PIERŚCIENIE I CIAŁA

Wykład 11

Konstrukcje geometryczne

Konstrukcje geometryczne wywodzą się ze starożytnej Grecji. Klasyczne konstrukcje dopuszczają użycie jedynie linijki i cyrkla. Możemy więc wykreślać proste i okręgi. Załóżmy, że dany jest niepusty zbiór $S \subset \mathbb{R}^2$ punktów na płaszczyźnie. Możemy wykonać dwie konstrukcje geometryczne:

(l) dla pary punktów $P, Q \in S$ wyznaczamy prostą przechodzącą przez przez punkty P, Q,

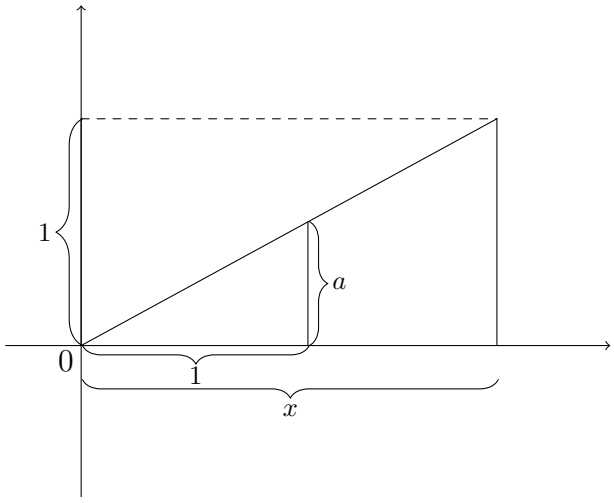
(c) dla trzech punktów $P, Q_1, Q_2 \in S$ wyznaczamy okrąg o środku w punkcie P i promieniu równym odległości punktów Q_1, Q_2.

Dla skończonego zbioru $S \subset \mathbb{R}^2$ mówimy że punkt P jest ***konstruowalny w jednym kroku*** z S przy pomocy linijki (l) i cyrkla (c), jeśli P jest punktem przecięcia dwóch różnych krzywych (linii prostych lub okręgów) otrzymanych z S przy pomocy konstrukcji (l) lub (c).

Punkt R jest ***konstruowalny ze zbioru*** S, jeśli istnieją punkty $R_1, ..., R_n = R$ takie, że R_1 jest konstruowalny w jednym kroku z S i dla każdego $i = 0, ..., n-1$ punkt R_{i+1} jest konstruowalny w jednym kroku ze zbioru $S \cup \{R_1, ..., R_i\}$. ***Liczbami konstruowalnymi*** z S nazywamy liczby rzeczywiste, które są współrzędnymi punktów konstruowalnych z S.

Niech $S = S_0$ będzie zbiorem złożonym z dwóch punktów $P_0 = (0, 0)$, $P_1 = (1, 0)$. O punktach konstruowalnych z S_0 mówimy krótko, że są to punkty konstruowalne.

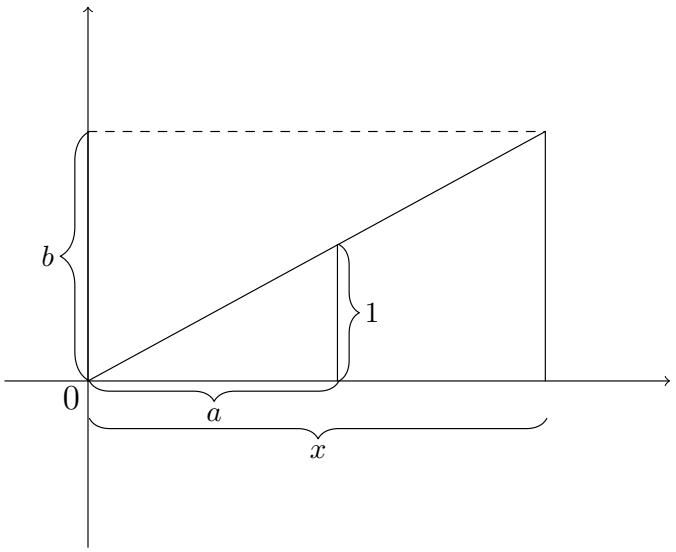
Jeśli punkty P, Q są konstruowalne, to konstruowalne są również punkty $P + Q$ (jako czwarty wierzchołek równoległoboku o wierzchołakch i P_0, P, Q) oraz $P - Q$. Wynika stąd w szczególności, że wszystkie liczby całkowite są konstruowalne. Ponadto, rysunek 1 pokazuje, że jeśli konstruowalny jest punkt $(0, a)$, gdzie $a \neq 0$, to konstruowalny jest również punkt $\left(\frac{1}{a}, 0\right)$.



