in G \mid \alpha x = x\}$, zwany *stabilizatorem* elementu x, jest podgrupą grupy G; $S_x < G$.
(iii) Wykazać, że dla $\alpha \in G$, $x \in X$, $y = \alpha x$ (elementy x, y leżą na jednej orbicie): $\sigma_\alpha(S_x) = S_y$, gdzie σ_α jest automorfizmem wewnętrznym grupy G wyznaczonym przez element α (zadanie 13),
$$\sigma_\alpha = \{\xi \mapsto \alpha\xi\alpha^{-1} \mid \xi \in G\} : G \xrightarrow{\sim} G.$$

O podgrupach, które są izomorficzne przez automorfizm wewnętrzny, mówimy, że są *sprzężone*. I tak stabilizatory elementów leżących na tej samej orbicie są sprzężone.

(iv) Wykazać że dla $x \in X$:

$$\{\alpha x \mapsto \alpha S_x \mid \alpha \in G\} : Gx \hookrightarrow\!\!\!\!\rightarrow G/S_x.$$

Tak więc dla danej orbity Gx liczba $|Gx|$ zwana *długością orbity* równa jest indeksowi stabilizatora dowolnego punktu leżącego na tej orbicie; $|Gx| = [G : S_x]$. Jest to tzw. *formuła orbit*.

(v) Zakładając elementarną znajomość geometrii można za pomocą formuły orbit wyznaczać rzędy grup izometrii własnych różnych obiektów geometrycznych. Na przykład dla grupy G izometrii własnych czworościanu foremnego zbiór X ścian tego czworościanu można traktować jako G-przestrzeń. Wówczas dla dowolnej ściany $\varphi \in X$ jej orbita pokrywa się z X; $|G\varphi| = |X| = 4$. Natomiast stabilizator S_φ ściany φ jest rzędu 6 (trzy symetrie i trzy obroty) – zatem $|G\varphi| = [G : S_x] = |G|/|S_x|$, skąd $|G| = |G\varphi| \cdot |S_\varphi| = 4 \cdot 6 = 24$.

Stosując tę metodę wyznaczyć rząd grupy izometrii własnych sześcianu i ogólnie kostki n-wymiarowej ($[0,1]^n$).

26. Dla ciała K, przestrzeni wektorowej X nad K i zbioru $A \subset X$ udowodnić prawa (i)–(iv) z 9.1.23.

27. Udowodnić, że podzbiór A przestrzeni $X \in \mathrm{Vect}_K$ jest liniowo niezależny wtt, gdy jest niezależny (w sensie strukturalnym, w kategorii Vect_K).

28*. Rozważmy równanie funkcyjne, w którym szukamy funkcji $f : R \to R$ spełniającej warunek:

(*) $$f(x+y) = f(x) + f(y) \qquad (\textit{równanie Cauchy'ego}).$$

(i) Udowodnić, że przy dodatkowym założeniu:

$$\exists\, \alpha, \beta, M \in \mathbb{R} : \alpha < \beta \ \wedge\ \forall\, x \in (\alpha, \beta) : f(x) < M \qquad \text{lub } \ldots > M$$

rozwiązaniem równania (*) są funkcje liniowe $f(x) = cx$, $c \in \mathbb{R}$.

Wskazówka: skorzystać z faktu, że między dwiema liczbami rzeczywistymi znajdziemy zawsze liczbę wymierną.

(ii) Wykazać, że bez dodatkowego warunku z (i) równanie (*) ma jeszcze inne „egzotyczne" rozwiązania.

Wskazówka: Potraktować $\mathbb{R}$ jako przestrzeń wektorową nad ciałem $\mathbb{Q}$.

29. Udowodnić nierówność Cauchy'ego:

(*) $$x_1, \ldots, x_n > 0 \implies \frac{x_1 + \ldots + x_n}{n} \geqslant \sqrt[n]{x_1 \ldots x_n}.$$

Wykazać, że równość zachodzi wtt, gdy $x_1 = \ldots = x_n$.
Wskazówka: Wystarczy ograniczyć się do przypadku, gdy $x_1 + \ldots + x_n = n$. W dowodzie indukcyjnym wykorzystać lemat: $0 < x < 1 < y \ \Rightarrow\ x + y > xy + 1$.

30. Dla $n \in \mathbb{N}$ wyznaczyć $W_n = \det a$, gdzie

$$a : I_n^2 \to \mathbb{Z}, \quad a_{ij} = \begin{cases} 1, & \text{gdy } |i-j| \leqslant 1 \\ 0, & \text{w przeciwnym wypadku.} \end{cases}$$

$W_{100} = ?$

31. Niech R będzie pierścieniem całkowitym. Dla $n \in \mathbb{N}^*$ *wyznacznikiem Vandermonde'a* układu $x : I_n \to R$ nazywamy skalar:

$$V(x) := \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix}$$

Wykazać, że:

$$x : I_n \hookrightarrow R \iff V(x) \neq 0.$$

32. Rozwiązać układ równań:

$$\begin{cases} \lambda x + y + z + t = 1 \\ x + \lambda y + z + t = \lambda \\ x + y + \lambda z + t = \lambda^2 \\ x + y + z + \lambda t = \lambda^3 \end{cases}$$

gdzie $\lambda \in \mathbb{R}$ jest parametrem.

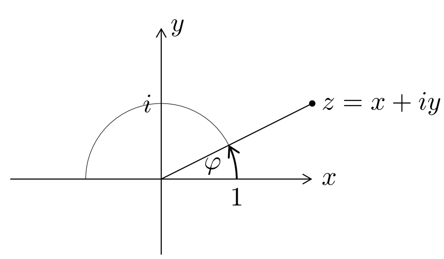
33. Udowodnić poniższy *lemat Steinitza o zamianie* (natychmiastowym wnioskiem z niego jest równoliczność baz przestrzeni wektorowej skończenie wymiarowej):

Jeżeli X jest przestrzenią wektorową nad ciałem R, $n, m \in \mathbb{N}$, $e : I_m \to X$ jest układem liniowo niezależnym i $v : I_n \to X$ jest układem generującym, to $m \leqslant n$ i można wymienić m wektorów spośród $v_1, \dots, v_n$ na wektory $e_1, \dots, e_m$ tak, aby ten nowy układ był dalej generujący.
WSKAZÓWKA: Zastosować indukcję na m.

34. Rozwiązać w $\mathbb{R}$, dokładnie, równanie $x^3 - x^2 - x - 1 = 0$.

35. W tym zadaniu zakładamy elementarną znajomość funkcji trygonometrycznych $\sin, \cos : \mathbb{R} \to \mathbb{R}$ i geometrii płaszczyzny $\mathbb{R}^2$.

Niezerową liczbę zespoloną $z = x + iy$ $(x, y \in \mathbb{R})$ można przedstawić w *postaci trygonometrycznej* $z = r(\cos\varphi + i \sin\varphi)$, gdzie $r = |z| = \sqrt{x^2 + y^2} > 0$ jest *modułem* liczby z, zaś liczba $\varphi \in \mathbb{R}$ jest miarą kąta między wektorami 1 i z; kąt ten, określony z dokładnością do całkowitej wielokrotności 2π (mówimy: *modulo* 2π), nazywamy *argumentem* liczby z.



Notujemy też: $e^{i\varphi} = \cos\varphi + i\sin\varphi$. Jeżeli jeszcze $w = se^{i\psi}$, $s > 0$, $\psi \in \mathbb{R}$, to, jak łatwo przeliczyć, $zw = rse^{i(\varphi+\psi)}$.
Tak więc mnożenie niezerowych liczb zespolonych sprowadza się do mnożenia ich modułów i dodawania (modulo 2π) argumentów. Fakt ten ułatwia operowanie przekształceniami płaszczyzny, w których występują obroty.

Oznaczmy dla $a \in \mathbb{C}$, $\varphi \in \mathbb{R}$: $\mathrm{Rot}_{a,\varphi}$ = obrót płaszczyzny $\mathbb{R}^2$ o kąt φ wokół punktu a; $\mathrm{Rot}_\varphi = \mathrm{Rot}_{0,\varphi}$. Wówczas dla $z \in \mathbb{C} = \mathbb{R}^2$:

$$\mathrm{Rot}_\varphi(z) = ze^{i\varphi}, \quad \mathrm{Rot}_{a,\varphi}(z) = (z-a)e^{i\varphi} + a.$$

(1) Obliczyć $\mathrm{Rot}_{(3,4),60^\circ}(1,2)$
(2) Niech $a, b \in \mathbb{C}$, $\varphi, \psi \in \mathbb{R}$.
$f = \mathrm{Rot}_{b,\psi} \circ \mathrm{Rot}_{a,\varphi} = ?$

36. Udowodnić własności (i)–(iii) przestrzeni afinicznych z 9.1.29.

37. Znaleźć centrum $Z = Z(\mathbb{K}^*)$ grupy multyplikatywnej $\mathbb{K}^*(= \mathbb{K}\setminus\{0\})$ kwaternionów niezerowych.

38*. W tym zadaniu zakładamy elementarną znajomość trygonometrii oraz dla $a, b, c \in \mathbb{R}^3$ własności geometrycznych i algebraicznych iloczynu skalarnego $a \circ b$ $(\in \mathbb{R})$ i iloczynu wektorowego $a \times b$ $(\in \mathbb{R}^3)$; w szczególności: $(a \times b) \times c = -(b \circ c)a + (a \circ c)b$.

Kwaternion $a = xi + yj + zk$, gdzie $x, y, z \in \mathbb{R}$, nazywamy *wektorowym*; można go utożsamiać z punktem $(x, y, z) \in \mathbb{R}^3$, traktując i, j, k jako wektory barowe, tj. $i = (1, 0, 0)$, $j = (0, 1, 0)$, $k = (0, 0, 1)$. Prostym rachunkiem sprawdzamy, że $ab = -a \circ b + a \times b$, a więc $ba = -a \circ b - a \times b$. Dodając i odejmując stronami te dwie równości otrzymujemy: $a \circ b = -\frac{1}{2}(ab + ba)$, $a \times b = \frac{1}{2}(ab - ba)$. Jeżeli $|a| = 1$, $a \in \mathbb{R}^3$, to $a^2 = -1$.

Wykazać, że obrót punktu $p \in \mathbb{R}^3$ o kąt $\varphi \in \mathbb{R}$ wokół osi $\mathbb{R}v$, gdzie $v \in \mathbb{R}^3$, $|v| = 1$, wyraża się wzorem $p' = qpq^{-1}$, gdzie $q = \cos\frac{\varphi}{2} + v\sin\frac{\varphi}{2}$ (wówczas $q\bar{q} = 1$, a więc $q^{-1} = \bar{q}$).
Wskazówka: Przejść na iloczyny skalarne i wektorowe. Rozpatrzyć wpierw przypadek szczególny, gdy środek obrotu jest początkiem układu.

Przykłady:

(1) Obrócić punkt $p = (x, y, z) \in \mathbb{R}^3$ wokół osi $\mathbb{R}w$, gdzie $w = (1, 1, 1) = i + j + k$, o kąt $\varphi = 120^\circ$ $(v = \frac{1}{\sqrt{3}}w)$.
(2) Obrócić punkt $p = (1, 0, 1) = i + k$ o kąt $\varphi = 120^\circ$ wokół osi $k + \mathbb{R}w$, gdzie wektor w jest taki jak w (i).

Uwaga: W przypadku (ii) oś obrotu nie przechodzi przez początek układu, a więc $p' = q(p-k)q^{-1} + k$.

39. Wykazać, że:

(i) Jeżeli do filtru należy zbiór skończony, to filtr ten jest główny.
(ii) Filtr Frécheta $\mathcal{F}$ na zbiorze nieskończonym X $(\mathcal{F} = \{A \subset X \mid A^\neg = X\setminus A \in \mathrm{Fin}\})$ nie jest główny.
(iii) Filtr Φ_a otoczeń punktu $a \in \mathbb{R}$ nie jest główny.

40. Dany jest zbiór X mocy $\alpha \geqslant \aleph_0$. Wykazać, że:

(i) $\beta \in \mathrm{Card} \ \wedge \ \aleph_0 \leqslant \beta \leqslant \alpha \implies \mathcal{F}_\beta = \{A \subset X \mid |X \setminus A| < \beta\} \in \mathrm{Fil}^*(X)$.

(ii) Każdy z filtrów $\mathcal{F}_\beta$ z (i) jest niegłówny.

(iii) Jeżeli $\alpha = \aleph_{\xi+1}$, $\xi \in \mathrm{Ord}$, to filtr $\mathcal{F}_\alpha$ jest α-*zupełny*, tzn.

$$\forall\, \mathcal{A} \subset \mathcal{F}_\alpha \ (0 \neq |\mathcal{A}| < \alpha \implies \bigcap \mathcal{A} \in \mathcal{F}_\alpha).$$

41. Wykazać, że w zbiorze $\mathrm{Fil}^*(X)$ filtrów właściwych na zbiorze nietrywialnym X ($|X| \geqslant 2$) nie istnieje filtr największy.

42. Udowodnić, że filtr $\mathcal{F}$ na zbiorze X jest niegłówny wtt, gdy $\forall\, A \in \mathcal{F}\ \exists\, B \in \mathcal{F} : B \subsetneq A$.

43. Elementy maksymalne w zbiorze $\mathrm{Fil}^*(X)$ nazywamy *ultrafiltrami* na X; ich ogół oznaczamy $\mathrm{Ultr}(X)$. Z lematu Zorna (a więc z AC) wynika, że $\forall\, \mathcal{F} \in \mathrm{Fil}^*(X)\ \exists \mathcal{U} \in \mathrm{Ultr}(X) : \mathcal{F} \subset \mathcal{U}$. $\langle$Dla niepustego łańcucha γ w $\{\mathcal{G} \in \mathrm{Fil}^*(X) \mid \mathcal{F} \subset \mathcal{G}\}$ majorantą jest $\bigcup \gamma\rangle$.

Wykazać, że dla filtru właściwego $\mathcal{U}$ na zbiorze X równoważne są warunki:

(a) $\mathcal{U} \in \mathrm{Ultr}(X)$

(b) $\forall\, A, B \subset X : A \cup B \in \mathcal{U} \ \Rightarrow \ A \in \mathcal{U} \ \vee \ B \in \mathcal{U}$

(c) $\forall\, A \subset X : A \in \mathcal{U} \ \vee \ A^\neg = X \setminus A \in \mathcal{U}$.

44. Wykazać że każdy ultrafiltr niegłówny $\mathcal{U}$ na $\mathbb{N}$ zawiera filtr Frécheta $\mathcal{F} = \{A \subset \mathbb{N} \mid A^\neg \in \mathrm{Fin}\}$.

45. Wykazać, że jeżeli $f : X \to Y$, $\mathcal{F} \in \mathrm{Fil}^*(X)$, $\mathcal{G} \in \mathrm{Fil}^*(Y)$, przy czym filtr $\mathcal{F}$ jest typu przeliczalnego, to

$$\underset{x \to \mathcal{F}}{f(x)} \longrightarrow \mathcal{G} \iff \forall\, u : \mathbb{N} \to X \ \big[\, \underset{n \to \infty}{u_n} \longrightarrow \mathcal{F} \iff \underset{n \to \infty}{f(u_n)} \longrightarrow \mathcal{G} \,\big].$$

Prawa strona tej równoważności znana jest jako *warunek Heinego* granicy.

46. Wykazać, że przestrzeń topologiczna X jest przestrzenią Hausdorffa wtt, gdy każda funkcja wchodząca do tej przestrzeni i określona na zbiorze z filtrem właściwym ma co najwyżej jedną granicę.

Symbolicznie:

$$X \in \mathrm{Top}(T_2) \iff \forall_{\substack{f : T \to X \\ \mathcal{F} \in \mathrm{Fil}^*(T) \\ a, b \in X}} \big[\, \underset{t \to \mathcal{F}}{f(t)} \longrightarrow a \ \wedge \ \underset{t \to \mathcal{F}}{f(t)} \longrightarrow b \implies a = b \,\big].$$

47. Dany jest zbiór X z filtrem właściwym $\mathcal{F}$.

Udowodnić, że:

(i) Jeżeli $f, g, h : X \to \mathbb{R}$, $a \in \mathbb{R}$,

$$\forall\, x \in X : f(x) \leqslant g(x) \leqslant h(x) \text{ oraz } \lim_{x \to \mathcal{F}} f(x) = \lim_{x \to \mathcal{F}} h(x) = a,$$

to $\lim_{x \to \mathcal{F}} f(x) = a$ (*Twierdzenie o trzech funkcjach*).

(ii) Jeżeli $f, g : X \to \mathbb{C}$, $a, b \in \mathbb{C}$, $f(x) \underset{x \to \mathcal{F}}{\longrightarrow} a$, $g(x) \underset{x \to \mathcal{F}}{\longrightarrow} b$, to

$$f(x) + g(x) \underset{x \to \mathcal{F}}{\longrightarrow} a + b \quad \text{i} \quad f(x) \cdot g(x) \underset{x \to \mathcal{F}}{\longrightarrow} a \cdot b.$$

(iii) Jeżeli $f : X \to \mathbb{C}^*$, $a \in \mathbb{C}^*$, $f(x) \underset{x \to \mathcal{F}}{\longrightarrow} a$, to $\frac{1}{f(x)} \underset{x \to \mathcal{F}}{\longrightarrow} \frac{1}{a}$.

Podobnie można sformułować i udowodnić twierdzenia o nierównościach dla granic funkcji wchodzących do $\mathbb{R}$, dla granicy funkcji monotonicznej (na $\mathbb{N}$ lub w przedziale) itp.

48. Cztery pojęcia topologiczne są podstawowe.

Dla przestrzeni topologicznej $(X, \varPhi)$ i zbioru $A \subset X$:

1) $\bar{A} = A^- = \operatorname{cl} A = \operatorname{cl}_X A = \{x \in X \mid \forall\, U \in \varPhi_x : U \cap A \neq \varnothing\}$ – *domknięcie* A
2) $\mathring{A} = A^\circ = \operatorname{int} A = \operatorname{int}_X A := \{x \in X \mid A \in \varPhi_x\}$ – *wnętrze* A
3) $\tau = \tau_X := \{A \subset X \mid A^\circ = A\}$ – zbiory *otwarte* w X
4) $\sigma = \sigma_X := \{A \subset X \mid A^- = A\}$ – zbiory *domknięte*.

Każde z tych pojęć może służyć do definicji kategorii przestrzeni topologicznych. Mamy więc pięć formalnie różnych kategorii zwyczajnych, które są równoważne przez funktory zwyczajne, jak zaznaczono na diagramie na stronie 247.

Należy:

1°) Udowodnić, że przedstawione poniżej odwzorowania są rzeczywiście wzajemnie odwrotnymi funktorami zwyczajnymi.
2°) Wykazać, że funkcja $f : X \to X'$ $(X, X' \in \mathrm{Top})$ jest ciągła wtt, gdy $\forall\, A \subset X$: $f(A^-) \subset f(A)^-$. Czy mamy odpowiednik tego faktu dla operacji wnętrza?

