Números Algébricos

Pedro F. dos Santos

IST

5 de dezembro de 2018

Números Algébricos

Definição

Um número $\lambda \in \mathbb{C}$ diz-se *algébrico* se existe $p(x) \in \mathbb{Q}[x]$ tal que $p(\lambda) = 0$.
Os números complexos que não são algébricos dizem-se *transcendentes*.

Números Algébricos

Definição

Um número $\lambda \in \mathbb{C}$ diz-se *algébrico* se existe $p(x) \in \mathbb{Q}[x]$ tal que $p(\lambda) = 0$.
Os números complexos que não são algébricos dizem-se *transcendentes*.

Exemplos

- Os números racionais são algébricos.

Números Algébricos

Definição

Um número $\lambda \in \mathbb{C}$ diz-se *algébrico* se existe $p(x) \in \mathbb{Q}[x]$ tal que $p(\lambda) = 0$.
Os números complexos que não são algébricos dizem-se *transcendentes*.

Exemplos

- Os números racionais são algébricos.
- As raízes de números racionais: se $q \in \mathbb{Q}$ e $n \in \mathbb{N}$ então $\sqrt[n]{q}$ é raíz de $p(x) = x^n - q$.

Números Algébricos

Definição

Um número $\lambda \in \mathbb{C}$ diz-se *algébrico* se existe $p(x) \in \mathbb{Q}[x]$ tal que $p(\lambda) = 0$.
Os números complexos que não são algébricos dizem-se *transcendentes*.

Exemplos

- Os números racionais são algébricos.
- As raízes de números racionais: se $q \in \mathbb{Q}$ e $n \in \mathbb{N}$ então $\sqrt[n]{q}$ é raíz de $p(x) = x^n - q$.
- Em particular, $i := \sqrt{-1}$ é algébrico.

Notação

- o *polinómio mínimo* de um número algébrico λ é o polinómio (mónico) $p(x) \in \mathbb{Q}[x]$ de menor grau tal que $p(\lambda) = 0$.

Notação

- o *polinómio mínimo* de um número algébrico λ é o polinómio (mónico) $p(x) \in \mathbb{Q}[x]$ de menor grau tal que $p(\lambda) = 0$.
- o *grau* de λ é o grau do seu polinómio mínimo.

Notação

- o *polinómio mínimo* de um número algébrico λ é o polinómio (mónico) $p(x) \in \mathbb{Q}[x]$ de menor grau tal que $p(\lambda) = 0$.
- o *grau* de λ é o grau do seu polinómio mínimo.

Factos

- O conjunto dos números algébricos, A, é um subcorpo de $\mathbb{C}$.

Notação

- o *polinómio mínimo* de um número algébrico λ é o polinómio (mónico) $p(x) \in \mathbb{Q}[x]$ de menor grau tal que $p(\lambda) = 0$.
- o *grau* de λ é o grau do seu polinómio mínimo.

Factos

- O conjunto dos números algébricos, A, é um subcorpo de $\mathbb{C}$.
- A é numerável (exercício!)

Notação

- o *polinómio mínimo* de um número algébrico λ é o polinómio (mónico) $p(x) \in \mathbb{Q}[x]$ de menor grau tal que $p(\lambda) = 0$.
- o *grau* de λ é o grau do seu polinómio mínimo.

Factos

- O conjunto dos números algébricos, A, é um subcorpo de $\mathbb{C}$.
- A é numerável (exercício!)
- Há muito menos números algébricos do que números transcendentes mas, em geral, é difícil mostrar que um dado número é transcendente.

Notação

- o *polinómio mínimo* de um número algébrico λ é o polinómio (mónico) $p(x) \in \mathbb{Q}[x]$ de menor grau tal que $p(\lambda) = 0$.
- o *grau* de λ é o grau do seu polinómio mínimo.

Factos

- O conjunto dos números algébricos, A, é um subcorpo de $\mathbb{C}$.
- A é numerável (exercício!)
- Há muito menos números algébricos do que números transcendentes mas, em geral, é difícil mostrar que um dado número é transcendente.

Transcendência de π

Só em 1882 é que se demonstrou (Lindemann) que π é transcendente.

Exemplo

O número $\alpha = \sum_n \frac{1}{2^{n!}}$ é transcendente.

Exemplo

O número $\alpha = \sum_n \frac{1}{2^{n!}}$ é transcendente.

Demonstração

Suponhamos que α é algébrico.

Exemplo

O número $\alpha = \sum_n \frac{1}{2^{n!}}$ é transcendente.

Demonstração

Suponhamos que α é algébrico.

Sejam:

- $f(x) = \prod_{i=1}^{d}(x - \alpha_i) \in \mathbb{Q}[x]$ o polinómio mínimo de α $(= \alpha_1)$

Exemplo

O número $\alpha = \sum_n \frac{1}{2^{n!}}$ é transcendente.

Demonstração

Suponhamos que α é algébrico.

