Notatki o algebrach początkowych

Antoni Kościelski

1 Podstawowe pojęcia algebry ogólnej

1.1 Sygnatura

Sygnaturą nazywamy zbiór symboli funkcyjnych i symboli stałych wraz z informacją o arności poszczególnych symboli funkcyjnych. Arność symbolu, to liczba naturalna związana z tym symbolem. Określa sposób zapisywania wyrażeń, w których ten symbol występuje. Symbole stałych czasem uważa się za symbole funkcyjne o arności 0.

Przykładem sygnatury może być zbiór złożony symboli $\cdot$, $^{-1}$ oraz 1 wraz z informacją, że pierwszy z wymienionych symboli ma arność 2, następny – arność 1, a ostatni jest stałą, czyli symbolem funkcyjnym o arności 0. Symbole te nic nie znaczą, natomiast możemy używać ich do tworzenia np. wyrażeń, wzorów itp.

Mówimy, że algebra A ma sygnaturę S, jeżeli symbolom funkcyjnym z S odpowiadają dokładnie działania w algebrze A i przy tym symbolowi o arności k odpowiada działanie k argumentowe, a stałym z sygnatury odpowiadają wyróżnione elementy algebry A.

Jeżeli S jest sygnaturą i A jest algebrą o sygnaturze S, to działanie z algebry A odpowiadające symbolowi f z sygnatury S będziemy oznaczać napisem f^A, a jeżeli będzie to możliwe, to także symbolem f. W takiej sytuacji symbol f będzie miał dwa znaczenia.

Przykład 1.1 Wszystkie grupy są algebrami o sygnaturze z symbolami $\cdot$, $^{-1}$ i 1 o wyżej określonej arności. Dotyczy to także grupy liczb całkowitych Z z dodawaniem. Wtedy $\cdot^Z = +$ ($\cdot$ to znak, a $+$ to funkcja, która parze liczb przyporządkowuje ich sumę), a $1^Z = 0$. Rzecz jasna, na ogół staramy unikać się takich sytuacji, jak w tym przykładzie.

1.2 Wyrażenia, czyli termy

Przypuśćmy, że mamy sygnaturę S. Niech X będzie zbiorem symboli zmiennych (używanych np. do oznaczania bliżej nieokreślonych elementów). Zbiór wyrażeń (termów) $\mathcal{T}_X$ nad sygnaturą S i ze zmiennymi ze zbioru X jest to najmniejszy spośród zbiorów T, które mają następujące własności:

1. jeżeli x jest zmienną ze zbioru X ($x \in X$), to $x \in T$,
2. jeżeli a jest stałą z sygnatury S, to $a \in T$,
3. jeżeli f jest symbolem funkcyjnym z sygnatury S i ma arność n, a $t_1, \ldots, t_n \in T$, to $f(t_1, \ldots, t_n) \in T$.

Przykład 1.2 Sposób zapisu złożonych termów zaproponowany w definicji zapewnia możliwość jednoznacznego odczytania z termu jego budowy. Na ogół jednak piszemy inaczej. Na

przykład, nie piszemy $\cdot(x, y)$, a raczej $x \cdot y$. Przy takiej notacji napis $x \cdot y \cdot z$ nie opisuje jednoznacznie termu. Może on znaczyć $(x \cdot y) \cdot z$ albo $x \cdot (y \cdot z)$. Termy te są różne. Jest to wyraźnie widoczne, jeżeli posłużymy się zapisem użytym w definicji termu. Podane termy będą miały wtedy postać $\cdot(\cdot(x, y), z)$ i odpowiednio $\cdot(x, \cdot(y, z))$. Uwzględnianie tradycyjnego zapisu wyrażeń prowadzi do zawiłej definicji termu. Wobec tego, za podstawową definicję termu będę uważał przytoczoną, ale będę posługiwać się także zwykłym zapisem. Wtedy będę zakładać, że wszyscy potrafią się domyśleć, jaka jest rzeczywista postać niezbyt dokładnie opisanych termów. W szczególności, napis $x \cdot y \cdot z$ użyty wtedy, gdy mówimy o termach, będzie oznaczać jeden z podanych termów, np. $\cdot(\cdot(x, y), z)$. Przykładem termu używającego sygnatury grup ze zmiennymi x, y i z może być napis

$$((x \cdot y)^{-1} \cdot (1 \cdot z))^{-1} \cdot (x^{-1} \cdot z).$$

1.3 Algebra wyrażeń (termów)

Niech $\mathcal{T}_X$ oznacza zbiór wyrażeń, czyli termów, zbudowanych za pomocą symboli z sygnatury S ze zmiennymi ze zbioru X. Zbiór ten jest uniwersum algebry zwanej algebrą termów. Jest to algebra o sygnaturze S. Stała a z sygnatury S oznacza w algebrze termów term a. Tak więc $a^{\mathcal{T}_X} = a$. Podobnie, n-arny symbol funkcyjny f z sygnatury S oznacza działanie $f^{\mathcal{T}_X} : \mathcal{T}_X^n \to \mathcal{T}_X$ zdefiniowane wzorem

$$f^{\mathcal{T}_X}(t_1, \ldots, t_n) = f(t_1, \ldots, t_n).$$

Tak więc symbol funkcyjny f oznacza w algebrze termów operację tworzenia termu postaci $f(\ldots)$.

Algebra termów (być może) pojawiła się po raz pierwszy w pracy Herbranda poświęconej badaniu dowodliwości formuł z kwantyfikatorami. Zawarte w tej pracy twierdzenie Herbranda jest jednym z podstawowych z działu informatyki zajmującym się automatycznym dowodzeniem twierdzeń. Próby realizacji algorytmu z twierdzenia Herbranda (czegoś w rodzaju metody zerojedynkowej dla formuł z kwantyfikatorami) doprowadziły do powstania programowania logicznego.

1.4 Informatyczny przykład algebry termów

Po pierwsze, dla potrzeb informatyki powinniśmy rozważać algebry wielorodzajowe. W przeciwieństwie do algebr rozważanych najczęściej w matematyce (których uniwersa składają się z jednorodnych elementów) w informatyce rozważa się algebry, których uniwersa są sumami kilku zbiorów. Elementy zbioru-składnika tej sumy są pewnego, określonego rodzaju. Działania w takiej algebrze są określone, jeżeli poszczególne argumenty są odpowiednich rodzajów, i mają wynik określonego rodzaju.

Rozważmy prymitywny język programowania zdefiniowany za pomocą następującej gramatyki:

$$\langle zmienna \rangle ::= x \mid y \mid z \mid \ldots$$

$$\langle stała \rangle ::= 0$$

$$\langle wyrażenie \rangle ::= \langle zmienna \rangle \mid \langle stała \rangle \mid \langle wyrażenie \rangle + 1$$

$$\langle warunek \rangle ::= \langle wyraźnie \rangle = \langle wyrażenie \rangle \mid \langle wyraźnie \rangle \neq \langle wyrażenie \rangle$$

$$\langle instrukcja \rangle ::= \langle zmienna \rangle := \langle wyrażenie \rangle$$

$$\langle instrukcja \rangle ::= \textbf{gdy } \langle warunek \rangle \textbf{ wykonaj } \langle instrukcja \rangle \textbf{ albo } \langle instrukcja \rangle$$

$$\langle instrukcja\rangle ::= \textbf{jeżeli } \langle warunek\rangle \textbf{ powtórz } \langle instrukcja\rangle$$

Taka gramatyka definiuje pięć rodzajów elementów: zmienne, stałe, wyrażenia, warunki i instrukcje. Dalej, gramatyka ta wyznacza pewną sygnaturę zawierającą symbole stałych (tzn. zeroargumentowe symbole funkcyjne): 0, x, y, z ... oraz następujące symbole funkcyjne:

1. jednoargumentowy symbol $+1$ wymagający argumentu rodzaju „wyrażenie" wyznaczający wartość rodzaju „wyrażenie",

2. dwuargumentowe symbole $=$ i $\neq$ wymagające argumentów rodzaju wyrażenie i wyznaczający wartość rodzaju „warunek",

3. dwuargumentowe symbole $:=$ i **jeżeli** ... **powtórz** ... wyznaczające wartości rodzaju „instrukcja". Pierwszy z nich wymaga argumentów odpowiednio rodzaju „zmienna" i „wyrażenie", a drugi – „warunek" i „instrukcja",

4. symbol **gdy** ... **wykonaj** ... **albo** ... arności 3 wymagający argumentu rodzaju „warunek" i dwóch argumentów rodzaju „instrukcja", dający wartość rodzaju „instrukcja".

