Wersja z 24 czerwca 2006 roku.

1 Podstawowe pojęcia algebry ogólnej

1.1 Sygnatura

Sygnaturą algebry 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 będą 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, $z \ldots$ oraz następujące symbole funkcyjne:

1. jednoargumentowy symbol $+1$ wymagający arumentu 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**$\ldots$**powtórz**$\ldots$ wyznaczające wartości rodzaju „instrukcja”. Pierwszy z nich wymaga argumentów odpowiednio rodzaju „zmienna” i „wyrażenie”, a drugi – „warunek” i „instrukcja”,

4. symbol **gdy**$\ldots$**wykonaj**$\ldots$**albo**$\ldots$ 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, czyli 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 wyliczyć dla obliczonych wartości 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 prawami 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 raczej symbol wskazujący miejsce, w które wstawiamy kolejno wszystkie dopuszczalne znaczenia x, czyli zmienna. Jeżeli mamy konsekwentnie rozróżniać zmienne od ich wartości, to te pojęcia musimy 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, a więc bierzemy $h(x) \cdot (h(y) \cdot h(z)) = (h(x) \cdot h(y)) \cdot h(z)$, a więc tak naprawdę liczymy wartość lewej i prawej strony przy wartościowaniu h. Jeżeli zawsze zachodzi ta równość, 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, czyli $val_h^{\mathcal{A}}(t_1)$ 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 $a^{\mathcal{B}} = a^{\mathcal{A}}$ oraz $f^{\mathcal{B}}$ jest obcięciem $f^{\mathcal{A}}$ do zbioru B, a więc $f^{\mathcal{B}}(a_1, \ldots, a_n) = f^{\mathcal{A}}(a_1, \ldots, a_n)$ dla wszystkich $a_1, \ldots, a_n \in B$.

2.2 Podgrupy

Pojęcie podalgebry zależy istotnie od sygnatury. Grupy możemy definiować jako algebry z różnymi sygnaturami. Może to sugerować różne definicje podgrupy.

Załóżmy, że G jest grupą i $H \subseteq G$ (grupy utożsamiamy tu z ich uniwersami). Przyjmujemy jednak, że H jest podgrupą grupy G, jeżeli

1. $1 \in H$,
2. $h_1 \cdot h_2 \in H$ dla wszystkich $h_1, h_2 \in H$,
3. $h^{-1} \in H$ dla dowolnego $h \in H$.

W tej definicji 1, $\cdot$ i $^{-1}$ oznaczają działania w grupie G.

Przykład 2.1 Zbiór liczb parzystych jest podgrupą addytywnej grupy liczb całkowitych. Spełnia wszystkie wyżej podane warunki. Możemy też rozważać algebrę liczb całkowitych z jednym działaniem, dodawaniem. Ta algebra może też być uważana za grupę. Można w niej bowiem w jeden sposób zdefiniować pozostałe działania grupowe i rozszerzyć ją do algebry będaćej grupą ze zwykła sygnaturą. Podalgebrą zbioru liczb całkowitych z dodawaniem jest np. zbiór liczb naturalnych. Zbiór liczb naturalnych nie spełnia trzeciego z wymienionych warunków i z tego powodu nie jest podgrupą.

Zachodzi następujące twierdzenie:

Twierdzenie 2.2 *Załóżmy, że G jest grupą i H jest niepustym, skończonym podzbiorem G takim, że $h_1 \cdot h_2 \in H$ dla wszystkich $h_1, h_2 \in H$. Wtedy H jest podgrupą grupy G.* □

2.3 Własności podalgebr

Twierdzenie 2.3 *Przekrój podalgebr jest podalgebrą.* □

Twierdzenie 2.4 *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 2.5 *Każda podgrupa jest grupą, każdy podpierścień jest pierścieniem , każdy podpierścień podpierścienia przemiennego jest pierścieniem przemiennym, itd.* □

Wniosek 2.6 *Każde podciało jest ciałem.*

Dowód. Ponieważ nie wszystkie własności wymagane od ciała są prawami równościowymi, więc uzasadnienie tego wniosku jest nieco bardziej skomplikowane, ale też jest proste. □

2.4 Generowanie algebr

Twierdzenie 2.7 *Przypuśćmy, że $\mathcal{A} = \langle A, \ldots \rangle$ jest algebrą o sygnaturze S 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). Przykładem tego typu rozumowania jest następujące twierdzenie.

