Polígonos e números construtíveis

Arthur Rezende Alves Neto

Universidade Federal do Paraná

13 de agosto de 2020

Construção euclidiana

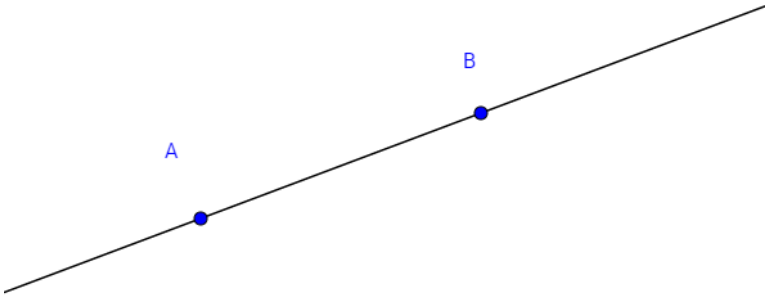
Para os matemáticos gregos solucionar um problema, provar uma proposição ou teorema era equivalente a construir, geometricamente, uma solução. E a maneira de se escrever essas soluções podem ser dadas por construções utilizando régua e compasso.

Construção euclidiana

Para os matemáticos gregos solucionar um problema, provar uma proposição ou teorema era equivalente a construir, geometricamente, uma solução. E a maneira de se escrever essas soluções podem ser dadas por construções utilizando régua e compasso.

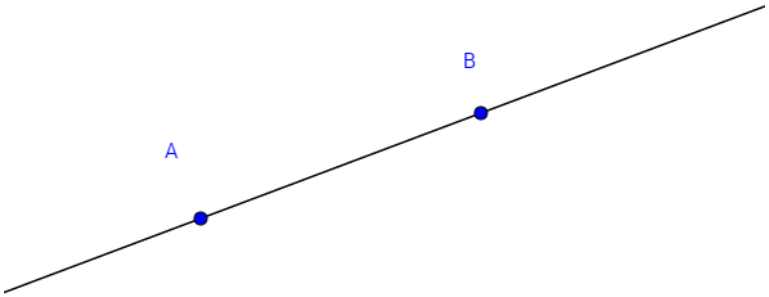
A régua utilizada não é graduada, apenas permite traçar uma reta passando por dois pontos ou estender uma reta dada. O compasso é utilizado para traçar circunferências dado um centro (ponta seca) e um raio (abertura do compasso), mas também pode ser utilizado para transportar segmentos.

Na prática estaremos utilizando os seguintes axiomas euclidianos:

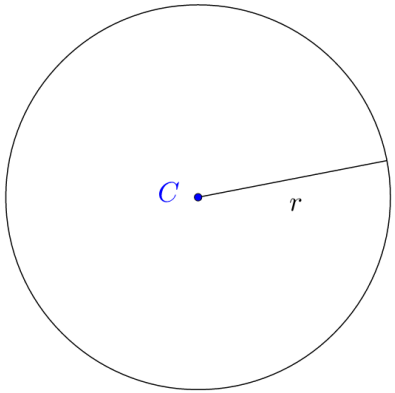


Sejam A e B dois pontos distintos. Podemos traçar uma única reta que passa por A e B.

Na prática estaremos utilizando os seguintes axiomas euclidianos:



Sejam A e B dois pontos distintos. Podemos traçar uma única reta que passa por A e B.



Dado um segmento de medida r e um ponto C, traçamos uma circunferência de raio r e centro em C.

A partir desses axiomas podemos começar com algumas construções básicas.

1. Sejam r uma reta e A um ponto, podemos construir uma reta g, que contêm o ponto A e é perpendicular à reta r.

A partir desses axiomas podemos começar com algumas construções básicas.

1. Sejam r uma reta e A um ponto, podemos construir uma reta g, que contêm o ponto A e é perpendicular à reta r.
2. Sejam r uma reta e A um ponto exterior à r, podemos construir uma reta g, que contêm o ponto A e é paralela à reta r.

A partir desses axiomas podemos começar com algumas construções básicas.

1. Sejam r uma reta e A um ponto, podemos construir uma reta g, que contêm o ponto A e é perpendicular à reta r.
2. Sejam r uma reta e A um ponto exterior à r, podemos construir uma reta g, que contêm o ponto A e é paralela à reta r.
3. Seja α um ângulo, podemos dividir α em dois ângulos congruentes.

Definições

Um segmento é **construtível** se pode ser obtido a partir de um número finito de construções utilizando os dois axiomas mencionados.

Definições

Um segmento é **construtível** se pode ser obtido a partir de um número finito de construções utilizando os dois axiomas mencionados.

Definição

*Um número real x é dito **construtível** se: $x = 0$ ou se existe um segmento de medida $|x|$ construtível. Tudo a partir de uma unidade pré-definida.*

Definições

Um segmento é **construtível** se pode ser obtido a partir de um número finito de construções utilizando os dois axiomas mencionados.

Definição

*Um número real x é dito **construtível** se: $x = 0$ ou se existe um segmento de medida $|x|$ construtível. Tudo a partir de uma unidade pré-definida.*

- Seja $n \in \mathbb{Z}$, então é construtível e $1/n$ é construtível.

Definições

Um segmento é **construtível** se pode ser obtido a partir de um número finito de construções utilizando os dois axiomas mencionados.

Definição

*Um número real x é dito **construtível** se: $x = 0$ ou se existe um segmento de medida $|x|$ construtível. Tudo a partir de uma unidade pré-definida.*

- Seja $n \in \mathbb{Z}$, então é construtível e $1/n$ é construtível.
- Sejam a e b dois números construtíveis, então $a + b$, $a - b$ e ab são números construtíveis.

Definições

Um segmento é **construtível** se pode ser obtido a partir de um número finito de construções utilizando os dois axiomas mencionados.

Definição

*Um número real x é dito **construtível** se: $x = 0$ ou se existe um segmento de medida $|x|$ construtível. Tudo a partir de uma unidade pré-definida.*

- Seja $n \in \mathbb{Z}$, então é construtível e $1/n$ é construtível.
- Sejam a e b dois números construtíveis, então $a + b$, $a - b$ e ab são números construtíveis.
- Se a é um número construtível, então $\sqrt{a}$ também é.

Seja $\mathcal{C} = \{x \in \mathbb{R}; x$ é um número construtível$\}$.

Seja $\mathcal{C} = \{x \in \mathbb{R}; x$ é um número construtível$\}$. Dado o fato de que

- $1 \in \mathcal{C}$;
- se $a, b \in \mathcal{C}$, então $a \pm b \in \mathcal{C}$, $ab \in \mathcal{C}$ e $\frac{a}{b} \in \mathcal{C}$.

Concluímos que $\mathcal{C}$ é um corpo, e mais ainda $\mathbb{Q} \subseteq \mathcal{C}$.

Seja $\mathcal{C} = \{x \in \mathbb{R}; x \text{ é um número construtível}\}$. Dado o fato de que

- $1 \in \mathcal{C}$;
- se $a, b \in \mathcal{C}$, então $a \pm b \in \mathcal{C}$, $ab \in \mathcal{C}$ e $\frac{a}{b} \in \mathcal{C}$.

Concluímos que $\mathcal{C}$ é um corpo, e mais ainda $\mathbb{Q} \subseteq \mathcal{C}$.

O ambiente mais natural para considerar as construções que fazemos é o plano, mais ainda, podemos pensar $\mathcal{C} \subseteq \mathbb{C}$.

Seja $\mathcal{C} = \{x \in \mathbb{R}; x$ é um número construtível$\}$. Dado o fato de que

- $1 \in \mathcal{C}$;
- se $a, b \in \mathcal{C}$, então $a \pm b \in \mathcal{C}$, $ab \in \mathcal{C}$ e $\frac{a}{b} \in \mathcal{C}$.

Concluímos que $\mathcal{C}$ é um corpo, e mais ainda $\mathbb{Q} \subseteq \mathcal{C}$.

O ambiente mais natural para considerar as construções que fazemos é o plano, mais ainda, podemos pensar $\mathcal{C} \subseteq \mathbb{C}$.

Definição

*Seja $z \in \mathbb{C}$, dizemos que é um **número construtível** se $z = 0$ ou se o segmento definido por z é construtível.*

Seja $z = a + ib \in \mathbb{C}$, então são equivalentes:

- z é um número construtível,
- a e b são números construtíveis,
- $|z|$ é um número construtível e o argumento de z é um ângulo construtível.

Seja $z = a + ib \in \mathbb{C}$, então são equivalentes:

- z é um número construtível,
- a e b são números construtíveis,
- $|z|$ é um número construtível e o argumento de z é um ângulo construtível.

Tome $z = a + ib$ e $w = c + id$ dois números complexos:

Seja $z = a + ib \in \mathbb{C}$, então são equivalentes:

- z é um número construtível,
- a e b são números construtíveis,
- $|z|$ é um número construtível e o argumento de z é um ângulo construtível.

Tome $z = a + ib$ e $w = c + id$ dois números complexos:

- $z \pm w = (a \pm c) + i(b \pm d)$,

Seja $z = a + ib \in \mathbb{C}$, então são equivalentes:

- z é um número construtível,
- a e b são números construtíveis,
- $|z|$ é um número construtível e o argumento de z é um ângulo construtível.

Tome $z = a + ib$ e $w = c + id$ dois números complexos:

- $z \pm w = (a \pm c) + i(b \pm d)$,
- $zw = (a + ib)(c + id) = (ac - bd) + i(ad + bc)$,

Seja $z = a + ib \in \mathbb{C}$, então são equivalentes:

- z é um número construtível,
- a e b são números construtíveis,
- $|z|$ é um número construtível e o argumento de z é um ângulo construtível.

Tome $z = a + ib$ e $w = c + id$ dois números complexos:

- $z \pm w = (a \pm c) + i(b \pm d)$,
- $zw = (a + ib)(c + id) = (ac - bd) + i(ad + bc)$,
- $\dfrac{z}{w} = \dfrac{a + ib}{c + id} = \left(\dfrac{ac + bd}{c^2 + d^2}\right) + i\left(\dfrac{bc - ad}{c^2 + d^2}\right)$.

Seja $z = a + ib \in \mathbb{C}$, então são equivalentes:

- z é um número construtível,
- a e b são números construtíveis,
- $|z|$ é um número construtível e o argumento de z é um ângulo construtível.

Tome $z = a + ib$ e $w = c + id$ dois números complexos:

- $z \pm w = (a \pm c) + i(b \pm d)$,
- $zw = (a + ib)(c + id) = (ac - bd) + i(ad + bc)$,
- $\dfrac{z}{w} = \dfrac{a + ib}{c + id} = \left(\dfrac{ac + bd}{c^2 + d^2}\right) + i\left(\dfrac{bc - ad}{c^2 + d^2}\right)$.

Se z e w são construtíveis, então $z \pm w$, zw e $\frac{z}{w}$ também são.

Sejam z e w números complexos, e suas formas polares $z = |z|\big(cos(\theta) + isen(\theta)\big)$ e $w = |w|\big(cos(\alpha) + isen(\alpha)\big)$

Sejam z e w números complexos, e suas formas polares $z = |z|\big(cos(\theta) + isen(\theta)\big)$ e $w = |w|\big(cos(\alpha) + isen(\alpha)\big)$

$$\begin{aligned} zw &= |z|\big(cos(\theta) + isen(\theta)\big)|w|\big(cos(\alpha) + isen(\alpha)\big) \\ &= |z||w|\big(cos(\theta) + isen(\theta)\big)\big(cos(\alpha) + isen(\alpha)\big) \end{aligned}$$

Sejam z e w números complexos, e suas formas polares $z = |z|\big(cos(\theta) + isen(\theta)\big)$ e $w = |w|\big(cos(\alpha) + isen(\alpha)\big)$

$$\begin{aligned} zw &= |z|\big(cos(\theta) + isen(\theta)\big)|w|\big(cos(\alpha) + isen(\alpha)\big) \\ &= |z||w|\big(cos(\theta) + isen(\theta)\big)\big(cos(\alpha) + isen(\alpha)\big) \\ &= |z||w|\big(cos(\theta)cos(\alpha) - sen(\theta)sen(\alpha)\big) \\ &\qquad +\big(sen(\theta)cos(\alpha) + sen(\alpha)cos(\theta)\big) \\ &= |z||w|\big(cos(\theta+\alpha)\big) + i\big(sen(\theta+\alpha)\big) \end{aligned}$$

Sejam z e w números complexos, e suas formas polares $z = |z|\big(cos(\theta) + isen(\theta)\big)$ e $w = |w|\big(cos(\alpha) + isen(\alpha)\big)$

$$\begin{aligned} zw &= |z|\big(cos(\theta) + isen(\theta)\big)|w|\big(cos(\alpha) + isen(\alpha)\big) \\ &= |z||w|\big(cos(\theta) + isen(\theta)\big)\big(cos(\alpha) + isen(\alpha)\big) \\ &= |z||w|\big(cos(\theta)cos(\alpha) - sen(\theta)sen(\alpha)\big) \\ &\qquad +\big(sen(\theta)cos(\alpha) + sen(\alpha)cos(\theta)\big) \\ &= |z||w|\big(cos(\theta+\alpha)\big) + i\big(sen(\theta+\alpha)\big) \end{aligned}$$

Se $z = |z|(cos(\theta) + isen(\theta))$ é um número construtível, então

$$\sqrt{z} = \sqrt{|z|}\left(cos\left(\frac{\theta}{2}\right) + isen\left(\frac{\theta}{2}\right)\right)$$

também é.

Dado a natureza dos processos de construções euclidianas, vemos que $\mathcal{C}$ é um subcorpo de $\mathbb{C}$ que contêm $\mathbb{Q}$, em outras palavras $\mathcal{C} \supseteq \mathbb{Q}$.

Dado a natureza dos processos de construções euclidianas, vemos que $\mathcal{C}$ é um subcorpo de $\mathbb{C}$ que contêm $\mathbb{Q}$, em outras palavras $\mathcal{C} \supseteq \mathbb{Q}$.

Definição

*Sejam $\mathbb{K}$ e $\mathbb{F}$ dois corpos, se $\mathbb{K}$ é um subcorpo de $\mathbb{F}$, dizemos que $\mathbb{F}$ é uma **extensão** de $\mathbb{K}$ e escrevemos $\mathbb{F}|\mathbb{K}$.*

Dado a natureza dos processos de construções euclidianas, vemos que $\mathcal{C}$ é um subcorpo de $\mathbb{C}$ que contêm $\mathbb{Q}$, em outras palavras $\mathcal{C} \supseteq \mathbb{Q}$.