49. Udowodnić, że dla przestrzeni topologicznej X i podzbioru $E \subset X$ poniższe trzy warunki są równoważne:

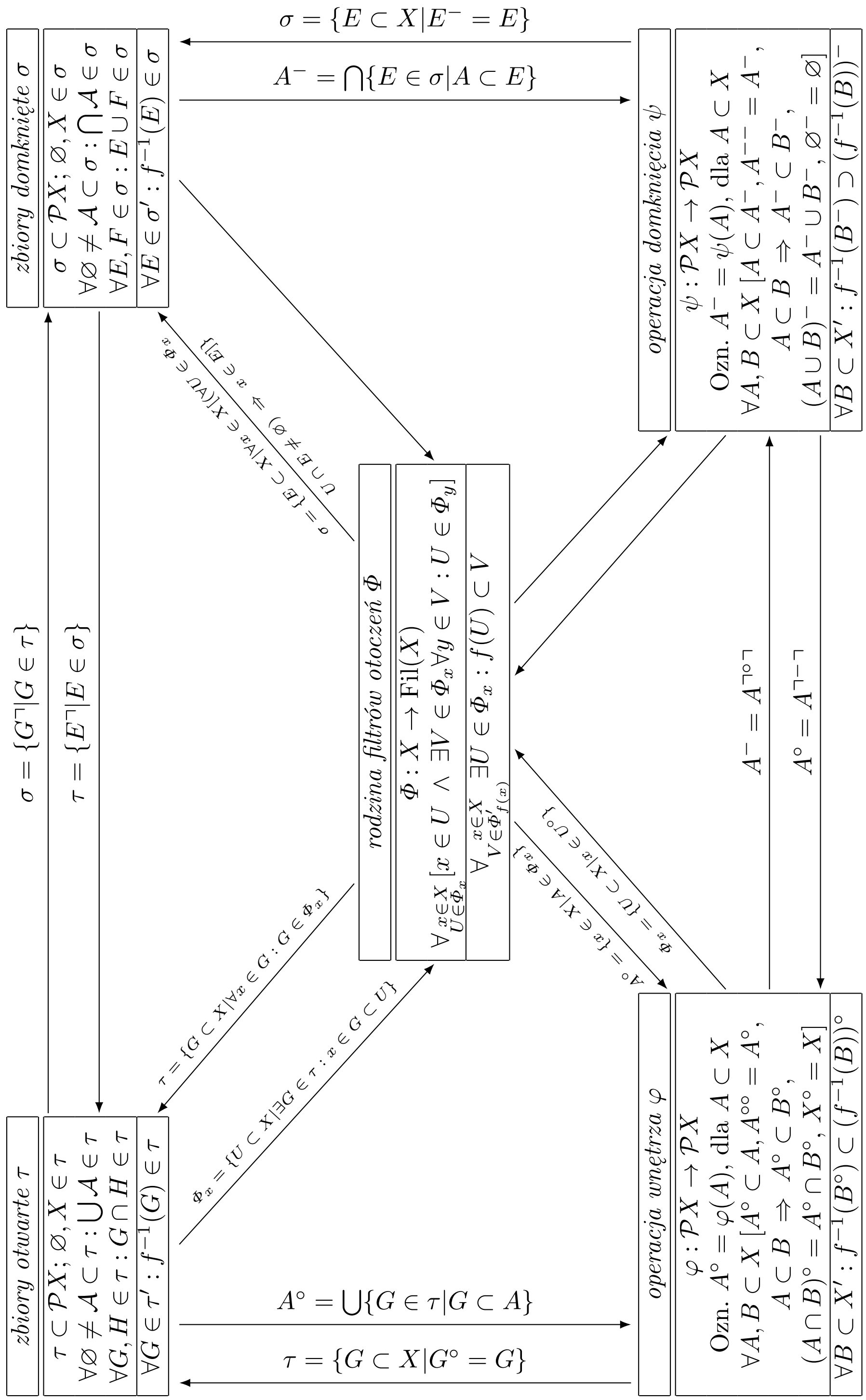
(1) E jest domknięty
(2) $\forall_{\substack{T,\, \mathcal{F} \in \mathrm{Fil}^*(T) \\ f : T \to E}} : \operatorname*{Lim}_{t \to \mathcal{F}} f(t) \subset E$
(3) $\forall_{\substack{T,\, \mathcal{F} \in \mathrm{Fil}^*(T) \\ f : T \to E}} : \operatorname*{Adh}_{t \to \mathcal{F}} f(t) \subset E$.

50. Udowodnić, że dla przestrzeni topologicznej X poniższe trzy warunki są równoważne:

(1) X jest zwarta
(2) $\forall_{\substack{T,\, \mathcal{F} \in \mathrm{Fil}^*(T) \\ f : T \to X}} : \operatorname*{Adh}_{t \to \mathcal{F}} f(t) \neq \varnothing$
(3) $\forall_{\substack{T,\, \mathcal{U} \in \mathrm{Ultr}(T) \\ f : T \to X}} : \operatorname*{Lim}_{t \to \mathcal{U}} f(t) \neq \varnothing$.

($\mathrm{Ultr}(T)$ to ogół ultrafiltrów na T).
Wskazówka: Dowód równoważności (1) $\Leftrightarrow$ (2) jest bezproblemowy. Dla dowodu równoważności (2) $\Leftrightarrow$ (3) wykazać wstępnie, że dla $\mathcal{U} \in \mathrm{Ultr}(T)$:

$$\operatorname*{Adh}_{t \to \mathcal{U}} f(t) = \operatorname*{Lim}_{t \to \mathcal{U}} f(t).$$



Równoważne definicje kategorii przestrzeni topologicznych

51.

(i) Udowodnić *twierdzenie Tichonowa*:

$$\forall\, X : I \to \mathrm{Comp}\ (\prod X \in \mathrm{Comp}).$$

(ii)* Twierdzenie Tichonowa jest wnioskiem z AC.

W roku 1950 J. Kelly (Fund. Math. 37) wykazał równoważność w ZF aksjomatu wyboru (AC) i twierdzenia Tichonowa. Udowodnić ten fakt.

Wskazówka: W dowodzie nie wprost implikacji Tw.Tichonowa $\Rightarrow$ AC, mając rodzinę zbiorów niepustych $X : I \to \mathbb{V}$ wziąć „element zewnętrzny” b, i każdy ze zbiorów $X'_i = X_i \cup \{b\}$ $(i \in I)$ potraktować jako przestrzeń topologiczną zwartą z topologią określoną przez odpowiednio dobraną rodzinę zbiorów otwartych.

52. Udowodnić poniższe własności przestrzeni topologicznych zwartych:

(1) $X \in \mathrm{Comp},\ Y \in \mathrm{Top},\ f : X \overset{.}{\twoheadrightarrow} Y \implies Y \in \mathrm{Comp}$.
(Obraz przestrzeni zwartej przez odwzorowanie ciągłe jest zwarty).

(2) $X \in \mathrm{Comp},\ Y \in \mathrm{Top}(T_2),\ f : X \overset{.}{\longrightarrow} Y,\ A \in \sigma_X =$ podzbiory domknięte w $X \implies f(A) \in \sigma_Y$.
(Odwzorowanie ciągłe kompaktu w przestrzeń Hausdorffa przeprowadza zbiory domknięte w zbiory domknięte).

(3) $X \in \mathrm{Comp},\ Y \in \mathrm{Top}(T_2),\ f : X \overset{.}{\hookrightarrow\!\!\!\!\rightarrow} Y \implies f : X \xrightarrow{\sim} Y$.

W szczególności:

(3.1) W kategorii $\mathrm{Comp}(T_2)$ bijekcje ciągłe są homeomorfizmami.

(3.2) W kategorii $\mathrm{Top}(T_2)$ przestrzeni Hausdorffa przestrzenie zwarte są elementami $\prec$-minimalnymi.

(4) Zwarta przestrzeń Hausdorffa X jest *normalna*, tzn. dwa jej podzbiory domknięte i rozłączne można rozszerzyć do podzbiorów otwartych rozłącznych.
(Jest to warunek rozdzielczości T_4:

$$\forall_{\substack{A,B\in\sigma_X\\ A\cap B=\varnothing}} \exists_{\substack{G,H\in\tau_X\\ G\cap H=\varnothing}} : A \subset G,\ B \subset H).$$

53. Dla przestrzeni jednostajnej X użyteczny jest lemat:

$$\forall\, R \in \mathcal{U}_X,\ n \in \mathbb{N}^*\ \exists\, S \in \mathrm{Sym}\, X : \underbrace{S \circ \ldots \circ S}_{n} = S^n \subset R.$$

Udowodnić ten fakt.

54. Wykazać, że dla przestrzeni jednostajnej X traktowanej jako przestrzeń topologiczna zachodzi równoważność:

$$X \text{ jest przestrzenią Hausdorffa} \iff \bigcap \mathrm{Sym}\, X = \mathrm{id}_X\,.$$

55. Wykazać, że każdy punkt przestrzeni topologicznej uniformizowalnej ma bazę otoczeń domkniętych, tzn. każde jego otoczenie zawiera otoczenie domknięte.
(Do przestrzeni takich stosuje się więc I-e twierdzenie o granicy podwójnej z następnego zadania 56).

56. Udowodnić *I-e twierdzenie o granicy podwójnej*:
Zakładamy, że $f : X \times Y \to Z$, $\mathcal{F} \in \mathrm{Fil}^*(X)$, $\mathcal{G} \in \mathrm{Fil}^*(Y)$, $Z \in \mathrm{Top}$, punkt $z \in Z$ posiada bazę $\mathcal{C}$ otoczeń domkniętych, $\underset{x \to \mathcal{F},\, y \to \mathcal{G}}{f(x,y)} \longrightarrow c$ (ten ostatni zapis oznacza, że $\underset{(x,y) \to \mathcal{F} \bar{\times} \mathcal{G}}{f(x,y)} \longrightarrow c$, gdzie $\mathcal{F} \bar{\times} \mathcal{G}$ jest filtrem produktowym na iloczynie kartezjańskim $X \times Y$; mówimy wówczas, że c jest *granicą podwójną*), $\varphi : Y \to Z$, $\forall\, y \in Y : \underset{x \to \mathcal{F}}{f(x,y)} \longrightarrow \varphi(y)$.
Teza: $\underset{y \to \mathcal{G}}{\varphi(y)} \longrightarrow c$.

Jeżeli Z jest przestrzenią Hausdorffa, to granice w niej są wyznaczone jednoznacznie i tezę twierdzenia można zapisać w postaci równości

$$\lim_{y \to \mathcal{G}} \lim_{x \to \mathcal{F}} f(x,y) = \lim_{\substack{x \to \mathcal{F} \\ y \to \mathcal{G}}} f(x,y),$$

której lewa strona to *granica iterowana* – jedna z dwu.
Przy wskazanych założeniach o przestrzeni Z i punkcie c teza głosi, że jeżeli istnieje granica podwójna równa c i w granicy iterowanej istnieje granica wewnętrzna, to istnieje granica iterowana równa granicy podwójnej.

57. Jeżeli $f : T \times X \to Y$, $\varphi : X \to Y$, gdzie $X, Y \in \mathrm{Top}$, $\mathcal{F} \in \mathrm{Fil}^*(T)$, $\forall\, x \in X : \underset{t \to \mathcal{F}}{f(t,x)} \longrightarrow \varphi(x)$ i wszystkie funkcje $f_t = \{x \mapsto f(t,x) \mid x \in X\} : X \to Y$ są ciągłe, to funkcja graniczna φ nie musi być ciągła.

Sytuacja się zmienia, gdy $Y \in \mathrm{Unif}$ i zbieżność jest *jednostajna* (zapis: $f(t,x) \to \varphi(x)$, gdy $t \to \mathcal{F}$, jednostajnie dla $x \in X$), tzn.

$$\forall\, R \in \mathrm{Sym}\, Y\ \exists\, A \in \mathcal{F}\ \forall\, t \in A,\ x \in X : f(t,x) \in K(\varphi(x), R) \quad (\Leftrightarrow (f(t,x), \varphi(x)) \in R).$$

Wówczas z ciągłości wszystkich funkcji f_t, $t \in T$ wynika ciągłość funkcji φ (mówimy: zbieżność jednostajna zachowuje ciągłość).

Udowodnić ten fakt.

58. Jeżeli $f : T \to X$, gdzie $X \in \mathrm{Unif}$, $\mathcal{F} \in \mathrm{Fil}^*(T)$, to mówimy, że funkcja f spełnia *warunek Cauchy'ego*, gdy $\forall\, R \in \mathrm{Sym}\, X\ \exists\, A \in \mathcal{F}\ \forall\, t, s \in A : (f(t), f(s)) \in R$.

Wykazać, że dla $x \in X$:

(i) Jeżeli $\underset{t \to \mathcal{F}}{f(t)} \longrightarrow x$, to f spełnia warunek Cauchy'ego.
(ii) Jeżeli f spełnia warunek Cauchy'ego i $x \in \underset{t \to \mathcal{F}}{\mathrm{Adh}}\, f(t)$

$$(\text{tzn.: } \forall\, A \in \mathcal{F},\ R \in \mathrm{Sym}\, X : f(A) \cap K(x,R) \neq \varnothing),$$

to $\underset{t \to \mathcal{F}}{f(t)} \longrightarrow x$.

59. Mówimy, że przestrzeń jednostajna jest *zupełna*, jeżeli każda funkcja wchodząca do niej, określona na zbiorze z filtrem i spełniająca warunek Cauchy'ego, ma granicę.

Wykazać, że:

(i) Jeżeli przestrzeń jednostajna X jest typu przeliczalnego (tzn. filtr otoczeń przekątnej ma bazę przeliczalną), to do jej zupełności wystarczy, aby każdy ciąg $x : \mathbb{N} \to X$ spełniający warunek Cauchy'ego był zbieżny.
(ii) Przestrzeń kartezjańska $\mathbb{R}^n$ jest zupełna.

60. Niech $f : T \times X \to Y$, $\mathcal{F} \in \operatorname{Fil}^*(X)$, $Y \in \operatorname{Unif}$. Mówimy, że funkcja f *spełnia jednostajnie* względem $x \in X$ warunek Cauchy'ego, gdy $t \to \mathcal{F}$, jeżeli

$$\forall\, R \in \operatorname{Sym} Y\ \exists\, A \in \mathcal{F}\ \forall\, t, s \in A,\ x \in X : (f(t,x), f(s,x)) \in R.$$

Wykazać, że jeżeli tak jest i przestrzeń Y jest zupełna, to istnieje funkcja $\varphi : X \to Y$ taka, że $f(t,x) \underset{t\to\mathcal{F}}{\longrightarrow} \varphi(x)$ jednostajnie dla $x \in X$.

61*. Udowodnić *II-e twierdzenie o granicy podwójnej*:

Jeżeli funkcja określona na iloczynie kartezjańskim dwóch zbiorów z filtrami i wchodząca do przestrzeni jednostajnej zupełnej Z ma w obu granicach iterowanych granice wewnętrzne (zob. zadanie 56) i jedno z tych przejść granicznych jest jednostajne, to dla funkcji tej istnieje granica podwójna.

Symbolicznie:

$$\big[f : X \times Y \to Z,\ \mathcal{F} \in \operatorname{Fil}^*(X),\ \mathcal{G} \in \operatorname{Fil}^*(Y),\ \varphi : X \to Z,\ \psi : Y \to Z,$$
$$\forall\, x \in X : f(x,y) \underset{y\to\mathcal{G}}{\longrightarrow} \varphi(x),\ f(x,y) \to \psi(y),\ \text{gdy } x \to F,\ \text{jednostajnie dla } y \in Y\big]$$
$$\Longrightarrow\ \exists\, c \in Z : \underset{x\to\mathcal{F},\, y\to\mathcal{G}}{f(x,y)} \longrightarrow c.$$

(Jeżeli dodatkowo założymy, że przestrzeń Z jest rozdzielcza, to granice w niej są wyznaczone jednoznacznie i, wykorzystując I-e twierdzenie o granicy podwójnej, możemy tezę drugiego twierdzenia o granicy podwójnej zapisać:

$$\exists\, c \in Z : \lim_{\substack{x\to\mathcal{F}\\ y\to\mathcal{G}}} f(x,y) = \lim_{x\to\mathcal{F}} \underbrace{\lim_{y\to\mathcal{G}} f(x,y)}_{\varphi(x)} = \lim_{y\to\mathcal{G}} \underbrace{\lim_{x\to\mathcal{F}} f(x,y)}_{\psi(y)} = c.$$

Twierdzenie powyższe stanowi silne i często wykorzystywane narzędzie do wyznaczania różnych granic; w sytuacji, gdy znamy $\lim\limits_{y\to\mathcal{G}} \psi(y) = c$, uzyskujemy $\lim\limits_{x\to\mathcal{F}} \varphi(x) = c$).

62*. (N. Bourbaki) Wykazać, że przestrzeń topologiczna X zwarta i rozdzielcza jest jednoznacznie uniformizowalna, to znaczy istnieje dokładnie jedna struktura jednostajna $\mathcal{U}$ na zbiorze X ($\mathcal{U} \in \operatorname{Fil}(X^2)$) indukująca topologię przestrzeni X. Filtr $\mathcal{U}$ otoczeń przekątnej tej struktury jednostajnej jest zbiorem otoczeń przekątnej id_X w przestrzeni topologicznej $X^2 = X \times X$.

Otrzymana w ten sposób przestrzeń jednostajna $(X,\mathcal{U})$ jest zupełna.

Wskazówka: Udowodnić wpierw, że zbiór $\mathcal{U}$ otoczeń przekątnej w przestrzeni topologicznej X^2 jest strukturą jednostajną. W dowodzie nie wprost prawa $\forall\, R \in \mathcal{U}\ \exists\, S \in \mathcal{U} : S \circ S \subset R$ wykorzystać zwartość przestrzeni $X \times X = X^2$.
(Taki dowód twierdzenia o jednostajności i zupełności zwartej przestrzeni Hausdorffa pochodzi od N. Bourbakiego: *Topologie générale*, chap. II, §4, th.1).

9.3. Odpowiedzi

1.

(1) card Map$(I_n^2, I_n) = n^{n^2}$.

(2) W tabelce działania $m : I_n^2 \to I_n$ trzeba wypełnić miejsca pod przekątną i na przekątnej; miejsc tych jest $\frac{n^2-n}{2} + n = \frac{n^2+n}{2}$. Odpowiedź: $n^{\frac{n^2+n}{2}}$.

(3) Element neutralny wybieramy na n sposobów, po czym mamy do zapełnienia $(n-1)^2$ miejsc n elementami.
Odpowiedź: $n \cdot n^{(n-1)^2} = n^{n^2-2n+2}$.

(4) Jak wyżej, tyle że w kwadracie $(n-1)\times(n-1)$ zapełniamy miejsca pod przekątną i na przekątnej w liczbie $\frac{(n-1)^2+(n-1)}{2} = \frac{n^2-n}{2}$. Odpowiedź: $n \cdot n^{\frac{n^2-n}{2}} = n^{\frac{n^2-n+2}{2}}$.

