Logika algebraiczna 2

Jerzy Pogonowski

Zakład Logiki i Kognitywistyki UAM
www.kognitywistyka.amu.edu.pl
pogon@amu.edu.pl

2021

Plan na dziś:

- Algebry
- Podalgebry
- Morfizmy
- Kongruencje
- Algebry ilorazowe
- Twierdzenia o izomorfizmie

Następny wykład:

- Produkty proste
- Produkty podproste
- Ultraprodukty
- Algebry termów
- Algebry wolne
- Rozmaitości

- Zakładamy, że słuchacze zetknęli się z opisem składni języków logiki pierwszego rzędu (językiem rachunku predykatów).
- Zestaw predykatów, symboli funkcyjnych i stałych indywidualnych, wraz z przypisanymi każdemu predykatowi oraz symbolowi funkcyjnemu liczbą jego argumentów nazywamy *sygnaturą* (typem) rozważanego języka.
- W interpretacjach takiego języka denotacjami predykatów są relacje, denotacjami symboli funkcyjnych są funkcje, a denotacjami stałych indywidualnych są elementy uniwersum interpretacji.
- Liczba argumentów tych relacji i funkcji jest jednoznacznie określona przez sygnaturę języka (niech np. $\tau(F)$ oznacza liczbę argumentów symbolu F z ich zestawu Ω).
- Rozważane dalej sygnatury (Ω, τ) będą złożone głównie z symboli funkcyjnych (stałe indywidualne mogą być uważane za 0-argumentowe symbole funkcyjne).

- Dla dowolnego zbioru A niech A^* oznacza zbiór wszystkich skończonych potęg kartezjańskich zbioru A, czyli $A^* = \{A, A^2, A^3, \ldots\}$.
- *Strukturą relacyjną* nazywamy dowolny układ:

$$\mathbf{A} = (A, \{r_i : i \in I\}, \{f_j : j \in J\}, \{a_k : k \in K\}),$$

gdzie:

1. A jest dowolnym zbiorem (uniwersum; $dom(\mathbf{A}) = A$);
2. $\{r_i : i \in I\}$ jest zbiorem relacji, z których każda jest określona na jakimś elemencie zbioru A^*;
3. $\{f_j : j \in J\}$ jest zbiorem funkcji, z których każda działa z jakiegoś elementu zbioru A^* w zbiór A;
4. $\{a_k : k \in K\}$ jest zbiorem elementów (wyróżnionych) zbioru A.

Sygnaturą struktury $\mathbf{A}$ jest zbiór symboli indeksowanych zbiorami I, J, K, wraz z przyporządkowaniem każdemu symbolowi liczby jego argumentów.

- Jeśli R jest predykatem, F symbolem funkcyjnym, a stałą indywidualną z ustalonej sygnatury, zaś $\mathbf{A}$ strukturą relacyjną o tej sygnaturze, to denotacje R, F oraz a w $\mathbf{A}$ będziemy oznaczali przez, odpowiednio, $R^{\mathbf{A}}$, $F^{\mathbf{A}}$ i $a^{\mathbf{A}}$.
- Struktura $\mathbf{A} = (A, \{r_i : i \in I\}, \{f_j : j \in J\}, \{a_k : k \in K\})$ jest:
  1. *strukturą relacyjną (czystą)*, gdy $J = K = \emptyset$;
  2. *algebrą*, gdy $I = \emptyset$.
- Algebry o tej samej sygnaturze nazywamy algebrami podobnymi.
- Zwykle rozważać będziemy algebry o skończonej liczbie funkcji (synonimicznie: operacji, działań).
- Elementy sygnatur algebr są często w literaturze oznaczane np. symbolami ω, $\circ$, $\oplus$, $\otimes$, itp., a ich denotacje w algebrze $\mathbf{A}$ symbolami, odpowiednio: $\omega^{\mathbf{A}}$, $\circ^{\mathbf{A}}$, $\oplus^{\mathbf{A}}$, $\otimes^{\mathbf{A}}$.
- Zakładamy, że słuchacze pamiętają pojęcia: łączności, przemienności, rozdzielności (operacji), elementu neutralnego i elementu odwrotnego operacji.

- Algebry języków zdaniowych: $\mathbf{S} = (S, \circ_1, \ldots, \circ_n)$, gdzie S jest zbiorem formuł, zaś $\circ_1, \ldots, \circ_n$ funktorami zdaniotwórczymi o argumentach zdaniowych. Np.: $\mathbf{S} = (S, \neg, \wedge, \vee, \rightarrow, \bot)$.
- Algebry Peana: $\mathbf{A} = (A, f, a)$, gdzie
  1. $a \in A$ (element początkowy algebry)
  2. $f : A \rightarrow A$ (funkcja następnika)
  3. $a \notin rng(f)$
  4. f jest funkcją różnowartościową
  5. Dla dowolnego zbioru $X \subseteq A$, jeśli $a \in X$ oraz $f(x) \in X$, o ile $x \in X$, dla wszystkich $x \in X$, to $X = A$.

  Istnieje dokładnie jedna (z dokładnością do izomorfizmu) algebra Peana. Jej konstrukcja pochodzi od Dedekinda.
- Można określić $2^{2^2} = 16$ operacji dwuargumentowych na zbiorze dwuelementowym oraz $3^{3^2} = 19683$ operacji dwuargumentowych na zbiorze trójelementowym.
- Algebry znane słuchaczom: uniwersa liczbowe z operacjami arytmetycznymi.
- Ważne typy struktur: grupy, pierścienie, ciała,...

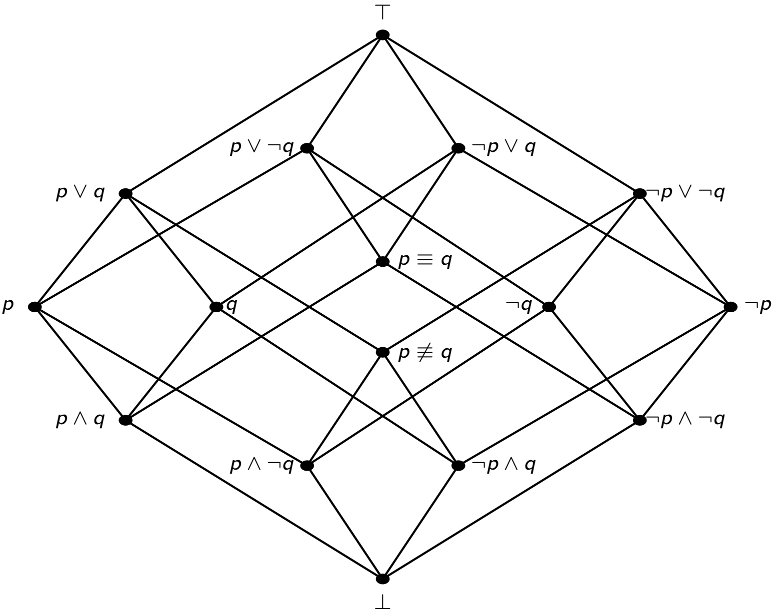
Określamy operacje $\oplus^3$ oraz $\otimes^3$ na zbiorze $\mathbb{N}$ wszystkich liczb naturalnych:

$\oplus^3$	$3n$	$3n+1$	$3n+2$
$3m$	0	1	2
$3m+1$	1	2	0
$3m+2$	2	0	1

$\otimes^3$	$3n$	$3n+1$	$3n+2$
$3m$	0	0	0
$3m+1$	0	1	2
$3m+2$	0	2	1

Określamy relację $\sim^3$ (równoważności) w $\mathbb{N}$: $x \sim^3 y$ wtedy i tylko wtedy, gdy x i y mają tę samą resztę z dzielenia przez 3.
Wtedy $\mathbb{N}/\sim^3 = \{[0]_{\sim^3}, [1]_{\sim^3}, [2]_{\sim^3}\}$.
Ponadto, jeśli $x \sim^3 y$ oraz $u \sim^3 v$, to: $x \oplus^3 u \sim^3 y \oplus^3 v$ oraz $x \otimes^3 u \sim^3 y \otimes^3 v$.
Odwzorowanie kanoniczne $k_{\sim^3} : \mathbb{N} \to \mathbb{N}/\sim^3$ dane jest wzorem: $k_{\sim^3}(x) = [x]_{\sim^3}$.
Mamy zatem: $k_{\sim^3}(x) = k_{\sim^3}(y)$ wtedy i tylko wtedy, gdy $x \sim^3 y$.

- Niech $\mathbf{S} = (S, \neg, \wedge, \vee, \rightarrow, \equiv, \bot, \top)$ będzie językiem klasycznego rachunku zdań, w którego formułach (zbudowanych przy użyciu podanych funktorów) występują jedynie zmienne zdaniowe p i q.
- Niech T będzie zbiorem tez klasycznego rachunku zdań w tym języku (przy ustalonym zbiorze aksjomatów i reguł wnioskowania).
- Określamy relację $\sim_T$ na zbiorze S: $\varphi \sim_T \psi$ wtedy i tylko wtedy, gdy równoważność $\varphi \equiv \psi$ jest tezą, czyli elementem T.
- Wtedy $\sim_T$ jest relacją równoważności, która dzieli zbiór S formuł na szesnaście klas. W zbiorze $S/\sim_T$ wprowadzić można strukturę algebraiczną (tzw. algebrę Lindenbauma-Tarskiego). Diagram Hassego tej struktury podany jest na następnym slajdzie. Klasa $[\varphi]_{\sim_T}$ jest pod klasą $[\psi]_{\sim_T}$ wtedy i tylko wtedy, gdy $\varphi \rightarrow \psi$ należy do T.
- Uproszczenia: zamiast klas podano ich reprezentantów, skorzystano też z tego, że $(p \rightarrow q) \equiv (\neg p \vee q)$, $(p \equiv q) \equiv (p \rightarrow q) \wedge (q \rightarrow p)$, $(p \equiv q) \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$ są tezami.


$\top$
$p \vee \neg q$
$\neg p \vee q$
$p \vee q$
$\neg p \vee \neg q$
$p \equiv q$
p
q
$\neg q$
$\neg p$
$p \not\equiv q$
$p \wedge q$
$\neg p \wedge \neg q$
$p \wedge \neg q$
$\neg p \wedge q$
$\bot$

- Algebrę $(A, \circ)$ z działaniem dwuargumentowym $\circ$ nazywamy *grupą*, gdy:
  1. $\circ$ jest łączne
  2. $\circ$ ma element neutralny
  3. dla każdego elementu $x \in A$ istnieje element odwrotny x^{-1} względem działania $\circ$.
- Jeśli $\circ$ jest przemienne, to grupę $(A, \circ)$ nazywamy *przemienną* (*abelową*).
- Dla przykładu, wszystkie bijekcje zbioru A na A tworzą grupę, ze złożeniem odwzorowań jako działaniem grupowym. Wtedy elementem neutralnym jest bijekcja identycznościowa, a elementem odwrotnym do danego elementu jest bijekcja do niego odwrotna.

- Algebrę $(A, \oplus, \otimes)$ nazywamy *pierścieniem*, gdy $\oplus$ oraz $\otimes$ są działaniami dwuargumentowymi takimi, że:
  1. $(A, \oplus)$ jest grupą abelową
  2. $\otimes$ jest łączne
  3. $\otimes$ jest lewo- oraz prawostronnie rozdzielne względem $\oplus$.
- Liczby całkowite z operacjami dodawania i mnożenia tworzą pierścień. Macierze kwadratowe z operacjami ich dodawania i mnożenia tworzą pierścień.
- Jeśli $\otimes$ ma element neutralny, to pierścień $(A, \oplus, \otimes)$ nazywamy *pierścieniem z jednością*.
- Mówimy, że element $x \neq \mathbf{0}$ pierścienia $(A, \oplus, \otimes)$ jest *właściwym dzielnikiem zera*, gdy istnieje $y \in A - \{\mathbf{0}\}$ taki, że $x \otimes y = \mathbf{0}$, gdzie $\mathbf{0}$ jest elementem neutralnym względem $\oplus$. Np. w pierścieniu klas reszt modulo 6 właściwymi dzielnikami zera są 2 i 3.
- Pierścienie (z przemiennym mnożeniem) z jednością oraz bez właściwych dzielników zera nazywamy *dziedzinami całkowitości* (np.: liczby całkowite).

- Algebrę $(A, \oplus, \otimes)$, gdzie A ma co najmniej dwa elementy, nazywamy *ciałem*, gdy $\oplus$ oraz $\otimes$ są działaniami dwuargumentowymi takimi, że:
  1. $(A, \oplus)$ jest grupą abelową z elementem neutralnym $\mathbf{0}$
  2. $\otimes$ jest łączne i przemienne
  3. $\otimes$ ma element neutralny $\mathbf{1}$
  4. dla każdego $x \neq \mathbf{0}$ istnieje y taki, że y jest elementem odwrotnym dla x względem działania $\otimes$
  5. $\otimes$ jest rozdzielne względem $\oplus$.
- Przykłady: liczby wymierne $\mathbb{Q}$, rzeczywiste $\mathbb{R}$, zespolone $\mathbb{C}$, ciało funkcji wymiernych, ze stosownie określonymi operacjami arytmetycznymi.
- Najmniejszą liczbę n taką, że $n \otimes \mathbf{1} = \mathbf{0}$ nazywamy *charakterystyką* ciała $(A, \oplus, \otimes)$. Jeżeli nie istnieje n taka, że $n \otimes \mathbf{1} = \mathbf{0}$, to mówimy, że ciało $(A, \oplus, \otimes)$ ma *charakterystykę* 0.