Przykładem termu nad tą sygnaturą jest

$$\textbf{gdy } x = y \textbf{ wykonaj } x := z \textbf{ albo } \textbf{ jeżeli } x \neq y \textbf{ powtórz } x := y + 1 + 1.$$

Jest to term rodzaju „instrukcja". Ta instrukcja nie musi mieć sensu! Mam też nadzieję, że nie kojarzy się ona z czymkolwiek sensownym. Na razie nic nie zostało powiedziane o znaczeniu poszczególnych konstrukcji programistycznych. Co więcej, nic już nie zostanie powiedziane, ponieważ nie ma takiej potrzeby: został tylko określony sposób zapisu instrukcji i innych elementów języka.

Zdefiniowany język złożony z elementów 5 rodzajów, a więc zmiennych, stałych, wyrażeń, warunków i instrukcji, można uważać za wielorodzajową algebrę termów nad podaną sygnaturą.

1.5 Wartość wyrażenia

Mamy daną sygnaturę S, zbiór zmiennych X oraz algebrę $\mathcal{A} = \langle A, \ldots\rangle$ o sygnaturze S. Niech h będzie funkcją taką, że $h : X \to A$. Tego rodzaju funkcję będziemy nazywać wartościowaniem zmiennych ze zbioru X w algebrze A, a krócej – wartościowaniem zmiennych.

Dla każdego wyrażenia $t \in \mathcal{T}_X$ (zbudowanego z symboli sygnatury S i zmiennych ze zbioru X) zdefiniujemy wartość $val_h^{\mathcal{A}}(t)$ tego wyrażenia w algebrze $\mathcal{A}$ przy wartościowaniu h. Wartość wyrażenia definiujemy rekurencyjnie w następujący sposób:

1. $val_h^{\mathcal{A}}(a) = a^{\mathcal{A}}$ dla każdej stałej a z sygnatury S (inaczej: wartością wyrażenia będącego symbolem stałej w algebrze $\mathcal{A}$ jest ten element algebry $\mathcal{A}$, który jest oznaczany symbolem a i został jako taki wskazany w definicji algebry $\mathcal{A}$),

2. $val_h^{\mathcal{A}}(x) = h(x)$ dla każdej zmiennej $x \in X$ (inaczej: wartością zmiennej przy wartościowaniu h jest element przyporządkowany zmiennej przez to wartościowanie),

3. $val_h^{\mathcal{A}}(f(t_1, \ldots, t_n)) = f^{\mathcal{A}}(val_h^{\mathcal{A}}(t_1), \ldots, val_h^{\mathcal{A}}(t_n))$ dla dowolnego n-arnego symbolu funkcyjnego f z sygnatury S i dowolnych termów $t_1, \ldots, t_n \in \mathcal{T}_X$, (a więc, aby wyliczyć wartość termu $f(t_1, \ldots, t_n)$, należy najpierw wyliczyć wartości termów $t_1, \ldots, t_n$, a następnie dla obliczonych wartości wyliczyć wartość działania oznaczanego symbolem f).

Przykład 1.3 Rozważamy sygnaturę dla grup, a więc zawierającą symbole $\cdot$, $^{-1}$ i 1. Wyrażeniem z symbolami tej sygnatury i zmiennymi x, y i z jest np. $(x \cdot y^{-1}) \cdot (1 \cdot z^{-1})$. W tym wyrażeniu nie do końca jest określona kolejność działań. Przyjmujemy jak zwykle, zgodnie z najczęściej stosowanymi zasadami, że jest to wyrażenie $t = (x \cdot (y^{-1})) \cdot (1 \cdot (z^{-1}))$. Niech h będzie wartościowaniem zmiennych takim, że $h(x) = 6$, $h(y) = 2$ i $h(z) = 5$. Funkcja h jest wartościowaniem zmiennych w algebrze liczb wymiernych Q z mnożeniem, odwracaniem i liczbą 1, a także jest wartościowaniem w algebrze liczb całkowitych Z z dodawaniem, braniem liczby przeciwnej i 0. Są to algebry o rozważanej sygnaturze. Zauważmy, że $val_h^Q(t) = \frac{3}{5}$, natomiast $val_h^Z(t) = -1$.

1.6 Równości w algebrze

Jeżeli mamy dwa termy t_1 i t_2 ze zmiennymi $x_1, \ldots, x_n$ i symbolami z sygnatury S oraz algebrę $\mathcal{A}$ o sygnaturze S, to często zastanawiamy się, czy w algebrze $\mathcal{A}$ dla wszystkich możliwych $x_1, \ldots, x_n \in A$ zachodzi prawo $t_1 = t_2$. Mówiąc nieco inaczej, zastanawiamy się, czy w algebrze $\mathcal{A}$ jest spełnione zdanie

$$\forall x_1 \ \ldots \ \forall x_n \ \ t_1 = t_2.$$

Przykładem takich praw są prawa łączności, przemienności i rozdzielności.

Problem z takimi zdaniami bierze się stąd, że na ogół utożsamiamy różne znaczenia symboli. Co może oznaczać np. x w równości $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, która na dodatek ma zachodzić dla wszystkich x, y i z? Raczej nie jest jakiś element algebry, bo za chwilę będziemy musieli rozważać inny element chociażby po to, by rozważyć je wszystkie. Jest to symbol wskazujący miejsce, w które wstawiamy kolejno wszystkie dopuszczalne znaczenia x, czyli zmienna. Jeżeli mamy konsekwentnie rozróżniać zmienne od ich wartości, to musimy te pojęcia jakoś inaczej zapisywać. Wprowadzamy więc pojęcie wartościowania. Jeżeli x jest zmienną, to $h(x)$ oznacza wartość zmiennej. Sprawdzając łączność bierzemy równość $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, zmienne zastępujemy ich wartościami, symbole oznaczające działania – działaniami, i sprawdzamy, czy $h(x) \cdot^A (h(y) \cdot^A h(z)) = (h(x) \cdot^A h(y)) \cdot^A h(z)$, Tak więc naprawdę liczymy wartość lewej i prawej strony przy wartościowaniu h. Jeżeli zawsze te wartości są równe, to uznajemy, że zachodzi prawo łączności.

