

Extensões abelianas de corpos quadráticos imaginários

Tiago J. Fonseca

Notas digitadas por Henrique de Cristo da Fonseca

Julho de 2026

Notas de aula do minicurso ministrado na 28ª Escola de Álgebra, realizada no ICMC/USP, São Carlos, 2026. Este trabalho foi realizado com apoio da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), Brasil. Processo nº 2020/15804-1.

Resumo

O teorema de Kronecker–Weber afirma que todo número algébrico de grupo de Galois abeliano pode ser escrito em termos de raízes da unidade. Por exemplo:

$$\sqrt{5} = e^{2\pi i/5} - e^{4\pi i/5} - e^{6\pi i/5} + e^{8\pi i/5}.$$

Mais precisamente, toda extensão abeliana do corpo dos racionais está contida em uma extensão ciclotômica. É natural se perguntar se há resultados parecidos para outros corpos de números; este é o décimo-segundo problema de Hilbert.

O objetivo deste minicurso é apresentar alguns aspectos da teoria clássica de extensões abelianas de corpos quadráticos imaginários (isto é, corpos da forma $\mathbb{Q}(\sqrt{-d})$, onde d é um inteiro positivo). Neste caso, no lugar da função exponencial, as extensões abelianas são descritas por valores especiais de funções modulares e elípticas. Ou, geometricamente, no lugar dos pontos de ordem finita no círculo unitário, consideramos pontos de ordem finita em uma curva elíptica. Este resultado deriva da chamada teoria da multiplicação complexa, considerada por Hilbert a “parte mais bela de toda a matemática”. A teoria acima serviu de base para o desenvolvimento da bem-estabelecida teoria de corpos de classes, e continua servindo de motivação para uma série de desenvolvimentos recentes em teoria dos números.

Conteúdo

1	Introdução	3
2	Ciclotomia	4
3	Reticulados no plano	7
4	Multiplicação complexa	10
5	Funções de reticulados	11
6	Funções modulares e coeficientes de Fourier	14
7	Algebricidade dos valores singulares	17
8	Funções elípticas	20

1 Introdução

Este minicurso é uma introdução sucinta à *teoria da multiplicação complexa*. Esta teoria de nome peculiar tem raízes na escola alemã de algebristas do final do século XIX e chegou a ser qualificada por Hilbert como “não apenas a parte mais bonita da matemática, mas de toda a ciência”.

Exagero, ou não, vale ressaltar que a teoria da multiplicação complexa vai muito além de uma curiosidade histórica e continua dando frutos até hoje. Eis uma pequena lista de desenvolvimentos relacionados a esta teoria:

- *Teoria dos corpos de classes explícita para corpos quadráticos imaginários*. Também conhecido como *Kronecker Jugendtraum*¹, este foi um dos pontos de partida da teoria de multiplicação complexa e também será o ponto de partida deste minicurso. Inspirou diretamente a formulação do 12º problema de Hilbert, ainda sem solução.
- *O problema do número de classes de Gauss*. Trata-se do seguinte problema deixado em aberto por Gauss em seu *Disquisitiones Arithmeticae*: classifique todos os discriminantes negativos D para os quais o número de classes $h(D) = 1$.² Resolvido por Heegner e Stark (1952 e 1969) através da teoria de multiplicação complexa e independentemente por Baker (1966) via formas lineares em logaritmos.
- *Fórmulas de Ramanujan–Chudnovsky*. Exemplo:

$$\frac{1}{\pi} = 12 \sum_{k=0}^{\infty} \frac{(-1)^k (6k)! (545140134k + 13591409)}{(3k)! (k!)^3 (640320)^{3k+3/2}}.$$

Estas são as fórmulas usadas atualmente para bater os recordes de casas decimais de π e estão relacionadas aos discriminantes negativos com número de classes 1. A fórmula acima (Chudnovsky, 1988) corresponde a $D = -163$.

- *Gross–Zagier e a conjectura BSD*. Em um trabalho espetacular publicado em 1986, Gross e Zagier usam a teoria de multiplicação complexa para descrever fórmulas explícitas para valores especiais de funções L de certas curvas elípticas. Com isso, demonstram um caso importante da conjectura de Birch e Swinnerton-Dyer, um dos problemas do milênio.
- *Primalidade*. O algoritmo ECPP (Elliptic Curve Primality Proving) de Atkin e Morain (1993) é atualmente um dos melhores algoritmos para testar a primalidade de números muito grandes. Sua formulação explora a teoria da multiplicação complexa para construir curvas elípticas específicas.

¹O sonho de juventude de Kronecker.

²Aqui, $h(D)$ denota o número de classes de equivalência de formas quadráticas primitivas positivas definidas $ax^2 + bxy + cy^2$, com a, b, c inteiros e discriminante $b^2 - 4ac = D$. A relação de equivalência é dada por mudança de variáveis unimodular.

- *Bialgebricidade, subvariedades especiais.* Recentemente, a parte da geometria aritmética relacionada ao estudo de subvariedades especiais de variedades de Shimura, interseções improváveis, e o fenômeno de estruturas bialgêbricas, ganhou proeminência devido a avanços importantes em problemas como a conjectura de André–Oort. Toda esta teoria pode ser interpretada como um formidável desenvolvimento geométrico da teoria da multiplicação complexa.

Neste minicurso, veremos simplesmente alguns elementos na direção do primeiro tópico listado acima. Uma exposição mais adequada a este tema envolveria uma incursão na *teoria algébrica dos números*, incluindo a *teoria dos corpos de classes*, e no estudo de *curvas elípticas* e *formas modulares*. É nossa intenção que estas aulas sirvam pelo menos de motivação para que o leitor se aprofunde nestes tópicos centrais na matemática contemporânea.

2 Ciclotomia

Seja $n \geq 1$ um inteiro e denote

$$\zeta_n = e^{2\pi i/n} = \cos(2\pi/n) + i \operatorname{sen}(2\pi/n) \in \mathbb{C}.$$

O número ζ_n é um exemplo de uma *raiz n -ésima da unidade*, isto é, uma raiz complexa do polinômio $x^n - 1$. Todas as raízes n -ésimas da unidade são potências de ζ_n :

$$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}.$$

Em geral, uma potência

$$\zeta_n^a = \cos(2\pi a/n) + i \operatorname{sen}(2\pi a/n), \quad a \in \mathbb{Z},$$

depende apenas da classe de a módulo n , isto é, $\zeta_n^a = \zeta_n^b$ se, e somente se, $a \equiv b \pmod{n}$. De forma mais conceitual, se $\mu_n \subset \mathbb{C}^\times$ denota o subgrupo das n -ésimas raízes da unidade, então

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mu_n, \quad a \pmod{n} \mapsto \zeta_n^a$$

é isomorfismo de grupos (do grupo aditivo $\mathbb{Z}/n\mathbb{Z}$ no grupo multiplicativo μ_n).

Exemplo 2.1. As raízes segundas da unidade são 1 e $\zeta_2 = -1$. As raízes terceiras da unidade são 1, $\zeta_3 = (-1 + i\sqrt{3})/2$ e $\zeta_3^2 = (-1 - i\sqrt{3})/2$. As raízes quartas da unidade são 1, $\zeta_4 = i$, $\zeta_4^2 = -1$ e $\zeta_4^3 = -i$.

Observação 2.2. As n -ésimas raízes da unidade também são chamadas de *números ciclotômicos*³, pois dividem o círculo unitário $S^1 = \{z \in \mathbb{C}^\times : |z| = 1\}$ em partes iguais e determinam os vértices de um polígono regular de n lados (se $n \geq 3$).

³Em grego, “ciclo” se refere ao círculo e “tomo” a divisão.

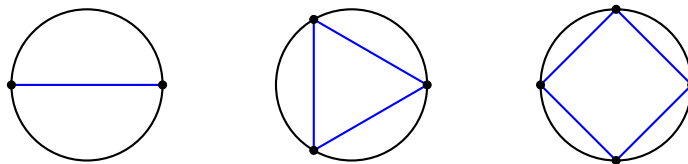
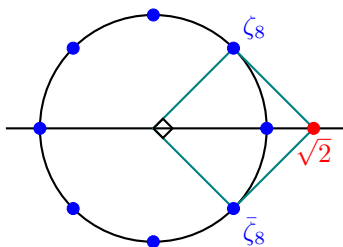


Figura 1: Os grupos μ_2 , μ_3 e μ_4 vistos no plano complexo.

Raízes da unidade são alguns dos números algébricos mais “simples” possíveis. A seguinte pergunta é natural: *quais números (algébricos) podemos escrever como combinação de raízes da unidade?* Aqui, entendemos “combinação” como uma expressão racional com coeficientes racionais.

Exemplo 2.3. Um desenho, ou uma conta simples, mostram que

$$\sqrt{2} = \zeta_8 + \bar{\zeta}_8 = \zeta_8 + \zeta_8^7.$$



Exemplo 2.4. Segue da fórmula para as terceiras raízes da unidade que

$$i\sqrt{3} = \zeta_3 - \zeta_3^2, \quad \text{logo} \quad \sqrt{3} = i\zeta_3^2 - i\zeta_3 = \zeta_{12}^{11} - \zeta_{12}^7.$$

Exercício 2.5. Mostre que toda expressão racional com coeficientes racionais em raízes da unidade é uma combinação linear com coeficientes racionais de raízes da unidade.

Para isso, use os dois fatos a seguir. Para $n, m \geq 1$, temos $\mu_n \mu_m \subset \mu_{nm}$. Além disso, $\mathbb{Q}(\zeta_N) = \mathbb{Q} + \mathbb{Q}\zeta_N + \cdots + \mathbb{Q}\zeta_N^{N-1}$ (soma de $\mathbb{Q}$ -subespaços, não necessariamente direta).

Os exemplos anteriores envolvem *números quadráticos*, ou seja, números complexos que são raízes de polinômios de grau 2 com coeficientes racionais. A proposição seguinte generaliza esses exemplos.