(5) Jeżeli $a, b \in A(X)$, to $\forall\, x, y \in X : (x(ab))y = ((xa)b)y = (xa)(by) = x(a(by)) = x((ab)y)$.

(6) Niech $X = \{x_1, \ldots, x_n\}$; sprawdzamy, czy $x_k \in A(X)$, wykorzystując (5) i biorąc k $(= 1, 2, \ldots, n)$ w odpowiedniej kolejności.

(7) W 2-elementowym zbiorze $X = \{a, b\}$ jest 16 działań. Klasyfikujemy je według głównej przekątnej tabelki działania na cztery klasy: $(a\ a)$, $(a\ b)$, $(b\ a)$, $(b\ b)$.

I) $(a\ a)$ $\quad \begin{array}{c|cc} & a & b \\ \hline a & a & a \\ b & a & a \end{array}, \quad \begin{matrix} a & a \\ b & a \end{matrix}, \quad \begin{matrix} a & b \\ a & a \end{matrix}, \quad \begin{matrix} a & b \\ b & a \end{matrix}.$

Łącznym jest oczywiście działanie określone przez pierwszą tabelkę.
Dla działania: $\cdot : X^2 \to X$ określonego drugą tabelką wystarczy (według (5)) sprawdzić, czy $b \in A =$ centrum asocjacyjne (gdyż $b^2 = a$). Należy więc sprawdzić, czy $\forall\, x, y \in X : (xb)y = x(by)$. Próbujemy kolejno: $(x, y) = (a, a)$, (a, b), (b, a), (b, b). Odpowiedź jest negatywna, gdyż $a = (bb)b \neq b(bb) = b$.
Analogicznie stwierdzamy, że działanie wyznaczone trzecią tabelką nie jest łączne (symetria!).
Działanie określone czwartą tabelką jest łączne, gdyż $b \in A$, co stwierdzamy sprawdzając równość $(xb)y = x(by)$ kolejno dla $(x, y) = (a, a)$, (a, b), (b, a), (b, b).

II) $(a\ b)$ Po przeliczeniu stwierdzamy, że wszystkie cztery działania określone tabelkami: $\begin{matrix} a & a \\ a & b \end{matrix}, \quad \begin{matrix} a & a \\ b & b \end{matrix}, \quad \begin{matrix} a & b \\ a & b \end{matrix}, \quad \begin{matrix} a & b \\ b & b \end{matrix}$ są łączne.

III) $(b\ a)$ Żadne z odpowiednich czterech działań nie jest łączne.

IV) $(b\ b)$ Łączne są działania o tabelkach $\begin{matrix} b & a \\ a & b \end{matrix}, \quad \begin{matrix} b & b \\ b & b \end{matrix}.$

Odpowiedź: 8. Tabelki: $\begin{matrix} a & a \\ a & a \end{matrix}, \quad \begin{matrix} a & b \\ b & a \end{matrix}, \quad \begin{matrix} a & a \\ a & b \end{matrix}, \quad \begin{matrix} a & a \\ b & b \end{matrix}, \quad \begin{matrix} a & b \\ a & b \end{matrix}, \quad \begin{matrix} a & b \\ b & b \end{matrix},$
$\begin{matrix} b & a \\ a & b \end{matrix}, \quad \begin{matrix} b & b \\ b & b \end{matrix}.$

2. Dowody są bezproblemowe – wykorzystujemy definicje.
Przykładowo:

Ad(1). Niech $X, Y, Z \in \mathcal{G}_1$.

1) Jeżeli $f : X \underset{\cdot}{\hookrightarrow} Y$, $g : Z \to X$ i $f \circ g : Z \underset{\cdot}{\longrightarrow} Y$, to $g : Z \underset{\cdot}{\longrightarrow} X$, gdyż

1°. dla $a, b \in Z$: $f(g(ab)) = f(g(a)) \cdot f(g(b)) = f(g(a) \cdot g(b))$, a więc $g(ab) = g(a) \cdot g(b)$.
2°. $f(g(e_Z)) = e_Y = f(e_X)$, a więc $g(e_Z) = e_X$.
2) Jeżeli $f : X \twoheadrightarrow Y$, $g : Y \to Z$ i $g \circ f : X \longrightarrow Z$, to $g : Y \longrightarrow Z$, gdyż
1°. dla $a, b \in Y$: $\exists)\, a', b' \in X : a = f(a'),\ b = f(b')$ i wówczas $g(ab) = g(f(a')f(b')) = g(f(a'))g(f(b')) = g(a)g(b)$.
2°. $g(e_Y) = g(f(e_X)) = e_Z$.

Ad (7). Niech $X \in \mathcal{G}_1$, $E \subset X$, $E' = \bigcup_{n=0}^{\infty} F_n$, gdzie $F_0 = E$, $F_{n+1} = F_n \cup \{e_X\} \cup \{xy \mid x, y \in F_n\}$.

Wówczas $E^- = E'$, ponieważ

1°. $E' \subsetneq X$, gdyż $e_X \in E'$ i dla $a, b \in E'$ $\exists\, n \in \mathbb{N} : a, b \in F_n$ $\quad \langle F_0 \subset F_1 \subset \ldots \rangle$, wystarczy więc indukcją na $n \in \mathbb{N}$ wykazać, że $a, b \in F_n \;\Rightarrow\; ab \in F_{n+1}$, co wynika wprost z definicji ciągu F.
2°. Jeżeli $E \subset A \subsetneq X$, to $E' \subset A$, gdyż $\forall\, n \in \mathbb{N} : F_n \subset A$ $\quad\langle$indukcja na $n\rangle$.
W ogólnym przypadku, gdy $X \in \mathcal{A}_\nu$, $\nu : \Omega \to \mathbb{N}$, to dla $E \subset X$:

$$E^- = \bigcup_{n=0}^{\infty} F_n, \quad \text{gdzie}$$

$$F_0 = E, \qquad F_{n+1} = F_n \cup \{\omega_X(a_1, \ldots, a_k) \mid \omega \in \Omega,\ k = \nu(\omega),\ (a_1, \ldots, a_k) \in F_n^k\}.$$

3*. Należy wykazać, że dla $A \subset E : A^- = \langle A \rangle$.
$\subset$) Dla $b \in A^-$ istnieją $a_1, \ldots, a_n \in A$ takie, że $b \in \{a_1, \ldots, a_n\}^-$; wówczas dla $\omega = (n, a, b) : b = \omega_X(a_1, \ldots, a_n) \in \langle A \rangle$.
$\supset$) Jeżeli $b \in \langle A \rangle = \bigcup_{k \in \mathbb{N}} F_k$, gdzie $F_0 = A$,

$$F_{k+1} = F_k \cup \{\omega_X(a_1, \ldots, a_n) \mid \omega \in \Omega,\ \nu(\omega) = n;\ a_1, \ldots, a_n \in F_k\},$$

to $\exists\, k \in \mathbb{N} : b \in F_k$. Wystarczy więc wykazać indukcją na $k \in \mathbb{N}$, że $F_k \subset A^-$. $F_0 = A \subset A^-$.

$\langle$HP: $F_k \subset A^-$, $F_{k+1} \not\subset A^-$. $\exists)\, b \in F_{k+1} \setminus A^-$, $b = \omega_X(a_1, \ldots, a_n)$, $\omega \in \Omega$, $\nu(\omega) = n$; $a_1, \ldots, a_n \in F_k$. Wówczas $\exists)\, a' = (a_1', \ldots, a_n') \in E^n$, $b' \in \{a_1', \ldots, a_n'\}^- : \omega = (n, a', b')$, i – na mocy definicji działania ω_X:

$$b = \omega_X(a_1, \ldots, a_n) = \begin{cases} b', & \text{gdy } a = a' \\ a_1, & \text{gdy } a \neq a'. \end{cases}$$

Jeśli $a = a'$, to $b = b' \in \{a_1, \ldots, a_n\}^- \subset F_k^- \subset A^-$ ↯.
Jeśli zaś $a \neq a'$, to $b = a_1 \in F_k \subset A^-$ ↯$\rangle$.

4. Dowody bezproblemowe. Przykładowo, dla grupoidów:

Ad (i). $1_Y \in \mathrm{Im}(F|A)$, gdyż $1_{X \times Y} = (1_X, 1_Y) \in F$ i $1_X \in A$, a więc $1_Y \in \{y \in Y \mid \exists\, x \in A : (x, y) \in F\} = \mathrm{Im}(F|A)$.

Jeżeli $y, z \in \mathrm{Im}(F|A)$, to $\exists)\, x, t \in A : (x, y), (t, z) \in F$; i wówczas $(xt, yz) \in F$, $xt \in A$, a więc $yz \in \mathrm{Im}(F|A)$.

Ad (ii).

$\Rightarrow$) $1_{X^2} = (1_X, 1_X) \in R \quad \langle$zwrotność $R\rangle$.
Jeżeli $(x, t), (y, z) \in R$, to $(xy, tz) \in R$.
$\Leftarrow$) Analogicznie.

5. Intuicyjnie jest to oczywiste, gdyż mając łączność możemy dowolnie rozstawiać nawiasy. Dowód ścisły indukcją na $m \in \mathbb{N}$ mógłby wyglądać następująco:

I) $m = 0$. Wówczas $b = \varnothing$, $\prod b = 1$, $a * b = a$.
II) Jeżeli $m \geqslant 1$ i równość zachodzi dla $m-1$, to $(\prod a)(\prod b) = (\prod a)((\prod(b|I_{m-1})) \cdot b_m) = ((\prod a)(\prod(b|I_{m-1})))b_m = \prod(a * (b|I_{m-1})) \cdot b_m = \prod(a * b)$.

6*.

(1) Równość ta wynika natychmiast z twierdzenia o redundancji dla operacji domknięcia $((A^- \cup B)^- = (A \cup B)^-)$.
(2) Dowód przeprowadzimy dla grupoidu $X \in \mathcal{G}_1$; dowód ogólny będzie analogiczny.
1°) $e = e_X \in F(X) \quad \langle$HP: $\exists)\, A \subset X : (A \cup \{e\})^- = X$, $A^- \neq X$. Ponieważ $A \cup \{e\} \subset A^-$, więc $X = (A \cup \{e\})^- \subset A^-$ ↯$\rangle$.
2°) $a, b \in F(X) \;\Rightarrow\; ab \in F(X)$.

$\langle$HP: $\exists)\, a, b \in F(X) : ab \notin F(X)$. $\exists)\, C \subset X : (C \cup \{ab\})^- = X$, $C^- \neq X$.
$(C \cup \{a\})^- \neq X \quad \langle$HP: $(C \cup \{a\})^- = X$. Wówczas $C^- = X$ ↯$\rangle$.
$(C \cup \{a, b\})^- \neq X \quad \langle$HP: $((C \cup \{a\}) \cup \{b\})^- = X$. Wówczas $(C \cup \{a\})^- = X$ ↯$\rangle$.
Ale $C \cup \{ab\} \subset (C \cup \{a, b\})^-$, skąd $X = (C \cup \{ab\})^- \subset (C \cup \{a, b\})^-$ ↯$\rangle$.

(3) Mechaniczne przeliczanie – izomorfizm „zachowuje wszystko".
(4) HP: $\exists)\, a \in X \setminus F(X)$. Wówczas według (1):

$$\mathcal{N} = \{Y \subset X \mid (Y \cup \{a\})^- = X,\ Y \neq X\} \neq \varnothing.$$

Według lematu Zorna $\exists)\, Y$ – element maksymalny w $\mathcal{N}$. Ponieważ $Y \subsetneq X$, więc $\exists)\, Z \subset X : Y \subsetneq Z \subsetneq X$. Zatem $Z \notin \mathcal{N}$, skąd $(Z \cup \{a\})^- \neq X$. Jednakże $X = (Y \cup \{a\})^- \subset (Z \cup \{a\})^-$ ↯.
(5)
1°) $F(X) \subset \bigcap \mathcal{M}$.

$\langle$HP: $\exists)\, a \in F(X) \setminus \bigcap \mathcal{M}$. $\exists)\, Y \in \mathcal{M} : a \notin Y$. $Y \subsetneq (Y \cup \{a\})^-$, a więc $(Y \cup \{a\})^- = X$, $Y = X$ ↯$\rangle$.

2°) $\bigcap \mathcal{M} \subset F(X)$.

$\langle$HP: $\exists)\, a \in \bigcap \mathcal{M} \setminus F(X)$. Według (1):

$$\mathcal{N} = \{Y \subset X \mid (Y \cup \{a\})^- = X,\ Y \neq X\} \neq \varnothing,$$

a więc znów według lematu Zorna $\exists)\, Y$ – element maksymalny w $\mathcal{N}$. $Y \in \mathcal{M} \quad \langle$HP: $\exists)\, Z \subset X : Y \subsetneq Z \subsetneq X$. Wówczas $Z \notin \mathcal{N}$, a więc $(Z \cup \{a\})^- \neq X$. Ale $X =$

$(Y \cup \{a\})^- \subset (Z \cup \{a\})^- \lightning\rangle$.
Zatem $\bigcap \mathcal{M} \subset Y$, czyli $a \in Y$, $Y = (Y \cup \{a\})^- = X \lightning\rangle$.

7*. Dana jest algebra skończenie generowana $X = \{a_1, \ldots, a_n\}^-$.

(1) Niech $Y \subsetneq X$.

$Y \in \mathcal{F} \overset{\text{df}}{\equiv} \{Z \subsetneq X \mid Y \subset Z\}$. Jeżeli $\mathcal{C}$ jest łańcuchem niepustym w $\mathcal{F}$, to $\bigcup \mathcal{C} \in \mathcal{F}$ $\langle$HP: $\bigcup \mathcal{C} = X$. Wówczas $\forall\, i \in I_n\ \exists\, Z \in \mathcal{C} : a_i \in Z$, a więc – ponieważ $\mathcal{C}$ jest łańcuchem – $\exists)\, Z \in \mathcal{C} : a_1, \ldots, a_n \in Z$, skąd $X = \{a_1, \ldots, a_n\}^- \subset Z \subsetneq X \lightning\rangle$. Zatem, na mocy lematu Zorna, istnieje w $\mathcal{F}$ element maksymalny.

(2) $\langle$HP: $\exists)\, B \subset X : B^- = X \ \wedge\ \forall\, C \subset B\ (C^- = X \ \Rightarrow\ |C| \geqslant \omega)$. Wówczas $\beta = |B| \geqslant \omega$. Można przyjąć, że liczba β jest możliwie najmniejsza; $\forall\, D \subset X\ [(|D| < \beta \ \wedge\ D^- = X) \ \Rightarrow\ \exists\, C \subset D\ (C^- = X \ \wedge\ |C| < \omega)]$. $\exists)\, b : \beta \hookrightarrow\!\!\!\!\rightarrow B$. Dla $\eta < \beta$ oznaczmy $H_\eta = \{b_\xi \mid \xi < \eta\}$; wówczas $|H_\eta| < \beta$ i $\bigcup\limits_{\eta<\beta} H_\eta = B$. Zatem $\forall\, \eta < \beta : H_\eta^- \neq X$.
$\exists)\, j \in I_n\ \forall\, \eta < \beta : a_j \notin H_\eta^-$ $\langle$HP: $\forall\, i \in I_n\ \exists\, \eta_i < \beta : a_i \in H_{\eta_i}^-$; wówczas dla $\eta = \max\{\eta_1, \ldots, \eta_n\} : \{a_1, \ldots, a_n\} \subset H_\eta^-$, a więc $H_\eta^- = X \lightning\rangle$. Zatem $a_j \notin \bigcup\limits_{\eta<\beta} H_\eta^-$; $B \subset \bigcup\limits_{\eta<\beta} H_\eta^-$, $X = B^- \subset \bigcup\limits_{\eta<\beta} H_\eta^-$ $\langle$gdyż suma niepustego łańcucha podalgebr jest podalgebrą$\rangle$. Tak więc $X = \bigcup\limits_{\eta<\beta} H_\eta^-$, $a_j \in \bigcup\limits_{\eta<\beta} H_\eta^- \lightning\rangle$.

8. Dowód nie różni się w sposób istotny od dowodu ostatniego zadania z rozdziału 8 (8.22).

9*.

(i) Dla grupoidu $(\mathbb{N}, \hat{}\,)$, $a\hat{}\,b = a^b$

$$(2\hat{}\,2)\hat{}\,3 = (2^2)^3 = 2^6 \neq 2\hat{}\,(2\hat{}\,3) = 2^8.$$

Podobnie, jak łatwo sprawdzić, pięć różnych rozstawień nawiasów w wyrażeniu $2\hat{}\,2\hat{}\,3\hat{}\,3$ daje pięć różnych wyników: 2^{18}, 2^{24}, 2^{54}, 2^{64}, 2^{256}.

(ii) Kategoria $\mathcal{G}$ grupoidów to kategoria A_ν algebr o sygnaturze $\nu = \{\omega \mapsto 2\}$.

Niech $V = \{v\}$ będzie jednoelementowym zbiorem „zmiennych formalnych”. Wówczas α_n jest liczbą termów o sygnaturze ν nad zbiorom V, w których zmienna v ma dokładnie n wystąpień.

Przypomnijmy: $T = \mathrm{Term}_\nu(V) = \bigcup\limits_{n\in\mathbb{N}} F_n$,

$$F_0 = V = \{v\}, \quad F_{n+1} = F_n \cup \{\omega ts \mid t, s \in F_n\}.$$

Tak więc

$$\begin{aligned} &F_0 = \{v\} \\ &F_1 = F_0 \cup \{\omega vv\} \\ &F_2 = F_1 \cup \{\omega v\omega vv, \omega\omega vvv, \omega\omega vv\omega vv\} \\ &\ldots\quad . \end{aligned}$$

Formalnie $\alpha_n = |A_n|$, gdzie

$$A_n = \{t \in T \mid |\{k \in \mathbb{N}^* \mid t(k) = v\}| = n\}.$$

Tak więc

$$A_1 = \{v\},\ A_2 = \{\omega vv\},\ A_3 = \{\omega v\omega vv, \omega\omega vvv\},$$
$$A_4 = \{\omega v\omega v\omega vv, \omega v\omega\omega vvv, \omega\omega v\omega vvv, \omega\omega\omega vvvv\},\ \ldots$$

Zauważmy, że $n \geqslant 2 \ \Rightarrow\ A_n = \bigcup_{k=1}^{n-1}\{\omega ts \mid t \in A_k, s \in A_{n-k}\}$. Zatem $\alpha_1 = 1$, $n \geqslant 2 \ \Rightarrow\ \alpha_n = \sum_{k=1}^{n-1} \alpha_k\alpha_{n-k}$.

$$\alpha_5 = \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_3\alpha_2 + \alpha_4\alpha_1 = 2(1\cdot 5 + 2\cdot 1) = 14$$
$$\alpha_6 = \alpha_1\alpha_5 + \alpha_2\alpha_4 + \alpha_3\alpha_3 + \alpha_4\alpha_2 + \alpha_5\alpha_1 = 2(14+5) + 4 = 42$$
$$\alpha_7 = \alpha_1\alpha_6 + \alpha_2\alpha_5 + \alpha_3\alpha_4 + \alpha_4\alpha_3 + \alpha_5\alpha_2 + \alpha_6\alpha_1 = 2(42+14+10) = 132.$$

Jeżeli zauważymy, że kolejne wyrazy ciągu $(n-1)\alpha_n$, dla $n = 2, 3, \ldots$, to $1 = \binom{2}{0}$, $4 = \binom{4}{1}$, $15 = \binom{6}{2}$, $56 = \binom{8}{3}$, $210 = \binom{10}{4}$, $792 = \binom{12}{5}$, to otrzymamy wzór jawny:

$$n \geqslant 2 \ \Rightarrow\ \alpha_n = \frac{1}{n-1}\binom{2n-2}{n-2}.$$

Ścisły dowód tego wzoru – dosyć wyrafinowany – znajdziemy np. w: The Otto Dunkel Memorial Problem Book, New York 1957, zadanie 155. Liczby α_n są znane w kombinatoryce jako *liczby Catalana*.

