FACULDADE DE CIÊNCIAS DA UNIVERSIDADE DO PORTO
DEPARTAMENTO DE MATEMÁTICA PURA

Divisão da lemniscata em partes iguais

ILDA MARISA DE SÁ REIS

SETEMBRO 2005

FACULDADE DE CIÊNCIAS DA UNIVERSIDADE DO PORTO
DEPARTAMENTO DE MATEMÁTICA PURA

Divisão da lemniscata em partes iguais

Tese submetida à Faculdade de Ciências da Universidade do Porto
para obtenção do grau de mestre
em Matemática – Fundamentos e Aplicações

ILDA MARISA DE SÁ REIS

SETEMBRO 2005

Agradecimentos

Em primeiro lugar, agradeço à Professora Doutora Maria de Fátima Carvalho a quem devo a orientação deste trabalho. Quero agradecer-lhe também pelo tema proposto, pelo constante encorajamento e pelas inúmeras sugestões que muito contribuiram para o melhoramento deste texto.

À Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança agradeço o apoio financeiro e as facilidades concedidas nos horários durante a frequência da parte curricular do mestrado.

Por último, gostaria de deixar uma palavra de gratidão a todos os que me incentivaram e acompanharam com interesse o meu trabalho.

Conteúdo

Introdução

O objectivo deste texto é o de completar, em detalhe, o lado direito da tabela que se anexa, que compara o papel de duas curvas – a circunferência unitária e a lemniscata de Bernoulli – na construção das inversas das funções comprimento de arco e na divisão em partes iguais.

As lemniscatas caracterizam-se por serem conjuntos de pontos do plano cujo produto das distâncias a dois pontos fixos é constante. O cálculo do comprimento total da lemniscata que aqui consideramos conduz a um integral elíptico (Bernoulli, 1694), de função que não tem primitiva imediata mas cujo valor se obtém por procedimento elementar através do algoritmo, delineado por Lagrange (1785) e Gauss (1790), que constrói a média aritmética e geométrica de dois números positivos. A função comprimento de arco da lemniscata tem propriedades semelhantes às conhecidas para a arco seno trigonométrico e a sua inversão conduz a um caso particular, de especial interesse, na família das funções elípticas: o seno da lemniscata, $senlem$. Esta é uma função periódica de período 2ω cuja extensão meromorfa aos complexos é duplamente periódica (de período 2ω e $2\omega i$) e portanto elíptica, onde 2ω designa o comprimento total da lemniscata que substitui neste contexto 2π, o comprimento da circunferência unitária e período da função seno trigonométrico, sen. Verifica fórmulas de adição análogas às da função seno, obtidas por Euler em 1751 depois de receber cópia da obra de Fagnano (1718) onde se deduz uma fórmula para o comprimento do dobro de um arco de lemniscata e, consequentemente, que é possível duplicar arcos de lemniscata, com régua não graduada e compasso.

A possibilidade de construir, com régua não graduada e compasso, um polígono regular de n lados é equivalente à divisão, com estes instrumentos, da circunferência unitária em n arcos de igual comprimento; e este procedimento corresponde à construção dos reais $sen\left(\frac{2k\pi}{n}\right)$, onde $0 \leq k \leq n-1$, uma

vez que os valores dos cossenos destes ângulos têm uma relação quadrática com os senos. Gauss e Wantzel provaram que esta construção é possível se e só se $n = 2^k p_1 p_2 \dots p_t$, onde $k \in \mathbb{N}_0$ e p_1, p_2, $\dots$, p_t são primos de Fermat distintos. Por falta de simetria, estas interligações geométricas não se transferem integralmente para o contexto da lemniscata e por isso não falaremos aqui da inscrição de polígonos regulares na lemniscata. O que Abel (1827) generalizou para a lemniscata foi a equivalência entre a possibilidade de construir, com régua não graduada e compasso, os reais $senlem\left(\frac{2k\omega}{n}\right)$, onde $0 \leq k \leq n-1$, e os valores de n como descritos acima. Ou seja, é possível dividir em n arcos de igual comprimento um quadrante da lemniscata se e só se n tem a factorização indicada.

Na apresentação que aqui fazemos deste assunto seguiremos de perto os textos de [Hadlock] e [Rosen]; a bibliografia contém outras referências que complementam o texto. Como apoio, incluiram-se alguns capítulos de abordagem geral, mas resumida, sobre funções elípticas, números construíveis, polígonos regulares construíveis – seguindo as demonstrações originais de Gauss e Wantzel – e a Teoria de Galois.

Circunferência	**Lemniscata**
$x^2+y^2=1$	$(x^2+y^2)^2-(x^2-y^2)=0$
arco de ângulo $\theta=\int_0^\theta \frac{1}{\sqrt{1-t^2}}dt$	arco de ângulo $\theta=\int_0^\theta \frac{1}{\sqrt{1-t^4}}dt$
comprimento total da curva $=2\pi$	comprimento total da curva $=\frac{2\pi}{mag\,(1,\sqrt{2})}=2\omega$
$\pi=\frac{\text{perímetro}}{\text{diâmetro}}$ de qualquer circunferência	$mag\,(a,b)=$ média aritmética/geométrica de a e b
duplicação de arco com régua não graduada e compasso	duplicação de arco com régua não graduada e compasso
$2\int_0^\theta \frac{1}{\sqrt{1-t^2}}dt=\int_0^{2\theta\sqrt{1-\theta^2}} \frac{1}{\sqrt{1-t^2}}dt$	$2\int_0^\theta \frac{1}{\sqrt{1-t^4}}dt=\int_0^{\frac{2\theta\sqrt{1-\theta^4}}{1+\theta^4}} \frac{1}{\sqrt{1-t^4}}dt$
seno trigonométrico ($sen:\mathbb{R}\to\mathbb{R}$ de período 2π)	seno da lemniscata ($senlem:\mathbb{R}\to\mathbb{R}$ de período $\frac{2\pi}{mag\,(1,\sqrt{2})}$)
$sen\,(x+y)=sen(x)\sqrt{1-sen^2(y)}+sen(y)\sqrt{1-sen^2(x)}$	$senlem\,(x+y)=\frac{senlem(x)\sqrt{1-senlem^4(y)}+senlem(y)\sqrt{1-senlem^4(x)}}{1+\left(senlem(x)senlem(y)\right)^2}$
Construtibilidade de $sen\,(\frac{2k\pi}{n})$, $k\in\{0,1,\cdots,n-1\}$	Construtibilidade de $senlem\,(\frac{2k\omega}{n})$, $k\in\{0,1,\cdots,n-1\}$
Divisão em n partes iguais se e só se $n=2^k\,p_1p_2\cdots p_t$, $k\in\mathbb{N}_0$, p_i primos de Fermat distintos	Divisão em n partes iguais se e só se $n=2^k\,p_1p_2\cdots p_t$, $k\in\mathbb{N}_0$, p_i primos de Fermat distintos

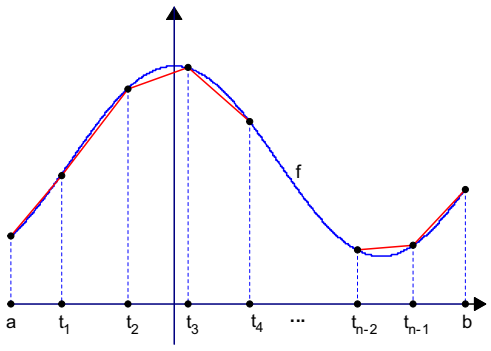
Capítulo 1

Seno trigonométrico

O conteúdo deste capítulo é elementar e usual numa primeira abordagem da análise. É aqui incluído como material preliminar para o capítulo 3. Há, na literatura, vários procedimentos, mais ou menos elaborados, para construir a função seno; escolhemos o que é apresentado na referência [Spivak], que utiliza a noção de comprimento de arco de uma circunferência por ser mais fácil de adaptar à lemniscata. Relativamente a noção de comprimento de arco apresentamos o essencial para relaciona-la com o cálculo de certos integrais.

1.1 Comprimento do gráfico de uma função

Para encontrar o comprimento do gráfico de uma função f entre os pontos $(a, f(a))$ e $(b, f(b))$, podemos dividir o intervalo $[a, b]$ em n subintervalos e considerar o comprimento da curva poligonal inscrita no gráfico de f como uma aproximação do seu comprimento.



É de esperar que, se a função for bastante regular, a curva poligonal esteja tanto mais próxima do gráfico de f quanto maior for o número de subintervalos de $[a,b]$. Esta ideia motiva a seguinte definição:

Definição 1.1.1 *Seja $f:[a,b]\to\mathbb{R}$ uma função contínua. Dada uma partição finita $P=\{a=t_0<t_1<t_2<\ldots<t_n=b\}$ do intervalo $[a,b]$, o* ***comprimento da curva poligonal*** *inscrita no gráfico de f determinado pela partição P é dado por*

$$l(f,P)=\sum_{i=1}^{n}\sqrt{(t_i-t_{i-1})^2+(f(t_i)-f(t_{i-1}))^2}.$$

O ***comprimento do gráfico de*** *f no intervalo $[a,b]$ é o supremo (que pode ser infinito) dos comprimentos das curvas poligonais sobre todas as partições de $[a,b]$.*

Desta definição resultam algumas consequências imediatas:

- Se f é uma função afim definida em $[a,b]$, então o comprimento do gráfico de f é a distância entre $(a,f(a))$ e $(b,f(b))$.

  Por f ser uma função afim, existem $r,s\in\mathbb{R}$ tais que $f(x)=rx+s$ para todo x de $[a,b]$. A distância entre $(a,f(a))$ e $(b,f(b))$ é

  $$\begin{aligned}\sqrt{(b-a)^2+(f(b)-f(a))^2} &= \sqrt{(b-a)^2+(rb-ra)^2}\\ &= \sqrt{1+r^2}\,(b-a).\end{aligned}$$

  Por outro lado, dada uma partição $P=\{a=t_0<t_1<t_2<\ldots<t_n=b\}$ do intervalo $[a,b]$, o comprimento da curva poligonal inscrita no gráfico de f é

  $$\begin{aligned}l(f,P) &= \sum_{i=1}^{n}\sqrt{(t_i-t_{i-1})^2+(rt_i-rt_{i-1})^2}\\ &= \sqrt{1+r^2}\sum_{i=1}^{n}(t_i-t_{i-1})\\ &= \sqrt{1+r^2}\,(t_n-t_0)\\ &= \sqrt{1+r^2}\,(b-a).\end{aligned}$$

Isto é, para qualquer partição P,

$$l(f,P) = \sqrt{1+r^2}\,(b-a).$$

E portanto o supremo dos comprimentos das curvas poligonais sobre todas as partições de $[a,b]$ é $\sqrt{1+r^2}\,(b-a)$, sendo que este é também o valor da distância de $(a, f(a))$ a $(b, f(b))$.

- Se f não é afim, existe uma partição $P = \{a,t,b\}$ do intervalo $[a,b]$ tal que $l(f,P)$ é maior que a distância entre $(a, f(a))$ e $(b, f(b))$.

  Não sendo f afim, existe um ponto t em $]a,b[$ cuja imagem não pertence à recta que une o ponto $(a, f(a))$ ao ponto $(b, f(b))$. Se considerarmos a partição $P = \{a,t,b\}$, a desigualdade triangular assegura que

  $$l(f,P) > \sqrt{(b-a)^2 + (f(b)-f(a))^2}.$$

  Logo o comprimento do gráfico de f, que não é um segmento de recta, é maior que a distância entre $(a, f(a))$ e $(b, f(b))$.

- De entre todas as funções contínuas definidas no intervalo $[a,b]$ que unem os pontos $(a, f(a))$ a $(b, f(b))$, a função afim é a que tem gráfico com menor comprimento.

  Se f é função afim então, como vimos anteriormente, o comprimento do seu gráfico é igual à distância entre $(a, f(a))$ e $(b, f(b))$. Caso contrário, existe uma partição P tal que a distância entre $(a, f(a))$ e $(b, f(b))$ é menor que $l(f,P)$, que por sua vez é menor ou igual ao comprimento do gráfico de f.

- No caso em que a função $f: [a,b] \to \mathbb{R}$ é diferenciável em $]a,b[$ e possui derivada contínua,

  Afirmação 1 *Para qualquer partição P de $[a,b]$, verificam-se as seguintes desigualdades*

  $$L\left(\sqrt{1+(f')^2}, P\right) \leq l(f,P) \leq U\left(\sqrt{1+(f')^2}, P\right) \tag{1.1}$$

  onde $L\left(\sqrt{1+(f')^2}, P\right)$ e $U\left(\sqrt{1+(f')^2}, P\right)$ são, respectivamente, a soma inferior e superior da função $\sqrt{1+(f')^2}$ associada à partição P.

Seja $P = \{a = t_0 < t_1 < t_2 < \ldots < t_n = b\}$ uma partição do intervalo $[a, b]$. Para cada $i = 1, 2, \ldots, n$, a função f é contínua em $[t_{i-1}, t_i]$ e diferenciável em $]t_{i-1}, t_i[$, logo pelo Teorema do Valor Médio, existe $t_i^* \in]t_{i-1}, t_i[$ tal que

$$f'(t_i^*) = \frac{f(t_i) - f(t_{i-1})}{t_i - t_{i-1}}.$$

Assim, o comprimento da curva poligonal inscrita no gráfico de f determinada pela partição P, pode ser reescrito da seguinte forma:

$$\begin{aligned} l(f, P) &= \sum_{i=1}^{n} \sqrt{(t_i - t_{i-1})^2 + (f(t_i) - f(t_{i-1}))^2} \\ &= \sum_{i=1}^{n} \sqrt{(t_i - t_{i-1})^2 + (f')^2(t_i^*)(t_i - t_{i-1})^2} \\ &= \sum_{i=1}^{n} \sqrt{1 + (f')^2(t_i^*)}\,(t_i - t_{i-1}). \end{aligned}$$

Por outro lado, para cada $i = 1, 2, \ldots, n$,

$$m_i \leq \sqrt{1 + (f')^2(t_i^*)} \leq M_i$$

onde

$$\begin{aligned} m_i &= \inf_{x \in [t_{i-1}, t_i]} \left\{ \sqrt{1 + (f')^2(x)} \right\} \\ M_i &= \sup_{x \in [t_{i-1}, t_i]} \left\{ \sqrt{1 + (f')^2(x)} \right\}. \end{aligned}$$

Logo

$$\sum_{i=1}^{n} m_i (t_i - t_{i-1}) \leq l(f, P) \leq \sum_{i=1}^{n} M_i (t_i - t_{i-1})$$

o que prova as desigualdades de (1.1).

Afirmação 2 *Para qualquer partição P de $[a, b]$,*

$$\sup_P \left\{ L\left(\sqrt{1 + (f')^2}, P \right) \right\} \leq \sup_P \{ l(f, P) \}. \tag{1.2}$$

Seja $s = \sup_P \{l(f,P)\}$. Por definição de supremo, $l(f,P) \leq s$ qualquer que seja a partição P de $[a,b]$. A desigualdade (1.1) garante que s é um majorante do conjunto $\left\{ L\left(\sqrt{1+(f')^2}, P\right) : P \text{ partição} \right\}$. Dado que o supremo de um conjunto é o menor dos majorantes, temos a desigualdade (1.2).

Afirmação 3 *Para qualquer partição P de $[a,b]$,*

$$\sup_P \{l(f,P)\} \leq \inf_P \left\{ U\left(\sqrt{1+(f')^2}, P\right) \right\}. \tag{1.3}$$

Seja $m = \inf_P \left\{ U\left(\sqrt{1+(f')^2}, P\right) \right\}$. Então, por definição de ínfimo, m é um minorante do conjunto $\left\{ U\left(\sqrt{1+(f')^2}, P\right) : P \text{ partição} \right\}$. Se P' e P'' forem duas partições de $[a,b]$ temos

$$l(f,P') \leq U\left(\sqrt{1+(f')^2}, P''\right)$$

pois se considerarmos a partição $Q = P' \cup P''$, obtemos por (1.1)

$$\begin{aligned} l(f,P') &\leq l(f,Q) \\ &\leq U\left(\sqrt{1+(f')^2}, Q\right) \\ &\leq U\left(\sqrt{1+(f')^2}, P''\right). \end{aligned}$$

Logo o conjunto $\left\{ U\left(\sqrt{1+(f')^2}, P\right) : P \text{ partição} \right\}$ é minorado por $l(f,P)$, qualquer que seja a partição P. Por outro lado,

$$l(f,P) \leq m$$

para todas as partições, pois o ínfimo de um conjunto é o maior dos seus minorantes. Logo o conjunto $\{l(f,P) : P \text{ partição}\}$ é majorado por m e portanto o seu supremo não excede m.

Afirmação 4 *Se a função* $\sqrt{1+(f')^2}$ *for integrável no intervalo* $[a,b]$,

$$\begin{aligned}\sup_P \left\{ L\left(\sqrt{1+(f')^2}, P\right)\right\} &= \inf_P \left\{ U\left(\sqrt{1+(f')^2}, P\right)\right\} \\ &= \sup_P \left\{ l\left(f, P\right)\right\}.\end{aligned}$$

E portanto, acabamos de provar a proposição que se segue que permite calcular o comprimento do gráfico da função f no intervalo $[a,b]$ recorrendo à noção de integral.

Proposição 1.1.2 *Seja* $f:\ [a,b] \to \mathbb{R}$ *uma função diferenciável tal que* $\sqrt{1+(f')^2}$ *é integrável no intervalo* $[a,b]$. *O comprimento do gráfico de* f *em* $[a,b]$ *é igual* $\int_a^b \sqrt{1+(f')^2}$.

1.2 Construção da função seno em $\left[0, \frac{\pi}{2}\right]$

Consideremos a função

$$\begin{array}{rccc} f: & [0,1] & \to & \mathbb{R} \\ & x & \mapsto & \sqrt{1-x^2} \end{array}.$$

A função f associa a cada x a ordenada de um ponto da circunferência unitária centrada na origem do plano. Usando a proposição (1.1.2), vamos construir uma nova função no intervalo $\left[0, \frac{\pi}{2}\right]$, à qual daremos o nome de *seno*.

Proposição 1.2.1 *O comprimento do gráfico da função* f *no intervalo* $[0,x]$ *é* $\int_0^x \frac{dt}{\sqrt{1-t^2}}$, *para qualquer* $x \in [0,1]$.

Prova. Pela proposição (1.1.2), para cada $0 \leq x < 1$, o comprimento do gráfico de f no intervalo $[0,x]$ é dado por

$$\int_0^x \sqrt{1+(f')^2\,(t)}dt = \int_0^x \frac{1}{\sqrt{1-t^2}}dt. \tag{1.4}$$

Quando $x = 1$, estamos perante um integral impróprio, sendo necessário averiguar se ainda é possível calcular o comprimento do gráfico de f usando a igualdade (1.4). Ora, para qualquer $0 < \epsilon < 1$,

$$\text{comprimento de } f \text{ em } [0, 1-\epsilon] = \int_0^{1-\epsilon} \frac{1}{\sqrt{1-t^2}} dt.$$

Para estender esta igualdade ao intervalo $[0, 1]$, bastará provar que

$$\lim_{\epsilon \to 0^+} \left(\begin{array}{c} \text{comprimento de} \\ f \text{ em } [0, 1-\epsilon] \end{array} \right) = \begin{array}{c} \text{comprimento de} \\ f \text{ em } [0, 1] \end{array}.$$

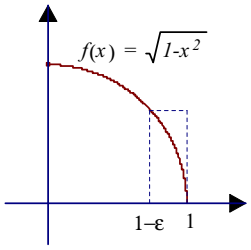
Mas

$$\begin{array}{c} \text{comprimento de} \\ f \text{ em } [0, 1] \end{array} = \begin{array}{c} \text{comprimento de} \\ f \text{ em } [0, 1-\epsilon] \end{array} + \begin{array}{c} \text{comprimento de} \\ f \text{ em } [1-\epsilon, 1] \end{array}.$$

Ora, por definição de comprimento do gráfico de uma função, o comprimento de qualquer curva poligonal inscrita não excede o comprimento do seu gráfico, em particular se considerarmos a partição $P = \{1-\epsilon, 1\}$,

$$l(f, P) \leq \text{comprimento de } f \text{ em } [1-\epsilon, 1],$$

por outro lado, de acordo com a figura que se segue,



$$l(f, P) < \epsilon + f(1-\epsilon)$$

e sendo o comprimento do gráfico de f em $[1-\epsilon, 1]$ o supremo sobre todas as curvas poligonais inscritas,

$$0 \leq \begin{array}{c} \text{comprimento de} \\ f \text{ em } [1-\epsilon, 1] \end{array} < \epsilon + f(1-\epsilon) = \epsilon + \sqrt{2\epsilon - \epsilon^2} < \epsilon + \sqrt{2\epsilon}$$

e portanto a igualdade pretendida resulta fazendo $\epsilon \to 0^+$. ■

Vamos agora estudar analiticamente a função que mede o comprimento do gráfico de f em subintervalos da forma $[0, x]$:

$$\begin{array}{rccc} AS: & [0,1] & \to & \mathbb{R}_0^+ \\ & x & \mapsto & \displaystyle\int_0^x \frac{dt}{\sqrt{1-t^2}} \end{array}$$

Notação 1.2.2 $AS(1) = \frac{l}{2}$.

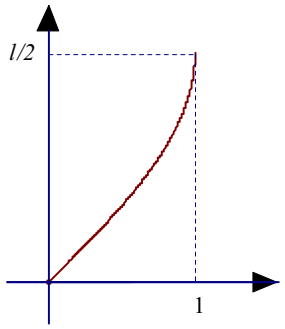
Em particular, da proposição (1.1.2) resulta que $\frac{l}{2}$ é o comprimento de um quarto da circunferência unitária. Pelo Teorema Fundamental do Cálculo, a função AS é contínua, derivável e

$$AS'(x) = \frac{1}{\sqrt{1-x^2}}$$

para qualquer x de $]0,1[$. Como a função AS' é sempre positiva no intervalo $]0,1[$, AS é estritamente crescente e consequentemente injectiva. Além disso, o seu gráfico tem a concavidade voltada para cima, pois

$$AS''(x) = \frac{x}{(1-x^2)\sqrt{1-x^2}}$$

é positiva em $]0,1[$. Logo o gráfico da função AS é o seguinte:



Como AS é uma função contínua, o Teorema do Valor Intermédio afirma que para cada x de $\left[0, \frac{l}{2}\right]$ existe um y em $[0,1]$ tal que $AS(y) = x$. Decorre da

injectividade de AS que um tal y é único. Designá-lo-emos por $\mathfrak{sen}\,(x)$. Para cada x em $\left[0, \frac{l}{2}\right]$, a aplicação

$$x \;\mapsto\; \mathfrak{sen}\,(x)$$

está bem definida e a sua imagem é o intervalo $[0,1]$. Em particular,

$$\mathfrak{sen}\,(0) = 0 \quad \text{e} \quad \mathfrak{sen}\left(\frac{l}{2}\right) = 1.$$

Além disso, para cada $x \in \left[0, \frac{l}{2}\right]$, faz sentido definir

$$\mathfrak{cos}\,(x) = \sqrt{1 - \mathfrak{sen}^2\,(x)}.$$

Proposição 1.2.3 *As funções $\mathfrak{sen}$ e $\mathfrak{cos}$ são diferenciáveis no intervalo $\left]0, \frac{l}{2}\right[$:*

$$\mathfrak{sen}'\,(x) = \mathfrak{cos}\,(x) \quad \textit{e} \quad \mathfrak{cos}'\,(x) = -\mathfrak{sen}\,(x)$$

para qualquer $x \in \left]0, \frac{l}{2}\right[$.

Prova. Da igualdade $AS\,(\mathfrak{sen}\,(x)) = x$ segue que AS e $\mathfrak{sen}$ são funções inversas, logo possuem o mesmo tipo de monotonia. Além disso, o domínio e a imagem da função $\mathfrak{sen}$ são intervalos pelo que esta é uma função contínua. Como AS é derivável e AS' não se anula, resulta que a função $\mathfrak{sen}$ é diferenciável e que temos

$$\begin{aligned} \mathfrak{sen}'\,(x) &= \frac{1}{AS'\,(\mathfrak{sen}\,(x))} \\ &= \sqrt{1 - \mathfrak{sen}^2\,(x)} \\ &= \mathfrak{cos}\,(x) \end{aligned}$$

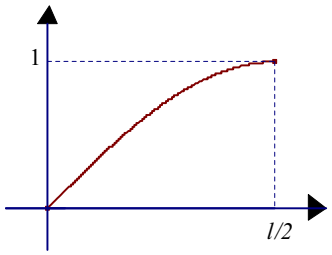
para qualquer $x \in \left]0, \frac{l}{2}\right[$.

A função $\mathfrak{cos}$ é diferenciável pois é composta de funções diferenciáveis. Como o valor absoluto de $\mathfrak{sen}$ é diferente de 1 em todo o intervalo $\left]0, \frac{l}{2}\right[$, resulta que

$$\begin{aligned} \mathfrak{cos}'\,(x) &= \frac{-2\mathfrak{sen}\,(x)\,\mathfrak{cos}\,(x)}{2\sqrt{1 - \mathfrak{sen}^2\,(x)}} \\ &= -\mathfrak{sen}\,(x)\,. \end{aligned}$$

■

A informação que obtivemos sobre a função $\mathfrak{sen}$ permite traçar o seu gráfico no intervalo $\left[0, \frac{l}{2}\right]$



Observação 1.2.4 *Na literatura matemática, costuma-se designar a função AS por arco seno e denotar por arcsen.*

1.3 Prolongamento da função seno a $\mathbb{R}$

Comecemos por estender as funções $\mathfrak{sen}$ e $\mathfrak{cos}$ ao intervalo $[0, l]$ de modo que o gráfico da primeira seja simétrico relativamente à recta $x = \frac{l}{2}$ e o da segunda o seja em em relação ao ponto $\left(\frac{l}{2}, 0\right)$. Defina-se

$$\boldsymbol{S}en\,(x) = \begin{cases} \mathfrak{sen}\,(x) & \text{se} \quad x \in \left[0, \frac{l}{2}\right] \\ \mathfrak{sen}\,(l-x) & \text{se} \quad x \in \left[\frac{l}{2}, l\right] \end{cases}$$

e

$$\boldsymbol{C}os\,(x) = \begin{cases} \mathfrak{cos}\,(x) & \text{se} \quad x \in \left[0, \frac{l}{2}\right] \\ -\mathfrak{cos}\,(l-x) & \text{se} \quad x \in \left[\frac{l}{2}, l\right] \end{cases}.$$

Estes prolongamentos preservam as propriedades das derivadas das funções $\mathfrak{sen}$ e $\mathfrak{cos}$.

Proposição 1.3.1 *Para qualquer $x \in \,]0, l[$,*

$$\boldsymbol{S}en'\,(x) = \boldsymbol{C}os\,(x) \quad e \quad \boldsymbol{C}os'\,(x) = -\boldsymbol{S}en\,(x)\,.$$

Prova. No caso em que $x \in \left]0, \frac{l}{2}\right[$, este enunciado não acrescenta nada de novo à proposição (1.2.3).

