Jerzy Hanusek

Uwagi o arytmetyce Grassmanna

Diametros nr 45, 107-121

2015

Diametros 45 (2015): 107-121
doi: 10.13153/diam.45.2015.799

Uwagi o arytmetyce Grassmanna

– Jerzy Hanusek –

Abstrakt. Praca Hermanna Grassmanna z roku 1861 była pierwszą próbę aksjomatycznego ujęcia arytmetyki (liczb całkowitych z wyróżnionym podzbiorem liczb dodatnich). Znaczenie historyczne tej pracy jest ogrom-ne, choć sama aksjomatyka okazała się niepełna. Opierając się na interpretacji teorii Grassmanna dokonanej przez Hao Wanga [1957], przedstawiam szczegółowe jej omówienie i definiuję klasę modeli tej teorii. Na koniec podaję propozycję modyfikacji aksjomatyki arytmetyki Grassmanna, która polega na dodaniu pewnego zdania elementarnego i usunięciu zdania nieelementarnego. Przedstawiam dowód, że po takiej modyfikacji teorii jej jedynym modelem z dokładnością do izomorfizmu jest model standardowy.

Słowa kluczowe: Hermann Grassmann, Giuseppe Peano, arytmetyka, teoria aksjomatyczna.

Uwagi historyczne

Aksjomaty arytmetyczne zwykle są kojarzone z nazwiskiem i postacią Giuseppe Peano oraz jego pracą z roku 1889 noszącą tytuł *Arithmetices principia, nova methodo exposita* (*Zasady arytmetyki prezentowane nową metodą*). Peano zamieścił w niej podziękowanie, z którego dowiadujemy się, że opierał się on w znacznej mierze na pracach Dedekinda i Grassmanna. Celem Dedekinda nie było zresztą skonstruowanie aksjomatycznej teorii arytmetyki, ale skonstruowanie czegoś, co dzisiaj moglibyśmy nazwać standardowym modelem arytmetyki liczb naturalnych. Wychodząc od definicji nieskończoności, poprzez słynny – ale odrzucony przez matematyków – dowód, że istnieje zbiór nieskończony, wykazał on, że istnieją tzw. zbiory prosto nieskończone. Są to liniowo uporządkowane zbiory, na których można zdefiniować poprzez indukcję działania arytmetyczne. Aksjomaty Peano można odnaleźć w pracy Dedekinda w formie postulatów, które powinien spełniać adekwatny model arytmetyki. Dlatego noszą one często nazwę aksjomatów Dedekinda-Peano. Grassmann jest w kontekście początków teorii arytmetycznych zdecydowanie zbyt rzadko wspominany, chociaż to właśnie on, niemal 30 lat wcześniej niż Peano i Dedekind, wykonał zasadniczą część pracy związanej z aksjomatyzacją arytmetyki.

Hermann Günter Grassmann (1809–1877) wydał w roku 1861 książkę o tytule *Lehrbuch der Arithmetik*. Stanowiła ona jedną z pierwszych prób, by wykład arytmetyki oprzeć na kilkunastu podstawowych prawach arytmetycznych, z których następnie można udowodnić wszystkie pozostałe. Arytmetyka przedstawiona przez Grassmanna nie ma explicite formy teorii aksjomatycznej, choć jak twierdzi Hao Wang, taka reinterpretacji tej teorii nie nastręcza trudności ([1957] s. 147). Można się oczywiście spierać, na ile Grassmann był świadomy pojęcia teorii aksjomatycznej. Zagadnienie to, niewątpliwie interesujące z historycznego punktu widzenia, nie jest jednak przedmiotem naszych rozważań. Jest nim natomiast formalna zawartość pracy Grassmanna. Przyjmujemy, że reinterpretacja przedstawiona przez Wanga [ibidem] jest trafna i w dalszej części tekstu będziemy się do niej odnosili.

Znaczenie pracy Grassmanna wydaje się ogromne. Jako pierwszy sformułował on rekurencyjne definicje operacji dodawania i mnożenia. Przedstawił je w formie, która obowiązuje do dzisiaj. Definicje te, jeżeli występują jako aksjomaty, nazywane są często Aksjomatami Grassmanna. Również jako pierwszy sformułował nieelementarny aksjomat indukcji, jako formalną podstawę dowodów przez indukcję. Możliwość dowodzenia przez indukcję jest jedną z charakterystycznych własności arytmetyki i jako taka była znana, i stosowana od dawna. Już w roku 1575 Francesco Maurolino udowodnił tą metodą, że suma pierwszych n liczb nieparzystych wynosi n^2. Jednak inną rzeczą jest stosowanie metody, a inną sformułowanie zasady, która metodę czyni prawomocną, i uświadomienie, że zasada ta powinna stanowić bazę każdej arytmetycznej teorii.

Teoria Grassmanna nie jest oparta na żadnym formalnym systemie logiki, gdyż pojęcie formalnego systemu logiki jeszcze wtedy nie istniało. Formalne pojęcie modelu teorii też oczywiście nie istniało, chociaż każda teoria była konstruowana z myślą o pewnej intuicyjnie rozumianej dziedzinie obiektów, do których odnosiły się pojęcia pierwotne teorii. Możemy zatem przyjąć, że twierdzeniami arytmetyki Grassmanna są te wszystkie zdania w przyjętym przez niego języku, o których da się wykazać, że muszą być prawdziwe w każdej dziedzinie, w której prawdziwy jest wybrany przez niego zbiór praw podstawowych teorii. W takim znaczeniu będziemy mówili o konsekwencji logicznej. Dla języka nieelementarnego zakładamy standardową semantykę.