Definição

*Sejam $\mathbb{K}$ e $\mathbb{F}$ dois corpos, se $\mathbb{K}$ é um subcorpo de $\mathbb{F}$, dizemos que $\mathbb{F}$ é uma **extensão** de $\mathbb{K}$ e escrevemos $\mathbb{F}|\mathbb{K}$.*

- $\mathbb{R}|\mathbb{Q}$, $\mathbb{C}|\mathbb{Q}$ e $\mathbb{C}|\mathbb{R}$.

Dado a natureza dos processos de construções euclidianas, vemos que $\mathcal{C}$ é um subcorpo de $\mathbb{C}$ que contêm $\mathbb{Q}$, em outras palavras $\mathcal{C} \supseteq \mathbb{Q}$.

Definição

*Sejam $\mathbb{K}$ e $\mathbb{F}$ dois corpos, se $\mathbb{K}$ é um subcorpo de $\mathbb{F}$, dizemos que $\mathbb{F}$ é uma **extensão** de $\mathbb{K}$ e escrevemos $\mathbb{F}|\mathbb{K}$.*

- $\mathbb{R}|\mathbb{Q}$, $\mathbb{C}|\mathbb{Q}$ e $\mathbb{C}|\mathbb{R}$.
- Defina $\mathbb{Q}(\sqrt{2}) = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$ e $\mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}$. Então $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ e $\mathbb{Q}(i)|\mathbb{Q}$.

Dado a natureza dos processos de construções euclidianas, vemos que $\mathcal{C}$ é um subcorpo de $\mathbb{C}$ que contêm $\mathbb{Q}$, em outras palavras $\mathcal{C} \supseteq \mathbb{Q}$.

Definição

*Sejam $\mathbb{K}$ e $\mathbb{F}$ dois corpos, se $\mathbb{K}$ é um subcorpo de $\mathbb{F}$, dizemos que $\mathbb{F}$ é uma **extensão** de $\mathbb{K}$ e escrevemos $\mathbb{F}|\mathbb{K}$.*

- $\mathbb{R}|\mathbb{Q}$, $\mathbb{C}|\mathbb{Q}$ e $\mathbb{C}|\mathbb{R}$.
- Defina $\mathbb{Q}(\sqrt{2}) = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$ e $\mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}$. Então $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ e $\mathbb{Q}(i)|\mathbb{Q}$.

Seja $\mathbb{F}|\mathbb{K}$, então podemos compreender $\mathbb{F}$ como um $\mathbb{K}$-espaço vetorial e nessas circunstâncias definimos $[\mathbb{F} : \mathbb{K}] := \dim_{\mathbb{K}} \mathbb{F}$.

Dado a natureza dos processos de construções euclidianas, vemos que $\mathcal{C}$ é um subcorpo de $\mathbb{C}$ que contêm $\mathbb{Q}$, em outras palavras $\mathcal{C} \supseteq \mathbb{Q}$.

Definição

*Sejam $\mathbb{K}$ e $\mathbb{F}$ dois corpos, se $\mathbb{K}$ é um subcorpo de $\mathbb{F}$, dizemos que $\mathbb{F}$ é uma **extensão** de $\mathbb{K}$ e escrevemos $\mathbb{F}|\mathbb{K}$.*

- $\mathbb{R}|\mathbb{Q}$, $\mathbb{C}|\mathbb{Q}$ e $\mathbb{C}|\mathbb{R}$.
- Defina $\mathbb{Q}(\sqrt{2}) = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$ e $\mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}$. Então $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ e $\mathbb{Q}(i)|\mathbb{Q}$.

Seja $\mathbb{F}|\mathbb{K}$, então podemos compreender $\mathbb{F}$ como um $\mathbb{K}$-espaço vetorial e nessas circunstâncias definimos $[\mathbb{F} : \mathbb{K}] := \dim_{\mathbb{K}} \mathbb{F}$.

- $[\mathbb{C} : \mathbb{R}] = 2$ e $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Suponha agora que $[\mathbb{F} : \mathbb{K}] < \infty$, tome $\alpha \in \mathbb{F} \setminus \mathbb{K}$, então $\{1, \alpha\} \subseteq \mathbb{F}$ é um conjunto LI em relação à $\mathbb{K}$.

Suponha agora que $[\mathbb{F} : \mathbb{K}] < \infty$, tome $\alpha \in \mathbb{F} \setminus \mathbb{K}$, então $\{1, \alpha\} \subseteq \mathbb{F}$ é um conjunto LI em relação à $\mathbb{K}$. Tome $\{1, \alpha, \alpha^2, ...\}$, que é um conjunto LD,

Suponha agora que $[\mathbb{F} : \mathbb{K}] < \infty$, tome $\alpha \in \mathbb{F} \setminus \mathbb{K}$, então $\{1, \alpha\} \subseteq \mathbb{F}$ é um conjunto LI em relação à $\mathbb{K}$. Tome $\{1, \alpha, \alpha^2, ...\}$, que é um conjunto LD, logo existe um n e $a_0, a_1, ..., a_n \in \mathbb{K}$ não todos nulos, tais que

$$a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n = 0,$$

Suponha agora que $[\mathbb{F} : \mathbb{K}] < \infty$, tome $\alpha \in \mathbb{F} \setminus \mathbb{K}$, então $\{1, \alpha\} \subseteq \mathbb{F}$ é um conjunto LI em relação à $\mathbb{K}$. Tome $\{1, \alpha, \alpha^2, ...\}$, que é um conjunto LD, logo existe um n e $a_0, a_1, ..., a_n \in \mathbb{K}$ não todos nulos, tais que

$$a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n = 0,$$

e com isso α é raiz do polinômio $a_0 + a_1x + ... + a_nx^n \in \mathbb{K}[x]$.

Suponha agora que $[\mathbb{F} : \mathbb{K}] < \infty$, tome $\alpha \in \mathbb{F} \setminus \mathbb{K}$, então $\{1, \alpha\} \subseteq \mathbb{F}$ é um conjunto LI em relação à $\mathbb{K}$. Tome $\{1, \alpha, \alpha^2, ...\}$, que é um conjunto LD, logo existe um n e $a_0, a_1, ..., a_n \in \mathbb{K}$ não todos nulos, tais que

$$a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n = 0,$$

e com isso α é raiz do polinômio $a_0 + a_1x + ... + a_nx^n \in \mathbb{K}[x]$.

- Dados $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$, dizemos que α é **algébrico sobre** $\mathbb{K}$ se α é raiz de um polinômio não nulo em $\mathbb{K}[x]$.

Suponha agora que $[\mathbb{F} : \mathbb{K}] < \infty$, tome $\alpha \in \mathbb{F} \setminus \mathbb{K}$, então $\{1, \alpha\} \subseteq \mathbb{F}$ é um conjunto LI em relação à $\mathbb{K}$. Tome $\{1, \alpha, \alpha^2, ...\}$, que é um conjunto LD, logo existe um n e $a_0, a_1, ..., a_n \in \mathbb{K}$ não todos nulos, tais que

$$a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n = 0,$$

e com isso α é raiz do polinômio $a_0 + a_1x + ... + a_nx^n \in \mathbb{K}[x]$.

- Dados $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$, dizemos que α é **algébrico sobre** $\mathbb{K}$ se α é raiz de um polinômio não nulo em $\mathbb{K}[x]$.
- Se ainda todos os elementos $\alpha \in \mathbb{F}$ forem algébricos sobre $\mathbb{K}$, diremos que $\mathbb{F}|\mathbb{K}$ é uma **extensão algébrica**.

Se $z \in \mathcal{C}$ é algébrico sobre $\mathbb{Q}$, diremos apenas que z é algébrico.

- $\sqrt{2}$ e $\sqrt[3]{\sqrt{2} - \sqrt{5}}$, são algébricos, mas π não.

Seja α um número algébrico, então existe $m_\alpha(x) \in \mathbb{Q}$ um polinômio mônico (coeficiente líder é 1) de menor grau, tal que $m_\alpha(\alpha) = 0$. Tal polinômio é chamado de **polinômio minimal de** α.

Seja α um número algébrico, então existe $m_\alpha(x) \in \mathbb{Q}$ um polinômio mônico (coeficiente líder é 1) de menor grau, tal que $m_\alpha(\alpha) = 0$. Tal polinômio é chamado de **polinômio minimal de** α.

Proposição

Sejam $\mathbb{F}|\mathbb{K}$, $\alpha \in \mathbb{F}$ *e* $p(x) \in \mathbb{K}[x]$ *mônico, tal que* $p(\alpha) = 0$. *Então são equivalentes:*

- $p(x)$ *é o polinômio minimal de* α,
- *se* $q(x) \in \mathbb{K}[x]$, *tal que* $q(\alpha) = 0$, *então* $p(x)|q(x)$,
- $p(x)$ *é irredutível.*

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$. Denotamos $\mathbb{K}(\alpha)$ como o menor subcorpo de $\mathbb{F}$ que contêm $\mathbb{K}$ e α.

Proposição

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$ algébrico sobre $\mathbb{K}$. Se $n = \partial(m_\alpha)$, então $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ e $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$.

Exemplos: $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ e $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$. Denotamos $\mathbb{K}(\alpha)$ como o menor subcorpo de $\mathbb{F}$ que contêm $\mathbb{K}$ e α.

Proposição

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$ algébrico sobre $\mathbb{K}$. Se $n = \partial(m_\alpha)$, então $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ e $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$.

Exemplos: $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ e $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.
Vamos calcular $[\mathbb{Q}(\sqrt{2} - \sqrt{3}) : \mathbb{Q}]$, primeiro tome

$$\sqrt{2} - \sqrt{3} = x$$

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$. Denotamos $\mathbb{K}(\alpha)$ como o menor subcorpo de $\mathbb{F}$ que contêm $\mathbb{K}$ e α.

Proposição

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$ algébrico sobre $\mathbb{K}$. Se $n = \partial(m_\alpha)$, então $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ e $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$.

Exemplos: $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ e $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.
Vamos calcular $[\mathbb{Q}(\sqrt{2} - \sqrt{3}) : \mathbb{Q}]$, primeiro tome

$$\sqrt{2} - \sqrt{3} = x \Rightarrow 5 - 2\sqrt{6} = x^2$$

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$. Denotamos $\mathbb{K}(\alpha)$ como o menor subcorpo de $\mathbb{F}$ que contêm $\mathbb{K}$ e α.

Proposição

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$ algébrico sobre $\mathbb{K}$. Se $n = \partial(m_\alpha)$, então $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ e $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$.

Exemplos: $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ e $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.
Vamos calcular $[\mathbb{Q}(\sqrt{2} - \sqrt{3}) : \mathbb{Q}]$, primeiro tome

$$\sqrt{2} - \sqrt{3} = x \Rightarrow 5 - 2\sqrt{6} = x^2 \Rightarrow -2\sqrt{6} = x^2 - 5$$
$$\Rightarrow 24 = x^4 - 10x^2 + 25$$

Então $\sqrt{2} - \sqrt{3}$ é raiz de $x^4 - 10x^2 + 1$,

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$. Denotamos $\mathbb{K}(\alpha)$ como o menor subcorpo de $\mathbb{F}$ que contêm $\mathbb{K}$ e α.

Proposição

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha \in \mathbb{F}$ algébrico sobre $\mathbb{K}$. Se $n = \partial(m_\alpha)$, então $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ e $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ é uma base de $\mathbb{K}(\alpha)$ sobre $\mathbb{K}$.

Exemplos: $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ e $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$.
Vamos calcular $[\mathbb{Q}(\sqrt{2} - \sqrt{3}) : \mathbb{Q}]$, primeiro tome

$$\sqrt{2} - \sqrt{3} = x \Rightarrow 5 - 2\sqrt{6} = x^2 \Rightarrow -2\sqrt{6} = x^2 - 5$$
$$\Rightarrow 24 = x^4 - 10x^2 + 25$$

Então $\sqrt{2} - \sqrt{3}$ é raiz de $x^4 - 10x^2 + 1$,que é irredutível, e portanto $[\mathbb{Q}(\sqrt{2} - \sqrt{3}) : \mathbb{Q}] = 4$.

Proposição

Sejam $\mathbb{F}|\mathbb{K}$ e $\mathbb{K}|\mathbb{L}$ duas extensões finitas, então a extensão $\mathbb{F}|\mathbb{L}$ é finita e

$$[\mathbb{F} : \mathbb{L}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

Proposição

Sejam $\mathbb{F}|\mathbb{K}$ e $\mathbb{K}|\mathbb{L}$ duas extensões finitas, então a extensão $\mathbb{F}|\mathbb{L}$ é finita e

$$[\mathbb{F} : \mathbb{L}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha_1 \in \mathbb{F} \setminus \mathbb{K}$, podemos então considerar a extensão $\mathbb{K}(\alpha_1)$.

Proposição

Sejam $\mathbb{F}|\mathbb{K}$ e $\mathbb{K}|\mathbb{L}$ duas extensões finitas, então a extensão $\mathbb{F}|\mathbb{L}$ é finita e

$$[\mathbb{F} : \mathbb{L}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha_1 \in \mathbb{F} \setminus \mathbb{K}$, podemos então considerar a extensão $\mathbb{K}(\alpha_1)$. Tome agora $\alpha_2 \in \mathbb{F} \setminus \mathbb{K}(\alpha_1)$, então podemos fazer a extensão

$$\mathbb{K}(\alpha_1, \alpha_2) := \mathbb{K}(\alpha_1)(\alpha_2).$$

Proposição

Sejam $\mathbb{F}|\mathbb{K}$ e $\mathbb{K}|\mathbb{L}$ duas extensões finitas, então a extensão $\mathbb{F}|\mathbb{L}$ é finita e

$$[\mathbb{F} : \mathbb{L}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

Sejam $\mathbb{F}|\mathbb{K}$ e $\alpha_1 \in \mathbb{F} \setminus \mathbb{K}$, podemos então considerar a extensão $\mathbb{K}(\alpha_1)$. Tome agora $\alpha_2 \in \mathbb{F} \setminus \mathbb{K}(\alpha_1)$, então podemos fazer a extensão

$$\mathbb{K}(\alpha_1, \alpha_2) := \mathbb{K}(\alpha_1)(\alpha_2).$$

- Note que

$$\begin{aligned} [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \\ &\leq (2)(2) \end{aligned}$$

mas $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, logo $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2$.