Se $x \in \left]\frac{l}{2}, l\right[$, então $0 < l - x < \frac{l}{2}$ e, aplicando o Teorema da Derivação da Função Composta temos que

$$\begin{aligned} \boldsymbol{S}en'(x) &= (\mathfrak{s}en(l-x))' \\ &= -\mathfrak{c}os(l-x) \\ &= \boldsymbol{C}os(x) \end{aligned}$$

e

$$\begin{aligned} \boldsymbol{C}os'(x) &= (-\mathfrak{c}os(l-x))' \\ &= -\mathfrak{s}en(l-x) \\ &= -\boldsymbol{S}en(x). \end{aligned}$$

Falta apenas provar que estas funções são diferenciáveis em $\frac{l}{2}$ e que as suas derivadas verificam as igualdades acima. Para isso vamos usar o seguinte resultado:

Lema 1.3.2 *Seja f uma função contínua num ponto α e V uma vizinhança de α. Se a derivada de f está definida em $V \setminus \{\alpha\}$ e existe $\lim_{x\to\alpha} f'(x)$, então f é derivável em α e f' é continua em α.*

Prova. Por definição, $f'(\alpha) = \lim_{x\to\alpha} \frac{f(x)-f(\alpha)}{x-\alpha}$. Pelas hipóteses do lema, podemos usar a Regra de L'Hôpital para calcular este limite, e obtemos $f'(\alpha) = \lim_{x\to\alpha} f'(x)$ ■

Assim aplicando o lema, obtemos

$$\boldsymbol{S}en'\left(\frac{l}{2}\right) = \lim_{x\to\frac{l}{2}} \boldsymbol{S}en'(x) = \lim_{x\to\frac{l}{2}} \boldsymbol{C}os(x) = \boldsymbol{C}os\left(\frac{l}{2}\right)$$

e

$$\boldsymbol{C}os'\left(\frac{l}{2}\right) = \lim_{x\to\frac{l}{2}} \boldsymbol{C}os'(x) = \lim_{x\to\frac{l}{2}} -\boldsymbol{S}en(x) = -\boldsymbol{S}en\left(\frac{l}{2}\right)$$

como queríamos provar. ■

Agora, vamos estender as funções $\boldsymbol{S}en$ e $\boldsymbol{C}os$ ao intervalo $[0, 2l]$. Estes prolongamentos serão feitos de modo a assegurar simetria dos gráficos relativamente ao ponto $(l, 0)$ e à recta $x = l$, respectivamente. Sejam

$$\mathcal{S}en(x) = \begin{cases} \boldsymbol{S}en(x) & \text{se} \quad x \in [0, l] \\ -\boldsymbol{S}en(2l - x) & \text{se} \quad x \in [l, 2l] \end{cases}$$

e

$$\mathcal{C}os\,(x) = \begin{cases} \boldsymbol{C}os\,(x) & \text{se} \quad x \in [0, l] \\ \boldsymbol{C}os\,(2l - x) & \text{se} \quad x \in [l, 2l] \end{cases} .$$

Estas funções são diferenciáveis em todo o intervalo $]0, 2l[$ e por argumento idêntico ao lema (1.3.2) têm em 0 e em $2l$ derivadas laterais finitas que verificam as igualdade da proposição (1.3.1).

Finalmente, prolonguemos as funções a toda a recta real de modo a obter funções periódicas de período $2l$.

Lema 1.3.3 $\mathbb{R} = \dot{\bigcup}_{i \in \mathbb{Z}} [2li, 2l\,(i+1)[$.

Prova. Seja $x \in \mathbb{R}$. Queremos encontrar i inteiro tal que $2li \leq x < 2l\,(i+1)$, isto é, $i \leq \frac{x}{2l} < i + 1$. Basta considerar $i = \left[\frac{x}{2l}\right]$ e este é mesmo o único inteiro que serve. ■

Por outras palavras, o lema anterior afirma que a recta real pode decompor-se em subintervalos disjuntos de amplitude $2l$. Deste modo, para qualquer número real, é possível encontrar um único elemento no intervalo $[0, 2l[$ que difere do primeiro num múltiplo de $2l$, isto é,

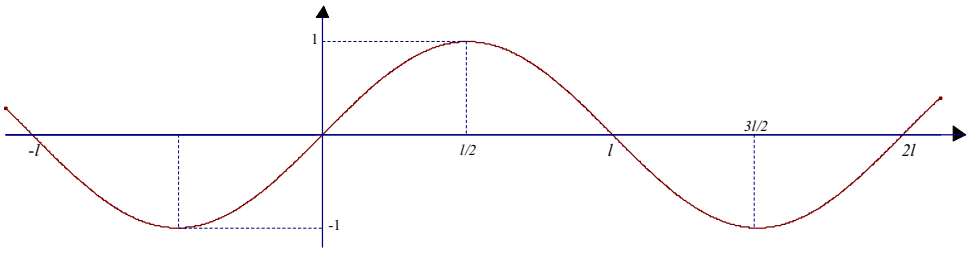
$$\forall x \in \mathbb{R} \quad \exists' k \in \mathbb{Z} : x + 2kl \in [0, 2l[\,.$$

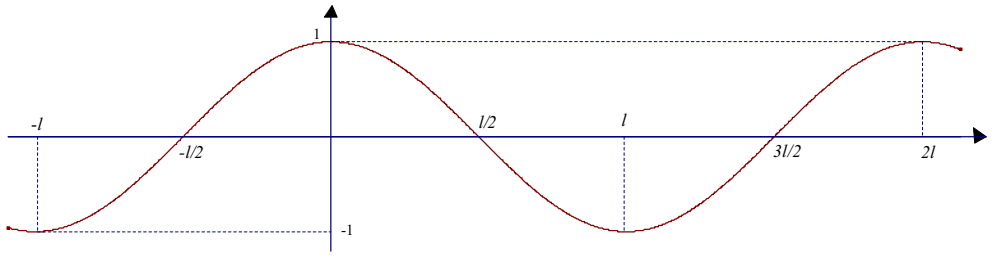
Assim, podemos definir

$$sen\,(x) = \mathcal{S}en\,(x + 2kl)$$

$$\cos\,(x) = \mathcal{C}os\,(x + 2kl)\,.$$

Por construção, estas funções são periódicas de período $2l$ e diferenciáveis. A estas funções chamamos respectivamente, **seno** e **cosseno trigonométricos** e os seus gráficos são os seguintes:



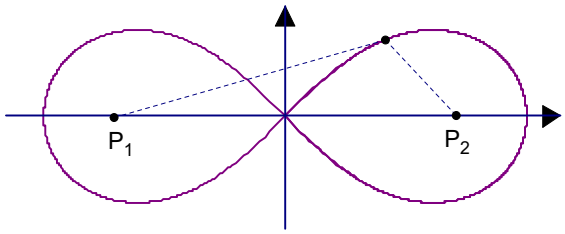


É possível provar que $l = \pi$, onde π é a razão entre o perímetro e o diâmetro de qualquer circunferência (detalhes em [Moise]) e portanto a circunferência unitária tem perímetro igual a $4AS\,(1) = 2l$.

Capítulo 2

A lemniscata

Neste capítulo, iremos descrever a lemniscata e calcular o seu comprimento para posteriormente construir uma função, com características idênticas às da função seno trigonométrico, associada a esta curva.



2.1 Descrição da lemniscata

A lemniscata é descrita pelo conjunto de pontos do plano cujo produto das distâncias a dois pontos fixos, P_1 e P_2, é constante. Seja d a métrica euclidiana e consideremos

$$P_1 = \left(-\frac{1}{\sqrt{2}}, 0\right) \quad \text{e} \quad P_2 = \left(\frac{1}{\sqrt{2}}, 0\right).$$

A lemniscata, que usaremos no que se segue, é o conjunto dos pontos do plano que verificam a condição

$$\left\{(x,y) \in \mathbb{R}^2 : d\left((x,y), P_1\right) \cdot d\left((x,y), P_2\right) = \frac{1}{2}\right\},$$

isto é, o conjunto dos pontos que satisfazem a igualdade

$$\left(x^2+y^2\right)^2-\left(x^2-y^2\right)=0. \tag{2.1}$$

Para que o conjunto de pontos que verifica a equação acima não seja vazio, x^2-y^2 tem que ser não negativo, o que permite concluir que a lemniscata é uma curva definida no cone determinado pelas condições

$$-x\leq y\leq x \quad \vee \quad x\leq y\leq -x.$$

Seja (x,y) um ponto do plano euclidiano. Então existem $r\in\mathbb{R}_0^+$ e $\theta\in[0,2\pi[$ tais que

$$x=r\cos\theta \quad \text{e} \quad y=r\sin\theta.$$

Se o ponto (x,y) satisfaz a igualdade (2.1) então $r^4=r^2\cos(2\theta)$, isto é, $r=0$ ou $r^2=\cos(2\theta)$. E portanto, em coordenadas polares, a lemniscata é representada pelo conjunto

$$\left\{(r,\theta)\in\mathbb{R}_0^+\times[0,2\pi[\,:r^2=\cos(2\theta)\right\}.$$

Para que o conjunto anterior seja diferente do conjunto vazio, é necessário impor condições à variável θ de modo a garantir que $\cos(2\theta)$ seja não negativo:

$$\theta\in\left[0,\frac{\pi}{4}\right]\cup\left[\frac{3\pi}{4},\frac{5\pi}{4}\right]\cup\left[\frac{7\pi}{4},2\pi\right[.$$

Este conjunto representa precisamente o cone de definição da lemniscata em coordenadas polares.

2.2 Comprimento da lemniscata

Como vimos na secção anterior, a equação que define a lemniscata em coordenadas cartesianas é

$$\left(x^2+y^2\right)^2-\left(x^2-y^2\right)=0.$$

Esta curva possui simetria relativamente aos dois eixos coordenados. Assim, para conhecer o comprimento da lemniscata é suficiente calcular o seu valor num dos quadrantes. Porém o cálculo torna-se mais simples se usarmos a

descrição polar da curva. Ora, no primeiro quadrante a lemniscata é descrita pela equação

$$r^2 = \cos(2\theta), \qquad \theta \in \left[0, \frac{\pi}{4}\right]. \tag{2.2}$$

Derivando implicitamente ambos os membros de (2.2) em ordem a θ, obtemos

$$\frac{dr}{d\theta} = -\frac{\sin 2\theta}{\sqrt{\cos 2\theta}}$$

e portanto o comprimento da lemniscata, que designaremos por 2ω, é dado por

$$4\int_0^{\frac{\pi}{4}} \sqrt{r^2 + \left(\frac{dr}{d\theta}\right)^2}\, d\theta = 4\int_0^{\frac{\pi}{4}} \frac{1}{\sqrt{\cos 2\theta}} d\theta.$$

(À semelhança do que aconteceu para a circunferência também na lemniscata o seu comprimento, no primeiro quadrante, é dado por um integral impróprio.) Recorrendo à mudança de variável $r = \sqrt{\cos 2\theta}$ obtemos

$$2\omega = 4\int_0^1 \frac{1}{\sqrt{1-r^4}} dr.$$

Este tipo de integral foi amplamente estudado nos séculos XVIII e XIX no âmbito da teoria dos integrais elípticos. É possível provar que a função $\frac{1}{\sqrt{1-r^4}}$ não tem primitiva elementar (detalhes em [Ritt]). No entanto, vamos descrever um algoritmo elementar que permite calcular valores aproximados do integral acima.

2.2.1 O algoritmo da média aritmética-geométrica

Dados dois números positivos a e b, o algoritmo da média aritmética-geométrica transforma-os num par de sucessões $(a_n)_n$ e $(b_n)_n$ definidas recursivamente por

$$a_0 = a \qquad\qquad b_0 = b$$

$$a_{n+1} = \frac{a_n + b_n}{2} \qquad\qquad b_{n+1} = \sqrt{a_n b_n}.$$

Estas sucessões são órbitas de um sistema dinâmico: se considerarmos a função

$$\begin{array}{rccc} H: & \mathbb{R}^+ \times \mathbb{R}^+ & \longrightarrow & \mathbb{R}^+ \times \mathbb{R}^+ \\ & (a,b) & \mapsto & \left(\dfrac{a+b}{2}, \sqrt{ab}\right) \end{array}$$

e a aplicarmos sucessivamente ao par ordenado $(a,b) \in \mathbb{R}^+ \times \mathbb{R}^+$, obtemos a sucessão $\left(H^n(a,b)\right)_n = (a_n, b_n)_n$. Questões naturais sobre o comportamento das suas órbitas são:

1. A sucessão $\left(H^n(a,b)\right)_n$ converge em $\mathbb{R}^+ \times \mathbb{R}^+$?

2. A sucessão $\left(H^n(a,b)\right)_n$ converge para um ponto fixo de H?

Dada a recorrência associada à iteração de H, que define estas sucessões, podemos responder às duas questões analisando apenas a primeira, uma vez que se a primeira pergunta tiver resposta positiva, então a segunda também porque H é uma função contínua.

Se (α, β) é um ponto fixo de H, isto é, $H(\alpha,\beta) = (\alpha,\beta)$, então α e β verificam

$$\left\{ \begin{array}{c} \frac{\alpha+\beta}{2} = \alpha \\ \sqrt{\alpha\beta} = \beta \end{array} \right. \qquad \left\{ \begin{array}{c} \alpha+\beta = 2\alpha \\ \alpha\beta = \beta^2 \end{array} \right. \qquad \alpha = \beta.$$

Portanto, se a órbita de (a,b) por H for convergente em $\mathbb{R}^+ \times \mathbb{R}^+$, então converge para um ponto fixo de H que tem as duas componentes iguais, o que significa que as sucessões $(a_n)_n$ e $(b_n)_n$ têm o mesmo limite.

Proposição 2.2.1 *Dados quaisquer números positivos a e b, as sucessões $(a_n)_n$ e $(b_n)_n$ definidas como atrás são convergentes.*

Prova. No caso em que $a = b$ as sucessões $(a_n)_n$ e $(b_n)_n$ são constantes. Suponhamos que $a > b$. Para qualquer $n \in \mathbb{N}_0$, valem as seguintes desigualdades:

i) $b_n < a_n$

Por hipótese, a desigualdade é válida para $n = 0$. Suponhamo-la válida para $n = p$ e provemos que a desigualdade ainda vale para $n = p + 1$.

Ora,

$$\begin{aligned} b_{p+1} < a_{p+1} &\Leftrightarrow \sqrt{a_p b_p} < \frac{a_p + b_p}{2} \\ &\Leftrightarrow 4a_p b_p < (a_p + b_p)^2 \\ &\Leftrightarrow (a_p - b_p)^2 > 0 \end{aligned}$$

e $a_p - b_p > 0$. E portanto, por indução sobre $\mathbb{N}$, a desigualdade $b_n < a_n$ é sempre válida.

ii) $b_n < b_{n+1}$

Por definição da sucessão $(b_n)_n$ temos que

$$\begin{aligned} b_n < b_{n+1} &\Leftrightarrow b_n < \sqrt{a_n b_n} \\ &\Leftrightarrow (b_n)^2 < a_n b_n \\ &\Leftrightarrow b_n < a_n \end{aligned}$$

pois os elementos da sucessão $(b_n)_n$ são estritamente positivos (implícito na sua definição). Logo a desigualdade $b_n < b_{n+1}$ decorre de i).

iii) $a_{n+1} < a_n$

Esta desigualdade é consequência de i) pois

$$\begin{aligned} a_{n+1} < a_n &\Leftrightarrow a_n + b_n < 2a_n \\ &\Leftrightarrow b_n < a_n. \end{aligned}$$

As desigualdades anteriores mostram que a sucessão $(b_n)_n$ é crescente e majorada por a e que a sucessão $(a_n)_n$ é decrescente e minorada por b, logo ambas as sucessões são convergentes. ■

Notação 2.2.2 *O limite comum das sucessões $(a_n)_n$ e $(b_n)_n$ designa-se por* ***média arimética-geométrica*** *e será denotado por $mag\,(a, b)$.*

Determinar a média arimética-geométrica de dois números positivos é um processo relativamente rápido.

Proposição 2.2.3 *O algoritmo da média arimética-geométrica é quadraticamente convergente.*

Prova. Comecemos por observar que, dados números positivos a e b,

$$a_{n+1}^2 - b_{n+1}^2 = \frac{(a_n - b_n)^2}{4} \tag{2.3}$$

pois

$$\begin{aligned} a_{n+1}^2 - b_{n+1}^2 &= \left(\frac{a_n + b_n}{2}\right)^2 - a_n b_n \\ &= \frac{(a_n + b_n)^2 - 4a_n b_n}{4} \\ &= \frac{(a_n - b_n)^2}{4}. \end{aligned}$$

Dividindo ambos os membros de (2.3) por $a_{n+1} + b_{n+1} = 2a_{n+2}$ obtemos

$$a_{n+1} - b_{n+1} = \frac{(a_n - b_n)^2}{8a_{n+2}}.$$

Como a sucessão $(a_n)_n$ é decrescente e converge para $mag\,(a,b)$, segue que, para todo n

$$a_{n+1} - b_{n+1} \leq \frac{(a_n - b_n)^2}{mag\,(a,b)}.$$

Logo a sucessão $(a_n - b_n)_n$ converge a uma taxa quadrática para zero, e portanto se tomarmos a_n como valor aproximado de $mag\,(a,b)$, o número de casas decimais certas desta aproximação é essencialmente duplicado após cada iteração do algoritmo. ■

2.2.2 Teorema de Gauss

O integral que permite calcular o comprimento da lemniscata relaciona-se com os que aparecem no enunciado do Teorema de Gauss:

Teorema 2.2.4 (de Gauss) *Para quaisquer números positivos a e b,*

$$\int_{-\infty}^{+\infty} \frac{dx}{\sqrt{(x^2 + a^2)\,(x^2 + b^2)}} = \frac{\pi}{mag\,(a,b)}.$$

Este teorema é a chave para o cálculo do comprimento da lemniscata. De facto, aplicando este teorema aos valores $a = 1$ e $b = \sqrt{2}$, temos que

$$\int_0^{+\infty} \frac{dx}{\sqrt{(x^2+1)(x^2+2)}} = \frac{\pi}{2mag\left(1,\sqrt{2}\right)}$$

pois a função integranda é par. Além disso, recorrendo à mudança de variável $x = \frac{\sqrt{1-r^2}}{r}$ onde $r \in]0,1]$, obtemos a igualdade

$$\int_0^{+\infty} \frac{dx}{\sqrt{(x^2+1)(x^2+2)}} = \int_0^1 \frac{dr}{\sqrt{1-r^4}}.$$

Por isso, o comprimento da lemniscata, que é dado por

$$4\int_0^1 \frac{dr}{\sqrt{1-r^4}} = \frac{2\pi}{mag\left(1,\sqrt{2}\right)}.$$

Logo $\omega = \frac{\pi}{mag\left(1,\sqrt{2}\right)}$. Implementando o algoritmo da média aritmética-geométrica, descrito na secção anterior, obtemos com apenas 4 iterações, $1.1981402347355922074\ldots$ como valor aproximado de $mag\left(1,\sqrt{2}\right)$ com todas as casas decimais aqui inscritas correctas. E portanto o comprimento total da lemniscata é aproximadamente $5.2428\ldots$.

Prova do Teorema de Gauss. Defina-se

$$I(a,b) = \int_{-\infty}^{+\infty} \frac{dx}{\sqrt{(x^2+a^2)(x^2+b^2)}}.$$

Se substituirmos a e b, respectivamente, pela média aritmética e geométrica destes dois valores, o valor de I permanece inalterado, isto é,

$$I(a,b) = I\left(\frac{a+b}{2}, \sqrt{ab}\right). \tag{2.4}$$

Ora

$$I\left(\frac{a+b}{2}, \sqrt{ab}\right) = \int_{-\infty}^{+\infty} \frac{dt}{\sqrt{\left(t^2 + \left(\frac{a+b}{2}\right)^2\right)(t^2+ab)}}.$$

Para prosseguir o cálculo deste integral usaremos para mudança de variável a bijecção $t:\ \mathbb{R}^+ \ \rightarrow\ \mathbb{R}$ definida por $t\left(x\right)=\frac{1}{2}\left(x-\frac{ab}{x}\right)$. Assim, temos

$$\begin{aligned}\int_0^{+\infty}\frac{dt}{\sqrt{\left(t^2+\left(\frac{a+b}{2}\right)^2\right)\left(t^2+ab\right)}} &= \lim_{p\rightarrow+\infty}\int_0^{p}\frac{dt}{\sqrt{\left(t^2+\left(\frac{a+b}{2}\right)^2\right)\left(t^2+ab\right)}}\\ &= \lim_{p\rightarrow+\infty}\int_{\sqrt{ab}}^{p+\sqrt{p^2+ab}}\frac{2dx}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}\\ &= \int_{\sqrt{ab}}^{+\infty}\frac{2dx}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}\end{aligned}$$

e

$$\begin{aligned}\int_{-\infty}^{0}\frac{dt}{\sqrt{\left(t^2+\left(\frac{a+b}{2}\right)^2\right)\left(t^2+ab\right)}} &= \lim_{p\rightarrow-\infty}\int_{p+\sqrt{p^2+ab}}^{\sqrt{ab}}\frac{2dx}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}\\ &= \int_{0}^{\sqrt{ab}}\frac{2dx}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}.\end{aligned}$$

Logo

$$I\left(\frac{a+b}{2},\sqrt{ab}\right)=\int_0^{+\infty}\frac{2dx}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}.$$

A igualdade (2.4) resulta agora de observar que a função integranda é par, pelo que

$$\int_0^{+\infty}\frac{2dx}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}=\int_{-\infty}^{+\infty}\frac{dx}{\sqrt{\left(x^2+a^2\right)\left(x^2+b^2\right)}}$$

sendo este último, por definição, o valor de $I\left(a,b\right)$.

A igualdade (2.4) aplicada sucessivamente, mostra-nos que a sucessão $\left(I\left(a_n,b_n\right)\right)_n$ é constante e portanto

$$I\left(a,b\right)=\lim_{n\rightarrow\infty}I\left(a_n,b_n\right).$$

Se a função I for contínua, então podemos calcular o valor de $I(a,b)$ facilmente pois nesse caso

$$I(a,b) = I\left(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\right)$$

e, pela proposição (2.2.1), sabemos que as sucessões $(a_n)_n$ e $(b_n)_n$ são convergente para $mag(a,b)$, logo

$$\begin{aligned} I(a,b) &= I(mag(a,b), mag(a,b)) \\ &= \int_{-\infty}^{+\infty} \frac{dx}{x^2 + mag^2(a,b)} \\ &= 2\lim_{p\to+\infty} \frac{1}{mag(a,b)} arctg\left(\frac{p}{mag(a,b)}\right) \\ &= \frac{\pi}{mag(a,b)} \end{aligned}$$

o que concluiria a prova.

À função I aplica-se a proposição seguinte:

Proposição 2.2.5 *Seja* $f: \mathbb{R}\times U \to \mathbb{R}$ *onde* $U \subset \mathbb{R}^2$ *é um aberto. Se se verificarem as seguintes condições:*

1. *Para cada* $y \in U$, *a função* $x \mapsto f(x,y)$ *é integrável.*
2. *Para cada* $x \in \mathbb{R}$ *e* $y_0 \in U$, $\lim_{y\to y_0} f(x,y) = f(x,y_0)$.
3. *Existe uma função* $f_1: \mathbb{R} \to \mathbb{R}$ *integrável tal que, para qualquer* $(x,y) \in \mathbb{R}\times U$, $|f(x,y)| \le |f_1(x)|$

Então a função $y \longmapsto \int_{-\infty}^{+\infty} f(x,y)\,dx$ *é contínua.*

Prova. Seja $(y_k)_k$ uma sucessão de elementos de U convergente para y. Defina-se $f_k(x) = f(x,y_k)$. Por hipótese, para cada $x \in \mathbb{R}$, a sucessão de funções $\{f_k\}_k$ converge pontualmente para a função $f(x,y)$, e existe uma função integrável, f_1, que majora cada elemento da sucessão $\{f_k\}_k$. Logo

$$\int_{-\infty}^{+\infty} f(x,y)\,dx = \lim_{k\to\infty} \int_{-\infty}^{+\infty} f(x,y_k)\,dx$$

pelo Teorema da Convergência Dominada (vide [Kolmogorov]). ■

Retomemos a prova do Teorema de Gauss. Defina-se

$$\begin{array}{rccc} f: & \mathbb{R}\times(\mathbb{R}^+\times\mathbb{R}^+) & \to & \mathbb{R} \\ & (x,a,b) & \mapsto & \frac{1}{\sqrt{(x^2+a^2)(x^2+b^2)}} \end{array}.$$

Se esta função verificar as condições da proposição anterior, então fica provada a continuidade da função I.

1. Para cada $(a,b)\in\mathbb{R}^+\times\mathbb{R}^+$, a função $x\mapsto f(x,a,b)$ é integrável.

   Suponhamos que $a\geq b$. Então

   $$\begin{aligned} \int_{-\infty}^{+\infty}\frac{dx}{\sqrt{(x^2+a^2)(x^2+b^2)}} &= \lim_{p\to+\infty}\int_0^p\frac{2dx}{\sqrt{(x^2+a^2)(x^2+b^2)}} \\ &\leq \lim_{p\to+\infty}\int_0^p\frac{2dx}{x^2+b^2} \\ &= \frac{\pi}{b}. \end{aligned}$$

   (No caso em que $a<b$, a prova é perfeitamente analoga).

2. Para cada $x\in\mathbb{R}$ e $(\alpha,\beta)\in\mathbb{R}^+\times\mathbb{R}^+$, $\lim\limits_{(a,b)\to(\alpha,\beta)} f(x,a,b)=f(x,\alpha,\beta)$.

   Esta afirmação resulta da função f ser contínua nas variáveis a e b.

3. Atendendo a que a noção de continuidade é um conceito local, a terceira condição da proposição (2.2.5) pode ser enfraquecida sem que se perca informação quanto à sua conclusão. Podemos reescrevê-la, no contexto do Teorema de Gauss, do seguinte modo:

   Para qualquer $(a,b)\in\mathbb{R}^+\times\mathbb{R}^+$, *existe uma função* $f_1:\ \mathbb{R}\ \to\ \mathbb{R}$ *integrável e uma vizinhança aberta de* (a,b), $U_{(a,b)}$, *tal que* $|f(x,\alpha,\beta)|\leq|f_1(x)|$, *para todo* $(x,\alpha,\beta)\in\mathbb{R}\times U_{(a,b)}$.

Seja $(a,b) \in \mathbb{R}^+ \times \mathbb{R}^+$. Consideremos o aberto

$$U_{(a,b)} = \left\{ (\alpha,\beta) \in \mathbb{R}^+ \times \mathbb{R}^+ : \alpha > \frac{a}{2} \quad \wedge \quad \beta > \frac{b}{2} \right\},$$

faça-se $c = \min\left\{\frac{a}{2}, \frac{b}{2}\right\}$ e $f_1(x) = \frac{1}{x^2+c^2}$ para todo x de $\mathbb{R}$. A função f_1 é integrável em $\mathbb{R}$ pois $\int_{-\infty}^{+\infty} f_1 = \frac{\pi}{c}$ e para todo o (α,β) de $U_{(a,b)}$,

$$\begin{aligned} f(x,\alpha,\beta) &= \frac{1}{\sqrt{(x^2+\alpha^2)\left(x^2+\beta^2\right)}} \\ &< \frac{1}{\sqrt{\left(x^2+\left(\frac{a}{2}\right)^2\right)\left(x^2+\left(\frac{b}{2}\right)^2\right)}} \\ &\leq \frac{1}{x^2+c^2}. \end{aligned}$$

A proposição (2.2.5), aplicada a $U_{(a,b)}$, f e f_1, permite concluir que a função

$$I : (a,b) \longrightarrow \int_{-\infty}^{+\infty} \frac{dx}{\sqrt{(x^2+a^2)(x^2+b^2)}}$$

é contínua. ■

Capítulo 3

Seno da lemniscata

Consideremos a função

$$x \mapsto \int_0^x \frac{dr}{\sqrt{1-r^4}}$$

definida em $[0,1]$. Por analogia com o que vimos no primeiro capítulo, designaremos esta função por *arco seno da lemniscata* e denotá-la-emos por ASL. Tal como foi feito para a circunferência, neste capítulo construiremos uma função com propriedades semelhantes à função seno trigonométrico a partir da função ASL.

3.1 Construção da função seno da lemniscata em $\left[0, \frac{\omega}{2}\right]$

Recorde-se do capítulo anterior, secção 2.2, que estamos a usar a notação $ASL\,(1) = \frac{\omega}{2}$.