W interpretacji Wanga arytmetyka Grassmanna jest quasi-aksjomatyczną teorią arytmetyki liczb całkowitych z wyróżnionym podzbiorem liczb dodatnich. Liczba 0 nie jest przez Grassmanna uważana za liczbę dodatnią. Teoria ma charakter quasi-aksjomatyczny, a nie aksjomatyczny, gdyż nie wszystkie pojęcia pierwotne zostały scharakteryzowane metodą aksjomatyczną. W języku, którego Grassmanna używa do budowy swojej teorii, a dokładniej w rekonstrukcji tego języka dokonanej przez Wanga [1957], mamy obok symboli funkcyjnych dla operacji dodawania, mnożenia i negacji, także symbol Pos na oznaczenie podzbioru liczb dodatnich. Wprowadza również

Grassmann jednoargumentowy symbol funkcyjny $\bullet$, który w nietypowy sposób stosuje wyłącznie do stałej 1.

W interpretacji Hao Wanga teoria Grassmanna przedstawia w następujący sposób.

I. zbiór symboli: $=, (,), a, b, c, d, ...$ (zmienne); stała indywiduowa 1, dwuargumentowe symbole funkcyjne $+, \cdot$, jednoargumentowe symbole funkcyjne $\bullet$, $\sim$, symbol Pos na oznaczenie podzbioru uniwersum dziedziny. Ponadto symbole logiczne: kwantyfikatory i spójniki zdaniowe. II. Definicja termu: 1 oraz $1^\bullet$ są termami, zmienne są termami; jeśli s i t są termami, to $(s+t)$ oraz $s \cdot t$ są termami.

III. Przyjęte definicje

$DG1$ $0 = 1 + 1^\bullet$.

$DG2$ Dla dowolnych a oraz b, $a - b$ jest liczbą c taką , że $b + c = a$.

$DG3$ $\sim a = 0 - a$.

$DG4$ $a > b \leftrightarrow a - b \in Pos$.

IV. Aksjomaty

$AG1$ $a = (a+1) + 1^\bullet$

$AG2$ $a = (a + 1^\bullet) + 1$

$AG3$ $a + (b+1) = (a+b) + 1$

$AG4$ $a \cdot 0 = 0$

$AG5$ $1 \in Pos$

$AG6$ $a \in Pos \to a + 1 \in Pos$

$AG7$ $(b = 0 \vee b \in Pos) \to x \cdot (y+1) = x \cdot y + x$

$AG8$ $b \in Pos \to a \cdot \sim b = \sim (a \cdot b)$

$AG9$ dla dowolnego zbioru A, jeżeli $1 \in A$ oraz dla każdego a, jeżeli $a \in A$, to $a + 1 \in A$ oraz $a + 1^\bullet \in A$, to dla każdego a, $a \in A$.

$AG10$ dla dowolnego zbioru A, jeżeli $1 \in A$ oraz dla każdego a, jeżeli $a \in A$, to $a + 1 \in A$, to dla każdego a, jeżeli $a \in Pos$, to $a \in A$.

Symbol $\bullet$ został użyty przez Grassmanna jak jednoargumentowy symbol funkcyjny, jednak zakres stosowalności tego symbolu został ograniczony wyłącznie do stałej 1. Rozsądnie zatem przyjąć, że w rzeczywistości Grassmann w swoim systemie przyjął dwie stałe 1 oraz $1^\bullet$. Następnie zdefiniował stałą 0 przyjmując, że $0 = 1 + 1^\bullet$. Symbol $\sim$ nie został zdefiniowany aksjomatycznie, ale poprzez definicję $DG2$ oraz $DG3$. Teorię opartą o przytoczone powyżej aksjomaty oznaczymy przez AG.

1. **Twierdzenia arytmetyki Grassmanna**

Poniżej przedstawiamy zestaw twierdzeń, które można udowodnić z aksjomatów Grassmanna. Znalezienie dowodów pozostawiamy czytelnikowi jako pożyteczne ćwiczenie zapoznające z funkcjonowaniem systemu Grassmanna. Dla ułatwienia podajemy również twierdzenia pomocnicze oraz zalecaną kolejność dowodzonych twierdzeń.

Fakt 1. *W oparciu o aksjomaty $AG1, AG2, AG3, AG7, AG9$ można udowodnić następujące twierdzenia:*

1.1 $a + 1 = b + 1 \to a = b$,

1.2 $a + 1^\bullet = b + 1^\bullet \to a = b$,

1.3 $a + (b + 1^\bullet) = (a + b) + 1^\bullet$,

1.4 $1 + a = a + 1$,

1.5 $1^\bullet + a = a + 1^\bullet$,

1.6 $(a + 1) + b = a + (1 + b)$,

1.7 $(a + 1^\bullet) + b = a + (1^\bullet + b)$,

1.8 $a + 0 = 0 + a = a$,

1.9 $a \cdot 1 = a$,

1.10 $a + b = b + a$,

1.11 $a + (b + c) = (a + b) + c$,

Udowodnimy teraz, że definicja $DG2$, a więc również definicja $DG3$, są poprawne. W dowodzie wykorzystujemy udowodniony wcześniej fakt, że w teorii AG dodawanie jest działanie łącznym i przemiennym. W prostych przypadkach nie będziemy wprowadzali notacyjnych rozróżnień między symbolami i ich interpretacjami.

Fakt 2. *W oparciu o aksjomaty $AG1, AG2, AG3, AG9$ można udowodnić, że*

$$(\forall x)(\exists! y)\ x + y = 1 + 1^\bullet.$$

Elementy, których suma daje $1 + 1^\bullet$, będziemy nazywali elementami przeciwnymi.

