ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1973

Seria: Matematyka-Fizyka z. 24 Nr kol. 386

Bolesław WANTUŁA

ZAGADNIENIE BROWKINA O CIAŁACH KWADRATOWYCH

J. Browkin postawił następujące zagadnienie[x]:

Czy istnieje ciąg nieskończony: $a_1, a_2, a_3, \ldots$, elementów R/K, spełniających warunek

$$\forall J \subset R/K; \quad i < j \leqslant N(J); \quad i,j \in N; \quad \left| a_i \not\equiv a_j \bmod(J) \right|, \qquad (A)$$

gdzie

K/Q - rozszerzenie algebraiczne ciała liczb wymiernych Q,
R/K - pierścień liczb całkowitych tego rozszerzenia,
J - ideał w R/K
N(J) - norma tego ideału.

D. Barsky podał nieelementarny dowód negatywnej odpowiedzi na postawione zagadnienie [1].

W pracy tej podany jest dowód całkowicie elementarny zagadnienia Browkina w przypadku ciał kwadratowych różnych od ciał: $Q(\sqrt{-1})$, $Q(\sqrt{2})$, $Q(\sqrt{3})$, $Q(\sqrt{-3})$, $Q(\sqrt{-5})$, $Q(\sqrt{-7})$, $Q(\sqrt{17})$.

Jeśli ograniczyć się do zbioru ideałów pierwszych, to odpowiedź dla pewnej klasy rozszerzeń jest również negatywna - dowód podano w przedstawionej pracy. Ograniczenie się do ideałów pierwszych o normie pierwszej, implikuje natychmiastową odpowiedź zmodyfikowany warunek (A) spełniony jest w każdym rozszerzeniu przez ciąg: 1,2,3...

Lemat 1

Jeśli dla rozszerzenia K/Q istnieje ciąg: $a_1, a_2, a_3 \ldots$ elementów R/K spełniający warunek (A), to

$$\forall i < j; \quad i,j \in N; \quad \left| a_i \neq a_j \right|.$$

[x] Informacje o tym zagadnieniu uzyskałem od prof. dr hab. W. Narkiewicza.

Dowód

W przeciwnym wypadku mamy

$$\exists\, m < n; \quad m,n \in N; \quad \left\{a_m = a_n\right\} .$$

Wystarczy wziąć $J \subset R/K$ taki, że $N(J) > n$, wtedy zachodzi

$$a_m \equiv a_n \bmod(J) .$$

Ideał spełniający ten warunek zawsze będzie można znaleźć, ponieważ w R/K istnieją ideały o dowolnie dużej normie.

Lemat 2

Przy założeniu, że $a_i \neq a_j$ warunek (A) jest równoważny warunkom:

$$\forall k \neq 0,1; \quad i \leq j < k; \quad i,j,k \in N: \quad \left\{/N(a_j - a_i)/ < k\right\} \qquad (B)$$

$$\forall k \neq 0,1; \quad i \leq j \leqslant k; \quad i,j,k \in N: \quad \left\{/N(\sum_{m=1}^{j-1} r_m)/ < k\right\} \qquad (C)$$

gdzie

$$r_i = a_{i+1} - a_i .$$

Dowód

Jeśli warunek (B) nie jest spełniony, wtedy

$$\exists k \neq 0;1; \quad 1 < j \leqslant k; \quad i,j,k \in N: \quad \left\{/N(a_j - a_i)/ \geqslant k\right\} .$$

ponieważ:

$$N\left[(a_j - a_i).R/K\right] = /N(a_j - a_i)/ \geqslant k \geqslant j > i, \quad \text{oraz} \quad a_j \equiv a_i \bmod \left[(a_j - a_i) . R/K\right] ,$$

więc warunek (A) nie jest spełniony.

Jeęli natomiast warunek (A) nie jest spełniony, to

$$\exists I \not\subset R/K; \quad 1 < j \leqslant N(I) = k : \left\{a_j \equiv a_i \bmod (I)\right\}$$

i mamy:

$$1 < j \leq k = N(I) \leq N\left[(a_j - a_1) \cdot R/K\right] = |N(a_j - a_1)|,$$

a zatem warunek (B) nie jest spełniony. Równoważność warunków (B) i (C) jest oczywista.