- Ciało jest *algebraicznie domknięte*, jeśli każdy wielomian stopnia co najmniej pierwszego jednej zmiennej ma pierwistek w tym ciele.
- Ciało jest *rzeczywiście domknięte*, gdy istnieje w nim porządek liniowy taki, że każdy element dodatni ma pierwiastek kwadratowy w tym ciele i każdy wielomian nieparzystego stopnia o współczynnikach z tego ciała ma w nim pierwiastek.
- Liczby rzeczywiste tworzą ciało rzeczywiście domknięte, ale nie algebraicznie domknięte. Jest to jedyne (z dokładnością do izomorfizmu) ciało uporządkowane w sposób zupełny. Jest też największym ciałem uporządkowanym K spełniającym aksjomat Archimedesa: $\forall a \in K \forall b \in K \exists n \in \mathbb{N}(0 < a < b \rightarrow b < n \cdot a)$.
- Liczby zespolone tworzą ciało algebraicznie domknięte. Nie istnieje w tym ciele porządek zgodny z działaniami arytmetycznymi.
- Ciało liczb hiperrzeczywistych nie jest archimedesowe.

- Niech $\mathbf{A} = (A, \omega_1^{\mathbf{A}}, \ldots, \omega_n^{\mathbf{A}})$ będzie algebrą sygnatury (Ω, τ). Mówimy, że algebra $\mathbf{B} = (B, \omega_1^{\mathbf{B}}, \ldots, \omega_n^{\mathbf{B}})$ jest podalgebrą algebry $\mathbf{A}$, gdy:
  1. $B \subseteq A$ i B jest zamknięty ze względu na wszystkie operacje $\omega_i^{\mathbf{A}}$
  2. $\omega_i^{\mathbf{B}} = \omega_i^{\mathbf{A}} \upharpoonright B^{\tau(\omega_i)}$, gdzie symbol $f \upharpoonright X$ oznacza ograniczenie funkcji f do zbioru X.
- Zbiór wszystkich podalgebr algebry $\mathbf{A}$ oznaczamy przez $Sub(\mathbf{A})$. Jeśli $\mathbf{B} \in Sub(\mathbf{A})$, to piszemy $\mathbf{B} \leqslant \mathbf{A}$.
- Jeśli $\emptyset \neq \{\mathbf{B}_j : j \in J\} \subseteq Sub(\mathbf{A})$, to $\mathbf{B} = (\bigcap\limits_{j \in J} dom(\mathbf{B}_j), \omega_1^{\mathbf{B}}, \ldots, \omega_n^{\mathbf{B}}) \in Sub(\mathbf{A})$, gdzie $\omega_i^{\mathbf{B}} = \omega_i^{\mathbf{A}} \upharpoonright (\bigcap\limits_{j \in J} dom(\mathbf{B}_j))^{\tau(\omega_i)}$.
- Jeśli $\emptyset \neq \{\mathbf{B}_j : j \in J\} \subseteq Sub(\mathbf{A})$ i $dom(\mathbf{B}_{j_1}) \subseteq dom(\mathbf{B}_{j_2})$ lub $dom(\mathbf{B}_{j_2}) \subseteq dom(\mathbf{B}_{j_1})$ dla wszystkich $j_1, j_2 \in J$, to $\mathbf{B} = (\bigcup\limits_{j \in J} dom(\mathbf{B}_j), \omega_1^{\mathbf{B}}, \ldots, \omega_n^{\mathbf{B}}) \in Sub(\mathbf{A})$, gdzie $\omega_i^{\mathbf{B}} = \omega_i^{\mathbf{A}} \upharpoonright (\bigcup\limits_{j \in J} dom(\mathbf{B}_j))^{\tau(\omega_i)}$.

- Niech $\mathbf{A} = (A, \omega_1^{\mathbf{A}}, \ldots, \omega_n^{\mathbf{A}})$ będzie algebrą i niech $X \subseteq A$.
- Przez $Sg^{\mathbf{A}}(X)$ oznaczamy najmniejszą podalgebrę algebry $\mathbf{A}$, której uniwersum zawiera zbiór X.
- Określamy zbiory X_m:
  1. $X_0 = X$
  2. $X_{m+1} = X_m \cup \{\omega_i^{\mathbf{A}}(a_1, \ldots, a_{\tau(\omega_i)}) : 1 \leqslant i \leqslant n \wedge a_1, \ldots, a_{\tau(\omega_i)} \in X_m\}$
- Wtedy $\bigcup\limits_{m \geqslant 0} X_m$ jest uniwersum algebry $Sg^{\mathbf{A}}(X)$.
- Mówimy, że zbiór X jest zbiorem generatorów algebry $\mathbf{A}$, gdy $Sg^{\mathbf{A}}(X) = \mathbf{A}$. Algebra jest skończenie generowana, gdy ma skończony zbiór generatorów.
- Niech $\mathbf{A}$ będzie algebrą i niech $X \subseteq dom(\mathbf{A})$ oraz $a \in dom(\mathbf{A})$. Wtedy: $a \in dom(Sg^{\mathbf{A}}(X))$ wtedy i tylko wtedy, gdy $a \in dom(Sg^{\mathbf{A}}(Y))$ dla pewnego skończonego $Y \subseteq X$.

- $(\{1, 2, 3, 5, 6, 10.15, 30\}, NWD(x, y), NWW(x, y))$ jest podalgebrą algebry $(\{n \in \mathbb{N} : 1 \leqslant n\}, NWD(x, y), NWW(x, y))$.
- Liczby całkowite $(\mathbb{Z}, +, \cdot, 0, 1)$ z dodawaniem i mnożeniem tworzą podalgebrę algebry liczb wymiernych $(\mathbb{Q}, +, \cdot, 0, 1)$ z dodawaniem i mnożeniem. Zauważmy różnicę: $(\mathbb{Q}, +, \cdot, 0, 1)$ jest ciałem, a $(\mathbb{Z}, +, \cdot, 0, 1)$ jest pierścieniem.
- Zbiorem generatorów algebry $\mathbf{S} = (S, \circ_1, \ldots, \circ_n)$ języka zdaniowego jest zbiór wszystkich zmiennych zdaniowych tego języka.
- Zbiór wszystkich *symetrii* trójkąta równobocznego ma sześć elementów: przekształcenie identycznościowe (obrót o 0°), obrót o 120°, obrót o 240° (oba względem środka trójkąta) oraz trzy symetrie względem prostych zawierających wysokości tego trójkąta. Operacją na tym zbiorze jest składanie przekształceń. Podalgebrą tej algebry jest zbiór złożony z przekształcenia identycznościowego oraz obu wspomnianych obrotów, z operacją składania przekształceń.