Dowód. Zastosujemy aksjomat $AG9$. Elementem przeciwnym dla elementu 1 jest element $1^\bullet$, gdyż $1 + 1^\bullet = 1 + 1^\bullet$. Załóżmy, że element z jest także elementem przeciwnym względem 1. Wtedy $1 + z = 1 + 1^\bullet = 1^\bullet + 1$ i z Faktów 1.1 oraz 1.10 otrzymujemy $z = 1^\bullet$. Zatem $1^\bullet$ jest jedynym elementem przeciwnym względem 1. Zakładamy, że dla elementu n istnieje dokładnie jeden element przeciwny b. Pokażemy, że dla elementu $n+1$ jedynym elementem przeciwnym jest $k = b+1^\bullet$. Jest tak bowiem $(n+1)+k = (n+1)+(b+1^\bullet) = ((n+1)+b)+1^\bullet = ((n+b)+1)+1^\bullet = n+b = 1+1^\bullet$. Jeżeli dla pewnego elementu z jest $(n + 1) + z = 1 + 1^\bullet$, to $n + (1 + z) = 1 + 1^\bullet$. Stąd $1 + z = b$, gdyż b jest jedynym elementem przeciwnym do n, i z $AG1$ oraz 1.10 $z = b + 1^\bullet = k$. Dla elementu $n + 1^\bullet$ jedynym elementem przeciwnym jest element $k = b + 1$. Jest tak, gdyż $(n + 1^\bullet) + k = (n + 1^\bullet) + (b + 1) = ((n + b) + 1^\bullet) + 1 = n + b = 1 + 1^\bullet$. Jeżeli $(n + 1^\bullet) + z = 1 + 1^\bullet$, to $n + (z + 1^\bullet) = 1 + 1^\bullet$. Stąd $z + 1^\bullet = b$ i $z = b + 1 = k$. □

Niech $\mathfrak{M}$ będzie dowolnym modelem teorii Grassmanna. Z aksjomatów $AG1$, $AG2$, $AG3$, $AG7$ i $AG9$ można zatem udowodnić, że dla dowolnego elementu a uniwersum modelu $\mathfrak{M}$ istnieje dokładnie jeden element b, taki, że $a + b = 0$, przy czym dla 1 takim elementem oczywiście jest $1^\bullet$. Możemy więc zdefiniować na całym uniwersum operację negacji[1] przyjmując, że dla każdego a, $\sim a$ jest elementem przeciwnym. Operacja ta będzie rozszerzeniem pierwotnego pojęcia negacji, które Grassmann stosował wyłącznie do elementu 1. W celu aksjomatycznego zdefiniowania tego pojęcia należy do Aksjomatyki Grassmanna dodać jeden aksjomat. Możemy wtedy przyjąć, że jedyną stałą w systemie jest stała 1. Symbol 0 będzie oznaczał, jak u Grassmanna, term stały $1+ \sim 1$. Wprowadzimy również do języka jednoargumentowy symbol predykatywny P na oznaczenie własności bycia liczbą dodatnią. Po tej modyfikacji otrzymujemy system aksjomatyczny AG^1 następującej postaci.

$AG^1 0$ $\quad a+ \sim a = 0$

$AG^1 1$ $\quad a = (a + 1)+ \sim 1$

$AG^1 2$ $\quad a = (a+ \sim 1) + 1$

$AG^1 3$ $\quad a + (b + 1) = (a + b) + 1$

$AG^1 4$ $\quad a \cdot 0 = 0$

$AG^1 5$ $\quad P(1)$

$AG^1 6$ $\quad P(a) \to P(a + 1)$

$AG^1 7$ $\quad (b = 0 \vee P(b)) \to a \cdot (b + 1) = a \cdot b + a$

$AG^1 8$ $\quad P(b) \to a\cdot \sim b =\sim (a \cdot b)$

[1] Używam terminu negacja na oznaczenie unarnej operacji dla wygody, zdając sobie sprawę, że standardowo termin ten jest używany na oznaczenie unarnego funktora zdaniowego.

AG^19 dla dowolnego zbioru A, jeżeli $1 \in A$ oraz dla każdego a, jeżeli $a \in A$, to $a{+}1 \in A$ oraz $a+ \sim 1 \in A$, to dla każdego a, $a \in A$.

AG^110 dla dowolnego zbioru A, jeżeli $1 \in A$ oraz dla każdego a, jeżeli $a \in A$, to $a + 1 \in A$, to dla każdego a, jeżeli $P(a)$, to $a \in A$.

Wszystkie wymienione wcześniej twierdzenia teorii AG pozostają twierdzeniami teorii AG^1, jeżeli tylko zastąpimy term $1^\bullet$ termem ~ 1. Ponadto twierdzeniami są następujące zdania. Dowody tak jak poprzednio pozostawiamy czytelnikowi jako proste ćwiczenie.

Fakt 3. *Twierdzeniami teorii AG^1 są następujące zdania:*

3.1 $\sim (a+1) =\sim a+ \sim 1,$

3.2 $\sim\sim a = a,$

3.3 $a\cdot \sim 1 =\sim a,$

3.4 $(P(a) \wedge a \neq 1) \rightarrow (\exists y)(P(y) \wedge a = y + 1),$

3.5 $(\neg P(a) \wedge a \neq 0) \rightarrow P(\sim a),$

3.6 $P(a) \rightarrow ((a+ \sim 1 = 0) \vee P(a+ \sim 1)),$

3.7 $a \cdot (b+ \sim 1) = a \cdot b+ \sim a,$

3.8 $a \cdot (b + 1) = a \cdot b + a,$

3.9 $1 \cdot a = a \cdot 1 = a,$

3.10 $\sim 1 \cdot a = a\cdot \sim 1 =\sim a,$

3.12 $\sim b \cdot a =\sim (b \cdot a),$

3.13 $a \cdot b = b \cdot a,$

3.14 $a \cdot (b + c) = (a \cdot b + a \cdot c),$

3.15 $a \cdot (b \cdot c) = (a \cdot b) \cdot c.$

Dla naszych dalszych rozważań jest istotne, jakie aksjomaty teorii AG^1 zostały użyte w dowodach powyższych twierdzeń. Okazuje się, że aksjomat AG^110 został użyty dopiero w dowodzie twierdzenia 3.4. Wcześniej nie był on wykorzystywany. Można też wykazać, że bez odwołania się do tego aksjomatu nie można twierdzenia 3.4 udowodnić. Twierdzenie to mówi, że każda liczba dodatnia różna od liczby 1 ma poprzednik, który jest liczbą dodatnią. Jeżeli rozważymy standardowy model arytmetyki liczb całkowitych ze standardowo zdefiniowanymi działaniami i przyjmiemy, że interpretacją symbolu predykatywnego P jest zbiór liczb całkowitych większych niż np. 2, to powyższe zdanie będzie w tym modelu fałszywe, a aksjomaty $AG^10 - AG^19$ będą prawdziwe. Zdanie to jest więc niedowodliwe w oparciu o te aksjomaty.