Voltando ao problema de determinar se um número $z \in \mathbb{C}$ é construtível ou não.

Voltando ao problema de determinar se um número $z \in \mathbb{C}$ é construtível ou não. Podemos dizer que $z \in \mathbb{C} \setminus 0$ é um número construtível se existir uma sequência de pontos $1 = z_0, z_1, ..., z_s \in \mathbb{C}$, onde $z_s = z$ e cada z_j, $j \geq 1$, é obtido por meio de construções com régua e compasso envolvendo os pontos $z_1, ..., z_{j-1}$.

Voltando ao problema de determinar se um número $z \in \mathbb{C}$ é construtível ou não. Podemos dizer que $z \in \mathbb{C} \setminus 0$ é um número construtível se existir uma sequência de pontos $1 = z_0, z_1, ..., z_s \in \mathbb{C}$, onde $z_s = z$ e cada z_j, $j \geq 1$, é obtido por meio de construções com régua e compasso envolvendo os pontos $z_1, ..., z_{j-1}$.
Suponha que $z \in \mathcal{C}$, então temos a sequência de números construtíveis $1 = z_0, z_1, ..., z_{s-1}$ e $z_s = z$. Vamos avaliar os graus das extensões

$$\mathbb{Q}(z_1)|\mathbb{Q}, \mathbb{Q}(z_1, z_2)|\mathbb{Q}(z_1), ..., \mathbb{Q}(z_1, ..., z_s)|\mathbb{Q}(z_1, ..., z_{s-1}).$$

Para simplificar vamos denotar $\mathbb{K}_j := \mathbb{Q}(z_1, ..., z_j)$, com $j \geq 2$.

Proposição

Cada uma das extensões $\mathbb{K}_j|\mathbb{K}_{j-1}$, $j = 3, ..., s$, tem grau um, dois ou quatro.

Proposição

Cada uma das extensões $\mathbb{K}_j|\mathbb{K}_{j-1}$, $j = 3, ..., s$, tem grau um, dois ou quatro.

Corolário

$[\mathbb{K}_s : \mathbb{Q}] = 2^k$, *para algum* $k = 0, 1, 2, ...$

Note que $[\mathbb{K}_s : \mathbb{Q}] = [\mathbb{K}_s : \mathbb{K}_{s-1}][\mathbb{K}_{s-1} : \mathbb{K}_{s-1}]...[\mathbb{K}_1 : \mathbb{Q}]$.

Proposição

Cada uma das extensões $\mathbb{K}_j|\mathbb{K}_{j-1}$, $j = 3, ..., s$, tem grau um, dois ou quatro.

Corolário

$[\mathbb{K}_s : \mathbb{Q}] = 2^k$, *para algum* $k = 0, 1, 2, ...$

Note que $[\mathbb{K}_s : \mathbb{Q}] = [\mathbb{K}_s : \mathbb{K}_{s-1}][\mathbb{K}_{s-1} : \mathbb{K}_{s-1}]...[\mathbb{K}_1 : \mathbb{Q}]$.

Teorema

Seja $z \in \mathcal{C}$, então z é um número algébrico e $\partial(m_z(x)) = 2^k$, para algum $k \geq 0$.

Exemplo

- $[cos(\theta) + isen(\theta)][cos(\alpha) + isen(\alpha)] = cos(\theta + \alpha) + i(\theta + \alpha).$

Exemplo

- $[cos(\theta) + isen(\theta)][cos(\alpha) + isen(\alpha)] = cos(\theta + \alpha) + i(\theta + \alpha).$

$$\Rightarrow \left[cos(\theta) + isen(\theta)\right]^n = cos(n\theta) + isen(n\theta).$$

Exemplo

- $[cos(\theta) + isen(\theta)][cos(\alpha) + isen(\alpha)] = cos(\theta + \alpha) + i(\theta + \alpha).$

$$\Rightarrow \left[cos(\theta) + isen(\theta)\right]^n = cos(n\theta) + isen(n\theta).$$

Então $cos(\theta) + isen(\theta) = \left(cos\left(\frac{\theta}{3}\right) + isen\left(\frac{\theta}{3}\right)\right)^3$

$$cos(\theta) + isen(\theta) =$$
$$cos^3\left(\frac{\theta}{3}\right) + 2icos^2\left(\frac{\theta}{3}\right) sen\left(\frac{\theta}{3}\right) - 3cos\left(\frac{\theta}{3}\right) sen\left(\frac{\theta}{3}\right) - isen\left(\frac{\theta}{3}\right)$$

Exemplo

- $[cos(\theta) + isen(\theta)][cos(\alpha) + isen(\alpha)] = cos(\theta + \alpha) + i(\theta + \alpha).$

$$\Rightarrow \left[cos(\theta) + isen(\theta)\right]^n = cos(n\theta) + isen(n\theta).$$

Então $cos(\theta) + isen(\theta) = \left(cos\left(\frac{\theta}{3}\right) + isen\left(\frac{\theta}{3}\right)\right)^3$

$$cos(\theta) + isen(\theta) =$$
$$cos^3\left(\frac{\theta}{3}\right) + 2icos^2\left(\frac{\theta}{3}\right) sen\left(\frac{\theta}{3}\right) - 3cos\left(\frac{\theta}{3}\right) sen\left(\frac{\theta}{3}\right) - isen\left(\frac{\theta}{3}\right)$$

Comparando as partes reais da equação, $cos(\theta/3)$ é raiz do polinômio $4x^3 - 3x - cos(\theta)$.

Exemplo

- $[cos(\theta) + isen(\theta)][cos(\alpha) + isen(\alpha)] = cos(\theta + \alpha) + i(\theta + \alpha).$

$$\Rightarrow \left[cos(\theta) + isen(\theta)\right]^n = cos(n\theta) + isen(n\theta).$$

Então $cos(\theta) + isen(\theta) = \left(cos\left(\frac{\theta}{3}\right) + isen\left(\frac{\theta}{3}\right)\right)^3$

$$cos(\theta) + isen(\theta) =$$
$$cos^3\left(\frac{\theta}{3}\right) + 2icos^2\left(\frac{\theta}{3}\right) sen\left(\frac{\theta}{3}\right) - 3cos\left(\frac{\theta}{3}\right) sen\left(\frac{\theta}{3}\right) - isen\left(\frac{\theta}{3}\right)$$

Comparando as partes reais da equação, $cos(\theta/3)$ é raiz do polinômio $4x^3 - 3x - cos(\theta)$.
Tome $\theta = \pi/3$. Então $cos\left(\frac{\pi}{9}\right)$ é raiz do polinômio $4x^3 - 3x - 1/2$, ou ainda de $8x^3 - 3x - 1$, que é irredutível, logo é o polinômio minimal de $cos\left(\frac{\pi}{9}\right)$.

Exemplo

- $[cos(\theta) + isen(\theta)][cos(\alpha) + isen(\alpha)] = cos(\theta + \alpha) + i(\theta + \alpha).$

$$\Rightarrow \left[cos(\theta) + isen(\theta)\right]^n = cos(n\theta) + isen(n\theta).$$

Então $cos(\theta) + isen(\theta) = \left(cos\left(\frac{\theta}{3}\right) + isen\left(\frac{\theta}{3}\right)\right)^3$

$$cos(\theta) + isen(\theta) =$$
$$cos^3\left(\frac{\theta}{3}\right) + 2icos^2\left(\frac{\theta}{3}\right) sen\left(\frac{\theta}{3}\right) - 3cos\left(\frac{\theta}{3}\right) sen\left(\frac{\theta}{3}\right) - isen\left(\frac{\theta}{3}\right)$$

Comparando as partes reais da equação, $cos(\theta/3)$ é raiz do polinômio $4x^3 - 3x - cos(\theta)$.
Tome $\theta = \pi/3$. Então $cos\left(\frac{\pi}{9}\right)$ é raiz do polinômio $4x^3 - 3x - 1/2$, ou ainda de $8x^3 - 3x - 1$, que é irredutível, logo é o polinômio minimal de $cos\left(\frac{\pi}{9}\right)$. E assim $cos\left(\frac{\pi}{9}\right)$ não é construtível.

Utilizando apenas régua e compasso, vamos construir um

- Triângulo, Quadrado e Hexágono regulares.

Utilizando apenas régua e compasso, vamos construir um

- Triângulo, Quadrado e Hexágono regulares.
- Caso do pentágono, para isso, vamos calcular $cos\left(\frac{2\pi}{5}\right)$.

Utilizando apenas régua e compasso, vamos construir um

- Triângulo, Quadrado e Hexágono regulares.
- Caso do pentágono, para isso, vamos calcular $cos\left(\frac{2\pi}{5}\right)$.

Note que

$$cos\left(2\frac{2\pi}{5}\right) = cos\left(2\pi - 2\frac{2\pi}{5}\right) = cos\left(3\frac{2\pi}{5}\right)$$

Utilizando apenas régua e compasso, vamos construir um

- Triângulo, Quadrado e Hexágono regulares.
- Caso do pentágono, para isso, vamos calcular $cos\left(\frac{2\pi}{5}\right)$.

Note que

$$cos\left(2\frac{2\pi}{5}\right) = cos\left(2\pi - 2\frac{2\pi}{5}\right) = cos\left(3\frac{2\pi}{5}\right)$$

$$\Rightarrow 2cos^2\left(\frac{2\pi}{5}\right) - 1 = 4cos^3\left(\frac{2\pi}{5}\right) - 3cos\left(\frac{2\pi}{5}\right)$$

Utilizando apenas régua e compasso, vamos construir um

- Triângulo, Quadrado e Hexágono regulares.
- Caso do pentágono, para isso, vamos calcular $cos\left(\frac{2\pi}{5}\right)$.

Note que

$$cos\left(2\frac{2\pi}{5}\right) = cos\left(2\pi - 2\frac{2\pi}{5}\right) = cos\left(3\frac{2\pi}{5}\right)$$

$$\Rightarrow 2cos^2\left(\frac{2\pi}{5}\right) - 1 = 4cos^3\left(\frac{2\pi}{5}\right) - 3cos\left(\frac{2\pi}{5}\right)$$

Logo $cos\left(\frac{2\pi}{5}\right)$ é raiz do polinômio $4x^3 - 2x^2 - 3x + 1$, mas $4x^3 - 2x^2 - 3x - 1 = (x-1)(4x^2 + 2x - 1)$.

Utilizando apenas régua e compasso, vamos construir um

- Triângulo, Quadrado e Hexágono regulares.
- Caso do pentágono, para isso, vamos calcular $cos\left(\frac{2\pi}{5}\right)$.

Note que

$$cos\left(2\frac{2\pi}{5}\right) = cos\left(2\pi - 2\frac{2\pi}{5}\right) = cos\left(3\frac{2\pi}{5}\right)$$

$$\Rightarrow 2cos^2\left(\frac{2\pi}{5}\right) - 1 = 4cos^3\left(\frac{2\pi}{5}\right) - 3cos\left(\frac{2\pi}{5}\right)$$

Logo $cos\left(\frac{2\pi}{5}\right)$ é raiz do polinômio $4x^3 - 2x^2 - 3x + 1$, mas $4x^3 - 2x^2 - 3x - 1 = (x-1)(4x^2 + 2x - 1)$. Avaliando as raízes de $4x^2 + 2x - 1$, concluímos que $cos\left(\frac{2\pi}{5}\right) = \frac{1}{4}\left(\sqrt{5} - 1\right)$

Utilizando apenas régua e compasso, vamos construir um

- Triângulo, Quadrado e Hexágono regulares.
- Caso do pentágono, para isso, vamos calcular $cos\left(\frac{2\pi}{5}\right)$.

Note que

$$cos\left(2\frac{2\pi}{5}\right) = cos\left(2\pi - 2\frac{2\pi}{5}\right) = cos\left(3\frac{2\pi}{5}\right)$$

$$\Rightarrow 2cos^2\left(\frac{2\pi}{5}\right) - 1 = 4cos^3\left(\frac{2\pi}{5}\right) - 3cos\left(\frac{2\pi}{5}\right)$$

Logo $cos\left(\frac{2\pi}{5}\right)$ é raiz do polinômio $4x^3 - 2x^2 - 3x + 1$, mas $4x^3 - 2x^2 - 3x - 1 = (x-1)(4x^2 + 2x - 1)$. Avaliando as raízes de $4x^2 + 2x - 1$, concluímos que $cos\left(\frac{2\pi}{5}\right) = \frac{1}{4}\left(\sqrt{5} - 1\right)$

- Se $a, b, c \in \mathcal{C}$, então todas as raízes de $ax^2 + bx + c$ são construtíveis.

Como vimos, a construção de um polígono regular é equivalente a construir um número complexo, mais especificamente

- Para construir o polígono de n lados precisamos construir o número complexo $z = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$.

Como vimos, a construção de um polígono regular é equivalente a construir um número complexo, mais especificamente

- Para construir o polígono de n lados precisamos construir o número complexo $z = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$.
- Utilizando a fórmula de Euler: $e^{i\theta} = cos(\theta) + isen(\theta)$. Queremos estudar os seguintes números complexos

$$z = e^{\frac{2\pi}{n}i}$$

Como vimos, a construção de um polígono regular é equivalente a construir um número complexo, mais especificamente

- Para construir o polígono de n lados precisamos construir o número complexo $z = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$.
- Utilizando a fórmula de Euler: $e^{i\theta} = cos(\theta) + isen(\theta)$. Queremos estudar os seguintes números complexos

$$z = e^{\frac{2\pi}{n}i}$$

Note que $z^n = \left(e^{\frac{2\pi}{n}i}\right)^n = e^{2\pi i} = 1$, logo z é raiz do polinômio $x^n - 1$,

Como vimos, a construção de um polígono regular é equivalente a construir um número complexo, mais especificamente

- Para construir o polígono de n lados precisamos construir o número complexo $z = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$.
- Utilizando a fórmula de Euler: $e^{i\theta} = cos(\theta) + isen(\theta)$. Queremos estudar os seguintes números complexos

$$z = e^{\frac{2\pi}{n}i}$$

Note que $z^n = \left(e^{\frac{2\pi}{n}i}\right)^n = e^{2\pi i} = 1$, logo z é raiz do polinômio $x^n - 1$, e

$$x^n - 1 = (x-1)\left(x^{n-1} + x^{n-2} + ... + x + 1\right).$$

Como vimos, a construção de um polígono regular é equivalente a construir um número complexo, mais especificamente

- Para construir o polígono de n lados precisamos construir o número complexo $z = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$.
- Utilizando a fórmula de Euler: $e^{i\theta} = cos(\theta) + isen(\theta)$. Queremos estudar os seguintes números complexos

$$z = e^{\frac{2\pi}{n}i}$$

Note que $z^n = \left(e^{\frac{2\pi}{n}i}\right)^n = e^{2\pi i} = 1$, logo z é raiz do polinômio $x^n - 1$, e

$$x^n - 1 = (x-1)\left(x^{n-1} + x^{n-2} + ... + x + 1\right).$$

Se $n > 1$, então z é raiz de $x^{n-1} + x^{n-2} + ... + x + 1$.