10. $\exists)\, \tau : \mathcal{P}G \setminus \{\varnothing\} \to G$ – funkcja wyboru. Wówczas funkcja $f = \{(A,B) \mapsto \tau(A)\tau(B)K \mid A \in G/H,\ B \in H/K\}$ jest bijekcją, $f : (G/H) \times (H/K) \hookrightarrow\!\!\!\!\rightarrow G/K$, co sprawdzamy mechanicznym rachunkiem.

11.

(i) Jeśli $a = 1$, to $\langle a\rangle = \{1\} = \{1^0\}$, $r = 1$.

Załóżmy, że $a \neq 1$ i niech $H = \{1, a, \ldots, a^{r-1}\}$.
Wówczas $a \in H < G \quad \langle k < r \ \Rightarrow\ (a^k)^{-1} = a^{r-k}\rangle$ oraz $a \in K < G \ \Rightarrow\ H \subset G$, a więc $\langle a\rangle = H$.
$\operatorname{rk} a = |H| = r$, gdyż $k < l < r \ \Rightarrow\ a^k \neq a^l \quad \langle$HP: $a^k = a^l$. $a^{l-k}a^k = a^l$, $a^{l-k} = a^l(a^k)^{-1} = a^l(a^l)^{-1} = 1$, $r \leqslant l-k < r$ ↯$\rangle$.

(ii) HP: $\exists)\, a \in G\ \forall\, b \in G : a \neq b^2$. Niech $r = \operatorname{rk} a$. Na mocy twierdzenia Lagrange'a $r|2n+1$, a więc $a^{2n+1} = 1$, $a^{2n+2} = (a^{n+1})^2 = a$ ↯.

(iii) Według twierdzenia Cauchy'ego istnieje w grupie G podgrupa $\{1, a\}$ rzędu 2, i wówczas $a \in G \setminus \{1\}$. $a^2 = 1$.

(iv) $a, b \in G \ \Rightarrow\ (ab)^2 = abab = 1$, a więc $bab = a$, $ab = ba$.

Jako przykład takiej grupy może służyć grupa addytywna dowolnego pierścienia Boole'a, np. $(\mathcal{P}X, \dot{-})$ dla $X \in \mathbb{V}$.

Załóżmy, że $\forall\, a \in G : a^2 = 1$.
HP: $\operatorname{rk} G = 2n+1$, $n \in \mathbb{N}^*$. $\exists)\, a \in G \setminus \{1\}$. Na mocy (ii) $\exists\, b \in G : a = b^2 = 1$ ↯.

12. Niech $a \in G$. $\exists)\, b \in G : ba = e$. $\exists)\, c \in G : cb = e$. Dla $d = ae$ mamy $bd = bae = e^2 = e$, a więc $d = ed = cbd = ce = cba = ea = a$, czyli $ae = a$.
Zatem e jest elementem neutralnym (jedynką) w G oraz $c = ce = cba = ea = a$, czyli $ab = e$, $b = a^{-1}$.

13. Mechaniczne rachunki. Na przykład:
ad (ii): $\forall\, a, b, x \in G : \sigma_{ab}(x) = abx(ab)^{-1} = abxb^{-1}a^{-1} = \sigma_a(\sigma_b(x))$, a więc $\sigma_{ab} = \sigma_a \circ \sigma_b$.

14. Dowody są bezproblemowe. Wykażemy np. (iv).
Schemat jest typowy.

(I) Jednoznaczność:

Przypuśćmy, że taki homomorfizm $g : \widehat{G} \xrightarrow{\cdot} H$ już mamy. Wówczas dla $a \in G$, $b \in \mathcal{R}(G)$: $g(\frac{a}{b}) = g(\iota(a) \cdot \iota(b)^{-1}) = g(\iota(a)) \cdot g(\iota(b)^{-1}) = g(\iota(a)) \cdot g(\iota(b))^{-1} = f(a) \cdot f(b)^{-1}$.

(II) Istnienie:

Określamy odwzorowanie $g : \widehat{G} \to H$ jak w (I); określenie jest poprawne, tzn. nie zależy od wyboru reprezentanta (a, b) ułamka $\frac{a}{b}$.
Istotnie, jeżeli $\frac{a}{b} = \frac{a'}{b'}$, gdzie $a, a' \in G$ i $b, b' \in \mathcal{R}(G)$, to $ab' = a'b$. $f(a)f(b') = f(a')f(b)$, a więc $f(a)f(b)^{-1} = f(a')f(b')^{-1}$.

Mechanicznym rachunkiem sprawdzamy, że g jest homomorfizmem $\widehat{G}$ w H oraz $f = g \circ \iota$.

15.

(i) Natychmiast widać, że dla $n \in \mathbb{N} : n\mathbb{Z} < \mathbb{Z}$, przy czym $0 \cdot \mathbb{Z} = \{0\}$, $1 \cdot \mathbb{Z} = \mathbb{Z}$.

Niech teraz $H < \mathbb{Z}$, $H \neq \{0\}$, $H \neq \mathbb{Z}$. Weźmy najmniejsze $n \in \mathbb{N}_2 = \{2, 3, \dots\}$ takie, że $n \in H \quad \langle k \in H \;\Rightarrow\; -k \in H \rangle$. $n\mathbb{Z} \subset H$. Dla dowolnego $a \in H$, $\exists!\, q, r \in \mathbb{Z}$: $a = nq + r$, $0 \leqslant r < n$, i ponieważ $nq \in H$, więc $r \in H$, $r = 0$, $a = nq \in n\mathbb{Z}$. Zatem $H \subset n\mathbb{Z}$, czyli $H = nZ$.

(ii) Niech $k \in \{1, \dots, m-1\}$, $k \perp m$. Wówczas $\exists)\, \alpha, \beta \in \mathbb{Z} : \alpha k + \beta m = 1$. Jeżeli $a \in \{1, \dots, m-1\}$, to $a = a\alpha k + a\beta m$. Przechodząc przez surjekcję naturalną do $\mathbb{Z}_m$ otrzymujemy: $a = [a\alpha]k$ ($[a\alpha] \in \{1, \dots, m-1\}$).

(iii) Określamy $f : Z_{mn} \to Z_m \times Z_n$, kładąc dla $x \in \mathbb{Z}_{mn}$:

$$f(x) = (x \pmod{m}, x \pmod{n}).$$

Łatwo sprawdzić, że f jest izomorfizmem.

16. $f : G \hookrightarrow\!\!\!\!\twoheadrightarrow G$, $f^{-1}(x) = xa$.
Działanie $*$ otrzymujemy przez transport struktury z grupy G; $\forall\, x, y \in G$:

$$x * y = f(f^{-1}(x) f^{-1}(y)) = xayaa^{-1} = xay,$$

elementem neutralnym grupy G jest $f(1_G) = a^{-1}$.

17. Przypuśćmy, że n-elementowy ($n \in \mathbb{N}^*$) zbiór $E = \{\frac{k_1}{m_1}, \dots, \frac{k_n}{m_n}\}$ ($k_i \in \mathbb{Z}, m_i \in \mathbb{N}^*$) generuje grupę $\mathbb{Q}$, czyli $\langle E \rangle = \{\alpha_1 \frac{k_1}{m_1} + \ldots + \alpha_n \frac{k_n}{m_n} \mid \alpha_1, \dots, \alpha_n \in \mathbb{Z}\} = \mathbb{Q} \quad \langle \dots \rangle$.
Weźmy liczbę pierwszą p niebędącą dzielnikiem żadnej z liczb $m_1, \dots, m_n$.
Wówczas $\exists)\, \alpha_1, \dots, \alpha_n \in \mathbb{Z} : \frac{1}{p} = \alpha_1 \frac{k_1}{m_1} + \ldots + \alpha_n \frac{k_n}{m_n}$, a więc

$$m_1 \ldots m_n = p\left(\alpha_1 \frac{k_1 m_1 \ldots m_n}{m_1} + \ldots + \alpha_n \frac{k_n m_1 \ldots m_n}{m_n}\right),$$

czyli $p | m_1 \ldots m_n$, $\exists\, i \in I_n : p | m_i$ ↯.

18*.

(i) Przypuśćmy, że G jest maksymalną podgrupą właściwą grupy $\mathbb{Q}$.
$0 \in G$. $\forall\, a, b \in G; \alpha, \beta \in \mathbb{Z} : \alpha a + \beta b \in G$.
$\exists)\, k \in \mathbb{Z}^*, n \in \mathbb{N}^* : \frac{k}{n} \in \mathbb{Q} \setminus G,\ k \perp n$.
$G \neq \{0\} \quad \langle \{0\} < \mathbb{Z} < G \rangle$.
$\exists)\, m \in \mathbb{N}^* \setminus G \quad \langle \exists)\, r \in \mathbb{Z}^*, s \in \mathbb{N}^* : \frac{r}{s} \in G$. Wówczas $r = s \cdot \frac{r}{s} \in G, r \in G \Leftrightarrow -r \in G \rangle$.
$H := \{\frac{x}{nm} \mid x \in G\} < \mathbb{Q} \quad \langle \dots \rangle$.
$G \subset H \quad \langle \forall\, x \in G : x = nm \cdot \frac{x}{nm} \in H \rangle$.
$G \neq H \quad \langle$HP: $G = H$. Wówczas $\frac{1}{n} = m \cdot \frac{1}{nm} \in H$, czyli $\frac{1}{n} \in G$, $\frac{k}{n} = k \cdot \frac{1}{n} \in G$ ↯$\rangle$.
Zatem $H = \mathbb{Q}$.
$\exists)\, x \in G : \frac{1}{n^2 m^2} = \frac{x}{nm}$, $\frac{1}{nm} \in G$, $\frac{k}{n} = km \frac{1}{nm} \in G$ ↯.
(ii) Przypuśćmy, że A jest minimalnym zbiorem generującym $\mathbb{Q}$.
$\exists)\, a \in A$. Dla $B = A \setminus \{a\}$, $\langle B \rangle \neq \mathbb{Q} \quad \langle$z minimalności $A\rangle$.
Z (i) wynika, że $\mathbb{Q} = F(\mathbb{Q})$ = podgrupa Frattiniego grupy $\mathbb{Q}$ (zadanie 6*), a więc, ponieważ $\langle B \cup \{a\} \rangle = \langle A \rangle = \mathbb{Q}$, to $\langle B \rangle = \mathbb{Q}$ ↯.

Komentarz: Nieznaczna modyfikacja powyższego dowodu daje twierdzenie: Zbiór generujący grupę addytywną $\mathbb{Q}$ po usunięciu podzbioru skończonego jest dalej zbiorem generującym.

19. Zauważmy, że $2^5 \equiv 2 \pmod{10}$; w dalszym ciągu dopisek „mod 10” będziemy opuszczali. Również $2^9 \equiv 2$.
$p + 1 = 2^{82\,589\,933} = 2^{9 \cdot 9\,176\,659 + 2} \equiv 2^{9\,176\,659} \cdot 4$,
$2^{9\,176\,659} = 2^{9 \cdot 1\,019\,628 + 7} \equiv 2^{1\,019\,628} \cdot 128$,
$2^{1\,019\,628} = 2^{9 \cdot 113\,292} \equiv 2^{113\,292} = 2^{9 \cdot 12\,588} \equiv 2^{12\,588} = 2^{5 \cdot 2517 + 3} \equiv 2^{2517} \cdot 8$,
$2^{2517} = 2^{9 \cdot 279 + 6} \equiv 2^{279} \cdot 64$,
$2^{279} = 2^{9 \cdot 31} \equiv 2^{31} = 2^{5 \cdot 6 + 1} \equiv 2^6 \cdot 2 = 128 \equiv 8$.
Zatem
$2^{2517} \equiv 8 \cdot 4 \equiv 2$, $2^{1\,019\,628} \equiv 2 \cdot 8 \equiv 6$, $2^{9\,176\,659} \equiv 6 \cdot 8 \equiv 8$, i ostatecznie $p + 1 \equiv 8 \cdot 4 \equiv 2$, a więc $p \equiv 1 \pmod{10}$.

20. $\exists)\, x : \mathbb{N} \hookrightarrow\!\!\!\!\twoheadrightarrow X, y : \mathbb{N} \hookrightarrow\!\!\!\!\twoheadrightarrow Y$,.
Izomorfizm $f = \{(x_{\alpha_0}, y_{\alpha_0}), (x_{\alpha_1}, y_{\alpha_1}), \dots\} : X \xrightarrow{\sim} Y$ otrzymamy, definiując indukcyjnie ciągi $\alpha, \beta : \mathbb{N} \to \mathbb{N}$. $\alpha_0 = \beta_0 = 0$. Dla $n > 0$ kładziemy na przemian:

1) Dla n nieparzystego: $\alpha_n = \min(\mathbb{N} \setminus \{\alpha_0, \dots, \alpha_{n-1}\})$,
$\beta_n = \min\{k \in \mathbb{N} \setminus \{\beta_0, \dots, \beta_{n-1}\} \mid \forall\, i < n\ (y_{\beta_i} < y_{\beta_k} \Leftrightarrow x_{\alpha_i} < x_{\alpha_n})\}$.

2) Dla n parzystego: $\beta_n = \min(\mathbb{N} \setminus \{\beta_0, \dots, \beta_{n-1}\})$,
$\alpha_n = \min\{k \in \mathbb{N} \setminus \{\alpha_0, \dots, \alpha_{n-1}\} \mid \forall\, i < n\ (x_{\alpha_i} < x_{\alpha_k} \Leftrightarrow y_{\beta_i} < y_{\beta_n})\}$.

21. HP: $\neg \dots$. Istnieją więc elementy $a, x \in G$, $a > 0$ takie, że $\forall\, n \in \mathbb{N} : na < x$. Rozważmy zbiór $A = \{na \mid n \in \mathbb{N}\}$. $A \neq \varnothing$ $\quad\langle a \in A\rangle$, $M(A) \neq \varnothing$ $\quad\langle x \in M(A)\rangle$, a więc z ciągłości G wynika, że $s = \sup A \in G$. Teraz $s \in M(A)$, czyli $\forall\, n \in \mathbb{N} : na \leqslant s$, a więc $\forall\, n \in \mathbb{N} : (n+1)a \leqslant s$, $na \leqslant s - a$. Zatem $s - a \in M(A)$, $s \leqslant s - a$, $a \leqslant 0$ ↯.

22. Przypuśćmy, że dla $A = \{a \in \mathbb{Q} \mid 0 < a,\ a^2 < 2\}$, $s = \sup A \in \mathbb{Q}$, $s^2 \neq 2$ $\langle \exists\, p, q \in \mathbb{N}^* : p \perp q,\ s = \frac{p}{q}$. HP: $s^2 = 2$, $p^2 = 2q^2$, $2|p^2$, $2|p$, $4|2q^2$, $2|q^2$, $2|q$, $p \not\perp q$ ↯$\rangle$. Możliwe są dwa przypadki:

1) $s^2 < 2$. Wówczas dla dostatecznie dużych n naturalnych: $(s + \frac{1}{n})^2 < 2$ $\quad\langle 2 < (s + \frac{1}{n})^2 = s^2 + \frac{2s}{n} + \frac{1}{n^2} \leqslant s^2 + \frac{2s+1}{n} \Leftrightarrow 2 - s^2 \leqslant \frac{2s+1}{n} \Leftrightarrow n \leqslant \frac{2s+1}{2-s^2}$. Zatem, jeżeli $n > \frac{2s+1}{2-s^2}$ $\quad\langle$archimedesowość $\mathbb{Q}$!$\rangle$, to $(s + \frac{1}{n})^2 < 2\rangle$ ↯.

2) $2 < s^2$. Wówczas dla dostatecznie dużych n: $2 < (s - \frac{1}{n})^2$ $\quad\langle s - \frac{1}{n} \notin M(A)$. $\exists)\, a \in A : s - \frac{1}{n} < a$; $2 > a^2 > (s - \frac{1}{n})^2 = s^2 - \frac{2s}{n} + \frac{1}{n^2} > s^2 - \frac{2s}{n}$, a więc $n < \frac{2s}{s^2-2}$. Zatem, jeżeli $n > \frac{2s}{s^2-2}$, to $(s - \frac{1}{n})^2 > 2\rangle$, czyli $s - \frac{1}{n} \in M(A)$ ↯.

23. Udowodnienie prawdziwości tych faktów nie sprawia większych trudności, ale jest dosyć żmudne. Łatwo widać, że dla niepustego i ograniczonego od góry zbioru $A \subset \mathbb{R}$: $\sup A = \bigcup A$.

Nieco trudniejsze momenty to:

1°) wskazanie elementu przeciwnego do liczby $\alpha \in \mathbb{R}$;

$$-\alpha = \{x \in \mathbb{Q} \mid \exists\, y \in \mathbb{Q} \setminus \alpha : x < -y\},$$

2°) wskazanie elementu odwrotnego do liczby $\alpha \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$;
jeżeli $\alpha > 0$, to $\alpha^{-1} = \{x \in \mathbb{Q} \mid \exists\, y \in \mathbb{Q} \setminus \alpha : x < y^{-1}\}$, dla $\alpha < 0$: $\alpha^{-1} = -(-\alpha)^{-1}$.

24. Jednoznaczność wynika z prawa:
$0 < b < c \ \Rightarrow\ b^n < c^n$ $\quad\langle$indukcja na $n = 1, 2, \dots\rangle$.
W dowodzie istnienia wystarczy ograniczyć się do przypadku, gdy $a > 1$ $\quad\langle$dla $0 < a < 1$: $\sqrt[n]{a} = 1/\sqrt[n]{1/a}\rangle$.
Bierzemy wówczas $b = \sup X$, gdzie $X = \{x \in \mathbb{R} \mid x^n < a\}$; $b \in \mathbb{R}$ $\quad\langle \dots \rangle$. $b^n = a$ $\langle$HP: $b^n \neq a$. Dwa przypadki.

1. $b^n < a$. Wówczas $b = \max X$. $\forall\, m \in \mathbb{N}^* : b + \frac{1}{m} \notin X$, a więc $a \leqslant (b + \frac{1}{m})^n = b^n + \sum\limits_{k=1}^{n} \binom{n}{k} b^{n-k} \cdot \frac{1}{m^k} \leqslant b^n + \frac{1}{m} \sum\limits_{k=1}^{n} b^{n-k} < a$, jeżeli $\sum\limits_{k=1}^{n} b^{n-k} < a - b^n$ ↯.