Sejam:

- $f(x) = \prod_{i=1}^{d}(x - \alpha_i) \in \mathbb{Q}[x]$ o polinómio mínimo de α $(= \alpha_1)$
- $M \in \mathbb{N}$ tal que $Mf(x) \in \mathbb{Z}[x]$.

Exemplo

O número $\alpha = \sum_n \frac{1}{2^{n!}}$ é transcendente.

Demonstração

Suponhamos que α é algébrico.

Sejam:

- $f(x) = \prod_{i=1}^{d}(x - \alpha_i) \in \mathbb{Q}[x]$ o polinómio mínimo de α $(= \alpha_1)$
- $M \in \mathbb{N}$ tal que $Mf(x) \in \mathbb{Z}[x]$.
- $x_N = \sum_{n=0}^{N} \frac{1}{2^{n!}} \in \mathbb{Q} \quad (x_N \xrightarrow[N\to\infty]{} \alpha)$

Exemplo

O número $\alpha = \sum_n \frac{1}{2^{n!}}$ é transcendente.

Demonstração

Suponhamos que α é algébrico.
Sejam:

- $f(x) = \prod_{i=1}^{d}(x - \alpha_i) \in \mathbb{Q}[x]$ o polinómio mínimo de α $(= \alpha_1)$
- $M \in \mathbb{N}$ tal que $Mf(x) \in \mathbb{Z}[x]$.
- $x_N = \sum_{n=0}^{N} \frac{1}{2^{n!}} \in \mathbb{Q} \quad (x_N \xrightarrow[N\to\infty]{} \alpha)$

Note-se que $f(x_N) \neq 0$, pois f não tem raízes racionais, excepto possivelmente α.

Exemplo

O número $\alpha = \sum_n \frac{1}{2^{n!}}$ é transcendente.

Demonstração

Suponhamos que α é algébrico.
Sejam:

- $f(x) = \prod_{i=1}^{d}(x - \alpha_i) \in \mathbb{Q}[x]$ o polinómio mínimo de α $(= \alpha_1)$
- $M \in \mathbb{N}$ tal que $Mf(x) \in \mathbb{Z}[x]$.
- $x_N = \sum_{n=0}^{N} \frac{1}{2^{n!}} \in \mathbb{Q} \quad (x_N \xrightarrow[N\to\infty]{} \alpha)$

Note-se que $f(x_N) \neq 0$, pois f não tem raízes racionais, excepto possivelmente α.

Daqui segue

$$|(2^{N!})^d Mf(x_N)| \geq 1.$$

v.s.f.f.

Demonstração *(cont)*

Temos

- $|f(x_N)| = \prod_i |x_N - \alpha_i| \leq K|x_N - \alpha|$, para algum K;

Demonstração *(cont)*

Temos

- $|f(x_N)| = \prod_i |x_N - \alpha_i| \leq K|x_N - \alpha|$, para algum K;
- $|x_N - \alpha| = \sum_{n>N} \frac{1}{2^{n!}} \leq \frac{2}{2^{(N+1)!}}$.

Demonstração *(cont)*

Temos

- $|f(x_N)| = \prod_i |x_N - \alpha_i| \leq K|x_N - \alpha|$, para algum K;
- $|x_N - \alpha| = \sum_{n>N} \frac{1}{2^{n!}} \leq \frac{2}{2^{(N+1)!}}$.

Logo, $|(2^{N!})^d Mf(x_N)| \leq \frac{(2^{N!})^d 2MK}{2^{(N+1)!}} \xrightarrow[N\to\infty]{} 0.$

Demonstração *(cont)*

Temos

- $|f(x_N)| = \prod_i |x_N - \alpha_i| \leq K|x_N - \alpha|$, para algum K;
- $|x_N - \alpha| = \sum_{n>N} \frac{1}{2^{n!}} \leq \frac{2}{2^{(N+1)!}}$.

Logo, $|(2^{N!})^d Mf(x_N)| \leq \frac{(2^{N!})^d 2MK}{2^{(N+1)!}} \xrightarrow[N\to\infty]{} 0.$

Contradição, pois

$$|(2^{N!})^d Mf(x_N)| \geq 1.$$

□

Números Construtíveis

Pontos Construtíveis

São aqueles que podem obtidos partindo de $0, 1 \in \mathbb{C}$ (identificado com o plano) fazendo intersecções de:

Números Construtíveis

Pontos Construtíveis

São aqueles que podem obtidos partindo de $0, 1 \in \mathbb{C}$ (identificado com o plano) fazendo intersecções de:

- rectas passando por pontos construídos;

Números Construtíveis

Pontos Construtíveis

São aqueles que podem obtidos partindo de $0, 1 \in \mathbb{C}$ (identificado com o plano) fazendo intersecções de:

- rectas passando por pontos construídos;
- circunferências com centro construído e passando por um ponto construído.

Números Construtíveis

Pontos Construtíveis

São aqueles que podem obtidos partindo de $0, 1 \in \mathbb{C}$ (identificado com o plano) fazendo intersecções de:

- rectas passando por pontos construídos;
- circunferências com centro construído e passando por um ponto construído.