- $n = 6$. Denote $z = e^{\frac{2\pi}{6}i}$, então z é raiz de $x^6 - 1$ e também de $x^5 + x^4 + x^3 + x^2 + x + 1$.

- $n = 6$. Denote $z = e^{\frac{2\pi}{6}i}$, então z é raiz de $x^6 - 1$ e também de $x^5 + x^4 + x^3 + x^2 + x + 1$. Por outro lado, $z^3 = \left(e^{\frac{\pi}{3}i}\right)^3 = -1$, então z também é raiz de $x^3 + 1$.

- $n = 6$. Denote $z = e^{\frac{2\pi}{6}i}$, então z é raiz de $x^6 - 1$ e também de $x^5 + x^4 + x^3 + x^2 + x + 1$. Por outro lado, $z^3 = \left(e^{\frac{\pi}{3}i}\right)^3 = -1$, então z também é raiz de $x^3 + 1$.

$$\begin{aligned} \Rightarrow x^6 - 1 &= (x-1)(x^3+1)(x^2+x+1) \\ &= (x-1)(x+1)(x^2-x+1)(x^2+x+1), \end{aligned}$$

- $n = 6$. Denote $z = e^{\frac{2\pi}{6}i}$, então z é raiz de $x^6 - 1$ e também de $x^5 + x^4 + x^3 + x^2 + x + 1$. Por outro lado, $z^3 = \left(e^{\frac{\pi}{3}i}\right)^3 = -1$, então z também é raiz de $x^3 + 1$.

$$\begin{aligned} \Rightarrow x^6 - 1 &= (x-1)(x^3+1)(x^2+x+1) \\ &= (x-1)(x+1)(x^2-x+1)(x^2+x+1), \end{aligned}$$

então z é raiz de $x^2 - x + 1$, e este é irredutível. Portanto $z = e^{\frac{2\pi}{6}i}$ é construtível.

- $n = 6$. Denote $z = e^{\frac{2\pi}{6}i}$, então z é raiz de $x^6 - 1$ e também de $x^5 + x^4 + x^3 + x^2 + x + 1$. Por outro lado, $z^3 = \left(e^{\frac{\pi}{3}i}\right)^3 = -1$, então z também é raiz de $x^3 + 1$.

$$\begin{aligned} \Rightarrow x^6 - 1 &= (x-1)(x^3+1)(x^2+x+1) \\ &= (x-1)(x+1)(x^2-x+1)(x^2+x+1), \end{aligned}$$

  então z é raiz de $x^2 - x + 1$, e este é irredutível. Portanto $z = e^{\frac{2\pi}{6}i}$ é construtível.
- $n = 5$. Denote $z = e^{\frac{2\pi}{5}i}$, e z é raiz de $x^5 - 1$, mas

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1).$$

- $n = 6$. Denote $z = e^{\frac{2\pi}{6}i}$, então z é raiz de $x^6 - 1$ e também de $x^5 + x^4 + x^3 + x^2 + x + 1$. Por outro lado, $z^3 = \left(e^{\frac{\pi}{3}i}\right)^3 = -1$, então z também é raiz de $x^3 + 1$.

$$\begin{aligned} \Rightarrow x^6 - 1 &= (x-1)(x^3+1)(x^2+x+1) \\ &= (x-1)(x+1)(x^2-x+1)(x^2+x+1), \end{aligned}$$

  então z é raiz de $x^2 - x + 1$, e este é irredutível. Portanto $z = e^{\frac{2\pi}{6}i}$ é construtível.
- $n = 5$. Denote $z = e^{\frac{2\pi}{5}i}$, e z é raiz de $x^5 - 1$, mas

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1).$$

  Logo z é raiz de $x^4 + x^3 + x^2 + x + 1$, esse é irredutível, e z é construtível.

Teorema (critério de Eisenstein)

Seja $p(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$, *suponha que exista um número primo* p, *tal que* $p \mid a_0, a_1, ..., a_{n-1}$, $p \nmid a_n$ *e* $p^2 \nmid a_0$. *Então* $p(x)$ *é irredutível sobre* $\mathbb{Q}[x]$.

Teorema (critério de Eisenstein)

Seja $p(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$, *suponha que exista um número primo* p, *tal que* $p \mid a_0, a_1, ..., a_{n-1}$, $p \nmid a_n$ *e* $p^2 \nmid a_0$. *Então* $p(x)$ *é irredutível sobre* $\mathbb{Q}[x]$.

- $p(x)$ é irredutível se, e só se, $p(x+1)$ é irredutível.

$$p(x) = g(x)h(x) \Rightarrow p(x+1) = g(x+1)h(x+1)$$

Teorema (critério de Eisenstein)

Seja $p(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$, *suponha que exista um número primo* p, *tal que* $p \mid a_0, a_1, ..., a_{n-1}$, $p \nmid a_n$ *e* $p^2 \nmid a_0$. *Então* $p(x)$ *é irredutível sobre* $\mathbb{Q}[x]$.

- $p(x)$ é irredutível se, e só se, $p(x+1)$ é irredutível.

$$p(x) = g(x)h(x) \Rightarrow p(x+1) = g(x+1)h(x+1)$$
$$p(x+1) = g(x)h(x) \Rightarrow p(x) = g(x-1)h(x-1).$$

Tome $f(x) = \sum_{k=0}^{p-1} x^k$, com p primo. Note que

$$f(x+1) = \sum_{k=0}^{p-1}(x+1)^k$$

Teorema (critério de Eisenstein)

Seja $p(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$, *suponha que exista um número primo* p, *tal que* $p \mid a_0, a_1, ..., a_{n-1}$, $p \nmid a_n$ *e* $p^2 \nmid a_0$. *Então* $p(x)$ *é irredutível sobre* $\mathbb{Q}[x]$.

- $p(x)$ é irredutível se, e só se, $p(x+1)$ é irredutível.

$$p(x) = g(x)h(x) \Rightarrow p(x+1) = g(x+1)h(x+1)$$
$$p(x+1) = g(x)h(x) \Rightarrow p(x) = g(x-1)h(x-1).$$

Tome $f(x) = \sum_{k=0}^{p-1} x^k$, com p primo. Note que

$$\begin{aligned} f(x+1) &= \sum_{k=0}^{p-1}(x+1)^k \\ &= x^{p-1} + px^{p-2} + p(p-1)x^{p-3} + ... + p, \end{aligned}$$

logo $f(x+1)$ é irredutível e $f(x)$ também.

- Seja p um número primo, temos que $x^{p-1} + x^{p-2} + ... + x + 1$ é irredutível.

- Seja p um número primo, temos que $x^{p-1} + x^{p-2} + ... + x + 1$ é irredutível.

Tome $n = 7$. Considere $z = e^{\frac{2\pi}{7}i}$, sabemos que z é raiz de $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, e esse é irredutível.

- Seja p um número primo, temos que $x^{p-1} + x^{p-2} + ... + x + 1$ é irredutível.

Tome $n = 7$. Considere $z = e^{\frac{2\pi}{7}i}$, sabemos que z é raiz de $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, e esse é irredutível. Logo z não é construtível e assim o heptágono regular não é construtível com régua e compasso.

- Seja p um número primo, temos que $x^{p-1} + x^{p-2} + ... + x + 1$ é irredutível.

Tome $n = 7$. Considere $z = e^{\frac{2\pi}{7}i}$, sabemos que z é raiz de $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, e esse é irredutível. Logo z não é construtível e assim o heptágono regular não é construtível com régua e compasso.

- Para que um polígono regular de p lados (com p primo) seja construtível, é necessário que $p - 1 = 2^k$, para algum k.

- Seja p um número primo, temos que $x^{p-1} + x^{p-2} + ... + x + 1$ é irredutível.

Tome $n = 7$. Considere $z = e^{\frac{2\pi}{7}i}$, sabemos que z é raiz de $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, e esse é irredutível. Logo z não é construtível e assim o heptágono regular não é construtível com régua e compasso.

- Para que um polígono regular de p lados (com p primo) seja construtível, é necessário que $p - 1 = 2^k$, para algum k.

Então os polígonos de 7, 11 e 13 lados não são construtíveis.

- Seja p um número primo, temos que $x^{p-1} + x^{p-2} + ... + x + 1$ é irredutível.

Tome $n = 7$. Considere $z = e^{\frac{2\pi}{7}i}$, sabemos que z é raiz de $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, e esse é irredutível. Logo z não é construtível e assim o heptágono regular não é construtível com régua e compasso.

- Para que um polígono regular de p lados (com p primo) seja construtível, é necessário que $p - 1 = 2^k$, para algum k.

Então os polígonos de 7, 11 e 13 lados não são construtíveis. O polígono de 17 lados é construtível e foi em 1796 que, aos dezenove anos, Gauss mostrou esse fato.

Primos de Fermat

Se $2^k + 1$ é um número primo, então $k = 2^n$ para algum $n \geq 0$.

Primos de Fermat

Se $2^k + 1$ é um número primo, então $k = 2^n$ para algum $n \geq 0$. Suponha por absurdo que $k \neq 2^n$ para todo $n \geq 0$, então k deve ter algum fator ímpar $s > 1$ e $n = ts$ para algum $t \geq 1$.

Primos de Fermat

Se $2^k + 1$ é um número primo, então $k = 2^n$ para algum $n \geq 0$. Suponha por absurdo que $k \neq 2^n$ para todo $n \geq 0$, então k deve ter algum fator ímpar $s > 1$ e $n = ts$ para algum $t \geq 1$. Note que

$$2^k + 1 = (2^t)^s + 1$$

Primos de Fermat

Se $2^k + 1$ é um número primo, então $k = 2^n$ para algum $n \geq 0$. Suponha por absurdo que $k \neq 2^n$ para todo $n \geq 0$, então k deve ter algum fator ímpar $s > 1$ e $n = ts$ para algum $t \geq 1$. Note que

$$2^k + 1 = (2^t)^s + 1 = (2^t + 1)\left[(2^t)^{s-1} - (2^t)^{s-2} + ... - 2^t + 1\right],$$

como $0 < t < k$, então $2 < 2^t + 1 < 2^k + 1$. Com isso $2^k + 1$ tem um fator não trivial e portanto não é um número primo.

Primos de Fermat

Se $2^k + 1$ é um número primo, então $k = 2^n$ para algum $n \geq 0$. Suponha por absurdo que $k \neq 2^n$ para todo $n \geq 0$, então k deve ter algum fator ímpar $s > 1$ e $n = ts$ para algum $t \geq 1$. Note que

$$2^k + 1 = (2^t)^s + 1 = (2^t + 1)\left[(2^t)^{s-1} - (2^t)^{s-2} + ... - 2^t + 1\right],$$

como $0 < t < k$, então $2 < 2^t + 1 < 2^k + 1$. Com isso $2^k + 1$ tem um fator não trivial e portanto não é um número primo.

Definição

Seja p um número primo da forma $2^{2^n} + 1$, para algum $n \geq 0$, então p é dito ***primo de Fermat****.*

Primos de Fermat

Se $2^k + 1$ é um número primo, então $k = 2^n$ para algum $n \geq 0$. Suponha por absurdo que $k \neq 2^n$ para todo $n \geq 0$, então k deve ter algum fator ímpar $s > 1$ e $n = ts$ para algum $t \geq 1$. Note que

$$2^k + 1 = (2^t)^s + 1 = (2^t + 1)\left[(2^t)^{s-1} - (2^t)^{s-2} + ... - 2^t + 1\right],$$

como $0 < t < k$, então $2 < 2^t + 1 < 2^k + 1$. Com isso $2^k + 1$ tem um fator não trivial e portanto não é um número primo.

Definição

Seja p um número primo da forma $2^{2^n} + 1$, para algum $n \geq 0$, então p é dito ***primo de Fermat****.*

Exemplos: $3, 5, 17, 257$ e 65537.

Definição

*Seja $n \geq 1$, então dizemos que z é uma **raiz n-ésima da unidade** se z é uma raiz de $x^n - 1$.*

Denotemos $\mathbb{U}_n := \{z \mid z^n = 1\}$.

Definição

*Seja $n \geq 1$, então dizemos que z é uma **raiz n-ésima da unidade** se z é uma raiz de $x^n - 1$.*

Denotemos $\mathbb{U}_n := \{z \mid z^n = 1\}$. Note que $\mathbb{U}_4 := \{1, i, -1, -i\}$.

Definição

*Seja $n \geq 1$, então dizemos que z é uma **raiz n-ésima da unidade** se z é uma raiz de $x^n - 1$.*

Denotemos $\mathbb{U}_n := \{z \mid z^n = 1\}$. Note que $\mathbb{U}_4 := \{1, i, -1, -i\}$.

Seja $z \in \mathbb{U}_n$, então $1 = |z^n| = |z|^n$, logo $|z| = 1$.

Definição

*Seja $n \geq 1$, então dizemos que z é uma **raiz n-ésima da unidade** se z é uma raiz de $x^n - 1$.*

Denotemos $\mathbb{U}_n := \{z \mid z^n = 1\}$. Note que $\mathbb{U}_4 := \{1, i, -1, -i\}$.

Seja $z \in \mathbb{U}_n$, então $1 = |z^n| = |z|^n$, logo $|z| = 1$. Assim $z = cos(\theta) + isen(\theta)$, e ainda

$$1 = [cos(\theta) + isen(\theta)]^n = cos(n\theta) + isen(n\theta)$$

disso $n\theta = 2\pi k \Rightarrow \theta = \dfrac{2\pi k}{n}$, com $k \in \mathbb{Z}$.

Definição

*Seja $n \geq 1$, então dizemos que z é uma **raiz n-ésima da unidade** se z é uma raiz de $x^n - 1$.*

Denotemos $\mathbb{U}_n := \{z \mid z^n = 1\}$. Note que $\mathbb{U}_4 := \{1, i, -1, -i\}$.

