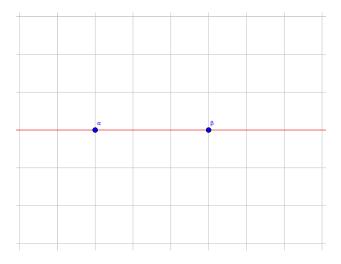
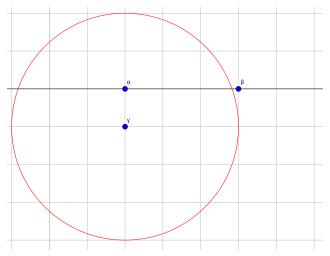
### Your Presentation

Andrzej Kokosza

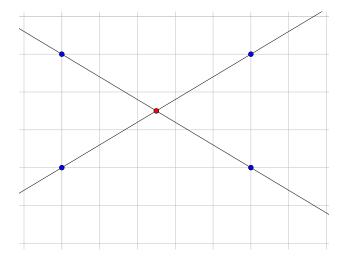
Oblicze 2016



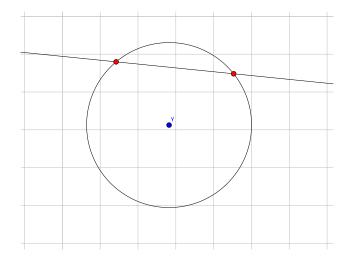
(C1) Dwa punkty  $\alpha \neq \beta$  można połączyć prostą.



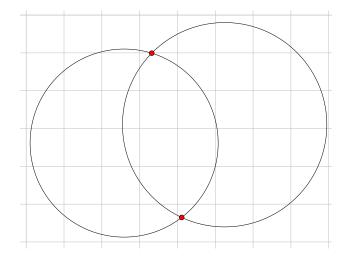
(C2) Dla puntów  $\alpha \neq \beta$  i  $\gamma$  można utworzyć okrąg o środku w  $\gamma$  i promieniu  $|\alpha\beta\>$ 



(P1) Punkt powstaje poprzez przecięcie 2 prostych.



(P2) Punkt powstaje przez przecięcie prostej i okręgu.

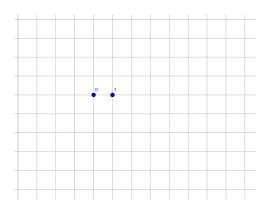


(P3) Punkt powstaje przez przecięcie dwóch okręgów.

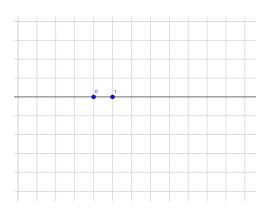
### Definicja

Liczba zespololona jest konstruowalna, gdy można utworzyć ją za pomocą aksjomatów C1, C2, P1, P2, P3 w skończonej liczbie kroków. z liczb 0, 1.

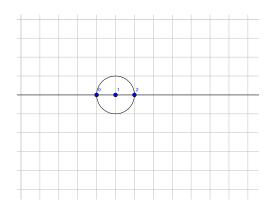
Przykład Liczby naturalne



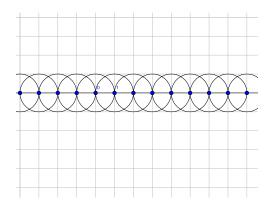
Przykład Liczby naturalne



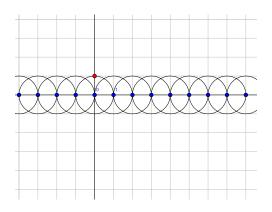
Przykład Liczby naturalne



Przykład Liczby naturalne



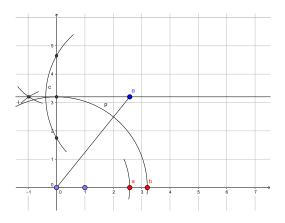
Przykład Liczby urojone całkowite

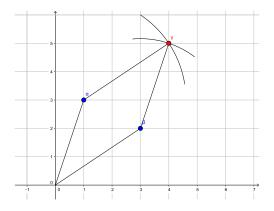


#### Twierdzenie

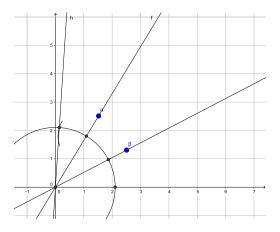
Niech  $\mathcal{C}=\{\alpha\in\mathbb{C}\mid \alpha \text{ jest konstuowalne}\}$   $\mathcal{C}$  jest podciałem  $\mathbb{C}$  Ponadto:

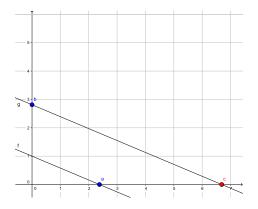
- (a) Niech  $\alpha = a + bi \in C$ , gdzie  $a, b \in \mathbb{R}$ , to  $a, b \in C$ .
- (b) Jeżeli  $\alpha \in \mathcal{C}$ , to  $\sqrt{\alpha} \in \mathcal{C}$



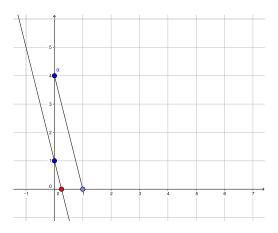


$$\alpha \cdot \beta = ae^{\theta} \cdot be^{\tau} = (ab)e^{\theta+\tau}$$

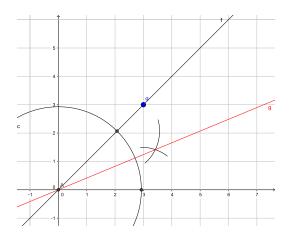


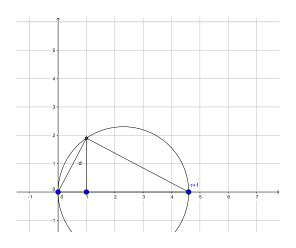


$$\frac{\alpha}{\beta} = \frac{ae^{\theta}}{be^{\tau}} = (\frac{a}{b})e^{\theta-\tau}$$



$$\sqrt{\alpha} = \sqrt{r}e^{\frac{\theta}{2}}$$





# Przypomnienie

#### **Twierdzenie**

Niech  $\alpha$  będzie liczbą zespoloną. Wtedy  $\alpha \in \mathcal{C}$  wtedy i tylko wtedy, gdy istnieją ciała

$$\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$$

takie, że  $\alpha \in F_n$  i  $[F_{i-1} : F_i] = 2$  dla  $0 < i \leqslant n$ 

#### Dowód.

( $\Leftarrow$ ) Załóżmy, że istnieje  $\mathbb{Q} = F_0 \subset ... \subset F_n \subset \mathbb{C}$  gdzie  $[F_{i-1}:F_i]=2$ . Możemy skorzystać z faktu, że jeżeli  $[F_{i-1}:F_i]=2$ , to  $F_i=F_{i-1}(\sqrt{\alpha_i})$  dla pewnego  $\alpha_i \in F_{i-1}$ . Poprzez indukcję udowodnimy, że dla  $0 < i \leqslant n$   $F_i \subset \mathbb{Q}$ . Oczywiście  $F_0=\mathbb{Q} \subset \mathcal{C}$ . Załóżmy, że  $F_{i-1} \subset \mathcal{C}$ ,  $F_i=F_{i-1}(\sqrt{\alpha_i})$ . Skoro  $\alpha_i \in \mathcal{C}$ , to  $\sqrt{\alpha_i} \in \mathcal{C}$ , stąd  $F_i=F_{i-1}(\sqrt{\alpha_i}) \in \mathcal{C}$ . Zatem  $F_n \in \mathcal{C}$ .

#### Dowód.

 $(\Rightarrow)$   $\alpha \in \mathcal{C}$  Udowodnimy, przez stworzenie wieży rozszerzeń  $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$  gdzie  $[F_{i-1}:F_i]=2$  takie, że  $F_n$  wartości urojone i rzeczywiste liczb, które powstają w trakcie konstrukcji  $\alpha$ . Przeprowadzimy indukcje po liczbie N użyć aksjomatów P1, P2, P3. Dla N=0  $\alpha=0$  lub  $\alpha=1$  zatem  $\mathbb{Q} = F_0 = F_n$ .