Números Construtíveis

Comprimentos de segmentos construtíveis.

Números Construtíveis

Pontos Construtíveis

São aqueles que podem obtidos partindo de $0, 1 \in \mathbb{C}$ (identificado com o plano) fazendo intersecções de:

- rectas passando por pontos construídos;
- circunferências com centro construído e passando por um ponto construído.

Números Construtíveis

Comprimentos de segmentos construtíveis.

Facto

Os números construtíveis são números algébricos. O seu grau é uma potência de 2.

Um número construtível famoso

Diz-se que duas quantidades estão em **razão de ouro** *se o rácio entre a maior, a, e a menor, b, é a razão entre o todo e a maior:*

$$a/b = (a+b)/a$$

Um número construtível famoso

Diz-se que duas quantidades estão em **razão de ouro** *se o rácio entre a maior, a, e a menor, b, é a razão entre o todo e a maior:*

$$a/b = (a+b)/a$$

O número $\Phi = a/b$ é chamado **Número de Ouro**.

Um número construtível famoso

Diz-se que duas quantidades estão em **razão de ouro** *se o rácio entre a maior, a, e a menor, b, é a razão entre o todo e a maior:*

$$a/b = (a+b)/a$$

O número $\Phi = a/b$ é chamado **Número de Ouro**.
Tem-se $\Phi = 1 + \Phi^{-1}$, pelo que

$$\Phi = \frac{1+\sqrt{5}}{2} \approx 1,618.$$

Um número construtível famoso

Diz-se que duas quantidades estão em **razão de ouro** *se o rácio entre a maior, a, e a menor, b, é a razão entre o todo e a maior:*

$$a/b = (a+b)/a$$

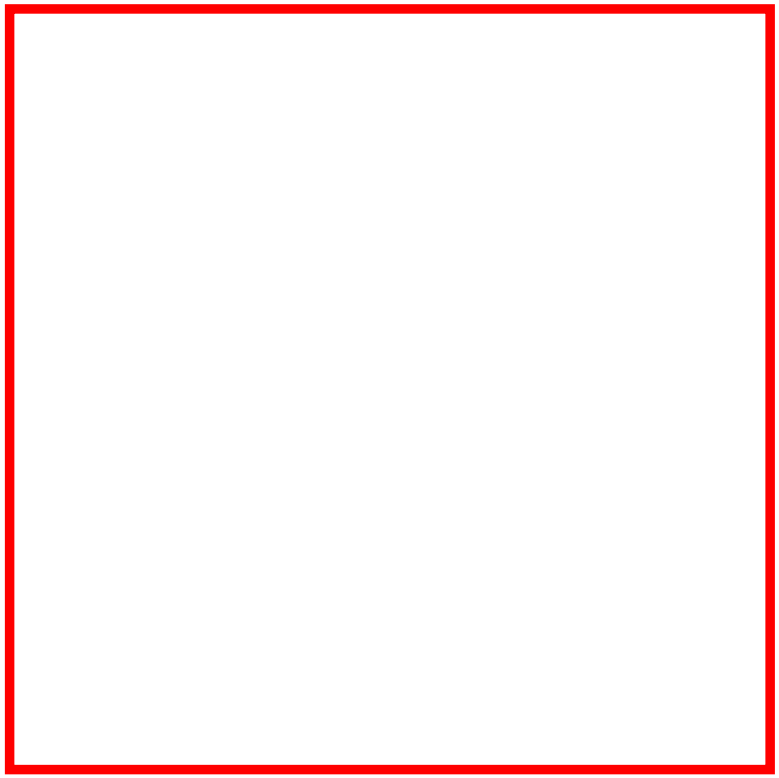
O número $\Phi = a/b$ é chamado **Número de Ouro**.
Tem-se $\Phi = 1 + \Phi^{-1}$, pelo que

$$\Phi = \frac{1+\sqrt{5}}{2} \approx 1,618.$$

Portanto Φ é um número construtível bastante simples.