Proposição 2.6. *Todo número quadrático é combinação de raízes da unidade.*

Demonstração. Todo número quadrático é da forma $r + s\sqrt{d}$, com $r, s \in \mathbb{Q}$ e d um inteiro livre de quadrados; escrevendo $\pm d$ como produto de primos, $\sqrt{d}$ é um produto de raízes quadradas de primos, possivelmente multiplicado por $i = \sqrt{-1}$. Já vimos que $\sqrt{2}$ é uma combinação de raízes da unidade, e sabemos

que i é uma raiz da unidade. Pelo Exercício 2.5, basta mostrar que $\sqrt{p}$ é uma combinação de raízes da unidade, para todo número primo ímpar p .

Para isso, considere a seguinte “soma de Gauss quadrática”:

$$g_p = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p} \right) \zeta_p^a$$

onde (a/p) denota o símbolo de Legendre. Agora calculamos:

$$g_p^2 = \sum_a \sum_{a'} \left(\frac{aa'}{p} \right) \zeta_p^{a+a'} = \sum_a \sum_b \left(\frac{a^2 b}{p} \right) \zeta_p^{a+ab} = \sum_a \sum_b \left(\frac{b}{p} \right) \zeta_p^{(1+b)a},$$

onde na segunda igualdade acima fizemos a “mudança de variável” $a' = ab$, possível pois a é invertível módulo p . Agora note que, se $b \neq -1$ módulo p , então $1+b$ é invertível módulo p , e portanto,

$$\sum_a \zeta_p^{(1+b)a} = \sum_c \zeta_p^c = -1,$$

onde c varia em $\mathbb{F}_p^\times$ (a soma de todas as raízes p -ésimas da unidade é zero). Já para $b = -1$, a soma interna vale $p-1$. Voltando ao cálculo de g_p^2 , obtemos

$$g_p^2 = \left(\frac{-1}{p} \right) (p-1) - \sum_{b \neq -1} \left(\frac{b}{p} \right) = \left(\frac{-1}{p} \right) p = (-1)^{(p-1)/2} p,$$

onde a identidade $\sum_{b \neq -1} (b/p) = -(-1/p)$ vem do fato de que exatamente a metade das classes invertíveis módulo p são quadrados (logo $\sum_b (b/p) = 0$). Assim, temos $g_p = \pm \sqrt{(-1)^{(p-1)/2} p}$, com a primeira raiz em μ_4 . Como $g_p \in \mathbb{Q}(\zeta_p)$, isto mostra que $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$. $\square$

Nem todo número algébrico é combinação de raízes da unidade.

Exemplo 2.7. O número $\sqrt[3]{2}$ não é combinação de raízes da unidade. Se o fosse, o corpo $\mathbb{Q}(\sqrt[3]{2})$ estaria contido em algum $\mathbb{Q}(\zeta_n)$. Como $\mathbb{Q}(\zeta_n)$ é uma extensão galoisiana de $\mathbb{Q}$, o fecho normal de $\mathbb{Q}(\sqrt[3]{2})$ (isto é, o corpo de raízes de $x^3 - 2$), a saber $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, também estaria contido em $\mathbb{Q}(\zeta_n)$. Pela teoria de Galois, isto daria um morfismo *sobrejetor*

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \rightarrow \text{Gal}(K/\mathbb{Q}).$$

Isto é absurdo, pois $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ (via $a \bmod n \mapsto (\zeta_n \mapsto \zeta_n^a)$) é abeliano, enquanto que $\text{Gal}(K/\mathbb{Q}) \cong S_3$ não é abeliano.

O exemplo acima se generaliza imediatamente a uma condição *necessária* para um número algébrico ser combinação de raízes da unidade: é preciso que seu grupo de Galois seja abeliano. Surpreendentemente, esta condição também é suficiente.

Teorema 2.8 (Kronecker–Weber; Hilbert, 1896). *Toda extensão abeliana de $\mathbb{Q}$ está contida em algum corpo ciclotômico $\mathbb{Q}(\zeta_n)$.*

Demonstrar este teorema foge do escopo deste minicurso; mencionemos apenas que qualquer demonstração envolve ferramentas da teoria algébrica dos números relacionadas à *ramificação* de números primos. De forma mais conceitual, o teorema de Kronecker–Weber diz o seguinte:

- (i) Os pontos de torção do grupo algébrico $\mathbb{C}^\times$ (isto é, o conjunto $\mu_\infty = \bigcup_n \mu_n$ das raízes da unidade) geram todas as extensões abelianas de $\mathbb{Q}$;
- (ii) Estes pontos são “valores especiais” da função transcendente

$$e : \mathbb{C} \rightarrow \mathbb{C}^\times, \quad z \mapsto e(z) = e^{2\pi iz},$$

neste caso, os valores nos pontos racionais: $\mu_\infty = e(\mathbb{Q})$.

Pergunta: existe algo análogo para outros corpos K no lugar de $\mathbb{Q}$? Este é o décimo-segundo problema de Hilbert. O único caso (além de $\mathbb{Q}$) em que temos uma resposta positiva completa e clássica a esta pergunta é aquele em que K é um *corpo quadrático imaginário*, isto é, uma extensão de grau 2 de $\mathbb{Q}$ que não está contida em $\mathbb{R}$ (ou seja, um corpo da forma $K = \mathbb{Q}(\sqrt{-d})$, onde d é um inteiro positivo). Nas próximas seções, veremos que estes corpos aparecem naturalmente na teoria de reticulados.

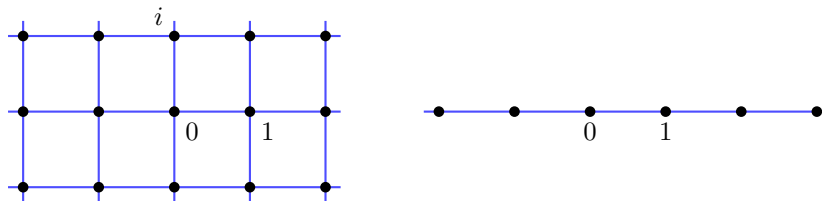
3 Reticulados no plano

Definição 3.1. Um *reticulado* em $\mathbb{C}$ é um subgrupo $\Lambda \subset \mathbb{C}$ da forma

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2,$$

onde $\omega_1, \omega_2 \in \mathbb{C}$ são $\mathbb{R}$ -linearmente independentes.

Exemplo 3.2. O conjunto $\mathbb{Z} + \mathbb{Z}i$ dos números complexos com parte real e imaginária inteiras é um reticulado em $\mathbb{C}$. O subgrupo $\mathbb{Z} \subset \mathbb{C}$ não é um reticulado pois não contém dois números complexos $\mathbb{R}$ -linearmente independentes.



Observação 3.3. A escolha específica da base ω_1, ω_2 acima não faz parte da definição do reticulado Λ . Por exemplo, $\mathbb{Z}i + \mathbb{Z}(1 - i)$ é o mesmo reticulado $\mathbb{Z} + \mathbb{Z}i$ considerado no parágrafo anterior. Em geral, duas bases (ω_1, ω_2) e

(ω'_1, ω'_2) definem o mesmo reticulado (isto é, $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z}\omega'_1 + \mathbb{Z}\omega'_2$) se, e somente se, existem inteiros a, b, c, d tais que $ad - bc = \pm 1$ e

$$\omega'_1 = a\omega_1 + b\omega_2, \quad \omega'_2 = c\omega_1 + d\omega_2.$$

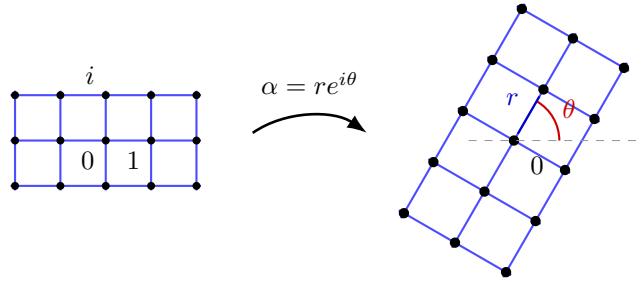
Em outras palavras, existe uma matriz em $\text{GL}_2(\mathbb{Z})$ que leva uma base na outra.

Exercício 3.4. Mostre que um reticulado em $\mathbb{C}$ é o mesmo que um subgrupo discreto $\Lambda \subset \mathbb{C}$ cujo quociente $\mathbb{C}/\Lambda$ é compacto. Essa definição topológica é mais elegante, mas a definição elementar dada acima é a que usamos na prática.

Definição 3.5. Sejam $\Lambda, \Lambda' \subset \mathbb{C}$ reticulados e $\alpha \in \mathbb{C}$ tal que $\alpha\Lambda \subset \Lambda'$. O morfismo de grupos

$$\Lambda \rightarrow \Lambda', \quad \omega \mapsto \alpha\omega,$$

é chamado de *homotetia* definida por α . O caso $\alpha = 0$ é um caso degenerado que chamaremos de *homotetia nula*. Se Λ e Λ' são reticulados para os quais existe uma homotetia não nula $\Lambda \rightarrow \Lambda'$ com $\alpha\Lambda = \Lambda'$ (isto é, a homotetia definida por α é um isomorfismo de grupos), diremos que Λ e Λ' são *homotéticos*.



Note que todos os reticulados em $\mathbb{C}$ são isomorfos entre si como grupos abstratos, pois são todos isomorfos a $\mathbb{Z}^2$. A relação de homotetia é mais forte.