Seja $z \in \mathbb{U}_n$, então $1 = |z^n| = |z|^n$, logo $|z| = 1$. Assim $z = cos(\theta) + isen(\theta)$, e ainda

$$1 = [cos(\theta) + isen(\theta)]^n = cos(n\theta) + isen(n\theta)$$

disso $n\theta = 2\pi k \Rightarrow \theta = \dfrac{2\pi k}{n}$, com $k \in \mathbb{Z}$. Como $sen(x)$ e $cos(x)$ são 2π periódicos:

$$z^n = 1 \Longleftrightarrow z = cos\left(\frac{2\pi k}{n}\right) + isen\left(\frac{2\pi k}{n}\right) = e^{\frac{2\pi k}{n}i},$$

com $k = 0, 1, ..., n-1$.

Seja $z \in \mathbb{U}_n$, então $z = e^{\frac{2\pi k}{n} i}$

Seja $z \in \mathbb{U}_n$, então $z = e^{\frac{2\pi k}{n} i} = \left(e^{\frac{2\pi}{n}}\right)^k$. Assim $\mathbb{U}_n = \left\{(\omega_n)^k \mid \omega_n = e^{\frac{2\pi}{n} i}\right\}$.

Seja $z \in \mathbb{U}_n$, então $z = e^{\frac{2\pi k}{n}i} = \left(e^{\frac{2\pi}{n}}\right)^k$. Assim $\mathbb{U}_n = \left\{(\omega_n)^k \mid \omega_n = e^{\frac{2\pi}{n}i}\right\}$.

- Seja $z = e^{\theta i} = cos(\theta) + isen(\theta)$,

Seja $z \in \mathbb{U}_n$, então $z = e^{\frac{2\pi k}{n}i} = \left(e^{\frac{2\pi}{n}}\right)^k$. Assim $\mathbb{U}_n = \left\{(\omega_n)^k \mid \omega_n = e^{\frac{2\pi}{n}i}\right\}$.

- Seja $z = e^{\theta i} = cos(\theta) + isen(\theta)$, então

$$\overline{z} = cos(\theta) - isen(\theta) = cos(-\theta) + isen(-\theta) = e^{-i\theta}.$$

Logo $z\overline{z} = 1$.

Seja $z \in \mathbb{U}_n$, então $z = e^{\frac{2\pi k}{n}i} = \left(e^{\frac{2\pi}{n}}\right)^k$. Assim $\mathbb{U}_n = \left\{(\omega_n)^k \mid \omega_n = e^{\frac{2\pi}{n}i}\right\}$.

- Seja $z = e^{\theta i} = cos(\theta) + isen(\theta)$, então

$$\overline{z} = cos(\theta) - isen(\theta) = cos(-\theta) + isen(-\theta) = e^{-i\theta}.$$

Logo $z\overline{z} = 1$.

Note que

$$\overline{e^{\frac{2\pi k}{n}i}} = e^{-\frac{2\pi k}{n}i} = e^{\frac{2\pi(n-k)}{n}i}.$$

Seja $z \in \mathbb{U}_n$, então $z = e^{\frac{2\pi k}{n}i} = \left(e^{\frac{2\pi}{n}}\right)^k$. Assim $\mathbb{U}_n = \left\{(\omega_n)^k \mid \omega_n = e^{\frac{2\pi}{n}i}\right\}$.

- Seja $z = e^{\theta i} = cos(\theta) + isen(\theta)$, então

$$\overline{z} = cos(\theta) - isen(\theta) = cos(-\theta) + isen(-\theta) = e^{-i\theta}.$$

Logo $z\overline{z} = 1$.

Note que

$$\overline{e^{\frac{2\pi k}{n}i}} = e^{-\frac{2\pi k}{n}i} = e^{\frac{2\pi(n-k)}{n}i}.$$

- Seja $z \in \mathbb{U}_n$, dizemos que z é uma **raiz n-ésima primitiva da unidade** se $z^k \neq 1$, para todo $1 < k < n$.

Seja γ uma raiz n-ésima primitiva da unidade, então $\mathbb{U}_n = \{\gamma^k \mid k = 0, 1, ..., n-1\}$.

Tome $\mathbb{U}_6 = \{1, e^{\frac{\pi}{3}i}, e^{\frac{2\pi}{3}i}, e^{\pi i}, e^{\frac{4\pi}{3}i}, e^{\frac{5\pi}{3}i}\}$, e $\mathbb{U}_3 = \{1, e^{\frac{2\pi}{3}i}, e^{\frac{4\pi}{3}i}\}$, logo $\mathbb{U}_3 \subseteq \mathbb{U}_6$.

Tome $\mathbb{U}_6 = \{1, e^{\frac{\pi}{3}i}, e^{\frac{2\pi}{3}i}, e^{\pi i}, e^{\frac{4\pi}{3}i}, e^{\frac{5\pi}{3}i}\}$, e $\mathbb{U}_3 = \{1, e^{\frac{2\pi}{3}i}, e^{\frac{4\pi}{3}i}\}$, logo $\mathbb{U}_3 \subseteq \mathbb{U}_6$. Como $\mathbb{U}_n$ são as raízes de $x^n - 1$, segue que $(x^3 - 1)|(x^6 - 1)$:

$$x^6 - 1 = (x^3 - 1)(x^3 + 1)$$

Tome $\mathbb{U}_6 = \{1, e^{\frac{\pi}{3}i}, e^{\frac{2\pi}{3}i}, e^{\pi i}, e^{\frac{4\pi}{3}i}, e^{\frac{5\pi}{3}i}\}$, e $\mathbb{U}_3 = \{1, e^{\frac{2\pi}{3}i}, e^{\frac{4\pi}{3}i}\}$, logo $\mathbb{U}_3 \subseteq \mathbb{U}_6$. Como $\mathbb{U}_n$ são as raízes de $x^n - 1$, segue que $(x^3 - 1)|(x^6 - 1)$:

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x^3 - 1)(x + 1)(x^2 - x + 1)$$

Tome $\mathbb{U}_6 = \{1, e^{\frac{\pi}{3}i}, e^{\frac{2\pi}{3}i}, e^{\pi i}, e^{\frac{4\pi}{3}i}, e^{\frac{5\pi}{3}i}\}$, e $\mathbb{U}_3 = \{1, e^{\frac{2\pi}{3}i}, e^{\frac{4\pi}{3}i}\}$, logo $\mathbb{U}_3 \subseteq \mathbb{U}_6$. Como $\mathbb{U}_n$ são as raízes de $x^n - 1$, segue que $(x^3 - 1)|(x^6 - 1)$:

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x^3 - 1)(x + 1)(x^2 - x + 1)$$

- $1, e^{\frac{2\pi}{3}i}$ e $e^{\frac{4\pi}{3}i}$ são as raízes de $(x^3 - 1)$,

Tome $\mathbb{U}_6 = \{1, e^{\frac{\pi}{3}i}, e^{\frac{2\pi}{3}i}, e^{\pi i}, e^{\frac{4\pi}{3}i}, e^{\frac{5\pi}{3}i}\}$, e $\mathbb{U}_3 = \{1, e^{\frac{2\pi}{3}i}, e^{\frac{4\pi}{3}i}\}$, logo $\mathbb{U}_3 \subseteq \mathbb{U}_6$. Como $\mathbb{U}_n$ são as raízes de $x^n - 1$, segue que $(x^3 - 1)|(x^6 - 1)$:

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x^3 - 1)(x + 1)(x^2 - x + 1)$$

- $1, e^{\frac{2\pi}{3}i}$ e $e^{\frac{4\pi}{3}i}$ são as raízes de $(x^3 - 1)$,
- $e^{\pi i} = -1$ é a raiz de $x + 1$ e

Tome $\mathbb{U}_6 = \{1, e^{\frac{\pi}{3}i}, e^{\frac{2\pi}{3}i}, e^{\pi i}, e^{\frac{4\pi}{3}i}, e^{\frac{5\pi}{3}i}\}$, e $\mathbb{U}_3 = \{1, e^{\frac{2\pi}{3}i}, e^{\frac{4\pi}{3}i}\}$, logo $\mathbb{U}_3 \subseteq \mathbb{U}_6$. Como $\mathbb{U}_n$ são as raízes de $x^n - 1$, segue que $(x^3 - 1)|(x^6 - 1)$:

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x^3 - 1)(x + 1)(x^2 - x + 1)$$

- $1, e^{\frac{2\pi}{3}i}$ e $e^{\frac{4\pi}{3}i}$ são as raízes de $(x^3 - 1)$,
- $e^{\pi i} = -1$ é a raiz de $x + 1$ e
- $e^{\frac{\pi}{3}i}$ e $e^{\frac{4\pi}{3}i}$ são as raízes de $x^2 - x + 1$, e também são as primitivas.

Tome $\mathbb{U}_6 = \{1, e^{\frac{\pi}{3}i}, e^{\frac{2\pi}{3}i}, e^{\pi i}, e^{\frac{4\pi}{3}i}, e^{\frac{5\pi}{3}i}\}$, e $\mathbb{U}_3 = \{1, e^{\frac{2\pi}{3}i}, e^{\frac{4\pi}{3}i}\}$, logo $\mathbb{U}_3 \subseteq \mathbb{U}_6$. Como $\mathbb{U}_n$ são as raízes de $x^n - 1$, segue que $(x^3 - 1)|(x^6 - 1)$:

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x^3 - 1)(x + 1)(x^2 - x + 1)$$

- $1, e^{\frac{2\pi}{3}i}$ e $e^{\frac{4\pi}{3}i}$ são as raízes de $(x^3 - 1)$,
- $e^{\pi i} = -1$ é a raiz de $x + 1$ e
- $e^{\frac{\pi}{3}i}$ e $e^{\frac{4\pi}{3}i}$ são as raízes de $x^2 - x + 1$, e também são as primitivas.

Para o caso $\mathbb{U}_5 = \{1, e^{\frac{2\pi}{5}i}, e^{\frac{4\pi}{5}i}, e^{\frac{6\pi}{5}i}, e^{\frac{8\pi}{5}i}\}$, temos

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1),$$

como $e^{\frac{2\pi}{5}i}, e^{\frac{4\pi}{5}i}, e^{\frac{6\pi}{5}i}, e^{\frac{8\pi}{5}i}$ são as raízes de $x^4 + x^3 + x^2 + x^1$, e este é irredutível, segue que $e^{\frac{2\pi k}{5}i}$, com $k = 1, 2, 3, 4$ são as raízes primitivas.

Tome $z \in \mathbb{U}_n$, então $z = e^{\frac{2\pi k}{n} i}$, suponha ainda que k e n tenham um fator $d > 1$ em comum. Então

$$\begin{cases} n = n'd, & \text{com } 1 \leq n' < n, \\ k = k'd, & \text{com } 1 \leq k' < k \end{cases}$$

Tome $z \in \mathbb{U}_n$, então $z = e^{\frac{2\pi k}{n} i}$, suponha ainda que k e n tenham um fator $d > 1$ em comum. Então

$$\begin{cases} n = n'd, & \text{com } 1 \leq n' < n, \\ k = k'd, & \text{com } 1 \leq k' < k \end{cases}$$

logo $z^{\frac{2\pi k}{n} i} = e^{\frac{2\pi k'}{n'} i}$ e $z^{n'} = e^{n' \frac{2\pi k'}{n'} i} = 1$. Por fim z não é uma raiz n-ésima primitiva da unidade.

Tome $z \in \mathbb{U}_n$, então $z = e^{\frac{2\pi k}{n} i}$, suponha ainda que k e n tenham um fator $d > 1$ em comum. Então

$$\begin{cases} n = n'd, & \text{com } 1 \leq n' < n, \\ k = k'd, & \text{com } 1 \leq k' < k \end{cases}$$

logo $z^{\frac{2\pi k}{n} i} = e^{\frac{2\pi k'}{n'} i}$ e $z^{n'} = e^{n' \frac{2\pi k'}{n'} i} = 1$. Por fim z não é uma raiz n-ésima primitiva da unidade.

Proposição

Seja $z = e^{\frac{2\pi k}{n} i} \in \mathbb{U}_n$, então z é uma raiz n-ésima primitiva da unidade se, e somente se, k e n não compartilharem fatores ≥ 1, ou seja, $mdc(k, n) = 1$.

Definição

*Para $n \geq 1$, definimos o n-ésimo **polinômio ciclotômico**, $\Phi_n(x)$, como*

$$\Phi_n(x) = \prod_{\substack{1 \leq k < n \\ mdc(k,n)=1}} \left(x - e^{\frac{2\pi k}{n} i}\right)$$

- $\Phi_1(x) = x - 1$,

Definição

*Para $n \geq 1$, definimos o n-ésimo **polinômio ciclotômico**, $\Phi_n(x)$, como*

$$\Phi_n(x) = \prod_{\substack{1 \leq k < n \\ mdc(k,n)=1}} \left(x - e^{\frac{2\pi k}{n} i}\right)$$

- $\Phi_1(x) = x - 1$,
- $\Phi_2(x) = x + 1$,

Definição

*Para $n \geq 1$, definimos o n-ésimo **polinômio ciclotômico**, $\Phi_n(x)$, como*

$$\Phi_n(x) = \prod_{\substack{1 \leq k < n \\ mdc(k,n)=1}} \left(x - e^{\frac{2\pi k}{n} i}\right)$$

- $\Phi_1(x) = x - 1$,
- $\Phi_2(x) = x + 1$,
- $\Phi_3(x) = (x - e^{\frac{2\pi}{3} i})(x - e^{\frac{4\pi}{3} i}) = x^2 + x + 1$,

Definição

*Para $n \geq 1$, definimos o n-ésimo **polinômio ciclotômico**, $\Phi_n(x)$, como*

$$\Phi_n(x) = \prod_{\substack{1 \leq k < n \\ mdc(k,n)=1}} \left(x - e^{\frac{2\pi k}{n} i}\right)$$

- $\Phi_1(x) = x - 1$,
- $\Phi_2(x) = x + 1$,
- $\Phi_3(x) = (x - e^{\frac{2\pi}{3} i})(x - e^{\frac{4\pi}{3} i}) = x^2 + x + 1$,
- $\Phi_4(x) = (x - e^{\frac{2\pi}{4} i})(x - e^{\frac{6\pi}{4} i}) = x^2 + 1$,