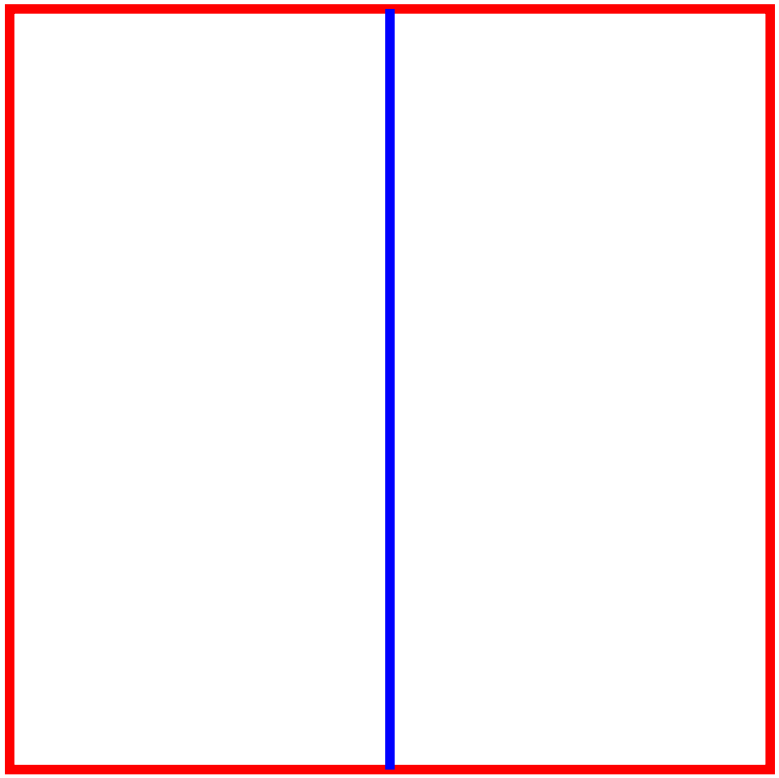
Construção Geométrica de Φ

1



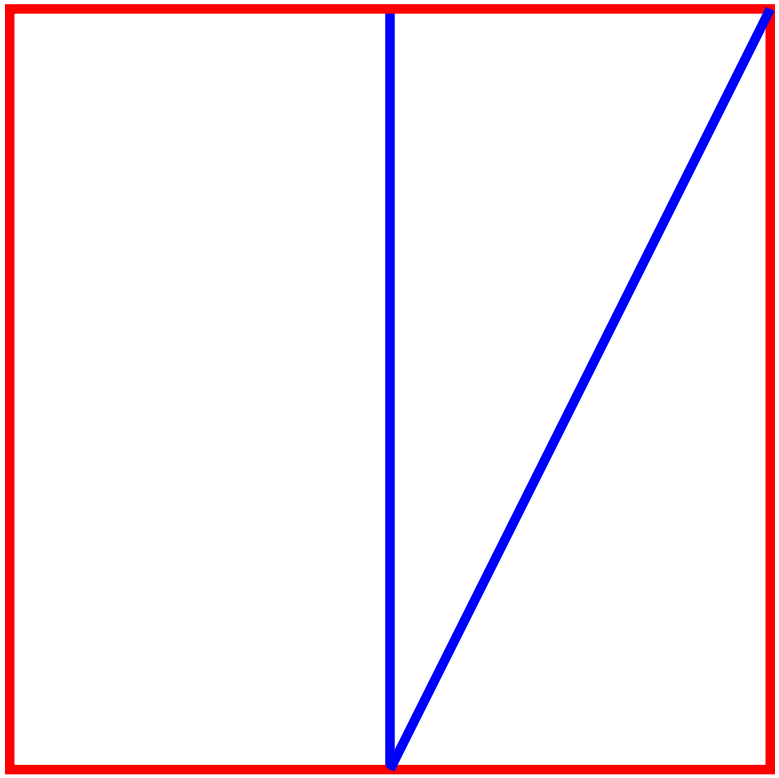
Construção Geométrica de Φ

1



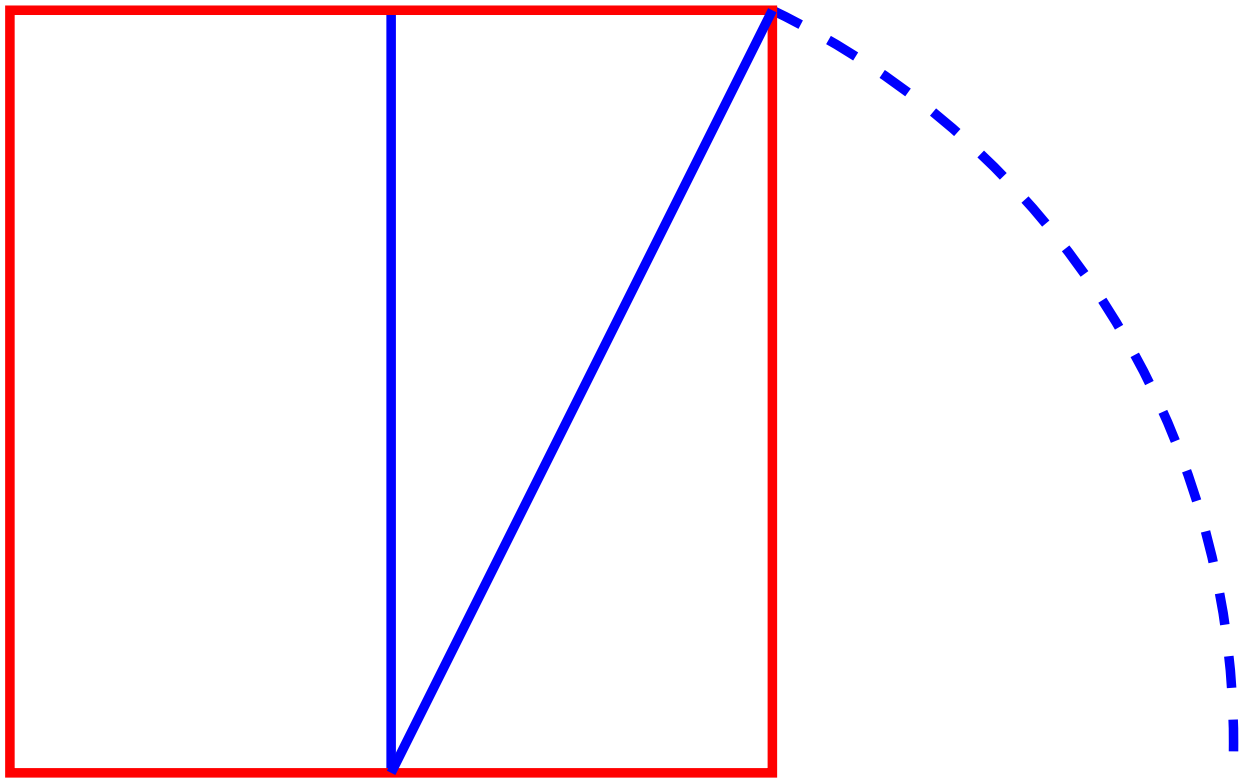
Construção Geométrica de Φ

1



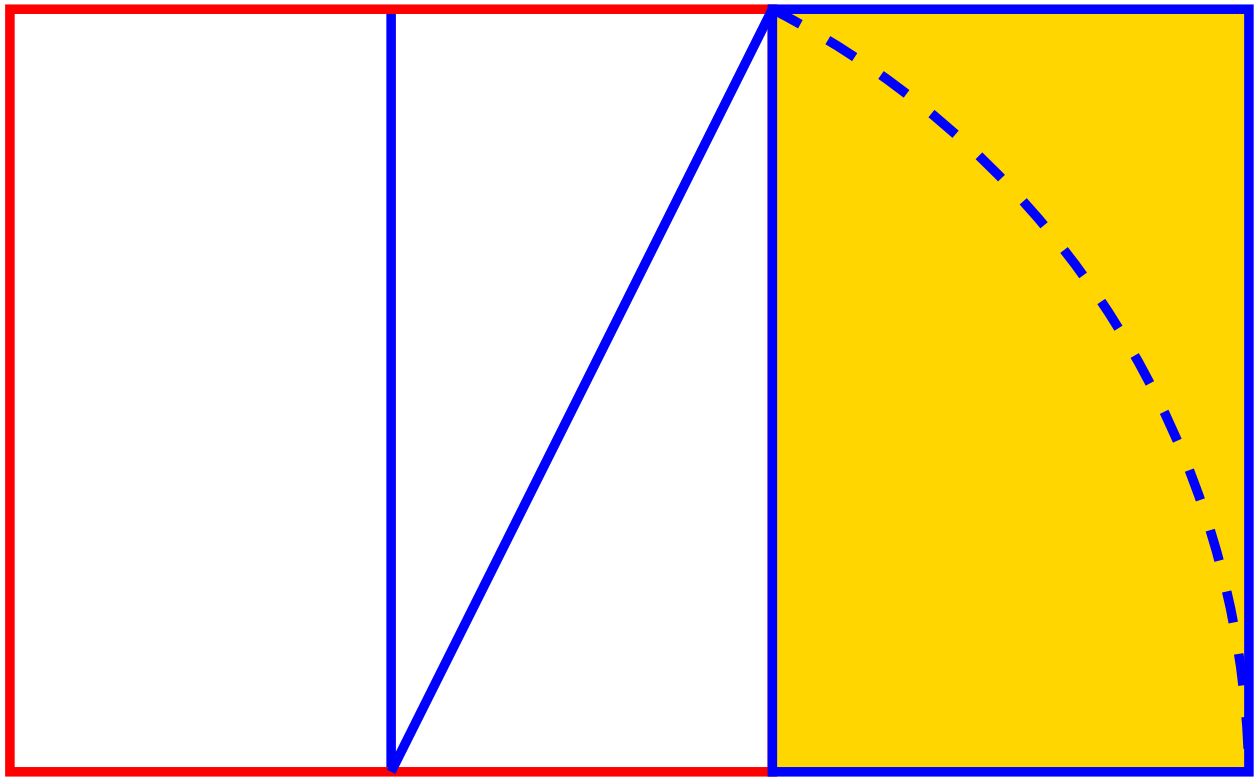
Construção Geométrica de Φ

1



Construção Geométrica de Φ

1



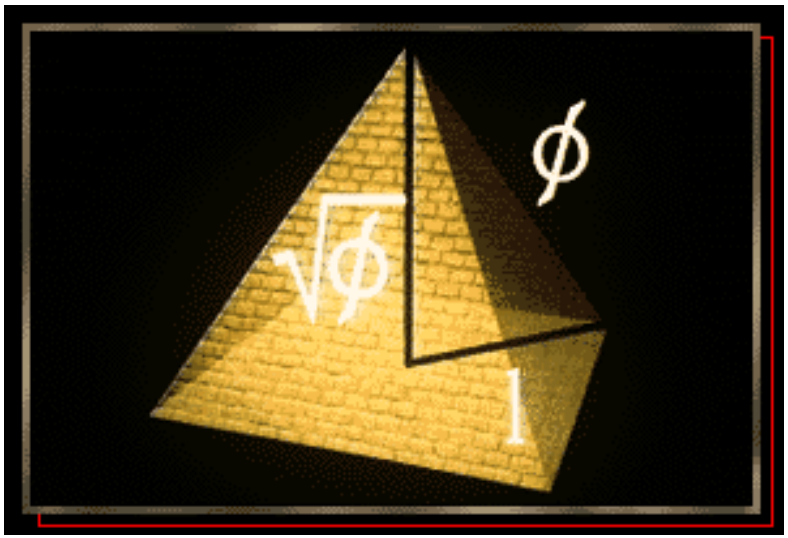
Φ

A estética de Φ

Ao longo dos tempos, Φ tem sido associado à harmonia e à estética. É uma proporção usada em muitas obras de arte:

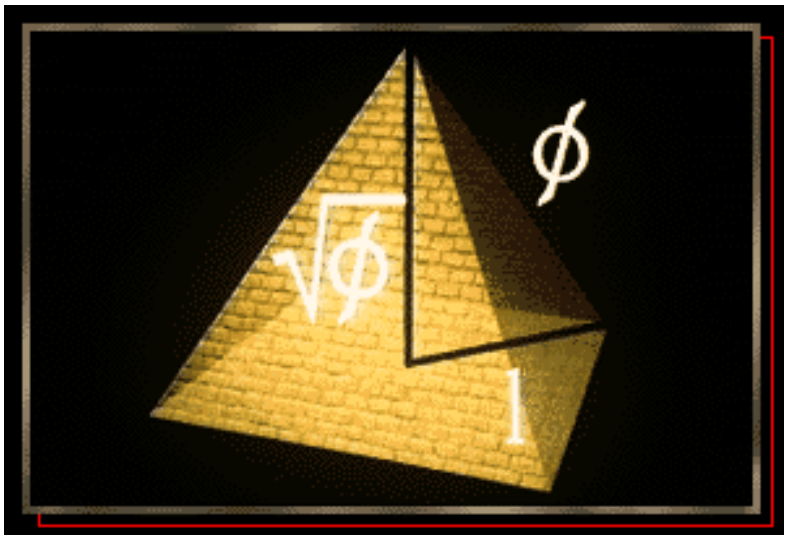
A estética de Φ