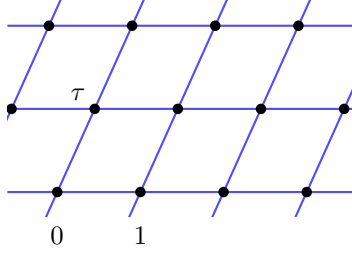
Exemplo 3.6. Se $\rho = \zeta_3$, então os reticulados $\mathbb{Z} + \mathbb{Z}i$ e $\mathbb{Z} + \mathbb{Z}\rho$ não são homotéticos. Mostremos que não existe uma homotetia não nula $\mathbb{Z} + \mathbb{Z}\rho \rightarrow \mathbb{Z} + \mathbb{Z}i$. Caso contrário, teríamos $\alpha \in \mathbb{C}^\times$ e inteiros a, b, c, d tais que $\alpha = a + ib$ e $\alpha\rho = c + id$. Dividindo uma equação pela outra, teríamos $\rho = (c + id)/(a + ib) \in \mathbb{Q}(i) = \mathbb{Q} + \mathbb{Q}i$. Isto é absurdo, pois $\text{Im}(\rho) = \sqrt{3}/2$ é irracional.

A homotetia define uma relação de equivalência entre reticulados. Daqui em diante, estudaremos os reticulados módulo homotetia.

Lema 3.7. Seja $\mathbb{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ o semiplano superior.

- (i) Todo reticulado é homotético a um reticulado da forma $\mathbb{Z} + \mathbb{Z}\tau$, com $\tau \in \mathbb{H}$.
- (ii) Sejam $\tau, \tau' \in \mathbb{H}$. Os reticulados $\mathbb{Z} + \mathbb{Z}\tau$ e $\mathbb{Z} + \mathbb{Z}\tau'$ são homotéticos se, e somente se, existe $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ tal que

$$\tau' = \gamma \cdot \tau := \frac{a\tau + b}{c\tau + d}.$$



Demonstração. (i) Fatore $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \omega_1(\mathbb{Z} + \mathbb{Z}(\omega_2/\omega_1))$. Como ω_1, ω_2 são $\mathbb{R}$ -linearmente independentes, $\omega_2/\omega_1 \notin \mathbb{R}$. Caso $\text{Im}(\omega_2/\omega_1) > 0$, tomamos $\tau := \omega_2/\omega_1$. Caso contrário, basta intercambiar ω_1 e ω_2 .

(ii) Suponha que exista $\alpha \in \mathbb{C}^\times$ tal que $\mathbb{Z} + \mathbb{Z}\tau = \alpha(\mathbb{Z} + \mathbb{Z}\tau')$. Então $(\alpha\tau', \alpha)$ e $(\tau, 1)$ são duas bases do mesmo reticulado e, pela Observação 3.3, existe $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ tal que $\alpha\tau' = a\tau + b$ e $\alpha = c\tau + d$. Dividindo uma equação pela outra, temos $\tau' = \gamma \cdot \tau$. Sabemos que $\det \gamma = \pm 1$, então basta mostrar que o determinante é positivo. Isso segue da seguinte fórmula geral, válida para toda matriz real γ com $c\tau + d \neq 0$ (verifique!):

$$\text{Im}(\gamma \cdot \tau) = \frac{\det(\gamma) \text{Im}(\tau)}{|c\tau + d|^2}.$$

Como $\text{Im}(\tau)$ e $\text{Im}(\tau')$ são positivos, $\det \gamma = 1$.

Reciprocamente, se $\tau' = \gamma \cdot \tau$ com $\gamma \in \text{SL}_2(\mathbb{Z})$, então

$$\mathbb{Z} + \mathbb{Z}\tau' = \frac{1}{c\tau + d}(\mathbb{Z}(c\tau + d) + \mathbb{Z}(a\tau + b)) = \frac{1}{c\tau + d}(\mathbb{Z} + \mathbb{Z}\tau),$$

pois $(c\tau + d, a\tau + b)$ e $(1, \tau)$ são bases do mesmo reticulado (Observação 3.3). (Ver também o Lema 6.1 adiante.) $\square$

Recapitulemos o que vimos de maneira conceitual. Denotamos por $B = \{(\omega_1, \omega_2) \in \mathbb{C}^2 : \text{Im}(\omega_2/\omega_1) > 0\}$ o conjunto das “bases orientadas” de reticulados. A aplicação $\tau \mapsto \mathbb{Z} + \mathbb{Z}\tau$ induz uma bijeção entre $\text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ ⁴ e o conjunto de reticulados módulo homotetia, conforme o diagrama a seguir:

$$\begin{array}{ccc}
 B & \xrightarrow{(\omega_1, \omega_2) \mapsto \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2} & \{\text{reticulados em } \mathbb{C}\} \\
 \downarrow (\omega_1, \omega_2) \mapsto \omega_2/\omega_1 & & \downarrow \\
 \mathbb{H} & \xrightarrow{\tau \mapsto \mathbb{Z} + \mathbb{Z}\tau} & \{\text{reticulados em } \mathbb{C}\} / \text{homotetia} \\
 \downarrow & \nearrow \text{bijeção} & \\
 \text{SL}_2(\mathbb{Z}) \backslash \mathbb{H} & \xrightarrow{\sim} &
 \end{array}$$

A aplicação $\mathbb{H} \rightarrow B$, $\tau \mapsto (1, \tau)$, é uma seção da flecha vertical à esquerda.

⁴Essa é a notação para o espaço de órbitas de uma ação à esquerda. Se a ação fosse à direita, escreveríamos $\mathbb{H} / \text{SL}_2(\mathbb{Z})$.

4 Multiplicação complexa

Nos interessamos agora pelas homotetias de um reticulado em si mesmo.

Definição 4.1. Dado um reticulado $\Lambda \subset \mathbb{C}$, denotamos por R_Λ o *anel das homotetias* de Λ em si mesmo. Note que $R_\Lambda \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$; em particular, R_Λ pode ser visto como um subanel de $\mathbb{C}$. Denotamos por $K_\Lambda \subset \mathbb{C}$ o corpo de frações de R_Λ .

O seguinte exercício mostra que o anel das homotetias de um reticulado em si mesmo depende apenas de sua classe de homotetia.

Exercício 4.2. Mostre que, se Λ é homotético a Λ' , então $R_\Lambda = R_{\Lambda'}$ (como subanéis de $\mathbb{C}$).

Todo inteiro define uma homotetia de um reticulado Λ em si mesmo (pois Λ é um grupo abeliano), isto é, $\mathbb{Z} \subset R_\Lambda$. Isto também segue imediatamente do fato que R_Λ é um subanel de $\mathbb{C}$.

Definição 4.3. Dizemos que Λ tem *multiplicação complexa* se $R_\Lambda \neq \mathbb{Z}$ (equivalentemente, $K_\Lambda \neq \mathbb{Q}$).

A terminologia é autoevidente: um reticulado tem multiplicação complexa se existe um número complexo α não inteiro tal que a multiplicação $z \mapsto \alpha z$ preserva este reticulado. (É um exercício mostrar que, necessariamente, tal α não é real.) Por exemplo, $\mathbb{Z} + \mathbb{Z}i$ tem multiplicação complexa pois $i \in R_{\mathbb{Z} + \mathbb{Z}i} \setminus \mathbb{Z}$. Mais geralmente:

Exemplo 4.4. Seja τ um *número quadrático imaginário*, isto é, tal que $\mathbb{Q}(\tau)$ é um corpo quadrático imaginário. Considere o reticulado $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. Se A, B, C são inteiros, com $A \neq 0$, tais que $A\tau^2 + B\tau + C = 0$, então $A\tau \in R_\Lambda \setminus \mathbb{Z}$; de fato, $A\tau \cdot 1 = A\tau \in \Lambda$ e $A\tau \cdot \tau = -C - B\tau \in \Lambda$. Logo, Λ tem multiplicação complexa.

O próximo teorema mostra que, a menos de homotetia, o exemplo acima é o caso geral! Para enunciá-lo, precisamos de uma definição: uma *ordem* em um corpo de números K é um subanel $R \subset K$ finito sobre $\mathbb{Z}$ (isto é, finitamente gerado como $\mathbb{Z}$ -módulo) tal que $\mathbb{Q}R = K$ (isto é, R contém uma $\mathbb{Q}$ -base de K).

Teorema 4.5. *Seja $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ um reticulado. Se Λ tem multiplicação complexa, então:*

- (i) *O quociente $\tau := \omega_2/\omega_1$ é um número quadrático imaginário.*
- (ii) *O anel R_Λ é uma ordem no corpo quadrático imaginário $\mathbb{Q}(\tau)$.*

Demonstração. Seja $\alpha \in R_\Lambda \setminus \mathbb{Z}$. Então, existem inteiros a, b, c, d tais que

$$\alpha\omega_1 = a\omega_1 + b\omega_2, \quad \alpha\omega_2 = c\omega_1 + d\omega_2.$$

Seja $\tau = \omega_2/\omega_1$. Dividindo a segunda equação pela primeira, obtemos

$$\tau = \frac{\omega_2}{\omega_1} = \frac{c\omega_1 + d\omega_2}{a\omega_1 + b\omega_2} = \frac{c + d\tau}{a + b\tau}.$$

A equação acima é equivalente a

$$b\tau^2 + (a - d)\tau - c = 0.$$

Note que $b \neq 0$, pois caso contrário teríamos $\alpha\omega_1 = a\omega_1$, isto é, $\alpha = a \in \mathbb{Z}$. Logo τ é raiz de um polinômio de grau 2 com coeficientes inteiros; como $\tau \notin \mathbb{R}$ (pela hipótese de $\mathbb{R}$ -independência de ω_1, ω_2), este polinômio é irredutível sobre $\mathbb{Q}$ e $\mathbb{Q}(\tau)$ é um corpo quadrático imaginário. Isto mostra (i).