Rysunek 1.

Rzeczywiście, z twierdzenia Talesa otrzymujemy $x = \frac{x}{1} = \frac{1}{a}$.

Rysunek 2 pokazuje z kolei, że jeśli konstruowalne są punkty $(a, 0)$ i $(0, b)$, to konstruowalny jest również punkt $(ab, 0)$. Ponownie korzystając z twierdzenia Talesa dostajemy $\frac{x}{b} = \frac{a}{1}$, czyli $x = ab$. Uwagi te pokazują, że wszystkie liczby wymierne są konstruowalne.



Rysunek 2.

Można także skonstruować kwadrat o boku długości 1, a zatem $\sqrt{2}$ jest konstruowalny. Inną liczbą konstruowalną jest $\sqrt{3}$, gdyż $\frac{\sqrt{3}}{2}$ jest długością wysokości w trójkącie równobocznym o boku długości 1.

Dla zbioru S punktów na płaszczyźnie przez $\mathbb{Q}_S$ oznaczamy podciało ciała $\mathbb{R}$, które jest rozszerzeniem ciała $\mathbb{Q}$ o zbiór wszystkich współrzędnych punktów z S.

Twierdzenie 1. *Niech S będzie skończonym zbiorem punktów na płaszczyźnie.*

(i) *Jeżeli punkt $R \in \mathbb{R}^2$ jest konstruowalny w jednym kroku z S, to*

$$(\mathbb{Q}_{S\cup\{R\}} : \mathbb{Q}_S) = 1 \quad \textit{lub} \quad 2. \tag{1}$$

(ii) *Jeżeli $S_1 = S \cup \{R_1, ..., R_n\}$, gdzie $R_1, ..., R_n$ są punktami konstruowalnymi z S, to $(\mathbb{Q}_{S_1} : \mathbb{Q}_S)$ jest potęgą liczby 2.*

Dowód. (i) Punkt R jest punktem przecięcia dwóch krzywych L_1, L_2 o równaniach:

$$L_1 : a_1(x^2 + y^2) + b_1x + c_1y + d_1 = 0,$$
$$L_2 : a_2(x^2 + y^2) + b_2x + c_2y + d_2 = 0,$$

gdzie $a_1, ..., d_2 \in \mathbb{Q}_S$. Jeśli $a_1 = a_2 = 0$, to R jest punktem przecięcia dwóch prostych i jego współrzędne należą do $\mathbb{Q}_S$. Zatem $\mathbb{Q}_{S\cup\{R\}} = \mathbb{Q}_S$.