Pelo Teorema Fundamental do Cálculo, a função ASL é contínua, derivável e

$$ASL'\,(x) = \frac{1}{\sqrt{1-x^4}}$$

para qualquer $x \in \,]0,1[$. Sendo ASL' positiva em $]0,1[$, a função ASL é estritamente crescente e consequentemente injectiva. O Teorema do Valor Intermédio afirma que para cada $x \in \left[0, \frac{\omega}{2}\right]$ existe um y em $[0,1]$ tal que

$$ASL\,(y) = x.$$

Decorre da injectividade da função ASL que um tal y é único. Designá-lo-emos por $\mathfrak{s}enlem\,(x)$. A unicidade de tal valor permite definir a função

$$\mathfrak{s}enlem: \quad \left[0, \tfrac{\omega}{2}\right] \quad \rightarrow \quad [0,1] \ .$$

Esta função goza ainda das seguintes propriedades:

- $\mathfrak{s}enlem$ é estritamente crescente

  As funções ASL e $\mathfrak{s}enlem$ são inversas e portanto têm o mesmo tipo de monotonia.

- $\mathfrak{s}enlem$ é uma função contínua

  A continuidade da função $\mathfrak{s}enlem$ decorre da função ASL ser contínua, injectiva e estar definida num intervalo.

- $\mathfrak{s}enlem$ é uma função diferenciável

  A função ASL é derivável em todo o intervalo $]0,1[$ e a sua derivada é sempre não nula, logo o Teorema da Derivada da Função Inversa garante que a função $\mathfrak{s}enlem$ é diferenciável e que

  $$\begin{aligned} \mathfrak{s}enlem'\,(x) &= \frac{1}{ASL'\,(\mathfrak{s}enlem\,(x))} \\ &= \sqrt{1-\mathfrak{s}enlem^4\,(x)} \end{aligned}$$

  para qualquer x do intervalo $\left]0, \tfrac{\omega}{2}\right[$.

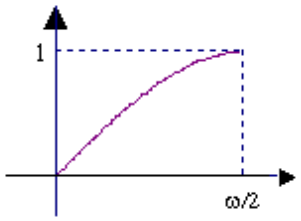
- $\mathfrak{s}enlem$ tem concavidade voltada para baixo

  Derivando duas vezes a função $\mathfrak{s}enlem$, obtemos

  $$\mathfrak{s}enlem''\,(x) = -2\mathfrak{s}enlem^3\,(x)$$

  de onde se deduz que $\mathfrak{s}enlem''$ é negativa em todo o intervalo $\left]0, \tfrac{\omega}{2}\right[$.

Esta informação permite-nos traçar o gráfico da função $\mathfrak{s}enlem$ no intervalo $\left[0, \frac{\omega}{2}\right]$



3.2 Prolongamento da função seno da lemniscata a $\mathbb{R}$

O prolongamento da função $\mathfrak{s}enlem$ à recta real será feito em várias etapas. Primeiro, estendemos a função $\mathfrak{s}enlem$ ao intervalo $[0, \omega]$ de modo que no intervalo $\left[\frac{\omega}{2}, \omega\right]$ tome os mesmos valores que em $\left[0, \frac{\omega}{2}\right]$ mas por ordem inversa. Esta imposição faz com que o gráfico da função obtida seja simétrico relativamente à recta $x = \frac{\omega}{2}$:

$$\mathbf{S}enlem\,(x) = \begin{cases} \mathfrak{s}enlem\,(x) & \text{se} \quad x \in \left[0, \frac{\omega}{2}\right] \\ \mathfrak{s}enlem\,(\omega - x) & \text{se} \quad x \in \left[\frac{\omega}{2}, \omega\right] \end{cases} .$$

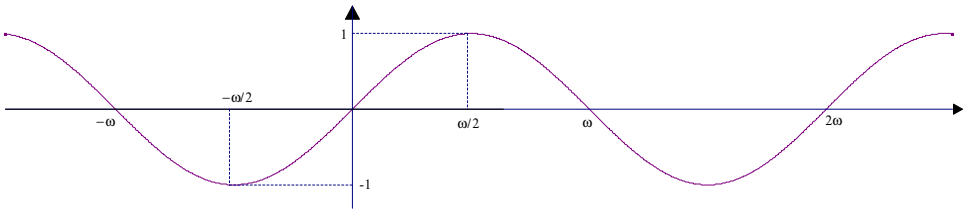
Esta função é diferenciável em todo o intervalo $]0, \omega[$. De seguida, estendemos a função $\boldsymbol{S}enlem$ ao intervalo $[0, 2\omega]$ por forma que o gráfico da função obtida seja simétrico em relação ao ponto $(\omega, 0)$:

$$\mathcal{S}enlem\,(x) = \begin{cases} \mathbf{S}enlem\,(x) & \text{se} \quad x \in [0, \omega] \\ -\mathbf{S}enlem\,(2\omega - x) & \text{se} \quad x \in [\omega, 2\omega] \end{cases} .$$

Finalmente, prolongamos esta função à recta real, de modo a obter uma função periódica de período 2ω. Uma vez que o conjunto dos números reais é decomponível em intervalos disjuntos de amplitude 2ω, para cada $x \in \mathbb{R}$ existe um único k inteiro tal que $x + 2\omega k \in [0, 2\omega[$ e, podemos definir

$$senlem\,(x) = \mathcal{S}enlem\,(x + 2\omega k)\,.$$

Por construção, esta função nasce periódica de período 2ω e é diferenciável; designá-la-emos por **seno da lemniscata** e o seu gráfico é



Capítulo 4

Funções elípticas

Este é um capítulo de apoio ao resto do texto. Trata-se de uma abordagem geral às funções elípticas, com destaque para as propriedades da função $\mathcal{P}$ de Weierstrass. Seguiremos de perto a referência [Lang73].

Consideremos dois números complexos, ω_1 e ω_2, linearmente independentes sobre o espaço vectorial dos números complexos sobre o corpo dos números reais. Seja

$$\begin{aligned} \Lambda &= <\omega_{1,}\omega_2> \\ &= \{n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}\} \end{aligned}$$

a rede associada a esses números. Uma função meromorfa de $\mathbb{C}$, f, diz-se uma **função elíptica em relação à rede** Λ se, para quaisquer z do domínio de f e $\lambda \in \Lambda$, verificar a igualdade

$$f(z+\lambda) = f(z).$$

Os elementos de Λ são **períodos** de f.

Como exemplo de funções elípticas temos as funções constantes. Estas são-no em relação a qualquer rede.

Se f e g são duas funções elípticas então também o são as funções $f+g$, $f-g$, $f.g$, e $\frac{f}{g}$ (se g não for identicamente nula).

Proposição 4.0.1 *O conjunto das funções elípticas em relação a uma rede Λ constitui um corpo com as operações usuais de adição e multiplicação de funções.*

O corpo das funções elípticas em relação a uma rede Λ denotar-se-á por $\mathfrak{M}(\Lambda)$.

Uma vez que os elementos da rede Λ são combinações inteiras de ω_1 e ω_2, a verificação da Λ-periodicidade pode fazer-se apenas para os dois períodos ω_1 e ω_2.

Proposição 4.0.2 *Uma função f é elíptica em relação à rede Λ se e somente se, para qualquer z do domínio de f,*

$$f(z) = f(z + \omega_1) \tag{4.1}$$

e

$$f(z) = f(z + \omega_2) \tag{4.2}$$

Prova. Se f é elíptica em relação à rede Λ então ω_1 e ω_2 são períodos de f e temos as igualdades (4.1) e (4.2). Por outro lado, se se verificarem estas igualdades então também temos

$$f(z) = f(z - \omega_1) \tag{4.3}$$

e

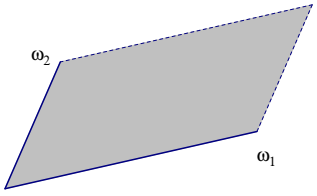
$$f(z) = f(z - \omega_2) \tag{4.4}$$

pois $f(z) = f((z - \omega_i) + \omega_i) = f(z - \omega_i)$ para $i = 1$ ou 2. Assim, para qualquer $\lambda = n\omega_1 + m\omega_2 \in \Lambda$, basta aplicar um número finito de vezes as igualdades (4.1),(4.2),(4.3) e (4.4) para verificar que f é elíptica. ■

Outra simplificação: pela periodicidade, para estudar as funções elípticas é suficiente cingirmo-nos à parte do seu domínio definida por

$$D(\Lambda) = \{r\omega_1 + s\omega_2 : 0 \leq r < 1, 0 \leq s < 1\}.$$

Os pontos deste conjunto determinam no plano complexo um paralelogramo designado por **paralelogramo fundamental**.



Para cada $z \in \mathbb{C}$ existe um único representante em $D(\Lambda)$, que denotaremos por (z), tal que $z - (z) \in \Lambda$. De facto, como por hipótese ω_1 e ω_2 são linearmente independentes em $\mathbb{R}^2$, geram $\mathbb{R}^2$ e, portanto, dado $z \in \mathbb{C}$ existem reais α e β tais que $z = \alpha\omega_1 + \beta\omega_2$. Logo podemos reescrever z da seguinte forma:

$$\begin{aligned} z &= \alpha\omega_1 + \beta\omega_2 \\ &= ([\alpha] + (\alpha - [\alpha]))\,\omega_1 + ([\beta] + (\beta - [\beta]))\,\omega_2 \\ &= (\alpha - [\alpha])\,\omega_1 + (\beta - [\beta])\,\omega_2 + [\alpha]\,\omega_1 + [\beta]\,\omega_2 \\ &= (z) + (z - (z)) \end{aligned}$$

onde $(z) = (\alpha - [\alpha])\,\omega_1 + (\beta - [\beta])\,\omega_2 \in D(\Lambda)$ e $z - (z) = [\alpha]\,\omega_1 + [\beta]\,\omega_2 \in \Lambda$. Logo, se f é elíptica, $f(z) = f((z))$.

Tal como já foi observado, as funções constantes fazem parte de $\mathfrak{M}(\Lambda)$. Importa agora saber se existem outras funções para além destas.

4.1 Propriedades das funções elípticas não constantes

Vamos mostrar algumas propriedades a que devem obedecer as funções elípticas não constantes.

Proposição 4.1.1 *Seja $f \in \mathfrak{M}(\Lambda)$ uma função sem pólos em $D(\Lambda)$. Então f é constante.*

Prova. Se a função f não tem pólos em $D(\Lambda)$, então por periodicidade também não tem pólos em $\mathbb{C}$. Logo f é uma função contínua em $\mathbb{C}$ e, em particular, no fecho de $D(\Lambda)$ que é um compacto. Mas então f é uma função limitada em $D(\Lambda)$ e consequentemente em $\mathbb{C}$. Logo, pelo Teorema de Liouville f é uma função constante. ■

Resulta desta proposição que as funções elípticas não constantes, caso existam, têm necessariamente pólos.

Proposição 4.1.2 *Se $f \in \mathfrak{M}(\Lambda)$, então a soma dos seus resíduos é zero.*

Prova. Comecemos por mostrar que este resultado é válido no caso em que f não tem pólos na fronteira de $D(\Lambda)$. Suponhamos que os geradores

da rede Λ, ω_1 e ω_2, constituem base directa. Assim a fronteira de $D(\Lambda)$, $\partial D(\Lambda)$, é a união dos caminhos C_1, C_2, C_3 e C_4 onde C_1 une 0 a ω_1, C_2 une ω_1 a $\omega_1+\omega_2$, C_3 une $\omega_1+\omega_2$ a ω_2 e finalmente C_4 une ω_2 a 0. Pelo Teorema dos Resíduos, a soma dos resíduos de f em $D(\Lambda)$ é

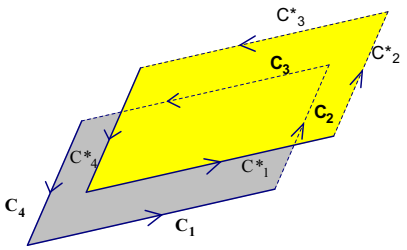
$$r = \frac{1}{2\pi i}\int_{\partial D(\Lambda)} f.$$

Atendendo à periodicidade de f, temos que

$$\int_{C_1} f = -\int_{C_3} f \quad \text{e} \quad \int_{C_2} f = -\int_{C_4} f$$

e portanto $r = 0$.

Se f tiver pólos na fronteira de $D(\Lambda)$, como tem um número finito deles, podemos reduzir este caso ao anterior começando por fazer uma translação de $\partial D(\Lambda)$ para $(\partial D(\Lambda))^* = C_1^* \vee C_2^* \vee C_3^* \vee C_4^*$, como sugere a figura,



de modo a que os pólos de f fiquem no interior de $(\partial D(\Lambda))^*$. ■

Esta proposição afirma que a existirem funções elípticas não constantes, estas terão que ter pelo menos dois pólos, distintos ou não, em $D(\Lambda)$, pois caso contrário, a soma dos resíduos seria não nula.

O resultado que se segue permite relacionar o número de pólos de uma função elíptica não constante com o número de zeros.

Proposição 4.1.3 *Seja $f \in \mathfrak{M}(\Lambda)$ uma função não constante que, em $D(\Lambda)$, admite como zeros os pontos a_1, a_2, ..., a_r e os seguintes pólos a_{r+1}, a_{r+2}, ..., a_{r+s}. Se m_i é a ordem do zero/pólo a_i, para todo $i = 1, 2, \ldots, r+s$, então*

$$\sum_{i=1}^{r+s} m_i = 0.$$

Ou seja, o número de zeros é igual ao número de pólos, se a contagem dos pontos singulares for feita de acordo com as respectivas multiplicidades.

Prova. A derivada de uma função elíptica é ainda uma função elíptica. A proposição (4.1.2) aplicada à função $\frac{f'}{f} \in \mathfrak{M}(\Lambda)$ afirma que a soma dos seus resíduos é nula.

Sem perda de generalidade podemos supor que f não tem zeros nem pólos na fronteira de $D(\Lambda)$ pois, caso contrário, começamos por usar o argumento explicitado no fim da prova da proposição (4.1.2). Neste caso a soma dos resíduos da função $\frac{f'}{f}$ é a diferença entre o número de zeros e o número de pólos de f, em $D(\Lambda)$, contados de acordo com as respectivas multiplicidades (vide [Coimbra], página 231). Logo estes dois números são iguais. ■

Conhecendo-se a soma dos zeros (respectivamente pólos) de uma função elíptica não constante é possível saber a soma dos seus pólos (respectivamente zeros) a menos de uma constante. De facto,

Proposição 4.1.4 *A soma dos zeros de uma função elíptica não constante é igual à soma dos seus pólos a menos de um período.*

Prova. Seja f uma função elíptica não constante sem zeros nem pólos na fronteira de $D(\Lambda)$. Sejam $\{a_i\}$ e $\{m_i\}$ como no enunciado da proposição anterior. O Teorema dos Resíduos aplicado à função $z\frac{f'}{f}$ afirma que

$$\frac{1}{2\pi i}\int_{\partial D(\Lambda)} z\frac{f'(z)}{f(z)}dz = \sum_{i=1}^{r+s} a_i m_i,$$

onde $\sum_{i=1}^{r+s} a_i m_i$ representa a soma de todos os pontos singulares de f em $D(\Lambda)$ contabilizados de acordo com a sua multiplicidade; o que queremos provar é que $\sum_{i=1}^{r+s} a_i m_i$ é um elemento da rede Λ. Ora,

$$\begin{aligned}\int_{\partial D(\Lambda)} z\frac{f'(z)}{f(z)}dz &= \int_0^{\omega_1} z\frac{f'(z)}{f(z)}dz + \int_{\omega_1}^{\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz \\ &\quad - \int_{\omega_2}^{\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz - \int_0^{\omega_2} z\frac{f'(z)}{f(z)}dz;\end{aligned}$$

como f é elíptica, fazendo a mudança de variável $u = z - \omega_1$ obtemos

$$\int_{\omega_1}^{\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz = \int_0^{\omega_2} u\frac{f'(u)}{f(u)}du + \omega_1\int_0^{\omega_2}\frac{f'(u)}{f(u)}du,$$

logo

$$\int_{\omega_1}^{\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz - \int_0^{\omega_2} z\frac{f'(z)}{f(z)}dz = \omega_1\int_0^{\omega_2}\frac{f'(z)}{f(z)}dz.$$

De forma inteiramente análoga, mostra-se que

$$\int_{\omega_2}^{\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz - \int_0^{\omega_1} z\frac{f'(z)}{f(z)}dz = \omega_2\int_0^{\omega_1}\frac{f'(z)}{f(z)}dz.$$

Assim

$$\sum_{i=1}^{r+s} a_i m_i = \frac{\omega_1}{2\pi i}\int_0^{\omega_2}\frac{f'(z)}{f(z)}dz - \frac{\omega_2}{2\pi i}\int_0^{\omega_1}\frac{f'(z)}{f(z)}dz.$$

Para concluir a prova basta que, para $j \in \{1,2\}$,

$$\int_0^{\omega_j}\frac{f'(z)}{f(z)}dz \in 2\pi i\mathbb{Z}.$$

Ora, para um tal j,

$$\begin{aligned}\int_0^{\omega_j}\frac{f'(z)}{f(z)}dz &= \ln f(\omega_j) - \ln f(0)\\ &= 2k\pi i \quad \text{para algum } k \in \mathbb{Z}\end{aligned}$$

pois $f(\omega_j) = re^{i\theta}$ e $f(0) = re^{i\widetilde{\theta}}$ onde $r \geq 0$ e $\theta - \widetilde{\theta}$ é múltiplo de 2π.

No caso de f ter zeros ou pólos na fronteira de $D(\Lambda)$, começamos pelo argumento do fim da prova da proposição (4.1.2). ■

4.2 A função $\mathcal{P}$ de Weierstrass

A função $\mathcal{P}$ de Weierstrass é definida por

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{0\neq\lambda\in\Lambda}\left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right)$$

onde $z \in \mathbb{C}\backslash\Lambda$. Vejamos que é uma função de $\mathfrak{M}(\Lambda)$ não constante.

Proposição 4.2.1 *$\mathcal{P}$ está bem definida.*

Prova. Devemos mostrar que, para cada z em $\mathbb{C}\backslash\Lambda$, a série que define a função $\mathcal{P}$ converge. Verifiquemos que esta série converge absolutamente e uniformemente em cada compacto S que não contenha pontos da rede Λ.

Seja S um tal compacto e fixemos z em S. Para cada $0 \neq \lambda \in \Lambda$, analisemos a diferença $\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}$. Consideremos a função $f(z) = \frac{1}{(z-\lambda)^2}$. Se $\left|\frac{z}{\lambda}\right| < 1$, podemos escrever

$$\begin{aligned}
\frac{1}{(z-\lambda)^2} &= \frac{1}{\lambda^2\left(1-\frac{z}{\lambda}\right)^2} \\
&= \frac{1}{\lambda^2}\left[\sum_{n=0}^{\infty}\left(\frac{z}{\lambda}\right)^n\right]^2 \\
&= \frac{1}{\lambda^2}\sum_{n=0}^{\infty}(n+1)\left(\frac{z}{\lambda}\right)^n
\end{aligned}$$

e portanto

$$\left|\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right| = \left|\frac{1}{\lambda^3}\right|\left|\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\lambda^{n-1}}\right|.$$

Além disso, se $0 \neq \lambda \in \Lambda$ é tal que $\left|\frac{z}{\lambda}\right| < \frac{1}{2}$, então

$$\begin{aligned}
\left|\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right| &= \left|\frac{1}{\lambda^3}\right|\left|\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\lambda^{n-1}}\right| \\
&\leq \frac{1}{|\lambda|^3}\sum_{n=1}^{\infty}(n+1)\frac{|z|^n}{|\lambda|^{n-1}} \\
&\leq \frac{1}{|\lambda|^3}\sum_{n=1}^{\infty}\frac{(n+1)|z|}{2^{n-1}} \\
&\leq \frac{CM}{|\lambda|^3}
\end{aligned}$$

onde C designa o valor da série convergente $\sum_{n=1}^{\infty}\frac{n+1}{2^{n-1}}$ e M é majorante de $|z|$ em S.

Finalmente, note-se que há apenas um número finito de λ's que não verificam a condição $2|z| < |\lambda|$; ou seja, a rede discreta Λ tem apenas um número finito de elementos no disco centrado em 0 e raio $2|z|$. Para eles, as estimativas anteriores não são válidas mas, como são em número finito, não comprometem a convergência da série envolvida na definição da função $\mathcal{P}$.

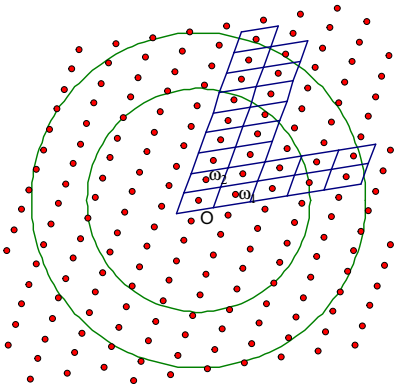
Para concluir a prova desta proposição basta mostrar que a série $\sum_{0\neq\lambda\in\Lambda} \frac{1}{|\lambda|^3}$ é convergente, caso particular do resultado que se segue:

Lema 4.2.2 *A série* $\sum_{0\neq\lambda\in\Lambda} \frac{1}{|\lambda|^s}$ *converge para qualquer* $s > 2$.

Prova. Fixado $s > 2$ e $k \in \mathbb{N}$,

$$\begin{aligned}\sum_{0\neq\lambda\in\Lambda} \frac{1}{|\lambda|^s} &= \sum_{|\lambda|\leq k} \frac{1}{|\lambda|^s} + \sum_{|\lambda|>k} \frac{1}{|\lambda|^s} \\ &= \sum_{n=1}^{k} \left(\sum_{n-1<|\lambda|\leq n} \frac{1}{|\lambda|^s} \right) + \sum_{|\lambda|>k} \frac{1}{|\lambda|^s}\end{aligned}$$

Para cada $n \in \mathbb{N}$, defina-se $p(n) = \#\{\lambda \in \Lambda : |\lambda| \leq n\}$. Vamos mostrar que os números $p(n) - p(n-1)$ e n são da mesma ordem de grandeza. Seja α o ângulo orientado entre as direcções determinadas por ω_1 e ω_2. Para cada ponto da rede, $\lambda \in \Lambda$, pertencente ao disco centrado na origem e raio n, desenhemos um paralelogramo de lados paralelos às direcções ω_1 e ω_2, de comprimento respectivamente igual a $|\omega_1|$ e $|\omega_2|$, cujo centro seja λ.



Pontos da rede Λ e discos de raio $n-1$ e n.

Cada um destes paralelogramos tem área igual a $A = |\omega_1\omega_2 \sin\alpha|$. Deste modo, estabelecemos uma correspondência entre os pontos da rede que per-

tencem ao disco de raio n e as áreas dos paralelogramos associados:

$$Ap\,(n) = \sum_{|\lambda|\leq n} \text{área do paralelogramo de centro } \lambda.$$

A área de todos estes paralelogramos não vai além da área do disco centrado na origem de raio $n+\frac{|\omega_1+\omega_2|}{2}$, nem fica aquém da do disco centrado na origem de raio $n-\frac{|\omega_1+\omega_2|}{2}$, ou seja,

$$\frac{\pi}{4}\left(2n-|\omega_1+\omega_2|\right)^2 \leq Ap\,(n) \leq \frac{\pi}{4}\left(2n+|\omega_1+\omega_2|\right)^2.$$

Logo,

$$\frac{\pi\,(2n-1)\,(1-|\omega_1+\omega_2|)}{A} \leq p\,(n)-p\,(n-1) \leq \frac{\pi\,(2n-1)\,(1+|\omega_1+\omega_2|)}{A}$$

o que mostra que $p\,(n)-p\,(n-1)$ e n são da mesma ordem de grandeza.

Assim,

$$\begin{aligned}
\sum_{n=1}^{k}\left(\sum_{n-1<|\lambda|\leq n}\frac{1}{|\lambda|^s}\right) &= \sum_{|\lambda|\leq 1}\frac{1}{|\lambda|^s}+\sum_{n=2}^{k}\left(\sum_{n-1<|\lambda|\leq n}\frac{1}{|\lambda|^s}\right)\\
&\leq \sum_{|\lambda|\leq 1}\frac{1}{|\lambda|^s}+\frac{2\pi\,(1+|\omega_1+\omega_2|)}{A}\sum_{n=1}^{k-1}\frac{1}{n^s}\\
&\leq \sum_{|\lambda|\leq 1}\frac{1}{|\lambda|^s}+\frac{2\pi\,(1+|\omega_1+\omega_2|)}{A}\sum_{n=1}^{\infty}\frac{1}{n^s}
\end{aligned}$$

logo $\sum_{0\neq\lambda\in\Lambda}\frac{1}{|\lambda|^s}$ é convergente pois a sucessão das somas parciais $\left(\sum_{|\lambda|\leq k}\frac{1}{|\lambda|^s}\right)_k$ é majorada por uma série convergente (uma vez que $s>2$ e só um número finito de pontos da rede Λ tem norma não superior a um). ■ ■

A expressão que define $\mathcal{P}$ mostra que ela é meromorfa e tem um pólo de multiplicidade dois em cada ponto da rede Λ.