2. **Modele arytmetyki Grassmanna**

Z udowodnionych wcześniej faktów wynika, że każdy model arytmetyki Grassmanna musi być przemiennym pierścieniem z jedynką, w którym wyróżnionym podzbiorem elementów dodatnich jest najmniejszy zbiór zawierający element 1 i domknięty na operację dodawania. Implikacja w drugą stronę jednak nie zachodzi. Ze względu na obecność nieelementarnych aksjomatów indukcji modelami arytmetyki Grassmanna nie będą na przykład niestandardowe – to znaczy zawierające w uniwersum elementy niestandardowe – modele elementarnej arytmetyki liczb całkowitych, które również są pierścieniami spełniającymi odpowiednie warunki. Jeżeli jednak weźmiemy dowolny pierścień przemienny z jedynką, w którym wyróżniony podzbiór pokrywa się z najmniejszym podzbiorem zawierającym 1 i domkniętym na dodawanie oraz w którym nie istnieją podpierścienie właściwe, to wszystkie aksjomaty teorii Grassmanna są w nim spełnione, a zatem jest to model teorii Grassmanna. Możemy odnotować zatem następujący fakt.

Fakt 4. *Klasa modeli arytmetyki Grassmanna pokrywa się z klasą pierścieni przemiennych z jedynką, które nie posiadają podpierścieni właściwych oraz w których wyróżnionym podzbiorem jest najmniejszy zbiór generowany przez element* 1 *ze względu na operację dodawania.*

Hao Wang zauważył, że aksjomaty Grassmanna spełnia również model trywialny. Oznacza to, że w arytmetyce Grassmanna nie można udowodnić między innymi następujących twierdzeń

$$1 + 1 \neq 1,$$

$$0 + 1 \neq 0,$$

$$\neg P(0),$$

$$(\exists x)\, \neg P(x),$$

$$(\forall x)\, x + 1 \neq x,$$

$$(\forall x)\, x + 1 = 1 \rightarrow \neg P(x).$$

Aksjomaty Grassmanna są spełnione również w pierścieniach $\mathfrak{C}_n$, reszt modulo n z wyróżnionym podzbiorem identycznym z całym uniwersum. Oznacza to, że w teorii Grassmana nie da się udowodnić, wbrew opinii Wanga, również prawa skracania dla mnożenia

$$c \neq 0 \wedge c \cdot a = c \cdot b \to a = b,$$

ani prawa całkowitości

$$a \cdot b = 0 \to a = 0 \vee b = 0.$$

Jest tak ponieważ w pierścieniu $\mathfrak{C}_4$ mamy $2 \cdot 2 = 2 \cdot 0 = 0$. Zatem definicja $DG4$ nie definiuje relacji porządkującej. Można udowodnić, że jest to relacja zwrotna i przechodnia, ale nie można udowodnić jej słabej antysymetrii.

Wang pisze [1957]: „Grassmann's calculus is defective in at last one important respect. There is no explicit mention of the fact that different numbers have different successors, or the fact that 1 is not the successor of any positive integer"[2]. Jednakże pierwsza z tych obserwacji wydaje się niepoprawna. Nie jest prawdą, że wśród aksjomatów arytmetyki Grassmanna brakuje zdania mówiącego, że różne liczby mają różne następniki

$$a \neq b \to (a + 1 \neq b + 1).$$

Jeżeli $a+1 = b+1$, to $(a+1)+\sim 1 = (b+1)+\sim 1$ i z aksjomatu $AG1$ otrzymujemy, że $a = b$. Funkcja następnika $n(a) = a + 1$ oraz funkcja poprzednika $p(a) = a + \sim 1$ są określone prawidłowo. Aksjomaty $AG1$ oraz $AG2$ gwarantują, że na każdym zbiorze Z, będącym uniwersum interpretacji arytmetyki Grassmanna, spełnione są warunki $n \circ p = id_Z$ oraz $p \circ n = id_Z$, gdzie id_Z jest funkcją identyczności na zbiorze Z. A zatem musi być tak, że operacje te są bijekcjami odwzorowującymi zbiór Z w siebie oraz $n^{-1} = p$ i $p^{-1} = n$.

Przez $\mathfrak{C}$ oznaczymy model standardowy liczb całkowitych z wyróżnionym podzbiorem liczb dodatnich. Intencją Grassmanna było, by jedynym modelem z dokładnością do izomorfizmu, w którym prawdziwe są wszystkie aksjomaty, był model $\mathfrak{C}$. Pokazaliśmy, że warunek ten nie jest spełniony. Aksjomatyka Grassmanna wymaga zatem uzupełnienia. Przypadek teorii Grassmanna nie jest w tym względzie odosobniony. Przykładem może być nieelementarna aksjomatyka teorii liczb całkowitych, już bez pojęcia liczby dodatniej (naturalnej), zamieszczona w [1980].

[2] Wang [1957] s. 149.

