ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1979

Seria: MATEMATYKA-FIZYKA z. 35 Nr kol. 624

Piotr Włodzimierz GAWRON

ROZWIĄZANIE RÓWNANIA $f^p = h$ W GRUPIE BIJEKCJI ZBIORU X

Streszczenie. W pracy podajemy warunek konieczny i wystarczający istnienia rozwiązań równania $f^p = h$ w grupie bijekcji zbioru X dla p będącego liczbą pierwszą. Rozwiązanie tego problemu dla p = 2 zostało podane przez Donalda Solitara (Kanada) na zebraniu PTM w Katowicach w 1975 roku. Pierwsze bardziej ogólne warunki podaliśmy w [1]. Ogólniejsze rozwiązanie uzyskał Łojasiewicz w [2].

Wprowadzimy następujące oznaczenia:

G - grupa wszystkich bijekcji zbioru X,

F, H - podgrupy cykliczne generowane odpowiednio przez elementy $f, h \in G$,

M - zbiór liczb naturalnych różnych od 0 z dołączonym elementem $\aleph_0$,

Hx, Fx - orbity punktu x względem naturalnego działania grup H i F na zbiorze X,

$n(h) = \bigcup \{Hx : |Hx| = n\}, \quad n \in M,$

$\bar{n}(h) = \left|\{Hx : |Hx| = n\}\right|, \quad n \in M,$

analogicznie definiujemy $n(f)$ i $\bar{n}(f)$.

Widzimy, że $X = \bigcup\{n(h) : n \in M\} = \bigcup\{\bar{n}(f) : n \in M\}$.

Dla krótkości oznaczeń założymy, że każde $m \in M$ dzieli dowolną liczbę kardynalną nieskończoną.

Teraz możemy sformułować

Twierdzenie

Jeżeli p jest liczbą pierwszą i $h \in G$, to zachodzi równoważność

$$(\exists f \in G)\ f^p = h \iff (\forall n \in M)\ p \mid n \Rightarrow p \mid \bar{n}(h).$$

Dowód

Niech dla pewnych $f \in G$ i $n \in M$, $f^p = h$ i $p \mid n$. Dowiedźmy, że $p \mid \bar{n}(h)$. Dla $\bar{n}(h) = 0$ teza jest trywialna, w przeciwnym wypadku pewien $x \in n(h) \supset Hx$. Dla pewnego $m \in M$ x należy też do $m(f)$. Rozpatrzymy możliwe przypadki

1a. $p \mid m$ i $p^2 \nmid m$,

1b. $p^2 \mid m$,

2. $p \nmid m$.

Dowiedziemy, że przypadki 1a i 2 są niezgodne z założeniem.

1. Weźmy k takie, by $a = pk$. Orbita Fx jest równa $Fx = \bigcup_{i=1}^{p} Hx_i$, gdzie $x_i = f^{i-1}(x)$ i wszystkie Hx_i są rozłączne, gdyż jeżeli dla pewnych i, $j(1 \leqslant i, j \leqslant p)$, $Hx_i = Hx_j$ wtedy dla pewnego $s \in N$ $h^s(x_i) = x_j$. Podstawiając $h = f^p$ mamy $f^{i-j+sp}(x) = x$, a ponieważ $x \in m(f)$ i $p|m$ więc p dzieli $sp+i-j$, czyli $i = j$. Z powyższego każda orbita względem F rozpada się na p orbit względem H, zatem $x \in k(h)$, czyli $k = n$.

1a. Gdy $p^2 \nmid m$, wtedy $p \nmid n$ co sprzeczne z założeniem.

1b. Gdy $p^2 | m$, to $p|n$ oraz każda orbita względem F leżąca w $m(f)$ rozpada się na p orbit względem H, zawartych w $n(h)$. Łatwo zauważyć, że każda orbita $Hx \subset n(h)$ powstaje w taki sposób. W związku z tym $p|\bar{n}(h)$.

2. Jeżeli $p \nmid m$, to istnieją liczby całkowite a i b takie że $ap+bm=1$. Wtedy

$$f(x) = f^{ap+bm}(x) = f^{ap}(x) = h^a(x).$$

Gdy $y \in Fx$, to z (1) $y = f^s(x) = h^{as}(x) \in Hx$ i na odwrót, jeżeli $y \in Hx$ to $y = h^s(x) = f^{ps}(x) \in Fx$. Widać, że $Fx = Hx$, czyli $m = n$ co sprzeczne z tym, że $p \nmid m$.

Udowodnimy teraz twierdzenie w drugą stronę. Zdefiniujemy funkcję f na każdym niepustym $n(h)$, $n \in M$. Weźmy takie n, by $p|n$, wtedy $p\ \bar{n}(h)$. Z każdej orbity Hx zawartej w $n(h)$ wybieramy po jednym elemencie i wybrane elementy ustawmy w różnowartościowy cięg $\{x_i\}$. Zdefiniujmy

$$f(x_i) = \begin{cases} x_{i+1} & \text{gdy } p \nmid i \\ h(x_{i+1-p}) & \text{gdy } p | i. \end{cases}$$

Ponieważ każdy $x \in n(h)$ należy do pewnego Hx_i, to istnieje $s(x) \in Z$ takie że $x = h^{s(x)}(x_i)$ i kładziemy $f(x) = h^{s(x)} f(x_i)$. Widać, że $f^p(x) = h(x)$.

Niech teraz $p \nmid n$. Wtedy istnieją liczby całkowite a i b takie, że $ap + bn = 1$. Dla $x \in n(h)$ zdefiniujemy $f(x) = h^a(x)$. Stwierdzamy, że $f^p(x) = h^{ap}(x) = h^{ap+bn}(x) = h(x)$. Łatwo widać, że tak określona funkcja f jest bijekcją na zbiorze X oraz jest spełnione $f^p = h$. c.b.d.o.

LITERATURA

[1] Gawron P.W.: O poszukiwaniu pierwiastka w grupie bijekcji dowolnego zbioru. I Sesja SKN Wydz. Mat. Fiz. Pol. Śl., Gliwice 1975, s. 49-51.

[2] Łojasiewicz S.: Solution générale de l'équation fonctionelle f(f(..(f(x))..) = g(x) - Ann. de la Soc. Polon. de Math. T. XXIV, 1951, s. 88-91.

РЕШЕНИЕ УРАВНЕНИЯ $f^p = g$ В ГРУППЕ БИЕКЦИЙ ПРОИЗВОЛЬНОГО МНОЖЕСТВА

Р е з ю м е

В статье даётся необходимое и достаточное условие существованая решения уравнения $f^p = g$ в группе биекций произвольного множества, где p - любое простое число.

THE SOLVABILITY OF THE EQUATION $f^p = g$ IN THE GROUP OF BIJECTIONS OF ANY SET

S u m m a r y

Necessary and sufficient conditions are given for solvability of equation $f^p = g$ in the group of bijections of any set for a prime p.