Segue da equação $\alpha\omega_1 = a\omega_1 + b\omega_2$ que $\alpha = a + b\tau$. Como $\alpha \in R_\Lambda$ era arbitrário (para $\alpha \in \mathbb{Z}$, a afirmação é trivial), isto mostra que $R_\Lambda \subset \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{Q}(\tau)$. Como $\mathbb{Z} + \mathbb{Z}\tau$ é um $\mathbb{Z}$ -módulo finitamente gerado e $\mathbb{Z}$ é noetheriano (pois é um DIP), segue que o submódulo R_Λ é finitamente gerado sobre $\mathbb{Z}$. Finalmente, como $\tau = \alpha/b - a/b$ para $\alpha \in R_\Lambda \setminus \mathbb{Z}$ como acima, concluímos que $\mathbb{Q}R_\Lambda = \mathbb{Q}(\tau)$, o que conclui a afirmação (ii). $\square$

Exercício 4.6. Seja $\tau \in \mathbb{H}$. Verifique que são equivalentes:

- (i) O número τ é quadrático imaginário.
- (ii) Existe uma matriz não múltipla da identidade $M \in M_{2 \times 2}(\mathbb{Z})$ com $\det M > 0$ tal que $\tau = M \cdot \tau$.
- (iii) O reticulado $\mathbb{Z} + \mathbb{Z}\tau$ tem multiplicação complexa.

Em resumo, se $\Lambda \subset \mathbb{C}$ é um reticulado qualquer, temos apenas “duas” possibilidades:

1. $K_\Lambda = \mathbb{Q}$ (caso genérico); ou
2. K_Λ é um corpo quadrático imaginário (Λ tem multiplicação complexa).

O teorema acima fornece uma caracterização surpreendente de corpos quadráticos imaginários em termos de reticulados. É isto que vamos explorar para construir extensões abelianas.

5 Funções de reticulados

Nosso objetivo nesta seção é produzir “invariantes numéricos” para reticulados. A saber, queremos funções do tipo

$$f: \{\text{reticulados}\}/\text{homotetia} \rightarrow \mathbb{C}, \quad \Lambda \mapsto f(\Lambda)$$

tais que, se o reticulado Λ tem multiplicação complexa, então $K_\Lambda(f(\Lambda))$ é uma extensão “interessante” de K_Λ . Para isso, precisamos de uma função complexa definida no conjunto dos reticulados que seja invariante por homotetia. Note que a definição de uma função de reticulados deve ser independente de base!

Exemplo 5.1. Se $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, então $A(\Lambda) := |\operatorname{Im}(\omega_1\bar{\omega}_2)| \in \mathbb{R}$ define uma função que não depende da escolha de (ω_1, ω_2) . Geometricamente, o número $A(\Lambda)$ é a área de um “paralelogramo fundamental” desse reticulado. Porém A não é invariante por homotetia, pois $A(\alpha\Lambda) = |\alpha|^2 A(\Lambda)$.

Exemplo 5.2 (Séries de Eisenstein). Outro invariante possível seria a soma de todos os pontos do reticulado Λ , mas obviamente surgiriam problemas de convergência. Para um inteiro $k \geq 3$, definimos a *série de Eisenstein*

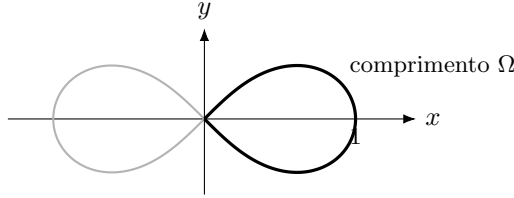
$$G_k(\Lambda) := \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^k}.$$

Deixamos como exercício verificar que essa série converge absolutamente (compare com a integral $\iint_{x^2+y^2 \geq 1} (x^2 + y^2)^{-k/2} dx dy$, que é finita para $k > 2$). Note que, para k ímpar, temos $G_k \equiv 0$ (os termos ω e $-\omega$ se cancelam). Novamente, obtivemos uma função que não é invariante por homotetia, uma vez que $G_k(\alpha\Lambda) = \alpha^{-k} G_k(\Lambda)$.

Observação 5.3. Há fórmulas explícitas para certos valores de séries de Eisenstein. Por exemplo, a teoria de funções elípticas permite calcular

$$G_4(\mathbb{Z} + \mathbb{Z}i) = \frac{\Omega^4}{15},$$

onde $\Omega := 2 \int_0^1 dt / \sqrt{1-t^4} = 2,62205\dots$ é a “constante da lemniscata”. Geometricamente, Ω é o comprimento de arco de um dos laços da lemniscata $(x^2 + y^2)^2 = x^2 - y^2$ (isto é, metade de seu comprimento total).



Definição 5.4. Uma função de reticulados f tem *peso* k se $f(\alpha\Lambda) = \alpha^{-k} f(\Lambda)$ para todo reticulado $\Lambda \subset \mathbb{C}$ e todo $\alpha \in \mathbb{C}^\times$.

Fixado k , as funções de reticulados de peso k formam um $\mathbb{C}$ -espaço vetorial. Mais ainda, as funções de reticulados formam uma $\mathbb{C}$ -álgebra graduada. De fato, se f tem peso k e g tem peso k' , então o produto fg tem peso $k + k'$.

Voltemos ao nosso objetivo de construir um invariante por homotetia. Em outras palavras, queremos uma função de peso 0. A ideia fundamental é que, se f e g têm o mesmo peso, então f/g tem peso 0. Parece bastante simples, mas surgem dificuldades.

Exemplo 5.5. A série de Eisenstein não trivial mais simples é G_4 , que tem peso 4. Note que G_4^2 e G_8 têm peso 8, de modo que $f = G_4^2/G_8$ tem peso 0. O problema é que f é constante! De fato, a teoria das formas modulares permite calcular $G_4^2/G_8 = 7/3$.

Exemplo 5.6. As séries de Eisenstein G_4^3 e G_6^2 têm peso 12 e não são proporcionais. Logo $f = G_4^3/G_6^2$ tem peso 0 e não é constante. O problema agora é

que G_6 se anula em $\mathbb{Z} + \mathbb{Z}i$, visto que

$$\sum_{(m,n) \neq (0,0)} \frac{1}{(m+ni)^6} = \frac{1}{i^6} \sum_{(m,n) \neq (0,0)} \frac{1}{(-mi+n)^6},$$

e a mudança de índices $(m, n) \mapsto (n, -m)$ mostra que a última soma é igual a $G_6(\mathbb{Z} + \mathbb{Z}i)$; isto é, $G_6(\mathbb{Z} + \mathbb{Z}i) = -G_6(\mathbb{Z} + \mathbb{Z}i)$. Isso significa que f não pode ser calculada em $\mathbb{Z} + \mathbb{Z}i$ e, portanto, não é uma função de reticulados bem definida.

Exercício 5.7. Seja $\rho = e^{2\pi i/3}$. Verifique que $G_4(\mathbb{Z} + \mathbb{Z}\rho) = 0$.

Proposição 5.8. *Sejam $g_2 := 60G_4$, $g_3 := 140G_6$ e $\Delta := g_2^3 - 27g_3^2$. Então $\Delta(\Lambda) \neq 0$ para todo reticulado $\Lambda \subset \mathbb{C}$.*

A demonstração mais natural desse fato se dá na linguagem de funções elípticas. Por isso deixamos para vê-la mais tarde (Corolário 8.7).

Definição 5.9. O *invariante modular* (ou *j-invariante* de Klein) é a função de reticulados de peso 0 definida por

$$j := 1728 \frac{g_2^3}{\Delta}.$$

O teorema a seguir é por vezes chamado de “Teorema Principal da Multiplicação Complexa”. É difícil atribuir autoria a esse resultado, então mencionamos os nomes mais relevantes.

Teorema 5.10 (Weber, Fueter, Hasse). *Seja $\Lambda \subset \mathbb{C}$ um reticulado com multiplicação complexa. Escrevemos $R = R_\Lambda$, $K = K_\Lambda$ e $j = j(\Lambda)$. Então*

- (i) *O número j é um inteiro algébrico.*
- (ii) *A extensão $K(j)$ é o corpo de classes de anel⁵ da ordem R .*

Como prometido, não supomos que o leitor conheça muita Teoria Algébrica dos Números – muito menos Teoria dos Corpos de Classes. Por isso, em vez de definirmos os termos acima detalhadamente, apenas comentamos brevemente o que o resultado significa. Seja $\mathcal{O}_K$ o anel de inteiros de K . Toda ordem de K é da forma $R = \mathbb{Z} + f\mathcal{O}_K$, onde o inteiro $f = [\mathcal{O}_K : R]$ é o *condutor* de R . A afirmação (ii) implica, em particular, que $K(j)$ é uma extensão abeliana de K com grupo de Galois isomorfo ao grupo de classes $\text{Pic}(R) = \text{Cl}(R)$, e que a extensão $K(j)/K$ é “não ramificada” em todos os primos de K que não dividem f . Quando $R = \mathcal{O}_K$, a extensão $K(j)$ é o *corpo de classes de Hilbert* de K : a maior extensão abeliana não ramificada de K .

Exemplo 5.11. Vamos calcular o invariante modular de $\Lambda = \mathbb{Z} + \mathbb{Z}i$. Note que Λ tem multiplicação complexa por $\alpha = i$, logo $R = \mathbb{Z}[i]$ e $K = \mathbb{Q}(i)$ na notação do teorema. Usando a definição de j e o fato de que $g_3(\Lambda) = 0$, segue que $j(\Lambda) = 1728$. Nesse caso, a extensão $K(j(\Lambda)) = K$ tem grau 1. Isso concorda com o fato de que o grupo de classes de $\mathbb{Z}[i]$ é trivial (trata-se de um DIP).

⁵Na literatura, encontrado pelo nome *ring class field*.

Exemplo 5.12. Vejamos um cálculo menos trivial. Sejam $\tau = (1 + i\sqrt{15})/2$ e $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. Então $R = \mathbb{Z}[\tau] = \mathcal{O}_K$, com $K = \mathbb{Q}(\sqrt{-15})$ (verifique). Calculando $j(\tau)$ numericamente com alta precisão (por exemplo, usando a expansão de Fourier da Seção 6) e usando o algoritmo LLL (“lattice basis reduction”) para encontrar uma relação algébrica de grau 2, obtemos

$$j(\Lambda) = \frac{-191025 - 85995\sqrt{5}}{2} = -191657,83\dots$$

Neste caso, $\text{Cl}(\mathcal{O}_K)$ tem ordem 2, de acordo com o fato de que $K(j(\Lambda)) = \mathbb{Q}(\sqrt{-15}, \sqrt{5})$ tem grau 2 sobre K .