- Zakładamy, że pojęcia injekcji, surjekcji i bijekcji są znane słuchaczom.
- Niech $\mathbf{A} = (A, \omega_1^{\mathbf{A}}, \ldots, \omega_n^{\mathbf{A}})$ i $\mathbf{B} = (B, \omega_1^{\mathbf{B}}, \ldots, \omega_n^{\mathbf{B}})$ będą algebrami sygnatury (Ω, τ).
- Mówimy, że odwzorowanie $h : A \to B$ jest homomorfizmem algebry $\mathbf{A}$ w algebrę $\mathbf{B}$, gdy dla wszystkich $\omega_i \in \Omega$ $(1 \leqslant n)$ oraz wszystkich $a_1, \ldots, a_{\tau_{\omega_i}}$: $h(\omega_i^{\mathbf{A}}(a_1, \ldots, a_{\tau_{\omega_i}})) = \omega_i^{\mathbf{B}}(h(a_1), \ldots, h(a_{\tau_{\omega_i}}))$.
- Homomorfizmy, które są bijekcjami nazywamy *izomorfizmami*. Używa się terminów:
  1. *monomorfizm* (włożenie) dla homomorfizmu, który jest injekcją;
  2. *epimorfizm* dla homomorfizmu, który jest surjekcją;
  3. *endomorfizm* dla homomorfizmu $\mathbf{A}$ w $\mathbf{A}$;
  4. *automorfizm* dla izomorfizmu $\mathbf{A}$ na $\mathbf{A}$.
- Mówimy, że algebry $\mathbf{A}$ i $\mathbf{B}$ są izomorficzne, gdy istnieje izomorfizm $\mathbf{A}$ na $\mathbf{B}$. Piszemy wtedy $\mathbf{A} \cong \mathbf{B}$.
- Niech $Hom(\mathbf{A}, \mathbf{B})$ oznacza zbiór wszystkich homomorfizmów z $\mathbf{A}$ w $\mathbf{B}$.

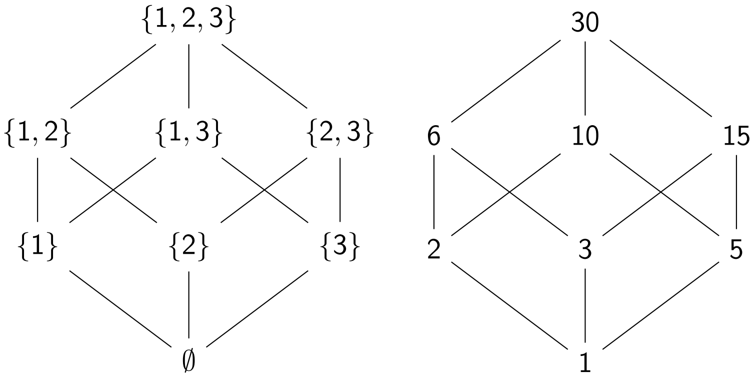
- Funkcja logarytmiczna $\ln : \mathbb{R}_+ \to \mathbb{R}$ jest homomorfizmem struktury $(\mathbb{R}_+, \cdot)$ w strukturę $(\mathbb{R}, +)$, ponieważ $\ln(x \cdot y) = \ln x + \ln y$.
- Niech $\mathbb{K}_4 = (\{e, a, b, c\}, \circ)$, gdzie $\circ$ określa tabelka z lewej:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\bullet$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

- Ta struktura (*grupa czwórkowa Kleina*) jest izomorficzna np. ze strukturą $(\wp(\{x, y\}), \div)$, czyli rodziną wszystkich podzbiorów dowolnego zbioru dwuelementowego wraz z operacją różnicy symetrycznej zbiorów $\div$. Ćwiczenie: określ ten izomorfizm.
- $\mathbb{K}_4$ nie jest izomorficzna ze strukturą $C_4 = (\{e, a, b, c\}, \bullet)$ (*grupą cykliczną rzędu cztery*), gdzie działanie $\bullet$ jest zdefiniowane tabelą z prawej.

Algebra $(\wp(\{1,2,3\}), \cap, \cup)$ jest izomorficzna z algebrą $(\{1,2,3,5,6,10,15,30\}, NWD(x,y), NWW(x,y))$:



Homomorfizmy i izomorfizmy określamy także dla dowolnych struktur relacyjnych, co później wykorzystamy.

- Niech $\mathbf{A} = (A, \omega_1^{\mathbf{A}}, \ldots, \omega_n^{\mathbf{A}})$ będzie algebrą, a θ relacją równoważności na A.
- Mówimy, że θ jest kongruencją algebry $\mathbf{A}$, gdy dla wszystkich $1 \leqslant i \leqslant n$ oraz wszystkich $a_1, b_1, \ldots, a_{\tau_{\omega_i}}, b_{\tau_{\omega_i}} \in A$:
  jeżeli $a_1 \theta b_1$, …,$a_{\tau_{\omega_i}} \theta b_{\tau_{\omega_i}}$, to $\omega_i^{\mathbf{A}}(a_1, \ldots, a_{\tau_{\omega_i}}) \theta \omega_i^{\mathbf{A}}(b_1, \ldots, b_{\tau_{\omega_i}})$.
- Najmniejszą (względem inkluzji) kongruencją w strukturze $\mathbf{A}$ jest relacja identyczności na zbiorze $dom(\mathbf{A})$ (oznaczana przez $0_{\mathbf{A}}$), a największą taką kongruencją jest relacja pełna w zbiorze $dom(\mathbf{A})$ (oznaczana przez $1_{\mathbf{A}}$). Zbiór wszystkich kongruencji algebry $\mathbf{A}$ będziemy oznaczali przez $Con(\mathbf{A})$.

Określona na slajdzie 7 relacja $\sim^3$ jest kongruencją algebry $(\mathbb{N}, \oplus^3, \otimes^3)$.
Określona na slajdzie 8 relacja $\sim_T$ jest kongruencją algebry języka klasycznego rachunku zdań (w którego formułach występują tylko zmienne p i q).
Relacja równoliczności zbiorów, określona w rodzinie wszystkich podzbiorów dowolnego zbioru X jest kongruencją struktury $(\wp(X), \cup, \cap)$.

- Niech $\mathbf{A} = (A, \omega_1^{\mathbf{A}}, \ldots, \omega_n^{\mathbf{A}})$ będzie algebrą, a θ kongruencją algebry $\mathbf{A}$.
- Algebrą ilorazową nazywamy algebrę $\mathbf{A}/\theta = (A/\theta, \omega_1^{\mathbf{A}/\theta}, \ldots, \omega_n^{\mathbf{A}/\theta})$, której operacje określone są warunkami (dla wszystkich $1 \leqslant i \leqslant n$ oraz $a_1, \ldots, a_{\tau_{\omega_i}} \in A$):
$\omega_i^{\mathbf{A}/\theta}([a_1]_\theta, \ldots, [a_{\tau_{\omega_i}}]_\theta) = [\omega_i^{\mathbf{A}}(a_1, \ldots, a_{\tau_{\omega_i}})]_\theta$.
- Poprawność tej definicji wynika z faktu, że θ jest kongruencją algebry $\mathbf{A}$. Jeśli $a_1 \theta b_1$, …,$a_{\tau_{\omega_i}} \theta b_{\tau_{\omega_i}}$, to $\omega_i^{\mathbf{A}}(a_1, \ldots, a_{\tau_{\omega_i}}) \theta \omega_i^{\mathbf{A}}(b_1, \ldots, b_{\tau_{\omega_i}})$, a więc wartość operacji w algebrze ilorazowej jest dobrze określona.
- Dla uproszczenia zapisu, często klasę abstrakcji $[a]_\theta$ elementu a oznacza się przez a/θ.
- Kongruencje związane są z homomorfizmami algebr. Każda funkcja $f : A \to B$ wyznacza pewną relacje równoważności na A. Definiujemy mianowicie: $x \sim_f y$ wtedy i tylko wtedy, gdy $f(x) = f(y)$.