#### Dowód.

Niech N>1 i punkt  $\alpha$  został otrzymany za pomocą P1, przecięcie się prostych  $I_1$ ,  $I_2$ . Proste powstały z punktów  $\alpha_1$  i  $\beta_1$  oraz  $\alpha_2$  i  $\beta_2$ .  $\alpha_1$ ,  $\beta_1$ ,  $\alpha_2$ ,  $\beta_2$  powstały w co najwyżej N-1 krokach, zatem z założenia indukcyjnego istnieje  $\mathbb{Q}=F_0\subset F_1\subset ...\subset F_n\subset \mathbb{C}$  gdzie  $[F_{i-1}:F_i]=2$ , że części urojone i rzeczywiste  $\alpha_1$ ,  $\beta_1$ ,  $\alpha_2$ ,  $\beta_2$  należą do  $F_n$ . Prosta  $I_1$  jest opisana równaniem  $a_1x+b_1y=c_1$ , ponieważ  $\alpha_1$ ,  $\beta_1\in F_n$  to  $a_1$ ,  $b_1$ ,  $c_1\in F_n$ . analogicznie równaniem  $I_2$  jest  $a_2x+b_2y=c_2$ .  $\alpha$  jest punktem przecięcia się  $I_1$ ,  $I_2$ . Zatem jego części urojone i rzeczywiste rozwiązaniem układu równań:

$$a_1x + b_1y = c_1$$
$$a_2x + b_2y = c_2$$

Stąd  $\alpha \in F_n$ 

#### Dowód.

Niech N>1 i punkt  $\alpha$  został otrzymany za pomocą P1, przecięcie się prostych  $I_1$ ,  $I_2$ . Proste powstały z punktów  $\alpha_1$  i  $\beta_1$  oraz  $\alpha_2$  i  $\beta_2$ .  $\alpha_1$ ,  $\beta_1$ ,  $\alpha_2$ ,  $\beta_2$  powstały w co najwyżej N-1 krokach, zatem z założenia indukcyjnego istnieje  $\mathbb{Q}=F_0\subset F_1\subset ...\subset F_n\subset \mathbb{C}$  gdzie  $[F_{i-1}:F_i]=2$ , że części urojone i rzeczywiste  $\alpha_1$ ,  $\beta_1$ ,  $\alpha_2$ ,  $\beta_2$  należą do  $F_n$ . Prosta  $I_1$  jest opisana równaniem  $a_1x+b_1y=c_1$ , ponieważ  $\alpha_1$ ,  $\beta_1\in F_n$  to  $a_1$ ,  $b_1$ ,  $c_1\in F_n$ . analogicznie równaniem  $I_2$  jest  $a_2x+b_2y=c_2$ .  $\alpha$  jest punktem przecięcia się  $I_1$ ,  $I_2$ . Zatem jego części urojone i rzeczywiste rozwiązaniem układu równań:

$$a_1x + b_1y = c_1$$
$$a_2x + b_2y = c_2$$

Stąd  $\alpha \in F_n$ 

#### Dowód.

Niech N>1 i punkt  $\alpha$  został otrzymany za pomocą P2, przecięcie się prostej I i okręgu o. Jak poprzednio można znaleźć  $\mathbb{Q}=F_0\subset F_1\subset ...\subset F_n\subset \mathbb{C}$  gdzie  $[F_{i-1}:F_i]=2$ , że części rzeczywiste i urojone punktów, z których powstały I i o, należą do  $F_n$ .

lpha jest rozwiązaniem układu równań.

$$a_1x + b_1y = c_1$$
  
$$x^2 + y^2 + a_2x + b_2y + c_2 = 0$$

Gdzie  $a_1, b_1, a_2, b_2, c_2 \in F_n$ . Załóżmy, że  $a_1 \neq 0$ , więc możemy przyjąć, że  $a_1 = 1$ .Po podstawieniu  $x = -b_1y + c_1$  otrzymujemy równanie kwadratowe:

$$(-b_1y + c_1)^2 + y^2 + a_2(-b_1y + c_1) + b_2y + c_2 = 0$$

#### Dowód.

$$(-b_1y + c_1)^2 + y^2 + a_2(-b_1y + c_1) + b_2y + c_2 = 0$$

W przypadku, gdy wartości y, będące rozwiązaniami równania, należą do  $F_n$ , to  $x=b_1y+c_1$  także należy do  $F_n$ , więc  $F_n$  jest szukanym ciałem

Gdy rozwiązania nie należą do  $F_n$ , to istnieje rozszerzenie  $F_{n+1}$  stopnia drugiego  $F_n$ , do którego należą wartości rozwiązania,  $x=b_1y-c_1$  także należy do  $F_{n+1}$ . Zatem  $F_{n+1}$  jest szukanym ciałem.