Z lematu 2 wynika natychmiast wniosek: Jeśli ciąg: $a_1, a_2, a_3 \ldots$ elementów R/K spełnia warunek (A), to $|N(r_i)| \leq 1$, $i = 1,2,3,\ldots$, w szczególności $r_1 = a_2 - a_1$ musi być jednostką.

Uwaga: Jeśli $a \in R/K$ oraz $|N(a)| = k$, to będziemy pisali $a = a(k)$ np.: $b(5)$ – oznaczać będzie element R/K, którego norma co do wartości bezwzględnej jest równa 5.

Lemat 3

Dla dowolnego rozszerzenia K/Q zachodzą równoważności:

$$\left[\exists s(1), t(i),\ u(k): \left\{S(1) + t(i) = U(k)\right\}\right] \equiv \left[\exists t(i),\ u(k): \left\{1 + t(i) = u(k)\right\}\right]$$

Dowód

Jeśli $S(1) + t(i) = u(k)$, to mnożąc obie strony równania przez $S(1)^{-1}$ otrzymamy:

$$1 + t(i) \cdot S(1)^{-1} = U(k)\, S(1)^{-1}.$$

Implikacja w drugą stronę jest oczywista.

Lemat 4

Jedynymi ciałami kwadratowymi, w których istnieją elementy $s,\ t \in R/K$ spełniające następujące związki:

1) $1 + t(1) = S(1)$,
2) $1 + t(1) = S(2)$,
3) $1 + t(2) = S(2)$

są odpowiednie ciała:

ad 1) $Q(\sqrt{-3})$, $Q(\sqrt{5})$,
ad 2) $Q(\sqrt{2})$, $Q(\sqrt{3})$, $Q(\sqrt{-1})$,
ad 3) $Q(\sqrt{-7})$, $Q(\sqrt{17})$.

Dowód

Niech $K = Q(\sqrt{D})$, gdzie D jest wolne od kwadratu i różne od 1. Liczby całkowite są postaci:

$$a = \frac{x + y \cdot \sqrt{D}}{2},$$

gdzie $x,y \in Z$, $x \equiv y \bmod (2)$ i dodatkowo $x \equiv y \equiv 0 \bmod (2)$, gdy $D \equiv 2,3 \bmod (4)$;

$$N(a) = \frac{x^2 - y^2 D}{4}.$$

Jeśli

$$t(k) = \frac{x + y \cdot \sqrt{D}}{2},$$

to: $1 + t(k) = S(1)$ zapisze się w postaci

$$\frac{x + y \cdot D + 2}{2} = S(1)$$

i otrzymamy:

$$N(1 + t(k)) = \frac{4 + 4x + x^2 - y^2 D}{4} = \pm 1,$$

stąd

a) $x = \pm 1 - 1 - k$, gdy $N(t(k)) = k$

b) $x = \pm 1 - 1 + k$, gdy $N(t(k)) = -k$.

W przypadku a) mamy:

$$x = \pm 1 - 1 - k \text{ i } 4N(t(k)) = (\pm 1-1-k)^2 - y^2 D = 4k$$

W przypadku b) mamy:

$$x = \pm 1 - 1 + k \text{ i } 4N(t(k)) = (\pm 1-1+k)^2 - y^2 D = -4k$$

Podstawiając za i,k odpowiednie wartości i uwzględniając, że D jest wolne od kwadratu i różne od 1 oraz fakt, że: $x \equiv y \bmod (2)$, gdy $D \equiv 1 \bmod (4)$ i $x \equiv y \equiv 0 \bmod (2)$, gdy $D \equiv 2,3 \bmod (4)$ wyznaczamy D i y z równości:

a) $-Dy^2 = 4k - (\pm i - 1 - k)^2$

b) $-Dy^2 = -4k - (\pm i - 1 + k)^2$ - co daje tezę lematu.

Twierdzenie 1

W ciałach kwadratowych różnych od ciał $Q(\sqrt{-1})$, $Q(\sqrt{2})$, $Q(\sqrt{-3})$, $Q(\sqrt{3})$, $Q(\sqrt{5})$, $Q(\sqrt{-7})$, $Q(\sqrt{17})$ - nie istnieje ciąg nieskończony: $a_1, a_2, a_3 \ldots$ elementów R/K spełniający warunek (A).