Proposição 4.2.3 *$\mathcal{P}$ é uma função par.*

Prova. A paridade de $\mathcal{P}$ é consequência da igualdade $\Lambda = -\Lambda$. ■

Derivando, termo a termo, a série que define a função $\mathcal{P}$ de Weierstrass obtemos

$$-2\sum_{\lambda\in\Lambda}\frac{1}{(z-\lambda)^3}.$$

Se mostrarmos que esta série converge absolutamente e uniformemente em cada compacto S que não contenha pontos da rede Λ obtemos a expressão da derivada da função $\mathcal{P}$. Ora, seja S um tal compacto e fixemos z em S. Para cada $0 \neq \lambda \in \Lambda$, consideremos a função $f(z) = \frac{1}{(z-\lambda)^3}$. Se $\left|\frac{z}{\lambda}\right| < 1$, podemos escrever

$$\begin{aligned}\frac{1}{(z-\lambda)^3} &= -\frac{1}{\lambda^3\left(1-\frac{z}{\lambda}\right)^3}\\ &= -\frac{1}{\lambda^3}\left[\sum_{n=0}^{\infty}\left(\frac{z}{\lambda}\right)^n\right]^3\\ &= -\frac{1}{\lambda^3}\sum_{n=0}^{\infty}\frac{(n+1)(n+2)}{2}\left(\frac{z}{\lambda}\right)^n\end{aligned}$$

e portanto

$$\left|\frac{1}{(z-\lambda)^3}\right| = \left|\frac{1}{\lambda^3}\right|\left|\sum_{n=0}^{\infty}\frac{(n+1)(n+2)}{2}\left(\frac{z}{\lambda}\right)^n\right|.$$

Além disso, se $0 \neq \lambda \in \Lambda$ é tal que $\left|\frac{z}{\lambda}\right| < \frac{1}{2}$, então

$$\begin{aligned}\left|\frac{1}{(z-\lambda)^3}\right| &= \left|\frac{1}{\lambda^3}\right|\left|\sum_{n=0}^{\infty}\frac{(n+1)(n+2)}{2}\frac{z^n}{\lambda^n}\right|\\ &\leq \frac{1}{|\lambda|^3}\sum_{n=0}^{\infty}\frac{(n+1)(n+2)}{2}\frac{|z|^n}{|\lambda|^n}\\ &\leq \frac{1}{|\lambda|^3}\sum_{n=0}^{\infty}\frac{(n+1)(n+2)}{2^{n+1}}\\ &= \frac{C}{|\lambda|^3}\end{aligned}$$

onde C designa o valor da série convergente $\sum_{n=0}^{\infty}\frac{(n+1)(n+2)}{2^{n+1}}$. Mais uma vez, os λ's que não verificam a condição $2|z| < |\lambda|$ são em número finito pelo que não comprometem a convergência da série em causa. Esta é majorada por

uma série convergente, como vimos no lema (4.2.2), e portanto a expressão da derivada de $\mathcal{P}$ é

$$\mathcal{P}'(z) = -2\sum_{\lambda\in\Lambda}\frac{1}{(z-\lambda)^3}.$$

Proposição 4.2.4 *$\mathcal{P}'$ é uma função ímpar e elíptica relativamente à rede Λ.*

Prova. Seja $z \in \mathbb{C}\backslash\Lambda$. Então

$$\begin{aligned}
\mathcal{P}'(-z) &= -2\sum_{\lambda\in\Lambda}\frac{1}{(-z-\lambda)^3} \\
&= 2\sum_{\lambda\in\Lambda}\frac{1}{(z+\lambda)^3} \\
&= 2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}, \quad \text{onde } \omega = -\lambda \\
&= -\mathcal{P}'(z).
\end{aligned}$$

Além disso, se $\omega \in \Lambda$

$$\begin{aligned}
\mathcal{P}'(z+\omega) &= -2\sum_{\lambda\in\Lambda}\frac{1}{(z+\omega-\lambda)^3} \\
&= -2\sum_{\mu\in\Lambda}\frac{1}{(z-\mu)^3}, \quad \text{onde } \mu = \lambda - \omega \\
&= \mathcal{P}'(z).
\end{aligned}$$

■

Corolário 4.2.5 *$\mathcal{P}$ é uma função elíptica relativamente à rede Λ.*

Prova. Como $\mathcal{P}'$ é uma função elíptica, então

$$\mathcal{P}'(z+\omega_1) = \mathcal{P}'(z+\omega_2) = \mathcal{P}'(z)$$

para qualquer $z \in \mathbb{C}\backslash\Lambda$. Como $\mathbb{C}\backslash\Lambda$ é conexo (complementar em $\mathbb{C}$ de um conjunto discreto), primitivando as igualdades anteriores obtemos

$$\mathcal{P}(z+\omega_1) = \mathcal{P}(z) + C_1 \tag{4.5}$$

e

$$\mathcal{P}(z+\omega_2) = \mathcal{P}(z) + C_2 \tag{4.6}$$

para algumas constantes C_1 e C_2 e z no aberto $\mathbb{C}\backslash\Lambda$. Bastará, agora, mostrar que $C_1 = C_2 = 0$ para concluir que $\mathcal{P}$ é uma função elíptica. Se fizermos na igualdade (4.5) $z = -\frac{\omega_1}{2}$ e na igualdade (4.6) $z = -\frac{\omega_2}{2}$, vemos que

$$\mathcal{P}\left(\frac{\omega_1}{2}\right) = \mathcal{P}\left(-\frac{\omega_1}{2}\right) + C_1$$

e

$$\mathcal{P}\left(\frac{\omega_2}{2}\right) = \mathcal{P}\left(-\frac{\omega_2}{2}\right) + C_2.$$

De onde se conclui que $C_1 = C_2 = 0$ pois $\mathcal{P}$ é uma função par. ■

Estas duas funções, $\mathcal{P}$ e $\mathcal{P}'$, são suficientes para caracterizar qualquer função elíptica. De facto, qualquer função elíptica h pode ser escrita na forma

$$h = \frac{f(\mathcal{P}, \mathcal{P}')}{g(\mathcal{P}, \mathcal{P}')}$$

onde f e g são funções polinomiais nas variáveis $\mathcal{P}$ e $\mathcal{P}'$.

Proposição 4.2.6 *O corpo $\mathfrak{M}(\Lambda)$ é gerado pelas funções $\mathcal{P}$ e $\mathcal{P}'$ no sentido explicitado.*

Prova. Seja $f \in \mathfrak{M}(\Lambda)$. Podemos escrever f como soma de uma função par com uma função ímpar do seguinte modo

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}.$$

Se f for uma função ímpar então $f\mathcal{P}'$ é uma função par; pelo que é suficiente provar que as funções pares são funções racionais de $\mathcal{P}$.

Lema 4.2.7 *Seja $f \in \mathfrak{M}(\Lambda)$ uma função par com um ponto singular em u. Se $(u) = (-u)$ então a ordem de f em u é par.*

Prova. Seja f uma função elíptica, par com um ponto singular em u tal que $(u) = (-u)$. No paralelogramo fundamental, $D(\Lambda)$, existem precisamente quatro pontos que verificam a igualdade $(2u) = (0)$, a saber

$$0, \quad \frac{\omega_1}{2}, \quad \frac{\omega_2}{2} \quad \text{e} \quad \frac{\omega_1 + \omega_2}{2}.$$

Como f é uma função par, f' é uma função ímpar; se u for um zero de f, então da hipótese $(u) = (-u)$, segue que $f'(u) = f'\overline{(-u)} = -f'(u)$ e portanto $f'(u) = 0$, o que garante que a ordem de f em u, $ord(f, u)$, é pelo menos dois.

Suponhamos ainda que $(u) \neq (0)$ e consideremos a função elíptica definida por

$$g(z) = \mathcal{P}(z) - \mathcal{P}(u).$$

Como u é um zero da função g e esta é par, então pelo argumento anterior a ordem de g em u é pelo menos dois. Por outro lado, as funções g e $\mathcal{P}$ têm os mesmos pólos; em $D(\Lambda)$, a função de Weierstrass tem exactamente um pólo em 0 de multiplicidade dois. Logo a proposição (4.1.3) aplicada à função g garante que a ordem de g em u é dois.

Consideremos a função $\frac{f}{g}$. Esta função é elíptica, par e está definida em u. Se $\left(\frac{f}{g}\right)(u) \neq 0$, então a ordem de $\frac{f}{g}$ em u é zero. Por outro lado, como as ordens das funções g e $\frac{f}{g}$ em u são finitas, temos que

$$\begin{aligned} ord(u, f) &= ord\left(u, \frac{f}{g}.g\right) \\ &= ord\left(u, \frac{f}{g}\right) + ord(u, g) \\ &= 2. \end{aligned}$$

Se $\left(\frac{f}{g}\right)(u) = 0$, então pelo argumento anterior, u é um zero de $\frac{f}{g}$ de ordem pelo menos dois. Procedamos como anteriormente comparando esta função com a função g. A função $\frac{f}{g^2}$ é elíptica, par e está definida em u. Se $\left(\frac{f}{g^2}\right)(u) \neq 0$ então a ordem de $\frac{f}{g^2}$ em u é zero e

$$\begin{aligned} ord(u, f) &= ord\left(u, \frac{f}{g^2}.g^2\right) \\ &= ord\left(u, \frac{f}{g^2}\right) + 2ord\left(u, g^2\right) \\ &= 2 \times 2. \end{aligned}$$

Se $\left(\frac{f}{g^2}\right)(u) = 0$, então voltamos a repetir o mesmo argumento. Este processo tem que terminar ao fim de um número finito de etapas porque estamos a supor que a ordem de f em u é finita. E portanto $ord(f, u)$ é par.

Se $(u) = (0)$, não é possível usar a função g desta maneira porque a função $\mathcal{P}$ tem um pólo em zero. Neste caso, consideramos a função $\mathcal{P}$ escrita como série de Laurent centrada em $z = 0$, isto é,

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{n=0}^{\infty} a_n z^{2n}$$

e definimos

$$g(z) = \frac{1}{\mathcal{P}(z)} = \frac{z^2}{1 + \sum_{n=1}^{\infty} a_n z^{2n}}.$$

Esta função é elíptica, par e tem um zero de ordem dois em zero.

Consideremos a função $\frac{f}{g}$. A função $\frac{f}{g}$ é elíptica, par e está defnida em 0. Se $\left(\frac{f}{g}\right)(0) \neq 0$, então a ordem de $\frac{f}{g}$ em 0 é zero e

$$\begin{aligned} ord(0, f) &= ord\left(0, \frac{f}{g} g\right) \\ &= ord\left(0, \frac{f}{g}\right) + ord(0, g) \\ &= 2. \end{aligned}$$

Se $\left(\frac{f}{g}\right)(0) = 0$, a ordem de $\frac{f}{g}$ em 0 é pelo menos dois. Consideremos a função $\frac{f}{g^2}$, que está definida em 0, é elíptica e par. Se $\left(\frac{f}{g^2}\right)(0) \neq 0$, então a ordem de $\frac{f}{g^2}$ em 0 é zero e

$$\begin{aligned} ord(0, f) &= ord\left(0, \frac{f}{g^2} g^2\right) \\ &= ord\left(0, \frac{f}{g^2}\right) + 2ord(0, g) \\ &= 2 \times 2. \end{aligned}$$

Se $\left(\frac{f}{g^2}\right)(0) = 0$, repetimos o mesmo argumento e terminamos como anteriormente.

Se u for um pólo de f, a sua multiplicidade é pelo menos dois pois no desenvolvimento de Laurent de f o coeficiente de $\frac{1}{z-u}$, b_1 digamos, é nulo

uma vez que, se γ designar um lacete simples,

$$\begin{aligned} b_1 &= \frac{1}{2\pi i}\int_{\gamma} f(\omega)\,d\omega \\ &= \frac{1}{2\pi i}\int_{-\gamma} -f(-z)\,dz \quad \text{fazendo } z=-\omega \\ &= -\frac{1}{2\pi i}\int_{-\gamma} f(\omega)\,d\omega \quad \text{porque } f \text{ é par} \\ &= -b_1. \end{aligned}$$

Se $(u)\neq(0)$, então consideramos a função fg onde

$$g(z)=\mathcal{P}(z)-\mathcal{P}(u)$$

é, como vimos, uma função com um zero em u de ordem dois. Se $(fg)(u)\neq 0$, então a ordem de fg em u é zero e

$$\begin{aligned} ord(u,f) &= ord\left(u,\frac{fg}{g}\right) \\ &= ord(u,fg)-ord(u,g) \\ &= -2. \end{aligned}$$

Se fg não estiver definida em u, então u é um pólo de fg de multiplicidade não inferior a dois (basta aplicar o argumento anterior à função fg que é par). Consideremos a função fg^2. Se $(fg^2)(u)\neq 0$ então a ordem de fg^2 em u é zero e

$$\begin{aligned} ord(u,f) &= ord\left(u,\frac{fg^2}{g^2}\right) \\ &= ord\left(u,fg^2\right)-2ord(u,g) \\ &= -2\times 2. \end{aligned}$$

Se fg^2 tiver um pólo em u voltamos a repetir o argumento.

Se $(u)=(0)$, procedemos de forma análoga comparando f com a função

$$g(z)=\frac{1}{\mathcal{P}(z)}=\frac{z^2}{1+\sum_{n=1}^{\infty}a_n z^{2n}}.$$

Em qualquer dos casos, fica concluido que a multiplicidade do ponto singular é necessariamente par. ■

Lema 4.2.8 *Se $a \in \mathbb{C}\backslash\Lambda$, então $\mathcal{P}(z) - \mathcal{P}(a)$ tem um zero duplo em $z = a$ se e somente se $(2a) = (0)$.*

Prova. Precisamos apenas de verificar que se $\mathcal{P}(z) - \mathcal{P}(a)$ tem um zero duplo em $z = a$, então $(2a) = (0)$, uma vez que a implicação contrária foi provada no lema anterior.

Em geral, se f é uma função par que admite um zero em u de ordem m, então, em consequência da igualdade

$$f^{(k)}(u) = (-1)^k f^{(k)}(-u),$$

f tem um zero em $-u$ com a mesma ordem. Logo a função $\mathcal{P}(z) - \mathcal{P}(a)$ tem um zero duplo em $z = -a$. Se $(a) \neq (-a)$, então $\mathcal{P}(z) - \mathcal{P}(a)$ seria uma função com quatro zeros e dois pólos no paralelogramo fundamental contrariando a proposição (4.1.3). Logo $(a) = (-a)$ ou seja $(2a) = (0)$.

Note-se que se $(2a) \neq (0)$, então a função $\mathcal{P}(z) - \mathcal{P}(a)$ tem dois zeros simples: em $z = a$ e em $z = -a$. ■

Voltemos à prova da proposição (4.2.6). Seja $\{u_i : i = 1, 2, \ldots, r\}$ o conjunto dos pontos singulares de f no paralelogramo fundamental, $D(\Lambda)$, distintos dos pontos da rede Λ. Defina-se

$$m_i = \begin{cases} ord(u_i, f) & \text{se} \quad (2u_i) \neq (0) \\ \frac{1}{2} ord(u_i, f) & \text{se} \quad (2u_i) = (0) \end{cases}$$

e

$$h(z) = \prod_{i=1}^{r} (\mathcal{P}(z) - \mathcal{P}(u_i))^{m_i}.$$

Para qualquer $(z) \neq (0)$ temos

$$ord(z, f) = ord(z, h).$$

Esta igualdade também vale no caso em que $(z) = (0)$ porque a proposição (4.1.3) aplicada à função elíptica $\frac{f}{h}$ garante que esta não tem zeros nem pólos e portanto pela proposição (4.1.1) existe uma constante C não nula tal que $\frac{f}{h} = C$. Logo

$$f(z) = C \prod_{i=1}^{r} (\mathcal{P}(z) - \mathcal{P}(u_1))^{m_i}$$

o que, além disso, confirma que qualquer função elíptica par pode ser escrita como uma função racional de $\mathcal{P}$. ■

De seguida, reescreveremos as funções $\mathcal{P}$ e $\mathcal{P}'$, como séries de Laurent centradas na origem, o que permitirá encontrar uma relação útil, no que se segue, entre estas duas funções. Assim

$$\begin{aligned}
\mathcal{P}(z) &= \frac{1}{z^2} + \sum_{0\neq\lambda\in\Lambda} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right) \\
&= \frac{1}{z^2} + \sum_{0\neq\lambda\in\Lambda} \left(\frac{1}{\lambda^2} \left(\frac{1}{1-\frac{z}{\lambda}} \right)^2 - \frac{1}{\lambda^2} \right) \\
&= \frac{1}{z^2} + \sum_{0\neq\lambda\in\Lambda} \left(\frac{1}{\lambda^2} \left[\sum_{m=0}^{\infty} \left(\frac{z}{\lambda} \right)^m \right]^2 - \frac{1}{\lambda^2} \right) \\
&= \frac{1}{z^2} + \sum_{0\neq\lambda\in\Lambda} \frac{1}{\lambda^2} \left(\left[\sum_{m=0}^{\infty} \left(\frac{z}{\lambda} \right)^m \right]^2 - 1 \right)
\end{aligned}$$

e portanto, efectuando o produto de Cauchy da série $\sum_{m=0}^{\infty} \left(\frac{z}{\lambda}\right)^m$ por si mesma, obtemos

$$\begin{aligned}
\mathcal{P}(z) &= \frac{1}{z^2} + \sum_{0\neq\lambda\in\Lambda} \sum_{m=1}^{\infty} (m+1) \left(\frac{z}{\lambda} \right)^m \frac{1}{\lambda^2} \\
&= \frac{1}{z^2} + \sum_{m=1}^{\infty} c_m z^m
\end{aligned}$$

onde

$$c_m = \sum_{0\neq\lambda\in\Lambda} \frac{m+1}{\lambda^{m+2}},$$

sendo que $c_m = 0$ para todo m ímpar pois $\mathcal{P}$ é uma função par. Usando a notação

$$s_m(\Lambda) = s_m = \sum_{0\neq\lambda\in\Lambda} \frac{1}{\lambda^m}$$

obtemos a seguinte expressão para a função $\mathcal{P}$

$$\mathcal{P}(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1)\, s_{2n+2}(\Lambda)\, z^{2n}.$$

Explicitando os primeiros termos,

$$\mathcal{P}(z) = \frac{1}{z^2} + 3s_4 z^2 + 5s_6 z^4 + 7s_8 z^6 + \ldots \tag{4.7}$$

e usando derivação termo a termo temos

$$\mathcal{P}'(z) = -\frac{2}{z^3} + 6s_4 z + 20s_6 z^3 + 42s_8 z^5 + \ldots \tag{4.8}$$

Proposição 4.2.9 *As funções $\mathcal{P}$ e $\mathcal{P}'$ relacionam-se através da fórmula*

$$\mathcal{P}'^2 = 4\mathcal{P}^3 - g_2\mathcal{P} - g_3$$

onde $g_2 = g_2(\Lambda) = 60s_4$ e $g_3 = g_3(\Lambda) = 140s_6$.

Prova. Consideremos a função

$$\varphi(z) = \mathcal{P}'^2(z) - 4\mathcal{P}^3(z) + g_2\mathcal{P}(z) + g_3.$$

Queremos mostrar que $\varphi(z) = 0$ para todo o $z \in \mathbb{C}\backslash\Lambda$. Pela proposição (4.1.1) é suficiente averiguar que φ não tem pólos e que o termo constante do desenvolvimento em série de Laurent em zero é nulo. Vejamos quais os termos polares e constante de cada uma das parcelas de φ:

parcela de φ	termos polares e constante
$\mathcal{P}'^2(z)$	$\frac{4}{z^6}; -\frac{24s_4}{z^2}; -80s_6;$
$-4\mathcal{P}^3(z)$	$-\frac{4}{z^6}; -\frac{36s_4}{z^2}; -60s_6;$
$g_2\mathcal{P}(z)$	$\frac{60s_4}{z^2};$
g_3	$140s_6.$

Somando as parcelas polares e constantes, vemos que φ é uma função elíptica sem pólos e com um zero na origem. Logo φ é identicamente nula. ■

Esta proposição mostra que os pontos da forma $((\mathcal{P}(z), \mathcal{P}'(z)))$ pertencem a curva em $\mathbb{C}^2$

$$y^2 = 4x^3 - g_2 x - g_3.$$

O objectivo agora é caracterizar os zeros de $\mathcal{P}'$. Defina-se

$$e_i = \mathcal{P}\left(\frac{\omega_i}{2}\right), \quad \text{para } i = 1, 2, 3$$

onde $\omega_3 = \omega_1 + \omega_2$. Como vimos anterioremente no lema (4.2.8), a função

$$h(z) = \mathcal{P}(z) - e_i$$

tem um zero de ordem dois em $\frac{\omega_i}{2}$. Logo, pela proposição (4.1.1)

$$\mathcal{P}'^2(z) = C(\mathcal{P}(z) - e_1)(\mathcal{P}(z) - e_2)(\mathcal{P}(z) - e_3)$$

para alguma constante C não nula. Para determinar a constante C escrevemos as funções $\mathcal{P}'^2(z)$ e $g(z) = (\mathcal{P}(z) - e_1)(\mathcal{P}(z) - e_2)(\mathcal{P}(z) - e_3)$ à custa das respectivas séries de Laurent em $z = 0$

$$\mathcal{P}'^2(z) = \frac{4}{z^6}\left(1 + \sum_{n=2}^{\infty} b_n z^{2n}\right)$$

e

$$g(z) = \frac{1}{z^6}\left(1 + \sum_{n=1}^{\infty} d_n z^{2n}\right).$$

Assim

$$\frac{\mathcal{P}'^2(z)}{g(z)} = \frac{4\left(1 + \sum\limits_{n=2}^{\infty} b_n z^{2n}\right)}{\left(1 + \sum\limits_{n=1}^{\infty} d_n z^{2n}\right)}$$

que vale 4 em $z = 0$, logo

$$\mathcal{P}'^2(z) = 4(\mathcal{P}(z) - e_1)(\mathcal{P}(z) - e_2)(\mathcal{P}(z) - e_3).$$

No paralelogramo fundamental $D(\Lambda)$, a função $\mathcal{P}$ tem um pólo de multiplicidade 2 e toma o valor e_i duas vezes para cada $i = 1, 2, 3$. Se $e_i = e_j$ para valores de i e j distintos, então $\mathcal{P}$ teria mais zeros que pólos o que é impossível pela proposição (4.1.3). Isto prova que

Proposição 4.2.10 *A função $\mathcal{P}'$ tem três zeros distintos em $D(\Lambda)$, a saber $\left(\frac{\omega_1}{2}\right), \left(\frac{\omega_2}{2}\right)$ e $\left(\frac{\omega_1+\omega_2}{2}\right)$.*

4.3 Fórmula de adição para $\mathcal{P}$

Consideremos o conjunto definido por

$$E = \left\{(x,y) \in \mathbb{C}^2 : y^2 = 4x^3 - g_2(\Lambda)\, x - g_3(\Lambda)\right\} \cup \left\{(\infty,\infty)\right\}.$$

Diz-se que E é a **curva elíptica** correspondente à rede Λ. Seja

$$\begin{array}{rccl} \xi: & \mathbb{C} & \longrightarrow & E \\ & z & \mapsto & \begin{cases} (\mathcal{P}(z), \mathcal{P}'(z)) & \text{se} \quad z \notin \Lambda \\ (\infty,\infty) & \text{se} \quad z \in \Lambda \end{cases} \end{array}$$

Proposição 4.3.1 *Sejam $z_1, z_2 \in \mathbb{C}$ distintos. Os pontos $\xi(z_1), \xi(z_2)$ e $\xi(-z_1 - z_2)$ pertencem à mesma recta em $\mathbb{C}$.*

Prova. Comecemos por observar que a proposição é trivialmente verificada no caso de algum dos pontos z_1, z_2 ou $-z_1 - z_2$ serem pontos da rede Λ.

Suponhamos que nenhum destes pontos pertence à rede. Sejam a e b números complexos tais que

$$y = ax + b$$

é a equação da recta definida pelos pontos $\xi(z_1)$ e $\xi(z_2)$. A função definida por

$$\mathcal{P}' - (a\mathcal{P} + b)$$

é elíptica e tem um pólo, em $z = 0$, de ordem três como se deduz de (4.7) e (4.8). Logo, pela proposição (4.1.3), tem três zeros contados de acordo com as suas multiplicidades, sendo que dois deles são z_1 e z_2. Se um deles tivesse multiplicidade dois, digamos z_1, então pela proposição (4.1.4) ter-se-ia

$$(2z_1 + z_2) = (0)$$

ou seja,

$$(z_1) = (-z_1 - z_2)$$

e portanto os pontos $\xi(-z_1 - z_2)$ e $\xi(z_1)$ seriam coincidentes. No caso de cada um dos zeros ter multiplicidade um, então a proposição (4.1.4) afirma que o terceiro zero verifica a igualdade

$$(z_1 + z_2 + z_3) = (0)$$

isto é,

$$(z_3) = (-z_1 - z_2)$$

e portanto

$$\mathcal{P}'(-z_1 - z_2) = a\mathcal{P}(-z_1 - z_2) + b$$

o que mostra que $\xi(-z_1 - z_2)$ pertence à recta definida por $\xi(z_1)$ e $\xi(z_2)$. ■

Decorre desta proposição que é possível encontrar uma fórmula para o cálculo de $\mathcal{P}(z_1 + z_2)$ envolvendo apenas $\mathcal{P}(z_1), \mathcal{P}(z_2), \mathcal{P}'(z_1)$ e $\mathcal{P}'(z_2)$:

Corolário 4.3.2 (Fórmula de adição) *Sejam z_1, z_2 em $\mathbb{C}\backslash\Lambda$ tais que $(z_1) \neq (\pm z_2)$. Então*

$$\mathcal{P}(z_1 + z_2) = -\mathcal{P}(z_1) - \mathcal{P}(z_2) + \frac{1}{4}\left(\frac{\mathcal{P}'(z_1) - \mathcal{P}'(z_2)}{\mathcal{P}(z_1) - \mathcal{P}(z_2)}\right)^2.$$

Prova. Sejam a e b números complexos tais que $y = ax + b$ é a equação da recta definida pelos pontos $\xi(z_1)$ e $\xi(z_2)$. Por definição, os pontos da recta que estão sobre a curva elíptica E verificam a igualdade

$$4x^3 - g_2(\Lambda)\, x - g_3(\Lambda) - (ax + b)^2 = 0.$$

Esta equação tem três raízes, contadas de acordo com as suas multiplicidades, a saber $\mathcal{P}(z_1), \mathcal{P}(z_2)$ e $\mathcal{P}(z_3)$ e portanto podemos reescrever esta igualdade do seguinte modo

$$4(x - \mathcal{P}(z_1))(x - \mathcal{P}(z_2))(x - \mathcal{P}(z_3)) = 0.$$

Comparando os coeficientes de x^2 nas duas igualdades anteriores temos que

$$\mathcal{P}(z_1) + \mathcal{P}(z_2) + \mathcal{P}(z_3) = \frac{a^2}{4}. \tag{4.9}$$

Além disso, pela proposição (4.1.4)

$$(z_3) = (-z_1 - z_2)$$

logo

$$\mathcal{P}(z_3) = \mathcal{P}(-z_1 - z_2) \overset{\mathcal{P} \text{ é par}}{=} \mathcal{P}(z_1 + z_2). \tag{4.10}$$

Por outro lado,

$$\mathcal{P}'(z_1) - \mathcal{P}'(z_2) = a\left(\mathcal{P}(z_1) - \mathcal{P}(z_2)\right) \tag{4.11}$$

porque $\xi(z_1)$ e $\xi(z_2)$ são pontos da recta de equação $y = ax + b$. Juntando a informação das igualdades (4.9), (4.10) e (4.11) obtemos

$$\mathcal{P}(z_1 + z_2) = -\mathcal{P}(z_1) - \mathcal{P}(z_2) + \frac{1}{4}\left(\frac{\mathcal{P}'(z_1) - \mathcal{P}'(z_2)}{\mathcal{P}(z_1) - \mathcal{P}(z_2)}\right)^2$$

como queríamos mostrar. ■

Se z_1 e z_2 são complexos nas condições do corolário anterior então

$$\begin{aligned}\xi(-z_1 - z_2) &= \left(\mathcal{P}(-z_1 - z_2), \mathcal{P}'(-z_1 - z_2)\right) \\ &= \left(\mathcal{P}(z_1 + z_2), -\mathcal{P}'(z_1 + z_2)\right).\end{aligned}$$

Tal como acontece para $\mathcal{P}(z_1 + z_2)$, também é possível expressar $\mathcal{P}'(z_1 + z_2)$ usando apenas $\mathcal{P}(z_1), \mathcal{P}(z_2), \mathcal{P}'(z_1)$ e $\mathcal{P}'(z_2)$. Vimos na demonstração da proposição (4.3.1) que

$$\mathcal{P}'(-z_1 - z_2) = a\mathcal{P}(-z_1 - z_2) + b$$

isto é,

$$\mathcal{P}'(z_1 + z_2) = -a\mathcal{P}(z_1 + z_2) - b$$

onde

$$a = \frac{\mathcal{P}'(z_1) - \mathcal{P}'(z_2)}{\mathcal{P}(z_1) - \mathcal{P}(z_2)}$$

e

$$b = \frac{\mathcal{P}'(z_1) + \mathcal{P}'(z_2) - a\left(\mathcal{P}(z_1) + \mathcal{P}(z_2)\right)}{2}.$$

Fazendo os cálculos obtemos a seguinte fórmula de adição para $\mathcal{P}'$:

$$\begin{aligned}\mathcal{P}'(z_1 + z_2) &= \frac{\mathcal{P}(z_1)\mathcal{P}'(z_1) - 2\mathcal{P}(z_1)\mathcal{P}'(z_2) + 2\mathcal{P}(z_2)\mathcal{P}'(z_1) - \mathcal{P}(z_2)\mathcal{P}'(z_2)}{\mathcal{P}(z_1) - \mathcal{P}(z_2)} \\ &\quad -\tfrac{1}{4}\left(\frac{\mathcal{P}'(z_1) - \mathcal{P}'(z_2)}{\mathcal{P}(z_1) - \mathcal{P}(z_2)}\right)^3\end{aligned}$$

Corolário 4.3.3 ***(Fórmula de duplicação)*** *Se $z \notin \Lambda$, então*

$$\mathcal{P}(2z) = -2\mathcal{P}(z) + \frac{1}{4}\left(\frac{\mathcal{P}''(z)}{\mathcal{P}'(z)}\right)^2.$$

Prova. Se $2z \notin \Lambda$ e se na fórmula de adição para $\mathcal{P}$ considerarmos z_1 variável a tender para z por valores distintos de z e de $-z$ temos

$$\begin{aligned}
\mathcal{P}(2z) &= \lim_{z_1 \to z} \mathcal{P}(z_1 + z) \\
&= \lim_{z_1 \to z} \left(-\mathcal{P}(z_1) - \mathcal{P}(z) + \frac{1}{4}\left(\frac{\mathcal{P}'(z_1) - \mathcal{P}'(z)}{\mathcal{P}(z_1) - \mathcal{P}(z)}\right)^2\right) \\
&= -2\mathcal{P}(z) + \frac{1}{4}\left(\lim_{z_1 \to z} \frac{\mathcal{P}'(z_1) - \mathcal{P}'(z)}{\mathcal{P}(z_1) - \mathcal{P}(z)}\right)^2 \\
&= -2\mathcal{P}(z) + \frac{1}{4}\left(\lim_{z_1 \to z} \frac{\frac{\mathcal{P}'(z_1) - \mathcal{P}'(z)}{z_1 - z}}{\frac{\mathcal{P}(z_1) - \mathcal{P}(z)}{z_1 - z}}\right)^2 \\
&= -2\mathcal{P}(z) + \frac{1}{4}\left(\frac{\mathcal{P}''(z)}{\mathcal{P}'(z)}\right)^2
\end{aligned}$$

por definição de $\mathcal{P}'(z)$ e $\mathcal{P}''(z)$.