Twierdzenie 2.8 *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 lub stała interpretowana jako g). Natomiast wartość

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

i – 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 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.

Spośród 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 $\mathcal{B}$.*

Dowód. □

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.* □

W przypadku ciał sytuacja jest podobna, ale też trochę inna. Są dwie możliwości: albo obraz homomorficzny ciała jest ciałem izomorficznym, a sam homomorfizm – izomorfizmem, albo jest algebrą jednoelementową, zawierającą tylko 0, która nie jest ciałem (każde ciało ma przynajmniej dwa różne elementy 0 i 1).

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). Zdefiniujmy relację w zbiorze A:

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

Jak widać, R 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 podany 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 tej algebrze, to możemy rozważać klasy abstracji $[x]_\sim$ tej relacji (jest to przecież relacja równoważności) i w zbiorze $A/_\sim$ tych klas abstrakcji możemy dla symbolu funkcyjnego $f \in S$ zdefiniować działanie $f_\sim$ przyjmując, że

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

i ponadto

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

dla stałej $a \in S$. Można mieć wątpliwości, czy podana definicja $f_\sim$ 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, więc $[f^{\mathcal{A}}(x_1, \ldots)]_\sim = [f^{\mathcal{A}}(y_1, \ldots)]_\sim$. □

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 ilorozowej 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 $f \in S$:

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

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.

3.6 Dzielniki normalne

W przypadku grup i bardziej skomplikowanych algebr można coś więcej powiedziec o kongruencjach. Relacje to są wyznaczone przez klasy abstrakcji elementu neutralnego. Mamy bowiem następujący lemat.

Lemat 3.8 *Jeżeli G jest grupą i $\sim$ jest kongruencją w G, to*

$$x \sim y \iff xy^{-1} \in [1]_\sim$$

dla wszystkich elementów $x, y \in G$.

Dowód. Przypuśćmy, że $x \sim y$. Ponieważ $\sim$ jest relacją równoważności, więc $y^{-1} \sim y^{-1}$. Ponieważ jest to kongruencja , to także $xy^{-1} \sim yy^{-1} = 1$. Stąd mamy, że $xy^{-1} \in [1]_\sim$. Implikację odwrotną dowodzimy bardzo podobnie. □

Twierdzenie 3.9 *Jeżeli G jest grupą i relacja $\sim$ w zbiorze G jest kongruencją, to klasa abstrakcji $[1]_\sim$ elementu neutralnego G jest dzielnikiem normalnym. Jeżeli mamy dzielnik normalny H grupy G, to relacja $\sim$ spełniająca równoważność*

$$x \sim y \iff xy^{-1} \in H$$

jest kongruncją.

Dowód. Łatwo dowodzi się pierwszą częśc twierdzenia. Aby przekonać się o prawdziwości drugiej części zauważmy, że zwrotność $\sim$ wynika z faktu, że $1 \in H$, symetryczność – z zamkniętości H ze względu na odwracanie, a przechodniość – z zamkniętości H na mnożenie.

Jeżeli $x_1 \sim y_1$ i $x_2 \sim y_2$, a więc jeżeli $x_1 y_1^{-1}, x_2 y_2^{-1} \in H$, to także

$$x_1 x_2 (y_1 y_2)^{-1} = x_1 (x_2 y_2^{-1}) y_1^{-1} = (x_1 (x_2 y_2^{-1}) x_1^{-1})(x_1 y_1^{-1}) \in H$$

i ostatecznie $x_1x_2 \sim y_1y_2$.