3. **Trafne rozszerzenie teorii AG**

Powiemy, że teoria T jest trafnym rozszerzeniem teorii AG, jeżeli zbiór aksjomatów teorii T powstał poprzez dodanie do zbioru aksjomatów teorii AG skończonego zbioru zdań elementarnych w jej języku (przy ewentualnym równoczesnym usunięciu aksjomatów zbędnych) oraz jedynym modelem teorii T z dokładnością do izomorfizmu jest model $\mathfrak{C}$, tzn. otrzymana aksjomatyka jest kategoryczna. Jest wiele różnych sposobów trafnego rozszerzenia teorii AG^1 (a więc i AG). Zaproponujemy jeden z nich. Do zbioru aksjomatów dodajemy następujący elementarny aksjomat:

G* $(\forall x)\, \neg P(x) \wedge P(x+1) \leftrightarrow x = 0.$

Tak rozszerzoną teorię oznaczymy przez AG^2. Można zamiast aksjomatu G^* przyjąć zdanie $\neg P(0)$, jednakże dowody są wtedy nieco bardziej skomplikowane i wymagają odwołania się do pewnych twierdzeń formułowanych w metajęzyku.

W dowodach twierdzeń teorii AG^1, przedstawionych do tej pory, aksjomat $AG^1 10$ został bezpośrednio użyty tylko raz, w dowodzie Faktu 3.4. Jeżeli więc pokażemy, że twierdzenie to można udowodnić w teorii AG^2 bez użycia aksjomatu $AG^1 10$, będzie to oznaczało, że wszystkie wcześniej udowodnione twierdzenia można udowodnić w AG^2 bez odwoływania się do aksjomatu $AG^1 10$.

Fakt 5. *W oparciu o aksjomaty $AG^1 1$, $AG^1 2$, $AG^1 3$, $AG^1 9$, G^* można udowodnić następujące twierdzenie:*

$$(\forall x)\{\, P(x) \wedge x \neq 1 \rightarrow (\exists y) P(y) \wedge y + 1 = x\}.$$

Dowód. Niech Z będzie zbiorem wszystkich elementów, spełniających odpowiednią formułę. Oczywiście $1 \in Z$. Zakładamy, że pewien element $n \in Z$, tzn. prawdziwe jest zdanie

$$(P(n) \wedge n \neq 1) \rightarrow (\exists y)\, (P(y) \wedge x = y + 1).$$

Rozważmy element $n+1$ taki, że $P(n+1)$ oraz $n+1 \neq 1$. Wtedy musi być tak, że $P(n)$. Gdyby bowiem było $\neg P(n)$, to z G^* otrzymujemy $n = 0$ i $1 \neq 1$. Możliwe są dwa przypadki:

1. $n = 1$. Wystarczy wtedy za y przyjąć 1, gdyż $P(1)$ oraz $n + 1 = 1 + 1$. Zatem $n + 1 \in Z$.

2. $n \neq 1$. Skoro $P(n)$ i $n \neq 1$, to z założenia istnieje element m taki, że $P(m)$ oraz $m + 1 = n$. Wtedy z aksjomatu $AG^1 6$ mamy $P(m+1)$ oraz $n + 1 = (m + 1) + 1$. Wystarczy przyjąć, że szukanym elementem jest $m + 1$. Zatem $n + 1 \in Z$.

Rozważmy teraz element $n+\sim 1$. Zakładamy, że $P(n+\sim 1)$ oraz $n+\sim 1 \neq 1$. Załóżmy, że $\neg P((n+\sim 1)+\sim 1)$. Wtedy z G^* otrzymujemy, że $(n+\sim 1)+\sim 1) = 0$ i $n+\sim 1 = 1$. Sprzeczność. Zatem jest $P((n+\sim 1)+\sim 1)$. Wystarczy przyjąć, że szukanym elementem jest $(n+\sim 1)+\sim 1$. □

Fakt 6. *W teorii AG^2 można bez odwoływania się do aksjomatu $AG^1 10$ udowodnić następujące twierdzenia.*

6.1 $0 \neq 1$,

6.2 $(\forall x) x \neq x+1$,

6.3 $\forall x) x \neq x+\sim 1$,

6.4 $(\forall x)(\forall y)\ (P(x) \wedge P(y) \rightarrow P(x+y))$,

6.5 $(\forall x) x+x=0 \rightarrow x=0$,

6.6 $(\forall x) P(x) \rightarrow \neg P(\sim x)$,

6.7 $(\forall x) x \neq 0 \rightarrow x \neq \sim x$,

6.8 $(\forall x)(\forall y)\ (x \neq 0 \wedge y \neq 0 \wedge x \neq y) \rightarrow P(x+\sim y) \vee P(y+\sim x)$,

Definiujemy teraz metodą Grassmanna relację binarną $\leq$ przyjmując, że

$$x \leq y \equiv x=y \vee (\exists z) P(z) \wedge x+z=y.$$

Korzystając z już udowodnionych twierdzeń, łatwo pokazać, że

Fakt 7. *W teorii AG^2 można bez odwoływania się do aksjomatu $AG^1 10$ udowodnić następujące twierdzenia.*

7.1 $(\forall x) x \leq x$,

7.2 $(\forall x)(\forall y) x \leq y \wedge y \leq x \rightarrow x=y$,

7.3 $(\forall x)(\forall y)(\forall z) x \leq y \wedge y \leq z \rightarrow x \leq z$,

7.4 $(\forall x)(\forall y)\ x \leq y \vee y \leq x$.

7.5 $(\forall x) x<1 \rightarrow \neg P(x)$.

7.6 $(\forall x)(\forall y) x \leq y \rightarrow x<y+1$.

Relacja $\leq$ jest więc relacją porządkującą. Możemy teraz udowodnić w teorii AG^2 twierdzenie o indukcji zupełnej. W sposób istotny wykorzystamy później fakt, że w dowodzie nie zostanie użyty aksjomat $AG^1 10$.