Jeśli co najmniej jedna z liczb a_1, a_2 jest różna od zera, to $M = a_2L_1 - a_1L_2$ jest prostą o równaniu postaci

$$b_3x + c_3y + d_3 = 0.$$

Załóżmy, że $c_3 \neq 0$. Wtedy $y = \frac{-b_3x-d_3}{c_3}$, co po wstawieniu do równania L_1 daje równanie postaci

$$ax^2 + bx + c = 0,$$

gdzie $a, b, c \in \mathbb{Q}_S$. Zatem $\mathbb{Q}_{S\cup\{R\}} = \mathbb{Q}_S(x, y) = \mathbb{Q}_S(x)$, przy czym x jest pierwiastkiem wielomianu stopnia 1 (jeśli $a = 0$) lub 2 (jeśli $a \neq 0$). Stąd

$$(\mathbb{Q}_{S\cup\{R\}} : \mathbb{Q}_S) = 1 \ \text{ lub } \ 2.$$

Jest to prawdą także w przypadku, gdy $b_3 \neq 0$, gdyż wtedy $\mathbb{Q}_{S\cup\{R\}} = \mathbb{Q}_S(y)$ i y jest pierwiastkiem wielomianu stopnia co najwyżej 2.

(ii) Mamy $S_1 = S \cup \{R_1, ..., R_n\}$, gdzie $R_1, ..., R_n$ są punktami konstruowalnymi z S. Daje to ciąg rozszerzeń

$$\mathbb{Q}_S \subset ... \subset \mathbb{Q}_{S\cup\{R_1,...,R_i\}} \subset \mathbb{Q}_{S\cup\{R_1,...,R_{i+1}\}} \subset ... \subset \mathbb{Q}_{S_1}$$

dla $i = 1, ..., n-2$, przy czym z (i) wiemy, że każde z tych rozszerzeń ma stopień 1 lub 2. Mamy

$$(\mathbb{Q}_{S_1} : \mathbb{Q}_S) = (\mathbb{Q}_{S_1} : \mathbb{Q}_{S\cup\{R_1,...,R_{n-1}\}})...(\mathbb{Q}_{S\cup\{R_1,R_2\}} : \mathbb{Q}_{S\cup\{R_1\}})(\mathbb{Q}_{S\cup\{R_1\}} : \mathbb{Q}_S),$$

a więc $(\mathbb{Q}_{S_1} : \mathbb{Q}_S)$ jest potęgą dwójki. □

Niech $S = \mathbb{Q}^2$. Ponieważ wszystkie punkty o wymiernych współrzędnych są konstruowalne (z S_0), więc punktami konstruowalnymi z S są punkty konstruowalne (z S_0). Mamy $\mathbb{Q}_S = \mathbb{Q}$ i jeżeli punkt P jest konstruowalny, to z twierdzenia 1 (ii) wynika, że $(\mathbb{Q}_{S\cup\{P\}} : \mathbb{Q})$ jest potęgą liczby 2. Pozwala to podać rozwiązania trzech słynnych problemów starożytnej greckiej matematyki:

- ***Podwojenie sześcianu:*** czy dla danego sześcian można skonstruować sześcian o dwukrotnie większej objętości?
- ***Trysekcja kąta:*** czy dany kąt można podzielić na trzy równe części?
- ***Kwadratura koła:*** czy mając dane koło można skonstruować kwadrat o tym samym polu?

We wszystkich tych problemach dopuszcza się jedynie użycie linijki i cyrkla.

Problem podwojenia sześcianu sprowadza się do tego, czy konstruowalna jest liczba $\sqrt[3]{2}$, gdyż jest to długość boku sześcianu o objętości 2. Niech $P = (0, \sqrt[3]{2})$. Wtedy $\mathbb{Q}_{S\cup\{P\}} = \mathbb{Q}(\sqrt[3]{2})$, a ponieważ wielomianem minimalnym liczby $\sqrt[3]{2}$ jest $x^3 - 2$, więc

$$\left(\mathbb{Q}\left(\sqrt[3]{2}\right) : \mathbb{Q}\right) = 3.$$

Nie jest to potęga dwójki, zatem $\sqrt[3]{2}$ nie jest liczbą konstruowalną.