Se $2z \in \Lambda$, a fórmula de duplicação é ainda válida no sentido em que ambos os membros da igualdade valem ∞ (pela proposição (4.2.10)). ■

Podemos proceder de modo inteiramente análogo para deduzir a fórmula de duplicação de $\mathcal{P}'$, obtendo

$$\mathcal{P}'(2z) = -\mathcal{P}'(z) + 3\frac{\mathcal{P}(z)\,\mathcal{P}''(z)}{\mathcal{P}'(z)} - \frac{1}{4}\left(\frac{\mathcal{P}''(z)}{\mathcal{P}'(z)}\right)^3.$$

Capítulo 5

Construções com régua não graduada e compasso

Comecemos por recordar o que se entende por construções com régua não graduada e compasso. Sejam P_1 e P_2 dois pontos do plano euclidiano. A régua não graduada é o instrumento que permite traçar a recta que une os pontos P_1 e P_2; o compasso é o instrumento que permite traçar a circunferência com centro num dos pontos dados e que passa no outro ponto. Estas são as únicas operações possíveis de realizar com estes instrumentos.

Uma construção geométrica inicia-se sempre a partir de dois pontos dados que serão designados por $(0,0)$ e $(1,0)$. Assim, o aparecimento de um novo ponto numa construção geométrica resulta da intersecção de duas rectas distintas, de uma recta com uma circunferência ou ainda da intersecção de duas circunferências distintas. Como uma construção geométrica envolve um número finito destas etapas é possível definir indutivamente o que se entende por ponto construível.

Definição 5.0.4 *Um ponto P do plano euclidiano diz-se* ***um ponto construível*** *com régua não graduada e compasso se for o último de uma sequência finita de pontos $P_1, P_2, \ldots, P_{n-1}, P_n = P$, onde $P_1 = (0,0)$, $P_2 = (1,0)$ e os restantes P_i resultam da*

- *intersecção de duas rectas distintas, cada uma das quais definida por dois pontos de $\{P_1, P_2, \ldots, P_{i-1}\}$;*
- *intersecção de uma recta, definida por dois dos pontos anteriores, e uma circunferência centrada em P_j $(j = 1, 2, \ldots, i-1)$ e passando por*

um ponto de $\{P_1, P_2, \ldots, P_{j-1}, P_{j+1}, \ldots, P_{i-1}\}$ *ou*

- *intersecção de duas circunferências, cada uma das quais centrada num ponto de* $\{P_1, P_2, \ldots, P_{i-1}\}$ *e passando por um outro ponto distinto de* $\{P_1, P_2, \ldots, P_{i-1}\}$.

Nem todos os pontos de uma recta ou circunferência são construíveis. De facto, dados os pontos $(0,0)$ e $(1,0)$, ambos já construídos, a régua traça a recta que os une; esta recta contém, por exemplo, o ponto $(\pi, 0)$ que não é construível.

5.1 Números reais construíveis

Identifiquemos o número real a com o ponto de coordenadas $(a, 0)$. Se a e b forem dois números construíveis, isto é, se os pontos $(a, 0)$ e $(b, 0)$ forem construíveis, são conhecidas da Geometria de Euclides, construções com régua não graduada e compasso para obter os pontos $(a + b, 0)$, $(a - b, 0)$, $(ab, 0)$ e $\left(\frac{a}{b}, 0\right)$ se $b \neq 0$ e portanto o corpo dos números racionais é construível. Por outro lado, se $\alpha > 0$ for um número construível, então $\sqrt{\alpha}$ também é um número construível, pois é o meio proporcional entre 1 e α. Além disso, se $\sqrt{\alpha} \in \mathbb{R}\backslash\mathbb{Q}$, o conjunto $\mathbb{Q}(\sqrt{\alpha}) = \{a + b\sqrt{\alpha} : a, b \in \mathbb{Q}\}$ com a adição e produto usuais de $\mathbb{R}$ é um novo corpo de números construíveis e diz-se uma extensão quadrática de $\mathbb{Q}$.

De um modo geral, dado um corpo $\mathbb{F}$, subcorpo de $\mathbb{R}$, tal que $\alpha \in \mathbb{F}$ e $\sqrt{\alpha} \notin \mathbb{F}$, o conjunto $\mathbb{F}(\sqrt{\alpha}) = \{a + b\sqrt{\alpha} : a, b \in \mathbb{F}\}$ com as operações induzidas usuais é ele próprio um corpo a que se dá o nome de **extensão quadrática** de $\mathbb{F}$.

Este procedimento permite-nos dar uma caracterização algébrica de número construível.

Proposição 5.1.1 *As seguintes afirmações são equivalentes sobre um número real* a*:*

1. a *é um número real construível.*

2. *Existe uma sequência finita de subcorpos de* $\mathbb{R}$, $\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_n$ *com* $a \in \mathbb{F}_n$ *e tal que* $\mathbb{F}_i$ *é uma extensão quadrática de* $\mathbb{F}_{i-1}$ *para qualquer* $i = 1, 2, \ldots, n$.

Prova. Seja a um número real construível que identificamos com o ponto construível $(a, 0)$. Por definição, o ponto $(a, 0)$ é o último elemento de uma sequência finita de pontos $P_1, P_2, \ldots, P_{k-1}, P_k = (a, 0)$ onde $P_1 = (0, 0)$ e $P_2 = (1, 0)$, nas condições da definição (5.0.4).

Se $k = 1$ ou $k = 2$, então $a \in \mathbb{Q}$, $n = 0$ e $\mathbb{F}_0 = \mathbb{Q}$.

Admitamos que existe um corpo $\mathbb{F}_{n-1}$ contendo os pontos $P_1, P_2, \ldots, P_{k-1}$ e que se obtém por sucessivas extensões quadráticas do corpo $\mathbb{Q}$. Queremos provar que o ponto P_k está numa extensão quadrática de $\mathbb{F}_{n-1}$. Ora, como observámos anteriormente, o ponto $P_k = (a, 0)$ resulta da intersecção de dois objectos distintos (rectas e/ou circunferências) construídos a partir dos pontos $P_1, P_2, \ldots, P_{k-1}$.

Lema 5.1.2 *Se $\mathbb{F}$ é um corpo de números construíveis, então*

- *a intersecção de duas rectas distintas unindo pontos cujas coordenadas estão em $\mathbb{F}$ é vazia ou um elemento de $\mathbb{F}$.*
- *A intersecção de uma recta com uma circunferência com coeficientes em $\mathbb{F}$ é vazia ou pertence a uma extensão quadrática de $\mathbb{F}$.*
- *A intersecção de duas circunferências distintas com coeficientes em $\mathbb{F}$ é vazia ou pertence a uma extensão quadrática de $\mathbb{F}$.*

Prova. Sejam $A_0 = (x_0, y_0)$ e $A_1 = (x_1, y_1)$ dois pontos distintos cujas coordenadas estão em $\mathbb{F}$. A equação da recta definida pelos pontos A_0 e A_1 pode ser escrita na forma

$$ax + by + c = 0,$$

onde os coeficientes $a = y_1 - y_0$, $b = x_0 - x_1$ e $c = x_1y_0 - x_0y_1$ são números construíveis de $\mathbb{F}$.

De forma análoga, podemos ver que a circunferência centrada em A_0 passando por A_1 pode ser escrita na forma

$$x^2 + y^2 + ax + by + c = 0$$

onde os coeficientes $a = -2x_0$, $b = -2y_0$ e $c = 2x_0x_1 + 2y_0y_1 - x_1^2 - y_1^2$ são números construíveis de $\mathbb{F}$.

- Sejam

$$a_0x + b_0y + c_0 = 0 \quad \text{e} \quad a_1x + b_1y + c_1 = 0$$

equações de duas rectas distintas com coeficientes em $\mathbb{F}$. O ponto de intersecção das duas rectas, quando existe (isto é, se as rectas não forem paralelas o que se traduz pela desigualdade $a_0b_1 - a_1b_0 \neq 0$), é a solução do sistema

$$\begin{cases} a_0x + b_0y + c_0 = 0 \\ a_1x + b_1y + c_1 = 0 \end{cases} \Leftrightarrow \begin{cases} x = \frac{b_0c_1 - b_1c_0}{a_0b_1 - a_1b_0} \\ y = \frac{a_1c_0 - a_0c_1}{a_0b_1 - a_1b_0} \end{cases}.$$

Logo (x, y) é um ponto construível de $\mathbb{F}$.

- Consideremos equações

$$a_0x + b_0y + c_0 = 0 \quad \text{e} \quad x^2 + y^2 + a_1x + b_1y + c_1 = 0$$

que representam uma recta e uma circunferência com coeficientes em $\mathbb{F}$, respectivamente. Admitindo que a intersecção destes dois objectos é não vazia e que b_0 é não nulo, a equação da recta reescreve-se $y = \frac{c_0 - a_0x}{b_0}$ e sua intersecção com a circunferência determina um ou dois pontos de abcissas que verificam uma equação do tipo

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

onde a, b, c são números construíveis de $\mathbb{F}$. Ou seja,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Se $\sqrt{b^2 - 4ac} \in \mathbb{F}$, então (x, y) é um ponto construível de $\mathbb{F}$; caso contrário, o ponto de intersecção pertence a uma extensão quadrática de $\mathbb{F}$.

No caso em que $b_0 = 0$, a equação da recta reduz-se a $x = -\frac{c_0}{a_0}$ e a sua intersecção com a circunferência é descrita pela equação

$$y^2 + b_1y + b_2 = 0$$

onde $b_2 \in \mathbb{F}$. A conclusão é análoga ao caso anterior.

- Finalmente, se

$$x^2 + y^2 + a_1x + b_1y + c_1 = 0 \quad \text{e} \quad x^2 + y^2 + a_2x + b_2y + c_2 = 0$$

são as equações de duas circunferências distintas com coeficientes em $\mathbb{F}$, então determinar o(s) ponto(s) de intersecção destes objectos, corresponde a encontrar a solução do sistema

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0 \end{cases}$$

ou do equivalente

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0 \\ (a_2 - a_1)\, x + (b_2 - b_1)\, y + c_2 - c_1 = 0 \end{cases}$$

sendo que este último sistema traduz a intersecção de uma recta com uma circunferência com coeficientes em $\mathbb{F}$ que, como vimos no ponto anterior, conduz a um elemento que pertence a $\mathbb{F}$ ou está em alguma extensão quadrática de $\mathbb{F}$. ■

Voltemos à prova da proposição (5.1.1). Este lema garante que o ponto P_k pertence a alguma extensão quadrática de $\mathbb{F}_{n-1}$, $\mathbb{F}_n$ digamos, como queríamos provar.

Reciprocamente, suponhamos que existe uma sequência finita de corpos $\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_n$ com $a \in \mathbb{F}_n$ e tal que $\mathbb{F}_i$ é uma extensão quadrática de $\mathbb{F}_{i-1}$ para qualquer $i = 1, 2, \ldots, n$. Queremos ver que a é um número construível. Se $n = 0$ então $a \in \mathbb{F}_0 = \mathbb{Q}$ e portanto é construível. Admitamos por indução, que os números de $\mathbb{F}_{n-1}$ são construíveis. Como $\mathbb{F}_n$ é uma extensão quadrática de $\mathbb{F}_{n-1}$, então $\mathbb{F}_n = \{a + b\sqrt{\alpha} : a, b \in \mathbb{F}_{n-1}\}$ para algum $\alpha \in \mathbb{F}_{n-1}$ tal que $\sqrt{\alpha} \notin \mathbb{F}_{n-1}$. Logo existem $\widehat{a}, \widehat{b} \in \mathbb{F}_{n-1}$ tais que $a = \widehat{a} + \widehat{b}\sqrt{\alpha}$. Por hipótese de indução os números $\widehat{a}, \widehat{b}, \alpha$ são construíveis e portanto a também é construível. ■

Consideremos a extensão quadrática $\mathbb{Q}\left(\sqrt{2}\right)$ do corpo dos racionais. Um polinómio de coeficientes racionais de que $\sqrt{2}$ é raiz é $x^2 - 2$; mas $\sqrt{2}$ também é raiz dos polinómios $x^3 - 2x$ ou $x^4 - 5x^2 + 6$.

Cada número construível é raiz de uma infinidade de polinómios com coeficientes racionais. Este facto motiva a seguinte definição:

Definição 5.1.3 *Seja a é um número construível. O* ***polinómio minimal*** *de a é o único polinómio mónico com coeficientes racionais e de grau mínimo que se anula em a.*

Que só existe um polinómio minimal resulta do facto de, se p e q o forem, então $p-q$ teria grau estritamente inferior e ainda se anularia em a, contrariando a minimalidade de p (ou q). Averiguar se um determinado polinómio é minimal pode não ser tarefa fácil. Porém, os conceitos de polinómio minimal e polinómio mónico irredutível são equivalentes.

O grau do polinómio minimal dá-nos informação sobre a construtibilidade de um número, como se pode ver na proposição que se segue.

Proposição 5.1.4 *Se um número a é construível, então o grau do seu polinómio minimal é uma potência de dois.*

Prova. Seja a um número construível. Pela proposição (5.1.1), existe uma sequência finita de extensões quadráticas do corpo dos racionais $\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_n$ tal que $a \in \mathbb{F}_n$ e $\mathbb{F}_i$ é um subcorpo de $\mathbb{R}$, para todo $i = 1, 2, \ldots, n$. Além disso, cada um destes $\mathbb{F}_i$'s pode ser encarado como um espaço vectorial de dimensão 2 sobre $\mathbb{F}_{i-1}$. Logo

$$[\mathbb{F}_n : \mathbb{Q}] = [\mathbb{F}_n : \mathbb{F}_{n-1}] [\mathbb{F}_{n-1} : \mathbb{F}_{n-2}] \ldots [\mathbb{F}_1 : \mathbb{Q}] = 2^n$$

Por outro lado, $a \in \mathbb{F}_n$ logo $\mathbb{Q} \subset \mathbb{Q}(a) \subset \mathbb{F}_n$, e temos que

$$[\mathbb{F}_n : \mathbb{Q}] = [\mathbb{F}_n : \mathbb{Q}(a)] [\mathbb{Q}(a) : \mathbb{Q}].$$

Como $[\mathbb{F}_n : \mathbb{Q}]$ é uma potência de 2, $[\mathbb{Q}(a) : \mathbb{Q}]$ tem necessariamente que ser uma potência de 2; sendo que este é o grau do polinómio minimal de a sobre $\mathbb{Q}$. ■

5.2 Números complexos construíveis

Estendamos a noção de construtibilidade ao conjunto dos números complexos.

Definição 5.2.1 *Um* ***número complexo*** *$z = a + bi$, com $a, b \in \mathbb{R}$ diz-se* ***construível*** *se a e b forem números construíveis (e portanto, se e só se o ponto (a, b) for construível).*

Seja $z = a + bi$ um número complexo construível. Por definição, a e b são números reais construíveis e portanto, pela proposição (5.1.1), existem sequências finitas de extensões quadráticas sobre o corpo dos números racionais

$$\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_n \quad \text{com} \quad a \in \mathbb{F}_n$$

e

$$\mathbb{Q} = \mathbb{G}_0 \subset \mathbb{G}_1 \subset \ldots \subset \mathbb{G}_m \quad \text{com} \quad b \in \mathbb{G}_m.$$

Para cada $j = 1, 2, \ldots, m$, o corpo $\mathbb{G}_j = \mathbb{G}_{j-1}\left(\sqrt{\alpha_{j-1}}\right)$ para algum $\sqrt{\alpha_{j-1}} \notin \mathbb{G}_{j-1}$. Se fizermos extensões sucessivas do corpo $\mathbb{F}_n$ adicionando cada elemento do conjunto $\left\{\sqrt{\alpha_{j-1}} : j = 1, 2, \ldots, m\right\}$, obtemos um novo corpo $\mathbb{F}_{n+m}$ que contém a e b. Logo existe uma sequência finita de corpos $\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_{n+m} \subset \mathbb{F}_{n+m}(i)$ que contém o complexo z. Reciprocamente, se existir uma sequência nestas condições, o argumento usado na prova da proposição (5.1.1) mostra que z é um número construível. Assim, provámos o seguinte resultado:

Proposição 5.2.2 *As seguintes afirmações são equivalentes*

1. *z é um número complexo construível.*

2. *Existe uma sequência finita de subcorpos de $\mathbb{C}$, $\mathbb{Q} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \ldots \subset \mathbb{F}_n$ com $z \in \mathbb{F}_n$ e tal que $\mathbb{F}_i$ é uma extensão quadrática de $\mathbb{F}_{i-1}$ para qualquer $i = 1, 2, \ldots, n$.*

Para os números complexos também vale uma proposição análoga a (5.1.4).

Proposição 5.2.3 *Se um número complexo z é construível, então o grau do seu polinómio minimal é uma potência de dois.*

No próximo capítulo dedicar-nos-emos ao estudo dos polígonos regulares construíveis na circunferência usando somente régua não graduada e compasso. A construtibilidade de raízes da unidade desempenha nesse contexto um papel bastante importante, por isso vamos decidir para dois casos particulares se estas raízes são ou não construíveis.

Definição 5.2.4 *Um número complexo ω diz-se uma* ***raiz n-ésima da unidade*** *se $\omega^n = 1$. Além disso, se $\omega^t \neq 1$ para todo $t = 1, 2, \ldots, n-1$ diz-se que ω é uma* ***raiz primitiva n-ésima da unidade****.*

Proposição 5.2.5 *Seja p um número primo e ω uma raiz primitiva p-ésima da unidade. Então o grau do polinómio minimal de ω sobre $\mathbb{Q}$ é $p-1$.*

Prova. Seja p um número primo e ω uma raiz primitiva p-ésima da unidade, então ω é raiz do polinómio

$$\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1.$$

Temos agora que provar que este polinómio é irredutível. Com a mudança de variável $x = u+1$, este quociente reescreve-se

$$\begin{aligned} \frac{x^p-1}{x-1} &= \frac{(u+1)^p-1}{u} \\ &= u^{p-1} + \binom{p}{1}u^{p-2} + \binom{p}{2}u^{p-3} + \cdots + \binom{p}{p-2}u + \binom{p}{p-1}. \end{aligned}$$

Pelo critério de irredutibilidade de Eisenstein, é suficiente provar que o primo p divide $\binom{p}{i}$ para todo $i = 1, 2, \ldots, p-1$ pois p não divide 1 e p^2 não divide $\binom{p}{p-1} = p$. Ora, para qualquer $1 \leq i \leq p-1$, $\binom{p}{i} \in \mathbb{N}$ pelo que $p|\binom{p}{i}$.

Em virtude do automorfismo

$$\begin{array}{rccc} \varphi: & \mathbb{C}[x] & \longrightarrow & \mathbb{C}[x] \\ & f(x) & \mapsto & f(x-1) \end{array}$$

enviar polinómios irredutíveis em polinómios irredutíveis, segue que

$$x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$$

é um polinómio irredutível. ■

Decorre da proposição (5.2.3) que as raízes primitivas p-ésimas da unidade com p primo são construíveis só se $p = 2^k + 1$ para algum $k \in \mathbb{N}$. Estudemos agoras as raízes primitivas p^2-ésimas da unidade, cuja relevância se manifestará no próximo capítulo.

Proposição 5.2.6 *Seja p um número primo e ω uma raiz primitiva p^2-ésima da unidade. Então o grau do polinómio minimal de ω sobre $\mathbb{Q}$ é $p(p-1)$.*

Prova. Seja p um número primo e ω uma raiz primitiva p^2-ésima da unidade. Então ω^t $(t \in \mathbb{N})$ é uma raiz primitiva p^2-ésima da unidade se e

só se p^2 e t são primos entre si. Vejamos porquê. Se p^2 e t têm factores em comum então ω^t é uma raiz p-ésima da unidade

$$\left(\omega^t\right)^p = \left(\omega^{p^2}\right)^{\frac{t}{p}} = 1$$

pois t é múltiplo inteiro de p. Reciprocamente, se p^2 e t são primos entre si e ω^t não é uma raiz primitiva p^2-ésima da unidade, então existe algum $1 \leq k \leq p^2 - 1$ tal que kt é múltiplo inteiro de p^2; caso contrário, pelo algoritmo da divisão de Euclides, existiriam inteiros q e r com $1 \leq r \leq p^2 - 1$ tais que $kt = qp^2 + r$ e portanto

$$\left(\omega^t\right)^k = \left(\omega^{p^2}\right)^q \omega^r = \omega^r = 1$$

contrariando o facto de ω ser uma raiz primitiva p^2-ésima da unidade. Logo $r = 0$ e p^2 divide kt; mas como $(p^2, t) = 1$, p^2 divide k o que não pode acontecer uma vez que $k < p^2$.

Logo $\omega^p, \omega^{2p}, \ldots, \omega^{p(p-1)}, \omega^{p^2}$ são raízes não primitivas p^2-ésimas da unidade. Mas qualquer um destes p números é raiz do polinómio $x^p - 1$. Logo ω é raiz do polinómio

$$\begin{aligned}\frac{x^{p^2}-1}{x^p-1} &= (x^p)^{p-1} + (x^p)^{p-2} + \ldots + (x^p)^2 + x^p + 1 \\ &= \sum_{i=1}^{p} (x^p)^{p-i}.\end{aligned}$$

Para provar que este polinómio é irredutível, recorreremos à mudança de variável $x = u + 1$. Assim

$$\begin{aligned}\frac{x^{p^2}-1}{x^p-1} &= \sum_{i=1}^{p} ((u+1)^p)^{p-i} \\ &= \sum_{i=1}^{p} \left(u^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} u^k\right)^{p-i} \\ &= \sum_{i=1}^{p} \left((u^p+1)^{p-i} + \sum_{j=0}^{p-i-1} \binom{p-i}{j} (u^p+1)^j \left(\sum_{k=1}^{p-1} \binom{p}{k} u^k\right)^{p-i-j}\right) \\ &= \sum_{i=1}^{p} \left((u^p+1)^{p-i} + h_i(u)\right)\end{aligned}$$

onde $h_i(u)$ é um polinómio de grau $p(p-i)-1$. Precisamos agora de mostrar que o polinómio $h_i(u)$ é múltiplo de p, isto é, que existe um polinómio de coeficientes inteiros $g_i(u)$ tal que $h_i(u) = pg_i(u)$.

O facto de p ser um número primo garante, tal como vimos na demonstração da proposição (5.2.5), que p divide $\binom{p}{k}$ para todo $1 \leq k \leq p-1$. Como, $\frac{\binom{p}{k}}{p}$ é um inteiro, $h_i(u) = pg_i(u)$ para algum polinómio $g_i(u)$ com coeficientes inteiros. Assim, podemos reescrever

$$\begin{aligned}\frac{x^{p^2}-1}{x^p-1} &= \sum_{i=1}^{p}\left((u^p+1)^{p-i} + pg_i(u)\right) \\ &= \sum_{i=1}^{p}(u^p+1)^{p-i} + pG(u)\end{aligned}$$

para algum polinómio $G(u)$ de grau p^2-p-1. Como

$$\sum_{i=1}^{p}(u^p+1)^{p-i} = \frac{(u^p+1)^p-1}{u^p},$$

então

$$\begin{aligned}\frac{x^{p^2}-1}{x^p-1} &= \frac{(u^p+1)^p-1}{u^p} + pG(u) \\ &= \frac{u^{p^2} + \sum_{i=0}^{p-1}\binom{p}{i}u^{pi}}{u^p} + pG(u) \\ &= u^{p(p-1)} + pR(u)\end{aligned}$$

onde $R(u)$ é um polinómio de grau $p(p-1)-1$ com coeficientes inteiros. Para podermos aplicar o critério de irredutibilidade de Eisenstein precisamos de garantir que p^2 não divide o termo independente de $u^{p(p-1)} + pR(u)$. Substituindo u por 0 na soma $\sum_{i=1}^{p}((u+1)^p)^{p-i}$, determinamos o valor do termo independente que é p, que não é divisível por p^2. Como as mudanças de variável lineares não alteram a irredutibilidade de um polinómio, segue que

$$(x^p)^{p-1} + (x^p)^{p-2} + \ldots + (x^p)^2 + x^p + 1$$

é irredutível. Além disso, como admite ω como raiz, este é também o polinómio minimal de ω e tem grau $p\,(p-1)$. ■

Para qualquer primo $p > 2$, $p\,(p-1)$ tem um factor ímpar, logo não é uma potência de 2 e portanto a proposição (5.2.3) afirma que as raízes primitivas p^2-ésimas da unidade não são construíveis.

Capítulo 6

Divisão da circunferência em partes iguais

Neste capítulo recordaremos, segundo o texto [Hadlock], **que polígonos regulares podem ser inscritos numa circunferência usando apenas régua não graduada e compasso**. A construção de um polígono regular de n lados é equivalente à construção das raízes n-ésimas da unidade, ou seja, à construção dos números complexos $e^{2k\pi i/n}$, onde $k = 0, 1, \ldots, n-1$.

6.1 O contributo de Gauss

Gauss determinou uma condição necessária para que um polígono regular possa ser construído com régua não graduada e compasso. Vejamos em detalhe este argumento.

Lema 6.1.1 *Se o polígono regular de n lados for construível, então também é construível o polígono regular de m lados, onde $m \geq 3$ é um divisor de n.*

Prova. Sejam $P_1, P_2, \ldots, P_n$ os vértices do polígono regular de n lados enumerados sequencialmente, por exemplo em sentido horário. Se $m \geq 3$ for um divisor de n, então existe $k \in \mathbb{N}$ tal que $n = mk$. O polígono regular de m lados obtém-se a partir do anterior unindo sucessivamente os vértices P_{lk+1} a $P_{(l+1)k+1}$, onde $0 \leq l \leq m-1$ e $P_{mk+1} = P_{n+1} = P_1$. ■

A proposição que se segue, caracteriza os divisores primos de um tal n.