Mówiąc ogólnie, w algebrze $\mathcal{A}$ spełnione jest prawo

$$\forall x_1 \ \ldots \ \forall x_n \ \ t_1 = t_2,$$

jeżeli dla dowolnego wartościowania h zmiennych $x_1, \ldots, x_n$ w algebrze $\mathcal{A}$, po wyliczeniu wartości obu termów $val_h^{\mathcal{A}}(t_1)$ i $val_h^{\mathcal{A}}(t_2)$, okazuje się, że te wartości są identyczne.

Po napisaniu jeszcze kilku podobnych warunków moglibyśmy zdefiniować, co to znaczy, że jakaś dowolna własność jest spełniona (zachodzi, lub jest prawdziwa) w danej algebrze. Nie jest to jednak potrzebne na wykładzie z algebry.

2 Podalgebry

2.1 Definicja

Niech $\mathcal{A} = \langle A, \ldots \rangle$ będzie algebrą o sygnaturze S i niech B będzie niepustym podzbiorem A. Jeżeli zbiór B z działaniami i wyróżnionymi elementami z algebry $\mathcal{A}$ tworzy algebrę, to nazywamy ją podalgebrą $\mathcal{A}$.

Definicję podalgebry można wyrazić inaczej w następujący sposób: $\mathcal{B} = \langle B, \ldots \rangle$ jest podalgebrą algebry $\mathcal{A}$, jeżeli

1. $a^{\mathcal{A}} \in B$ dla każdej stałej z sygnatury S,
2. $f^{\mathcal{A}}(a_1, \ldots, a_n) \in B$ dla wszystkich n, wszystkich n-arnych symboli funkcyjnych f z sygnatury S i wszystkich $a_1, \ldots, a_n \in B$.

W podalgebrze $\mathcal{B}$ zachodzą równości $a^{\mathcal{B}} = a^{\mathcal{A}}$ dla wszystkich stałych $a \in S$ oraz wszystkie działania $f^{\mathcal{B}}$ są obcięciami $f^{\mathcal{A}}$ do zbioru B, a więc $f^{\mathcal{B}}(a_1, \ldots, a_n) = f^{\mathcal{A}}(a_1, \ldots, a_n)$ dla wszystkich $a_1, \ldots, a_n \in B$ oraz $f \in S$.

2.2 Własności podalgebr

Twierdzenie 2.1 *Przekrój podalgebr jest podalgebrą.* □

Twierdzenie 2.2 *Jeżeli w algebrze $\mathcal{A}$ zachodzi prawo*

$$\forall x_1 \ldots \forall x_n \;\; t_1 = t_2$$

dla pewnych termów t_1 i t_1, to w dowolnej podalgebrze algebry $\mathcal{A}$ to prawo też zachodzi. □

Wniosek 2.3 *Każda podgrupa jest grupą, każdy podpierścień jest pierścieniem, każdy podpierścień podpierścienia przemiennego jest pierścieniem przemiennym, itd.* □

2.3 Generowanie algebr

Twierdzenie 2.4 *Przypuśćmy, że $\mathcal{A} = \langle A, \ldots \rangle$ jest algebrą o sygnaturze S i i $V \subseteq A$ jest dowolnym zbiorem. Niech X będzie zbiorem zmiennych, a h – wartościowaniem zmiennych ze zbioru X przyjmującym jako wartości wszystkie elementy zbioru V i nic innego. Zbiór*

$$C(X) = \{val_h^{\mathcal{A}}(t) \in A : t \in \mathcal{T}_X\}.$$

jest podalgebrą algebry $\mathcal{A}$. Co więcej jest to najmniejsza podalgebra $\mathcal{A}$ zawierająca zbiór V.

Dowód. Po pierwsze, zdefiniowany zbiór jest podalgebrą algebry $\mathcal{A}$. Aby się o tym przekonać weźmy działanie f w algebrze $\mathcal{A}$ i odpowiednio dużo elementów postaci $val_h^{\mathcal{A}}(t_i)$ dla $t_i \in \mathcal{T}_X$. Mamy pokazać, że $f^{\mathcal{A}}(val_h^{\mathcal{A}}(t_1), \ldots)$ też jest elementem $C(X)$. Oczywiście, na podstawie definicji funkcji *val* mamy, że

$$f^{\mathcal{A}}(val_h^{\mathcal{A}}(t_1), \ldots) = val_h^{\mathcal{A}}(f(t_1, \ldots)) \in C(X).$$

Należy jeszcze pokazać, ze jest to podalgebra zawarta we wszystkich innych podalgebrach algebry $\mathcal{A}$ zawierających V. Jeżeli $\mathcal{B} = \langle B, \ldots \rangle$ jest taką podalgebrą, to przez indukcję ze względu na wielkość termu dowodzimy, że $val_h^{\mathcal{A}}(t) \in B$. Dla termów – zmiennych z X mamy $val_h^{\mathcal{A}}(x) = h(x) \in V \subseteq B$. Jeżeli natomiast $val_h^{\mathcal{A}}(t_1), \ldots \in B$, to – ponieważ B jest podalgebrą – $f^{\mathcal{A}}$ przekształca B w B i $val_h^{\mathcal{A}}(f(t_1, \ldots)) = f^{\mathcal{A}}(val_h^{\mathcal{A}}(t_1), \ldots) \in B$. □

Najmniejszą podalgebrę algebry $\mathcal{A}$ zawierającą zbiór V nazywamy podalgebrą generowaną przez zbiór V. Zbiór $V \subseteq A$ generuje algebrę $\mathcal{A}$, jeżeli $\mathcal{A}$ jest najmniejszą podalgebrą $\mathcal{A}$ generowaną przez V.

Przytoczone twierdzenie często pozwala znaleźć opis algebry generowanej przez coś i znaleźć sposób definiowania takiej algebry. Np. zakładając, że mamy ciało zawierające ciało liczb rzeczywistych i pierwiastek z -1 można, korzystając z podanego twierdzenia, przewidzieć definicję ciała liczb zespolonych, a więc generowanego przez liczby rzeczywiste i pierwiastek z -1 (pamiętajmy, że w przypadku ciał trzeba postępować ostrożnie, ponieważ w ciałach nie wszystkie wyrażenia mają określoną wartość). Podobne rozumowania wykorzystamy w dowodzie następującego twierdzenia.

Twierdzenie 2.5 *Jeżeli grupa G jest generowana przez element $g \in G$, to składa się z potęg tego elementu, a więc*

$$G = \{g^n : n \in Z\}.$$

Dowód. Aby to dowieść wystarczy pokazać, że wartość każdego termu ze jedną zmienną interpretowaną jako g (lub z jedną stałą oznaczającą g) jest potęgą g o wykładniku całkowitym. Można to zrobić posługując się indukcją ze względu na budowę termu (wielkość termu).

Dla prostych termów jest to oczywiste: $val_h^{\mathcal{A}}(1) = g^0$ i $val_h^{\mathcal{A}}(x) = g$ (x to zmienna interpretowana jako g, czyli spełniająca równość $h(x) = g$ lub stała interpretowana jako g, a więc taka, że $x^{\mathcal{A}} = g$). Natomiast wartość

$$val_h^{\mathcal{A}}(t_1 \cdot t_2) = val_h^{\mathcal{A}}(t_1) \cdot_G val_h^{\mathcal{A}}(t_1)$$

– na mocy założenia indukcyjnego – jest równa

$$= g^n \cdot_G g^m = g^{n+m}$$

dla pewnych n i m. Podobnie postępujemy w przypadku termów z operacją odwracania. □

3 Homomorfizmy

3.1 Definicja homomorfizmu

Przypuśćmy, że mamy dane dwie algebry $\mathcal{A} = \langle A, \ldots \rangle$ i $\mathcal{B} = \langle B, \ldots \rangle$ o tej samej sygnaturze S. Funkcję $h : A \to B$ nazywamy homomorfizmem algebry w algebrę $\mathcal{B}$, jeżeli

1. $h(a^{\mathcal{A}}) = a^{\mathcal{B}}$ dla każdej stałej a z sygnatury S,
2. $h(f^{\mathcal{A}}(a_1, \ldots)) = f^{\mathcal{B}}(h(a_1), \ldots)$ dla każdego symbolu funkcyjnego $f \in S$ i dla wszystkich $a_1, \ldots \in A$.