Ao longo dos tempos, Φ tem sido associado à harmonia e à estética. É uma proporção usada em muitas obras de arte:



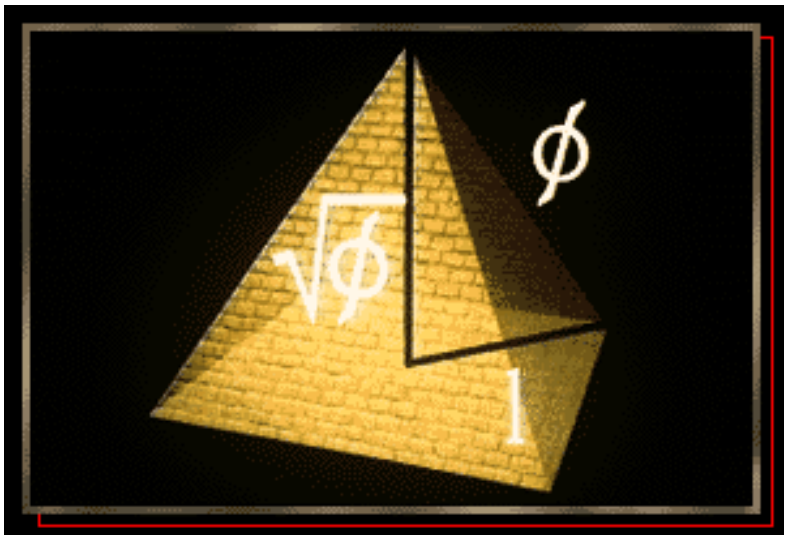
A estética de Φ

Ao longo dos tempos, Φ tem sido associado à harmonia e à estética. É uma proporção usada em muitas obras de arte:



A estética de Φ

Ao longo dos tempos, Φ tem sido associado à harmonia e à estética. É uma proporção usada em muitas obras de arte:



A letra Φ é a inicial de Fídias, um escultor e arquitecto grego.

Quadratura do Círculo

Problema

Construir geometricamente um quadrado com a mesma área que um círculo dado.

Quadratura do Círculo

Problema

Construir geometricamente um quadrado com a mesma área que um círculo dado.

O registo mais antigo de uma tentativa de resolver este problema é o de Anaxágoras (499 AC - 428 AC).

Quadratura do Círculo

Problema

Construir geometricamente um quadrado com a mesma área que um círculo dado.

O registo mais antigo de uma tentativa de resolver este problema é o de Anaxágoras (499 AC - 428 AC).

O problema deve ter sido bastante popular pois é referido numa peça, por volta 414 AC, e a partir daí a expressão *"quadratura do círculo"* tornou-se sinónimo de impossibilidade.

