27. KONSTRUKCJE WIELOKĄTÓW FOREMNYCH

Rozważmy następujące zadanie: skonstruować n-kąt foremny wpisany w okrąg o promieniu jednostkowym.

Zauważmy, że jeśli środek okręgu będzie leżał w początku układu współrzędnych, a jeden z wierzchołków wielokąta będzie punktem $(1, 0)$, to wszystkie wierzchołki wielokąta będą w punktach odpowiadających pierwiastkom stopnia n z jedności. Wobec tego problem wykonalności konstrukcji n-kąta foremnego sprowadza się do pytania, czy można skonstruować punkty płaszczyzny odpowiadające pierwiastkom stopnia n z jedności. Zauważmy najpierw, że jeśli punkt odpowiadający liczbie zespolonej $z = a+b_i$ można skonstruować z danego zbioru X_0, to liczba z jest liczbą algebraiczną stopnia będącego potęgą liczby 2 względem ciała $Q(X_0)$. Istotnie, jeśli można skonstruować punkt $A = (a, b)$, to liczby a, b, i są algebraiczne względem ciała $Q(X_0)$, przy czym należą do pewnego rozszerzenia konstruowalnego L ciała $Q(X_0)$. Wynika stąd, że $(L:Q(X_0)) = 2^m$. Ponieważ $z = a+b_i \in L$, więc $Q(X_0) \subset Q(X_0, z) \subset L$, a zatem $(Q(X_0, z):Q(X_0))$

jest dzielnikiem liczby 2^m. Wobec tego liczba z jest elementem algebraicznym względem ciała $Q(X_0)$, którego stopień jest dzielnikiem liczby 2^m, jest więc potęgą liczby 2.

W sformułowanym wyżej zadaniu ciałem danych jest ciało liczb wymiernych Q. Podamy teraz kilka lematów, które umożliwią wyjaśnienie następującego zagadnienia: dla jakich liczb naturalnych n pierwiastki stopnia n z jedności są liczbami algebraicznymi, których stopnie mają postać 2^k.

Lemat 1. *Jeśli p jest liczbą pierwszą, to*

$$\varepsilon_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

jest liczbą algebraiczną stopnia $p-1$.

Dowód. Ponieważ ε_p jest pierwiastkiem wielomianu

$$x^p-1 = (x-1)(x^{p-1}+x^{p-2}+\ldots+x+1)$$

więc wystarczy udowodnić, że wielomian

$$f_p = x^{p-1}+x^{p-2}+\ldots+x+1$$

jest nierozkładalny nad ciałem Q. Przyjmijmy $x = y+1$ i zapiszmy

$$f_p(x) = x^{p-1}+x^{p-2}+\ldots+x+1 = \frac{x^p-1}{x-1} = \frac{(y+1)^p-1}{(y+1)-1} =$$

$$= \frac{1}{y}\left(y^p+\binom{p}{1}y^{p-1}+\binom{p}{2}y^{p-2}+\ldots+\binom{p}{p-1}y+1-1\right) =$$

$$= y^{p-1}+\sum_{j=2}^{p-1}\binom{p}{j}y^{j-1}+p \qquad (*)$$

Nierozkładalność ostatniego wielomianu wynika z kryterium Eisensteina, gdyż każdy współczynnik prócz najwyższego dzieli się przez p. Istotnie

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$

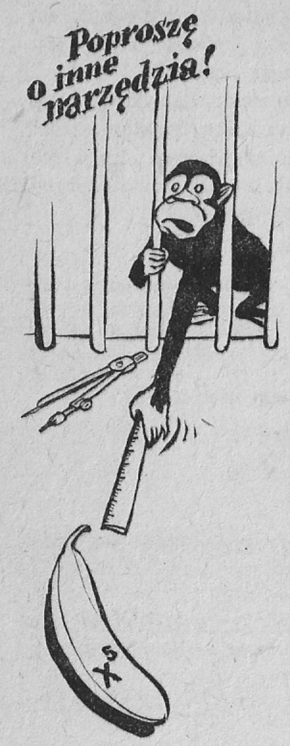
przy czym każdy czynnik pierwszy w mianowniku jest mniejszy od p. Ponadto wyraz wolny dzieli się przez p, ale nie przez p^2.