Przykład 3.1 Przykładem homomorfizmów określonych na algebrze termów $\mathcal{T}_X$ są funkcje $val_h^{\mathcal{A}}$ o wartościach w dowolnej algebrze $\mathcal{A}$ (o określonej sygnaturze), dla dowolnego wartościowania zmiennych.

Wśród homomorfizmów wyróżniamy epimorfizmy, czyli homomorfizmy typu „na", monomorfizmy, czy homomorfizmy różnowartościowe i izomorfizmy, czyli bijekcje będące homomorfizmami.

Algebrę $\mathcal{B}$ nazywamy obrazem homomorficznym algebry $\mathcal{A}$, jeżeli istnieje epimorfizm przekształcający A na B.

3.2 Równości w obrazie homomorficznym

Twierdzenie 3.2 *Przypuśćmy, że h jest homomorfizmem przekształcającym algebrę $\mathcal{A} = \langle A, \ldots \rangle$ na algebrę $\mathcal{B} = \langle B, \ldots \rangle$. Wtedy równości spełnione w algebrze $\mathcal{A}$ są również spełnione w algebrze $\mathcal{B}$.* □

Wniosek 3.3 *Obraz homomorficzny grupy jest grupą, obraz homomorficzny pierścienia jest pierścieniem, obraz homomorficzny pierścienia przemiennego z jednością jest pierścieniem przemiennym z jednością itd.* □

3.3 Kongruencje

Przypuśćmy, że h jest homomorfizmem przekształcającym algebrę $\mathcal{A} = \langle A, \ldots \rangle$ na algebrę $\mathcal{B} = \langle B, \ldots \rangle$ o tej samej sygnaturze. W zbiorze A zdefiniujmy relację

$$a_1 \sim a_2 \iff h(a_1) = h(a_2).$$

Jak widać, $\sim$ jest relacją równoważności. Ponadto, relacja $\sim$ spełnia następujący warunek:

jeżeli $a_1 \sim b_1, \ldots, a_n \sim b_n$ oraz $f \in S$ jest n argumentowym działaniem, to

$$f^{\mathcal{A}}(a_1, \ldots, a_n) \sim f^{\mathcal{A}}(b_1, \ldots, b_n).$$

Relację równoważności spełniającą ten warunek nazywamy kongruencją. Tak więc dowolny homomorfizm określony na algebrze $\mathcal{A}$ definiuje kongruencję w zbiorze A.

Lemat 3.4 *Przekrój kongruencji jest kongruencją.* □

3.4 Algebra ilorazowa

Jeżeli mamy algebrę $\mathcal{A} = \langle A, \ldots \rangle$ i kongruencję $\sim$ w algebrze $\mathcal{A}$, to możemy rozważać klasy abstracji $[x]_\sim$ (jest to przecież relacja równoważności) i w zbiorze $A/_\sim$ klas abstrakcji możemy dla symbolu funkcyjnego $f \in S$ zdefiniować działanie $f_\sim$ przyjmując, że

$$f_\sim([x_1]_\sim, \ldots) = [f^{\mathcal{A}}(x_1, \ldots)]_\sim.$$

Podobnie przyjmujemy, że

$$a_\sim = [a^{\mathcal{A}}]$$

dla stałej $a \in S$. Można mieć wątpliwości, czy podana definicja funkcji $f_\sim$ poprawna. Można bowiem spodziewać się, że podczas obliczania $f_\sim([y_1]_\sim, \ldots)$ okaże się, że $[y_1]_\sim = [x_1]_\sim, \ldots$ i jednocześnie $[f^{\mathcal{A}}(y_1, \ldots)]_\sim \neq [f^{\mathcal{A}}(x_1, \ldots)]_\sim$.

Lemat 3.5 *Jeżeli relacja $\sim$ jest kongruencją, to podane definicje działań w $A/_\sim$ są poprawne.*

Dowód. Warunek $[y_1]_\sim = [x_1]_\sim, \ldots$ oznacza, że $y_1 \sim x_1, \ldots$ Ponieważ $\sim$ jest kongruencją, więc także $f^{\mathcal{A}}(x_1, \ldots) \sim f^{\mathcal{A}}(y_1, \ldots)$. Elementy równoważne wyznaczają te same klasy abstrakcji. Stąd $[f^{\mathcal{A}}(x_1, \ldots)]_\sim = [f^{\mathcal{A}}(y_1, \ldots)]_\sim$. □

Zdefiniowaliśmy więc algebrę

$$\mathcal{A}/_\sim = \langle A/_\sim, f_\sim, \ldots, a_\sim, \ldots \rangle.$$

Jest to algebra nad sygnaturą S. Algebrę tę nazywamy ilorazową.

Konstrukcja algebry ilorazowej jest w rzeczywistości konstrukcją obrazu homomorficznego. Mamy bowiem następujące twierdzenie.

Twierdzenie 3.6 *Jeżeli relacja $\sim$ jest kongruencją w algebrze $\mathcal{A}$, to algebra ilorazowa $\mathcal{A}/_\sim$ jest obrazem homomorficznym $\mathcal{A}$ wyznaczonym przez homomorfizm χ przyporządkowujący $x \in A$ klasę abstracji $\chi(x) = [x]_\sim$. Co więcej kongruencja wyznaczona przez homomorfizm χ jest identyczna z relacją $\sim$.*

Dowód. Twierdzenie to jest oczywiste. Fakt, że χ jest homomorfizmem wynika wprost z definicji χ. Pozostałe fragmenty tezy twierdzenia wynikają natychmiast ze znanych własności relacji równoważności. □

3.5 Kongruencja wyznacza obraz homomorficzny

Twierdzenie 3.7 *Przypuśćmy, że mamy daną algebrę $\mathcal{A} = \langle A, \ldots\rangle$ o sygnaturze S i dwa obrazy homomorficzne $\mathcal{B}_1 = \langle B_1, \ldots\rangle$ i $\mathcal{B}_2 = \langle B_2, \ldots\rangle$ tej algebry wyznaczone odpowiednio przez homomorfizmy h_1 i h_2. Jeżeli homomorfizmy h_1 i h_2 wyznaczają tę samą kongruencję $\sim$, a więc*

$$h_1(x) = h_1(y) \iff x \sim y \iff h_2(x) = h_2(y)$$

dla wszystkich $x, y \in A$, to algebry $\mathcal{B}_1$ i $\mathcal{B}_2$ są izomorficzne.

Dowód. Izomorfizmem algebr $\mathcal{B}_1$ i $\mathcal{B}_2$ jest funkcja $I : B_1 \to B_2$ zdefiniowana wzorem

$$I(h_1(a)) = h_2(a)$$

dla $a \in A$. Taka definicja może nie być poprawna. Jej poprawność wynika z implikacji

$$h_1(x) = h_1(y) \Rightarrow h_2(x) = h_2(y).$$

Implikacja odwrotna, która też jest jednym z założeń, pociąga za sobą różnowartościowość funkcji I. Funkcja ta jest oczywiście typu „na".