Nosso próximo objetivo será demonstrar um resultado parcial na direção do Teorema 5.10: o fato que o invariante $j(\Lambda)$ de um reticulado com multiplicação complexa é sempre um número algébrico. Um tal número é chamado na literatura clássica de *valor singular* da função j .

6 Funções modulares e coeficientes de Fourier

Começamos com a seguinte observação: toda função de reticulados f pode ser vista como uma função definida no semiplano superior $\mathbb{H}$. Explicitamente:

$$f : \mathbb{H} \rightarrow \mathbb{C}, \quad \tau \mapsto f(\mathbb{Z} + \mathbb{Z}\tau).$$

Por abuso, usamos a mesma notação para a função de reticulados e para a função correspondente definida em $\mathbb{H}$.

Lema 6.1. Se $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ e $\tau \in \mathbb{H}$, então

$$\mathbb{Z} + \mathbb{Z}\gamma\tau = \frac{1}{c\tau + d}(\mathbb{Z} + \mathbb{Z}\tau).$$

Demonstração. Fatorando $(c\tau + d)^{-1}$ em $\mathbb{Z} + \mathbb{Z}\gamma\tau$, obtemos

$$\mathbb{Z} + \mathbb{Z}\gamma\tau = \mathbb{Z} + \mathbb{Z}\frac{a\tau + b}{c\tau + d} = \frac{1}{c\tau + d}(\mathbb{Z}(c\tau + d) + \mathbb{Z}(a\tau + b)).$$

Agora basta observar que $(1, \tau)$ e $(c\tau + d, a\tau + b)$ são bases do mesmo reticulado. $\square$

Se uma função de reticulados f tem peso k , então, pelo lema anterior, a função correspondente em $\mathbb{H}$ satisfaz a seguinte lei de transformação pela ação de uma matriz $\gamma \in \text{SL}_2(\mathbb{Z})$:

$$\begin{aligned} f(\gamma\tau) &= f(\mathbb{Z} + \mathbb{Z}\gamma\tau) = f\left(\frac{1}{c\tau + d}(\mathbb{Z} + \mathbb{Z}\tau)\right) \\ &= (c\tau + d)^k f(\mathbb{Z} + \mathbb{Z}\tau) = (c\tau + d)^k f(\tau). \end{aligned}$$

Uma função definida em $\mathbb{H}$ que satisfaz tal equação funcional é dita *modular* de peso k . Há portanto uma correspondência entre funções de reticulados de peso k e funções modulares de peso k . Em particular, tomando $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, toda função modular satisfaz $f(\tau + 1) = f(\tau)$.

Observação 6.2. O termo “modular” vem de “módulo”, que neste contexto significa “parâmetro”, pois pontos em $\mathbb{H}$ parametrizam reticulados em $\mathbb{C}$.

Proposição 6.3. *Para todo inteiro par $k \geq 4$, a função modular*

$$G_k : \mathbb{H} \rightarrow \mathbb{C}, \quad \tau \mapsto \sum_{(m,n) \neq (0,0)} \frac{1}{(m + n\tau)^k}$$

é holomorfa e admite a seguinte expansão de Fourier:

$$G_k(\tau) = 2\zeta(k) \left(1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) e^{2\pi i n \tau} \right),$$

onde $\zeta(k) = \sum_{n=1}^{\infty} 1/n^k$ é a zeta de Riemann, B_k é o k -ésimo número de Bernoulli e $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

Lembremos que os números de Bernoulli são números racionais definidos pela função geradora $x/(e^x - 1) = \sum_{k=0}^{\infty} (B_k/k!)x^k$ e que a fórmula de Euler calcula explicitamente os valores da função zeta nos inteiros positivos *pares*:

$$2\zeta(k) = -\frac{B_k}{k!} (2\pi i)^k = (-1)^{k/2+1} \frac{B_k}{k!} (2\pi)^k, \quad k \text{ par.}$$

Por exemplo, $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$ e $\zeta(6) = \pi^6/945$.

Exercício 6.4. Demonstre a proposição acima. A holomorfia segue do fato que a série converge uniformemente em compactos. A expansão de Fourier é uma consequência da seguinte fórmula (também devida a Euler) para a função cotangente complexa: $\pi \cotan(\pi z) = \lim_{N \rightarrow \infty} \sum_{|n| \leq N} 1/(z + n)$.

Denotando $q := e^{2\pi i \tau}$, cada G_k admite uma expansão da forma

$$G_k(\tau) = (2\pi)^k \left(\sum_{n=0}^{\infty} a_n q^n \right), \quad a_n \in \mathbb{Q}.$$

A racionalidade desses coeficientes será um ponto crucial na demonstração do teorema de algebricidade dos valores singulares.

Exemplo 6.5. Explicitamente, usando as fórmulas acima (note que $-2k/B_k = 240$ para $k = 4$ e -504 para $k = 6$), obtemos:

$$g_2(\tau) = \frac{(2\pi)^4}{12} \left(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \right),$$

$$g_3(\tau) = \frac{(2\pi)^6}{216} \left(1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n \right).$$

Em particular, uma conta simples mostra que a função Δ admite uma expansão de Fourier da forma

$$\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2 = (2\pi)^{12} \left(q + \sum_{n=2}^{\infty} b_n q^n \right), \quad b_n \in \mathbb{Q}$$

(o coeficiente de q é $(720 + 1008)/1728 = 1$), e a função j admite uma expansão de Fourier da forma

$$j(\tau) = 1728 \frac{g_2(\tau)^3}{\Delta(\tau)} = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n, \quad c_n \in \mathbb{Q}.$$

Exercício 6.6. Mostre que os coeficientes b_n e c_n das expansões acima são inteiros. Para isso, considere $U = \sum_{n \geq 1} \sigma_3(n) q^n$ e $V = \sum_{n \geq 1} \sigma_5(n) q^n$, de modo que

$$\frac{\Delta}{(2\pi)^{12}} = \frac{(1 + 240U)^3 - (1 - 504V)^2}{1728},$$

e reduza o problema a mostrar que $(1 + 240U)^3 \equiv (1 - 504V)^2 \pmod{1728}$ (coeficiente a coeficiente). Usando que $1728 = 2^6 \cdot 3^3$ divide $3 \cdot 240^2$, 240^3 e 504^2 , verifique que essa congruência equivale a $U \equiv V \pmod{12}$. Esse último fato segue da relação $d^3 \equiv d^5 \pmod{12}$, que vale para todo inteiro d . Para os c_n , use que $\Delta/(2\pi)^{12} = q(1 + \sum_{n \geq 1} b_{n+1} q^n)$ e que o inverso de uma série $1 + O(q)$ com coeficientes inteiros também tem coeficientes inteiros.

Note que a função j é modular de peso 0, ou seja, é $\mathrm{SL}_2(\mathbb{Z})$ -invariante:

$$j(\gamma\tau) = j(\tau), \quad \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

Na verdade, essa é “essencialmente” a única função com essa propriedade, conforme diz a proposição seguinte.

Proposição 6.7. *Seja $f: \mathbb{H} \rightarrow \mathbb{C}$ uma função holomorfa. Se f é modular de peso 0 e tem expansão de Fourier da forma $f(\tau) = \sum_{n \geq -N} a_n q^n$ para algum inteiro $N \geq 0$, então f é um polinômio em j com coeficientes em $\mathbb{C}$, isto é, $f \in \mathbb{C}[j]$.*

Demonstração. O ponto fundamental é que o j -invariante induz uma bijeção $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H} \xrightarrow{\sim} \mathbb{C}$. A sobrejetividade pode ser obtida demonstrando-se que a imagem $j(\mathbb{H})$ é aberta e fechada em $\mathbb{C}$. A “injetividade” $j(\tau) = j(\tau') \iff \tau' \in \mathrm{SL}_2(\mathbb{Z}) \cdot \tau$ segue da teoria de funções elípticas (mais especificamente, do fato de que g_2 e g_3 determinam unicamente um reticulado). Como f é $\mathrm{SL}_2(\mathbb{Z})$ -

invariante, obtemos então o seguinte diagrama comutativo

$$\begin{array}{ccc}
 \mathbb{H} & \xrightarrow{f} & \mathbb{C} \\
 \downarrow & \nearrow & \uparrow \\
 \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H} & & \\
 \downarrow j & \nearrow F & \\
 \mathbb{C} & &
 \end{array}$$

isto é, existe uma única função $F: \mathbb{C} \rightarrow \mathbb{C}$ tal que $f = F \circ j$. Afirmamos que F é holomorfa. Primeiro, F é contínua: se $U \subset \mathbb{C}$ é aberto, então $F^{-1}(U) = j(f^{-1}(U))$ é aberto, pois j é holomorfa não constante e portanto uma aplicação aberta. Segundo, perto de todo ponto $j(\tau_1)$ com $j'(\tau_1) \neq 0$, a função j admite uma inversa local holomorfa e $F = f \circ j^{-1}$ é holomorfa. Como os zeros de j' formam um subconjunto discreto e $\mathrm{SL}_2(\mathbb{Z})$ -invariante de $\mathbb{H}$, e como $j' = -2\pi i q^{-1} + O(1)$ não se anula para $\mathrm{Im} \tau \gg 0$, esses zeros formam um número finito de órbitas (de fato, apenas as órbitas de i e de ρ). Assim, F é contínua em $\mathbb{C}$ e holomorfa fora de um conjunto finito, logo holomorfa em $\mathbb{C}$ (teorema da singularidade removível de Riemann).