Dla rozwiązania problemu trysekcji kąta wykażemy, że nie można podzielić kąta 30° na trzy równe części. Sprowadza się to do wykazania, że $\sin 10^\circ$ nie jest liczbą konstruowalną. Wykorzystamy wzór $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$. Przyjmując $\theta = 10^\circ$ dostajemy

$$4\sin^3 10^\circ - 3\sin 10^\circ = -\sin 30^\circ = -\frac{1}{2},$$

zatem $a = 2\sin 10^\circ$ jest pierwiastkiem wielomianu $f(x) = x^3 - 3x + 1$. Jest to wielomian nierozkładalny nad $\mathbb{Q}$. Rzeczywiście podstawiając $y = x + 1$ otrzymujemy wielomian

$$f(y-1) = (y-1)^3 - 3(y-1) + 1 = y^3 - 3y^2 + 3,$$

który jest nierozkładalny na mocy kryterium Eisensteina zastosowanego dla $p = 3$. Zatem $(\mathbb{Q}(a) : \mathbb{Q}) = 3$.

Mamy $\mathbb{Q}(a) \subset \mathbb{Q}_{S\cup\{P\}}$, gdzie $P = (a, 0)$ i gdyby punkt P był konstruowalny, to stopień $(\mathbb{Q}_{S\cup\{P\}} : \mathbb{Q})$ byłby potęgą dwójki. Ale

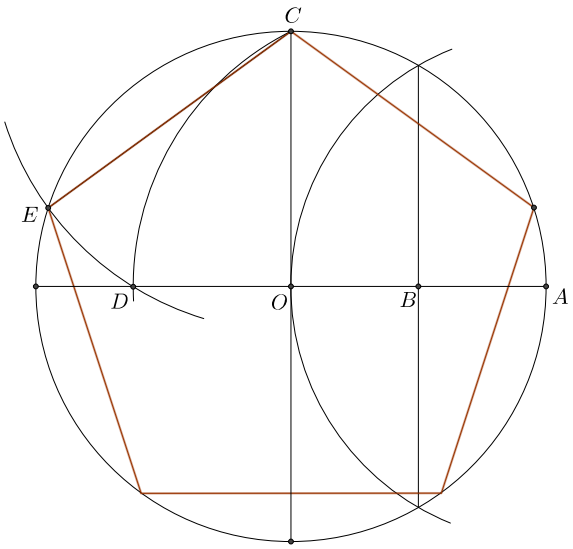
$$(\mathbb{Q}_{S\cup\{P\}} : \mathbb{Q}) = (\mathbb{Q}_{S\cup\{P\}} : \mathbb{Q}(a))(\mathbb{Q}(a) : \mathbb{Q}) = 3(\mathbb{Q}_{S\cup\{P\}} : \mathbb{Q}(a)),$$

co prowadzi do sprzeczności.

Problem kwadratury koła sprowadza się do problemu, czy liczba $\sqrt{\pi}$ jest konstruowalna, gdyż $\sqrt{\pi}$ jest długością boku kwadratu o polu równym polu koła o promieniu 1. Ale $\sqrt{\pi}$ jest liczbą przestępną. Gdyby bowiem $\sqrt{\pi}$ było liczbą algebraiczną, to z wniosku 2, wykład 10 wynika, że $\pi = \sqrt{\pi}^2$ także byłoby liczbą algebraiczną. Każda liczba konstruowalna jest liczbą algebraiczną, więc liczba $\sqrt{\pi}$ nie jest konstruowalna.

Starożytni matematycy greccy rozważali także ***problem konstruowalności n-kątów foremnych***. Konstruowalny jest trójkąt równoboczny, kwadrat, pięciokąt i sześciokąt foremny. Konstrukcje trójkąta, kwadratu i sześciokąta są oczywiste.

Nieco bardziej skomplikowana jest konstrukcja pięciokąta. Polega ona na tym, że rysujemy okrąg o środku O i w nim dwie prostopadłe średnice. Wyznaczamy środkowy punkt B odcinka OA i z punktu B zakreślamy łuk CD. Następnie z punktu C zakreślamy łuk DE. W ten sposób otrzymujemy odcinek CE, który jest bokiem pięciokąta foremnego.