Aby dowieść, że I jest homomorfizmem, zauważmy, że

$$I(a^{\mathcal{B}_1}) = I(h_1(a^{\mathcal{A}})) = h_2(a^{\mathcal{A}}) = a^{\mathcal{B}_2}$$

dla wszystkich stałych a z sygnatury S. Podobnie jest dla symbolu funkcyjnego $f \in S$:

$$\begin{aligned} &I(f^{\mathcal{B}_1}(y_1, \ldots)) = I(f^{\mathcal{B}_1}(h_1(x_1), \ldots)) = I(h_1(f^{\mathcal{A}}(x_1, \ldots))) = h_2(f^{\mathcal{A}}(x_1, \ldots)) = \\ &= f^{\mathcal{B}_2}(h_2(x_1), \ldots) = f^{\mathcal{B}_2}(I(h_1(x_1)), \ldots) = f^{\mathcal{B}_2}(y_1), \ldots) \end{aligned}$$

dla wszystkich $y_1, \ldots \in B_1$ i dla $x_1, \ldots \in A$ spełniających równości $h_1(x_1) = y_1, \ldots$ Możliwość wskazania elementów $x_1, \ldots$ wynika z założenia, że h_1 jest epimorfizmem. Druga i czwarta z podanych równości wynikają odpowiednio z założeń, że h_1 i h_2 są homomorfizmami. Poza tym korzystamy z definicji I. □

Udowodnione twierdzenie mówi, że obrazy homomorficzne algebry są wyznaczone (z dokładnością do izomorfizmu) przez kongruencje, które w tej algebrze można zdefiniować. Wiadomo też, że odpowiedniość między kongruencjami i obrazami homomorficznymi nie jest wzajemnie jednoznaczna. Zdarza się, że różne kongruencje też wyznaczają obrazy homomorficzne, które są izomorficzne.

4 Klasy algebr i algebry początkowe

4.1 Klasy algebr

Klasa algebr to pewna rodzina algebr, np. możemy mówić o klasie grup. Algebra należy do klasy grup wtedy i tylko wtedy, gdy jest grupą. Będziemy jednak posługiwać się zwrotem *klasa algebr* w znaczeniu bardziej specyficznym. Zwrot ten będzie oznaczać pewne szczególne klasy algebr.

Niech S będzie ustaloną sygnaturą zawierającą pzrynajmniej jedną stałą. Symbolem $\mathcal{T}$ będziemy oznaczać algebrę termów utworzonych za pomocą symboli z sygnatury S i nie zawierających zmiennych. W końcu, niech $\mathcal{R}$ oznacza pewien zbiór równości postaci

$$\forall x_1 \ \ldots \ \forall x_n \ \ t_1(x_1, \ldots, x_n) = t_2(x_1, \ldots, x_n),$$

gdzie $x_1, \ldots, x_n$ są pomocniczymi zmiennymi, a $t_1 = t_1(x_1, \ldots, x_n)$ i $t_2 = t_2(x_1, \ldots, x_n)$ są termami utworzonymi ze zmiennych $x_1, \ldots, x_n$ i symboli z sygnatury S. Mając sygnaturę S i zbiór równości $\mathcal{R}$ będziemy rozważać klasę algebr $\mathcal{K}$ złożonych z obrazów homomorficznych algebry termów $\mathcal{T}$ spełniających wszystkie prawa ze zbioru $\mathcal{R}$. Dalej $\mathcal{K}$ będzie oznaczało tak zdefiniowaną klasę algebr.

Klasą $\mathcal{K}$ można też inaczej scharakteryzować.

Lemat 4.1 *Algebra A o sygnaturze S należy do klasy $\mathcal{K}$ wtedy i tylko wtedy, gdy jest generowana przez zbiór $\{a^A \in A : a \in S \wedge a$ jest stałą$\}$ interpretacji stałych z sygnatury S i są w niej spełnione wszystkie równości ze zbioru $\mathcal{R}$.*

Dowód. Przypuśćmy, że algebra A jest obrazem algebry termów $\mathcal{T}$ przez homomorfizm h. Niech B będzie podalgebrą A zawierającą zbiór $X = \{a^A \in A : a \in S \wedge a$ jest stałą$\}$. Przez indukcję ze względu na budowę termu pokazujemy, że $h(t) \in B$ dla dowolnego termu $t \in \mathcal{T}$. Dla stałych jest to oczywiste: $h(a) = a^A \in B$ na mocy założenia o B. Jeżeli termy $t_1, \ldots, t_n$ homomorfizm h przekształca w elementy B, to to samo robi z termem $f(t_1, \ldots, t_n)$, gdyż B jest zbiorem zamkniętym ze względu na działanie f^A oraz

$$h(f(t_1, \ldots, t_n)) = h(f^{\mathcal{T}}(t_1, \ldots, t_n)) = f^A(h(t_1), \ldots, h(t_n)) \in B.$$

Stąd wynikają następujące zawierania: $A = h(\mathcal{T}) \subseteq B \subseteq A$. Ostatecznie otrzymujemy, że $A = B$, a więc A jest jedyną i najmniejszą podalgebrą A zawierającą zbiór X.

Przyjmimy teraz dla dowodu drugiego zawierania, że A jest algebrą generowaną przez zbiór X. Weźmy funkcję $h : \mathcal{T} \to A$ zdefiniowaną przez indukcję wzorami $h(a) = a^A$ oraz

$$h(f(t_1, \ldots, t_n)) = f^A(h(t_1), \ldots, h(t_n)).$$

Jest to poprawna definicja pewnej funkcji, która jest homomorfizmem. Nietrudno zauważyć, że $h(\mathcal{T})$ jest podalgebrą A zawierającą X. Jest więc równa całej algebrze A. Stąd A jest obrazem algebry termów wyznaczonym przez homomorfizm h. □

Teraz łatwo podać kilka przykładów klas algebr.

Przykład 4.2 Taką klasą jest np. klasa wszystkich grup cyklicznych, czyli generowanych przez pojedynczy element. Wystarczy wziąć sygnaturę $S = \{\cdot, 1, ^{-1}, g\}$ oraz zbiór $\mathcal{R}$ wszystkich równości podawanych w definicji grup. Można też rozważać klasę grup generowanych przez trzy elementy a, b i c spełniające $a \cdot b = c$, $b \cdot c = a$ i $c \cdot a = b$. Wtedy należałoby przyjąć, że $S = \{\cdot, 1, ^{-1}, a, b, c\}$, a zbiór $\mathcal{R}$ – oprócz równości z definicji grupy – powinien zawierać wymienione własności generatorów.

Przykład 4.3 Innym, podobnym przykładem może być klasa wszystkich pierścieni będących obrazami algebry termów nad sygnaturą złożoną z symboli $+, \cdot, -, 0$ i 1 (są to tak naprawdę pierścienie generowane przez 1, a więc tzw. pierścienie proste).

Przykład 4.4 Możemy też po prostu rozważać klasę wszystkich obrazów homomorficznych algebry termów $\mathcal{T}$. W tym przypadku nie żądamy spełniania jakichkolwiek równości, albo przyjmujemy, że $\mathcal{R} = \emptyset$.