Proposição 6.1.2 *Se o polígono regular de n lados for construível e p for um divisor primo ímpar de n, então existe $k \in \mathbb{N}_0$ tal que $p = 2^{2^k} + 1$.*

Prova. Sendo p um divisor primo ímpar de n, $p \geq 3$ e pelo lema (6.1.1) é construível o polígono regular de p lados. Isto é equivalente a afirmar que são construíveis as raízes primitivas p-ésimas da unidade. Estas raízes são, como vimos na proposição (5.2.5), raízes de um polinómio com coeficientes racionais de grau $p-1$. Pela proposição (5.2.3), $p = 2^t + 1$ para algum t natural. Resta-nos mostrar que t é uma potência de 2. No caso em que $t = 1$, $k = 0$. Suponhamos que $t > 1$. Se t não é uma potência de 2, então t tem pelo menos um factor primo ímpar $q \geq 3$. Seja r natural tal que $t = qr$. Assim,

$$\begin{aligned} p &= 2^t + 1 \\ &= (2^r)^q + 1 \\ &= (2^r + 1)\left[(2^r)^{q-1} - (2^r)^{q-2} + \ldots + (2^r)^2 - 2^r + 1\right]. \end{aligned}$$

Esta factorização contradiz a primalidade de p pois

$$2^r + 1 \geq 3$$

e o outro factor, que possui q parcelas e pode-se escrever da seguinte forma

$$\underbrace{\left((2^r)^{q-1} - (2^r)^{q-2}\right)}_{>0} + \ldots + \underbrace{\left((2^r)^2 - 2^r\right)}_{>0} + 1$$

é também maior que um. Logo t é uma potência de 2 e os divisores primos de n são da forma $2^{2^k} + 1$, para algum $k \in \mathbb{N}_0$. ■

Como 7 não é da forma $2^{2^k} + 1$ para nenhum $k \in \mathbb{N}_0$, decorre que o heptágono regular não é construível com régua não graduada e compasso. Os números primos da forma $2^{2^n} + 1$, com $n \in \mathbb{N}_0$, dizem-se **números primos de Fermat**.

Gauss provou que os polígonos regulares construíveis têm necessariamente que satisfazer a seguinte condição:

Teorema 6.1.3 *Se um polígono regular de n lados é construível, então*

$$n = 2^k p_1 p_2 \ldots p_t$$

onde $k \in \mathbb{N}_0$ e $p_1, p_2, \ldots, p_t$ são primos de Fermat distintos.

Prova. Suponhamos que é construível o polígono regular de n lados. Pela Teorema Fundamental da Aritmética, existem $q_1, q_2, \ldots q_l$ primos distintos ímpares e $r \in \mathbb{N}_0$, $\alpha_1, \alpha_2, \ldots \alpha_l \in \mathbb{N}$ tais que $n = 2^r q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_l^{\alpha_l}$. O esquema que se segue descreve os passos essenciais da demonstração deste teorema:

Pode construir-se o polígono regular de n lados
$n = 2^r q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_l^{\alpha_l}$

$\Big\downarrow$ proposição 6.1.4

$\alpha_i = 1 \qquad \forall i \in \{1,\ldots l\}$

$\Big\downarrow$ proposição 6.1.2

q_i é um primo de Fermat

Proposição 6.1.4 *Se for construível um polígono regular de n lados e se $q > 2$ for um factor primo de n, então q^2 não divide n.*

Prova. Seja $q > 2$ um factor primo de n. Se q^2 dividisse n então pelo lema (6.1.1) seria possível construir um polígono regular de q^2 lados, isto é, seria possível construir as raízes primitivas q^2-ésimas da unidade. Mas vimos, na proposição (5.2.6), que estas raízes não são construíveis. Logo q^2 não é divisor de n. ■ ■

6.2 O contributo de Wantzel

Wantzel provou que a condição necessária estabelecida por Gauss é também suficiente.

Teorema 6.2.1 *É possível construir um polígono regular de $n \geq 3$ lados se n for da forma*

$$n = 2^k p_1 p_2 \ldots p_m$$

onde $k \in \mathbb{N}_0$ e $p_1, p_2, \ldots, p_t$ são primos de Fermat distintos.

O argumento para n primo de Fermat é essencialmente aritmético, em $\mathbb{Z}_n$. Aplicando indução a uma pirâmide de somas de raízes primitivas

n-ésimas da unidade cujo topo é composto por uma dessas raízes primitivas concluimos que este é construível, o que garante que o polígono regular de n lados é construível. No entanto, o argumento não é construtivo, não indica como construir o polígono regular de n lados, apenas prova que a construção é possível.

Prova. Se for conhecida a construção de um polígono regular de l lados então também se conhece a construção para o polígono regular de $2^k l$ ($k \in \mathbb{N}$) lados, pois este obtém-se do anterior por sucessivas bissecções dos seus lados. Assim, ficamos reduzidos a construir um polígono regular de $p_1 p_2 \dots p_m$ lados, onde os p_i's são primos de Fermat distintos.

Comecemos por mostrar que é possível construir um polígono regular de p lados, onde $p = 2^{2^r} + 1$, com $r \in \mathbb{N}_0$, é um número primo de Fermat. Seja ω uma raiz primitiva p-ésima da unidade. Queremos provar que ω é construível.

Seja g uma raiz primitiva módulo p, isto é, um número inteiro $g \geq 2$ tal que $g^{p-1} = 1 \bmod p$ mas $g^m \neq 1 \bmod p$ para todo $m = 1, 2, \dots, p-2$, (vide [Hadlock], página 102). Assim os $p-1$ números $g, g^2, g^3, \dots, g^{p-1}$ são todos incongruentes módulo p e nenhum é congruente com zero (se $g^i = 0 \bmod p$ para algum i, então $g^{p-1} = 0 \bmod p$ – igualdade incompatível com o facto de g ser uma raiz primitiva da unidade). Deste modo, as raízes primitivas p-ésimas da unidade, que são os elementos do conjunto $\{\omega, \omega^2, \dots, \omega^{p-1}\}$, podem ser representadas por

$$\omega^g, \omega^{g^2}, \dots, \omega^{g^{p-1}}.$$

Doravante, denotaremos ω^k por $[k]$. Assim, o conjunto das raízes primitivas p-ésimas da unidade é composto pelos elementos

$$S = \left\{ [g], \left[g^2\right], \dots, \left[g^{p-1}\right] \right\}.$$

Note-se que cada elemento do conjunto S é a g-ésima potência do seu antecessor.

Defina-se

$$S_1 = \left\{ [g], \left[g^3\right], \left[g^5\right], \dots, \left[g^{p-2}\right] \right\}$$

e

$$S_2 = \left\{ \left[g^2\right], \left[g^4\right], \left[g^6\right], \dots, \left[g^{p-1}\right] \right\}.$$

Cada um destes conjuntos é gerado por g^2-ésimas potências de qualquer um dos seus elementos. Podemos também observar que as sucessivas g^2-ésimas

potências do primeiro elemento de S geram o conjunto S_1 enquanto que as do segundo elemento de S geram S_2. Cada conjunto S_i $(i = 1, 2)$ pode, de forma análoga, ser subdividido em dois conjuntos S_{i1} e S_{i2}: os elementos de S_{i1} são gerados pelas sucessivas g^4-ésimas potências do primeiro elemento de S_i e os elementos de S_{i2} são gerados pelas sucessivas g^4-ésimas potências do segundo elemento de S_i. Este processo pode ser iterado tantas vezes quantas as necessárias até obteremos conjuntos singulares. Vamos introduzir alguns conceitos para formalizar este processo iterativo.

Designaremos por m-**conjunto** cada um dos conjuntos resultantes após m iterações. De acordo com esta terminologia,

S é um 0-conjunto;
S_1 e S_2 são 1-conjuntos;
S_{11}, S_{12}, S_{21} e S_{22} são 2-conjuntos

Cada um dos m-conjuntos pode ser gerado por sucessivas g^{2^m}-ésimas potências de qualquer um dos seus elementos e contém exactamente $\frac{p-1}{2^m}$ elementos. Cada m-conjunto, $S_{i_1 i_2 \ldots i_m}$ ($i_j = 1$ ou $i_j = 2$ para qualquer $j = 1, 2, \ldots, m$), dá origem a dois $(m+1)$-conjuntos, a saber $S_{i_1 i_2 \ldots i_m 1}$ e $S_{i_1 i_2 \ldots i_m 2}$. Os conjuntos resultantes da divisão de cada m-conjunto dizem-se **conjuntos complementares**. Como $p - 1 = 2^{2^r}$ para algum $r \in \mathbb{N}$, a iteração de ordem $m = 2^r$ isola cada uma das raízes primitivas p-ésima da unidade.

A soma dos elementos de um conjunto será designada por **período**. O período de um m-conjunto diz-se um m-**período**. Dois m-**períodos** dizem-se **complementares** se forem m-períodos de conjuntos complementares.

Proposição 6.2.2 *Cada m-período ($m = 0, 1, \ldots, 2^r$) é um número construível.*

Prova. Esta prova será feita usando indução sobre o valor de m.

Para $m = 0$, ω é uma raiz do polinómio $x^p - 1$, logo a soma de todas as raízes primitivas p-ésimas da unidade vale -1, isto é,

$$\omega^{p-1} + \omega^{p-2} + \ldots + \omega^2 + \omega = -1.$$

Logo o único 0-período é um número construível.

Fixemos $m \in \{1, 2, \ldots, 2^r\}$ e suponhamos que todos os períodos de ordem inferior a m são construíveis. Seja η_1 um m-período e η_2 o m-período complementar. Provemos que $\eta_1 + \eta_2$ e $\eta_1 \eta_2$ são números construíveis. De facto,

se tal acontecer, como estes números são as raízes da equação quadrática de coeficientes construíveis

$$x^2 - (\eta_1 + \eta_2)\, x + \eta_1 \eta_2 = 0$$

segue que o m-período η_1 (e η_2) é construível, o que termina o argumento de indução.

Por hipótese de indução, está garantida a construtibilidade de $\eta_1 + \eta_2$ pois este é precisamente um $(m-1)$-período. Vejamos agora o que acontece com $\eta_1\eta_2$. Ora, η_1 e η_2 representam a soma dos elementos de m-conjuntos S e $\tilde{S}$ complementares. O conjunto $S \cup \tilde{S}$ é um $(m-1)$-conjunto gerado pelas sucessivas $g^{2^{m-1}}$-ésimas potências de algum ω^k. Consideremos $h = g^{2^{m-1}}$. Então

$$S \cup \tilde{S} = \left\{ [k], [kh], \left[kh^2\right], \ldots, \left[kh^{t-1}\right] \right\}$$

onde $t = \frac{p-1}{2^{m-1}}$ pois a potência seguinte já repete elementos de $S \cup \tilde{S}$

$$h^t = \left(g^{2^{m-1}}\right)^{\frac{p-1}{2^{m-1}}} = g^{p-1} = 1 \bmod p.$$

No caso particular em que $m = 2^r$, o conjunto $S \cup \tilde{S} = \{[k], [kh]\}$ e portanto, $\eta_1\eta_2 = 1$ que é um número construível, pois como g é uma raiz primitiva módulo p e $p = 2^{2^r} + 1$, temos

$$h^2 = 1 \bmod p \qquad \text{e} \qquad h = -1 \bmod p.$$

Falta analisar o caso em que $m < 2^r$. Ora, por construção de S e $\tilde{S}$,

$$\left\{ \begin{array}{rcl} \eta_1 & = & [k] + [kh^2] + \ldots + [kh^{t-2}] \\ \eta_2 & = & [kh] + [kh^3] + \ldots + [kh^{t-1}] \end{array} \right. .$$

O produto $\eta_1\eta_2$ pode por isso ser escrito convenientemente da seguinte forma

$$\begin{array}{rcccccccc} \eta_1\eta_2 & = & [k+kh] & + & [kh^2+kh^3] & + & \ldots & + & [kh^{t-2}+kh^{t-1}] \\ & + & [k+kh^3] & + & [kh^2+kh^5] & + & \ldots & + & [kh^{t-2}+kh] \\ & + & [k+kh^5] & + & [kh^2+kh^7] & + & \ldots & + & [kh^{t-2}+kh^3] \\ & & \vdots & & \vdots & & \vdots & & \vdots \\ & + & [k+kh^{t-1}] & & [kh^2+kh] & + & \ldots & + & [kh^{t-2}+kh^{t-3}]\,. \end{array}$$

Observemos agora que:

1) Cada linha da soma de $\eta_1\eta_2$ é gerada pelas sucessivas h^2-ésimas potências de qualquer um dos seus elementos;

2) Nenhum dos expoentes é congruente com 0 módulo p.

   Basta ver o que acontece com os expoentes da primeira coluna, as restantes colunas tem uma análise idêntica Se

$$k + kh^{2j+1} = 0 \bmod p$$

   para algum $0 \leq j \leq \frac{t-2}{2}$, então, como p e k são primos entre si, ter-se-ia

$$h^{2j+1} = -1 \bmod p$$

   e portanto

$$\begin{aligned} h^{4j+2} &= 1 \bmod p \\ g^{2^{m-1}(4j+2)} &= 1 \bmod p \end{aligned}$$

   ou seja, $2^{m-1}(4j+2)$ seria múltiplo de $p-1$ porque g é uma raiz primitiva módulo p. Por outro lado,

$$2 \leq 4j + 2 \leq 2t - 2 = \frac{p-1}{2^{m-2}} - 2$$

   o que implica que

$$2^{m-1}(4j+2) \leq 2(p-1) - 2^m < 2(p-1)$$

   e portanto

$$2^{m-1}(4j+2) = p - 1$$

   ou seja,

$$p - 1 = 2^m(2j+1).$$

   Uma vez que $p-1$ não tem factores ímpares, o único valor possível para j é o zero, o que conduz a uma contradição:

$$p - 1 = 2^m < 2^{2^r} = p - 1.$$

   Logo nenhum dos expoentes é congruente com zero módulo p.

3) O produto $\eta_1\eta_2$ é composto pela soma de $\frac{p-1}{2^m}$ linhas, onde cada uma representa um m-período. Além disso, o m-período da i-ésima linha é complementar do da $\left(\frac{p-1}{2^m} - i\right)$-ésima linha. E é sempre possível emparelhar duas linhas pois estas são em número par.

Decorre das observações anteriores que o produto $\eta_1\eta_2$ é soma de $\frac{p-1}{2^{m+1}}$ números construíveis por serem $(m-1)$-períodos. Logo $\eta_1\eta_2$ é construível. ■

Como todos os m-períodos são construíveis, em particular também o são os 2^r-períodos. Como já havíamos observado, cada 2^r-período representa uma raiz primitiva p-ésima da unidade. Logo quando p é um número primo de Fermat, é construível o polígono regular de p lados.

Para concluir a prova deste teorema falta mostrar apenas que se p e q são primos entre si e são construíveis os polígonos regulares de p e q lados então é construível o polígono regular de pq lados. Por hipótese são construíveis os ângulos $\frac{2\pi}{p}$ e $\frac{2\pi}{q}$. Como p e q são primos entre si, existem pelo Algoritmo de Euclides, $s, t \in \mathbb{Z}$ tais que

$$1 = sp + tq$$

ou seja,

$$\frac{2\pi}{pq} = \frac{2\pi s}{q} + \frac{2\pi t}{p}$$

isto é, o ângulo $\frac{2\pi}{pq}$ é soma de múltiplos de ângulos construíveis e por isso é ele próprio um ângulo construível. ■

Capítulo 7

Divisão da lemniscata em partes iguais

Construir, com régua não graduada e compasso, um polígono regular de n lados é equivalente a dividir, com estes instrumentos, uma circunferência em n partes iguais. O que significa construir as raízes n-ésimas da unidade, $e^{\frac{2k\pi i}{n}}$ onde $k = 0, 1, \ldots, n-1$, ou equivalentemente, construir os números reais $sen\left(\frac{2k\pi}{n}\right)$ com $k = 0, 1, \ldots, n-1$, uma vez que o seno e cosseno trigonométricos se relacionam por uma igualdade quadrática.

Destes procedimentos, por falta de simetria, o que generalizaremos para a lemniscata será apenas o correspondente à última formulação – substituindo-se 2π, comprimento da circunferência unitária, por 2ω, comprimento da lemniscata. Ou seja, analisaremos para que valores de n é possível construir os valores de $senlem\left(\frac{2k\omega}{n}\right)$, onde $k = 0, 1, \ldots, n-1$. O título deste capítulo é, portanto, sobretudo sugestivo; o conteúdo segue de perto o artigo [Rosen].

Comecemos por reformular o argumento da divisão da circunferência em partes iguais para posteriormente o adaptar ao caso da lemniscata.

7.1 Novo olhar sobre a divisão da circunferência

A aplicação definida por

$$\begin{array}{rccc} \xi: & \frac{\mathbb{R}}{<2\pi>} & \to & S^1 \\ & [t] & \mapsto & e^{i[t]} \end{array}$$

é uma bijecção entre $\frac{\mathbb{R}}{<2\pi>}$ e a circunferência unitária, S^1. Como $\left(\frac{\mathbb{R}}{<2\pi>}, +\right)$ é um grupo com a operação de adição usual podemos, por transporte de estrutura, munir S^1 de uma estrutura de grupo. A operação induzida em S^1, "$*$", coincide com a operação produto, "$\cdot$", dos números complexos unitários: sejam z e w dois elementos de S^1; por transporte de estrutura temos que

$$z * w = \xi\left(\xi^{-1}(z) + \xi^{-1}(w)\right).$$

Como ξ é uma bijecção, existem $t, s \in \mathbb{R}$ tais que $z = \xi(t)$ e $w = \xi(s)$. Assim

$$\begin{array}{rcl} z * w & = & \xi\left(\xi^{-1}(\xi([t])) + \xi^{-1}(\xi([s]))\right) \\ & = & \xi([t] + [s]) \\ & = & e^{i([t]+[s])} \\ & = & e^{i[t]} \cdot e^{i[s]} \\ & = & \xi([t]) \cdot \xi([s]) \\ & = & z \cdot w. \end{array}$$

Deste modo ξ é um homomorfismo de grupos, sendo $\xi([0]) = 1_{\mathbb{C}}$ o elemento neutro de $(S^1, \cdot)$.

Para cada n natural, consideremos o conjunto

$$C_n = \left\{z \in S^1 : z^d = 1_{\mathbb{C}} \text{ e } d \mid n\right\}.$$

Este conjunto representa as raízes n-ésimas da unidade (primitivas ou não).

Como ξ é um homomorfismo bijectivo,

$$\begin{aligned}
C_n &= \bigcup_{d|n} \left\{ \xi([t]) : (\xi([t]))^d = 1_{\mathbb{C}} \right\} \\
&= \bigcup_{d|n} \{ \xi([t]) : \xi([dt]) = \xi([0]) \} \\
&= \bigcup_{d|n} \{ \xi([t]) : [dt] = [0] \} \\
&= \bigcup_{d|n} \{ \xi([t]) : dt = 2k\pi \text{ para algum } k \in \mathbb{Z} \} \\
&= \bigcup_{d|n} \left\{ \xi([t]) : t = \frac{2k\pi}{d} \text{ onde } k = 0, 1, \ldots, d-1 \right\} \\
&= \left\{ \xi([t]) : t = \frac{2k\pi}{n} \text{ onde } k = 0, 1, \ldots, n-1 \right\} \\
&= \left\{ e^{i\frac{2k\pi}{n}} \text{ onde } k = 0, 1, \ldots, n-1 \right\} \\
&= \left\{ \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right) : k = 0, 1, \ldots, n-1 \right\}.
\end{aligned}$$

A descrição dos elementos de C_n mostra-nos que este conjunto é finito e possui n elementos.

Proposição 7.1.1 *C_n é invariante por automorfismos de $\mathbb{C}\setminus\{0\}$, para qualquer n natural.*

Prova. Sejam n natural e α um automorfismo de $(\mathbb{C}\setminus\{0\}, \cdot)$. Queremos mostrar que $\alpha(C_n) = C_n$ para qualquer $n \in \mathbb{N}$. Seja $z \in C_n$. Então $z^d = 1_{\mathbb{C}}$ para algum divisor d de n. Como α é um automorfismo, $\alpha\left(z^d\right) = \alpha(1_{\mathbb{C}})$, ou seja, $(\alpha(z))^d = 1_{\mathbb{C}}$ o que mostra que $\alpha(C_n) \subseteq C_n$. Para provar a inclusão contrária basta observar que α^{-1} é também um automorfismo e portanto a inclusão $\alpha^{-1}(C_n) \subseteq C_n$ é válida pelo argumento anterior. O automorfismo α aplicado a esta inclusão permite concluir que $C_n \subseteq \alpha(C_n)$. ■

Em particular, para qualquer $k \in \mathbb{N}$, o conjunto $C_n \subset S^1$ é invariante pelo morfismo

$$\begin{array}{rccc} \alpha_k : & \mathbb{C}\setminus\{0\} & \to & \mathbb{C}\setminus\{0\} \\ & z & \mapsto & z^k \end{array}.$$

Além disso, $\alpha_n(C_n) = 1_{\mathbb{C}}$ pois todos os elementos de C_n satisfazem a equação $z^n = 1$ o que prova o seguinte resultado:

Corolário 7.1.2 *C_n é um conjunto algébrico, para qualquer n natural.*

Por conseguinte, os elementos do conjunto

$$A = \left\{ sen\left(\frac{2k\pi}{n}\right) : k = 0, 1, \ldots, n-1 \right\}$$

são algébricos pois são a parte imaginária de complexos algébricos (vide [Niven], página 85). Convém recordar que a divisão da circunferência em n partes iguais, com régua não graduada e compasso, corresponde a exigir a algebricidade do conjunto A, e que cada um dos seus elementos seja construível. Vamos ver de que modo a Teoria de Galois pode auxiliar na resolução deste problema.

Como vimos no capítulo 5, um número α é construível, com régua não graduada e compasso, se e só se $\mathbb{Q}(\alpha)$ está contido nalgum corpo $\mathbb{K} \subseteq \mathbb{C}$ obtido a partir de um número finito de extensões quadráticas do corpo dos números racionais. Isto é equivalente a exigir que α esteja num corpo $\mathbb{K}$ que seja Galois sobre $\mathbb{Q}$ e tal que a ordem do grupo de Galois de $\mathbb{K}$ sobre $\mathbb{Q}$ seja uma potência de dois (vide [Brison]).

Defina-se $\mathbb{K}_n = \mathbb{Q}(C_n)$. A extensão $\frac{\mathbb{K}_n}{\mathbb{Q}}$ é Galois. Seja G_n o grupo de Galois da extensão $\frac{\mathbb{K}_n}{\mathbb{Q}}$, isto é,

$$G_n = \left\{ \alpha : \alpha \text{ é automorfismo de } \mathbb{K}_n \text{ e } \alpha_{|\mathbb{Q}} = Id_{\mathbb{Q}} \right\}.$$

A aplicação definida por

$$\begin{array}{rccccc} \mathcal{H}: & G_n & \to & Aut(C_n) & & \\ & \alpha & \mapsto & \mathcal{H}(\alpha): & C_n & \to & C_n \\ & & & & c_n & \mapsto & \alpha(c_n) \end{array}$$

é um monomorfismo entre G_n e os automorfismos de C_n. De facto, se α e $\widetilde{\alpha}$ são automorfismos de G_n e $c_n \in C_n$, então temos

$$\begin{aligned} \mathcal{H}((\alpha\widetilde{\alpha})(c_n)) &= \alpha\widetilde{\alpha}(c_n) \\ &= \alpha(\widetilde{\alpha}(c_n)) \\ &= \alpha(\mathcal{H}(\widetilde{\alpha})(c_n)) \\ &= \mathcal{H}(\alpha)(\mathcal{H}(\widetilde{\alpha})(c_n)) \\ &= \mathcal{H}(\alpha)\mathcal{H}(\widetilde{\alpha})(c_n); \end{aligned}$$

além disso, se $\alpha \neq \widetilde{\alpha}$, então existe algum $c_n \in C_n$ tal que $\alpha(c_n) \neq \widetilde{\alpha}(c_n)$, logo $\mathcal{H}(\alpha) \neq \mathcal{H}(\widetilde{\alpha})$ o que prova que $\mathcal{H}$ é um homomorfismo injectivo e portanto G_n é isomorfo a um subgrupo de $Aut(C_n)$.

Proposição 7.1.3 *A ordem do grupo $Aut(C_n)$ é uma potência de dois se e somente se $n = 2^k p_1 \dots p_t$ onde $k \in \mathbb{N}_0$ e $p_1, \dots, p_t$ são primos de Fermat distintos.*

Prova. Seja α um automorfismo de C_n. Atendendo a que os automorfismos enviam geradores em geradores, para caracterizar um automorfismo de C_n é suficiente definir a imagem do elemento $e^{i\frac{2\pi}{n}}$ porque os geradores de C_n são os elementos da forma $e^{i\frac{2a\pi}{n}}$ onde $1 \leq a \leq n-1$ e a fracção $\frac{a}{n}$ é irredutível. Temos então que $\alpha(1_{\mathbb{C}}) = 1_{\mathbb{C}}$ e $\alpha\left(e^{i\frac{2\pi}{n}}\right) = e^{i\frac{2\pi a}{n}}$, onde $1 \leq a \leq n-1$ e a fracção $\frac{a}{n}$ é irredutível. Logo

$$\#\{Aut(C_n)\} = \varphi(n)$$

onde φ é a função de Euler.

Para cada natural n, seja $2^{\alpha_0} q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$ a sua decomposição em factores primos, onde $q_1, q_2, \dots q_s$ são primos ímpares distintos, $\alpha_0 \in \mathbb{N}_0$ e $\alpha_1, \alpha_2, \dots \alpha_s \in \mathbb{N}$, então

$$\varphi(n) = \begin{cases} q_1^{\alpha_1 - 1} q_2^{\alpha_2 - 1} \dots q_s^{\alpha_s - 1} (q_1 - 1)(q_2 - 1) \dots (q_s - 1) & \text{se } \alpha_0 = 0 \\ 2^{\alpha_0 - 1} q_1^{\alpha_1 - 1} q_2^{\alpha_2 - 1} \dots q_s^{\alpha_s - 1} (q_1 - 1)(q_2 - 1) \dots (q_s - 1) & \text{se } \alpha_0 \in \mathbb{N} \end{cases}$$

(vide [Hardy]).

Suponhamos que $\varphi(n) = 2^l$ para algum $l \in \mathbb{N}$. Se n não é uma potência de dois, então $\alpha_i = 1$ para todo $i = 1, \dots, s$, caso contrário apareceriam factores distintos de dois na decomposição de $\varphi(n)$. Logo, se $\alpha_0 = 0$ temos

$$(q_1 - 1)(q_2 - 1) \dots (q_s - 1) = 2^l$$

senão temos

$$2^{\alpha_0 - 1} (q_1 - 1)(q_2 - 1) \dots (q_s - 1) = 2^l$$

o que implica que, para todo $i = 1, \dots, s$,

$$q_i = 2^{t_i} + 1$$

para algum $t_i \in \mathbb{N}$. Uma vez que q_i é primo vimos na demonstração da proposição (6.1.2) que t_i é uma potência de 2. E portanto os $q_i's$ são primos de Fermat distintos.

A implicação contrária é imediata. ■

Decorre desta prova que $Aut\,(C_n)$ é isomorfo a $\mathbb{Z}_n^*$ – subgrupo dos elementos invertiveis de $\mathbb{Z}_n$. Por outro lado, G_n também é isomorfo $\mathbb{Z}_n^*$ (vide [Brison], página 145), e portanto G_n é isomorfo a $Aut\,(C_n)$. Assim, a ordem de G_n é uma potência de dois se e só se $n = 2^k p_1 \dots p_t$ onde $k \in \mathbb{N}_0$ e $p_1, \dots, p_t$ são primos distintos de Fermat. Deste modo concluimos para que valores de n são construíveis os elementos de C_n.

O argumento para a lemniscata será uma reprodução fiel deste adaptado ao conjunto

$$A_L = \left\{ senlem\left(\frac{2k\omega}{n}\right) : k = 0, 1, \dots, n-1 \right\}.$$

Abel mostrou que a função seno da lemniscata pode ser estendida a uma função meromorfa de $\mathbb{C}$, ϕ, elíptica relativamente à rede $L =< 2\omega, 2\omega i >$, cujos zeros são pontos da rede $< \omega, \omega i >$ e cujos pólos se obtêm a partir dos zeros somando a cada um $\frac{\omega+\omega i}{2}$. Além disso deu uma fórmula para o cálculo de ϕ:

$$\phi\,(z) = z \prod_{\alpha} \left(1 - \frac{z^4}{\alpha^4}\right) \prod_{\beta} \left(1 - \frac{z^4}{\beta^4}\right)^{-1} \tag{7.1}$$

onde $\alpha \in \{\text{zeros de } \phi\}$, $\beta \in \{\text{pólos de } \phi\}$ e $0 \leq \arg z \leq \frac{\pi}{2}$. Provou ainda a fórmula de adição de ϕ

$$\phi\,(s+t) = \frac{\phi\,(s)\sqrt{1-\phi^4\,(t)} + \phi\,(t)\sqrt{1-\phi^4\,(s)}}{1+\phi^2\,(s)\,\phi^2\,(t)}$$

que se assemelha à fórmula de adição do seno trigonométrico.