Fakt 8. *W teorii AG^2 twierdzeniem jest następujące zdanie: jeżeli do zbioru Z należy każdy element dodatni n, jeżeli tylko należą do niego wszystkie elementy dodatnie i mniejsze od n, to do zbioru Z należą wszystkie elementy dodatnie.*

Dowód. Zakładamy, że zbiór Z spełnia powyższy warunek, tzn. jeżeli do Z należą wszystkie elementy dodatnie i mniejsze od pewnego elementu dodatniego n, to n także należy do Z. Pokażemy, że dla każdej liczby dodatniej n, wszystkie liczby dodatnie mniejsze lub równe n należą do zbioru Z. Oczywiście w sposób trywialny z faktu tego wynika, że wszystkie liczby dodatnie należą do zbioru Z. Definiujemy zbiór pomocniczy Z^* przyjmując, że element n należy do Z^* wtedy i tylko wtedy, gdy spełnia warunek: jeżeli n jest elementem dodatnim, to wszystkie elementy dodatnie mniejsze lub równe n należą do zbioru Z. Rozważmy element 1. Jest to element dodatni i wszystkie mniejsze elementy dodatnie należą do zbioru Z (gdyż one nie istnieją). Zatem z założenia $1 \in Z$. Stąd wszystkie dodatnie elementy mniejsze lub równe od 1 należą do Z. W takim razie $1 \in Z^*$. Zakładamy teraz , że $n \in Z^*$.

Rozważmy element $n + 1$. Załóżmy, że jest to element dodatni. Są dwie możliwości. Jeżeli $n + 1 = 1$, to wiemy już, że $n + 1 \in Z^*$. W przeciwnym wypadku element $(n+1)+\sim 1 = n$ jest elementem dodatnim (zob. Fakt 5). Z założenia wszystkie elementy dodatnie mniejsze lub równe od n należą do Z. Oznacza to, że wszystkie elementy dodatnie mniejsze od $n + 1$ należą do Z (zob. Fakt 7.6). Zatem $n + 1 \in Z$ i $n + 1 \in Z^*$.

Rozważmy element $n+ \sim 1$. Zakładamy, że jest to element dodatni. Wtedy z aksjomatu $AG^1 6$ n też musi być elementem dodatnim. Zatem wszystkie elementy dodatnie mniejsze lub równe n należą do Z. Jeżeli jakiś element dodatni jest mniejszy lub równy $n+ \sim 1$, to jest mniejsze od n. Zatem wszystkie te elementy należą do Z i stąd $n+ \sim 1 \in Z^*$.

Z aksjomatu $AG^1 9$ otrzymujemy więc, że wszystkie elementy należą do zbioru Z^*. Dla każdego elementu dodatniego n, wszystkie elementy dodatnie mniejsze lub równe z n należą do Z. Stąd wszystkie elementy dodatnie należą do Z. □

Prostym wnioskiem z Faktu 8 jest następujący fakt będący pewnym wariantem zasady minimum.

Fakt 9. *W teorii AG^2 twierdzeniem jest następujące zdanie: dla dowolnego zbioru Z, jeżeli zbiór elementów dodatnich nie należących do zbioru Z jest niepusty, to w zbiorze tym istnieje element najmniejszy.*

Dowód. Załóżmy, że istnieje element dodatni nienależący do zbioru Z. Wtedy z Faktu 8 musi istnieć element dodatni n taki, że wszystkie elementy dodatnie mniejsze od n należą do Z oraz n nie należy do Z. Oczywiście jest on elementem najmniejszym w zbiorze elementów dodatnich nie należących do zbioru Z. □

Możemy teraz pokazać, że aksjomat $AG^1 10$ jest w aksjomatyce AG^2 aksjomatem zależnym. Korzystamy z faktu, że wszystkie wcześniejsze twierdzenia teorii AG^2 zostały udowodnione bez użycia aksjomatu $AG^1 0$.

Fakt 10. *W aksjomatyce AG^2 aksjomat $AG^1 10$ jest aksjomatem zależnym i może być wyeliminowany.*

Dowód. Zakładamy, że do pewnego zbioru Z należy 1 oraz spełniony jest warunek: $(\forall x) x \in Z \to x + 1 \in Z$. Przypuśćmy, że nie wszystkie elementy dodatnie należą do Z. Wtedy istnieje najmniejszy element dodatni n taki, $n \notin Z$. Z założenia $n \neq 1$. Wiemy, że dla każdego elementu dodatniego różnego od 1 istnieje dodatni poprzednik. Zatem istnieje element dodatni p taki, że $n = p + 1$. Z warunku minimalności elementu n wnosimy, że $p \in Z$. Wtedy jednak z założenia otrzymujemy, że $p + 1 = n \in Z$. Sprzeczność. □

Można zatem pominąć aksjomat $AG^1 10$. Tak otrzymaną teorię oznaczymy przez AG^3.

Fakt 11. *Wszystkie modele arytmetyki Grassmanna AG^3 (więc też AG^2) są izomorficzne z modelem standardowym $\mathfrak{C}$.*

Dowód. Niech $\mathfrak{M}$ będzie dowolnym modelem teorii AG^3. Definiujemy odwzorowanie $h : \mathfrak{M} \mapsto \mathfrak{C}$, przyjmując

$$h(x) = \begin{cases} f(x) & \text{if } x \text{ jest dodatnim elementem w } M \\ f'(x) & \text{if } x \text{ nie jest dodatnim elementem w } M, \end{cases}$$

gdzie

$$f(1^{\mathfrak{M}}) = 1^{\mathfrak{C}}$$
$$f(x +^{\mathfrak{M}} 1^{\mathfrak{M}}) = f(x) +^{\mathfrak{C}} 1^{\mathfrak{C}}$$

oraz

$$f'(x) = \begin{cases} 0^{\mathfrak{C}} & \text{jeżeli } x = 0^{\mathfrak{M}} \\ \sim^{\mathfrak{C}} f(\sim^{\mathfrak{M}} x) & \text{jeżeli } x \neq 0^{\mathfrak{M}}. \end{cases}$$