Przykład 4.5 Kolejny przykład nie jest w pełni poprawny, ale będziemy go analizować w przyszłości. Przedstawione konstrukcje można wykorzystać do określenia algebry liczb zespolonych. W tym celu należałoby wziąć sygnaturę złożoną z symboli $+, \cdot, 0, 1, -, ^{-1}, i$ oraz continuum stałych oznaczających wszystkie możliwe liczby rzeczywiste, a także odpowiedni zbiór

równości $\mathcal{R}$ takich, jak prawa łączności i przemienności, prawo rozdzielności, prawa wyrażające definicje elementów neutralnych i odwrotnych. Wskazując sygnaturę i zbiór $\mathcal{R}$ definiujemy pewną klasę algebr. Do klasy opisanej przez wymienioną sygnaturę i zbiór $\mathcal{R}$ powinna należeć algebra liczb zespolonych.

Przykład 4.6 Przykład informatyczny wymaga algebry dwurodzajowej. Przyjmijmy, że mamy dwa rodzaje elementów: znaki $\mathcal{Z}$ oraz zawartości stosów $\mathcal{S}$ i na elementach tych rodzajów mamy określone działania oznaczane symbolami p, u, w i e. Symbol p jest dwuargumentowy i wymaga pierwszego argumentu rodzaju $\mathcal{Z}$ i drugiego – rodzaju $\mathcal{S}$. Pozostałe symbole są jednoargumentowe i wymagają argumentu rodzaju $\mathcal{S}$. Wartości działań oznaczanych symbolami p i u są rodzaju $\mathcal{S}$, a pozostałych – rodzaju $\mathcal{Z}$. Mamy też prawo posługiwać się stałymi 0 i 1 rodzaju $\mathcal{Z}$ oraz ε rodzaju $\mathcal{S}$. Tak więc mamy sygnaturę $S = \{p, u, w, e, 0, 1, \varepsilon\}$. Bierzemy też zbiór $\mathcal{R}$ praw

$$u(\varepsilon) = \varepsilon,\ u(p(x,y)) = y,\ w(p(x,y)) = x,\ e(p(x,y)) = 1,\ e(\varepsilon) = 0,$$

które mają zachodzić dla wszystkich x rodzaju $\mathcal{Z}$ i y rodzaju $\mathcal{S}$. Mamy więc prosty język pozwalający mówić o operacjach wykonywanych na stosach. Klasa algebr wyznaczona przez sygnaturę S i zbiór $\mathcal{R}$ jest klasą wszystkich możliwych semantyk tego prostego języka.

Każda klasa algebr ma następujące własności:

Lemat 4.7 *Jeżeli algebra A należy do klasy $\mathcal{K}$ i B jest obrazem homomorficznym A, to $B \in \mathcal{K}$. Do każdej klasy algebr należy algebra jednoelementowa (działania w takiej algebrze można zdefiniować tylko w jeden sposób i są w niej prawdziwe wszystkie możliwe równości).* □

4.2 Własności algebry termów $\mathcal{T}$

Niech S będzie dowolną sygnaturą zawierającą przynajmniej jedną stałą. Weźmy algebrę termów stałych $\mathcal{T}$ zbudowanych z symboli z sygnatury S.

Twierdzenie 4.8 *Każde dwa homomorfizmy algebry termów $\mathcal{T}$ w algebrę A są sobie równe.*

Dowód. Przypuśćmy, że mamy dwa homomorfizmy $h_1, h_2 : \mathcal{T} \to A$. Pokażemy przez indukcję ze względu na budowę termów, że $h_1(t) = h_2(t)$ dla wszystkich termów $t \in \mathcal{T}$.

Równość ta jest oczywista dla stałych $a \in S$. Mamy bowiem $h_1(a) = a^A = h_2(a)$. Podobnie, dla termów postaci $f(t, \ldots)$ mamy

$$h_1(f(t,\ldots)) = f^A(h_1(t),\ldots) = f^A(h_2(t),\ldots) = h_2(f(t,\ldots)),$$

przy czym środkowa równość wynika z założenia indukcyjnego. □

4.3 Algebry początkowe

Przypuśćmy, że rozważamy klasę algebr $\mathcal{K}$. Algebra $A \in \mathcal{K}$ jest początkowa w klasie $\mathcal{K}$, jeżeli dla każdej algebry B należącej do klasy $\mathcal{K}$ (także algebry A) istnieje dokładnie jeden epimorfizm przekształcający A na B.

W poprzednim rozdziale pokazaliśmy, że jeżeli $\mathcal{K}$ jest klasą wszystkich obrazów homomorficznych algebry termów $\mathcal{T}$, to $\mathcal{T}$ jest algebrą początkową w klasie $\mathcal{K}$.

Zauważmy, że

Twierdzenie 4.9 *Każde dwie algebry początkowe w klasie $\mathcal{K}$ są izomorficzne.*

Dowód. Przypuśćmy, że algebry A i B są początkowe w klasie $\mathcal{K}$. Wtedy obie należą do klasy $\mathcal{K}$ i istnieją epimorfizmy $h_1 : A \to B$ oraz $h_2 : B \to A$. Złożenie h_1h_2 jest epimorfizmem przekształcającym B na B. Takim epimorfizmem jest także funkcja identycznościowa id określona na B. Ponieważ B jest algebrą początkową, więc $h_1h_2 = id$. Z udowodnionej równości wynika, że funkcja h_2 jest różnowartościowa. Ostatecznie, funkcja h_2 jest izomorfizmem przekształcającym algebrę B na A. □

Twierdzenie 4.10 *Jeżeli A jest algebrą początkową w klasie $\mathcal{K}$, to $\mathcal{K}$ jest klasą wszystkich obrazów homomorficznych algebry A.*

Dowód. Ponieważ A jest algebrą początkową w klasie $\mathcal{K}$, więc każda algebra z klasy $\mathcal{K}$ jest obrazem homomorficznym A. Z drugiej strony, wszystkie obrazy homomorficznem algebry A należą do $\mathcal{K}$, gdyż rozważamy specyficzne klasy algebr, które są zamknięte ze względu na branie obrazu homomorficznego (patrz lemat 4.7). □

4.4 Istnienie algebr początkowych

Najpierw zbadamy, kiedy obraz homomorficzny algebry termów $\mathcal{T}$ spełnia daną równość. Jak zwykle, S jest ustaloną sygnaturą z przynajmniej jedną stałą, a $\mathcal{T}$ – algebrą termów stałych zbudowanych z symboli sygnatury S.

Lemat 4.11 *Niech $\sim$ będzie kongruencją w algebrze termów $\mathcal{T}$. Przyjmijmy, że $t_1 = t_1(x_1, \ldots, x_n)$ oraz $t_2 = t_2(x_1, \ldots, x_n)$ są dwoma termami zbudowanymi ze zmiennych $x_1, \ldots, x_n$ i symboli funkcyjnych z sygnatury S. W algebrze ilorazowej $\mathcal{T}/_\sim$ spełniona jest równość*

$$\forall x_1 \ \ldots \ \forall x_n \ \ t_1(x_1, \ldots, x_n) = t_2(x_1, \ldots, x_n)$$

wtedy i tylko wtedy, gdy zachodzą wszystkie kongruencje

$$t_1(s_1, \ldots, s_n) \sim t_2(s_1, \ldots, s_n),$$

gdzie $s_1, \ldots, s_n \in \mathcal{T}$ są dowolnymi termami, a $t(s_1, \ldots, s_n)$ oznacza wynik podstawiania w termie t termów $s_1, \ldots, s_n$ odpowiednio za zmienne $x_1, \ldots, x_n$.