#### Dowód.

Niech N>1 i punkt  $\alpha$  został otrzymany za pomocą P3, przecięcie się dwóch okręgów  $o_1$  i  $o_2$ . Jak poprzednio  $\alpha$  jest rozwiązaniem równania

$$x^{2} + y^{2} + a_{1}x + b_{1}y + c_{1} = 0$$
  
 $x^{2} + y^{2} + a_{2}x + b_{2}y + c_{2} = 0$ 

Po odjęciu stronami otrzymujemy:

$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$$
  
$$x^2 + y^2 + a_2x + b_2y + c_2 = 0$$

Co sprowadza się do poprzedniego przypadku.

#### Wniosek

 ${\cal C}$  jest najmniejszym ciałem zamkniętym na operację pierwiastka kwadratowego.

#### Dowód.

Wiemy, że  $\mathcal C$  jest zamknięty na operację  $\sqrt{\ }$ . Załóżmy, że istnieje  $F\subset \mathbb C$  będzie ciałem zamkniętym na  $\sqrt{\ }$ . Weźmy dowolne  $\alpha\in \mathcal C$ . Z poprzedniego twierdzenia wiemy, istnieje wieża ciał  $\mathbb Q=F_0\subset F_1\subset ...\subset F_n\subset \mathbb C$ , gdzie  $F_i=F_{i-1}(\alpha_i)$ . Stąd  $F_n\in F$ , zatem  $\mathcal C\subset F$ .

#### Wniosek

Jeżeli  $\alpha \in \mathcal{C}$ , to  $[\mathbb{Q}(\alpha):\mathbb{Q}]=2^n$  dla pewnego  $n \in \mathbb{N}$ . Więc każda liczba konstruowalna jest algebraiczna nad  $\mathbb{Q}$  oraz jej wielomian minimalny jest stopnia  $2^n$ .

#### Dowód.

Jeżeli  $\alpha \in \mathcal{C}$ , to istnieje wieża ciał z poprzedniego twierdzenia  $\mathbb{Q} = F_0 \subset F_1 \subset ... \subset F_n \subset \mathbb{C}$ , gdzie  $[F_i : F_{i-1}] = 2$ . Stąd

$$[F_n : \mathbb{Q}] = [F_n : F_0] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}]...[F_2 : F_1] = 2^m$$

Ponieważ  $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset F_n$ , to  $[\mathbb{Q}(\alpha\mathbb{Q})]$  dzieli  $[F_n : \mathbb{Q}]$ . Zatem  $[\mathbb{Q}(\alpha\mathbb{Q})] = 2^n$ .

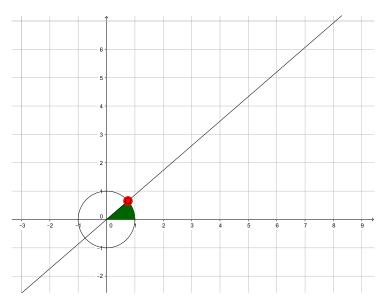
## Trysekcja kąta

### Przykład

Na przykładzie kąta  $\frac{2}{3}\pi$ . Kąt  $\theta$  utożsamiamy z liczbą  $e^{\theta}$ 

Trysekcja kąta

# Przykład



## Trysekcja kąta

#### Przykład

Pokażemy, że nie da się podzielić kąta  $\frac{2}{3}\pi$  na trzy, czyli skonstruować kąta  $\frac{2}{9}\pi$ 

Kat  $\theta$  utożsamiamy z liczbą  $e^{\theta}$ .

Czyli badamy konstruowalność punku  $e^{\frac{2}{9}\pi} = \zeta_9$ . Wielomianem minimalnym  $\zeta_9$  jest  $x^6 + x^3 + 1$ , którego stopień to 6. Stąd  $\zeta_9$  nie jest konstruowalny.

# Podwojenie Objętości sześcianu

#### Przykład

Problem sprowadza się do skonstruowania liczby  $\sqrt[3]{2}$ . jego wielomian minimalny to  $x^3-2$ , jego stopień wynosi 3. Co oznacza, że  $\sqrt[3]{2}$  nie jest konstruowalny.