Rysunek 3.

Aby sprawdzić poprawność tej konstrukcji zauważmy, że pierwiastki stopnia 5 z 1 to wierzchołki pięciokąta foremnego wpisanego w okrąg jednostkowy. Są one dane wzorami

$$\omega_k = \cos\frac{2k\pi}{5} + i\sin\frac{2k\pi}{5},$$

gdzie $k = 0, 1, 2, 3, 4$. Dla $k = 1$ mamy

$$\omega_1 = \frac{\sqrt{5}-1}{4} + i\frac{\sqrt{10+2\sqrt{5}}}{4}.$$

Stąd długość boku pięciokąta jest równa

$$|\omega_1 - 1| = \left|\frac{\sqrt{5}-5}{4} + i\frac{\sqrt{10+2\sqrt{5}}}{4}\right| = \sqrt{\frac{5-\sqrt{5}}{2}}.$$

Wróćmy do naszej konstrukcji. Przyjmijmy, że odcinek OA ma długość 1. Korzystając z twierdzenia Pitagorasa otrzymujemy

$$|BC| = \sqrt{|OB|^2 + |OC|^2} = \frac{\sqrt{5}}{2}.$$

Odcinek DB ma taką samą długość jak odcinek BC, czyli $|DB| = \frac{\sqrt{5}}{2}$ i stąd

$$|OD| = |DB| - |OB| = \frac{\sqrt{5}-1}{2},$$

gdyż $|OB| = \frac{1}{2}$. Zatem

$$|CE| = |DC| = \sqrt{|OD|^2 + |OC|^2} = \sqrt{\frac{5-\sqrt{5}}{2}}.$$

Twierdzenie 2 (twierdzenie Wantzela)**.** *Jeżeli n-kąt foremny jest konstruowalny i liczba pierwsza $p > 1$ dzieli n, to $p = 2^k + 1$ dla pewnego $k \in \mathbb{N}$.*

Dowód. Jeżeli n-kąt foremny jest konstruowalny i liczba $p > 1$ dzieli n, to również p-kąt foremny jest konstruowalny. Wierzchołki p-kąt foremnego to liczby zespolone

$$\omega_k = \cos\frac{2k\pi}{p} + i\sin\frac{2k\pi}{p},$$

gdzie $k = 0, 1, \ldots, p-1$. W szczególności konstruowalny jest punkt $\omega_1 = \left(\cos\frac{2\pi}{p}, \sin\frac{2\pi}{p}\right)$ i zgodnie z twierdzeniem 1 mamy $(E : \mathbb{Q}) = 2^m$ dla pewnego $m \in \mathbb{N}$, gdzie $E = \mathbb{Q}\left(\cos\frac{2\pi}{p}, \sin\frac{2\pi}{p}\right)$. Ponadto $(E(i) : E) = 2$, gdyż liczba i ma wielomian minimalny $x^2+1 \in E[x]$. Stąd

$$(E(i) : \mathbb{Q}) = (E(i) : E)(E : \mathbb{Q}) = 2^{m+1}.$$

Ale $\omega_1 \in E(i)$, więc

$$(E(i) : \mathbb{Q}(\omega_1))(\mathbb{Q}(\omega_1) : \mathbb{Q}) = (E(i) : \mathbb{Q}) = 2^{m+1},$$

co pokazuje, że $(\mathbb{Q}(\omega_1) : \mathbb{Q})$ dzieli 2^{m+1}, a więc $(\mathbb{Q}(\omega_1) : \mathbb{Q}) = 2^k$ dla pewnego $k \in \mathbb{N}$.