Quadratura do Círculo

Resposta

A quadratura do círculo é impossível, i.e., não é possível construir geometricamente um quadrado com a área de um círculo dado.

Quadratura do Círculo

Resposta

A quadratura do círculo é impossível, i.e., não é possível construir geometricamente um quadrado com a área de um círculo dado.

Demonstração.

Se a quadratura do círculo fosse possível, seria possível construir um quadrado com área π. Portanto o comprimento dos seus lados $\sqrt{\pi}$ seria construtível (logo algébrico). Conclui-se que π seria algébrico. $\square$

Último Teorema de Fermat (UTF)

Teorema (Wiles, 1994)

Para todo o $n \in \mathbb{N}$ *tal que* $n > 2$*, não existem soluções inteiras de*

$$x^n + y^n = z^n$$

tais que $xyz \neq 0$*.*

Lamé

Em 1847 Lamé anunciou um método para provar o UTF:

Lamé

Em 1847 Lamé anunciou um método para provar o UTF:

Suponhamos que $x, y, z \in \mathbb{Z}$ satisfazem

$$x^p + y^p = z^p, \qquad p > 2 \quad \text{primo.}$$

Lamé

Em 1847 Lamé anunciou um método para provar o UTF:

Suponhamos que $x, y, z \in \mathbb{Z}$ satisfazem

$$x^p + y^p = z^p, \qquad p > 2 \quad \text{primo.}$$

Consideremos o número algébrico $\zeta = e^{2\pi i/p}$

Lamé

Em 1847 Lamé anunciou um método para provar o UTF:

Suponhamos que $x, y, z \in \mathbb{Z}$ satisfazem

$$x^p + y^p = z^p, \qquad p > 2 \quad \text{primo.}$$

Consideremos o número algébrico $\zeta = e^{2\pi i/p}$ e

$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots a_n\zeta^n \mid a_i \in \mathbb{Z},\ n \in \mathbb{N}\} \subset \mathbb{C}.$$

Lamé

Em 1847 Lamé anunciou um método para provar o UTF:

Suponhamos que $x, y, z \in \mathbb{Z}$ satisfazem

$$x^p + y^p = z^p, \qquad p > 2 \quad \text{primo.}$$

Consideremos o número algébrico $\zeta = e^{2\pi i/p}$ e

$$\mathbb{Z}[\zeta] = \{a_0 + a_1\zeta + \cdots a_n\zeta^n \mid a_i \in \mathbb{Z},\ n \in \mathbb{N}\} \subset \mathbb{C}.$$

Neste anel de números algébricos obter-se-ia a seguinte factorização

$$(x + y)(x + y\zeta) \cdots (x + y\zeta^{p-1}) = z^p$$

O método de Lamé

Ideia

- mostrar que na factorização

$$(x+y)(x+y\zeta)\cdots(x+y\zeta^{p-1}) = z^p$$

os factores do lado esquerdo são primos entre si.

O método de Lamé

Ideia

- mostrar que na factorização

$$(x+y)(x+y\zeta)\cdots(x+y\zeta^{p-1}) = z^p$$

os factores do lado esquerdo são primos entre si.

- daqui concluir-se-ia que existiriam $t_0, \ldots, t_{p-1}$ tais que

$$x+y = t_0^p, \quad x+y\zeta = t_1^p, \quad \cdots \quad , x+y\zeta^{p-1} = t_{p-1}^p$$

O método de Lamé

Ideia

- mostrar que na factorização

$$(x+y)(x+y\zeta)\cdots(x+y\zeta^{p-1}) = z^p$$

os factores do lado esquerdo são primos entre si.

- daqui concluir-se-ia que existiriam $t_0, \ldots, t_{p-1}$ tais que

$$x+y = t_0^p, \quad x+y\zeta = t_1^p, \quad \cdots \quad , x+y\zeta^{p-1} = t_{p-1}^p$$

- obter-se-ia então uma contradição pelo método de *descida infinita* de Fermat.

O erro de Lamé

- O método de Lamé pressupõe que a factorização dos elementos de $\mathbb{Z}[\zeta]$ em irredutíveis é *única*.

O erro de Lamé

- O método de Lamé pressupõe que a factorização dos elementos de $\mathbb{Z}[\zeta]$ em irredutíveis é *única*.
- Liouville apresentou esta objecção no fim da apresentação de Lamé na Academia das Ciências de Paris.

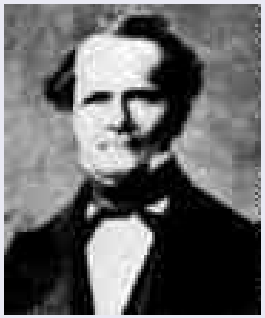
O erro de Lamé

- O método de Lamé pressupõe que a factorização dos elementos de $\mathbb{Z}[\zeta]$ em irredutíveis é *única*.
- Liouville apresentou esta objecção no fim da apresentação de Lamé na Academia das Ciências de Paris.
- Dois meses depois, as dúvidas de Liouville foram confirmadas por Kummer, que demonstrou que, para $p = 23$, o anel $\mathbb{Z}[\zeta]$ não é um *domínio de factorização única*.