2. $a < b^n$. Wówczas $b \notin X$, $b = \min M(X)$, $1 < b$, $\forall\, m \in \mathbb{N}^* \exists\, x \in X : b - \frac{1}{m} < x$, $(b - \frac{1}{m})^n < x^n < a$. Dla oszacowania od dołu potęgi $(b - \frac{1}{m})^n$ można np. skorzystać z *nierówności Bernoullego*:

$$\forall\, x \geqslant -1,\ n \in \mathbb{N} : (1+x)^n \geqslant 1 + nx \qquad \langle \text{Indukcja na } n\rangle.$$

Tak więc $(b - \frac{1}{m})^n = b^n(1 - \frac{1}{bm})^n \geqslant b^n(1 - \frac{n}{bm}) = b^n - \frac{nb^{n-1}}{m}$.

Jeżeli $m \in \mathbb{N}^*$ i $\frac{nb^{n-1}}{m} < b^n - a$, to $(b - \frac{1}{m})^n > a$ ↯.

25.

(i) $x = 1\,x \in Gx$, a więc $Gx \neq \varnothing \quad \wedge \quad \bigcup\limits_{x \in X} Gx = X$.

Ponadto dla $x, y \in X : y \in Gx \ \Rightarrow\ Gx = Gy \quad \langle (\exists)\, \alpha \in G : y = \alpha x$. Zatem $Gy \subset Gx$, i ponieważ $x = \alpha^{-1}y$, więc także $Gx \subset Gy\rangle$, a więc orbity są parami rozłączne.

(ii) $1\,x = x$, a więc $1 = 1_G \in S_x$.

Jeżeli $\alpha, \beta \in S_x$, czyli $\alpha x = \beta x = x$, to $\alpha\beta \in S_x \quad \langle \alpha\beta x = \alpha x = x\rangle$ oraz $\alpha^{-1} \in S_x$ $\langle \alpha^{-1}x = \alpha^{-1}\alpha x = 1\,x = x\rangle$.

(iii) Jeśli $\xi \in S_x$, to $\xi x = x$, $\sigma_\alpha(\xi)y = \alpha\xi\alpha^{-1}y = \alpha\xi x = \alpha x = y$, a więc $\sigma_\alpha(\xi) \in S_y$, czyli $\sigma_\alpha(S_x) \subset S_y$. Analogicznie $x = \alpha^{-1}y$, $\sigma_{\alpha^{-1}}(S_y) \subset S_x$, a więc $\sigma_\alpha(\sigma_{\alpha^{-1}}(S_y)) \subset \sigma_\alpha(S_x)$.
Jednak $\sigma_\alpha \circ \sigma_{\alpha^{-1}} = \mathrm{id}_G$, zatem $S_y \subset \sigma_\alpha(S_x)$.

(iv) Wystarczy wykazać, że dla $\alpha, \beta \in G$:

$$\alpha x = \beta x \iff \alpha S_x = \beta S_x.$$

$\Rightarrow$) Wykażemy np. że $\alpha S_x \subset \beta S_x$. Niech $\xi \in S_x$. Wówczas $\xi x = x$. $\beta^{-1}\alpha\xi x = \beta^{-1}\alpha x = \beta^{-1}\beta x = x$, a więc $\beta^{-1}\alpha\xi \in S_x$, $\alpha\xi \in \beta S_x$.
$\Leftarrow$) HP: $\alpha x \neq \beta x$. Wówczas $\beta^{-1}\alpha x \neq x$, $\beta^{-1}\alpha \notin S_x$. Jednakże $\alpha = \alpha\cdot 1 \in \alpha S_x = \beta S_x$, czyli $\exists)\, \gamma \in S_x : \alpha = \beta\gamma$, i wówczas $\beta^{-1}\alpha x = \beta^{-1}\beta\gamma x = \gamma x = x$ ↯.

(v) Zbiór X ścian sześcianu traktujemy jako G-przestrzeń (G = grupa izometrii własnych sześcianu). Dla $\varphi \in X$ orbita $G\varphi = X$, a więc $|G\varphi| = |X| = 6$.

Natomiast stabilizator $S_\varphi < G$ ściany $\varphi \in X$ jest rzędu 8 (cztery symetrie i cztery obroty). Zatem, dla $\varphi \in X : |G| = |G\varphi| \cdot |S_\varphi| = 6 \cdot 8 = 48$.

Oznaczając przez r_n ($n \in \mathbb{N}$) rząd grupy izometrii kostki $[0,1]^n$ będziemy mieli $r_n = 2^n\, n!$, gdyż jest tak dla $n \leqslant 3$. Jeżeli $n \geqslant 4$ i $r_{n-1} = 2^{n-1} \cdot (n-1)!$, to stosując formułę orbit i uwzględniając fakt, że kostka n-wymiarowa ma $2n$ ścian ($(n-1)$-wymiarowych), otrzymujemy: $r_n = 2n \cdot r_{n-1} = 2^n \cdot n!$.

26.

(i) $\Rightarrow$) HP: $\exists)\, n \in \mathbb{N}^*$, $a : I_n \hookrightarrow A$, $\alpha : I_n \to K$; $\sum\limits_{i=1}^{n} \alpha_i a_i = 0$, $\alpha_n \neq 0$. Wówczas $a_n = \sum\limits_{i=1}^{n-1} (-\alpha_i\alpha_n^{-1})a_i \in \langle A \setminus \{a_n\}\rangle$ ↯.
$\Leftarrow$) HP: $\exists)\, a \in A$, $a \in \langle A \setminus \{a\}\rangle$. Wówczas $\exists)\, n \in \mathbb{N}^*$, $b : I_n \hookrightarrow A \setminus \{a\}$, $\beta : I_n \to K$;

$$a = \sum_{i=1}^{n} \beta_i b_i, \quad (-1)a + \sum_{i=1}^{n} \beta_i b_i = 0 \quad ↯.$$

(ii) Dla podzbioru liniowo niezależnego $A \subset X$ niech $\mathcal{B} = \{B \mid A \subset B \subset X \ \wedge\ B$ – liniowo niezależny$\}$. $\mathcal{B} \neq \varnothing$, gdyż $A \in \mathcal{B}$.

Jeżeli $\varnothing \neq \mathcal{C} \subset \mathcal{B}$ i $\mathcal{C}$ jest łańcuchem, to $\bigcup\mathcal{C} \in \mathcal{B}$, gdyż $A \subset \bigcup\mathcal{C}$ i zbiór $\bigcup\mathcal{C}$ jest liniowo niezależny $\quad\langle$HP: $\exists)\, n \in \mathbb{N}$, $a : I_n \hookrightarrow \bigcup\mathcal{C}$, $\alpha : I_n \to K$; $\sum\limits_{i=1}^{n} \alpha_i a_i = 0$,

$a_n \neq \varnothing$. $\exists)\, c \in \mathcal{C} : a : I_n \to C \quad \langle$gdyż $\mathcal{C}$ jest łańcuchem$\rangle$ ↯$\rangle$.
Zatem istnieje w $\mathcal{B}$ element maksymalny.
(iii) Niech $X \in \mathrm{Vect}_K$ i niech $A \subset X$ będzie maksymalnym liniowo niezależnym podzbiorem X. Wówczas $\langle A\rangle = X \quad \langle$z maksymalności A wynika, że $\forall\, x \in X \setminus A : x \in \langle A\rangle\rangle$.
(iv) Niech $Y \in \mathrm{Vect}_K$, $\varphi : A \to Y$, gdzie A jest podzbiorem liniowo niezależnym i generującym przestrzeni $X \in \mathrm{Vect}_K$. Wówczas dla każdego $x \in X$ istnieje dokładnie jedno odwzorowanie $\xi : A \to K$ takie, że $\{a \in A \mid \xi_a \neq 0\} \in \mathrm{Fin}$ i $x = \sum\limits_{a\in A} \xi_a \cdot a$; kładąc teraz dla takiego x:

$$f(x) = \sum_{a\in A} \xi_a \cdot \varphi(a) \quad \text{otrzymujemy rozszerzenie} \quad \varphi \subset f : X \xrightarrow{\cdot} Y.$$

27.

$\Rightarrow$) Podzbiór liniowo niezależny $A \subset X$ ma rozszerzenie do bazy $A \subset B \subset X$ przestrzeni X, i wówczas odwzorowanie $\varphi : A \to Y$, gdzie $Y \in \mathrm{Vect}_K$ ma rozszerzenie $\varphi \subset \varphi \cup \{x \mapsto 0 \mid x \in B \setminus A\} \subset f : X \xrightarrow{\cdot} Y$.
$\Leftarrow$) HP: $\exists)\, a \in A : a \in \langle A \setminus \{a\}\rangle$; wówczas odwzorowanie $\varphi = ((A \setminus \{a\}) \times \{0\}) \cup \{a \mapsto 1\} : A \to K$ $(K \in \mathrm{Vect}_K)$ nie ma rozszerzenia liniowego $\varphi \subset f : X \xrightarrow{\cdot} K$ $\langle f(a) = 0 \neq 1 = \varphi(a)\rangle$ ↯.

28*.

(i) Załóżmy, że funkcja $f : \mathbb{R} \to \mathbb{R}$ spełnia równanie $(*)$. Łatwo widać, że

$$\forall\, x \in \mathbb{Q} : f(x) = cx, \quad \text{gdzie } c = f(1).$$

Załóżmy, że funkcja f spełnia dodatkowo warunek ograniczoności od góry w pewnym przedziale (α, β); $\alpha < x < \beta \;\Rightarrow\; f(x) < M$.
HP: $\exists)\, x \in \mathbb{R} : f(x) \neq cx$.

Możliwe są dwa przypadki

1) $f(x) > cx$
Wówczas dla $n \in \mathbb{N}^*$ iloczyn $n[f(x) - cx]$ może przyjmować dowolnie duże wartości; jednak $\exists)\, w \in \mathbb{Q} : nx - w \in (\alpha, \beta) \quad \langle \ldots nx - \beta < w < nx - \alpha\rangle$ i dla takiego w: $n[f(x)-cx] = f(nx)-cw+cw-ncx = f(nx-w)-c(nx-w) < M+|c|\cdot\max(|\alpha|, |\beta|)$ ↯.
2) $f(x) < cx$
Analogicznie dla $n \in \mathbb{N}^*$ iloczyn $n[cx - f(x)]$ może być dowolnie duży;
$\exists)\, w \in \mathbb{Q} : w - nx \in (\alpha, \beta) \quad \langle \ldots \alpha + nx < w < \beta + nx\rangle$ $n[cx - f(x)] = ncx - cw + cw - f(nx) = c(nx - w) - f(w - nx) < M + |c| \cdot \max(|\alpha|, |\beta|)$ ↯.

(ii) Zakładamy tylko, że funkcja $f : \mathbb{R} \to \mathbb{R}$ spełnia równanie $(*)$.

Ciało $\mathbb{R}$ można traktować jako przestrzeń wektorową nad $\mathbb{Q}$; $\mathbb{R} \in \mathrm{Vect}_{\mathbb{Q}}$.
Istnieje więc baza $B \subset \mathbb{R}$ przestrzeni $\mathbb{R}$ w kategorii $\mathrm{Vect}_{\mathbb{Q}}$ (tzw. *baza Hamela*), i wówczas dla $x \in \mathbb{R} : \exists!)\, \gamma = \gamma^x : B \to \mathbb{Q}$, $x = \sum\limits_{b\in B} \gamma^x(b) \cdot b$, $\{b \in B \mid \gamma^x(b) \neq 0\} \in \mathrm{Fin}$.
Przy ustalonym $b \in B$ funkcja $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \gamma^x(b)$ (= współrzędna elementu x

stojąca przy wektorze b bazy Hamela B) jest takim nietypowym rozwiązanie równania $(*)$ $\langle$przyjmuje tylko wartości wymierne$\rangle$.

29. W przypadku ogólnym wziąć $x_i' = \frac{nx_i}{x_1+\ldots+x_n}$.

Dowód w przypadku gdy $x_1+\ldots+x_n = n$ prowadzimy indukcją na n. Dla $n=1$ twierdzenie jest oczywiste. Załóżmy, że $n \geqslant 2$ i teza zachodzi dla $n-1$. Wystarczy wykazać, że $(\exists\, i,j : x_i \neq x_j) \;\Rightarrow\; x_1 \ldots x_n < 1$. Wykorzystamy lemat:
$0 < x < 1 < y \implies x+y > xy+1$ $\quad\langle\; x+y-xy-1 = y(1-x)-(1-x) = (1-x)(y-1) > 0\rangle$.
Niech na przykład $x_{n-1} < 1 < x_n$. Wówczas $x_1+\ldots+(x_{n-1}+x_n) = n-1$, a więc $x_1 \ldots x_n < x_1 \ldots (x_{n-1}+x_n-1) \leqslant 1$ na mocy założenia indukcyjnego i lematu.

30. Po rozpisaniu:

$$W_n = \begin{vmatrix} 1 & 1 & & & & 0 \\ 1 & 1 & 1 & & & \\ & 1 & 1 & 1 & & \\ & & \ldots & \ldots & & \\ 0 & & & 1 & 1 & 1 \\ & & & & 1 & 1 \end{vmatrix}$$

$W_0 = W_1 = 1$, $W_2 = 0$.
Dla $n \geqslant 3$ rozwinięcie według pierwszego wiersza daje wzór rekurencyjny $W_n = W_{n-1} - W_{n-2}$.
Kolejne wyrazy naszego ciągu przedstawia tabelka

n	0	1	2	3	4	5	6	7	8	...
W_n	1	1	0	-1	-1	0	1	1	0	...

Tak więc $W_{3k} = W_{3k+1} = (-1)^k$; $W_{3k+2} = 0$ dla $k \in N$, czyli

$$W_n = \begin{cases} 0 & \text{gdy } n \equiv 2 \pmod 3 \\ (-1)^{\left[\frac{n}{3}\right]} & \text{w pozostałych przypadkach} \end{cases} \qquad \langle\text{Indukcja} \ldots\rangle.$$

W szczególności $a_{100} = (-1)^{33} = -1$.

31. Wystarczy wykazać, że $V_n = \prod\limits_{\substack{i,j=1\\ i<j}}^{n} (x_j - x_i)$.

Dodając do n-tego wiersza naszego wyznacznika wiersz $(n-1)$-y przemnożony przez $-x_1$, następnie do $(n-1)$-ego wiersza wiersz $(n-2)$-i przemnożony przez $-x_1$ itd. otrzymamy wyznacznik, który po rozwinięciu względem pierwszej kolumny daje formułę rekurencyjną:

$$V(x) = (x_2 - x_1)\ldots(x_n - x_1)V(x_2, \ldots, x_n),$$

dla $n \geqslant 2$, i dalej prostą indukcją uzyskujemy żądaną równość.

32. Wyznacznik macierzy współczynników $= (\lambda-1)^3(\lambda+3)$.
Jeżeli $\lambda \neq 1$ i $\lambda \neq -3$, to układ ma dokładnie jedno rozwiązanie:

$$(x,y,z,t) = \frac{1}{\lambda+3}(-\lambda^2-2\lambda-2,\ -\lambda^2-\lambda+1,\ 2\lambda+1,\ \lambda^3+3\lambda^2+2\lambda+1).$$

Dla $\lambda = 1$ układ ma nieskończenie wiele rozwiązań postaci

$$x = 1 - y - z - t; \qquad y, z, t \in \mathbb{R}.$$

Dla $\lambda = -3$ układ nie ma rozwiązania $\langle$rząd macierzy współczynników $< 4 =$ rząd macierzy uzupełnionej$\rangle$.

33. Dla $m \leqslant 1$ teza jest oczywista $\langle$wektor $a \in X$ jest liniowo niezależny wtt, gdy $a \neq 0\rangle$.

Załóżmy, że $m \geqslant 2$ i lemat jest prawdziwy dla $m - 1$.

Wówczas $m - 1 \leqslant n$ i można wymienić $m - 1$ wektorów spośród $v_1, \ldots, v_n$, na przykład wektory $v_1, \ldots, v_{m-1}$, na wektory $e_1, \ldots, e_{m-1}$ tak, aby nowy układ $(e_1, \ldots, e_{m-1}, v_m, \ldots, v_n)$ był też generujący. Wówczas

$$e_m = \alpha_1 e_1 + \ldots + \alpha_{m-1} e_{m-1} + \alpha_m v_m + \ldots + \alpha_n v_n,$$

dla pewnych skalarów $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$. Któryś ze skalarów $\alpha_m, \ldots, \alpha_n$ jest niezerowy, na przykład $\alpha_m \neq 0$ $\langle$bo inaczej układ $e_1, \ldots, e_m$ byłby liniowo zależny$\rangle$, i wówczas $v_m \in \langle e_1, \ldots, e_{m-1}, e_m, v_{m+1}, \ldots, v_n\rangle$, a więc układ $(e_1, \ldots, e_m, v_{m+1}, \ldots, v_n)$ jest generujący.

34. Po przesunięciu niewiadomej: $x = y + \alpha$, $\alpha = \frac{1}{3}$, otrzymujemy równanie:

$$y^3 - \frac{4}{3}y - \frac{38}{27} = 0.$$

Podstawienie $y = z + \frac{\beta}{z}$, $\beta = \frac{4}{9}$ prowadzi do równania:

$$z^3 + \frac{64}{729z^3} - \frac{38}{27} = 0,$$

które po podstawieniu $t = z^3$ daje równanie kwadratowe

$$729t^2 - 1026t + 64 = 0.$$

Równanie to ma dwa pierwiastki rzeczywiste:

$$t_{1,2} = \frac{19 \pm 3\sqrt{33}}{27}.$$

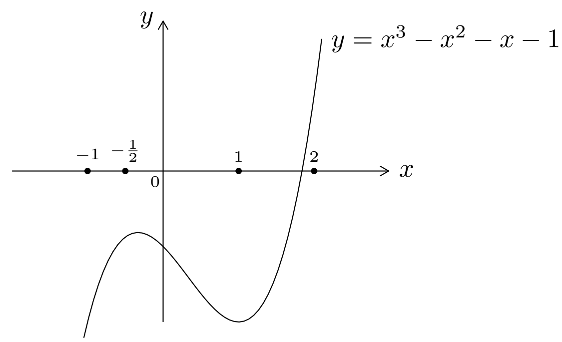
Biorąc pierwszy z nich otrzymamy $z = \frac{\sqrt[3]{19+3\sqrt{33}}}{3}$, a więc

$$x = \frac{\sqrt[3]{19 + 3\sqrt{33}}}{3} + \frac{4}{3\sqrt[3]{19 + 3\sqrt{33}}} + \frac{1}{3} = 1.839\ldots$$

Wzięcie drugiego pierwiastka da ten sam wynik, gdyż

$$\sqrt[3]{19 + 3\sqrt{33}} \cdot \sqrt[3]{19 - 3\sqrt{33}} = 4.$$

Łatwo sprawdzić (przez wydzielenie albo badając przebieg funkcji), że równanie wyjściowe innych pierwiastków rzeczywistych nie ma.