Liczbę $(\mathbb{Q}(\omega_1) : \mathbb{Q})$ możemy wyznaczyć znajdując wielomian minimalny dla ω_1. Wiemy, że ω_1 jest pierwiastkiem stopnia p z 1, czyli pierwiastkiem wielomianu $x^p - 1$. Ale

$$x^p - 1 = (x-1)(1 + x + x^2 + ... + x^{p-1}),$$

a więc ω_1 jest pierwiastkiem wielomianu

$$f(x) = 1 + x + x^2 + ... + x^{p-1} = \frac{x^p - 1}{x - 1}.$$

Wielomian ten jest nierozkładalny. Rzeczywiście

$$f(x+1) = \frac{1}{x}\left((x+1)^p - 1\right) = \frac{1}{x}\sum_{k=1}^{p}\binom{p}{k}x^k = \sum_{k=1}^{p}\binom{p}{k}x^{k-1}$$

i ponieważ p jest liczbą pierwszą, więc p dzieli $\binom{p}{k}$ dla $k = 1, 2, ..., p-1$. Ponadto p nie dzieli $\binom{p}{p} = 1$ i p^2 nie dzieli $\binom{p}{1} = p$. Korzystając z kryterium Eisensteina stwierdzamy więc, że $f(x+1)$ jest wielomianem nierozkładalnym, a stąd także f jest nierozkładalny. Zatem f jest wielomianem minimalnym liczby ω_1 i w konsekwencji

$$2^k = (\mathbb{Q}(\omega_1) : \mathbb{Q}) = \operatorname{st} f = p - 1,$$

czyli $p = 2^k + 1$. □

Z twierdzenia 2 wynika w szczególności, że niemożliwa jest konstrukcja siedmiokąta foremnego, a bardziej ogólnie żadnego $7n$-kąta foremnego.

Pełna odpowiedź na problem konstruowalności n-kątów foremnych wymaga użycia liczb pierwszych Fermata.

Liczba Fermata to liczba naturalna postaci $F_n = 2^{2^n}+1$, gdzie n jest nieujemną liczbą całkowitą. Jeśli jest to liczba pierwsza, to nazywamy ją ***liczbą pierwszą Fermata***. Pięć liczb pierwszych Fermata: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$.

Twierdzenie 3 (twierdzenie Gaussa-Wantzela)**.** *n-kąt foremny daje się skonstruować za pomocą cyrkla i linijki wtedy i tylko wtedy, gdy n jest liczbą postaci 2^k, gdzie $k \in \mathbb{N}$ lub postaci $2^k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_s$, gdzie $k \in \mathbb{N} \cup \{0\}$ i $p_1, p_2, ..., p_s$ są różnymi liczbami pierwszymi Fermata.*

Na stronie Wikipedii `https://en.wikipedia.org/wiki/Constructible_polygon` umieszczone są animacje pokazujące konstrukcje 15-kąta, 17-kąta, 257-kąta i 65537-kąta foremnego.

Grupy permutacji S_n

Przypomnijmy, że przez S_n oznaczamy grupę wszystkich permutacji zbioru $\{1, 2, ..., n\}$ (lub równoważnie innego ustalonego zbioru n-elementowego) z działaniem złożenia. Grupa S_n ma rząd $n!$ i dla $n \geqslant 3$ jest to grupa nieprzemienna. Permutację $\sigma \in S_n$ zapisujemy w postaci graficznej jako

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}.$$

Permutacją cykliczną długości m nazywamy taką permutację $\sigma \in S_n$, dla której istnieją liczby $1 \leqslant j_1 < j_2 < ... < j_m \leqslant n$ takie, że $\sigma(j_k) = j_{k+1}$ dla $k = 1, 2, ..., m-1$, $\sigma(j_m) = j_1$ i $\sigma(j) = j$ dla $j \notin \{j_1, j_2, ..., j_k\}$. Piszemy wtedy $\sigma = (j_1, j_2, ..., j_m)$. Zauważmy, że elementem odwrotnym do takiej permutacji σ jest

$$\sigma^{-1} = (j_m, j_{m-1}, ..., j_2, j_1).$$

Ogólnie mówimy, że elementy $a_1, a_2, ..., a_m$ grupy G generują tę grupę, jeśli każdy element $a \in G$ można przedstawić w postaci

$$a = a_1^{k_1} a_2^{k_2} ... a_m^{k_m} \tag{2}$$

dla pewnych liczb $k_1, k_2, ..., k_m \in \mathbb{Z}$.