### Teoria Galois

## Liczby konstruowalne

#### Twierdzenie

Niech  $\alpha \in \mathbb{C}$  będzie algebraiczne nad  $\mathbb{Q}$  i  $\mathbb{Q} \subset L$  będzie ciałem rozkładu wielomianu minimalnego  $\alpha$  nad  $\mathbb{Q}$ . Wtedy  $\alpha$  jest konstruowalne wtedy i tylko wtedy, gdy  $[L:\mathbb{Q}]$  jest potęgą dwójki.

## Liczby konstruowalne

#### Dowód.

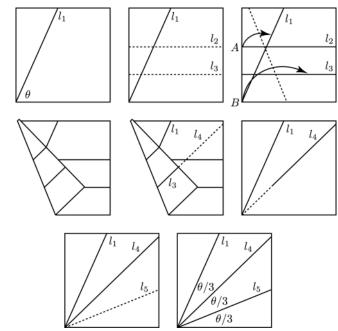
( $\Leftarrow$ ) Załóżmy, że  $[L:\mathbb{Q}]$  jest potęgą dwójki. Ponieważ  $L/\mathbb{Q}$  jest Galois, to  $|Gal(L/\mathbb{Q})| = [L:\mathbb{Q}] = 2^n$ .  $Gal(L/\mathbb{Q})$  jest rozwiązywalna, więc istnieją podgrupy:

$$\{e\} = \textit{G}_m \subset \textit{G}_{m-1} \subset ... \subset \textit{G}_1 \subset \textit{G}_0 = \textit{Gal}(\textit{L}/\mathbb{Q})$$

takie, że  $G_{i-1}$  jest podgrupą normalną dla  $G_i$  o indeksie 2. Z odpowiedniości Galois wynika, że istnieje wieża ciał

$$\mathbb{Q}=L_{G_0}\subset L_{G_1}\subset ...\subset L_{G_m}=L,$$

gdzie  $[L_{G_i}:L_{G_{i-1}}]=2$ . Zatem  $\alpha$  jest konstruowalne.



#### Lemat

Niech  $P_1$  będzie punktem na płaszczyźnie nie leżącym na linii  $l_1$ . Linia l, o którą odbicie  $P_1$  leży na prostej  $l_1$ , jest styczna z parabolą o ogniskowej w  $P_1$  i kierownicy  $l_1$ .

#### Przykład

pokażemy, jak za pomocą stycznej do 2 paraboli policzyć pierwiastki wielomianu  $x^3 + ax + b = c$  rozważmy parabole

$$(y - \frac{a}{2})^2 = 2bx \text{ oraz } y = \frac{1}{2}x^2$$

Niech I będzie prostą styczną do tych parabol. w punktach  $(x_1, y_1)$  pierwszą oraz  $(x_2, y_2)$  drugą. współczynnik nachylenia prostej wynosi:

$$m = \frac{b}{y_1 - \frac{1}{2}a}$$

stąd  $m \neq 0$  oraz:

$$x_1 = \frac{zb}{2m^2}$$
$$y_1 = \frac{zb}{m} + \frac{a}{2}$$

### Przykład

Jeśli podstawimy pod  $m = \frac{y_1 - y_2}{x_1 - x_2}$  otrzymamy:

$$m = \frac{y_1 - y_2}{x_1 - x_2} = \frac{\frac{m^2}{2} - (\frac{b}{m} + \frac{a}{2})}{m - \frac{2}{2m^2}} = \frac{m^4 - 2m - qm^2}{2m^3 - b}$$

Co sprowadza się do:

$$m^3 + am^2 + bm + c = 0$$

#### Readable Mathematics

Let  $X_1, X_2, \ldots, X_n$  be a sequence of independent and identically distributed random variables with  $\mathsf{E}[X_i] = \mu$  and  $\mathsf{Var}[X_i] = \sigma^2 < \infty$ , and let

$$S_n = \frac{X_1 + X_2 + \dots + X_n}{n} = \frac{1}{n} \sum_{i=1}^{n} X_i$$

denote their mean. Then as n approaches infinity, the random variables  $\sqrt{n}(S_n - \mu)$  converge in distribution to a normal  $\mathcal{N}(0, \sigma^2)$ .