Definição

*Para $n \geq 1$, definimos o n-ésimo **polinômio ciclotômico**, $\Phi_n(x)$, como*

$$\Phi_n(x) = \prod_{\substack{1 \leq k < n \\ mdc(k,n)=1}} \left(x - e^{\frac{2\pi k}{n} i}\right)$$

- $\Phi_1(x) = x - 1$,
- $\Phi_2(x) = x + 1$,
- $\Phi_3(x) = (x - e^{\frac{2\pi}{3} i})(x - e^{\frac{4\pi}{3} i}) = x^2 + x + 1$,
- $\Phi_4(x) = (x - e^{\frac{2\pi}{4} i})(x - e^{\frac{6\pi}{4} i}) = x^2 + 1$,
- se p é primo, então $\Phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1$.

$$x^6 - 1 =$$
$$= (x-1)(x - e^{\frac{\pi}{3}i})(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i})(x - e^{\frac{5\pi}{3}i})$$

$$x^6 - 1 =$$
$$= (x-1)(x - e^{\frac{\pi}{3}i})(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i})(x - e^{\frac{5\pi}{3}i})$$
$$= \Phi_6(x)(x-1)(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i})$$

$$
\begin{aligned}
x^6 - 1 &= \\
&= (x-1)(x - e^{\frac{\pi}{3}i})(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i})(x - e^{\frac{5\pi}{3}i}) \\
&= \Phi_6(x)(x-1)(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i}) \\
&= \Phi_6(x)\Phi_3(x)(x-1)(x+1)
\end{aligned}
$$

$$
\begin{aligned}
x^6 - 1 &= \\
&= (x-1)(x - e^{\frac{\pi}{3}i})(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i})(x - e^{\frac{5\pi}{3}i}) \\
&= \Phi_6(x)(x-1)(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i}) \\
&= \Phi_6(x)\Phi_3(x)(x-1)(x+1) \\
&= \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x).
\end{aligned}
$$

$$
\begin{aligned}
x^6 - 1 &= \\
&= (x-1)(x - e^{\frac{\pi}{3}i})(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i})(x - e^{\frac{5\pi}{3}i}) \\
&= \Phi_6(x)(x-1)(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i}) \\
&= \Phi_6(x)\Phi_3(x)(x-1)(x+1) \\
&= \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x).
\end{aligned}
$$

- $x^n - 1 = \prod_{0<d|n} \Phi_d(x).$

$$
\begin{aligned}
x^6 - 1 &= \\
&= (x-1)(x - e^{\frac{\pi}{3}i})(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i})(x - e^{\frac{5\pi}{3}i}) \\
&= \Phi_6(x)(x-1)(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i}) \\
&= \Phi_6(x)\Phi_3(x)(x-1)(x+1) \\
&= \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x).
\end{aligned}
$$

- $x^n - 1 = \prod_{0<d|n} \Phi_d(x).$

Segue por indução que $\Phi_n(x) \in \mathbb{Z}[x]$.

$$
\begin{aligned}
x^6 - 1 = & \\
&= (x-1)(x - e^{\frac{\pi}{3}i})(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i})(x - e^{\frac{5\pi}{3}i}) \\
&= \Phi_6(x)(x-1)(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i}) \\
&= \Phi_6(x)\Phi_3(x)(x-1)(x+1) \\
&= \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x).
\end{aligned}
$$

- $x^n - 1 = \prod_{0<d|n} \Phi_d(x).$

Segue por indução que $\Phi_n(x) \in \mathbb{Z}[x]$. $\Phi_1(x) = x - 1$,

$$
\begin{aligned}
x^6 - 1 &= \\
&= (x-1)(x - e^{\frac{\pi}{3}i})(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i})(x - e^{\frac{5\pi}{3}i}) \\
&= \Phi_6(x)(x-1)(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i}) \\
&= \Phi_6(x)\Phi_3(x)(x-1)(x+1) \\
&= \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x).
\end{aligned}
$$

- $x^n - 1 = \prod_{0<d|n} \Phi_d(x).$

Segue por indução que $\Phi_n(x) \in \mathbb{Z}[x]$. $\Phi_1(x) = x - 1$,

$$x^n - 1 = \Phi_n(x) \prod_{\substack{0<d<n-1 \\ d|n}} \Phi_d(x),$$

por hipótese de indução $\Phi_d(x) \in \mathbb{Z}[x]$ e $x^n - 1 \in \mathbb{Z}[x]$,

$$
\begin{aligned}
x^6 - 1 &= \\
&= (x-1)(x - e^{\frac{\pi}{3}i})(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i})(x - e^{\frac{5\pi}{3}i}) \\
&= \Phi_6(x)(x-1)(x - e^{\frac{2\pi}{3}i})(x - e^{\pi i})(x - e^{\frac{4\pi}{3}i}) \\
&= \Phi_6(x)\Phi_3(x)(x-1)(x+1) \\
&= \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x).
\end{aligned}
$$

- $x^n - 1 = \prod_{0<d|n} \Phi_d(x).$

Segue por indução que $\Phi_n(x) \in \mathbb{Z}[x]$. $\Phi_1(x) = x - 1$,

$$x^n - 1 = \Phi_n(x) \prod_{\substack{0<d<n-1 \\ d|n}} \Phi_d(x),$$

por hipótese de indução $\Phi_d(x) \in \mathbb{Z}[x]$ e $x^n - 1 \in \mathbb{Z}[x]$, logo $\Phi_n(x) \in \mathbb{Z}[x]$.

Teorema

Seja $n \geq 1$, então $\Phi_n(x)$ é um polinômio irredutível sobre $\mathbb{Q}[x]$.

Teorema

Seja $n \geq 1$, então $\Phi_n(x)$ é um polinômio irredutível sobre $\mathbb{Q}[x]$.

Sabemos que $\partial\left(\Phi_n(x)\right) = \#\{1 \leq k \leq n \mid mdc(k,n) = 1\}$. Então vamos definir a seguinte função:

$$\varphi : \mathbb{N} \to \mathbb{N}, \varphi(n) = \#\{1 \leq k \leq n \mid mdc(k,n) = 1\}.$$

- $\varphi(p) = p - 1$, para p um número primo.

Teorema

Seja $n \geq 1$, então $\Phi_n(x)$ é um polinômio irredutível sobre $\mathbb{Q}[x]$.

Sabemos que $\partial\left(\Phi_n(x)\right) = \#\{1 \leq k \leq n \mid mdc(k,n) = 1\}$. Então vamos definir a seguinte função:

$$\varphi : \mathbb{N} \to \mathbb{N}, \varphi(n) = \#\{1 \leq k \leq n \mid mdc(k,n) = 1\}.$$

- $\varphi(p) = p - 1$, para p um número primo.
- $\varphi(p^s) = p^{s-1}(p-1)$, para p primo.

Teorema

Seja $n \geq 1$, então $\Phi_n(x)$ é um polinômio irredutível sobre $\mathbb{Q}[x]$.

Sabemos que $\partial\left(\Phi_n(x)\right) = \#\{1 \leq k \leq n \mid mdc(k,n) = 1\}$. Então vamos definir a seguinte função:

$$\varphi : \mathbb{N} \to \mathbb{N}, \varphi(n) = \#\{1 \leq k \leq n \mid mdc(k,n) = 1\}.$$

- $\varphi(p) = p - 1$, para p um número primo.
- $\varphi(p^s) = p^{s-1}(p-1)$, para p primo.
- $\varphi(mn) = \varphi(m)\varphi(n)$.

- $n \in \mathbb{N}$, $\varphi(n)$ é uma potência de 2 se, e só se, $n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

- $n \in \mathbb{N}$, $\varphi(n)$ é uma potência de 2 se, e só se, $n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

Se $n = \prod_{s=1}^{m} p_s^{t_s}$, então $\varphi(n) = \prod_{s=1}^{m} \varphi(p_s^{t_s})$. Logo $\varphi(n)$ é uma potência de dois se, e só se, $\varphi(p^f)$ é uma potência de 2 para todo primo p e $f \in \mathbb{N}$, tal que $p^f | n$.

- $n \in \mathbb{N}$, $\varphi(n)$ é uma potência de 2 se, e só se, $n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

Se $n = \prod_{s=1}^{m} p_s^{t_s}$, então $\varphi(n) = \prod_{s=1}^{m} \varphi(p_s^{t_s})$. Logo $\varphi(n)$ é uma potência de dois se, e só se, $\varphi(p^f)$ é uma potência de 2 para todo primo p e $f \in \mathbb{N}$, tal que $p^f | n$. Reescrevendo a afirmação

- Dados p um primo e $f \in \mathbb{N}$, então $\varphi(p^f)$ é uma potência de 2 se, e só se, $p = 2$ ou p é um primo de Fermat e $f = 1$.

- $n \in \mathbb{N}$, $\varphi(n)$ é uma potência de 2 se, e só se, $n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

Se $n = \prod_{s=1}^{m} p_s^{t_s}$, então $\varphi(n) = \prod_{s=1}^{m} \varphi(p_s^{t_s})$. Logo $\varphi(n)$ é uma potência de dois se, e só se, $\varphi(p^f)$ é uma potência de 2 para todo primo p e $f \in \mathbb{N}$, tal que $p^f | n$. Reescrevendo a afirmação

- Dados p um primo e $f \in \mathbb{N}$, então $\varphi(p^f)$ é uma potência de 2 se, e só se, $p = 2$ ou p é um primo de Fermat e $f = 1$.

Assuma que $\varphi(p^f)$ é potência de 2.

- $n \in \mathbb{N}$, $\varphi(n)$ é uma potência de 2 se, e só se, $n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

Se $n = \prod_{s=1}^{m} p_s^{t_s}$, então $\varphi(n) = \prod_{s=1}^{m} \varphi(p_s^{t_s})$. Logo $\varphi(n)$ é uma potência de dois se, e só se, $\varphi(p^f)$ é uma potência de 2 para todo primo p e $f \in \mathbb{N}$, tal que $p^f | n$. Reescrevendo a afirmação

- Dados p um primo e $f \in \mathbb{N}$, então $\varphi(p^f)$ é uma potência de 2 se, e só se, $p = 2$ ou p é um primo de Fermat e $f = 1$.

Assuma que $\varphi(p^f)$ é potência de 2. Se $p = 2$, não há nada a fazer. Se p é ímpar, então $\varphi(p^f) = 2^m$, mas $\varphi(p^f) = p^{f-1}(p-1)$, então é necessário que $f = 1$.

- $n \in \mathbb{N}$, $\varphi(n)$ é uma potência de 2 se, e só se, $n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

Se $n = \prod_{s=1}^{m} p_s^{t_s}$, então $\varphi(n) = \prod_{s=1}^{m} \varphi(p_s^{t_s})$. Logo $\varphi(n)$ é uma potência de dois se, e só se, $\varphi(p^f)$ é uma potência de 2 para todo primo p e $f \in \mathbb{N}$, tal que $p^f | n$. Reescrevendo a afirmação

- Dados p um primo e $f \in \mathbb{N}$, então $\varphi(p^f)$ é uma potência de 2 se, e só se, $p = 2$ ou p é um primo de Fermat e $f = 1$.

Assuma que $\varphi(p^f)$ é potência de 2. Se $p = 2$, não há nada a fazer. Se p é ímpar, então $\varphi(p^f) = 2^m$, mas $\varphi(p^f) = p^{f-1}(p-1)$, então é necessário que $f = 1$. Logo $2^m = \varphi(p) = p - 1$, assim p é um primo de Fermat.

Assuma que $p = 2$ ou p é um primo de Fermat e $f = 1$.

Assuma que $p = 2$ ou p é um primo de Fermat e $f = 1$. Se $p = 2$, então $\varphi(2^f) = 2^{f-1}$ que é uma potência de 2. Se p é um primo de Fermat, então $p = 2^{2^j} + 1$ e $\varphi(p) = p - 1 = 2^{2^j}$ que é uma potência de 2.

Assuma que $p = 2$ ou p é um primo de Fermat e $f = 1$. Se $p = 2$, então $\varphi(2^f) = 2^{f-1}$ que é uma potência de 2. Se p é um primo de Fermat, então $p = 2^{2^j} + 1$ e $\varphi(p) = p - 1 = 2^{2^j}$ que é uma potência de 2.
Concluímos dessa forma que se $\varphi(n)$ é uma potência de 2, então $n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

Assuma que $p = 2$ ou p é um primo de Fermat e $f = 1$. Se $p = 2$, então $\varphi(2^f) = 2^{f-1}$ que é uma potência de 2. Se p é um primo de Fermat, então $p = 2^{2^j} + 1$ e $\varphi(p) = p - 1 = 2^{2^j}$ que é uma potência de 2.
Concluímos dessa forma que se $\varphi(n)$ é uma potência de 2, então $n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

- O polígono regular de n lados é construtível
- $\Rightarrow e^{\frac{2\pi}{n}i}$ é construtível

Assuma que $p = 2$ ou p é um primo de Fermat e $f = 1$. Se $p = 2$, então $\varphi(2^f) = 2^{f-1}$ que é uma potência de 2. Se p é um primo de Fermat, então $p = 2^{2^j} + 1$ e $\varphi(p) = p - 1 = 2^{2^j}$ que é uma potência de 2.
Concluímos dessa forma que se $\varphi(n)$ é uma potência de 2, então $n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

- O polígono regular de n lados é construtível
- $\Rightarrow e^{\frac{2\pi}{n}i}$ é construtível
- $\Rightarrow \partial(\Phi_n(x)) = \varphi(n)$ é uma potência de 2

Assuma que $p = 2$ ou p é um primo de Fermat e $f = 1$. Se $p = 2$, então $\varphi(2^f) = 2^{f-1}$ que é uma potência de 2. Se p é um primo de Fermat, então $p = 2^{2^j} + 1$ e $\varphi(p) = p - 1 = 2^{2^j}$ que é uma potência de 2.
Concluímos dessa forma que se $\varphi(n)$ é uma potência de 2, então $n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

- O polígono regular de n lados é construtível
- $\Rightarrow e^{\frac{2\pi}{n} i}$ é construtível
- $\Rightarrow \partial(\Phi_n(x)) = \varphi(n)$ é uma potência de 2
- $\Rightarrow n = 2^k p_1 p_2 ... p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, ..., j$.

