Do lema da aula anterior segue o teorema fundamental desta secção:

Teorema. *Se o ponto $P = (x, y) \in \mathbb{R}^2$ é construtível a partir de $\mathcal{P}$ então $[K_0(x) : K_0]$ e $[K_0(y) : K_0]$ são potências de 2.*

Demonstração. Por definição, existe uma sequência finita de pontos de $\mathbb{R}^2$,

$$P_1, \ldots, P_n = P,$$

tais que, para cada $i = 1, \ldots, n$, o ponto $P_i = (x_i, y_i)$ é construtível num passo a partir de $\mathcal{P}_{i-1}$. Pelo lema anterior, $[K_i : K_{i-1}] \in \{1, 2, 4\}$. Ora

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \ldots [K_1 : K_0]$$

pelo que $[K_n : K_0]$ é uma potência de 2. Finalmente, as igualdades

$$[K_n : K_0] = [K_n : K_0(x)][K_0(x) : K_0]$$

$$[K_n : K_0] = [K_n : K_0(y)][K_0(y) : K_0]$$

provam a tese. ∎

Com estes resultados, podemos finalmente resolver os quatro problemas geométricos clássicos.

Corolário 1. *Não é possível duplicar o cubo.*

Demonstração. Podemos partir de um cubo de lado unitário e, portanto, de volume 1, que tem como uma das arestas o segmento entre $(0, 0)$ e $(1, 0)$ no eixo OX. Um cubo de volume 2 teria um lado de comprimento α tal que $\alpha^3 = 2$.

A duplicação do cubo é equivalente à construção, a partir de $\mathcal{P} = \{(0, 0), (1, 0)\}$, de uma aresta de comprimento $\sqrt[3]{2}$, ou, o que é equivalente, à construção do ponto $(\sqrt[3]{2}, 0)$ a partir de $\mathcal{P}$. Como $K_0 = \mathbb{Q}$, se tal fosse possível, então $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ seria uma potência de 2, pelo Teorema. Ora isto é impossível, visto que $\sqrt[3]{2}$ é raiz de $x^3 - 2$, que é irredutível sobre $\mathbb{Q}$ pelo critério de Eisenstein. Portanto o polinómio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ é $x^3 - 2$ pelo que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Logo o cubo não pode ser duplicado. ∎

Corolário 2. *Não é possível trissecar um ângulo de amplitude* $60°$.

Demonstração. Comecemos com $\mathcal{P} = \{(0,0),(1,0)\}$. Na nossa notação, $K_0 = \mathbb{Q}$. Construamos a circunferência c de centro $O = (0,0)$ que passa por $A = (1,0)$. Como vimos, é fácil construir o ponto $B \in c$ tal que $\widehat{AOB} = \frac{\pi}{3}$.

Se fosse possível trissecar o ângulo $\widehat{AOB}$, seria possível construir, a partir de $\mathcal{P}$, o ponto $C \in c$ tal que $\widehat{AOC} = \frac{\pi}{9}$ e, portanto, o ponto $(\cos\frac{\pi}{9}, 0) \in [OA]$. Mas então também o ponto $(2\cos\frac{\pi}{9}, 0)$ seria construtível, pelo que $[\mathbb{Q}(2\cos\frac{\pi}{9}) : \mathbb{Q}]$ seria uma potência de 2 o que é falso:

De facto, como para qualquer θ, $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, temos

$$4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9} = \cos\frac{\pi}{3} = 1/2.$$

Então $\cos\frac{\pi}{9}$ é raiz do polinómio $8x^3 - 6x - 1 = 0$, ou seja, $2\cos\frac{\pi}{9}$ é raiz do polinómio $x^3 - 3x - 1$. Mas $x^3 - 3x - 1 \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$, porque não tem raízes racionais. Em conclusão $[\mathbb{Q}(2\cos\frac{\pi}{9}) : \mathbb{Q}] = 3$. ∎

Corolário 3. *Não é possível quadrar o círculo.*

Demonstração. Podemos supor que a unidade de medida é tal que o raio do círculo é 1, e então temos de construir um quadrado que tenha lado de medida $\sqrt{\pi}$. Portanto a quadratura do círculo equivale à construção do número $(\sqrt{\pi}, 0)$. Mas se $(\sqrt{\pi}, 0)$ fosse construtível então $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = 2^n$ para algum $n \in \mathbb{N}_0$, e então $[\mathbb{Q}(\pi) : \mathbb{Q}]$ dividiria 2^n e, em particular, π seria algébrico sobre $\mathbb{Q}$. Isto é absurdo visto que, como Lindemann mostrou em 1882, π é transcendente sobre $\mathbb{Q}$. ∎