Jeżeli natomiast $x \sim y$, to warunek $y^{-1} \sim x^{-1}$ zachodzi ponieważ

$$y^{-1}(x^{-1})^{-1} = y^{-1}x = y^{-1}(xy^{-1})y \in H. \ \square$$

Prawdziwe jest też mocniejsze twierdzenie od wyżej podanego, stwierdzające, że w grupie kongruencje i dzielniki normalne wzajemnie sobie odpowiadają.

W teorii pierścieni rolę dzielników normalnych przejmują ideały. Można dowieść twierdzenia analogiczne do podanych o kongruencjach w pierścieniach i ideałach.

3.7 Algebra początkowa

Przypuśćmy, że rozważamy klasę algebr $\mathcal{K}$. A więc np. rozważamy wszystkie grupy, albo grupy o parzystej liczbie elementów, albo też grupy, które są generowane przez ustaloną liczbę elementów. Algebrę $\mathcal{A} \in \mathcal{K}$ nazywamy algebrą początkową w klasie $\mathcal{K}$, jeżeli dla każdej algebry $\mathcal{B} \in \mathcal{K}$ istnieje dokładnie jeden homomorfizm przekształcający algebrę $\mathcal{A}$ na $\mathcal{B}$.

Twierdzenie 3.10 *Każde dwie algebry początkowe w klasie $\mathcal{K}$ są izomorficzne.*

Dowód. Przypuśćmy, że $\mathcal{A}$ i $\mathcal{B}$ są algebrami początkowymi w klasie $\mathcal{K}$. Istnieją więc epimorfizmy f przekształcający $\mathcal{A}$ na $\mathcal{B}$ i g przekształcający $\mathcal{B}$ na $\mathcal{A}$. Złożenie fg jest epimorfizmem przekształcającym $\mathcal{B}$ na $\mathcal{B}$. Innym takim homomorfizmem jest funkcja identycznościowa określona na uniwersum $\mathcal{B}$. Z warunku jednoznaczności otrzymujemy, że fg jest funkcją identycznościową. Podobnie dowodzimy, że gf jest funkcją identycznościową. Oznacza to, że funkcje f i g są bijekcjami, a także izomorfizmami. $\square$

Dalej będziemy rozważać klasy $\mathcal{K}$ algebr o określonej sygnaturze, będący obrazem $val_h^{\mathcal{A}}(\mathcal{T}_X)$ algebry termów $\mathcal{T}_X$ (dla ustalonego zbioru X), w których jest spełniony pewien skończony zbiór równośći

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

dla pewnych termow $t_1, t_2 \in \mathcal{T}_{X \cup \{x_1,\ldots,x_n\}}$. O takich klasach będziemy mówić, że są definiowane równościowo.

Przykładem klasy definiowanej równościowo jest klasa wszystkich grup cyklicznych. Są to algebry o sygnaturze $\cdot, ^{-1}, 1$, każda grupa cykliczna jest obrazem podanej postaci algebry termów $\mathcal{T}_X$ dla jednoelementowego zbioru X, spełnione są w niej aksjomaty grupy, które dają się zapisać w postaci równości. Jedną z równości jest prawo łączności. Algebrą początkową w tej klasie jest każda nieskończona grupa cykliczna, np. grupa addytywna liczb całkowitych.

Innym przykładem takiej klasy jest klasa wszystkich algebr o ustalonej sygnaturze generowanych przez określoną liczbę elementów. Algebrą początkową w takiej klasie jest algebra termów $\mathcal{T}_X$ dla odpowiedniego zbioru X. W tym przypadku algebry z tej klasy spełniają pusty zbiór równości.

Twierdzenie 3.11 *W każdej, definiowanej w ten sposób klasie algebr $\mathcal{K}$ jest algebra początkowa.*