Teorema (Teorema de Gauss-Wantzel)

O polígono regular de n lados é construtível se, e somente se, $n = 2^k p_1 p_2 \cdot \ldots \cdot p_j$, onde $k \geq 0$ e p_l são primos distintos de Fermat, para $l = 1, \ldots, j$

Exemplos

O polígono regular de n lados é construtível para:

Exemplos

O polígono regular de n lados é construtível para:

- $n = 3$,
- $n = 4 = 2^4$,
- $n = 5$,
- $n = 6 = 2 \cdot 3$,
- $n = 8 = 2^3$,
- $n = 10 = 2 \cdot 5$,
- $n = 12 = 2^2 \cdot 3$,
- $n = 15 = 3 \cdot 5$,
- $n = 16 = 2^4$,
- $n = 17$,
- $n = 20 = 2^2 \cdot 5$,

Construção do Heptadecágono

Como sabemos para construir o polígono regular de 17 lados precisamos construir $\omega = e^{\frac{2\pi}{17}i}$.

Construção do Heptadecágono

Como sabemos para construir o polígono regular de 17 lados precisamos construir $\omega = e^{\frac{2\pi}{17}i}$. Sabemos que $\mathbb{U}_{17} = \{\omega^k \mid 0 \leq k < 17\}$, mais ainda $\{\omega^k\}_{k\geq 1}$ são as raízes primitivas e têm por polinômio minimal $\Phi_{17}(x) = x^{16} + x^{15} + ... + x + 1$.

Construção do Heptadecágono

Como sabemos para construir o polígono regular de 17 lados precisamos construir $\omega = e^{\frac{2\pi}{17}i}$. Sabemos que $\mathbb{U}_{17} = \{\omega^k \mid 0 \leq k < 17\}$, mais ainda $\{\omega^k\}_{k\geq 1}$ são as raízes primitivas e têm por polinômio minimal $\Phi_{17}(x) = x^{16} + x^{15} + ... + x + 1$. Ordene as raízes primitivas dessa forma:

$$\omega, \omega^3, \omega^9, \omega^{10}, \omega^{13}, \omega^5, \omega^{15}, \omega^{11}, \omega^{16}, \omega^{14}, \omega^8, \omega^7, \omega^4, \omega^{12}, \omega^2, \omega^6.$$

Construção do Heptadecágono

Como sabemos para construir o polígono regular de 17 lados precisamos construir $\omega = e^{\frac{2\pi}{17}i}$. Sabemos que $\mathbb{U}_{17} = \{\omega^k \mid 0 \leq k < 17\}$, mais ainda $\{\omega^k\}_{k\geq 1}$ são as raízes primitivas e têm por polinômio minimal $\Phi_{17}(x) = x^{16} + x^{15} + ... + x + 1$. Ordene as raízes primitivas dessa forma:

$$\omega, \omega^3, \omega^9, \omega^{10}, \omega^{13}, \omega^5, \omega^{15}, \omega^{11}, \omega^{16}, \omega^{14}, \omega^8, \omega^7, \omega^4, \omega^{12}, \omega^2, \omega^6.$$

Tome os número complexos

$$y_1 = \omega + \omega^9 + \omega^{13} + \omega^{15} + \omega^{16} + \omega^8 + \omega^4 + \omega^2,$$

$$y_2 = \omega^3 + \omega^{10} + \omega^5 + \omega^{11} + \omega^{14} + \omega^7 + \omega^{12} + \omega^6.$$

Construção do Heptadecágono

É possível mostrar que $y_1 + y_2 = -1$ e $y_1 y_2 = 4(y_1 + y_2) = -4$.

Construção do Heptadecágono

É possível mostrar que $y_1 + y_2 = -1$ e $y_1 y_2 = 4(y_1 + y_2) = -4$.
Logo y_1 e y_2 são raízes do polinômio

$$y^2 + y - 4 = 0$$

Construção do Heptadecágono

É possível mostrar que $y_1 + y_2 = -1$ e $y_1 y_2 = 4(y_1 + y_2) = -4$.
Logo y_1 e y_2 são raízes do polinômio

$$y^2 + y - 4 = 0$$

Avaliando suas raízes, podemos concluir que

$$y_1 = \frac{-1 + \sqrt{17}}{2} \quad \text{e} \quad y_2 = \frac{-1 - \sqrt{17}}{2}.$$

Tome os números complexos:

$$\begin{array}{rcccl}
x_1 & = & \omega + \omega^{13} + \omega^{16} + \omega^4 & = & 2\left(cos\left(2\pi/17\right) + cos\left(4(2\pi/17)\right)\right) \\
x_2 & = & \omega^9 + \omega^{15} + \omega^8 + \omega^2 & = & 2\left(cos\left(2(2\pi/17)\right) + cos\left(8(2\pi/17)\right)\right) \\
x_3 & = & \omega^3 + \omega^5 + \omega^{14} + \omega^{12} & = & 2\left(cos\left(3(2\pi/17)\right) + cos\left(5(2\pi/17)\right)\right) \\
x_4 & = & \omega^{10} + \omega^{11} + \omega^7 + \omega^6 & = & 2\left(cos\left(6(2\pi/17)\right) + cos\left(7(2\pi/17)\right)\right)
\end{array}$$

Construção do Heptadecágono

Verifica-se que $x_1 > x_2$ e são raízes de $x^2 - y_1 x - 1 = 0$; enquanto $x_3 > x_4$ e são raízes de $x^2 - y_2 x - 1$.

Construção do Heptadecágono

Verifica-se que $x_1 > x_2$ e são raízes de $x^2 - y_1 x - 1 = 0$; enquanto $x_3 > x_4$ e são raízes de $x^2 - y_2 x - 1$. Assim, concluímos

$$x_1 = \frac{-1+\sqrt{17}}{4} + \frac{\sqrt{34-2\sqrt{17}}}{4}, \quad x_2 = \frac{-1+\sqrt{17}}{4} - \frac{\sqrt{34-2\sqrt{17}}}{4}$$

$$x_3 = \frac{-1-\sqrt{17}}{4} + \frac{\sqrt{34+2\sqrt{17}}}{4}, \quad x_4 = \frac{-1-\sqrt{17}}{4} - \frac{\sqrt{34+2\sqrt{17}}}{4}.$$

Tomando agora os números complexos

$$z_1 = \omega + \omega^{16} = 2cos\left(\frac{2\pi}{17}\right)$$

$$z_2 = \omega^{13} + \omega^4 = 2cos\left(4\frac{2\pi}{17}\right)$$

Construção do Heptadecágono

Como $z_1 > z_2$ e ambos são raízes de $z^2 - x_1 z + x_3 = 0$.

Construção do Heptadecágono

Como $z_1 > z_2$ e ambos são raízes de $z^2 - x_1 z + x_3 = 0$. Então

$$cos\left(\frac{2\pi}{17}\right) = \frac{x_1}{2} = \frac{x_1 + \sqrt{x_1^2 - 4x_3}}{4}.$$

Construção do Heptadecágono

Como $z_1 > z_2$ e ambos são raízes de $z^2 - x_1 z + x_3 = 0$. Então

$$cos\left(\frac{2\pi}{17}\right) = \frac{x_1}{2} = \frac{x_1 + \sqrt{x_1^2 - 4x_3}}{4}.$$

Logo

$$cos\left(\frac{2\pi}{17}\right) = \frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}}{16} + \frac{\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}}{8}$$

A ideia da recíproca do teorema de Gauss-Wantzel, segue de outro teorema de Gauss

Teorema (Gauss, *Disquistiones Arithmeticae*-1821)

Seja p um primo de Fermat, então o polígono regular de p lados é construtível com régua e compasso.

A ideia da recíproca do teorema de Gauss-Wantzel, segue de outro teorema de Gauss

Teorema (Gauss, *Disquistiones Arithmeticae*-1821)

Seja p um primo de Fermat, então o polígono regular de p lados é construtível com régua e compasso.

Sejam p_1 e p_2 dois primos distintos de Fermat, tome os números complexos $z_1 = e^{\frac{2\pi}{p_1}i}$ e $z_2 = e^{\frac{2\pi}{p_2}i}$. Note que

$$z_1 z_2 = e^{(p_1+p_2)\frac{2\pi}{p_1 p_2}i},$$

mas $mdc(p_1p_2, p_1 + p_2) = 1$,

A ideia da recíproca do teorema de Gauss-Wantzel, segue de outro teorema de Gauss

Teorema (Gauss, *Disquistiones Arithmeticae*-1821)

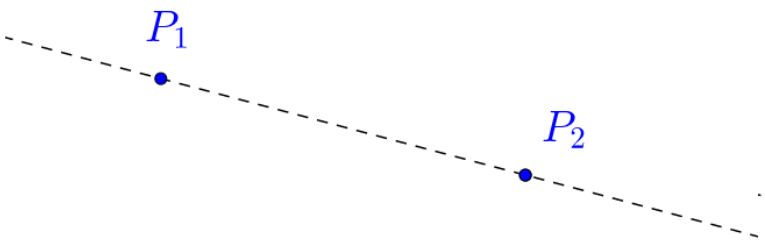
Seja p um primo de Fermat, então o polígono regular de p lados é construtível com régua e compasso.

Sejam p_1 e p_2 dois primos distintos de Fermat, tome os números complexos $z_1 = e^{\frac{2\pi}{p_1}i}$ e $z_2 = e^{\frac{2\pi}{p_2}i}$. Note que

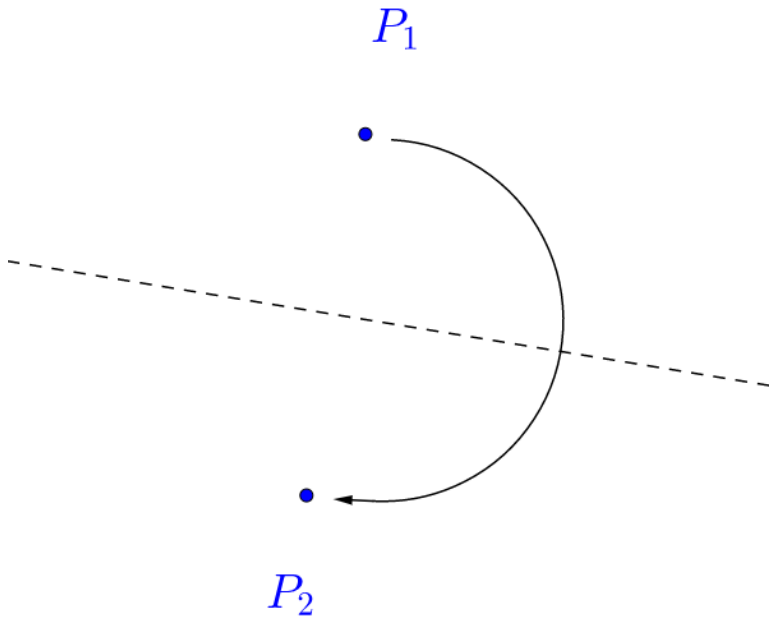
$$z_1 z_2 = e^{(p_1+p_2)\frac{2\pi}{p_1 p_2}i},$$

mas $mdc(p_1p_2, p_1 + p_2) = 1$, logo z_1z_2 é uma raiz p_1p_2-ésima primitiva da unidade e $\mathbb{U}_{p_1p_2} = \{(z_1z_2)^k \mid 0 \leq k < p_1p_2\}$.

Axiomas

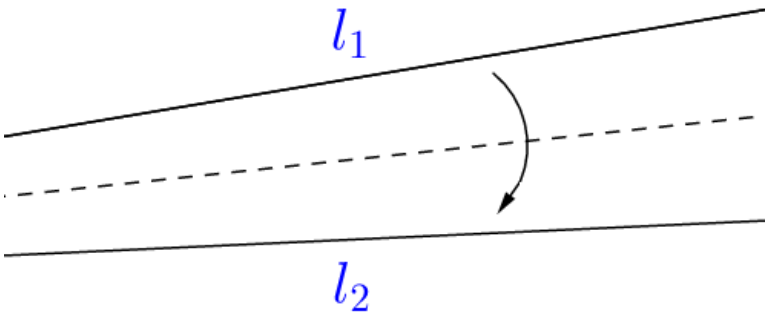


(O_1) Dados dois pontos P_1 e P_2, podemos dobrar uma linha que passa pelos dois pontos.

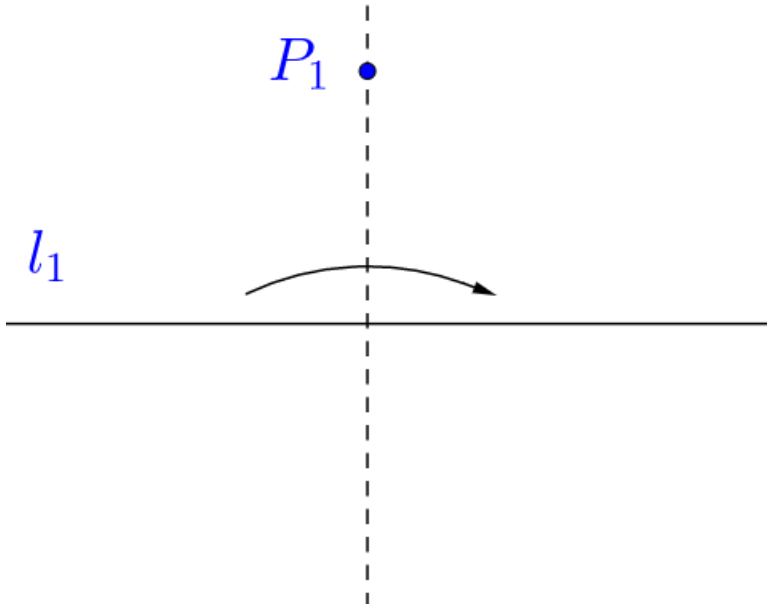


(O_2) Dados dois pontos P_1 e P_2, podemos dobrar P_1 em P_2.