Powyższa definicja jest poprawna, ponieważ wiemy, że jeżeli jakiś element uniwersum modelu $\mathfrak{M}$ jest różny od $0^{\mathfrak{M}}$ i nie jest dodatni, to jego jedynym elementem przeciwnym jest element dodatni (zob. Fakt 6.7). Funkcja h odwzorowuje zbiór elementów dodatnich modelu $\mathfrak{M}$ w zbiór elementów dodatnich modelu $\mathfrak{C}$ oraz zbiór elementów niedodatnich modelu $\mathfrak{M}$ w zbiór elementów niedodatnich modelu $\mathfrak{C}$. Warunek homomorficzności dla symbolu predykatywnego P jest więc spełniony. Pokażemy, że dla dowolnego elementu a uniwersum modelu $\mathfrak{M}$ funkcja h spełnia następujące warunki:

$$f(a +^{\mathfrak{M}} 1^{\mathfrak{M}}) = f(a) +^{\mathfrak{C}} 1^{\mathfrak{C}} \tag{1}$$
$$f(a +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}}) = f(a) +^{\mathfrak{C}} \sim^{\mathfrak{C}} 1^{\mathfrak{C}} \tag{2}$$
$$f(\sim^{\mathfrak{M}} a) = \sim^{\mathfrak{C}} f(a). \tag{3}$$

Pokażemy najpierw, że identyczności te są spełnione dla dowolnego dodatniego elementu a. Identyczność (1) jest spełniona dla elementów dodatnich z definicji. Jeżeli $a = 1$, to $f(1^{\mathfrak{M}} +^{\mathfrak{M}} \sim 1^{\mathfrak{M}}) = f(0^{\mathfrak{M}}) = 0^{\mathfrak{C}} = 1^{\mathfrak{C}} +^{\mathfrak{C}} \sim^{\mathfrak{C}} 1^{\mathfrak{C}} = f(1^{\mathfrak{M}}) +^{\mathfrak{C}} \sim 1^{\mathfrak{C}})$. W przeciwnym razie $a = p +^{\mathfrak{M}} 1^{\mathfrak{M}}$ dla pewnego dodatniego elementu p. Wtedy $f(p +^{\mathfrak{M}} 1^{\mathfrak{M}}) = f(p) +^{\mathfrak{C}} 1^{\mathfrak{C}}$, a zatem $f(a +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}}) = f(p +^{\mathfrak{M}} 1^{\mathfrak{M}} +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}}) = f(p) = f(p +^{\mathfrak{M}} 1^{\mathfrak{M}}) +^{\mathfrak{C}} \sim^{\mathfrak{C}} 1^{\mathfrak{C}} = f(a) +^{\mathfrak{C}} \sim^{\mathfrak{C}} 1^{\mathfrak{C}}$. Wreszcie jeżeli a jest elementem dodatnim, to $\sim^{\mathfrak{M}} a$ jest elementem niedodatnim i z definicji $f(\sim^{\mathfrak{M}} a) = \sim^{\mathfrak{C}} f(\sim^{\mathfrak{M}} \sim^{\mathfrak{M}} a) = \sim^{\mathfrak{C}} f(a)$. Zakładamy teraz, że element a nie jest dodatni. Łatwo sprawdzić, że wszystkie identyczności zachodzą dla $0^{\mathfrak{M}}$. Zakładamy, że $a \neq 0^{\mathfrak{M}}$. Wtedy $\sim^{\mathfrak{M}} a$ jest elementem dodatnim. Pokazaliśmy już, że $f(\sim^{\mathfrak{M}} \sim^{\mathfrak{M}} a) = \sim^{\mathfrak{C}} f(\sim^{\mathfrak{M}} a)$. Zatem $f(\sim^{\mathfrak{M}} a) = \sim^{\mathfrak{C}} f(a)$. Wiemy też, że $f(\sim^{\mathfrak{M}} a +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}}) = f(\sim^{\mathfrak{M}} a) +^{\mathfrak{C}} \sim^{\mathfrak{C}} 1^{\mathfrak{C}})$, więc $f(\sim^{\mathfrak{M}} (a +^{\mathfrak{M}} 1^{\mathfrak{M}})) = \sim^{\mathfrak{C}} (f(a) +^{\mathfrak{C}} 1^{\mathfrak{C}}))$ i $f(a +^{\mathfrak{M}} 1^{\mathfrak{M}})) = f(a) +^{\mathfrak{C}} 1^{\mathfrak{C}})$. Wiemy, że

$$\begin{aligned} f(\sim^{\mathfrak{M}} a +^{\mathfrak{M}} 1^{\mathfrak{M}}) &= f(\sim^{\mathfrak{M}} a) +^{\mathfrak{C}} 1^{\mathfrak{C}}) \\ &= \sim^{\mathfrak{C}} f(a) +^{\mathfrak{C}} 1^{\mathfrak{C}} \\ &= \sim^{\mathfrak{C}} (f(a) +^{\mathfrak{C}} \sim^{\mathfrak{C}} 1^{\mathfrak{C}}). \end{aligned}$$

Z drugiej strony

$$\begin{aligned} f(\sim^{\mathfrak{M}} a +^{\mathfrak{M}} 1^{\mathfrak{M}}) &= f(\sim^{\mathfrak{M}} (a +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}})) \\ &= \sim^{\mathfrak{C}} f(a +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}}). \end{aligned}$$

Otrzymujemy więc, że $f(a +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}}) = f(a) +^{\mathfrak{C}} \sim^{\mathfrak{C}} 1^{\mathfrak{C}}$, co kończy tę część dowodu.