Dowód. Dowód tego lematu jest bardzo formalny. Najpier zauważmy, że zgodnie z definicją, spełnianie w algebrze $\mathcal{T}/_\sim$ równości

$$\forall x_1 \ \ldots \ \forall x_n \ \ t_1(x_1, \ldots, x_n) = t_2(x_1, \ldots, x_n)$$

zachodzi wtedy i tylko wtedy, gdy dla każdego wartościowania v zmiennych $x_1, \ldots, x_n$ w algebrze $\mathcal{T}/_\sim$ zachodzi równość

$$val_v^{\mathcal{T}/\sim}(t_1(x_1, \ldots, x_n)) = val_v^{\mathcal{T}/\sim}(t_2(x_1, \ldots, x_n)). \tag{1}$$

Teraz musimy zrozumieć jak się liczy wartość termu. Po pierwsze, mamy dwa rodzaje termów: termy stałe ze zbioru $\mathcal{T}$ i termy ze zmiennymi $x_1, \ldots, x_n$ ze zbioru $\mathcal{T}_{\{x_1,\ldots,x_n\}}$. Algebra termów $\mathcal{T}$ jest podalgebrą $\mathcal{T}_{\{x_1,\ldots,x_n\}}$. Na każdej z tych algebr mamy określone wartości termów $val^{\mathcal{T}/\sim} : \mathcal{T} \to \mathcal{T}/_\sim$ oraz $val_v^{\mathcal{T}/\sim} : \mathcal{T}_{\{x_1,\ldots,x_n\}} \to \mathcal{T}/_\sim$. Wszystkie te wartościowania są określone na algebrze $\mathcal{T}$ i są homomorfizmami tej algebry. Z twierdzenia 4.8 wynika, że wszystkie

homomorfizmy przekształcające $\mathcal{T}$ w $\mathcal{T}/_\sim$, także homomorfizm zdefiniowany w konstrukcji ilorazowej, są równe. Tak więc

$$t \in \mathcal{T} \Rightarrow val_v^{\mathcal{T}/\sim}(t) = val^{\mathcal{T}/\sim}(t) = [t]_\sim \tag{2}$$

(w szczególności, wartość termu stałego nie zależy od wartościowania v).

Teraz wyliczymy wartość termu stałego otrzymanego w wyniku podstawiania. Zauważmy, że

$$val^{\mathcal{T}/\sim}(t(s_1, \ldots, s_n)) = val_v^{\mathcal{T}/\sim}(t(x_1, \ldots, x_n)) \tag{3}$$

dla wartościowania v takiego, że $v(x_i) = val^{\mathcal{T}/\sim}(s_i)$. Wzór ten dowodzi się łatwo przez indukcję ze względu na budowę termu $t \in \mathcal{T}_{\{x_1,\ldots,x_n\}}$.

Co więcej, każde wartościowanie v w algebrze $\mathcal{T}/_\sim$ jest postaci $v(x_i) = [s_i]_\sim$ i może zostać zdefiniowane wzorami $v(x_i) = val^{\mathcal{T}/\sim}(s_i)$ dla pewnych termów stałych s_i. Stąd wynika, że własność „dla każdego wartościowania v zachodzi wzór (1)" jest równoważna stwierdzeniu „dla dowolnych termów $s_1, \ldots, s_n \in \mathcal{T}$ i dla wartościowania v takiego, że $v(x_i) = val^{\mathcal{T}/\sim}(s_i)$ zachodzi równość (1)". Z kolei równość (1) – na podstawie wzoru (3) – może przybrać formę

$$val^{\mathcal{T}/\sim}(t_1(s_1, \ldots, s_n)) = val^{\mathcal{T}/\sim}(t_2(s_1, \ldots, s_n)).$$

Ta jest równoważna

$$[t_1(s_1, \ldots, s_n)]_\sim = [t_2(s_1, \ldots, s_n)]_\sim$$

na mocy (2) oraz równości

$$t_1(s_1, \ldots, s_n) \sim t_2(s_1, \ldots, s_n).$$

W ten sposób zakończyliśmy dowód lematu. □

Istotną treść poprzedniego lematu można wyrazić w formie wniosku:

Wniosek 4.12 *Niech $\sim$ będzie kongruencją w algebrze termów stałych $\mathcal{T}$. Dla dowolnej równości r istnieje zbiór par termów $X_r \subseteq \mathcal{T}^2$ taki, że spełnianie r w algebrze ilorazowej $\mathcal{T}/_\sim$ jest równoważne zawieraniu $X_r \subseteq \sim$.* □

Twierdzenie 4.13 *W każdej klasie algebr jest algebra początkowa.*

Dowód. Weźmy klasę algebr o sygnaturze S, będącą klasą obrazów homomorficznych algebry termów $\mathcal{T}$ spełniających równości ze zbioru $\mathcal{R}$. Tak więc mamy skonstruować obraz homomorficzny algebry $\mathcal{T}$. Możemy to zrobić konstruując pewną kongruencję.

Przyjmijmy, że w zbiorze $\mathcal{R}$ są równości $r_1, \ldots, r_m$. Dla tych równości korzystamy z wniosku 4.12 i bierzemy zbiory $X_{r_1}, \ldots, X_{r_m}$. Niech

$$X_\mathcal{R} = X_{r_1} \cup \ldots \cup X_{r_m}.$$

Konstruowana kongruencja powinna zawierać zbiór $X_\mathcal{R}$.

Algebra początkowa jest największą algebrą w swojej klasie, pozostałe są jej obrazami. Konstruując tę algebrę powinniśmy utożsamiać możliwie mało elementów $\mathcal{T}$. Dlatego wybieramy możliwie małą kongruencję. Niech więc $\sim_0$ będzie najmniejszą kongruencją zawierającą zbiór $X_\mathcal{R}$. Pokażemy, że algebra $\mathcal{T}/_{\sim_0}$ jest algebrą początkową w klasie $\mathcal{K}$. Oczywiście, ta algebra jest obrazem homomorficznym $\mathcal{T}$ i spełnia – na mocy wniosku 4.12 – wszystkie równości ze zbioru $\mathcal{R}$.

Niech A będzie dowolną algebrą z klasy $\mathcal{K}$ i niech h będzie epimorfizmem przekształcającym $\mathcal{T}$ na A. W końcu, niech $\sim$ oznacza kongruencję w algebrze $\mathcal{T}$ spełniającą równoważność

$$x \sim y \iff h(x) = h(y).$$

W algebrze A są spełnione wszystkie równości z $\mathcal{R}$. Algebra $\mathcal{T}/_\sim$ jest izomorficzna z A, jest więc obrazem homomorficznym A i też spełnia wszystkie równości z $\mathcal{R}$, np. na mocy twierdzenia 3.2. Z wniosku 4.12 wynika, że zbiór $X_\mathcal{R}$ jest zawarty w $\sim$. Wobec tego, kongruencja $\sim$ zawiera najmniejszą kongruencję $\sim_0$ zawierającą $X_\mathcal{R}$. Tak więc $\sim_0 \subseteq \sim$.

Teraz już łatwo zdefiniować epimorfizm $f : \mathcal{T}_{\sim_0} \to A$. Przyjmijmy, że

$$f([t]_{\sim_0}) = h(t)$$

dla wszystkich $t \in \mathcal{T}$.

Najpierw trzeba sprawdzić poprawność definicji f. Jeżeli klasy $[t_1]_{\sim_0}$ i $[t_2]_{\sim_0}$ są równe, to $t_1 \sim_0 t_2$. Z zawierania $\sim_0 \subseteq \sim$ wynika, że także $t_1 \sim t_2$. Z definicji kongruencji $\sim$ otrzymujemy, że $h(t_1) = h(t_2)$.