Dowód

Zwróćmy uwagę, że jedynymi ciałami, w których zachodzą związki:

1) $S(1) + t(1) = U(1)$; 2) $S(1) + t(1) = U(2)$

3) $S(1) + t(2) = U(1)$; 4) $S(1) + t(2) = U(2)$,

są ciała wykluczone przez nas z rozważań [związek 2) jest równoważny związkowi 3)] - co wynika z lematu 4 i lematu 3.

Jeśli w R/K istnieje ciąg: $a_1, a_2, a_3 \ldots$ spełniający warunek (A), to musi być - zgodnie z warunkiem (C):

a) $/N(r_1)/ = 1$; b) $/N(r_2)/ = 1,2$; c) $/N(r_1 + r_2)/ = 1,2$;

- jednakże jeśli zachodzi a) i b),to w rozważanych ciałach nie może zajść c), gdyż zgodnie z 1), 2), 3), 4) suma jednostki z jednostką lub jednostki z elementem o normie dwa nie może mieć normy mniejszej niż trzy [oczywiście $r_1 + r_2$ musi być różne od zera, gdyż wtedy $a_1 = a_3$ - co nie może zajść w ciągu spełniającym warunek (A) - lemat 1].

Twierdzenie

Jeśli w R/K nie ma ideałów o normie dwa oraz $S(1) + t(1) \neq U(1)$, to w R/K nie istnieje ciąg: $a_1, a_2, a_3 \ldots$ spełniający warunek (A) dla ideałów pierwszych.

Dowód

Zauważmy, że jeśli ciąg: $a_1, a_2, a_3 \ldots$ spełnia warunek (A) dla ideałów pierwszych, to $r_1 = a_2 - a_1$ musi być jednostką - gdyby bowiem było $/N(r_1)/ \geq 1$, to: $r_1 \cdot R/K = p_1^m, p_2^n, p_3^s \ldots$ (rozkład na czynniki idealne pierwsze) i $r_1 \in P_1$, a ponieważ $N(P_1) \geq 3$ więc warunek (A) nie byłby spełniony. Zgodnie z założeniami twierdzenia musi być: $/N(r_1+r_2)/ > 3$ albo

$/N(r_2)/ \geqslant 3$. W obu przypadkach można stosować to samo rozumowanie - zastosujemy je, gdy $/N(r_2)/ \geqslant 3$:

$$r_2 \cdot R/K = P_1^m \cdot P_2^n, P_3^s \ldots, \quad N(P_1) \geqslant 3 \quad \text{oraz} \quad a_2 \equiv a_3 \bmod (P_1)$$

- zatem warunek (A) nie jest spełniony.

REFERENCES

1. O. Barsky: Sur les systemes complets de restes modulo les ideaux d un corps de nombres, Acta Arithmetica 22 (1972).

ПРОБЛЕМА БРОВКИНА ДЛЯ КВАДРАТИЧНЫХ ПОЛЕЙ

Р е з ю м е

И. Бровкину принадлежит следующая проблема: Пусть K алгебраическое расширение поля рациональных чисел, в котором существует последовательность $a_1, a_2, a_3 \ldots$ целых чисел такая, что для всех идеалов I в кольце целых чисел поля K все классы вычетов (mod I) принадлежат последовательности: $a_1, a_2, \ldots, a_{N(I)}$. Доказать что K поле рациональных чисел. Д. Барский провёл неэлементарное доказательство этой проблемы [1]. В настоящей работе произведено целиком элементарное доказательство, что K не является квадратичным расширением поля

BROWKIN'S PROBLEM IN THE CASE OF SQUARE FIELDS

S u m m a r y

The following problem has been set up by J.Browkin: Let K be a field of algebraic numbers so that one may find a sequence if integers in K, say $a_1, a_2, a_3 \ldots$ so that for every ideal I in the ring of integers of K all the remaining classes (mod I) are represented by the sequence $a_1, a_2, a_3 \ldots a_{N(I)}$. To prowe that K is the field of rational numbers D. Barsky has put forward the non- elementary proof of this problem [1]. This paper contains the elementary proof that K is not a square field.