Daí, procedemos por indução em N . Suponha que $N = 0$. Então $f(\tau) = \sum_{n \geq 0} a_n q^n \rightarrow a_0$ quando $\mathrm{Im}(\tau) \rightarrow \infty$, pois $|q| = e^{-2\pi \mathrm{Im}(\tau)}$; logo f é limitada em uma região $\{\mathrm{Im}(\tau) \geq T\}$. Seja $\mathcal{F} = \{\tau \in \mathbb{H} : |\mathrm{Re} \tau| \leq 1/2, |\tau| \geq 1\}$ o domínio fundamental usual de $\mathrm{SL}_2(\mathbb{Z})$ (todo ponto de $\mathbb{H}$ é equivalente a um ponto de $\mathcal{F}$; ver [4, Cap. VII]). Como $\mathcal{F} \cap \{\mathrm{Im} \tau \leq T\}$ é compacto, f é limitada em $\mathcal{F}$ e, por invariância, em todo $\mathbb{H}$. Logo F é uma função inteira limitada e, pelo Teorema de Liouville, F é constante. Portanto $f = F \circ j$ é constante.

Para o passo indutivo, suponha $N \geq 1$ e considere $g = f - a_{-N} j^N$. Como $j^N = q^{-N} + O(q^{-N+1})$, a função g é holomorfa, modular de peso 0 e tem expansão de Fourier da forma $\sum_{n \geq -(N-1)} a'_n q^n$. Por hipótese de indução, $g \in \mathbb{C}[j]$, donde $f = g + a_{-N} j^N \in \mathbb{C}[j]$. $\square$

7 Algebricidade dos valores singulares

Teorema 7.1. *Se $\tau_0 \in \mathbb{H}$ é quadrático imaginário, então $j(\tau_0)$ é algébrico.*

Demonstração. Passo 1: escolha de M . Sejam A, B, C inteiros, com $A > 0$, tais que $A\tau_0^2 + B\tau_0 + C = 0$, e seja $|D| = 4AC - B^2 > 0$ (pois $\tau_0 \notin \mathbb{R}$). Para cada $n \in \mathbb{Z}$, considere

$$M_n = \begin{pmatrix} n - B & -C \\ A & n \end{pmatrix} \in \mathrm{M}_{2 \times 2}(\mathbb{Z}).$$

Um cálculo direto mostra que $M_n \cdot \tau_0 = \tau_0$ (compare com o Exemplo 4.4 e o Exercício 4.6) e que $4 \det M_n = (2n - B)^2 + |D| > 0$. Escolha n tal que $\mathrm{mdc}(A, n) = 1$ e $|2n - B| \geq 2$ (por exemplo, $n = 1 + kA$ com k grande). Fixamos então $M = M_n$, que satisfaz

- (a) $M \cdot \tau_0 = \tau_0$;
- (b) $m := \det M > 1$;
- (c) M não é múltiplo escalar de um elemento de $\mathrm{SL}_2(\mathbb{Z})$.

De fato, $4m = (2n - B)^2 + |D| > 4$. Para (c), suponha $M = \lambda\gamma$ com $\lambda \in \mathbb{R}$ e $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Como $\det \gamma = 1$, as entradas de γ são primas entre si, logo existe uma combinação inteira delas igual a 1; a mesma combinação das entradas de M dá λ , donde $\lambda \in \mathbb{Z}$ e λ divide todas as entradas de M . Como $\mathrm{mdc}(A, n) = 1$, temos $\lambda = \pm 1$ e $m = \lambda^2 = 1$, absurdo.

(Note que, se $M = \lambda\gamma$, então $j_M = j$ e o argumento abaixo não diria nada; esta é a única razão da condição (c).) Como $\det M > 0$, a matriz M preserva $\mathbb{H}$, e podemos considerar a função holomorfa

$$j_M: \mathbb{H} \rightarrow \mathbb{C}, \quad \tau \mapsto j(M \cdot \tau),$$

e o subgrupo $\Gamma := M^{-1} \mathrm{SL}_2(\mathbb{Z}) M \cap \mathrm{SL}_2(\mathbb{Z})$.

Passo 2: j_M é Γ -invariante e Γ tem índice finito. Para $\gamma = M^{-1}\delta M \in \Gamma$, com $\delta \in \mathrm{SL}_2(\mathbb{Z})$,

$$j_M(\gamma \cdot \tau) = j(MM^{-1}\delta M\tau) = j(\delta M\tau) = j(M\tau) = j_M(\tau),$$

onde a terceira igualdade segue de j ter peso 0. Para ver que Γ tem índice finito em $\mathrm{SL}_2(\mathbb{Z})$, exibimos um subgrupo de Γ que tem índice finito em $\mathrm{SL}_2(\mathbb{Z})$. Considere o *subgrupo de congruência* $\Gamma(m) := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv I \pmod{m}\}$. Usando a sequência exata

$$1 \rightarrow \Gamma(m) \rightarrow \mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \rightarrow 1,$$

concluimos que $\Gamma(m)$ tem índice finito em $\mathrm{SL}_2(\mathbb{Z})$ (de fato, basta a injetividade de $\mathrm{SL}_2(\mathbb{Z})/\Gamma(m) \rightarrow \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$). Para mostrar que $\Gamma(m) \subset \Gamma$, seja $\gamma = I + mA \in \Gamma(m)$ com $A \in M_{2 \times 2}(\mathbb{Z})$. Então

$$M\gamma M^{-1} = I + MA(mM^{-1}).$$

O lado esquerdo tem determinante 1, e o lado direito tem coeficientes inteiros, pois mM^{-1} é a matriz adjunta de M . Logo

$$\delta := M\gamma M^{-1} \in \mathrm{SL}_2(\mathbb{Z}) \quad \text{e} \quad \gamma = M^{-1}\delta M \in \Gamma.$$

Passo 3: um polinômio com coeficientes modulares. Seja $d = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ e considere a decomposição em classes laterais

$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma\gamma_1 \sqcup \cdots \sqcup \Gamma\gamma_d,$$

onde $\gamma_1 = I$ por comodidade. Pelo Passo 2, a função $j_M(\gamma_i\tau)$ depende apenas da classe lateral $\Gamma\gamma_i$, e não do representante escolhido. Definimos o polinômio

$$\begin{aligned} F(x) := \prod_{i=1}^d (x - j_M(\gamma_i\tau)) &= x^d - [j_M(\gamma_1\tau) + \cdots + j_M(\gamma_d\tau)]x^{d-1} + \cdots \\ &\quad + (-1)^d [j_M(\gamma_1\tau) \cdots j_M(\gamma_d\tau)], \end{aligned}$$

visto como polinômio na variável x com coeficientes no anel de funções holomorfas em $\mathbb{H}$. Denotamos por $F_i(\tau)$ o coeficiente de x^i em $F(x)$; assim $F_d = 1$.

Afirmamos que cada $F_i(\tau)$ é uma função holomorfa invariante por $\mathrm{SL}_2(\mathbb{Z})$. De fato, $\mathrm{SL}_2(\mathbb{Z})$ age à direita em $\Gamma \backslash \mathrm{SL}_2(\mathbb{Z})$ permutando as classes $\Gamma\gamma_1, \dots, \Gamma\gamma_d$: para $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, existem uma permutação σ de $\{1, \dots, d\}$ e elementos $h_i \in \Gamma$ tais que $\gamma_i\gamma = h_i\gamma_{\sigma(i)}$, donde $j_M(\gamma_i\gamma\tau) = j_M(\gamma_{\sigma(i)}\tau)$. Como $F_i(\tau)$ é, por definição, uma expressão simétrica (elementar) em $j_M(\gamma_1\tau), \dots, j_M(\gamma_d\tau)$, segue que $F_i(\gamma\tau) = F_i(\tau)$ para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Passo 4: expansões de Fourier. Para cada i , a matriz $M\gamma_i$ tem coeficientes inteiros e determinante m . Multiplicando à esquerda por um elemento de $\mathrm{SL}_2(\mathbb{Z})$ que leva a primeira coluna $(x, y)^T$ de $M\gamma_i$ em $(\mathrm{mdc}(x, y), 0)^T$ (e eventualmente por $-I$), podemos escrever

$$M\gamma_i = \delta_i \begin{pmatrix} A_i & B_i \\ 0 & D_i \end{pmatrix},$$

com $\delta_i \in \mathrm{SL}_2(\mathbb{Z})$ e $A_i, B_i, D_i \in \mathbb{Z}$, $A_i, D_i > 0$, $A_i D_i = m$. Então, escrevendo $\zeta_D = e^{2\pi i/D}$,

$$\begin{aligned} j_M(\gamma_i\tau) &= j(M\gamma_i\tau) = j\left(\delta_i \cdot \frac{A_i\tau + B_i}{D_i}\right) = j\left(\frac{A_i\tau + B_i}{D_i}\right) \\ &= \sum_{n \geq -1} c_n e^{2\pi i n(A_i\tau + B_i)/D_i} = \sum_{n \geq -1} c_n \zeta_{D_i}^{nB_i} q^{nA_i/D_i}, \end{aligned} \quad (*)$$

onde $c_{-1} = 1$ e $c_n \in \mathbb{Q}$ são os coeficientes de Fourier de j . Como cada D_i divide m , temos $\zeta_{D_i}^{nB_i} \in \mathbb{Q}(\zeta_m)$ e q^{nA_i/D_i} é uma potência inteira de $q^{1/m} := e^{2\pi i\tau/m}$. Logo cada $F_i(\tau)$, sendo um polinômio nas funções $(*)$ com coeficientes inteiros, admite uma expansão da forma $\sum_{k \geq -K} a_{i,k} q^{k/m}$ com $a_{i,k} \in \mathbb{Q}(\zeta_m)$ e apenas um número finito de expoentes negativos. Como $F_i(\tau+1) = F_i(\tau)$, e a substituição $\tau \mapsto \tau+1$ multiplica $q^{k/m}$ por $e^{2\pi i k/m}$, a unicidade da expansão de Laurent em $q^{1/m}$ implica que $a_{i,k} = 0$ sempre que $m \nmid k$. Portanto

$$F_i(\tau) = \sum_{n \geq -N} a_n^{(i)} q^n, \quad a_n^{(i)} \in \mathbb{Q}(\zeta_m),$$

para algum $N \geq 0$. Pela Proposição 6.7, existe um polinômio $P_i(y) \in \mathbb{C}[y]$ tal que $F_i = P_i(j)$. Na realidade, o seguinte exercício mostra que $P_i \in \mathbb{Q}(\zeta_m)[y]$ para todo i .