Bezpośrednio z definicji f i faktu, że h jest epimorfizmem wynika, że funkcja f jest typu „na".

Własność wymaganą od homomorfizmów sprawdzimy dla funkcji f na przykładzie działania $\cdot$. Mamy więc

$$f([t_1]_{\sim_0} \cdot^{\mathcal{T}_{\sim_0}} [t_2]_{\sim_0}) = f([t_1 \cdot t_2]_{\sim_0}) = h(t_1 \cdot t_2) = h(t_1) \cdot^A h(t_2),$$

przy czym pierwsza równość wynika z definicji działań w algebrze ilorazowej, druga – z definicji f, ostatnia zaś z faktu, że h jest homomorfizmem.

Aby zakończyć dowód, należy wykazać jedyność homomorfizmu f. Przypuśćmy więc, że mamy dwa homomorfizmy $f_1, f_2 : \mathcal{T}/_{\sim_0} \to A$. Wtedy możemy zdefiniować dwa homomorfizmy $f_i' : \mathcal{T} \to A$ takie, że

$$f_i'(t) = f_i([t]_{\sim_0}).$$

Jest to jednak sprzeczne z twierdzeniem 4.8. □

Znajdziemy jeszcze algebrę początkową w klasie wszystkich grup cyklicznych. Przyjmijmy, że do tej klasy należą algebry o sygnaturze $S = \{\cdot, 1, ^{-1}, g\}$.

Twierdzenie 4.14 *Algebrą początkową w klasie $\mathcal{K}$ wszystkich grup cyklicznych jest zbiór liczb całkowitych Z z dodawaniem (zerem i braniem elementu przeciwnego).*

Dowód. Najpierw ustalmy, co oznaczają w addytywnej grupie liczb całkowitych Z poszczególne symbole sygnatury S. Tak więc

$$\cdot^Z = +, \;\; 1^Z = 0 \;\; (dla\ 1 \in S), \;\; {}^{-1^Z} = - \;\; \text{oraz} \;\; g^Z = 1 \in Z.$$

Zwykle stosowany zapis g^n będziemy rozumieć jako zdefiniowany w zwykły sposób term stały ze zbioru $\mathcal{T}$:

$$g^0 = 1, \;\; g^{n+1} = g^n \cdot g \;\; \text{oraz} \;\; g^{-n} = (g^{-1})^n$$

dla wszystkich $n \in N$. Zauważmy też, że 1 w pierwszym wzorze to symbol sygnatury S, a nie liczba całkowita 1.

Niech $val^Z : \mathcal{T} \to Z$ oznacza funkcję przyporządkowującą termowi stałemu jego wartość. Zauważmy, że

$$val^Z(g^n) = n$$

dla wszystkich liczb całkowitych n. Sprawdzimy tę równość przez indukcję tylko dla liczb naturalnych, pozostawiając resztę dowodu jako ćwiczenie. Mamy dla wszystkich $n \in N$

$$val^Z(g^0) = val^Z(1) = 1^Z = 0$$

oraz

$$val^Z(g^{n+1}) = val^Z(g^n \cdot g) = val^Z(g^n) \cdot^Z val^Z(g) = n + g^Z = n + 1.$$

Z udowodnionego wzoru wynika w pierwszym rzędzie, że algebra Z należy do klasy $\mathcal{K}$. Tak jest, gdyż funkcja val^Z okazała się typu „na", a jest ona homomorfizmem. Jest też oczywiste, że algebra liczb całkowitych z dodawaniem jest grupą.

Aby dowieść, że Z jest algebrą początkową, wykażemy, że kongruencja

$$t_1 \sim t_2 \iff val^Z(t_1) = val^Z(t_2)$$

jest najmniejszej kongruencją $\sim_0$ w algebrze $\mathcal{T}$ taką, że algebra ilorazowa $\mathcal{T}/_{\sim_0}$ jest grupą. Zachodzi – oczywiście – zawieranie $\sim_0 \subseteq \sim$.

W grupach z jednym generatorem każdy element jest całkowitą potęgą generatora. Dla grupy $\mathcal{T}/_{\sim_0}$ fakt ten można wyrazić w następujący sposób: dla każdego $t \in \mathcal{T}$ istnieje liczba całkowita n taka, że

$$val^{\mathcal{T}/_{\sim_0}}(t) = val^{\mathcal{T}/_{\sim_0}}(g^n).$$

Równość tę dowodzimy dość łatwo przez indukcję ze względu na budowę termu t. Jedyna trudność w dowodzie polega na konieczności korzystania z rachunków takich, jak

$$\begin{aligned} &val^{\mathcal{T}/_{\sim_0}}(g^n \cdot g^m) = val^{\mathcal{T}/_{\sim_0}}(g^n) \cdot^{\mathcal{T}/_{\sim_0}} val^{\mathcal{T}/_{\sim_0}}(g^m) = \\ &= (val^{\mathcal{T}/_{\sim_0}}(g))^n \cdot^{\mathcal{T}/_{\sim_0}} (val^{\mathcal{T}/_{\sim_0}}(g))^m = (val^{\mathcal{T}/_{\sim_0}}(g))^{n+m} = \\ &= val^{\mathcal{T}/_{\sim_0}}(g^{n+m}). \end{aligned}$$

Aby zrealizować plan dowodu, powinniśmy jeszcze wykazać, że $\sim \subseteq \sim_0$. Weźmy więc dwa termy $t, s \in \mathcal{T}$ takie, że $t \sim s$. Dla tych termów bierzemy liczby całkowite n i m takie, że

$$val^{\mathcal{T}/_{\sim_0}}(t) = val^{\mathcal{T}/_{\sim_0}}(g^n) \text{ oraz } val^{\mathcal{T}/_{\sim_0}}(s) = val^{\mathcal{T}/_{\sim_0}}(g^m).$$

Z twierdzenia 4.8 wynika, że

$$val^{\mathcal{T}/_{\sim_0}}(t) = [t]_{\sim_0},$$

a stąd

$$g^n \sim_0 t \sim s \sim_0 g^m.$$

Po skorzystaniu z zawierania $\sim_0 \subseteq \sim$ otrzymujemy, że

$$g^n \sim g^m.$$

Tak więc

$$n = val^Z(g^n) = val^Z(g^m) = m.$$

Ostatecznie otrzymujemy, że

$$t \sim_0 g^n = g^m \sim_0 s,$$

i to kończy dowód. □

Uwaga: dowód twierdzenia 4.14 jest bardzo prosty, choć korzysta z bardzo skomplikowanego aparatu. Realizuje bardzo prostą ideę: w grupach cyklicznych każdy element jest potęgą generatora. Nie można utworzyć większej grupy cyklicznej, niż taka, w której wszystkie potęgi generatora są różne. Przykładem takiej grupy jest właśnie addytywna grupa liczb całkowitych. Ta grupa musi być więc algebrą początkową. Samo twierdzenie można też dowieść łatwiej, innymi metodami, korzystającymi ze znanych własności grup cyklicznych.

Inną sytuację mamy w przykładzie informatycznym 4.6. Do znalezienia algebry początkowej opisanej tam klasy algebr można wykorzystać metodę z dowodu twierdzenia 4.14. Aby znaleźć tę algebrę innymi metodami należałoby opracować najpierw jakąś teorię algebr tego typu. Może to się okazać bardzo proste, ale chyba nie zostało jeszcze zrobione.