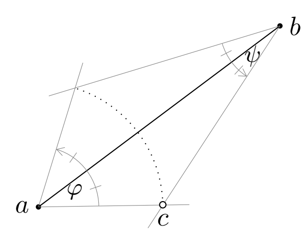
35.

(i) $\mathrm{Rot}_{(3,4),60^\circ}(1,2) = ((1,2)-(3,4))e^{i\frac{\pi}{3}} + (3,4) = (-2-2i)(\frac{1}{2}+i\frac{\sqrt{3}}{2}) + 3 + 4i = \ldots = \sqrt{3}+2+i(3-\sqrt{3}) = (\sqrt{3}+2, 3-\sqrt{3})$.

(ii) $$\mathrm{Rot}_{b,\psi}\circ\mathrm{Rot}_{a,\varphi} = \begin{cases} \mathrm{Rot}_{c,\varphi+\psi}, & \text{gdy } \varphi+\psi \neq 0 \pmod{2\pi} \\ & \text{gdzie } c = \frac{(1-e^{i\varphi})e^{i\psi}a+(1-e^{i\psi})b}{1-e^{i(\varphi+\psi)}} \\ \tau_v = \{z\mapsto z+v \mid z\in\mathbb{C}\} & \text{w przeciwnym wypadku,} \\ & \text{gdzie } v=(b-a)(1-e^{i\psi}) \end{cases}$$

$\langle z \mapsto ((z-a)e^{i\varphi}+a-b)e^{i\psi}+b = ze^{i(\varphi+\psi)} - ae^{i\varphi}e^{i\psi} + ae^{i\psi} - be^{i\psi} + b = ze^{i(\varphi+\psi)} + ae^{i\psi}(1-e^{i\varphi}) + b(1-e^{i\psi})$.
Jeżeli $\varphi+\psi = 0 \pmod{2\pi}$, to $z\mapsto z+v$, gdzie $v = ae^{i\psi}(1-e^{i\psi}) + b(1-e^{i\psi}) = (b-a)(1-e^{i\psi})$.
W przeciwnym wypadku $z\mapsto (z-c)e^{i(\varphi+\psi)} + c = ze^{i(\varphi+\psi)} + c(1-e^{i(\varphi+\psi)})$, gdzie $c(1-e^{i(\varphi+\psi)}) = ae^{i\psi}(1-e^{i\varphi}) + b(1-e^{i\psi})\rangle$.

Uwaga: W przypadku, gdy złożenie dwóch obrotów jest obrotem, formuła na nowy środek obrotu c nie ma praktycznego znaczenia. Natomiast punkt c łatwo wyznaczyć konstrukcyjnie jako jedyny punkt stały naszego złożenia.



36. Przy ustalonym $p\in X$ ($X\in \mathrm{Af}_K$) oznaczmy przez $+$ i $\cdot$ działania $\underset{p}{+}$ i $\underset{p}{\cdot}$ dodawania punktów przestrzeni X i mnożenia ich przez skalary z ciała K w przestrzeni wektorowej X_p.

Wówczas dla $a \in X$ mamy izomorfizm przestrzeni wektorowych $\tau = \tau_{p,a} : X_p \xrightarrow{\sim} X_a$, $\tau(x) = x + a$. Zatem dla $x, y \in X$; $\alpha \in K$:

$$\begin{gathered} x \underset{a}{+} y = \tau(\tau^{-1}(x \underset{a}{+} y)) = \tau(\tau^{-1}(x) + \tau^{-1}(y)) = (x - a + y - a) + a = x + y - a, \\ \alpha \underset{a}{\cdot} x = \tau(\tau^{-1}(\alpha \underset{a}{\cdot} x)) = \tau(\alpha \cdot \tau^{-1}(x)) = \alpha(x - a) + a = \alpha x + (1 - \alpha)a. \end{gathered}$$

Odwzorowanie $F : \mathrm{Vect}_K \to \mathrm{Af}_K$ jest funktorem zwyczajnym, gdyż dla $X, X' \in \mathrm{Vect}_K$ oraz $f : X \underset{\mathrm{Vect}_K}{\longrightarrow} X'$, jeśli $a, x, y \in X$, $\alpha \in K$, to

$$\begin{gathered} f(x \underset{a}{+} y) = f(x + y - a) = f(x) + f(y) - f(a) = f(x) \underset{f(a)}{+} f(y), \\ f(\alpha \underset{a}{\cdot} x) = f(\alpha x + (1 - \alpha)a) = \alpha f(x) + (1 - \alpha) f(a) = \alpha \underset{f(a)}{\cdot} f(x), \end{gathered}$$

czyli $f : X_a \underset{\mathrm{Vect}_K}{\longrightarrow} X'_{f(a)}$, a więc $f : F(X) \underset{\mathrm{Af}_K}{\longrightarrow} F(X')$.

Podobnie bezpośrednim rachunkiem sprawdzamy własności (ii) i (iii):

Łatwo widać, że dla $V \underset{\mathrm{Vect}}{\subset} X$, $a \in X$: $V + a \underset{\mathrm{Af}}{\subset} X$, a także $a \in U \underset{\mathrm{Af}}{\subset} X \implies U - a \underset{\mathrm{Vect}}{\subset} X \ \wedge\ U = (U - a) + a$.

Jeżeli $U, V \underset{\mathrm{Vect}}{\subset} X$, $a, b \in X$ i $U + a = V + b$, to $U \subset V$. $\langle$Jeśli $u \in U$, to $u + a \in V + b$, a więc $\exists)\, v \in V : u + a = v + b$, $u = v + (b - a)$. Jednak $a = 0 + a \in U + a = V + b$, zatem $\exists)\, w \in V : a = w + b$, i wówczas $w = b - a$, $u = v + w \in V\rangle$.
Podobnie $V \subset U$, a więc $U = V$.

37. $Z = \mathbb{R}^*$ $\langle$Oczywiście $\mathbb{R}^* \subset Z$. HP: $\exists)\, q = a + bi + cj + dk \in Z \setminus \mathbb{R}^*$; $a, b, c, d \in \mathbb{R}$.

Łatwo widać, że $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$, co można zilustrować diagramem:

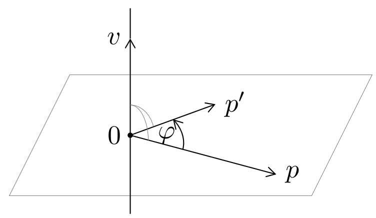
$$\begin{tikzcd} & k \arrow[dl] & \\ i \arrow[rr, "+"] & & j \arrow[ul] \end{tikzcd}$$

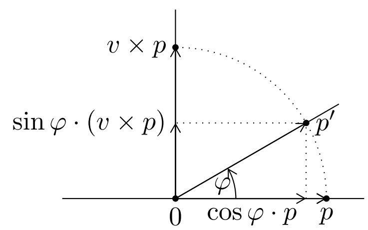
Teraz $iq = qi$, a więc $ai - b + ck - dj = ai - b - ck + dj$, czyli $2dj - 2ck = 0$, skąd $c = d = 0$, $q = a + bi$. Również $jq = qj$, zatem $aj - bk = aj + bk$, $2bk = 0$, $b = 0$, $q = a \in \mathbb{R}^*$ ↯$\rangle$.

38*. Oznaczmy $c = \cos \frac{\varphi}{2}$, $s = \sin \frac{\varphi}{2}$; wówczas $q = c + sv$, $|q|^2 = q\bar{q} = (c + sv)(c - sv) = c^2 - s^2v^2 = c^2 + s^2 = 1$, a więc $q^{-1} = \bar{q} = c - sv$. Niech $p' =$ wynik obrotu punktu p.

Rozważmy wpierw przypadek szczególny, gdy środek obrotu jest w punkcie 0. Wówczas $p \perp v$, $p \circ v = 0$, $qpq^{-1} = (c + sv)p(c - sv) = (cp + svp)(c - sv) = c^2p - scpv + scvp - s^2vpv = c^2p - 2sc \cdot \frac{1}{2}(vp - pv) - s^2vpv = c^2p + 2sc(v \times p) - s^2vpv$.

Teraz $vpv = (-v \circ p + v \times p)v = (v \times p)v = -(v \times p) \circ v + (v \times p) \times v = (v \times p) \times v = (v \circ v)p - (p \circ v)v = p$, a więc $qpq^{-1} = (c^2 - s^2)p + 2sc(v \times p) = \cos\varphi \cdot p + \sin\varphi \cdot (v \times p)$.





Wektory $\cos\varphi \cdot p$, $\sin\varphi \cdot (v \times p)$ są składowymi wektora p' względem osi wyznaczonych przez wektory v, $v \times p$, a więc $p' = \cos\varphi \cdot p + \sin\varphi \cdot (v \times p)$ (*formuła Rodriguesa*).

W przypadku ogólnym środek obrotu jest punktem tv dla pewnego $t \in \mathbb{R}$. Wówczas $p' = q(p - tv)q^{-1} + tv = qpq^{-1} - tqvq^{-1} + tv = qpq^{-1} + t(v - qvq^{-1})$. Jednak $qvq^{-1} = c^2v + 2sc(v \times v) - s^2v^3 = c^2v - s^2v^3 = (c^2 - s^2v^2)v = (c^2 + s^2)v = v$, a więc $p' = qpq^{-1}$.

(i) $p' = (z, x, y)$.
(ii) $p' = (0, 1, 1)$.

39.

(i) $\mathcal{F} = \iota(A)$, gdzie $A \in \mathcal{F}$ jest zbiorem najmniejszej mocy należącym do $\mathcal{F}$.
(ii) HP: $\exists)\, A \in \mathcal{F} : \mathcal{F} = \iota(A)$. Wówczas $A \neq \varnothing$, gdyż $\varnothing^{\urcorner} = X \notin \mathrm{Fin}$. $\exists)\, a \in A$. $(A \setminus \{a\})^{\urcorner} = A^{\urcorner} \cup \{a\} \in \mathrm{Fin}$, a więc $A \subset A \setminus \{a\}$ ↯.
(iii) HP: $\exists)\, U \in \varPhi_a : \varPhi_a = \iota(U)$. $\exists)\, r > 0 : (a - r, a + r) \subset U$. $(a - \frac{r}{3}, a + \frac{r}{3}) \in \varPhi_a$, $a + \frac{2}{3}r \in U \subset (a - \frac{r}{3}, a + \frac{r}{3})$ ↯.

40.

(i) Oczywiście $X \in \mathcal{F}_\beta$ oraz dla $A \in \mathcal{F}_\beta$ i $A \subset B \subset Y$: $|B^{\urcorner}| \leqslant |A^{\urcorner}| < \beta$, a więc $B \in \mathcal{F}_\beta$.

Jeżeli $A, B \in \mathcal{F}_\beta$, to $|(A \cap B)^{\urcorner}| = |A^{\urcorner} \cup B^{\urcorner}| \leqslant |A^{\urcorner}| + |B^{\urcorner}| < \beta$, a więc $A \cap B \in \mathcal{F}_\beta$.
(ii) HP: $\exists)\, A \subset X : \mathcal{F}_\beta = \iota(A) = \{B \mid A \subset B \subset X\}$. Wówczas $A \in \mathcal{F}_\beta$, $|A^{\urcorner}| < \beta$, $A \neq \varnothing$, $\exists)\, a \in A$, $|(A \setminus \{a\})^{\urcorner}| \leqslant |A^{\urcorner} \cup \{a\}| < \beta$, $A \setminus \{a\} \in \mathcal{F}_\beta$, $A \subset A \setminus \{a\} \subsetneq A$ ↯.
(iii) $|(\bigcap \mathcal{A})^{\urcorner}| = |\bigcup\limits_{a \in \mathcal{A}} A^{\urcorner}| \leqslant \sum\limits_{A \in \mathcal{A}} |A^{\urcorner}| \leqslant |\mathcal{A}| \cdot \aleph_\xi = \aleph_\xi < \alpha$, a więc $\bigcap \mathcal{A} \in \mathcal{F}_\alpha$.

41. HP: $\exists)\, \mathcal{F} \in \mathrm{Fil}^*(X)\ \forall \mathcal{G} \in \mathrm{Fil}^*(X) : \mathcal{G} \subset \mathcal{F}$. $\exists)\, a, b \in X : a \neq b$. $\iota(\{a\}), \iota(\{b\}) \in \mathrm{Fil}^*(X)$, $\{a\} \in \iota(\{a\}) \subset \mathcal{F}$, i analogicznie $\{b\} \in \mathcal{F}$, a więc $\varnothing = \{a\} \cap \{b\} \in \mathcal{F}$ ↯.

42. Natychmiast widać, że filtr spełniający podany warunek jest niegłówny. Przypuśćmy, że istnieje filtr niegłówny $\mathcal{F}$ na zbiorze X taki, że $\exists)\, A \in \mathcal{F}\ \forall B \in \mathcal{F} : \neg B \subsetneq A$. $\mathcal{F} \neq \iota(A)$, a więc $\iota(A) \subsetneq \mathcal{F}$. $\exists)\, B \in \mathcal{F} : B \notin \iota(A)$, $A \not\subset B$.
Jednak $A \cap B \in \mathcal{F}$, $A \cap B \subset A$, a więc $A \cap B = A$, $A \subset B$ ↯.

43. Implikacje $(b) \Rightarrow (c) \Rightarrow (a)$ są oczywiste.

Dla dowodu implikacji $(a) \Rightarrow (b)$ wystarczy zauważyć, że gdyby $A \cup B \in \mathcal{U}$, $A \notin \mathcal{U}$ i $B \notin \mathcal{U}$, to jedna z rodzin $\mathcal{U} \cup \{A\}, \mathcal{U} \cup \{B\}$ byłaby scentrowana $\langle$bo w przeciwnym wypadku: $\exists)\, C, D \in \mathcal{U} : A \cap C = \varnothing,\ B \cap D = \varnothing$, i wówczas $C \subset A^\neg$, $D \subset B^\neg$, a więc $\mathcal{U} \ni C \cap D \subset A^\neg \cap B^\neg = (A \cup B)^\neg$ ↯⟩.

44. Hp: $\mathcal{F} \not\subset \mathcal{U}$. Wówczas $\exists)\, A \in \mathcal{F} \setminus \mathcal{U}$, a więc $A^\neg \in \mathcal{U}$ ⟨zadanie 43⟩. Jednak $A^\neg \in \mathrm{Fin}$, więc na mocy 39(i) filtr $\mathcal{U}$ jest główny ↯.

45. Trzeba udowodnić implikację „$\Leftarrow$".
Niech $B : \mathbb{N} \to \mathcal{F}$ będzie bazą monotoniczną filtru $\mathcal{F}$.
HP: $\neg\, f(x) \underset{x \to \mathcal{F}}{\longrightarrow} \mathcal{G}$. Wówczas $\exists)\, G \in \mathcal{G}\ \forall\, n \in \mathbb{N} : f(B_n) \setminus G \neq \varnothing$, czyli $B_n \setminus f^{-1}(G) \neq \varnothing$.
$\exists)\, \tau : \mathcal{P}X \setminus \{\varnothing\} \to X$ – funkcja wyboru.
Określamy ciąg $u : \mathbb{N} \to X$, $u_n = \tau(B_n \setminus f^{-1}(G))$.
Wówczas $\forall\, n \in \mathbb{N} : u_n \in B_n$, $f(u_n) \notin G$. Zatem $u_n \underset{n\to\infty}{\longrightarrow} \mathcal{F}$, a więc $f(u_n) \underset{n\to\infty}{\longrightarrow} \mathcal{G}$, $\exists)\, k \in \mathbb{N}\ \forall\, n \in \mathbb{N}\ [n \geqslant k \ \Rightarrow\ f(u_n) \in G]$, w szczególności $f(u_k) \in G$ ↯.

46. Dla dowodu implikacji „$\Leftarrow$" przypuśćmy, że $X \notin \mathrm{Top}(T_2)$. Wówczas $\exists)_{\substack{a,b \in X \\ a \neq b}}\ \forall\, U \in \varPhi_a,\ V \in \varPhi_b : U \cap V \neq \varnothing$;

$$\mathcal{F} = \{A \subset X \mid \exists)\, U \in \varPhi_a, V \in \varPhi_b : U \cap V \subset A\} \in \mathrm{Fil}^*(X).$$

Dla funkcji $f = \mathrm{id}_X$: $f(x) \underset{x\to\mathcal{F}}{\longrightarrow} a$, $f(x) \underset{x\to\mathcal{F}}{\longrightarrow} b$, a więc $a = b$ ↯.

47. Dowody są typowe dla analizy matematycznej i polegają na „dopasowaniu" odpowiedniego zbioru filtrowego do zadanego $\varepsilon > 0$.

Udowodnimy np. (iii).

Niech $\varepsilon > 0$, $\varepsilon' = \min\left\{\frac{|a|}{2}, \frac{\varepsilon |a|^2}{2}\right\}$. $\exists)\, A \in \mathcal{F}\ \forall\, x \in A : |f(x) - a| < \varepsilon'$.
Niech $x \in A$. Wówczas $\left|\frac{1}{f(x)} - \frac{1}{a}\right| = \left|\frac{f(x)-a}{f(x)\cdot a}\right| < \frac{\varepsilon'}{|f(x)|\cdot|a|}$.
Teraz $|a| \leqslant |f(x) - a| + |f(x)| < \varepsilon' + |f(x)|$, a więc $|f(x)| > |a| - \varepsilon' \geqslant \frac{|a|}{2}$, $\frac{1}{|f(x)|} < \frac{2}{|a|}$, czyli $\left|\frac{1}{f(x)} - \frac{1}{a}\right| < \frac{2\varepsilon'}{|a|^2} \leqslant \varepsilon$.

48. Dowody wszystkich tych zależności są proste i sprowadzają się jedynie do wykorzystania przyjętych definicji. Na przykład dla przestrzeni topologicznych X, X' z systemami filtrów otoczeń $\varPhi$ i $\varPhi'$ funkcja $f : X \to X'$ ciągła w sensie „centralnej" definicji otoczeniowej spełnia warunek:

$$\forall\, B \subset X' : f^{-1}(B^-) \supset f^{-1}(B)^-$$

⟨HP: $\exists)\, B \subset X'$, $x \in f^{-1}(B)^- \setminus f^{-1}(B^-)$. Wówczas $f(x) \notin B^-$, $\exists)\, V \in \varPhi'_{f(x)} : V \cap B = \varnothing$. Z ciągłości funkcji f w punkcie wnioskujemy, że $\exists)\, U \in \varPhi_x : f(U) \subset V$.

Teraz $U \cap f^{-1}(B) \neq \varnothing$, a więc $f(z) \in V \cap B$ ↯⟩.