Wobec tego wielomian f_p jest istotnie nierozkładalny, zatem jest wielomianem minimalnym liczby ε_p i stopień tej liczby względem ciała Q wynosi $p-1$. ■

Lemat 2. *Jeśli p jest liczbą pierwszą, to*

$$\varepsilon_{p^2} = \cos\frac{2\pi}{p^2} + i\sin\frac{2\pi}{p^2}$$

jest liczbą algebraiczną stopnia $p(p-1)$.



Dowód. Rozważmy wielomian $g_p(x) = f_p(x^p)$. Ponieważ $(\varepsilon_{p^2})^p = \varepsilon_p$, więc ε_{p^2} jest pierwiastkiem wielomianu g_p. Stopień tego wielomianu jest równy st$f_p \cdot p = (p-1)p$. Wystarczy więc udowodnić, że wielomian g_p jest nierozkładalny nad ciałem Q. Mamy

$$g_p(x+1) = f_p((x+1)^p) = f_p\left(\sum_{i=1}^{p}\binom{p}{i}x^i+1\right)$$

Przyjmijmy

$$y=\sum_{i=1}^{p}\binom{p}{i}x^i$$

Na podstawie równania (*) zachodzi

$$g_p(x+1)=f_p(y+1)=y^{p-1}+\sum_{j=2}^{p-1}\binom{p}{j}y^{j-1}+p=$$

$$=\left(x^p+\sum_{i=1}^{p-1}\binom{p}{i}x^i\right)^{p-1}+\sum_{j=2}^{p-1}\binom{p}{j}\left(\sum_{i=1}^{p}\binom{p}{i}x^i\right)^{j-1}+p$$

Wobec tego w ostatnim wielomianie najwyższy współczynnik wynosi 1, pozostałe dzielą się przez p, a wyraz wolny jest równy p. Wielomian ten jest więc nierozkładalny na mocy kryterium Eisensteina. ■

Lemat 3. *Niech p będzie liczbą pierwszą, $p > 2$. Wówczas stopień liczby algebraicznej ε_p jest potęgą liczby 2 wtedy i tylko wtedy, gdy $p = 2^{2^k}+1$ dla pewnego całkowitego k.*

Dowód. Z lematu 1 wynika, że ε_p jest liczbą algebraiczną stopnia $p-1$, więc jeśli $p = 2^{2^k}+1$, to $p-1 = 2^{2^k}$. Zatem stopień liczby algebraicznej ε_p jest potęgą liczby 2.

Załóżmy, że stopień liczby algebraicznej ε_p jest potęgą liczby 2, tj. $p-1 = 2^n$ dla pewnego n. Gdyby liczba n miała czynnik nieparzysty $2r+1 > 1$, to $n = (2r+1)s$ i na mocy wzoru

$$a^{2r+1}+b^{2r+1} = (a+b)(a^{2r}-a^{2r-1}b+a^{2r-2}b^2- \ldots -ab^{2r-1}+$$
$$+b^{2r})$$

byłoby

$$p = 2^n+1 = (2^s)^{2r+1}+1 =$$
$$= (2^s+1)\cdot((2^s)^{2r}-(2^s)^{2r-1}+(2^s)^{2r-2}- \ldots -1)$$

co oznaczałoby, że p jest liczbą złożoną wbrew założeniu. Wobec tego n jest potęgą dwójki, $n = 2^k$, więc $p = 2^{2^k}+1$. ■

Liczby o postaci $F_k = 2^{2^k}+1$ nazywamy liczbami Fermata.

Dla $k = 0; 1, 2, 3, 4$ otrzymujemy w ciągu liczb Fermata liczby pierwsze 3, 5, 17, 257, 65537, natomiast okazuje się, że liczba F_5 jest złożona. Stwierdzono, że dla kilkudziesięciu wartości $k > 4$ liczby F_k są złożone (m.in. dla $k = 5, 6, 7, \ldots$ $\ldots, 16$). Nie wiadomo dotychczas, czy istnieje w ciągu (F_k) choć jeszcze jedna liczba pierwsza dla $k > 4$.

Lemat 4

A. *Jeśli można skonstruować n-kąt foremny, to można skonstruować $2n$-kąt foremny.*

B. *Jeśli można skonstruować n-kąt foremny, oraz m-kąt foremny, przy czym liczby m, n są względnie pierwsze, to można skonstruować mn-kąt foremny.*

C. *Jeśli można skonstruować n-kąt foremny oraz $n = kr$, to można skonstruować k-kąt foremny.*

Dowód

A. Mając dane kolejne wierzchołki A i B n-kąta foremnego, prowadzimy dwusieczną kąta AOB, gdzie O jest środkiem okręgu opisanego na n-kącie. Dwusieczna ta przecina okrąg w punkcie C, przy czym A, C, B są kolejnymi wierzchołkami $2n$-kąta foremnego. Pozostałe wierzchołki wyznaczymy, odkładając kolejno łuk AC na okręgu.