- Jeśli $f : \mathbf{A} \to \mathbf{B}$ jest homomorfizmem, to relacja $\sim_f \subseteq (dom(\mathbf{A}))^2$ zdefiniowana wzorem: $x \sim_f y$ wtedy i tylko wtedy, gdy $f(x) = f(y)$ jest kongruencją algebry $\mathbf{A}$.
- Jeśli, z drugiej strony, θ jest kongruencją algebry $\mathbf{A}$, to *odwzorowanie kanoniczne* $k_\theta : \mathbf{A} \to \mathbf{A}/\theta$ dane wzorem $k_\theta(a) = a/\theta$ jest homomorfizmem.
- Tak więc, dla dowolnej algebry $\mathbf{A}$:
  1. Każdy obraz homomorficzny algebry $\mathbf{A}$ jest izomorficzny z pewną algebrą ilorazową algebry $\mathbf{A}$.
  2. Każda algebra ilorazowa algebry $\mathbf{A}$ jest izomorficzna z pewnym homomorficznym obrazem algebry $\mathbf{A}$.
- Mówimy, że algebra $\mathbf{A}$ jest *prosta*, jeśli ma tylko dwie kongruencje: identyczność na $dom(\mathbf{A})$ oraz relację pełną na tym zbiorze.
- Algebra $\mathbf{A}$ jest prosta wtedy i tylko wtedy, gdy ma dokładnie dwa (z dokładnością do izomorfizmu) obrazy homomorficzne: samą siebie oraz algebrę *zdegenerowaną*, czyli jednoelementową.

- Rozważmy strukturę $(\wp(\mathbb{N}), \cup, \cap)$ oraz relację $\sim$, zdefiniowaną następująco: $A \sim B$ wtedy i tylko wtedy, gdy $1 \in A \cap B$ lub $1 \in \mathbb{N} - (A \cup B)$.
- Relacja $\sim$ jest równoważnością i ma dokładnie dwie klasy abstrakcji: $[\mathbb{N}]_\sim$ oraz $[\emptyset]_\sim$.
- Relacja ta jest też kongruencją w strukturze $(\wp(\mathbb{N}), \cup, \cap)$, możemy więc określić działania $\cup^\sim$ oraz $\cap^\sim$ na jej klasach abstrakcji:

$\cup^\sim$	$[\emptyset]_\sim$	$[\mathbb{N}]_\sim$
$[\emptyset]_\sim$	$[\emptyset]_\sim$	$[\mathbb{N}]_\sim$
$[\mathbb{N}]_\sim$	$[\mathbb{N}]_\sim$	$[\mathbb{N}]_\sim$

$\cap^\sim$	$[\emptyset]_\sim$	$[\mathbb{N}]_\sim$
$[\emptyset]_\sim$	$[\emptyset]_\sim$	$[\emptyset]_\sim$
$[\mathbb{N}]_\sim$	$[\emptyset]_\sim$	$[\mathbb{N}]_\sim$

- *Konstrukcja liczb całkowitych*. Dana jest algebra $(\mathbb{N}, +, \cdot)$. Określamy relację $\approx_1 \subseteq (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N})$:
- $(x, y) \approx_1 (u, v)$ wtedy i tylko wtedy, gdy $x + v = u + y$.
- $\approx_1$ jest równoważnością. Niech $\mathbb{Z} = \mathbb{N}^2 / \approx_1$ (liczby całkowite).
- Odwzorowanie $\varphi_1 : \mathbb{N} \to \mathbb{Z}$ określone wzorem $\varphi_1(k) = [(k, 0)]_{\approx_1}$ jest injekcją.
- Ponieważ $\approx_1$ jest kongruencją, więc możemy określić działania w $\mathbb{Z}$:
    1. $[(x, y)]_{\approx_1} \oplus_1 [(u, v)]_{\approx_1} = [x + u, y + v]_{\approx_1}$
    2. $[(x, y)]_{\approx_1} \odot_1 [(u, v)]_{\approx_1} = [x \cdot u + y \cdot v, u \cdot y + x \cdot v]_{\approx_1}$.
- Odwzorowanie φ_1 jest homomorfizmem algebry $(\mathbb{N}, +, \cdot)$ w algebrę $(\mathbb{Z}, \oplus_1, \odot_1)$, czyli $\varphi_1(m) \oplus_1 \varphi_1(n) = \varphi_1(m + n)$ oraz $\varphi_1(m) \odot_1 \varphi_1(n) = \varphi_1(m \cdot n)$.
- W $\mathbb{Z}$ można określić odejmowanie $\ominus_1$ i porządek $\leqslant_1$:
  $[(x, y)]_{\approx_1} \ominus_1 [(u, v)]_{\approx_1} = [x + v, y + u]_{\approx_1}$
  $[(x, y)]_{\approx_1} \leqslant_1 [(u, v)]_{\approx_1}$ wtedy i tylko wtedy, gdy $x + v \leqslant y + u$.

- Proponujemy słuchaczom samodzielne zmierzenie się z wykazaniem poprawności wyżej określonych działań oraz wykazaniem, że φ_1 jest homomorfizmem.
- $(\{[(x, 0)]_{\approx_1} : x \in \mathbb{N}\}, \oplus_1, \odot_1)$ jest podalgebrą algebry $(\mathbb{Z}, \oplus_1, \odot_1)$ i jest izomorficzna z $(\mathbb{N}, +, \cdot)$. Są to nieujemne liczby całkowite. Fakt ten skłania do pewnych uproszczeń w notacji liczb całkowitych:
  1. zamiast $[(x, 0)]_{\approx_1}$ piszemy po prostu x
  2. zamiast $[(0, x)]_{\approx_1}$ piszemy po prostu $-x$
  3. przyjmując powyższe uproszczenia, możemy napisać: $\mathbb{Z} = \mathbb{N} \cup \{-x : x \in \mathbb{N}\}$, co jest bliskie praktyce szkolnej.
- Podana wyżej definicja pochodzi od Hermanna Grassmanna (1809–1877), który podał również opis aksjomatyczny liczb całkowitych.