De seguida, mostraremos que do ponto de vista da construtibilidade de $\phi\left(\frac{2k\omega}{n}\right)$, a função ϕ pode ser substituída pela função $\mathcal{P}$ de Weierstrass associada à rede $< 2\omega, 2\omega i >$.

7.2 Relação entre as funções ϕ e $\mathcal{P}$

Seja $\mathcal{P}$ a função de Weierstrass associada à rede $L =< 2\omega, 2\omega i >$.

Proposição 7.2.1 *A curva elíptica associada à rede L (veja-se a proposição 4.2.9) é neste caso, descrita pela equação*

$$y^2 = 4x^3 - \frac{x}{4}.$$

Prova. Temos que mostrar que

$$g_2 = g_2(L) = 60s_4 = 60 \sum_{0 \neq l \in L} l^{-4} = \frac{1}{4}$$

e

$$g_3 = g_3(L) = 140s_6 = 140 \sum_{0 \neq l \in L} l^{-6} = 0.$$

A última igualdade é imediata pois a rede L é invariante pela multiplicação do escalar i, isto é, $iL = L$:

$$\sum_{0 \neq l \in L} l^{-6} = \sum_{0 \neq l \in L} (il)^{-6} = -\sum_{0 \neq l \in L} l^{-6}$$

ou seja

$$\sum_{0 \neq l \in L} l^{-6} = 0$$

e portanto $g_3(L) = 0$. Para provar a primeira igualdade precisamos de estimar $\sum_{0 \neq l \in L} l^{-4}$. Ora, em geral,

Lema 7.2.2 *Seja $G = \{a + bi : (a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}\}$ o conjunto dos inteiros gaussianos não nulos. Então*

$$\sum_{G} (a + bi)^{-4} = \frac{\omega^4}{15}.$$

Prova. Para qualquer rede R, $\sum_{0\neq\gamma\in R} \gamma^{-4}$ denotar-se-á por $|R|$. Consideremos as redes R_1, R_2 e R_3 definidas do seguinte modo:

$$\begin{aligned} R_1 &= <\omega, \omega i> \\ R_2 &= \left\{ \frac{m+ni}{2}\omega : m,n \in \mathbb{Z} \text{ são ímpares} \right\} \\ R_3 &= \left\{ \frac{m+ni}{2}\omega : m,n \in \mathbb{Z} \text{ têm paridade distinta} \right\} \end{aligned}$$

Note-se que

$$|R_1| = \omega^{-4} \sum_{(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}} (a+bi)^{-4}$$

pelo que o nosso objectivo nesta prova passa por recorrer às redes R_2 e R_3 de modo a encontrar uma forma alternativa de calcular o valor de $|R_1|$. Comecemos por verificar que

$$\frac{1}{2}R_1 = R_1 \cup R_2 \cup R_3. \tag{7.2}$$

Sejam $r, s \in \mathbb{Z}$ tais que $(r+si)\,\omega \in R_1$. Então $\frac{r+si}{2}\omega$ é um elemento de R_1 se r e s são ambos pares; é um elemento de R_2 se r e s são ambos ímpares e é um elemento de R_3 se r e s têm paridades distintas. Logo $\frac{1}{2}R_1 \subseteq R_1 \cup R_2 \cup R_3$. A outra inclusão decorre do facto dos conjuntos R_1, R_2 e R_3 estarem contidos em $\frac{1}{2}R_1$.

As redes R_1, R_2 e R_3 representam conjuntos mutuamente disjuntos. De facto, se $R_1 \cap R_2 \neq \varnothing$, então existem $m, n, r, s \in \mathbb{Z}$ com m e n ímpares tais que

$$(r+si)\,\omega = \frac{m+ni}{2}\omega$$

o que implica que $m = 2r$ e $n = 2s$, o que é impossível sendo m e n ímpares. De forma inteiramente análoga se prova que $R_1 \cap R_3 = \varnothing$ e $R_2 \cap R_3 = \varnothing$.

Da igualdade (7.2) e do facto dos conjuntos R_1, R_2 e R_3 serem mutuamente disjuntos temos que

$$\left|\frac{1}{2}R_1\right| = |R_1| + |R_2| + |R_3|\,;$$

além disso,

$$\left|\frac{1}{2}R_1\right| = \sum_{0\neq\gamma\in R_1} \left(\frac{\gamma}{2}\right)^{-4} = 16 \sum_{0\neq\gamma\in R_1} \gamma^{-4} = 16\,|R_1|$$

logo

$$15\left|R_1\right| = \left|R_2\right| + \left|R_3\right|. \tag{7.3}$$

Por outro lado, se $m, n \in \mathbb{Z}$ e m e n são ímpares tais que $\frac{m+ni}{2}\omega \in R_2$, então

$$\frac{1+i}{2}\frac{m+ni}{2}\omega = \frac{\frac{m-n}{2} + \frac{m+n}{2}i}{2}\omega \in R_3$$

pois a paridade de $\frac{m-n}{2}$ e $\frac{m+n}{2}\left(= \frac{m-n}{2} + n\right)$ é distinta. Assim, fica provado que $\frac{1+i}{2}R_2 \subseteq R_3$. Para provar a inclusão contrária, consideremos $m, n \in \mathbb{Z}$ com paridades distintas, então

$$\frac{m+ni}{2}\omega = \frac{1+i}{2}\frac{(m+n)+(n-m)\,i}{2}\omega \in \frac{1+i}{2}R_2$$

pois $m+n$ e $m-n$ representam ambos números ímpares. Logo

$$\frac{1+i}{2}R_2 = R_3. \tag{7.4}$$

Mas

$$\left|\frac{1+i}{2}R_2\right| = \sum_{0\neq\gamma\in R_2}\left(\frac{1+i}{2}\gamma\right)^{-4} = -4\sum_{0\neq\gamma\in R_2}\gamma^{-4} = -4\left|R_2\right|,$$

e portanto da igualdade (7.4) resulta que

$$-4\left|R_2\right| = \left|R_3\right|. \tag{7.5}$$

Reunindo a informação das igualdades (7.3) e (7.5), segue que

$$\left|R_2\right| = -5\left|R_1\right|. \tag{7.6}$$

Da derivação logarítmica de

$$\phi(z) = z\prod_{\alpha\in R_1}\left(1-\frac{z^4}{\alpha^4}\right)\prod_{\beta\in R_2}\left(1-\frac{z^4}{\beta^4}\right)^{-1}$$

(isto é, da derivação da função $\ln\phi$) obtemos

$$\begin{aligned}
z\frac{\phi'(z)}{\phi(z)} &= 1 + \sum_{\alpha\in R_1} -\frac{4z^4}{\alpha^4 - z^4} - \sum_{\beta\in R_2} -\frac{4z^4}{\beta^4 - z^4} \\
&= 1 + \sum_{\beta\in R_2}\frac{1}{\beta^4}\frac{4z^4}{1-\frac{z^4}{\beta^4}} - \sum_{\alpha\in R_1}\frac{1}{\alpha^4}\frac{4z^4}{1-\frac{z^4}{\alpha^4}} \\
&= 1 + 4z^4\left(\sum_{\beta\in R_2}\frac{1}{\beta^4}\frac{1}{1-\frac{z^4}{\beta^4}} - \sum_{\alpha\in R_1}\frac{1}{\alpha^4}\frac{1}{1-\frac{z^4}{\alpha^4}}\right).
\end{aligned}$$

Os quocientes do segundo membro podem ser reescritos formalmente como séries de potências em zero:

$$\begin{aligned}\frac{1}{1-\frac{z^4}{\beta^4}} &= 1+\left(\frac{z}{\beta}\right)^4+\left(\frac{z}{\beta}\right)^8+\left(\frac{z}{\beta}\right)^{12}+\dots\\ \frac{1}{1-\frac{z^4}{\alpha^4}} &= 1+\left(\frac{z}{\alpha}\right)^4+\left(\frac{z}{\alpha}\right)^8+\left(\frac{z}{\alpha}\right)^{12}+\dots\end{aligned}$$

e portanto

$$\begin{aligned}z\frac{\phi'(z)}{\phi(z)} &= 1+4z^4\left(\sum_{\beta\in R_2}\tfrac{1}{\beta^4}\left(1+\left(\tfrac{z}{\beta}\right)^4+\left(\tfrac{z}{\beta}\right)^8+\left(\tfrac{z}{\beta}\right)^{12}+\dots\right)\right.\\ &\quad\left.-\sum_{\alpha\in R_1}\tfrac{1}{\alpha^4}\left(1+\left(\tfrac{z}{\alpha}\right)^4+\left(\tfrac{z}{\alpha}\right)^8+\left(\tfrac{z}{\alpha}\right)^{12}+\dots\right)\right)\\ &= 1+4z^4\left(\sum_{\beta\in R_2}\frac{1}{\beta^4}-\sum_{\alpha\in R_1}\frac{1}{\alpha^4}\right)+r(z),\end{aligned}$$

ou seja,

$$z\frac{\phi'(z)}{\phi(z)}=1+(|R_2|-|R_1|)\,z^4+r(z) \tag{7.7}$$

onde $r(z)$ é uma expressão que envolve apenas termos com potências de ordem superior a quatro.

Relembremos agora que a função ϕ restrita ao intervalo $[0,1]$ é a função *senlem* estudada no capítulo 3, e que esta nasceu como a inversa da função comprimento de arco da lemniscata, pelo que, para todo $z\in[0,1]$,

$$z=\int_0^{\phi(z)}\frac{dt}{\sqrt{1-t^4}}.$$

Derivando ambos os membros desta igualdade, obtemos

$$1=\frac{\phi'(z)}{\sqrt{1-\phi^4(z)}}$$

o que implica que

$$\phi'^2(z)=1-\phi^4(z), \tag{7.8}$$

igualdades que permanecem válidas para toda a extensão ϕ.

Calculando as sucessivas derivadas de ϕ em $z = 0$, obtemos $\phi(0) = 0$; $\phi'(0) = 1$; $\phi''(0) = 0$; $\phi'''(0) = 0$ e $\phi^{(4)}(0) = 0$; e portanto os desenvolvimentos em série de potências de ϕ e ϕ' em torno do ponto $z = 0$ são, respectivamente,

$$\begin{aligned} \phi(z) &= z + cz^5 + \dots \\ \phi'(z) &= 1 + 5cz^4 + \dots \end{aligned}$$

para algum $c \in \mathbb{R}$. Substituindo estes desenvolvimentos na igualdade (7.8) e comparando os coeficientes de z^4, concluimos que $c = -\frac{1}{10}$. Por outro lado, comparando os coeficientes de z^5 na igualdade (7.7), concluimos que

$$|R_2| - |R_1| = -\frac{2}{5} \tag{7.9}$$

pois

$$z\phi'(z) = \phi(z)\left(1 + (|R_2| - |R_1|)\, z^4 + \dots\right)$$

ou seja

$$z - \frac{z^5}{2} + \dots = \left(z - \frac{z^5}{10} + \dots\right)\left(1 + (|R_2| - |R_1|)\, z^4 + \dots\right).$$

Finalmente, reunindo a informação das igualdades (7.6) e (7.9), deduzimos que

$$|R_1| = \frac{1}{15}$$

e portanto

$$\sum_{a,b \in \mathbb{Z}\setminus\{0\}} (a + bi)^{-4} = \frac{\omega^4}{15}.$$

■

Retomemos a prova da proposição (7.2.1). Pelo lema anterior temos que

$$\begin{aligned} g_2 = 60 \sum_{0 \neq l \in L} l^{-4} &= 60 \sum_{a,b \in \mathbb{Z}\setminus\{0\}} (2a\omega + 2b\omega i)^{-4} \\ &= \frac{15}{4}\omega^{-4} \sum_{a,b \in \mathbb{Z}\setminus\{0\}} (a + bi)^{-4} \\ &= \frac{1}{4}. \end{aligned}$$

■

A proposição (7.2.1) informa que, a relação entre as funções $\mathcal{P}$ e $\mathcal{P}'$ de Weierstrass associadas à rede $L =< 2\omega, 2\omega i >$ é dado por

$$\mathcal{P}'^2 = 4\mathcal{P}^3 - \frac{\mathcal{P}}{4}. \tag{7.10}$$

Desta igualdade resulta que para qualquer $\alpha \in \mathbb{C}\backslash L$ é construível $\mathcal{P}'(\alpha)$ se $\mathcal{P}(\alpha)$ o for. O recíproco da afirmação anterior não é válido, no entanto, é possível afirmar que

Corolário 7.2.3 *Para qualquer $\alpha \in \mathbb{C}\backslash L$, $\mathcal{P}(\alpha)$ é construível se $\mathcal{P}'(\alpha)$ for nulo.*

Prova. Pela igualdade (7.10), dado $\alpha \in \mathbb{C}\backslash L$ sabemos que $\mathcal{P}'(\alpha) = 0$ se e somente se

$$\mathcal{P}(\alpha) = 0 \quad \text{ou} \quad 4\mathcal{P}^2(\alpha) - \frac{1}{4} = 0.$$

Em qualquer dos casos $\mathcal{P}(\alpha)$ é construível, no primeiro caso porque é um número racional e no segundo porque é raíz de um polinómio quadrático de coeficientes construíveis. ■

O uso da função $\mathcal{P}$ de Weierstrass em substituição da função ϕ é legitimado pelo próximo resultado.

Proposição 7.2.4 *Seja $\alpha \in \mathbb{C}\backslash L$. Então $\phi(\alpha)$ é construível se e só se $\mathcal{P}(\alpha)$ é construível.*

Prova. (se) Suponhamos que $\mathcal{P}(\alpha)$ é construível. Em $D(L)$, os zeros e pólos de ϕ são

$$\{0, \omega, i\omega, (1+i)\omega\}$$

e

$$\left\{\frac{1+i}{2}\omega, \frac{3+i}{2}\omega, \frac{1+3i}{2}\omega, \frac{3+3i}{2}\omega\right\}$$

respectivamente. Consideremos a função definida por

$$g(z) = \frac{\mathcal{P}'(z)}{(\mathcal{P}(z) - \mathcal{P}(z_0))(\mathcal{P}(z) - \mathcal{P}(z_1))}$$

onde $z_0 = \frac{1+i}{2}\omega$ e $z_1 = \frac{3+i}{2}\omega$. Os zeros de g em $D(L)$, são:

- zeros de $\mathcal{P}'(z)$, isto é, elementos de $\{\omega, i\omega, (1+i)\omega\}$ e

- pólos do denominador de g que não sejam compensados pelos pólos de $\mathcal{P}'(z)$. Mas em $D(L)$, $\mathcal{P}(z)$ e $\mathcal{P}'(z)$ têm um único pólo, a saber $z=0$. Como vimos em (4.7) e (4.8), o quociente $g(z)$ pode ser escrito da seguinte forma

$$g(z)=\frac{\left(-2+\sum_{n=2}^{\infty}a_n z^{2n}\right)z}{\left(1+\sum_{n=2}^{\infty}b_n z^{2n}-\mathcal{P}(z_0)\,z^2\right)\left(1+\sum_{n=2}^{\infty}b_n z^{2n}-\mathcal{P}(z_1)\,z^2\right)}.$$

  E portanto $z=0$ é também um zero de g.

Os pólos de g, em $D(L)$, são:

- zeros de $\mathcal{P}(z)-\mathcal{P}(z_0)$, isto é, elementos de $\left\{\frac{1+i}{2}\omega,\frac{3+3i}{2}\omega\right\}$;
- zeros de $\mathcal{P}(z)-\mathcal{P}(z_1)$, isto é, elementos de $\left\{\frac{3+i}{2}\omega,\frac{1+3i}{2}\omega\right\}$ e
- pólos de $\mathcal{P}'$ que não sejam compensados pelos pólos do denominador de g. O único candidato é $z=0$, mas este, como vimos, é um zero de g.

Logo, pela proposição (4.1.1),

$$\phi(z)=Ag(z)$$

para alguma constante A, porque as funções elípticas ϕ e g têm os mesmos zeros e pólos. Como $\phi\left(\frac{\omega}{2}\right)=1$, se $g\left(\frac{\omega}{2}\right)$ for construível, então A é construível. Daqui resultará que, para cada $\alpha\in\mathbb{C}\backslash L$,

$$\phi(\alpha)\text{ é construível }\Leftrightarrow\ g(\alpha)\ \text{ é construível.}$$

Ora, se $\mathcal{P}(z_0)$, $\mathcal{P}(z_1)$ e $\mathcal{P}\left(\frac{\omega}{2}\right)$ são construíveis (o que implica que $\mathcal{P}'\left(\frac{\omega}{2}\right)$ é construível pelo corolário 7.2.3)), então, da definição de g, resulta que $g\left(\frac{\omega}{2}\right)$ é construível.

Lema 7.2.5 *Se $\alpha\in\mathbb{C}\backslash L$ e $\mathcal{P}(\alpha)$ é construível então $\mathcal{P}\left(\frac{\alpha}{2}\right)$ é construível.*

Prova. Fixemos $\alpha\in\mathbb{C}\backslash L$. Da definição de $\mathcal{P}$ deduz-se que para todo o z em $\mathbb{C}\backslash L$, $\mathcal{P}(iz)=-\mathcal{P}(z)$ e, derivando, que $\mathcal{P}'(iz)=i\mathcal{P}'(z)$. Usando a

fórmula de adição de $\mathcal{P}$ e a que relaciona $\mathcal{P}$ e $\mathcal{P}'$, isto é, a igualdade (7.10), temos que

$$\mathcal{P}\left((1+i)\,z\right) = -\frac{i}{8}\frac{16\mathcal{P}^2\left(z\right)-1}{4\mathcal{P}\left(z\right)} \tag{7.11}$$

e

$$\mathcal{P}\left((1-i)\,z\right) = \frac{i}{8}\frac{16\mathcal{P}^2\left(z\right)-1}{4\mathcal{P}\left(z\right)}. \tag{7.12}$$

Fazendo $z = \frac{\alpha}{1+i}$ na igualdade (7.11), obtemos

$$\mathcal{P}\left(\alpha\right) = -\frac{i}{8}\frac{16\mathcal{P}^2\left(\frac{\alpha}{1+i}\right)-1}{4\mathcal{P}\left(\frac{\alpha}{1+i}\right)}$$

logo $\mathcal{P}\left(\frac{\alpha}{1+i}\right)$ satifaz a equação quadrática

$$\mathcal{P}^2\left(\frac{\alpha}{1+i}\right) - 2i\mathcal{P}\left(\alpha\right)\mathcal{P}\left(\frac{\alpha}{1+i}\right) + \frac{1}{16} = 0$$

cujos coeficientes são construíveis; e portanto $\mathcal{P}\left(\frac{\alpha}{1+i}\right)$ é construível. Fazendo $z = \frac{\alpha}{2}$ na igualdade (7.12), obtemos

$$\mathcal{P}\left(\left(1-i\right)\frac{\alpha}{2}\right) = \frac{i}{8}\frac{16\mathcal{P}^2\left(\frac{\alpha}{2}\right)-1}{4\mathcal{P}\left(\frac{\alpha}{2}\right)}$$

logo $\mathcal{P}\left(\frac{\alpha}{2}\right)$ satisfaz a equação quadrática de coeficientes construíveis

$$\mathcal{P}^2\left(\frac{\alpha}{2}\right) + 2i\mathcal{P}\left(\left(1-i\right)\frac{\alpha}{2}\right)\mathcal{P}\left(\frac{\alpha}{2}\right) - \frac{1}{16} = 0,$$

pois $\mathcal{P}\left(\left(1-i\right)\frac{\alpha}{2}\right) = \mathcal{P}\left(\frac{\alpha}{1+i}\right)$. E portanto $\mathcal{P}\left(\frac{\alpha}{2}\right)$ é construível. ■

Corolário 7.2.6 *$g\left(\frac{\omega}{2}\right)$ é construível.*

Prova. A proposição (4.2.10) e o corolário (7.2.3) garantem que os números $\mathcal{P}\left(\omega\right)$, $\mathcal{P}\left(i\omega\right) = -\mathcal{P}\left(\omega\right)$ e $\mathcal{P}\left(\left(1+i\right)\omega\right)$ são construíveis. Concluimos agora, pelo lema (7.2.5), que $\mathcal{P}\left(\frac{\omega}{2}\right)$ e $\mathcal{P}\left(z_0\right) = \mathcal{P}\left(\frac{(1+i)\omega}{2}\right)$ são construíveis. Além disso, $\mathcal{P}\left(\left(3+i\right)\omega\right) = \mathcal{P}\left(\left(1+i\right)\omega\right)$ e portanto, de novo pelo lema (7.2.5), $\mathcal{P}\left(z_1\right) = \mathcal{P}\left(\frac{(3+i)\omega}{2}\right)$ é construível. ■

Conclusão: $\mathcal{P}(\alpha)$ construível $\Rightarrow$ $g(\alpha)$ construível
$\Updownarrow$
$\phi(\alpha)$ construível.

(só se) O argumento para a implicação recíproca é análogo ao anterior depois de uma mudança conveniente nos geradores da rede L. Suponhamos agora que $\phi(\alpha)$ é construível. Se $a, b \in \mathbb{Z}$ então

$$\begin{aligned} 2a\omega + 2b\omega i &= (a+b)(1+i)\omega + (a-b)(1-i)\omega \\ &= (1+i)[b(1+i)\omega + a(1-i)\omega] \end{aligned}$$

logo $L = (1+i)M$ onde $M =< (1+i)\omega, (1-i)\omega >$. Seja $\mathcal{P}_1$ a função de Weierstrass associada à rede M. Então

$$\begin{aligned} 2i\mathcal{P}((1+i)z) &= \frac{2i}{((1+i)z)^2} + 2i\sum_{0\neq l\in L}\left(\frac{1}{((1+i)z-l)^2} - \frac{1}{l^2}\right) \\ &= \frac{1}{z^2} + \sum_{0\neq m\in M}\left(\frac{1}{(z-m)^2} - \frac{1}{m^2}\right) \\ &= \mathcal{P}_1(z), \end{aligned}$$

isto é,

$$\mathcal{P}_1(z) = 2i\mathcal{P}((1+i)z)$$

e portanto

$$\mathcal{P}_1'(z) = 2i(1+i)\mathcal{P}'((1+i)z).$$

Pela igualdade (7.11), obtemos uma relação as funções $\mathcal{P}$ e $\mathcal{P}_1$

$$\mathcal{P}_1(z) = \frac{16\mathcal{P}^2(z) - 1}{16\mathcal{P}(z)}. \tag{7.13}$$

Os zeros e pólos de ϕ, em $D(M)$, são $\{0, \omega\}$ e $\left\{\frac{1+i}{2}\omega, \frac{1-i}{2}\omega\right\}$ respectivamente. Estes são também os zeros e pólos, em $D(M)$, da função

$$h(z) = \frac{\mathcal{P}_1(z) - \mathcal{P}_1(\omega)}{\mathcal{P}_1'(z)}.$$

uma vez que:

- os zeros de h são:
  - os zeros de $\mathcal{P}_1(z) - \mathcal{P}_1(\omega)$, que em $D(M)$ correspondem apenas a ω
  - pólos de $\mathcal{P}_1'$, em $D(M)$, que não são compensados pelos pólos de $\mathcal{P}_1(z) - \mathcal{P}_1(\omega)$: tal como a aconteceu com a função g, o único pólo de $\mathcal{P}_1'$ nestas condições é zero que é zero de h;
- os pólos de h são os zeros de $\mathcal{P}_1'$, isto é, elementos de $\left\{\frac{1+i}{2}\omega, \frac{1-i}{2}\omega\right\}$. Note-se que 0 é pólo $\mathcal{P}_1(z) - \mathcal{P}_1(\omega)$, em $D(M)$, mas é zero de h e que ω é um zero de $\mathcal{P}_1'$ cuja ordem é inferior à ordem em $\mathcal{P}_1(z) - \mathcal{P}_1(\omega)$ e por isso transformou-se também em zero de h.

Logo, pela proposição (4.1.1)

$$\phi(z) = B\frac{\mathcal{P}_1(z) - \mathcal{P}_1(\omega)}{\mathcal{P}_1'(z)}$$

para alguma constante B porque as funções elípticas ϕ e h têm os mesmos zeros e pólos. Note-se que

$$\begin{cases} \mathcal{P}_1(\omega) &= 2i\mathcal{P}((1+i)\omega) \\ \mathcal{P}_1\left(\frac{\omega}{2}\right) &= 2i\mathcal{P}\left((1+i)\frac{\omega}{2}\right) \\ \mathcal{P}_1'\left(\frac{\omega}{2}\right) &= 2i(1+i)\mathcal{P}'\left((1+i)\frac{\omega}{2}\right) \end{cases}$$

e que acabámos de verificar que $\mathcal{P}((1+i)\omega)$ e $\mathcal{P}\left((1+i)\frac{\omega}{2}\right)$ – e portanto $\mathcal{P}'\left((1+i)\frac{\omega}{2}\right)$ pelo corolário (7.2.3) – são construíveis. Logo, como $\phi\left(\frac{\omega}{2}\right) = 1$, resulta que B é construível.

Sejam $u_0 = \frac{1+i}{2}\omega$ e $u_1 = \frac{1-i}{2}\omega$. Como os zeros de $\mathcal{P}_1'$, em $D(M)$, são os de $\mathcal{P}'((1+i)z)$, isto é, u_0, u_1 e ω, da prova da proposição (4.2.6) resulta que

$$\mathcal{P}_1'^2(z) = C(\mathcal{P}_1(z) - \mathcal{P}_1(u_0))(\mathcal{P}_1(z) - \mathcal{P}_1(u_1))(\mathcal{P}_1(z) - \mathcal{P}_1(\omega))$$

uma vez que $\mathcal{P}_1'^2(z)$ é uma função par. Além disso, fazendo $\alpha = 1+i$, temos

$$\begin{aligned} & \frac{\mathcal{P}_1'^2(z)}{(\mathcal{P}_1(z) - \mathcal{P}_1(u_0))(\mathcal{P}_1(z) - \mathcal{P}_1(u_1))(\mathcal{P}_1(z) - \mathcal{P}_1(\omega))} \\ = & \frac{\mathcal{P}'^2(\alpha z)}{(\mathcal{P}(\alpha z) - \mathcal{P}(\alpha u_0))(\mathcal{P}(\alpha z) - \mathcal{P}(\alpha u_1))(\mathcal{P}(\alpha z) - \mathcal{P}(\alpha\omega))} \\ = & \frac{\left(-\frac{2}{\alpha^3} + \sum_{n=2}^{\infty} a_n z^{2n}\right)^2}{\left(\frac{1}{\alpha^2} + \sum_{n=2}^{\infty} b_n z^{2n} - d_1 z^2\right)\left(\frac{1}{\alpha^2} + \sum_{n=2}^{\infty} b_n z^{2n} - d_2 z^2\right)\left(\frac{1}{\alpha^2} + \sum_{n=2}^{\infty} b_n z^{2n} - d_3 z^2\right)} \end{aligned}$$

função que vale 4 em $z = 0$. Logo $C = 4$. E portanto

$$\begin{aligned}\phi^2(z) &= \frac{B^2}{4}\frac{\left(\mathcal{P}_1(z)-\mathcal{P}_1(\omega)\right)^2}{\left(\mathcal{P}_1(z)-\mathcal{P}_1(u_0)\right)\left(\mathcal{P}_1(z)-\mathcal{P}_1(u_1)\right)\left(\mathcal{P}_1(z)-\mathcal{P}_1(\omega)\right)} \\ &= \frac{B^2}{4}\frac{\mathcal{P}_1(z)-\mathcal{P}_1(\omega)}{\left(\mathcal{P}_1(z)-\mathcal{P}_1(u_0)\right)\left(\mathcal{P}_1(z)-\mathcal{P}_1(u_1)\right)}\end{aligned}$$

o que implica que, se $\phi(\alpha)$ é construível, então $\mathcal{P}_1(\alpha)$ também é uma vez que:

- como já vimos,

$$\begin{cases}\mathcal{P}_1(\omega) &= 2i\mathcal{P}\left((1+i)\omega\right) \\ \mathcal{P}_1(u_0) &= 2i\mathcal{P}(\omega i) \\ \mathcal{P}_1(u_1) &= 2i\mathcal{P}(\omega)\end{cases}$$

  são construíveis

- de

$$\phi^2(\alpha) = \frac{B^2}{4}\frac{\mathcal{P}_1(\alpha)-\mathcal{P}_1(\omega)}{\left(\mathcal{P}_1(\alpha)-\mathcal{P}_1(u_0)\right)\left(\mathcal{P}_1(\alpha)-\mathcal{P}_1(u_1)\right)}$$

  concluimos que $\mathcal{P}_1(\alpha)$ satisfaz a equação quadrática de coeficientes construíveis

$$X\mathcal{P}_1^2(\alpha) + Y\mathcal{P}_1(\alpha) + Z = 0$$

  onde

$$\begin{cases}X &= 4\phi^2(\alpha) \\ Y &= -4\phi^2(\alpha)\left(\mathcal{P}_1(u_1)-\mathcal{P}_1(u_0)\right) - B^2 \\ Z &= 4\phi^2(\alpha)\mathcal{P}_1(u_0)\mathcal{P}_1(u_1) + B^2\mathcal{P}_1(\omega)\end{cases}.$$

A construtibilidade de $\mathcal{P}(\alpha)$ deduz-se finalmente da igualdade (7.13). ■

Esta proposição permite-nos voltar ao estudo da função $\mathcal{P}$ de Weierstrass e investigar os valores de n para os quais os números $\mathcal{P}\left(\frac{2k\omega}{n}\right)$ com $k = 0, 1, \ldots, n-1$, são construíveis.