Corolário 4. *Não é possível inscrever um heptágono regular numa circunferência.*

Demonstração. Se essa construção fosse possível, o ponto $(\cos\frac{2\pi}{7}, \sin\frac{2\pi}{7})$ seria construtível a partir de $\mathcal{P} = \{(0,0),(1,0)\}$. Mas tal não é verdade, pois o polinómio mínimo de $\cos\frac{2\pi}{7}$ sobre $\mathbb{Q}$ é $x^3 + \frac{1}{2}x^2 - \frac{1}{2}x - \frac{1}{8}$, pelo que $[\mathbb{Q}(\cos\frac{2\pi}{7}) : \mathbb{Q}] = 3$. ∎

[O Teorema não é verdadeiro na direcção inversa, como se tornará claro durante o estudo da Teoria de Galois: existem números algébricos de grau uma potência de 2 que não dão origem a pontos do plano construtíveis. A Teoria de Galois fornece um critério mais eficiente para determinar se um dado par de números algébricos define um ponto construtível]

Construção de polígonos regulares

Acabámos de observar que, contrariamente ao caso do pentágono, é impossível construir um heptágono regular. E quanto ao caso geral de um polígono com n lados?

POLÍGONOS CONSTRUTÍVEIS

Um polígono diz-se *construtível* se todos os seus vértices são pontos construtíveis de $\mathbb{R}^2$.

Tal como vimos no caso $n = 7$, a construção de um polígono regular com n lados resume-se à construção do ponto $(\cos(2\pi/n), \sin(2\pi/n))$:

Se inscrevermos um polígono regular com n lados no círculo unitário em torno da origem de $\mathbb{R}^2$, com um vértice no ponto $(1, 0)$, então os outros vértices estão nos pontos

$$\Big\{(\cos\Big(\frac{2\pi k}{n}\Big), \sin\Big(\frac{2\pi k}{n}\Big)) \mid 0 < k < n\Big\}.$$

Se conseguirmos construir o ponto $(\cos(2\pi/n), \sin(2\pi/n))$, então conseguimos construir os outros vértices a partir deste. Assim, o polígono é construtível se e só se este ponto é construtível.

Os Gregos foram capazes de construir, com régua e compasso, polígonos regulares com 3 e 5 lados, mas não foram capazes de construir um com 7 lados (que, como acabámos de ver, é uma tarefa impossível).

Nenhum progresso foi feito neste problema durante mais de 2000 anos até que, em 1796, Gauss[1] surpreendeu o mundo matemático com a construção de um polígono regular com 17 lados.

Gauss descobriu mesmo um critério suficiente para que um polígono regular de n lados (um *n-gono*) seja construtível com régua e compasso:

> *O n-gono regular é construtível com régua e compasso se*
>
> $$n = 2^{\alpha} p_1 \dots p_t,$$
>
> *onde $\alpha \in \mathbb{N}_0$ e os p_i são primos ímpares distintos da forma $p_i = 2^{2^{r_i}} + 1$ ($r_i \in \mathbb{N}_0$).*

[1] Na altura, com 19 anos!

E se n não tiver tal forma? A resposta foi dada em 1837 por Pierre Wantzel, que provou o recíproco do Teorema de Gauss: se n não for desta forma, a construção é impossível[2].

O número $F_r = 2^{2^r} + 1$, $r \in \mathbb{N}_0$, chama-se o *r-ésimo número de Fermat*, enquanto um *primo de Fermat* é um número F_r que seja primo. Aqui está uma tabela dos primeiros cinco números F_r que são primos de Fermat, descobertos pelo próprio Fermat:

r	$2^{2^r}+1$
0	3
1	5
2	17
3	257
4	65537

Fermat conjecturou que qualquer F_r é primo, mas Euler mostrou em 1732 que

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417.$$

Hoje ainda não se conhece mais nenhum primo de Fermat além dos encontrados por Fermat. Portanto, só se sabe que um polígono regular com p-lados (p primo) é construtível para $p = 2, 3, 5, 17, 257, 65537$. Para o polígono com 17 lados é apresentada uma construção em [H.S.M. Coxeter, *Introduction to Geometry*, 2ª ed., Wiley, 1989] e [I. Stewart, *Galois Theory*, 3ª ed., Chapman & Hall, 2004]. No primeiro destes livros podemos encontrar ainda uma demonstração muito elegante e curiosa de que 641 divide $2^{2^5} + 1$.

[2] A prova do Teorema de Gauss e desta impossibilidade requere pouco mais do que as ideias que vimos até agora sobre extensões de corpos, e pode ser consultada em, por exemplo, [I. Stewart, *Galois Theory*, 3ª ed., Chapman & Hall, 2004].