Generatorami grupy S_n są transpozycje, czyli permutacje postaci (i, j). W tym przypadku można pominąć wykładniki we wzorze (2), czyli każdą permutację można przestawić jako iloczyn (czyli złożenie) skończonej liczby transpozycji. Wynika to z faktu, że

$$(i, j)^2 = (i, j)(i, j) = I,$$

gdzie I jest permutacją tożsamościową, czyli $I(s) = s$ dla $s = 1, 2, ..., n$. Stąd

$$(i, j)^{-1} = (j, i) = (i, j),$$

a więc $(i, j)^k = I$, gdy k jest liczbą parzystą i $(i, j)^k = (i, j)$, gdy k jest liczbą nieparzystą.

Przykład 1. Niech

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

Przedstawiamy najpierw σ jako iloczyn permutacji cyklicznych:

$$\sigma = (1, 5, 2, 6)(3, 4).$$

Teraz wystarczy pierwszą permutację cykliczną zapisać jako iloczyn transpozycji zgodnie ze schematem

$$(1, 5, 2, 6) = (1, 6)(1, 2)(1, 5).$$

Zatem

$$\sigma = (1, 6)(1, 2)(1, 5)(3, 4).$$

Zbiór wszystkich transpozycji nie jest jednak najmniejszym zbiorem generującym S_n.

Twierdzenie 4. *Dla $n \geqslant 3$ następujące zbiory generują grupę S_n:*

(1) *zbiór wszystkich transpozycji postaci $(i, i + 1)$, gdzie $i = 1, 2, ..., n - 1$.*
(2) *zbiór złożony z transpozycji $(1, 2)$ i cyklu $(1, 2, ..., n)$.*

Dowód. (1) Wystarczy wykazać, że każdą transpozycję (i, j), gdzie $i < j$ można przedstawić jako iloczyn pewnej liczby transpozycji postaci $(i, i + 1)$. Dowód prowadzimy przez indukcję względem $j - i$.

Jeśli $j - i = 1$, to $j = i + 1$, więc $(i, j) = (i, i + 1)$. Załóżmy, że nasza teza jest prawdziwa dla wszystkich transpozycji (i, j) takich, że $j - i = k$ i niech (p, q) będzie transpozycją taką, że $q - p = k + 1$. Mamy

$$(p, q) = (p, p + 1)(p + 1, q)(p, p + 1), \tag{3}$$

przy czym dla środkowej transpozycji $q - (p + 1) = k$, więc z założenia indukcyjnego $(p + 1, q)$ jest iloczynem pewnej liczby transpozycji postaci $(i, i + 1)$. Wstawiając ten iloczyn do (3) w miejsce $(p + 1, q)$ otrzymujemy przedstawienie (p, q) w postaci iloczynu transpozycji postaci $(i, i + 1)$.

(2) Wobec tego, co już wykazaliśmy, wystarczy sprawdzić, że każdą transpozycję postaci $(i, i + 1)$ można wyrazić przy pomocy transpozycji $(1, 2)$ i cyklu $\sigma = (1, 2, ..., n)$. Mamy $\sigma^{-1} = (n, ..., 2, 1)$, więc

$$\sigma(1, 2)\sigma^{-1} = (2, 3)$$

i ogólnie

$$\sigma^k(1, 2)\sigma^{-k} = (k + 1, k + 2)$$

dla każdego $k = 1, 2, ..., n - 2$. □