- *Konstrukcja liczb wymiernych*. Dana jest algebra $(\mathbb{Z}, \oplus_1, \odot_1)$. Określamy relację $\approx_2 \subseteq (\mathbb{Z} \times (\mathbb{Z} - \{0\})) \times (\mathbb{Z} \times (\mathbb{Z} - \{0\}))$:
- $(x, y) \approx_2 (u, v)$ wtedy i tylko wtedy, gdy $x \odot_1 v = y \odot_1 u$.
- $\approx_2$ jest równoważnością. Niech $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} - \{0\})) / \approx_2$ (liczby wymierne). $\approx_2$ jest kongruencją, więc możemy zdefiniować działania w algebrze ilorazowej w znany już sposób, a także wprowadzić nowe działanie (dzielenie):
    - $[(x, y)]_{\approx_2} \oplus_2 [(u, v)]_{\approx_2} = [((x \odot_1 v) \oplus_1 (y \odot_1 u), (y \odot_1 v)]_{\approx_2}$
    - $[(x, y)]_{\approx_2} \ominus_2 [(u, v)]_{\approx_2} = [((x \odot_1 v) \ominus_1 (y \odot_1 u), (y \odot_1 v)]_{\approx_2}$
    - $[(x, y)]_{\approx_2} \odot_2 [(u, v)]_{\approx_2} = [(x \odot_1 u, y \odot_1 v)]_{\approx_2}$
    - $[(x, y)]_{\approx_2} \oslash_2 [(u, v)]_{\approx_2} = [x \odot_1 v, y \odot_1 u]_{\approx_2}$, o ile $[(u, v)]_{\approx_2} \neq [(0, 1)]_{\approx_2}$.
- Odwzorowanie $\varphi_2 : \mathbb{Z} \to \mathbb{Q}$ określone wzorem $\varphi_2(x) = [(x, 1)]_{\approx_2}$ jest monomorfizmem.

- Dla każdej liczby wymiernej $[(x, y)]_{\approx_2}$ mamy: $[(x, y)]_{\approx_2} = [(x, 1)]_{\approx_2} \oslash_2 [(y, 1)]_{\approx_2}$.
- Liczbę wymierną $[(x, 1)]_{\approx_2}$, na mocy Tradycji i faktu, że φ_2 jest izomorfizmem $(\mathbb{Z}, \oplus_1, \odot_1)$ na $(\{[(x, 1)]_{\approx_2} : x \in \mathbb{Z}\}, \oplus_2, \odot_2)$, zwykle utożsamiamy z liczbą całkowitą x.
- Liczbę wymierną $[(x, y)]_{\approx_2}$ zapisać możemy więc w znany ze szkoły sposób, jako ułamek $\frac{x}{y}$. Wtedy:
- $\mathbb{Q} = \{\frac{x}{y} : x \in \mathbb{Z} \text{ oraz } y \in \mathbb{Z} - \{0\}\}$.

Obie powyższe konstrukcje systemów liczbowych przytaczamy jedynie jako ilustrację wykorzystania kongruencji w tworzeniu algebr ilorazowych. Jedna z konstrukcji liczb rzeczywistych (ta podana przez Cantora) także wykorzystuje konstrukcje ilorazowe (punktem wyjścia są nieskończone ciągi liczb wymiernych). W praktyce matematycznej posługujemy się raczej aksjomatycznym wprowadzeniem różnych systemów liczbowych.

- Jeśli $f : \mathbf{A} \rightarrow \mathbf{B}$ jest homomorfizmem, to relację $ker_f \subseteq dom(\mathbf{A}) \times dom(\mathbf{A})$ określoną warunkiem $x\ ker_f\ y$ wtedy i tylko wtedy, gdy $f(x) = f(y)$ nazywamy jądrem homomorfizmu f. Relacja ta jest kongruencją algebry $\mathbf{A}$.
- Jeśli θ jest dowolną kongruencją algebry $\mathbf{A}$, to niech k_θ będzie odwzorowaniem algebry $\mathbf{A}$ na algebrę ilorazową $\mathbf{A}/\theta$ określonym warunkiem: $k_\theta(x) = [x]_\theta$. Wtedy odwzorowanie to jest homomorfizmem $\mathbf{A}$ na $\mathbf{A}/\theta$, nazywanym homorfizmem kanonicznym, a jego jądrem jest kongruencja θ.

Twierdzenie (o homomorfizmie). Niech $\mathbf{A}$, $\mathbf{B}$ i $\mathbf{C}$ będą algebrami tego samego typu. Niech dalej $f : \mathbf{A} \rightarrow \mathbf{B}$ będzie homomorfizmem, a $g : \mathbf{A} \rightarrow \mathbf{C}$ będzie homomorfizmem surjektywnym, przy czym $ker_g \subseteq ker_f$. Wtedy istnieje dokładnie jeden homomorfizm $h : \mathbf{C} \rightarrow \mathbf{B}$ taki, że $h \circ g = f$.

$$\begin{tikzcd}
\mathbf{A} \arrow[r, "f"] \arrow[d, "g"'] & \mathbf{B} \\
\mathbf{C} \arrow[ur, "h"'] &
\end{tikzcd}$$

Dowód. Niech $h = \{(g(a), f(a)) : a \in A\}$. Pokażemy, że: h jest funkcją, nadto jedyną funkcją taką, że $h \circ g = f$, i wreszcie, że h jest homomorfizmem $\mathbf{C}$ w $\mathbf{B}$.

Jeśli $g(a) = g(b)$, to $(a, b) \in ker_g$, a zatem także $(a, b) \in ker_f$, co oznacza, że $f(a) = f(b)$. Widać więc, że relacja h jest funkcją. Jej dziedziną jest C, ponieważ g jest surjekcją. Ponadto, $h(g(a)) = f(a)$ dla dowolnego $a \in A$, czyli $h \circ g = f$. Niech $h' \circ g = f$. Wtedy dla dowolnego $c \in C$ istnieje $a \in A$ takie, że $g(a) = c$. Ponadto:

$h'(c) = h'(g(a)) = (h' \circ g)(a) = f(a) = (h \circ g)(a) = h(g(a)) = h(c)$, czyli $h = h'$, co oznacza, że funkcja h jest wyznaczona jednoznacznie.