Axiomas

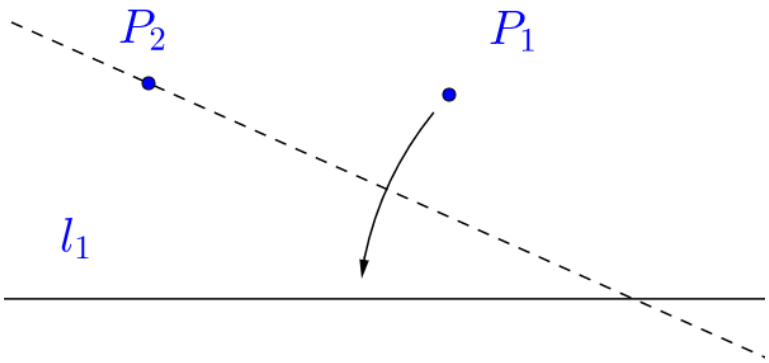


(O_3) Dadas duas linhas l_1 e l_2 podemos dobrar a linha l_1 na linha l_2

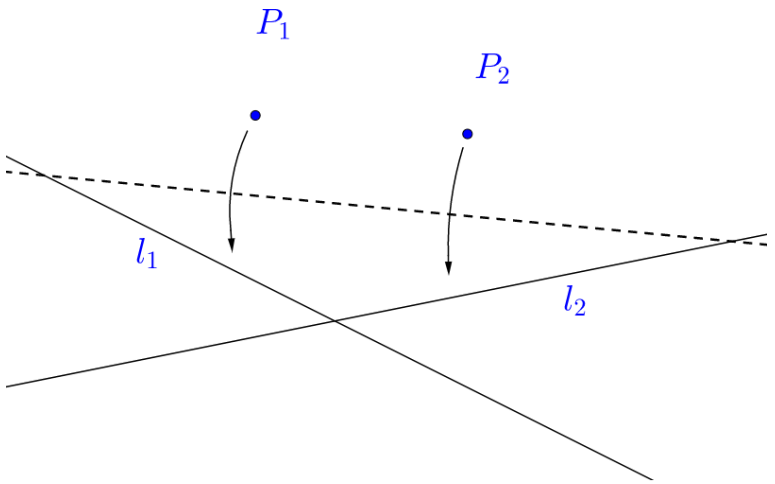


(O_4) Dados um ponto P_1 e uma linha l_1, podemos fazer uma dobra perpendicular à l_1 que passa por P_1.

Axiomas



(O_5) Dados dois pontos P_1 e P_2 e uma linha l_1, podemos fazer uma dobra que coloca P_1 em l_1 e que passa pelo ponto P_2.



(O_6) Dados dois pontos P_1 e P_2 e duas linhas l_1 e l_2, podemos fazer uma dobra que coloca P_1 em l_1 e P_2 em l_2.

Primeiro, vamos construir os eixos real e imaginário, depois marcamos i.

Primeiro, vamos construir os eixos real e imaginário, depois marcamos i.

- $\mathbb{Z}[i] = \{n + im \mid n, m \in \mathbb{Z}\}$ são construtíveis via origami.

Primeiro, vamos construir os eixos real e imaginário, depois marcamos i.

- $\mathbb{Z}[i] = \{n + im \mid n, m \in \mathbb{Z}\}$ são construtíveis via origami.
- $1/n$, para $n \in \mathbb{Z}$ são construtíveis via origami.

Primeiro, vamos construir os eixos real e imaginário, depois marcamos i.

- $\mathbb{Z}[i] = \{n + im \mid n, m \in \mathbb{Z}\}$ são construtíveis via origami.
- $1/n$, para $n \in \mathbb{Z}$ são construtíveis via origami.
- Se $a, b \in \mathbb{R}$ são construtíveis via origami, então ab e abi também são.

Primeiro, vamos construir os eixos real e imaginário, depois marcamos i.

- $\mathbb{Z}[i] = \{n + im \mid n, m \in \mathbb{Z}\}$ são construtíveis via origami.
- $1/n$, para $n \in \mathbb{Z}$ são construtíveis via origami.
- Se $a, b \in \mathbb{R}$ são construtíveis via origami, então ab e abi também são.
- Denotemos $\mathbb{O}$ os números complexos construtíveis via origami, vimos que $\mathbb{O}$ é um subcorpo dos complexos e $\mathbb{O}|\mathbb{Q}$.

Primeiro, vamos construir os eixos real e imaginário, depois marcamos i.

- $\mathbb{Z}[i] = \{n + im \mid n, m \in \mathbb{Z}\}$ são construtíveis via origami.
- $1/n$, para $n \in \mathbb{Z}$ são construtíveis via origami.
- Se $a, b \in \mathbb{R}$ são construtíveis via origami, então ab e abi também são.
- Denotemos $\mathbb{O}$ os números complexos construtíveis via origami, vimos que $\mathbb{O}$ é um subcorpo dos complexos e $\mathbb{O}|\mathbb{Q}$.
- Da mesma forma que para $\mathcal{C}$, temos que se um número real $a \in \mathbb{O}$, então $\sqrt{r} \in \mathbb{O}$.

Considere os pontos $F_1 = (a, 1)$ e $F_2 = (b, c)$, com $c \neq 0$. Tome ainda as retas $r_1 : y = -1$ e $r_2 : x = -c$. Quando aplicamos o sexto axioma (O_6), sabemos que estamos construindo uma reta l que é tangente simultaneamente as seguintes parábolas:

$$\begin{cases} \pi_1 : (x-a)^2 &= 4y, \\ \pi_2 : (y-b)^2 &= 4cx \end{cases}$$

Considere os pontos $F_1 = (a, 1)$ e $F_2 = (b, c)$, com $c \neq 0$. Tome ainda as retas $r_1 : y = -1$ e $r_2 : x = -c$. Quando aplicamos o sexto axioma (O_6), sabemos que estamos construindo uma reta l que é tangente simultaneamente as seguintes parábolas:

$$\begin{cases} \pi_1 : (x-a)^2 &= 4y, \\ \pi_2 : (y-b)^2 &= 4cx \end{cases}$$

Se l é tangente à π_1, no ponto (x_1, y_1), então o coeficiente angular de l é $m = \frac{x_1 - a}{2}$. Por outro lado, se l é tangente à π_2, no ponto (x_2, y_2), então $m = \frac{2c}{y_2 - b}$.

Considere os pontos $F_1 = (a, 1)$ e $F_2 = (b, c)$, com $c \neq 0$. Tome ainda as retas $r_1 : y = -1$ e $r_2 : x = -c$. Quando aplicamos o sexto axioma (O_6), sabemos que estamos construindo uma reta l que é tangente simultaneamente as seguintes parábolas:

$$\begin{cases} \pi_1 : (x-a)^2 &= 4y, \\ \pi_2 : (y-b)^2 &= 4cx \end{cases}$$

Se l é tangente à π_1, no ponto (x_1, y_1), então o coeficiente angular de l é $m = \frac{x_1 - a}{2}$. Por outro lado, se l é tangente à π_2, no ponto (x_2, y_2), então $m = \frac{2c}{y_2 - b}$. Entretanto l passa por (x_1, y_1) e (x_2, y_2),

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Considere os pontos $F_1 = (a, 1)$ e $F_2 = (b, c)$, com $c \neq 0$. Tome ainda as retas $r_1 : y = -1$ e $r_2 : x = -c$. Quando aplicamos o sexto axioma (O_6), sabemos que estamos construindo uma reta l que é tangente simultaneamente as seguintes parábolas:

$$\begin{cases} \pi_1 : (x-a)^2 &= 4y, \\ \pi_2 : (y-b)^2 &= 4cx \end{cases}$$

Se l é tangente à π_1, no ponto (x_1, y_1), então o coeficiente angular de l é $m = \frac{x_1 - a}{2}$. Por outro lado, se l é tangente à π_2, no ponto (x_2, y_2), então $m = \frac{2c}{y_2 - b}$. Entretanto l passa por (x_1, y_1) e (x_2, y_2),

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{\frac{2c}{m} + b - m^2}{\frac{c}{m^2} - 2m - a} = \frac{2cm + bm^2 - m^4}{c - 2m^3 - am^2}$$

Considere os pontos $F_1 = (a, 1)$ e $F_2 = (b, c)$, com $c \neq 0$. Tome ainda as retas $r_1 : y = -1$ e $r_2 : x = -c$. Quando aplicamos o sexto axioma (O_6), sabemos que estamos construindo uma reta l que é tangente simultaneamente as seguintes parábolas:

$$\begin{cases} \pi_1 : (x-a)^2 &= 4y, \\ \pi_2 : (y-b)^2 &= 4cx \end{cases}$$

Se l é tangente à π_1, no ponto (x_1, y_1), então o coeficiente angular de l é $m = \frac{x_1 - a}{2}$. Por outro lado, se l é tangente à π_2, no ponto (x_2, y_2), então $m = \frac{2c}{y_2 - b}$. Entretanto l passa por (x_1, y_1) e (x_2, y_2),

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{\frac{2c}{m} + b - m^2}{\frac{c}{m^2} - 2m - a} = \frac{2cm + bm^2 - m^4}{c - 2m^3 - am^2}$$

$$\Rightarrow m^3 + am^2 + bm + c = 0.$$

- Logo se $x \in \mathbb{O} \cap \mathbb{R}$, então $\sqrt[3]{x} \in \mathbb{O}$.

- Logo se $x \in \mathbb{O} \cap \mathbb{R}$, então $\sqrt[3]{x} \in \mathbb{O}$.
- Seja $z = |z|(cos(\theta) + isen(\theta)) \in \mathbb{O}$, então

$$\sqrt[3]{z} = \sqrt[3]{|z|}\left(cos\left(\frac{\theta}{3}\right) + isen\left(\frac{\theta}{3}\right)\right) \in \mathbb{O}.$$

- Logo se $x \in \mathbb{O} \cap \mathbb{R}$, então $\sqrt[3]{x} \in \mathbb{O}$.
- Seja $z = |z|(cos(\theta) + isen(\theta)) \in \mathbb{O}$, então

$$\sqrt[3]{z} = \sqrt[3]{|z|}\left(cos\left(\frac{\theta}{3}\right) + isen\left(\frac{\theta}{3}\right)\right) \in \mathbb{O}.$$

Teorema

Um número complexo α pertence à $\mathbb{O}$ se, e somente se, existe uma sequência de subcorpos

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset ... \subset \mathbb{K}_{n-1} \subset \mathbb{K}_n \subseteq \mathbb{C}.$$

tal que $\alpha \in \mathbb{K}_n$ e $[\mathbb{K}_i : \mathbb{K}_{i-1}] = 2$ ou 3, para $1 \leq i \leq n$.

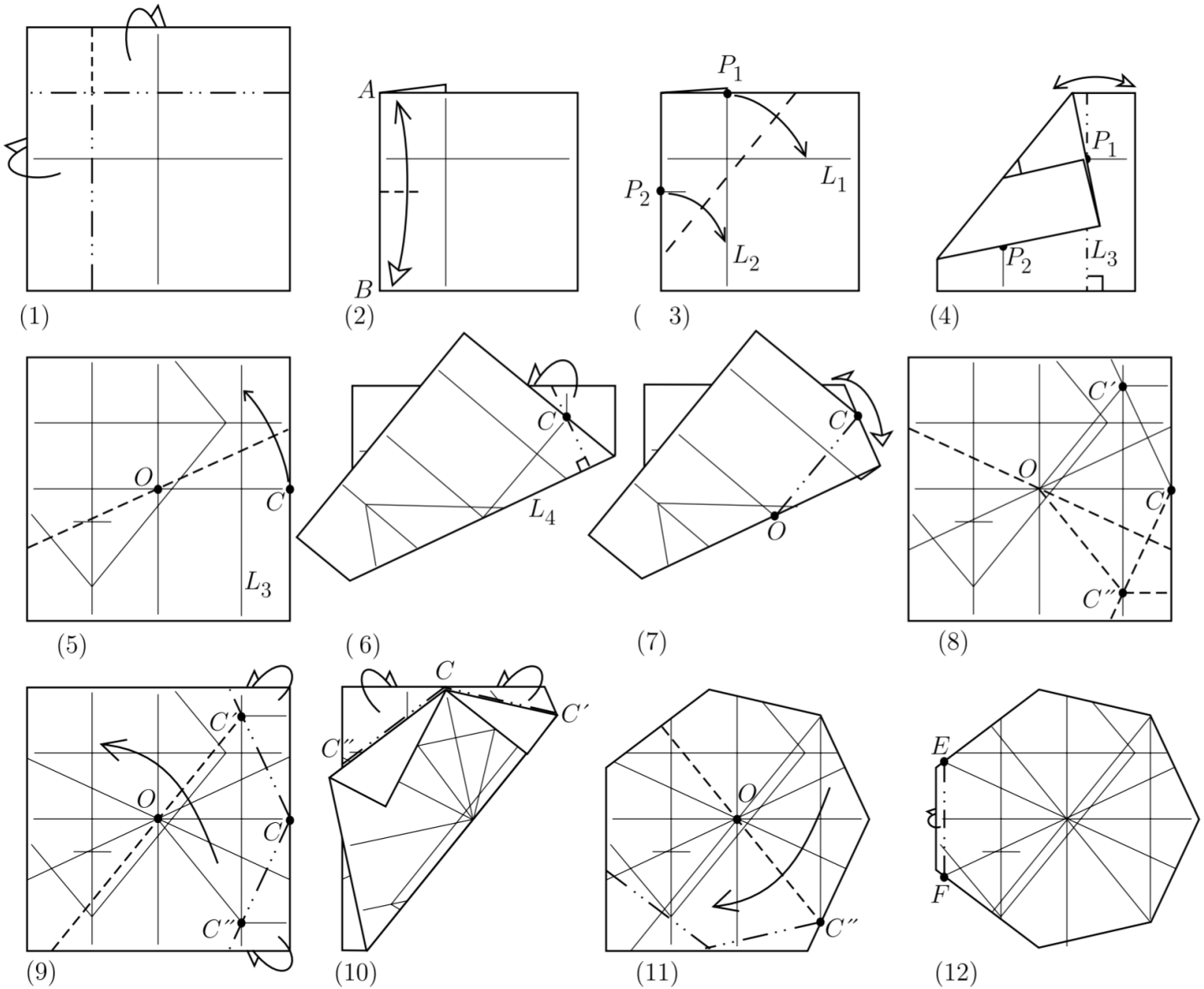
Teorema

O polígono regular de n lados é construtível via origami se, e somente se, $n = 2^a 3^b p_1 p_2 ... p_j$, onde $a, b \geq 0$ e p_l são primos da forma $2^c 3^d + 1$.

Teorema

O polígono regular de n lados é construtível via origami se, e somente se, $n = 2^a 3^b p_1 p_2 ... p_j$, onde $a, b \geq 0$ e p_l são primos da forma $2^c 3^d + 1$.

Por exemplo o heptágono regular pode ser construído via origami


(1)
A
B
(2)
P_1
P_2
L_1
L_2
(3)
P_1
P_2
L_3
(4)
O
C
L_3
(5)
C
L_4
(6)
C
O
(7)
C′
O
C
C″
(8)
C
C′
C″
O
(9)
C
C′
C″
(10)
O
C″
(11)
E
F
(12)

Obrigado =D