B. Istnieją liczby całkowite r, s, dla których $rn+sm = 1$. Wobec tego

$$\varepsilon_{mn} = \varepsilon_{mn}^{rn+sm} = \varepsilon_{mn}^{rn}\cdot\varepsilon_{mn}^{sm} = \varepsilon_m^r\cdot\varepsilon_n^s$$

Wynika stąd, że jeśli ε_m, ε_n należą do pewnego rozszerzenia konstruowalnego ciała Q, to ε_{mn} też należy do tego rozszerzenia. Można więc skonstruować mn-kąt foremny.

C. Wystarczy wybrać co r-ty wierzchołek wielokąta. ■

Dla podania ostatecznej odpowiedzi na pytanie o konstruowalność wielokątów foremnych powołamy się na twierdzenie, którego dowodu nie będziemy tu przytaczać.

Skończone rozszerzenie Galois L ciała K jest konstruowalne wtedy i tylko wtedy, gdy (L:K) jest potęgą dwójki.

Możemy teraz udowodnić

Twierdzenie (Gauss) *n-kąt foremny wpisany w okrąg o promieniu 1 można skonstruować wtedy i tylko wtedy, gdy*

$$n = 2^k\cdot p_1\cdot p_2, \ldots, p_r$$

gdzie k jest wykładnikiem całkowitym nieujemnym, $p_1, p_2, \ldots$ $\ldots, p_r$ są parami różnymi liczbami pierwszymi Fermata.

Dowód. Załóżmy, że $n = 2^k p_1 p_2 \dots p_r$, gdzie $p_1, p_2, \dots, p_r$ są parami różnymi liczbami pierwszymi Fermata. Z lematu 3 oraz przytoczonego wyżej twierdzenia wynika, że można skonstruować p_i-kąt foremny, natomiast z kilkakrotnie stosowanego lematu 4 wynika, że można skonstruować n-kąt foremny.

Załóżmy teraz, że n-kąt foremny jest konstruowalny. Rozłóżmy liczbę n na czynniki pierwsze

$$m = 2^k p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$$

Gdyby wśród tych czynników pierwszych występowała liczba pierwsza $p > 2$ nie będąca liczbą Fermata, to z lematu 4C wynikałoby, że p-kąt foremny jest konstruowalny, co wobec lematu 3 nie jest możliwe. Gdyby pewien wykładnik k_i był większy niż 1, to $p_i^2 | n$, a wobec tego byłby konstruowalny wielokąt foremny mający p_i^2 boków, a zatem liczba εp_i^2 byłaby liczbą algebraiczną stopnia 2^t. To jednak nie jest możliwe, bo na mocy lematu 2 liczba ta ma stopień $p_i(p_i - 1)$, który ma czynnik nieparzysty p_i. Wobec tego wszystkie wykładniki $k_1, k_2, \dots, k_r$ są równe 1 i wszystkie liczby p_i są parami różnymi liczbami pierwszymi Fermata. ■

Przykłady

1. Można skonstruować n-kąt foremny dla $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20$. Nie można skonstruować siedmiokąta, dziewięciokąta, jedenastokąta itp.

2. Ponieważ $120 = 2^3 \cdot 3 \cdot 5$, więc 120-kąt foremny jest konstruowalny, natomiast $360 = 2^3 \cdot 3^2 \cdot 5$, więc 360-kąt foremny nie jest konstruowalny. Wynika stąd, że można skonstruować kąt 3° (kąt o wierzchołku leżącym w środku okręgu opisanego na 120-kącie, mający ramiona przechodzące przez sąsiednie wierzchołki), nie można natomiast skonstruować kąta 1°.

3. Kąt $m°$ (m – liczba całkowita) jest konstruowalny wtedy i tylko wtedy, gdy m jest liczbą podzielną przez 3.

Zadania

27.1 Wyznaczyć wszystkie liczby n o następującej własności: dowolny kąt można podzielić konstrukcyjnie na n równych części.

27.2 Wykazać, że mając na płaszczyźnie parabolę opisaną równaniem $y = x^2$, można skonstruować siedmiokąt foremny.