Nasza funkcja spełnia również warunek:

$$(*) \qquad \forall\, A \subset X : f(A^-) \subset f(A)^-$$

⟨HP: $\exists)\, A \subset X$, $x \in A^- : f(x) \notin f(A)^-$, a więc $\exists)\, V \in \varPhi'_{f(x)} : V \cap f(A) = \varnothing$.
$\exists)\, U \in \varPhi_x : f(U) \subset V$. Teraz $U \cap A \neq \varnothing$, $\exists)\, z \in U \cap A$ i wówczas $f(z) \in V \cap f(A)$ ↯⟩.
Łatwo też sprawdzić, że funkcja spełniająca warunek $(*)$ jest ciągła – np. pokazujemy domkniętość przeciwobrazów zbiorów domkniętych.

Natomiast dla operacji wnętrza nie mamy żadnego uniwersalnego odpowiednika prawa $(*)$.

Na przykład weźmy przestrzenie $\mathbb{R}$ i $\mathbb{R}^2$ z topologią naturalną. Jeżeli $f : \mathbb{R}^2 \to \mathbb{R}$, $f(x,y) = x$ (rzutowanie), to dla $A = \{(x,0) \mid x \in \mathbb{R}\} \subset \mathbb{R}^2$ będziemy mieli $A^\circ = \varnothing$, a więc $\varnothing = f(A^\circ) \subsetneq f(A)^\circ = \mathbb{R}^\circ = \mathbb{R}$.

Teraz dla $g : \mathbb{R} \to \mathbb{R}^2$, $g(x) = (x,0)$ (włożenie), $A = \mathbb{R}$ otrzymamy $f(A^\circ) = f(\mathbb{R}) = \mathbb{R} \times \{0\} \supsetneq f(A)^\circ = (\mathbb{R} \times \{0\})^\circ = \varnothing$.

49. (3) $\Rightarrow$ (2) $\quad \langle \operatorname{Lim} f(t) \subset \operatorname{Adh} f(t) \rangle$.

Pozostają jeszcze dwie implikacje:
(1) $\Rightarrow$ (3)) $\quad \langle$HP: (1) $\wedge \neg$(3). $\exists) \, T, \mathcal{F} \in \operatorname{Fil}^*(T)$, $f : T \to E$, $x \in \operatorname*{Adh}_{t \to \mathcal{F}} f(t)$, $x \notin E$. Wówczas $x \in E^\neg \in \Phi_x$. $T \in \mathcal{F}$. $f(T) \cap E^\neg \neq \varnothing$, $\exists) \, t \in T : f(t) \in E^\neg$ ↯$\rangle$.
(2) $\Rightarrow$ (1)) $\quad \langle$HP: (2) $\wedge \neg$(1). $\neg \forall x \in X \; [(\forall U \in \Phi_x : U \cap E \neq \varnothing) \;\Rightarrow\; x \in E]$. Zatem $\exists) \, x \in X : \forall U \in \Phi_x : U \cap E \neq \varnothing$, $x \notin E$.
Teraz $\exists) \, \mathcal{F} \in \operatorname{Fil}^*(E) \; \forall A \subset E \; (A \in \mathcal{F} \Leftrightarrow \exists U \in \Phi_x : U \cap E \subset A)$. $f = \operatorname{id}_E : E \to E \, (\subset X)$.
$\underset{t \to \mathcal{F}}{f(t) \longrightarrow x} \quad \langle$HP: $\neg \forall U \in \Phi_x \; \exists A \in \mathcal{F} : A = f(A) \subset U$. Zatem $\exists) \, U \in \Phi_x \; \forall A \in \mathcal{F} : A \not\subset U$. $U \cap E \in \mathcal{F}$. $\exists) \, t \in U \cap E : t \notin U$ ↯$\rangle$.
Zatem $x \in E$ ↯$\rangle$.

50. (1) $\Rightarrow$ (2) $\quad \langle$HP: (1) $\wedge \neg$(2). $\exists)_{\substack{T, \mathcal{F} \in \operatorname{Fil}^*(T) \\ f : T \to X}} : \operatorname*{Adh}_{t \to \mathcal{F}} f(t) = \varnothing$.
Wówczas $\forall x \in X \; \exists U \in \Phi_x, A \in \mathcal{F} : f(A) \cap U = \varnothing$.
Niech $\tau =$ ogół podzbiorów otwartych w X.
Na mocy (AC) $\exists) \, G : X \to \tau, A : X \to \mathcal{F} \; \forall x \in X : x \in G_x$ i $f(A_x) \cap G_x = \varnothing$.
Z pokrycia $\{G_x \mid x \in X\}$ przestrzeni X można wyjąć pokrycie skończone; $\exists E \subset X : E \in \operatorname{Fin}$, $X = \bigcup_{x \in E} G_x$. Wówczas $B := \bigcap_{x \in E} A_x \in \mathcal{F}$. $B \neq \varnothing$. $\exists) \, b \in B$. $\exists) \, x \in E : f(b) \in G_X$, czyli $G_x \in \Phi_x$ oraz $f(b) \in f(B) \cap G_x = \varnothing$ ↯$\rangle$.
(2) $\Rightarrow$ (1) $\quad \langle$HP: (2) $\wedge \neg$(1). $\exists) \, \mathcal{A}$ – rodzina scentrowana podzbiorów domkniętych w X taka, że $\bigcap A = \varnothing$. $\exists) \, \mathcal{F} \in \operatorname{Fil}^*(X) : \mathcal{A} \subset \mathcal{F}$. Dla $f = \operatorname{id}_X : \exists) \, x \in \operatorname*{Adh}_{x \to \mathcal{A}} f(x)$ i wówczas $\forall U \in \Phi_x, A \in \mathcal{A} : A \cap U \neq \varnothing$, a więc $\forall A \in \mathcal{A} : x \in A^- = A$, czyli $x \in \bigcap \mathcal{A} = \varnothing$ ↯$\rangle$.

Dla dowodu równoważności (1)$\Leftrightarrow$(3) zauważmy wpierw, że:

$$\forall_{\substack{X \in \operatorname{Top}, T, \mathcal{U} \in \operatorname{Ultr}(T) \\ f : T \to X}} : \operatorname*{Adh}_{t \to \mathcal{U}} f(t) = \operatorname*{Lim}_{t \to \mathcal{U}} f(t)$$

$\langle$HP: $\exists) \, x \in \operatorname*{Adh}_{t \to \mathcal{U}} f(t) : x \notin \operatorname*{Lim}_{t \to \mathcal{U}} f(t)$.
$\neg \forall U \in \Phi_x \; \exists) \, A \in U : f(A) \subset U$. $\exists) \, U \in \Phi_x \; \forall A \in \mathcal{U} : f(A) \not\subset U$. Wówczas $f^{-1}(U) \notin \mathcal{U} \quad \langle$bo gdyby $f^{-1}(U) \in \mathcal{U}$, to $f(f^{-1}(U)) \subset U$ ↯$\rangle$, a więc $A = T \setminus f^{-1}(U) \in \mathcal{U}$. $f(A) \cap U \neq \varnothing$. $\exists) \, t \in A : f(t) \in U$, $t \in f^{-1}(U)$, $t \notin A$ ↯$\rangle$.
Zatem (2) $\Rightarrow$ (3).
(3) $\Rightarrow$ (2) $\quad \langle$HP: (3) $\wedge \neg$(2).
$\exists)_{\substack{T, \mathcal{F} \in \operatorname{Fil}^*(T) \\ f : T \to X}} : \operatorname*{Adh}_{t \to \mathcal{F}} f(t) = \varnothing$.
$\exists) \, \mathcal{U} \in \operatorname{Ultr}(T) : \mathcal{F} \subset \mathcal{U}$. $\exists) \, x \in \operatorname*{Lim}_{t \to \mathcal{U}} f(t)$.

Wówczas $x \in \operatorname*{Adh}_{t\to\mathcal{F}} f(t)$ $\langle$HP: $\neg\ldots$ $\exists)\, A \in \mathcal{F}, V \in \Phi_x : f(A) \cap V = \varnothing$. $\exists)\, B \in \mathcal{U} : f(B) \subset V$. Jednak $A \in \mathcal{U}$, $A \cap B \in \mathcal{U}$, $A \cap B \neq \varnothing$, $\exists)\, t \in A \cap B$. $f(t) \in f(B) \subset V$, $f(t) \in f(A) \cap V$ ↯$\rangle$$\rangle$.

51.

(i) HP: $\exists)\, X : I \to \mathrm{Comp}$, $f : T \to \prod X$, $\mathcal{U} \in \mathrm{Ultr}(T)$, $\operatorname*{Lim}_{t\to\mathcal{U}} f(t) = \varnothing$. $\forall\, i \in I : \operatorname*{Lim}_{t\to\mathcal{U}}(\mathrm{pr}_i \circ f)(t) \neq \varnothing$, gdzie $\mathrm{pr}_i : \prod X \to X_i$ jest i-tą projekcją; $\mathrm{pr}_i(x) = x_i$ dla $x \in \prod X$.
$\exists)\, x \in \prod X\ \forall\, i \in I : x_i \in \mathrm{Lim}\, \mathrm{pr}_i(f(t))$ $\langle$na mocy AC$\rangle$.

Wówczas $x \in \operatorname*{Lim}_{t\to\mathcal{U}} f(t)$ $\langle$Niech $U \in \Phi_x$. Wówczas $\prod V \subset U$, gdzie $V : I \to \mathbb{V}$, $\forall\, i \in I : V_i \in \Phi_{x_i}$, $\{i \in I \mid V_i \neq X_i\} \in \mathrm{Fin}$.
$\exists)\, A : I \to \mathcal{U} : \forall\, i \in I : (\mathrm{pr}_i \circ f)(A_i) \subset V_i$, $\{i \in I \mid A_i \neq T\} \in \mathrm{Fin}$. Zatem $B := \bigcap_{i\in I} A_i \in \mathcal{U}$ i $f(B) \subset \prod V \subset U\rangle$ ↯.

(ii)* HP: $\neg$ AC.
$\exists)\, X : I \to \mathbb{V}$, $\forall\, i \in I : X_i \neq \varnothing$, $\prod X = \varnothing$.
$\exists)\, b \in \mathbb{V} \setminus \bigcup_{i\in I} X_i$.

Dla $i \in I$ zbiór $X_i' = X_i \cup \{b\}$ traktujemy jako przestrzeń topologiczną z rodziną zbiorów otwartych

$$\tau_i = \{A \subset X_i \mid X_i \setminus A \in \mathrm{Fin}\ \ \vee\ \ A = \varnothing\ \ \vee\ \ A = \{b\}\};$$

przestrzeń ta jest zwarta, a więc na mocy twierdzenia Tichonowa przestrzeń produktowa $\prod X'$ $(= \prod_{i\in I} X_i')$ też jest zwarta.

Dla $i \in I$ niech $G_i = \{x \in \prod X' \mid x_i = b\}$ $(\in \tau_i)$. Wówczas $\prod X' = \bigcup_{i\in I} G_i$ $\langle\forall\, x \in \prod X'\ \exists)\, i \in I : x_i = b$, gdyż $\prod X = \varnothing\rangle$.

Zatem $\exists)\, J \subset I : J \in \mathrm{Fin}$, $\bigcup_{j\in J} G_j = \prod X'$.

Teraz na mocy skończonego aksjomatu wyboru ($\mathrm{AC_{fin}}$): $\exists)\, y \in \prod_{j\in J} X_j$.

Niech $x = y \cup \{i \mapsto b \mid i \in I \setminus J\}$.
Wówczas $x \in \prod X'$, a więc $\exists)\, j \in J : x \in G_j$. Zatem $x_j = b$, ale $x_j = y_j \in X_j$, czyli $x_j \neq b$ ↯.

52.

(1) Niech $\alpha \in \tau_Y$ = zbiory otwarte w Y i $\bigcup \alpha = Y$.

Wówczas $\alpha' = \{f^{-1}(A) \mid A \in \alpha\} \subset \tau_X$ i $\bigcup \alpha' = X$, a więc $\exists)\, \beta \subset \alpha : \beta \in \mathrm{Fin}$, $\bigcup_{B\in\beta} f^{-1}(B) = X$, i wówczas $\bigcup \beta = Y$. $\langle$Jeśli $y \in Y$, to $\exists)\, x \in X : y = f(x)$. $\exists)\, B \in \beta : x \in f^{-1}(B)$, a więc $y = f(x) \in B\rangle$.

(2) Zbiór A jako domknięty w przestrzeni zwartej jest zwarty. Zatem według (1) zbiór $f(A)$ jest zwarty, a więc, ponieważ Y jest przestrzenią Hausdorffa, $f(A)$ jest domknięty w Y.

(3) Wniosek z (2).

(4) 1°) Wykażemy wpierw, że przestrzeń X spełnia warunek rozdzielczości T_3, zwany też warunkiem *regularności*:

$$\forall\, A \in \sigma_X, x \in X \setminus A\ \exists)_{\substack{G,H\in\tau_X\\ G\cap H=\varnothing}} : A \subset G,\ x \in H.$$

Dla $y \in A$ wybieramy zbiory otwarte U_y, V_y $(\in \tau_X)$ takie, że $U_y \cap V_y = \varnothing$, $x \in U_y$, $y \in V_y$.

Z pokrycia $\{V_y \mid y \in A\}$ można wyjąć pokrycie skończone $A \subset V_{y_1} \cup \ldots \cup V_{y_n} = G \in \tau_X$ i wówczas bierzemy $H = U_{y_1} \cap \ldots \cap U_{y_n}$.

2°) Wykorzystujemy 1°) i powtarzamy rozumowanie:

Dla $x \in A$ bierzemy U_x, $V_x \in \tau_X$ takie, że $x \in U_x$, $B \subset V_x$.

Ze zwartości A wynika, że istnieje pokrycie skończone

$$A \subset U_{x_1} \cup \ldots \cup U_{x_n} = G \in \tau_X,$$

a następnie $H = V_{x_1} \cap \ldots \cap V_{x_n}$.

53. Oznaczmy $RS = S \circ R$, $R^2 = RR$ itp. dla $R, S \subset X^2$.

Dowód lematu jest indukcyjny.

I. Dla $n = 1$ jest tak, gdyż zbiór $\mathrm{Sym}\, X$ jest bazą filtru $\mathcal{U}_X$.

II. Dla $n = 2$: $\exists)\, T \in \mathcal{U}_X : T^2 \subset R$. $\exists)\, S \in \mathrm{Sym}\, X : S \subset T$; i wówczas $S^2 \subset T^2 \subset R$.

III. Załóżmy, że $n \geqslant 3$ i nasz lemat jest prawdziwy dla $k < n$.

Wówczas $\exists)\, S \in \mathrm{Sym}\, X : S^{n-1} \subset R$, oraz $\exists)\, T \in \mathrm{Sym}\, X : T^2 \subset S$.

Jeżeli $n = 2k$, to $T^n = T^{2k} = (T^2)^k \subset S^k \subset S^{n-1} \subset R$.

Jeżeli $n = 2k - 1$, to analogicznie $T^n \subset T^{2k} \subset R$.

54. $\Rightarrow$) HP: $\mathrm{id}_X \subsetneq \bigcap \mathrm{Sym}\, X$, a więc
$\exists)\, (x, y) \in \bigcap \mathrm{Sym}\, X : x \neq y$, i dalej
$\exists)\, R, S \in \mathrm{Sym}\, X : K(x, R) \cap K(y, S) = \varnothing$; $(x, y) \in R$; $y \in K(x, R) \cap K(y, S)$ ↯.

$\Leftarrow$) HP: $\exists)\, x, y \in X$: $x \neq y \ \wedge\ \forall U \in \Phi_x,\ V \in \Phi_y : U \cap V \neq \varnothing$. Wówczas $(x, y) \notin \mathrm{id}_X$, a więc $\exists)\, R \in \mathrm{Sym}\, X : (x, y) \notin R$. $\exists)\, S \in \mathrm{Sym}\, X : S \circ S \subset R$. $K(x, S) \cap K(y, S) \neq \varnothing$. $\exists)\, z \in K(x, S) \cap K(y, S)$, a więc (x, z), $(y, z) \in S$, czyli $(z, y) \in S$, $(x, y) \in S \circ S \subset R$ ↯.

55. Niech $X \in \mathrm{Unif}$, $x \in X$, $R \in \mathrm{Sym}\, X$.
$\exists)\, S \in \mathrm{Sym}\, X : S \circ S \subset R$. Wówczas
$K(x, S)^- \subset K(x, R)$ ⟨HP: $\exists)\, y \in K(x, S)^- \setminus K(x, R)$. $K(y, S) \cap K(x, S) \neq \varnothing$. $\exists)\, z \in K(y, S) \cap K(x, S)$; (y, z), $(x, z) \in S$, a więc $(x, y) \in S \circ S \subset R$, czyli $y \in K(x, R)$ ↯⟩.

56. HP: $\neg \forall V \in \mathcal{C}\ \exists)\, B \in \mathcal{G} : \varphi(B) \subset V$, a więc
$\exists)\, V \in \mathcal{C}\ \forall B \in \mathcal{G} : \varphi(B) \not\subset V$.
$\exists)\, A \in \mathcal{F},\ B \in \mathcal{G} : f(A \times B) \subset V$.
$\exists)\, y \in B : \varphi(y) \notin V$. Teraz $f(x, y) \underset{x \to \mathcal{F}}{\longrightarrow} \varphi(y)$ oraz $\varphi(y) \in Z \setminus V$ i zbiór $Z \setminus V$ jest otwarty, a więc $\exists)\, A' \in \mathcal{F}\ \forall x \in A' : f(x, y) \in Z \setminus V$. $\exists)\, x \in A \cap A'$; wówczas $f(x, y) \in Z \setminus V$. Jednak $(x, y) \in A \times B$, a więc $f(x, y) \in V$ ↯.

57. HP: $\exists)\, x \in X : \neg \forall\, R \in \operatorname{Sym} Y\ \exists)\, U \in \Phi_x : \varphi(U) \subset K(\varphi(x), R)$.
$\exists)\, R \in \operatorname{Sym} X\ \forall\, U \in \Phi_x : \varphi(U) \not\subset K(\varphi(x), R)$.
$\exists)\, S \in \operatorname{Sym} X : S^3 = S \circ S \circ S \subset R$.
$\exists)\, A \in \mathcal{F}\ \forall\, t \in A,\ z \in X : f(t,z) \in K(\varphi(z), S)$. $\langle$Jednostajna zbieżność$\rangle$.
$\exists)\, t \in A$. Funkcja $\{z \mapsto f(t,z) \mid z \in X\}$ jest ciągła w x, a więc $\exists)\, U \in \Phi_x\ \forall\, z \in U : f(t,z) \in K(f(t,x), S)$.
$\exists)\, z \in U : \varphi(z) \notin K(\varphi(x), R)$.
Jednak $f(t,z) \in K(\varphi(z), S)$, i $f(t,x) \in K(\varphi(x), S)$, czyli $(\varphi(z), f(t,z)), (f(t,z), f(t,x)), (f(t,x), \varphi(x)) \in S$, a więc $(\varphi(z), \varphi(x)) \in S^3 \subset R$, $\varphi(z) \in K(\varphi(x), R)$ ↯.

58.