Exercício 7.2. Dado um polinômio $P = \sum_k \alpha_k y^k$ com coeficientes $\alpha_k \in \mathbb{C}$, considere a expansão de Fourier $P(j(\tau)) = \sum_{n \geq -N} a_n q^n$. Mostre que $\alpha_k \in \mathbb{Q}(a_{-N}, a_{-N+1}, \dots)$ para todo k . (Sugestão: o coeficiente líder é $\alpha_N = a_{-N}$; subtraia $a_{-N} j^N$ e use indução, lembrando que os c_n são racionais.)

Passo 5: conclusão. Obtemos uma relação de dependência algébrica entre as funções j_M e j : o polinômio

$$P(x, y) := \sum_{i=0}^d P_i(y) x^i \in \mathbb{Q}(\zeta_m)[x, y]$$

é mônico em x (em particular, não nulo) e satisfaz $P(j_M(\tau), j(\tau)) = F(j_M(\tau)) = 0$ para todo $\tau \in \mathbb{H}$, pois $\gamma_1 = I$.

Fatore a maior potência possível de $x - y$ em $P(x, y)$:

$$P(x, y) = (x - y)^r Q(x, y), \quad Q \in \mathbb{Q}(\zeta_m)[x, y], \quad (x - y) \nmid Q(x, y).$$

Afirmamos que $j_M \neq j$ como funções em $\mathbb{H}$. De fato, por $(*)$ com $i = 1$ (lembrando que $\gamma_1 = I$, logo $M = \delta_1 \begin{pmatrix} A_1 & B_1 \\ 0 & D_1 \end{pmatrix}$), temos $j_M(\tau) = \zeta_{D_1}^{-B_1} q^{-A_1/D_1} + \sum_{n \geq 0} (\dots)$, enquanto $j(\tau) = q^{-1} + \sum_{n \geq 0} c_n q^n$. Ambas são expansões de Laurent em $q^{1/m}$. Se $j_M = j$, comparando os termos de menor expoente obtemos $A_1/D_1 = 1$ e $\zeta_{D_1}^{-B_1} = 1$, isto é, $A_1 = D_1 =: a$ e $a \mid B_1$. Mas então

$$M = a \cdot \delta_1 \begin{pmatrix} 1 & B_1/a \\ 0 & 1 \end{pmatrix}$$

seria múltiplo escalar de um elemento de $\mathrm{SL}_2(\mathbb{Z})$, contradizendo a escolha de M .

Como $P(j_M, j) = (j_M - j)^r Q(j_M, j) = 0$, $j_M - j$ é uma função holomorfa não identicamente nula em $\mathbb{H}$ (conexo) e o anel de funções holomorfas em um aberto conexo é um domínio, concluímos que $Q(j_M(\tau), j(\tau)) = 0$ para todo $\tau \in \mathbb{H}$. Avaliando em τ_0 , e usando $j_M(\tau_0) = j(M\tau_0) = j(\tau_0)$, obtemos

$$Q(j(\tau_0), j(\tau_0)) = 0.$$

Finalmente, como $x - y$ não divide $Q(x, y)$, o polinômio $Q(x, x) \in \mathbb{Q}(\zeta_m)[x]$ é não nulo (de fato, $Q(x, y) \equiv Q(x, x) \pmod{(x - y)}$). Assim, $j(\tau_0)$ é raiz de um polinômio não nulo com coeficientes no corpo de números $\mathbb{Q}(\zeta_m)$ e, portanto, é um número algébrico. $\square$

Observação 7.3. Refinando esse argumento (trocando j_M pelo conjunto de todas as funções $j(M'\tau)$ com M' primitiva de determinante m), obtém-se o *polinômio modular* $\Phi_m(x, y) \in \mathbb{Z}[x, y]$, e prova-se que $\Phi_m(x, x)$ tem coeficiente líder ± 1 quando m não é um quadrado. Isso demonstra a parte (i) do Teorema 5.10: $j(\tau_0)$ é um inteiro algébrico. Ver [2, §11] ou [6, Cap. II].

8 Funções elípticas

Nesta última seção, pincelamos as relações entre a Multiplicação Complexa e a teoria das Curvas Elípticas. Começamos com funções duplamente periódicas, também conhecidas como funções elípticas. A seguir, fixamos um reticulado $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

Definição 8.1. Uma *função elíptica* (em relação a Λ) é uma função $f: \mathbb{C} \rightarrow \mathbb{C} \cup \{\infty\}$ meromorfa tal que $f(z + \omega) = f(z)$ para quaisquer $z \in \mathbb{C}$ e $\omega \in \Lambda$.

Duas propriedades básicas, ambas consequências do Teorema de Liouville e do teorema dos resíduos aplicados a um paralelogramo fundamental P , serão

usadas a seguir: (a) uma função elíptica sem polos é constante; (b) uma função elíptica não constante f assume cada valor $c \in \mathbb{C}$ o mesmo número de vezes em P (contadas com multiplicidade), a saber, o número de polos de f em P (contados com multiplicidade). Para (b), integre $f'/(f - c)$ sobre o bordo de P (“princípio do argumento”): as contribuições de lados opostos se cancelam por periodicidade.

Exemplo 8.2. A função $\wp$ de Weierstrass é definida como

$$\wp_{\Lambda}(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

É possível mostrar que $\wp$ é elíptica e par, com polos de ordem 2 em todo ponto de Λ e nenhum outro polo. Além disso, sua série de Laurent em $z = 0$ é

$$\begin{aligned} \wp_{\Lambda}(z) &= \frac{1}{z^2} + \sum_{n \geq 1} (n+1)G_{n+2}(\Lambda)z^n \\ &= \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 5G_6(\Lambda)z^4 + \dots \end{aligned}$$

Proposição 8.3. A função $\wp_{\Lambda}$ satisfaz a equação diferencial

$$\wp'_{\Lambda}(z)^2 = 4\wp_{\Lambda}(z)^3 - g_2(\Lambda)\wp_{\Lambda}(z) - g_3(\Lambda). \quad (1)$$

Demonstração. Escreva $\wp = \wp_{\Lambda}$, $G_k = G_k(\Lambda)$. Derivando a série de Laurent, $\wp'(z) = -2z^{-3} + 6G_4z + 20G_6z^3 + O(z^5)$. Elevando ao quadrado e ao cubo:

$$\begin{aligned} \wp'(z)^2 &= 4z^{-6} - 24G_4z^{-2} - 80G_6 + O(z^2), \\ \wp(z)^3 &= z^{-6} + 9G_4z^{-2} + 15G_6 + O(z^2). \end{aligned}$$

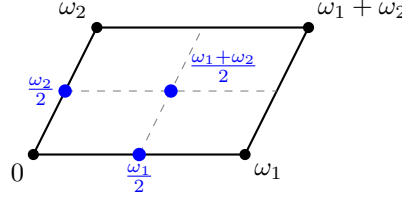
Logo

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) = -140G_6 + O(z^2) = -g_3 + O(z^2).$$

O lado esquerdo é uma função elíptica cujos únicos polos possíveis estão em Λ ; pela conta acima, ela não tem polo em 0 (e portanto em nenhum ponto de Λ , por periodicidade). Pela propriedade (a), ela é constante, e avaliando em $z = 0$ vemos que essa constante é $-g_3$. $\square$

Observação 8.4. O polinômio $P(x) = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ que aparece na equação diferencial acima tem discriminante $16\Delta(\Lambda)$. (Lembre que o discriminante de $ax^3 + cx + e$ é $-4ac^3 - 27a^2e^2$.)

Proposição 8.5. O polinômio $P(x)$ definido acima tem três raízes distintas: $e_1 = \wp_{\Lambda}(\omega_1/2)$, $e_2 = \wp_{\Lambda}(\omega_2/2)$ e $e_3 = \wp_{\Lambda}((\omega_1 + \omega_2)/2)$. Em particular, $P(x) = 4(x - e_1)(x - e_2)(x - e_3)$.



Demonstração. Seja $u \in \{\omega_1/2, \omega_2/2, (\omega_1 + \omega_2)/2\}$. Então $2u \in \Lambda$, $u \notin \Lambda$ e

$$\wp'_\Lambda(u) = \wp'_\Lambda(-u + 2u) = \wp'_\Lambda(-u) = -\wp'_\Lambda(u),$$

usando que $\wp'_\Lambda$ é duplamente periódica e ímpar. Logo $\wp'_\Lambda(u) = 0$, e segue da equação diferencial (1) que e_1, e_2, e_3 são raízes de $P(x)$.

Para ver que são distintas, note que, como $\wp'_\Lambda(u) = 0$, a função elíptica $\wp_\Lambda - \wp_\Lambda(u)$ tem um zero de ordem pelo menos 2 em u . Por outro lado, $\wp_\Lambda$ tem um único polo (de ordem 2) em um paralelogramo fundamental, logo, pela propriedade (b), $\wp_\Lambda - c$ tem exatamente 2 zeros (com multiplicidade) em um paralelogramo fundamental, para todo $c \in \mathbb{C}$. Se fosse, por exemplo, $e_1 = e_2$, então $\wp_\Lambda - e_1$ teria pelo menos 4 zeros (dois em $\omega_1/2$ e dois em $\omega_2/2$, que são pontos distintos módulo Λ), absurdo. Como P tem coeficiente líder 4 e três raízes distintas e_1, e_2, e_3 , temos $P(x) = 4(x - e_1)(x - e_2)(x - e_3)$. $\square$

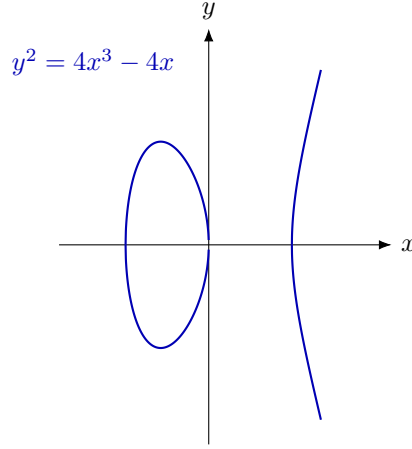
Observação 8.6. O mesmo argumento mostra que $\wp_\Lambda(z_1) = \wp_\Lambda(z_2)$ se, e somente se, $z_1 \equiv \pm z_2 \pmod{\Lambda}$.