7.3 A solução para a lemniscata

Relembremos que para a rede $L =< 2\omega, 2\omega i >$, o conjunto E apresentado na secção 4.3, representa os pontos de $\mathbb{C}^2$ que estão na curva elíptica $y^2 = 4x^3 - \frac{x}{4}$ juntamente com o ponto infinito.

Proposição 7.3.1 *A aplicação*

$$\begin{array}{rccc} \xi: & \frac{\mathbb{C}}{L} & \longrightarrow & E \\ & (z) & \mapsto & \begin{cases} (\mathcal{P}(z), \mathcal{P}'(z)) & se \quad z \notin L \\ (\infty, \infty) & se \quad z \in L \end{cases} \end{array}$$

é uma bijecção.

Prova. Comecemos por mostrar que ξ é uma aplicação injectiva. Sejam $z_1, z_2 \in \mathbb{C}$ e suponhamos que $\xi(z_1) = \xi(z_2)$. Se $\xi(z_1) = \xi(z_2) = (\infty, \infty)$, então $z_1, z_2 \in L$ e portanto $(z_1) = (z_2)$. Caso contrário, temos

$$(\mathcal{P}(z_1), \mathcal{P}'(z_1)) = (\mathcal{P}(z_2), \mathcal{P}'(z_2))$$

isto é,

$$\mathcal{P}(z_1) = \mathcal{P}(z_2) \quad \text{e} \quad \mathcal{P}'(z_1) = \mathcal{P}'(z_2). \tag{7.14}$$

Da primeira igualdade de (7.14) segue que

$$(z_1) = (z_2) \quad \text{ou} \quad (z_1) = (-z_2).$$

Se $(z_1) = (-z_2)$ então, da segunda igualdade de (7.14) e do facto de $\mathcal{P}'$ ser uma função ímpar, concluiríamos que z_2 era uma raiz de $\mathcal{P}'$. Pela proposição (4.2.10) ter-se-ia que

$$(z_2) = (\omega) \quad \text{ou} \quad (z_2) = (i\omega) \quad \text{ou} \quad (z_2) = ((1+i)\omega).$$

Mas então $(z_2) = (-z_2)$ e portanto temos a igualdade $(z_1) = (z_2)$. Logo ξ é uma aplicação injectiva.

Vejamos agora que ξ é uma aplicação sobrejectiva. Para qualquer $\lambda \in L$, $\xi(\lambda) = (\infty, \infty)$. Seja agora $(x, y) \in E \setminus \{(\infty, \infty)\}$. Queremos encontrar $z \in \mathbb{C} \setminus L$ tal que

$$\xi(z) = (x, y)$$

Defina-se $g(z) = \mathcal{P}(z) - x$. Em $D(L)$, a função $\mathcal{P}$ tem um único pólo, a saber 0, cuja multiplicidade é dois, logo pela proposição (4.1.3), a função

g tem exactamente dois zeros, em $D(L)$, contados de acordo com as suas multiplicidades, digamos z_1 ez_2. Assim $\mathcal{P}(z_1) = \mathcal{P}(z_2) = x$. Resta-nos verificar se

$$\mathcal{P}'(z_1) = y.$$

Por definição dos pontos de E, e pelo facto de $x = \mathcal{P}(z_1)$, devemos ter

$$y^2 = 4\mathcal{P}^3(z_1) - \frac{\mathcal{P}(z_1)}{4} = \mathcal{P}'^2(z_1)$$

e portanto $\mathcal{P}'(z_1) = \pm y$. Se $\mathcal{P}'(z_1) = y$, então

$$\begin{aligned} \xi(z_1) &= (\mathcal{P}(z_1), \mathcal{P}'(z_1)) \\ &= (x, y). \end{aligned}$$

Se $\mathcal{P}'(z_1) = -y$, então $\mathcal{P}'(-z_1) = y$ porque $\mathcal{P}'$ é uma função ímpar; e como $\mathcal{P}$ é uma função par, $\mathcal{P}(-z_1) = \mathcal{P}(z_1) = x$, logo

$$\begin{aligned} \xi(-z_1) &= (\mathcal{P}(-z_1), \mathcal{P}'(-z_1)) \\ &= (x, y). \end{aligned}$$

Logo ξ é sobrejectiva. ■

Corolário 7.3.2 *Se em $\frac{\mathbb{C}}{L}$ considerarmos a operação quociente da soma usual em $\mathbb{C}$ e em E a operação induzida por transporte de estrutura feita pela bijecção ξ, então $\frac{\mathbb{C}}{L}$ e E são grupos isomorfos.*

Prova. Só falta mostrar que ξ é um homomorfismo. Designemos por "$+$" a soma em $\frac{\mathbb{C}}{L}$ e por "$\boxplus$" a soma em E. Sejam (a, b) e $(c, d) \in E$. Como ξ é sobrejectiva, existem $c_1, c_2 \in \mathbb{C}$ tais que

$$(c_1) = \xi^{-1}((a, b)) \quad \text{e} \quad (c_2) = \xi^{-1}((c, d)).$$

Assim, por definição de transporte,

$$\begin{aligned} (a, b) \boxplus (c, d) &= \xi(c_1) \boxplus \xi(c_2) \\ &= \xi((c_1) + (c_2)). \end{aligned}$$

E portanto, dados z_1 e z_2 de $\mathbb{C}$

$$\begin{aligned} \xi((z_1) + (z_2)) &= \xi\left(\xi^{-1}(\xi(z_1)) + \xi^{-1}(\xi(z_2))\right) \\ &= \xi\left(\xi^{-1}(\xi(z_1))\right) \boxplus \xi\left(\xi^{-1}(\xi(z_2))\right) \\ &= \xi(z_1) \boxplus \xi(z_2). \end{aligned}$$

■

Note-se que a definição de "$\boxplus$" corresponde à igualdade

$$(\mathcal{P}(z_1+z_2),\mathcal{P}'(z_1+z_2)) = (\mathcal{P}(z_1),\mathcal{P}'(z_1)) \boxplus (\mathcal{P}(z_2),\mathcal{P}'(z_2))$$

para todo o z_1 e z_2 de $\mathbb{C}\backslash L$ e que (0) e ∞ são respectivamente o elemento neutro de $\frac{\mathbb{C}}{L}$ e de E.

Para cada $n \in \mathbb{N}$, consideremos o conjunto dos pontos de E cuja ordem divide n, isto é,

$$E_n = \{e \in E : ke = \infty \quad \text{e} \quad k \mid n\}.$$

Estes conjuntos vão ter aqui o papel que os conjuntos C_n desempenham na divisão da circunferência em partes iguais. Como ξ é sobrejectiva, para cada $e \in E_n$ existe $z \in \mathbb{C}$ tal que $\xi(z) = e$. Além disso, como ξ é um homomorfismo, temos que

$$\xi(kz) = k\xi(z) = ke = \infty = \xi(0).$$

Logo

$$\begin{aligned}
E_n &= \bigcup_{k|n} \{\xi(z) : \xi(kz) = \xi(0)\} \\
&= \bigcup_{k|n} \{\xi(z) : kz \in L\} \\
&= \bigcup_{k|n} \{\xi(z) : kz = 2a\omega + 2bi\omega \text{ para alguns } a,b \in \mathbb{Z}\} \\
&= \bigcup_{k|n} \left\{\xi(z) : z = \frac{2a\omega + 2bi\omega}{k} \text{ onde } 0 \le a,b < k\right\} \\
&= \left\{\xi(z) : z = \frac{2a\omega + 2bi\omega}{n} \text{ onde } 0 \le a,b < n\right\} \\
&= \left\{\left(\mathcal{P}\left(\frac{2a\omega + 2bi\omega}{n}\right), \mathcal{P}'\left(\frac{2a\omega + 2bi\omega}{n}\right)\right) : 0 \le a,b < n\right\}
\end{aligned}$$

Daqui se deduz que E_n é um conjunto com um número finito de elementos.

Proposição 7.3.3 *Para cada n natural, os elementos de E_n são algébricos.*

Prova. De acordo com a descrição do conjunto E_n basta-nos verificar que os elementos do conjunto

$$\left\{\mathcal{P}\left(\frac{2a\omega + 2bi\omega}{n}\right) : 0 \le a,b < n\right\}$$

são algébricos porque, como já foi observado na secção anterior, $\mathcal{P}$ e $\mathcal{P}'$ relacionam-se pela igualdade (7.10) e o conjunto dos números algébricos é um corpo. A fórmula de adição para a função $\mathcal{P}$ de Weierstrass e o facto de $\mathcal{P}(i\omega) = -\mathcal{P}(\omega)$ faz com que só seja necessário mostrar a algebricidade dos elementos do conjunto

$$\left\{\mathcal{P}\left(\frac{k\omega}{n}\right) : 0 \leq k < n\right\}.$$

Pela proposição (7.2.4), mostrar que cada elemento deste conjunto é algébrico é equivalente a mostrar que os elementos do conjunto

$$\left\{\phi\left(\frac{k\omega}{n}\right) : 0 \leq k < n\right\}$$

são algébricos. Usando a fórmula de adição da função ϕ (semelhante à fórmula de adição do seno trigonométrico) e o facto desta se anular nos múltiplos inteiros de ω (recordemos que a função ϕ restrita ao conjunto dos números reais coincide com a função seno da lemniscata estudada no capítulo 3), é possível exibir um polinómio de coeficientes racionais que admite uma raiz em $\phi\left(\frac{k\omega}{n}\right)$, procedimento em tudo análogo ao que é usual para $sen\left(\frac{k\pi}{n}\right)$, que permite concluir que os elementos de E_n são algébricos. ■

Defina-se $\mathbb{K}_n = \mathbb{Q}(E_n)$. A extensão $\frac{\mathbb{K}_n}{\mathbb{Q}}$ é Galois (vide [Brison]). Seja G_n o grupo de Galois da extensão $\frac{\mathbb{K}_n}{\mathbb{Q}}$. A aplicação definida por

$$\begin{array}{rccccc} \mathcal{H}: & G_n & \to & Aut(E_n) & & \\ & \alpha & \mapsto & \mathcal{H}(\alpha): & E_n & \to & E_n \\ & & & & e_n & \mapsto & \alpha(e_n) \end{array}$$

é um monomorfismo entre G_n e os automorfismos de E_n e portanto G_n é isomorfo a um subgrupo de $Aut(E_n)$. À semelhança do que foi feito para a divisão da circunferência em partes iguais, deveríamos agora demonstrar que a ordem do grupo dos automorfismo de E_n é uma potência de dois de modo a garantir a construtibilidade dos elementos de E_n. Porém

$$Aut(E_n) \approx Aut\left(\frac{L}{nL}\right) \approx Aut(\mathbb{Z}_n \oplus \mathbb{Z}_n) \approx GL_2(\mathbb{Z}_n)$$

sendo que a ordem deste último grupo nunca é uma potência de dois. O argumento utilizado na divisão da circunferência não se adapta textualmente ao caso da lemniscata. Observemos contudo que a rede $L =< 2\omega, 2\omega i >$ tem uma estrutura adicional. De facto

$$\begin{aligned} L &= < 2\omega, 2\omega i > \\ &= \{2a\omega + 2bi\omega : a, b \in \mathbb{Z}\} \\ &= \{(a + bi)\, 2\omega : a, b \in \mathbb{Z}\} \\ &= \mathbb{Z}(i)\,(2\omega) \end{aligned}$$

possui uma estrutura de $\mathbb{Z}(i)$ módulo. Assim, $\frac{\mathbb{C}}{L}$ e por intermédio do isomorfismo ξ da proposição (7.3.1), E são $\mathbb{Z}(i)$ módulos sendo a acção de i em E dada por $i(x, y) = (-x, iy)$ uma vez que, como vimos,

$$\begin{aligned} \xi(iz) &= (\mathcal{P}(iz), \mathcal{P}'(iz)) \\ &= (-\mathcal{P}(z), i\mathcal{P}'(z)) \end{aligned}$$

para todo o z de $\mathbb{C}\backslash L$. Retomemos então o argumento anterior mas agora a partir de $\mathbb{K} = \mathbb{Q}(i)$ e da extensão $\mathbb{K}_n = \mathbb{K}(E_n)$ que é Galois sobre $\mathbb{K}$.

Proposição 7.3.4 *Para cada $n \in \mathbb{N}$, o conjunto E_n é invariante pelos automorfismos de $\mathbb{K}_n$.*

Prova. Sejam n natural e α um automorfismo de $\mathbb{K}_n$. Comecemos por provar a inclusão $\alpha(E_n) \subseteq E_n$. Seja $e \in E_n$. Por definição de E_n, $ne = \infty$. Como α é um automorfismo, $n\alpha(e) = \alpha(ne) = \alpha(1_{\mathbb{C}}) = \infty$, o que mostra que $\alpha(E_n) \subseteq E_n$. Usando idêntica inclusão para α^{-1}, obtemos a inclusão complementar, $\alpha(E_n) \supseteq E_n$. ■

Seja $\mathcal{G}_n$ o grupo de Galois da extensão $\frac{\mathbb{K}_n}{\mathbb{K}}$. Como $\mathcal{G}_n$ deixa invariante os elementos de $\mathbb{K}$, a acção de $\mathcal{G}_n$ em E_n preserva a estrutura de $\mathbb{Z}(i)$ módulo e portanto existe um monomorfismo entre $\mathcal{G}_n$ e $Aut_{\mathbb{Z}(i)}(E_n)$. Logo $\mathcal{G}_n$ é um subgrupo de $Aut_{\mathbb{Z}(i)}(E_n)$. Falta-nos agora averiguar em que condições é que a ordem do grupo dos automorfismo de E_n enquanto $\mathbb{Z}(i)$ módulo é uma potência de dois.

Proposição 7.3.5 *A ordem do grupo $Aut_{\mathbb{Z}(i)}(E_n)$ é uma potência de dois se e somente se $n = 2^k p_1 \dots p_t$, onde $k \in \mathbb{N}_0$ e $p_1, \dots, p_t$ são primos de Fermat distintos.*

Prova. Em primeiro lugar, observemos que

$$E_n \approx \frac{\frac{1}{n}L}{L} \approx \frac{L}{nL} \approx \frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}$$

enquanto $\mathbb{Z}(i)$ módulos. E portanto

$$Aut_{\mathbb{Z}(i)}(E_n) \approx Aut_{\mathbb{Z}(i)}\left(\frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}\right).$$

Mas

$$Aut_{\mathbb{Z}(i)}\left(\frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}\right) \approx \left(\frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}\right)^*$$

onde $\left(\frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}\right)^*$ designa o conjunto de unidades do anel $\frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}$. Além disso,

Lema 7.3.6 *A ordem dos invertíveis de $\frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}$ é uma potência de dois se e somente se $n = 2^k p_1 \dots p_t$, onde $k \in \mathbb{N}_0$ e $p_1, \dots, p_t$ são primos de Fermat distintos.*

Prova. Seja n um natural. Se a factorização de n é dada por $2^l q_1^{\alpha_1} q_2^{\alpha_2} \dots q_r^{\alpha_r}$, onde $l \in \mathbb{N}_0$ e os q_i's são primos ímpares, a ordem dos invertíveis de $\mathbb{Z}_n(i) = \frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}$, que designaremos por $|\mathbb{Z}_n(i)^*|$, é dada por

$$\begin{cases} \prod\limits_{\substack{p \text{ primo,} \\ p=1 \bmod 4 \\ p|n}} p^{2\alpha_i-2}(p-1)^2 \prod\limits_{\substack{p \text{ primo,} \\ p=3 \bmod 4 \\ p|n}} p^{2\alpha_i-2}(p^2-1) & \text{se} \quad l=0 \\ 2^{2l-1} \prod\limits_{\substack{p \text{ primo,} \\ p=1 \bmod 4 \\ p|n}} p^{2\alpha_i-2}(p-1)^2 \prod\limits_{\substack{p \text{ primo,} \\ p=3 \bmod 4 \\ p|n}} p^{2\alpha_i-2}(p^2-1) & \text{se} \quad l \in \mathbb{N} \end{cases}.$$

Tendo em conta que

$$\varphi(n) = n \prod_{\substack{p \text{ primo} \\ p|n}} \left(\frac{p-1}{p}\right),$$

$|\mathbb{Z}_n(i)^*|$ pode reescrever-se como

$$\begin{cases} \varphi(n) \prod\limits_{\substack{p \text{ primo,} \\ p=1 \bmod 4 \\ p|n}} p^{\alpha_i-1}(p-1) \prod\limits_{\substack{p \text{ primo,} \\ p=3 \bmod 4 \\ p|n}} p^{\alpha_i-1}(p+1) & \text{se} \quad l=0 \\ 2\varphi^2(n) \prod\limits_{\substack{p \text{ primo,} \\ p=3 \bmod 4 \\ p|n}} \frac{p+1}{p-1} & \text{se} \quad l \in \mathbb{N} \end{cases}$$

onde φ designa a função de Euler.

Se $n = 2^k p_1 \dots p_t$, onde $k \in \mathbb{N}_0$, cada $p_i = 2^{2^{\beta_i}} + 1$ é primo de Fermat e os p_i's são distintos, então, como vimos, $\varphi(n)$ é uma potência de dois. Além disso, o único primo de Fermat que é congruente com 3 módulo 4 é 3; se este aparece na factorização de n, então a fórmula de $|\mathbb{Z}_n(i)^*|$ contém o factor

$$\prod_{\substack{p \text{ primo,} \\ p=3 \bmod 4 \\ p|n}} p^{\alpha_i - 1}(p+1) = 4$$

ou

$$\prod_{\substack{p \text{ primo,} \\ p=3 \bmod 4 \\ p|n}} \frac{p+1}{p-1} = \frac{4}{2} = 2.$$

E assim

$$\begin{aligned} |\mathbb{Z}_n(i)^*| &= 4\varphi(n) \prod_{\substack{p \text{ primo,} \\ p=3 \bmod 4 \\ p|n}} p^{\alpha_i - 1}(p-1) \\ &= 4\varphi(n) \prod_{\substack{p \text{ primo,} \\ p=3 \bmod 4 \\ p|n}} (p-1) \\ &= 4\varphi(n) \prod_{\substack{p \text{ primo,} \\ p=3 \bmod 4 \\ p|n}} 2^{2^{\beta_i}} \end{aligned}$$

ou

$$\begin{aligned} |\mathbb{Z}_n(i)^*| &= 2\varphi^2(n) \prod_{\substack{p \text{ primo,} \\ p=3 \bmod 4 \\ p|n}} \frac{p+1}{p-1} \\ &= 4\varphi^2(n); \end{aligned}$$

trata-se, em ambos os casos, de uma potência de dois.

Reciprocamente, das fórmulas para $|\mathbb{Z}_n(i)^*|$ e $\varphi(n)$ deduzimos que $|\mathbb{Z}_n(i)^*|$ é divisível por $\varphi(n)$. E portanto, se $|\mathbb{Z}_n(i)^*|$ é uma potência de dois, então $\varphi(n)$ é uma potência de dois. Como vimos, isto implica que n é produto de

uma potência de dois por um conjunto finito de primos de Fermat distintos.
■ ■

Este resultado, juntamente com o Teorema de Lagrange, garante que a ordem de $\mathcal{G}_n$ é uma potência de dois se e só se $n = 2^k p_1 \dots p_t$, onde $k \in \mathbb{N}_0$ e $p_1, \dots, p_t$ são primos distintos de Fermat. Pela proposição (7.2.4) temos que:

Proposição 7.3.7 *Se $n = 2^k p_1 \dots p_t$, onde $k \in \mathbb{N}_0$ e $p_1, \dots, p_t$ são primos de Fermat distintos, então os elementos do conjunto*

$$\left\{ \phi\left(\frac{2l\omega}{n}\right) : l = 0, 1, \dots . n-1 \right\}$$

são construíveis.

Por outras palavras, este resultado diz-nos que, para os valores de n explicitados no enunciado da proposição, é possível dividir a lemniscata com régua não graduada e compasso em n partes iguais. Recordemos que no capítulo 6, vimos que este mesmo resultado é válido no caso da circunferência. Mostraremos de seguida que, tal como para a circunferência, também para a lemniscata vale o recíproco.

Teorema 7.3.8 *Se a lemniscata for divisível em n partes iguais então*

$$n = 2^k p_1 p_2 \dots p_t$$

onde $k \in \mathbb{N}_0$ e $p_1, \dots, p_t$ são primos de Fermat distintos.

Prova. Por hipótese, $\phi\left(\frac{2\omega}{n}\right)$ é um número construível, então pela proposição (7.2.4), $\mathcal{P}\left(\frac{2\omega}{n}\right)$ é construível. Além disso,

Lema 7.3.9 *Seja M o corpo gerado por $\left\langle \mathbb{Q}(i), \mathcal{P}^2\left(\frac{2\omega}{n}\right)\right\rangle$. Então a extensão $\frac{M}{\mathbb{Q}(i)}$ é Galois e o seu grupo de Galois é isomorfo a $\left(\frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}\right)^*$ módulo a imagem do grupo $\langle \pm 1, \pm i\rangle$.*

Prova. Sejam $L_0 = \mathbb{Z}(i)$, rede de $\mathbb{C}$, e $\mathcal{P}_0$ a função de Weierstrass associada a L_0. Consideremos a função

$$h: \quad z \quad \mapsto \quad g_2^{-1}(L_0)\,\mathcal{P}_0^2(z)$$

onde $g_2(L_0) = 4\omega^4$ pelo lema (7.2.2), ou seja,

$$h(z) = \frac{\omega^{-4}}{4}\mathcal{P}_0^2(z).$$

A extensão $\mathbb{Q}(i)\left(h\left(\frac{1}{n}\right)\right)$ de $\mathbb{Q}(i)$ é precisamente o grupo $\left(\frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}\right)^*$ módulo o subgrupo de 2^2 elementos $\langle \pm 1, \pm i\rangle$ (vide [Lang73], página 135). Ora

$$h\left(\frac{1}{n}\right) = \frac{\omega^{-4}}{4}\mathcal{P}_0^2\left(\frac{1}{n}\right).$$

Mas

$$\mathcal{P}_0(z) = (2\omega)^2 \mathcal{P}(2\omega z)$$

pois

$$\begin{aligned}
\mathcal{P}(2\omega z) &= \frac{1}{(2\omega z)^2} + \sum_{0\neq\lambda\in L}\left(\frac{1}{(2\omega z-\lambda)^2} - \frac{1}{\lambda^2}\right) \\
&= \frac{1}{(2\omega)^2}\left(\frac{1}{z^2} + \sum_{\alpha\in L_0}\left(\frac{1}{(z-\alpha)^2} - \frac{1}{\alpha^2}\right)\right) \\
&= \frac{1}{(2\omega)^2}\mathcal{P}_0(z).
\end{aligned}$$

E portanto

$$\begin{aligned}
h\left(\frac{1}{n}\right) &= \frac{\omega^{-4}}{4}(2\omega)^4\mathcal{P}^2\left(\frac{2\omega}{n}\right) \\
&= 4\mathcal{P}^2\left(\frac{2\omega}{n}\right).
\end{aligned}$$

■

Como $\mathcal{P}\left(\frac{2\omega}{n}\right)$ é construível, $\mathcal{P}^2\left(\frac{2\omega}{n}\right)$ também é construível e logo a ordem do grupo de Galois da extensão M sobre $\mathbb{Q}(i)$ é uma potência de dois (uma vez que a extensão $\mathbb{Q}(i)$ sobre $\mathbb{Q}$ tem ordem dois). Pelo lema (7.3.9), $\left(\frac{\mathbb{Z}(i)}{n\mathbb{Z}(i)}\right)^*$ tem ordem igual a uma potência de dois e portanto, pelo lema (7.3.6), $n = 2^k p_1 p_2 \ldots p_t$, onde $k \in \mathbb{N}_0$ e $p_1, p_2, \ldots, p_t$ são primos de Fermat distintos.
■

Bibliografia

[Brison] O. J. Brison, *Teoria de Galois*, Departamento de Matemática, Faculdade de Ciências da Universidade de Lisboa, 1999.

[Coimbra] C. Matos, J. C. Santos, *Curso de Análise Complexa*, Escolar Editora, 2000.

[Hadlock] C. R. Hadlock, *Field Theory and Its Classical Problems*, The Carus Mathematical Monographs N^o 19, The Mathematical Association of America, 1978.

[Hardy] G. Hardy, E. Wright, *An Introduction to the Theory of Numbers*, Oxford Science Publications, 1979.

[Ireland] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag 1990.

[Koch] H. Koch, *Number Theory, Algebraic Numbers and Functions*, Graduate Studies in Mathematics 24, AMS 2000.

[Kolmogorov] A.N. Kolmogorov, S.V. Fomin, *Elementos da Teoria das Funções e de Análise Funcional*, Editora Mir Moscou, 1982.

[Lang73] S. Lang, *Elliptic Function*, Addison–Wesley, Reading Massachusetts, 1973.

[Lang93] S. Lang, *Real and Functional Analysis*, Springer Verlag, 1993.

[Moise] E. Moise, *Elementary Geometry from an Advanced Standpoint*, Addison–Wesley, 1963.

[Niven] I. NIVEN, *Irrational Numbers*, The Carus Mathematical Monographs N^o 11, The Mathematical Association of America, 1967.

[Ritt] J. RITT, *Integration in Finite Terms: Liouville's Theory of Elementary Methods*, Columbia University Press, 1948.

[Rosen] M. ROSEN, *Abel's Theorem on the Lemniscate*, The American Mathematical Monthly, Vol. 88, pag 387-395, 1981.

[Siegel] C. L. SIEGEL, *Topics in Complex Function Theory,* Vol. 1, Wiley-Interscience, New York, 1969.

[Spivak] M. SPIVAK, *Cálculo Infinitesimal*, Editorial Reverté, S.A., 1981.

[Stillwell] J. STILLWELL, *Mathematics and Its History*, Springer, New York, 1989.

[Young] R. M. YOUNG, *Excursions in Calculus - An Interplay of the Continuous and the Discrete*, The Mathematical Association of America, 1992.