Niech ω będzie dowolnym m-argumentowym symbolem funkcyjnym z sygnatury rozważanych algebr oraz niech $c_1, \ldots, c_m \in C$. Ponieważ g jest surjekcją, więc istnieją $a_1, \ldots, a_m \in A$ takie, że $g(a_i) = c_i$ dla wszystkich $1 \leqslant i \leqslant m$. Na mocy tego, że f i g są homomorfizmami, mamy:

$$
\begin{array}{l}
h(\omega^{\mathbf{C}}(c_1, \ldots, c_m)) = \\
h(\omega^{\mathbf{C}}(g(a_1), \ldots, g(a_m))) = \\
h(g(\omega^{\mathbf{A}}(a_1, \ldots, a_m))) = \\
(h \circ g)(\omega^{\mathbf{A}}(a_1, \ldots, a_m)) = \\
f(\omega^{\mathbf{A}}(a_1, \ldots, a_m)) = \\
\omega^{\mathbf{B}}(f(a_1), \ldots, f(a_m)) = \\
\omega^{\mathbf{B}}((h \circ g)(a_1), \ldots, (h \circ g)(a_m)) = \\
\omega^{\mathbf{B}}(h(g(a_1)), \ldots, h(g(a_m))) = \\
\omega^{\mathbf{B}}(h(c_1), \ldots, h(c_m)).
\end{array}
$$

A zatem h jest homomorfizmem $\mathbf{C}$ w $\mathbf{B}$.

□

Twierdzenie (pierwsze o izomorfizmie). Niech $f : \mathbf{A} \to \mathbf{B}$ będzie surjektywnym homomorfizmem. Jeśli $\theta = ker_f$, to istnieje dokładnie jeden izomorfizm $h : \mathbf{A}/\theta \to \mathbf{B}$ taki, że $h \circ k_\theta = f$.

$$\begin{tikzcd}
\mathbf{A} \arrow[r, "f"] \arrow[d, "k_\theta"'] & \mathbf{B} \\
\mathbf{A}/\theta \arrow[ur, "h"'] &
\end{tikzcd}$$

Dowód. Ponieważ z założenia $\theta = ker_{k_\theta} = ker_f$, więc korzystając z poprzedniego twierdzenia wiemy, że istnieje dokładnie jeden homomorfizm $h : \mathbf{A}/\theta \to \mathbf{B}$ taki, że $h \circ k_\theta = f$. Trzeba pokazać, że h jest bijekcją.

- Ponieważ f jest surjekcją, więc dla każdego $b \in B$ istnieje $a \in A$ taki, że $f(a) = b$.
- Mamy zatem:

$$b = f(a) = (h \circ k_\theta)(a) = h(k_\theta(a)) = h([a]_\theta),$$

  czyli h jest surjekcją.
- Przypuśćmy, że $h(a/\theta) = h(b/\theta)$.
- Wtedy $f(a) = f(b)$, co oznacza, że $(a, b) \in ker_f = \theta$.
- A zatem $a/\theta = b/\theta$, czyli h jest injekcją.

$\square$

Niech θ i ϕ będą kongruencjami algebry **A** i załóżmy, że $\theta \subseteq \phi$. W zbiorze ilorazowym A/θ określamy relację ϕ/θ warunkiem: $(x/\theta, y/\theta) \in \phi/\theta$ wtedy i tylko wtedy, gdy $(x, y) \in \phi$. Wtedy ϕ/θ jest kongruencją algebry ilorazowej $\mathbf{A}/\theta$, ponieważ:

1. ϕ/θ jest relacją równoważności na A, co wynika bezpośrednio z definicji.
2. Niech $\omega^{\mathbf{A}}$ będzie dowolną operacją m-argumentową algebry **A** oraz niech $a_1, b_1, \ldots, a_m, b_m \in A$ będą takie, że $(a_i/\theta, b_i/\theta) \in \phi/\theta$ dla wszystkich $1 \leqslant i \leqslant m$. Oznacza to, że $(a_i, b_i) \in \phi$ dla wszystkich $1 \leqslant i \leqslant m$. Ponieważ ϕ jest kongruencją, więc mamy $(\omega^{\mathbf{A}}(a_1, \ldots, a_m), \omega^{\mathbf{A}}(b_1, \ldots, b_m)) \in \phi/\theta$, czyli ϕ/θ jest kongruencją algebry ilorazowej $\mathbf{A}/\theta$.

Twierdzenie (drugie o izomorfizmie). Niech θ i ϕ będą kongruencjami algebry **A** takimi, że $\theta \subseteq \phi$. Wtedy algebry $\mathbf{A}/\phi$ i $(\mathbf{A}/\theta)/(\phi/\theta)$ są izomorficzne.

$$\begin{tikzcd} \mathbf{A} \arrow[r, "k_\phi"] \arrow[d, "k_\theta"'] & \mathbf{A}/\phi \\ \mathbf{A}/\theta \arrow[ur, "h"'] & \end{tikzcd}$$

- **Dowód**. Wykorzystamy twierdzenie o homomorfizmie, więc wygodnie przyjąć oznaczenia dla odwzorowań kanonicznych i algebr ilorazowych: $f = k_\phi$, $g = k_\theta$, $\mathbf{B} = \mathbf{A}/\phi$, $\mathbf{C} = \mathbf{A}/\theta$.
- Wtedy $f : \mathbf{A} \to \mathbf{B}$ oraz $g : \mathbf{A} \to \mathbf{C}$.
- Z założenia $ker_g = \theta \subseteq \phi = ker_f$.
- Spełnione są zatem założenia twierdzenia o homomorfizmie, czyli istnieje homomorfizm $h : \mathbf{C} \to \mathbf{B}$ (a więc $h : \mathbf{A}/\theta \to \mathbf{A}/\phi$) taki, że $h \circ g = f$.

Pokażemy, że $ker_h = \phi/\theta$. Mamy mianowicie następujący ciąg równoważności:

1. $(a/\theta, b/\theta) \in ker_h$ wtedy i tylko wtedy, gdy
2. $h(a/\theta) = h(b/\theta)$ wtedy i tylko wtedy, gdy
3. $(h \circ g)(a) = (h \circ g)(b)$ wtedy i tylko wtedy, gdy
4. $f(a) = f(b)$ wtedy i tylko wtedy, gdy
5. $a/\phi = b/\phi$ wtedy i tylko wtedy, gdy
6. $(a, b) \in \phi$ wtedy i tylko wtedy, gdy
7. $(a/\theta, b/\theta) \in \phi/\theta$.

Tak więc, $ker_h = \phi/\theta$. Skoro f i g są surjekcjami, to $h(A/\theta) = A/\phi$. Teza naszego twierdzenia wynika zatem z pierwszego twierdzenia o izomorfizmie.

$\square$

Twierdzenie (trzecie o izomorfizmie). Niech **B** będzie podalgebrą algebry **A**, a θ kongruencją algebry **A**. Oznaczmy: $B\theta = \{a \in A : \exists b \in B\ a\theta b\}$ i niech **B**θ będzie algebrą generowaną przez $B\theta$. Wtedy **B**θ jest podalgebrą algebry **A** i algebry $\mathbf{B}/(\theta \cap B^2)$ oraz $\mathbf{B}\theta/(\theta \cap (B\theta)^2)$ są izomorficzne.

Dowód. Udowodnimy najpierw, że **B**θ jest podalgebrą algebry **A**.