Corolário 8.7. *O discriminante $\Delta(\Lambda)$ não se anula. Mais precisamente,*

$$\Delta(\Lambda) = \frac{1}{16} \text{disc}(P) = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 \neq 0.$$

Isso demonstra a Proposição 5.8.

Observação 8.8. Geometricamente, uma equação cúbica $y^2 = 4x^3 - ax - b$ com $a^3 - 27b^2 \neq 0$ define uma *curva elíptica* complexa E (mais precisamente, E é o fecho projetivo desta curva em $\mathbb{P}^2$, que tem um único ponto adicional, o “ponto no infinito” $(0 : 1 : 0)$). A figura abaixo mostra os pontos reais de E no caso $a = 4, b = 0$.



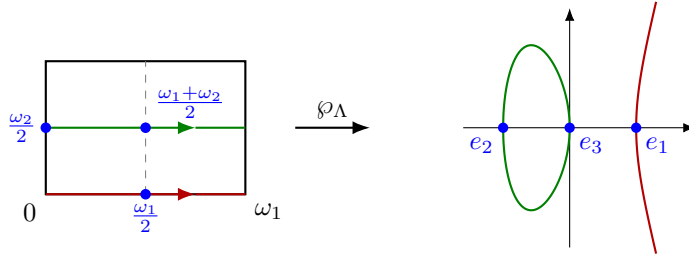
Se $\Lambda \subset \mathbb{C}$ é um reticulado tal que $g_2(\Lambda) = a$ e $g_3(\Lambda) = b$, então as funções elípticas $\wp_\Lambda$ e $\wp'_\Lambda$ uniformizam a curva elíptica complexa E :

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E \subset \mathbb{P}^2, \quad z \bmod \Lambda \mapsto \begin{cases} (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1), & z \notin \Lambda, \\ (0 : 1 : 0), & z \in \Lambda. \end{cases}$$

O quociente $\mathbb{C}/\Lambda$ à esquerda é um “toro complexo” (um grupo de Lie complexo compacto de dimensão 1), enquanto E é uma curva algébrica com estrutura de grupo algébrico, cujo elemento neutro é o ponto no infinito; a bijeção acima é um isomorfismo de grupos. Sob essa uniformização, $\wp_\Lambda$ é a coordenada x e $\wp'_\Lambda$ é a coordenada y de E .

Nessa linguagem, homotetias de reticulados $\Lambda \rightarrow \Lambda'$ correspondem a morfismos de grupos algébricos $E \rightarrow E'$; em particular, $R_\Lambda \cong \text{End}(E)$, e Λ tem multiplicação complexa se, e somente se, $\text{End}(E) \neq \mathbb{Z}$. Além disso, o j -invariante $j(\Lambda) = j(E) = 1728a^3/(a^3 - 27b^2)$ classifica E a menos de isomorfismo sobre $\mathbb{C}$ e determina o *corpo de definição* minimal de E : a saber, $\mathbb{Q}(j(E))$. Ou seja, a algebricidade dos valores singulares (que provamos na última seção) diz que toda curva elíptica com multiplicação complexa pode ser definida sobre $\overline{\mathbb{Q}}$.

Observação 8.9. A conexão entre reticulados e curvas elípticas também passa pelas *integrais elípticas*: a uniformização acima é a inversa de uma integral elíptica. Para explicar isso, suponha, para simplificar, que $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ é retangular, com $\omega_1 \in \mathbb{R}_{>0}$ e $\omega_2 \in i\mathbb{R}_{>0}$. Então $a = g_2(\Lambda)$ e $b = g_3(\Lambda)$ são reais, $\wp_\Lambda$ é real nos segmentos horizontais e verticais que passam pelos pontos de $\frac{1}{2}\Lambda$, e as raízes e_1, e_2, e_3 são reais, com $e_2 < e_3 < e_1$. Na figura, o segmento horizontal (em verde) de $\omega_2/2$ a $\omega_2/2 + \omega_1$ é levado no laço compacto da curva real, e o eixo real (em vermelho) na componente ilimitada.



Usando a coordenada uniformizada $x = \wp_\Lambda(z)$, de modo que $dx = \wp'_\Lambda(z) dz = y dz$, seguem as identidades

$$\begin{aligned}\omega_1 &= 2 \int_{\omega_2/2}^{(\omega_1+\omega_2)/2} dz = 2 \int_{e_2}^{e_3} \frac{dx}{\sqrt{4x^3 - ax - b}}, \\ \omega_2 &= 2 \int_{\omega_1/2}^{(\omega_1+\omega_2)/2} dz = 2i \int_{e_3}^{e_1} \frac{dx}{\sqrt{-(4x^3 - ax - b)}}.\end{aligned}$$

(No intervalo $[e_2, e_3]$ o polinômio $4x^3 - ax - b$ é não negativo, e em $[e_3, e_1]$ é não positivo.)

Finalmente, enunciaremos a descrição explícita das extensões abelianas de um corpo quadrático imaginário. Seja $\Lambda \subset \mathbb{C}$ um reticulado com multiplicação complexa e seja $e_\Lambda := |R_\Lambda^\times|/2$ (lembrando que R_Λ é o anel das homotetias). Em geral, temos $e_\Lambda = 1$ (isto é, $R_\Lambda^\times = \{\pm 1\}$), exceto nos casos especiais (a menos de homotetia) $e_{\mathbb{Z}+\mathbb{Z}i} = 2$ e $e_{\mathbb{Z}+\mathbb{Z}\rho} = 3$.

Definição 8.10. A função τ de Weber é

$$\tau_\Lambda(z) := (-\wp_\Lambda(z))^{e_\Lambda} \cdot c(\Lambda),$$

onde

$$c(\Lambda) = \begin{cases} 2^7 3^5 g_2(\Lambda) g_3(\Lambda) / \Delta(\Lambda), & \text{se } e_\Lambda = 1, \\ 2^8 3^4 g_2(\Lambda)^2 / \Delta(\Lambda), & \text{se } e_\Lambda = 2, \\ 2^9 3^6 g_3(\Lambda) / \Delta(\Lambda), & \text{se } e_\Lambda = 3. \end{cases}$$

(A constante $c(\Lambda)$ é escolhida de modo que τ_Λ seja invariante por homotetia, isto é, $\tau_{\alpha\Lambda}(\alpha z) = \tau_\Lambda(z)$; a potência e_Λ torna τ_Λ invariante pela ação de $R_\Lambda^\times$, isto é, $\tau_\Lambda(uz) = \tau_\Lambda(z)$ para $u \in R_\Lambda^\times$.)

Teorema 8.11. *Seja K um corpo quadrático imaginário e seja $\Lambda = \mathcal{O}_K = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ seu anel de inteiros. Toda extensão abeliana de K está contida em uma extensão de K gerada por $j(\Lambda)$ e números da forma $\tau_\Lambda((a\omega_1 + b\omega_2)/n)$, com $a, b, n \in \mathbb{Z}$, $n \geq 1$. Ou seja, a extensão abeliana maximal de K é*

$$K^{\text{ab}} = K(j(\Lambda), \tau_\Lambda(z) : z \in \mathbb{Q}\Lambda \setminus \Lambda).$$

Observação 8.12. A função $\wp_\Lambda$ (ou τ_Λ) também é uma aplicação exponencial, no sentido de Teoria de Lie. De fato, a uniformização $z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$ é

a aplicação exponencial do grupo de Lie complexo E :

$$\begin{array}{ccc} \mathrm{Lie}(E) & \xrightarrow{\exp} & E \\ \wr \parallel & \nearrow & \\ \mathbb{C} & & (\wp_\Lambda : \wp'_\Lambda : 1) \end{array}$$

cujo núcleo é Λ , assim como $z \mapsto e^{2\pi iz}$ é a aplicação exponencial de $\mathbb{C}^\times$, com núcleo $\mathbb{Z}$. Os valores $\tau_\Lambda((a\omega_1 + b\omega_2)/n)$ correspondem aos pontos de torção de E (mais precisamente, às imagens desses pontos no quociente $E/\mathrm{Aut}(E)$). Resumindo a analogia:

Corpo	Função	Grupo algébrico
$\mathbb{Q}$	$\exp$	$\mathbb{G}_m = \mathbb{C}^\times$
K quadrático imaginário	$j, \wp$ (ou τ)	E com multiplicação complexa

Algumas referências

- [1] Armand Borel et al. *Seminar on Complex Multiplication*. Vol. 21. Lecture Notes in Mathematics. Berlin, Heidelberg: Springer-Verlag, 1966.
- [2] David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. New York: John Wiley & Sons, 1989.
- [3] Reinhard Schertz. *Complex Multiplication*. Vol. 15. New Mathematical Monographs. Cambridge: Cambridge University Press, 2010.
- [4] Jean-Pierre Serre. *A Course in Arithmetic*. Vol. 7. Graduate Texts in Mathematics. New York: Springer-Verlag, 1973.
- [5] Jean-Pierre Serre. «Complex Multiplication». Em: *Algebraic Number Theory*. Ed. por J. W. S. Cassels e A. Fröhlich. London: Academic Press, 1967. Cap. 13, pp. 292–296.
- [6] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Vol. 151. Graduate Texts in Mathematics. New York: Springer-Verlag, 1994.
- [7] Don Zagier. «Elliptic Modular Forms and Their Applications». Em: *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway*. Ed. por Jan Hendrik Bruinier et al. Universitext. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 1–103.