O erro de Lamé

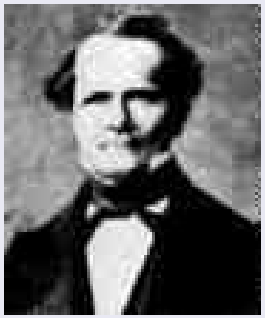
- O método de Lamé pressupõe que a factorização dos elementos de $\mathbb{Z}[\zeta]$ em irredutíveis é *única*.
- Liouville apresentou esta objecção no fim da apresentação de Lamé na Academia das Ciências de Paris.
- Dois meses depois, as dúvidas de Liouville foram confirmadas por Kummer, que demonstrou que, para $p = 23$, o anel $\mathbb{Z}[\zeta]$ não é um *domínio de factorização única*.
- De facto, $\mathbb{Z}[\zeta]$ não é um *domínio de factorização única* para todo o primo $p \geq 23$.

Kummer



Na sequência do anúncio de Lamé, Kummer:

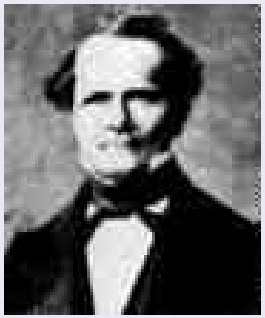
Kummer



Na sequência do anúncio de Lamé, Kummer:

- introduziu uma quantidade h - o número de classes - que mede quão longe está o anel $\mathbb{Z}[\zeta]$ de ser um domínio de factorização única.

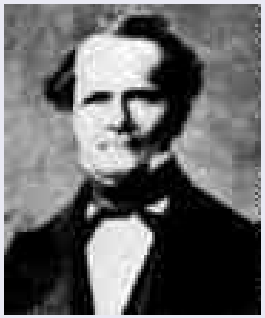
Kummer



Na sequência do anúncio de Lamé, Kummer:

- introduziu uma quantidade h - o número de classes - que mede quão longe está o anel $\mathbb{Z}[\zeta]$ de ser um domínio de factorização única.
- usou a mesma factorização que Lamé, mas substituiu os elementos de $\mathbb{Z}[\zeta]$ por objectos chamados *números ideais*, que deram origem à noção actual de *ideal*.

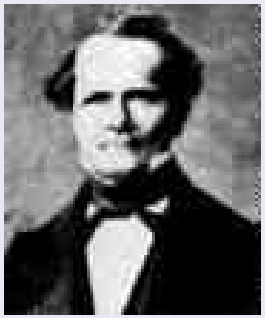
Kummer



Na sequência do anúncio de Lamé, Kummer:

- introduziu uma quantidade h - o número de classes - que mede quão longe está o anel $\mathbb{Z}[\zeta]$ de ser um domínio de factorização única.
- usou a mesma factorização que Lamé, mas substituiu os elementos de $\mathbb{Z}[\zeta]$ por objectos chamados *números ideais*, que deram origem à noção actual de *ideal*.
- provou que para os ideais de $\mathbb{Z}[\zeta]$ é válida a unicidade de factorização em (ideais) primos.

Kummer



Na sequência do anúncio de Lamé, Kummer:

- introduziu uma quantidade h - o número de classes - que mede quão longe está o anel $\mathbb{Z}[\zeta]$ de ser um domínio de factorização única.
- usou a mesma factorização que Lamé, mas substituiu os elementos de $\mathbb{Z}[\zeta]$ por objectos chamados *números ideais*, que deram origem à noção actual de *ideal*.
- provou que para os ideais de $\mathbb{Z}[\zeta]$ é válida a unicidade de factorização em (ideais) primos.
- introduziu os *primos regulares*: primos p tais que $p \nmid h$.

Teorema de Kummer

Teorema:

Se p é um primo regular, então não existem soluções não triviais de

$$x^p + y^p = z^p.$$

Teorema de Kummer

Teorema:

Se p é um primo regular, então não existem soluções não triviais de

$$x^p + y^p = z^p.$$

- Esta foi a primeira demonstração do UTF para uma classe de expoentes.

Teorema de Kummer

Teorema:

Se p é um primo regular, então não existem soluções não triviais de

$$x^p + y^p = z^p.$$

- Esta foi a primeira demonstração do UTF para uma classe de expoentes.
- Só há 3 primos irregulares < 100, para os quais Kummer provou o UTF separadamente.

Teorema de Kummer

Teorema:

Se p é um primo regular, então não existem soluções não triviais de

$$x^p + y^p = z^p.$$

- Esta foi a primeira demonstração do UTF para uma classe de expoentes.
- Só há 3 primos irregulares < 100, para os quais Kummer provou o UTF separadamente.
- Não se sabe se os primos regulares são infinitos.

Conclusão

Os Números Algébricos são nossos Amigos!