(i) HP: $\exists)\, R \in \operatorname{Sym} X\ \forall\, A \in \mathcal{F}\ \exists\, t, s \in A : (f(t), f(s)) \notin R$.
$\exists)\, S \in \operatorname{Sym} X : S^2 = S \circ S \subset R$. $\exists)\, A \in \mathcal{F}\ \forall\, t \in A : (f(t), x) \in S$.
$\exists)\, t, s \in A : (f(t), f(s)) \notin R$.
Jednak $(f(t), x), (f(s), x) \in S$, a więc $(f(t), f(s)) \in S^2 \subset R$ ↯.

(ii) HP: $\exists)\, R \in \operatorname{Sym} X\ \forall\, A \in \mathcal{F} : f(A) \not\subset K(x, R)$.
$\exists)\, S \in \operatorname{Sym} X : S^2 = S \circ S \subset R$. $\exists)\, A \in \mathcal{F}\ \forall\, t, s \in A : (f(t), f(s)) \in S$.
$\exists)\, t \in A : f(t) \notin K(x, R)$.
$f(A) \cap K(x, S) \neq \varnothing$, a więc $\exists)\, s \in A : (f(s), x) \in S$.
Tak więc $(f(t), f(s)),\ (f(s), x) \in S$, czyli $(f(t), x) \in S^2 \subset R$, $f(t) \in K(x, R)$ ↯.

59.

(i) Zakładamy, że przestrzeń jednostajna X ma przeliczalną bazę otoczeń przekątnej $\{S_n \mid n \in \mathbb{N}\}$, $S_n \in \operatorname{Sym} X$, $S_{n+1} \subset S_n$.

Załóżmy, że funkcja $f : T \to X$ spełnia warunek Cauchy'ego względem filtru $\mathcal{F} \in \operatorname{Fil}^*(X)$; tak więc $\forall\, n \in \mathbb{N}\ \exists\, A \in \mathcal{F}\ \forall\, t, s \in A : (f(t), f(s)) \in S_n$. Wówczas $\exists)\, A : \mathbb{N} \to \mathcal{F}\ \forall\, n \in \mathbb{N},\ t, s \in A_n : (f(t), f(s)) \in S_n$ $\langle$wg AC$\rangle$.
$\exists)\, \tau : \mathbb{N} \to T\ \forall\, n \in \mathbb{N} : \tau_n \in A_n$.
Ciąg $f \circ \tau$ spełnia warunek Cauchy'ego $\langle$HP: $\neg \ldots\ \exists)\, p \in \mathbb{N}\ \forall\, k \in \mathbb{N}\ \exists\, n, m \geqslant k : (f(\tau_n), f(\tau_m)) \notin S_p$. $\exists)\, k \in \mathbb{N} : S_k^2 \subset S_p$.
$\exists)\, n, m \geqslant k : (f(\tau_n), f(\tau_m)) \notin S_p$. $\exists)\, t \in A_n \cap A_m$. Wówczas $(f(t), f(\tau_n)) \in S_n \subset S_k$, $(f(t), f(\tau_m)) \in S_m \subset S_k$, a więc $(f(\tau_n), f(\tau_m)) \in S_k^2 \subset S_p$ ↯$\rangle$.
Zatem $\exists)\, x \in X : \underset{n\to\infty}{f(\tau_n) \longrightarrow x}$, i wówczas $\underset{t\to\mathcal{F}}{f(t) \longrightarrow x}$ $\langle$HP: $\neg \ldots\ \exists)\, p \in \mathbb{N}\ \forall\, k \in \mathbb{N} : f(A_k) \not\subset K(x, S_p)$. $\exists)\, k \in \mathbb{N} : S_k^2 \subset S_p$.
$\exists)\, n \geqslant k : f(\tau_n) \in K(x, S_k)$, $(f(\tau_n), x) \in S_k$.
$\exists)\, t \in A_n : f(t) \notin K(x, S_p)$, $(f(t), x) \notin S_p$.
Jednak $(f(\tau_n), f(t)) \in S_n \subset S_k$, a więc $(f(t), x) \in S_k^2 \subset S_p$ ↯$\rangle$.

(ii) $\mathbb{R}^n$ jest typu przeliczalnego $\langle S_n = \{(x, y) \in (\mathbb{R}^n)^2 \mid |x - y| < \frac{1}{n}\}\rangle$.
Wystarczy więc wykazać, że ciąg $x : \mathbb{N}^* \to \mathbb{R}^n$ spełniający warunek Cauchy'ego ma punkt skupienia $\langle$zadanie 58.(ii)$\rangle$; ciąg taki jest ograniczony $\langle$Łatwy dowód nie wprost$\rangle$, a więc wszystkie jego wyrazy należą do pewnej kuli domkniętej $K = K(0, r) = \{z \in \mathbb{R}^n \mid |z| \leqslant r\}$. Ze zwartości kuli K wynika istnienie w niej punktu skupienia ciągu x.

60. Z zupełności przestrzeni Y wynika, że:

$$\exists)\, \varphi : X \to Y\ \forall\, x \in X : f(t,x) \underset{t\to\mathcal{F}}{\longrightarrow} \varphi(x) \qquad \langle \text{AC} \rangle.$$

Należy wykazać, że zbieżność jest jednostajna dla $x \in X$.
HP: $\neg\forall\, R \in \operatorname{Sym} Y\ \exists)\, A \in \mathcal{F}\ \forall\, t \in A,\ x \in X : f(t,x) \in K(\varphi(x), R)$, a więc
$\exists)\, R \in \operatorname{Sym} Y\ \forall\, A \in \mathcal{F}\ \exists\, t \in A,\ x \in X : f(t,x) \notin K(\varphi(x), R)$.
$\exists)\, S \in \operatorname{Sym} Y : S^2 = S \circ S \subset R$.
$\exists)\, A \in \mathcal{F}\ \forall\, t, s \in A,\ x \in X : (f(t,x), f(s,x)) \in S$.
$\exists)\, t \in A,\ x \in X : (f(t,x), \varphi(x)) \notin R$.
Teraz $f(s,x) \underset{s\to\mathcal{F}}{\longrightarrow} \varphi(x)$, a więc $\exists)\, B \in \mathcal{F}\ \forall\, s \in B : f(s,x) \in K(\varphi(x), S)$. $\exists)\, s \in A \cap B$.
Wówczas $(f(t,x), f(s,x))$, $(f(s,x), \varphi(x)) \in S$, a więc $(f(t,x), \varphi(x)) \in S^2 \subset R$, czyli $f(t,x) \in K(\varphi(x), R)$ ↯.

61*. Spełnione są warunki Cauchy'ego zwykłej zbieżności i jednostajnej zbieżności (zadania 58, 60):
(1) $\forall\, x \in X\ \forall\, R \in \operatorname{Sym} Z\ \exists\, B \in \mathcal{G}\ \forall\, y, y' \in B : (f(x,y), f(x,y')) \in R$,
(2) $\forall\, R \in \operatorname{Sym} Z\ \exists\, A \in \mathcal{F}\ \forall\, x, x' \in A,\ y \in Y : (f(x,y), f(x',y)) \in R$.

Przestrzeń Z jest zupełna, więc wystarczy wykazać, że funkcja f spełnia warunek Cauchy'ego względem filtru $\mathcal{F} \bar{\times} \mathcal{G}$.
HP: $\neg\forall\, R \in \operatorname{Sym} Z\ \exists\, A \in \mathcal{F},\ B \in \mathcal{G}\ \forall\, (x,y), (x',y') \in A \times B : (f(x,y), f(x',y')) \in R$,
a więc $\exists)\, R \in \operatorname{Sym} Z\ \forall\, A \in \mathcal{F},\ B \in \mathcal{G}\ \exists\, (x,y), (x',y') \in A \times B : (f(x,y), f(x',y')) \notin R$.
$\exists)\, S \in \operatorname{Sym} Z : S^3 = S \circ S \circ S \subset R$.
Według (2): $\exists)\, A \in \mathcal{F}\ \forall\, x, x' \in A,\ y \in Y : (f(x,y), f(x',y)) \in S$.
$\exists)\, a \in A$.
Według (1): $\exists)\, B \in \mathcal{G}\ \forall\, y, y' \in B : (f(a,y), f(a,y')) \in S$.
Teraz $\exists)\, x, x' \in A,\ y, y' \in B : (f(x,y), f(x',y')) \notin R$.

Jednak:
$(f(x,y), f(a,y))$, $(f(a,y), f(a,y'))$, $(f(a,y'), f(x',y')) \in S$, a więc $(f(x,y), f(x',y')) \in S^3 \subset R$ ↯.

62*.

1) Wykażemy, że zbiór $\mathcal{U} = \{R \subset X^2 \mid \mathrm{id}_X \subset R^\circ\}$, gdzie R° oznacza wnętrze zbioru R w topologii produktowej, jest strukturą jednostajną (filtrem otoczeń przekątnej) na zbiorze X. Łatwo widać, że $\mathcal{U}$ jest filtrem na X^2. Dla $R \in \mathcal{U} : R^{-1} \in \mathcal{U}$ $\langle$gdyż odwzorowanie $\{(x,y) \mapsto (y,x) \mid x, y \in X\}$ jest homeomorfizmem przestrzeni topologicznej X^2 na siebie$\rangle$.
HP: $\exists)\, R \in \mathcal{U}\ \forall\, S \in \mathcal{U} : S^2 = S \circ S \not\subset R$.
Wówczas zbiór $\mathcal{A} = \{S^2 \setminus R \mid S \in \mathcal{U}\}$ jest bazą filtrową na X^2 $\langle \varnothing \notin \mathcal{A},\ \mathcal{A} \neq \varnothing$ $\langle$gdyż $R^2 \setminus R \in \mathcal{A}\rangle$,
$\forall\, S, T \in \mathcal{U} : (S \cap T)^2 \setminus R \subset (S^2 \setminus R) \cap (T^2 \setminus R)$ $\langle$gdyż $(S \cap T)^2 \setminus R \subset S^2 \setminus R$, i analogicznie dla T$\rangle\rangle$.

Zatem funkcja $\mathrm{id}_{X^2} : X^2 \to X^2$ ma punkt skupienia według filtru o bazie $\mathcal{A}$ (przestrzeń X^2 jest zwarta).
$\exists)\, x, y \in X\ \forall\, S \in \mathcal{U},\ W \in \Phi_{(x,y)} : W \cap (S^2 \setminus R) \neq \varnothing$.
$x \neq y$ $\langle$HP: $x = y$. Wówczas $R \in \Phi_{(x,y)}, R \cap (R^2 \setminus R) \neq \varnothing$ ↯$\rangle$.

Przestrzeń X jako zwarta przestrzeń Hausdorffa jest normalna $\langle$zadanie 52.(4)$\rangle$, a więc każdy jej punkt ma bazę otoczeń domkniętych. Tak więc
$\exists)\, U, V, U_1, V_1 \subset X : U^\circ = U,\ V^\circ = V,\ U \supset U_1 = U_1^- \in \Phi_x,\ V \supset V_1 = V_1^- \in \Phi_y$, $U \cap V = \varnothing$.

Niech $S = U^2 \cup V^2 \cup [X \setminus (U_1 \cup V_1)]^2$ (kwadraty kartezjańskie). Wówczas $\mathrm{id}_X \subset S = S^\circ \subset X^2$ $\quad\langle$HP: $\exists)\, z \in X : (z,z) \notin S$. Zatem $z \notin U$, $z \notin V$, a więc $z \notin U_1 \cup V_1$, $z \in X \setminus (U_1 \cup V_1)$, czyli $(z,z) \in S$ ↯$\rangle$.
Tak więc $S \in \mathcal{U}$, $S^2 \setminus R \in \mathcal{A}$.
Teraz $W = U_1 \times V_1 \in \Phi_{(x,y)}$, a więc $\exists)\, (z,t) \in W \cap (S^2 \setminus R)$. Wówczas $z \in U_1$, $t \in V_1$, $(z,t) \in (S \circ S) \setminus R$, a więc $\exists)\, u \in X : (z,u), (u,t) \in S$.
Wówczas $(z,u) \in U^2 = U \times U$ $\quad\langle$bo $z \in U_1\rangle$.

Zatem $u \in U$, $(u,t) \in U^2$, $t \in U$, czyli $t \in U \cap V_1 = \varnothing$ ↯.
2) Topologia Φ' na zbiorze X ($\Phi' : X \to \mathrm{Fil}(X)$) indukowana na zbiorze X przez strukturę jednostajną $\mathcal{U}$ z 1) jest identyczna z topologią wyjściową Φ.

$\langle$ 1°) Topologia Φ' jest rozdzielcza.
$\langle$Niech $x, y \in X$, $x \neq y$.
$\exists)\, R \in \mathcal{U} : (x,y) \notin R$.
$\exists)\, S \in \mathcal{U} : S^{-1} = S$ i $S^2 = S \circ S \subset R$.
Wówczas $K(x,S) \cap K(y,S) = \varnothing\rangle$.
2°) Topologia Φ jest silniejsza od topologii Φ' ($\Phi' \prec \Phi$), tzn. $\forall\, x \in X : \Phi'_x \subset \Phi_x$

$\langle$Niech $U \in \Phi'_x$. $\exists)\, R \in \mathcal{U} : K(x,R) \subset U$.
$\exists)\, V \in \Phi_x : V \times V \subset R$ $\quad\langle(x,x) \in R^\circ\rangle$.
Wówczas $V \subset K(x,R)$ $\quad\langle z \in V \;\Rightarrow\; (z,x) \in V \times V \subset R\rangle$, a więc $V \subset U$, skąd $U \in \Phi_x\rangle$.

Topologie zwarte są elementami minimalnymi w klasie wszystkich topologii Hausdorffa (zob. zadanie 52.(3.2)), a więc, na mocy 1°) i 2°), $\Phi' = \Phi\rangle$.

3) Jeżeli $\mathcal{U}'$ jest strukturą jednostajną na zbiorze X indukującą topologię wyjściową Φ, to $\mathcal{U}' = \mathcal{U}$. Istnieje więc dokładnie jedna struktura jednostajna na zbiorze X indukująca daną topologię zwartą i rozdzielczą.

$\langle\subset)$ HP: $\exists)\, R \in \mathcal{U}' \setminus \mathcal{U}$. $\exists)\, S \in \mathcal{U}' : S^{-1} = S,\ S \circ S \subset R$.
$\forall\, x \in X : K(x,S) \in \Phi_x$, $(x,x) \in K(x,S) \times K(x,S) \subset R$, a więc $\mathrm{id}_X \subset R^\circ$, czyli $R \in \mathcal{U}$ ↯.
$\supset)$ HP: $\exists)\, R \in \mathcal{U} \setminus \mathcal{U}'$. $\forall\, S \in \mathcal{U}' : S \not\subset R$, $S \setminus R \neq \varnothing$.
Zbiór $\mathcal{A} = \{S \setminus R \mid S \in \mathcal{U}'\}$ jest bazą filtrową na X^2 $\quad\langle\varnothing \notin \mathcal{A}$, $\mathcal{A} \neq \varnothing$ $\quad\langle X^2 \setminus R \in \mathcal{A}\rangle$, $\forall\, S, T \in \mathcal{U}' : (S \cap T) \setminus R \subset (S \setminus R) \cap (T \setminus R)\rangle$.
Zatem funkcja $\mathrm{id}_{X^2} : X^2 \to X^2$ ma punkt skupienia według filtru o bazie $\mathcal{A}$;
$\exists)\, x, y \in X\ \forall\, S \in \mathcal{U}',\ W \in \Phi_{(x,y)} : W \cap (S \setminus R) \neq \varnothing$.
Jest $x \neq y$ $\quad\langle$HP: $x = y$. Wówczas $R \in \Phi_{(x,y)}$, a więc $R \cap (S \setminus R) \neq \varnothing$ ↯$\rangle$.
Z rozdzielczości X wynika, że $\exists)\, S \in \mathcal{U}' : K(x,S) \cap K(y,S) = \varnothing$. $\exists)\, T \in \mathcal{U}' : T^{-1} = T$, $T^3 = T \circ T \circ T \subset S$. Wówczas $[K(x,T) \times K(y,T)] \cap (T \setminus R) \neq \varnothing$.

$\exists) \, z \in K(x,T)$, $t \in K(y,T) : (z,t) \in T \setminus R$, a więc (x,z), (z,t), $(t,y) \in T$, $(x,y) \in T^3 \subset S$, czyli $y \in K(x,S) \cap K(y,S) = \varnothing$ ↯$\rangle$.

4) Przestrzeń jednostajna $(X,\mathcal{U})$ jest zupełna. $\langle$Załóżmy, że $f : T \to X$, $\mathcal{F} \in \mathrm{Fil}^*(X)$ i f spełnia warunek Cauchy'ego.

Ze zwartości przestrzeni topologicznej X wynika, że $\exists) \, x \in \operatorname*{Adh}_{t \to \mathcal{F}} f(t)$. Wówczas $\underset{t \to \mathcal{F}}{f(t) \longrightarrow x}$ (zadanie 58.(iii))$\rangle$.

Bibliografia

[Browkin 68] Browkin J., *Wybrane zagadnienia algebry*, PWN, Warszawa 1968

[Church 96] Church A., *Introduction to mathematical logic*, Princeton University Press, Princeton 1996

[Cohn 65] Cohn P.M., *Universal Algebra*, Harper & Row, New York, 1965

[Conway... 99] Conway J.H., Guy R.K., *Księga liczb*, tłum. J. Bartol, WNT, Warszawa 1999

[Graham... 02] Graham R.L., Nešetřil J., *Ramsey Theory and Paul Erdős (recent results in a historical perspective)*, In: Paul Erdős and his Mathematics. II, Bolyai Society Math. Studies 11, Springer Verlag (2002), pp. 339–365

[Graham... 02'] Graham R.L., Knuth D.E., Patashnik O., *Matematyka konkretna*, PWN, Warszawa 2002

[Grell 06] Grell B., Wstęp do matematyki, Zbiory, struktury, modele, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006

[Hungerford 74] Hungerford T.W., *Algebra*, Springer Verlag, New York 1974

[Herrlich 06] Herrlich H., *Axiom of Choice*, Springer Verlag, Berlin–Heidelberg 2006

[Jech 03] Jech T., *Set Theory*, Springer Verlag, Berlin–Heidelberg 2003

[Kelley 57] Kelley J.L., *General Topology*, Van Nostrand, New York 1957

[Kuratowski... 78] Kuratowski K., Mostowski A., *Teoria mnogości. Wraz ze wstępem do opisowej teorii mnogości*, PWN, Warszawa 1978

[Marek... 75] Marek W., Onyszkiewicz J., *Elementy logiki i teorii mnogości w zadaniach*, PWN, Warszawa 1975

[Mostowski 48] Mostowski A.*Logika matematyczna*, „Monografie Matematyczne" t. XVIII, Warszawa–Wrocław 1948.

[Tarski 95] Tarski A., *Pisma logiczno-filozoficzne*, t. I. *Prawda*, tłum. J. Zygmunt, PWN, Warszawa 1985.

Indeks

G

H

I

Q

R

T

Oznaczenia

1.

2.

3.

4.

5.

6.

7.

8.

9.