- Niech ω będzie operacją m-argumentową i niech $a_1, \ldots, a_m \in B\theta$. Wtedy istnieją $b_1, \ldots, b_m \in B$ takie, że $(a_i, b_i) \in \theta$ dla wszystkich $1 \leqslant i \leqslant m$. Ponieważ θ jest kongruencją, więc: $(\omega^{\mathbf{A}}(a_1, \ldots, a_m), \omega^{\mathbf{A}}(b_1, \ldots, b_m)) \in \theta$.
- Mamy $\omega^{\mathbf{A}}(b_1, \ldots, b_m) \in B$, ponieważ **B** jest podalgebrą algebry **A**.
- Z tego otrzymujemy, że $\omega^{\mathbf{A}}(a_1, \ldots, a_m) \in B\theta$.
- Pokazaliśmy, że zbiór $B\theta$ jest zamknięty na operacje algebry **A**, a więc **B**θ jest podalgebrą algebry **A**.

Udowodnimy teraz, że algebry $\mathbf{B}/(\theta \cap B^2)$ oraz $\mathbf{B}\theta/(\theta \cap (B\theta)^2)$ są izomorficzne.

- Ponieważ θ jest kongruencją w $\mathbf{A}$ oraz $\mathbf{B}\theta$ jest podalgebrą algebry $\mathbf{A}$, więc $\psi = \theta \cap (B\theta)^2$ jest kongruencją algebry $\mathbf{B}\theta$.
- Niech $h : B \to B\theta/\psi$ będzie odwzorowaniem określonym wzorem $h(b) = b/\psi$. Pokażemy, że h jest homomorfizmem algebry $\mathbf{B}$ na algebrę $\mathbf{B}\theta/\psi$.
- Niech ω będzie operacją m-argumentową i niech $b_1, \ldots, b_m \in B$. Mamy wtedy:
  1. $h(\omega^{\mathbf{B}}(b_1, \ldots, b_m)) =$
  2. $\omega^{\mathbf{B}}(b_1, \ldots, b_m)/\psi =$
  3. $\omega^{\mathbf{B}\theta}(b_1, \ldots, b_m)/\psi =$
  4. $\omega^{\mathbf{B}\theta/\psi}(b_1/\psi, \ldots, b_m/\psi) =$
  5. $\omega^{\mathbf{B}\theta/\psi}(h(b_1, \ldots, h(b_m)))$.

- Oznacza to, że h jest homorfizmem algebry $\mathbf{B}/(\theta \cap B^2)$ na algebrę $\mathbf{B}\theta/(\theta \cap (B\theta)^2)$.
- Jądrem homomorfizmu h jest $\theta \cap B^2$.
- Dla dowolnych $b_1, b_2 \in B$ mamy bowiem:
  1. $(b_1, b_2) \in ker_h$ wtedy i tylko wtedy, gdy
  2. $h(b_1) = h(b_2)$ wtedy i tylko wtedy, gdy
  3. $b_1/\psi = b_2/\psi$ wtedy i tylko wtedy, gdy
  4. $(b_1, b_2) \in \psi$.
- Tak więc, $ker_h = \psi \cap B^2 = \theta \cap (B\theta)^2 \cap B^2 = \theta \cap B^2$, ponieważ $B \subseteq B\theta$.
- Na mocy pierwszego twierdzenia o izomorfizmie, h jest zatem izomorfizmem algebr $\mathbf{B}/(\theta \cap B^2)$ oraz $\mathbf{B}\theta/(\theta \cap (B\theta)^2)$.

$\square$

Twierdzenie (o odpowiedniości). Niech $\mathbf{A}$ będzie algebrą, a θ jej kongruencją. Niech $\Gamma = \{\phi \in Con(\mathbf{A}) : \theta \subseteq \phi\}$ oraz $\Lambda = Con(\mathbf{A}/\theta)$. Wtedy odwzorowanie $f : \Gamma \to \Lambda$ dane wzorem $f(\phi) = \phi/\theta$ jest bijekcją, zachowującą inkluzję kongruencji, czyli taką, że: jeśli $\theta \subseteq \phi_1 \subseteq \phi_2$, to $f(\phi_1) \subseteq f(\phi_2)$.

- **Dowód**. Niech $g(\alpha) = \{(x, y) \in A^2 : (x/\theta, y/\theta) \in \alpha\}$, dla wszystkich $\alpha \in \Lambda$. Wtedy $g(\alpha)$ jest równoważnością na zbiorze A. Pokażemy, że $g(\alpha)$ jest kongruencją algebry $\mathbf{A}$.
- Niech zatem $\omega^{\mathbf{A}}$ będzie m-argumentową operacją algebry $\mathbf{A}$ oraz niech $a_1, b_1, \ldots, a_m, b_m \in A$ będą takie, że $(a_i/\theta, b_i/\theta) \in \alpha$ dla $1 \leqslant i \leqslant m$.
- Ponieważ α jest kongruencją algebry $\mathbf{A}/\theta$, więc: $(\omega^{\mathbf{A}/\theta}(a_1/\theta, \ldots, a_m/\theta), \omega^{\mathbf{A}/\theta}(b_1/\theta, \ldots, b_m\theta)) \in \alpha$.
- Na mocy definicji operacji w algebrze ilorazowej otrzymujemy stąd, że: $(\omega^{\mathbf{A}}(a_1, \ldots, a_m)/\theta, \omega^{\mathbf{A}}(b_1, \ldots, b_m)/\theta) \in \alpha$. To z kolei oznacza, że relacja $g(\alpha)$ jest kongruencją algebry $\mathbf{A}$.

- Zachodzi inkluzja $\theta \subseteq g(\alpha)$, a więc $g(\alpha) \in \Gamma$. Zauważmy, że:
  1. $(x/\theta, y/\theta) \in \alpha$ wtedy i tylko wtedy, gdy
  2. $(x, y) \in g(\alpha)$ wtedy i tylko wtedy, gdy
  3. $(x/\theta, y/\theta) \in g(\alpha)/\theta$.
- To pokazuje, że $\alpha = g(\alpha)/\theta$, co z kolei oznacza, że złożenie $f \circ g$ jest relacją identyczności na Λ. Podobnie, złożenie $g \circ f$ jest relacją identyczności na Γ. Funkcje spełniające takie warunki muszą być wzajemnie jednoznaczne, co wynika ze znanego faktu dotyczącego funkcji.
- Wreszcie, jeśli $\theta \subseteq \phi_1 \subseteq \phi_2$, to $\phi_1/\theta \subseteq \phi_2/\theta$, czyli: $f(\phi_1) = \phi_1/\theta \subseteq \phi_2/\theta = f(\phi_2)$.

$\square$

W języku teorii krat twierdzenie to mówi, że przedział $[\theta, \nabla_{\mathbf{A}}]$ (będący podkratą kraty kongruencji algebry $\mathbf{A}$) jest izomorficzny z kratą kongruencji algebry $\mathbf{A}/\theta$.