Z łatwością pokazujemy teraz, że odwzorowanie f jest homomorfizmem, tzn. dla dowolnych elementów a i b z uniwersum modelu $\mathfrak{M}$ spełnione są warunki

$$f(a +^{\mathfrak{M}} b) = f(a) +^{\mathfrak{C}} f(b) \tag{4}$$
$$f(a \cdot^{\mathfrak{M}} b) = f(a) \cdot^{\mathfrak{C}} f(b) \tag{5}$$
$$f(\sim^{\mathfrak{M}} a) = \sim^{\mathfrak{C}} f(a). \tag{6}$$

Zachodzenie warunku (6) zostało już pokazane. Dwa pozostałe warunki dowodzimy, odwołując się do aksjomatu $G10$. Jeżeli $b = 1^{\mathfrak{M}}$ to wiemy już, że warunki są spełnione. Zakładamy, są one spełnione dla pewnego elementu m. Wtedy

$$\begin{aligned} f(a +^{\mathfrak{M}} (m +^{\mathfrak{M}} 1^{\mathfrak{M}}) &= f(a +^{\mathfrak{M}} m) +^{\mathfrak{C}} 1^{\mathfrak{C}} \\ &= (f(a) +^{\mathfrak{C}} f(m)) +^{\mathfrak{C}} 1^{\mathfrak{C}} \\ &= f(a) +^{\mathfrak{C}} f(m +^{\mathfrak{M}} 1^{\mathfrak{M}}). \end{aligned}$$

Podobnie

$$\begin{aligned} f(a +^{\mathfrak{M}} (m +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}})) &= f(a +^{\mathfrak{M}} m) +^{\mathfrak{C}} \sim^{\mathfrak{C}} 1^{\mathfrak{C}} \\ &= (f(a) +^{\mathfrak{C}} f(m)) +^{\mathfrak{C}} \sim^{\mathfrak{C}} 1^{\mathfrak{C}} \\ &= f(a) +^{\mathfrak{C}} f(m +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}}). \end{aligned}$$

Korzystamy teraz z faktu, że f jest zachowuje operację dodawania.

$$\begin{aligned} f(a \cdot^{\mathfrak{M}} (m +^{\mathfrak{M}} 1^{\mathfrak{M}})) &= f(a \cdot^{\mathfrak{M}} m +^{\mathfrak{M}} a) \\ &= f(a \cdot^{\mathfrak{M}} m) +^{\mathfrak{C}} f(a) \\ &= (f(a) \cdot^{\mathfrak{C}} f(m)) +^{\mathfrak{C}} f(a)) \\ &= f(a) \cdot^{\mathfrak{C}} (f(m) +^{\mathfrak{C}} 1^{\mathfrak{C}}) \\ &= f(a) \cdot^{\mathfrak{C}} f(m +^{\mathfrak{M}} 1^{\mathfrak{M}}). \end{aligned}$$

A także

$$\begin{aligned} f(a \cdot^{\mathfrak{M}} (m +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}})) &= f(a \cdot^{\mathfrak{M}} m +^{\mathfrak{M}} \sim^{\mathfrak{M}} a) \\ &= f(a \cdot^{\mathfrak{M}} m) +^{\mathfrak{C}} f(\sim^{\mathfrak{M}} a) \\ &= (f(a) \cdot^{\mathfrak{C}} f(m)) +^{\mathfrak{C}} \sim^{\mathfrak{C}} f(a) \\ &= f(a) \cdot^{\mathfrak{C}} (f(m) +^{\mathfrak{C}} \sim^{\mathfrak{C}} 1^{\mathfrak{C}}) \\ &= f(a) \cdot^{\mathfrak{C}} f(m +^{\mathfrak{M}} \sim^{\mathfrak{M}} 1^{\mathfrak{M}}). \end{aligned}$$

Trzeba jeszcze pokazać, że odwzorowanie f jest bijekcją. Niech a i b będą różnymi elementami uniwersum modelu $\mathfrak{M}$ takimi, że $f(a) = f(b)$. Wtedy $a <^{\mathfrak{M}} b$ lub $b <^{\mathfrak{M}} a$. Zatem istnieje dodatni element s taki, że $a +^{\mathfrak{M}} s = b$ lub $b +^{\mathfrak{M}} s = a$. Załóżmy, że zachodzi pierwszy przypadek (w drugim postępujemy analogicznie). Wtedy $f(a) +^{\mathfrak{C}} f(s) = f(b)$ i $f(s) = 0$, co jest sprzeczne z definicją funkcji f. Pozostaje pokazać, że odwzorowanie f jest surjekcją. Zakładamy, że istnieje element $c \in C$ taki, że dla każdego $m \in M$, $f(m) \neq c$. Możemy przyjąć, że jest to element dodatni. Jeżeli bowiem c nie jest elementem dodatnim, to musi być różny od $0^{\mathfrak{C}}$. Wtedy $\sim^{\mathfrak{C}} c$ jest elementem dodatnim. Gdyby istniał element $m \in M$ taki, że $f(m) =\sim^{\mathfrak{C}} c$, to $f(\sim^{\mathfrak{M}} m) =\sim^{\mathfrak{C}}\sim^{\mathfrak{C}} c = c$. Istnieje zatem najmniejszy element dodatni $a \in C$ nienależący do zbioru wartości odwzorowania f i musi on być różny od $1^{\mathfrak{C}}$. Zatem istnieje element dodatni b taki, że $b +^{\mathfrak{C}} 1^{\mathfrak{C}} = a$. Dla elementu b istnieje element $d \in M$ taki, że $f(d) = b$. Wtedy jednak $f(d +^{\mathfrak{M}} 1^{\mathfrak{M}}) = f(d) +^{\mathfrak{C}} 1^{\mathfrak{C}} = b +^{\mathfrak{C}} 1^{\mathfrak{C}} = a$. Sprzeczność. □

Bibliografia

Judah, Goldstern [1998] – H. Judah, M. Goldstern, *The Incompleteness Phenomenon. A New Course in Mathematical Logic,* AK Peters, Wellesley, MA 1998.

Grassmann [1861] – H. Grassmann, *Lerhbuch der Arithmetic*, 1961.

Słupecki, Hałkowska, Piróg-Rzepecka [1980] – J. Słupecki, K. Hałkowska, K. Piróg-Rzepecka, *Elementy arytmetyki teoretycznej*, Wydawnictwo Szkolne i Pedagogiczne, Warszawa 1980.

Wang [1957] – H. Wang, *The Axiomatization of Arithmetic*, „The Journal of Symbolic Logic" 22 (2) June 1957.