TÓPICOS EM TEORIA DOS NÚMEROS

MURILO CORATO ZANARELLA

2021

O QUE SERÃO ESSAS AULAS

A ideia dessas aulas é explicar resultados clássicos de pesquisa em teoria dos números de maneira acessível a um público familiarizado com as técnicas de olimpíada de matemática, porém, ao mesmo tempo, utilizando a linguagem usada em pesquisa de matemática. Para isso, eu tentarei usar o conhecimento prévio de olimpíadas como base da intuição para novos conceitos, e destacar como podemos perceber esse conhecimento prévio em contextos mais gerais e abstratos.

Teoria dos números é, de maneira grosseira, dividida em *algébrica* e *analítica*. Inicialmente, iremos estudar ambas separadamente, mas com a passar do tempo veremos fenômenos que acontecem na intersecção das duas áreas. O primeiro exemplo disso e o primeiro grande objetivo dessas aulas será explicar a prova do teorema de Dirichlet:

Theorem (Dirichlet)**.** *Seja n um inteiro positivo e a primo com n. Então existem infinitos primos p tal que $p \equiv a \mod n$.*

Basicamente, iremos usar métodos analíticos para reduzir o teorema a provar que certos valores $L(1, \chi)$ são diferentes de 0, e usaremos métodos algébricos para provar esse segundo fato.

Antes disso, porém, precisamos cobrir dois grandes pré-requisitos: *álgebra* e *análise complexa*. Podemos pensar nesses dois requisitos como as linguagens da teoria algébrica e analítica, respectivamente.

1. 6 de Março

Hoje veremos a noção de *grupos*, *anéis* e *corpos*. Também falaremos um pouco sobre fatoração em anéis.

Estruturas Algébricas. Grupos, anéis e corpos são exemplos de estruturas algébricas, e iremos tratá-las com a seguinte filosofia:

(1) Essas estruturas surgem por abstrair certas propriedades interessantes de objetos: as *propriedades* dos exemplos virarão *definições*. Deve-se pensar nisso como em olimpíada chamamos algo de *bonito* por satisfazer alguma propriedade que nos interessa.
(2) Tão importante quanto as estruturas em si são os mapas entre elas.

1.1. **Grupos.** Grupos surgem da abstração da ideia de *simetria*.

Exemplo 1.1. As simetrias de um triângulo equilátero consistem de 3 rotações e 3 reflexões.

Certas propriedades que podemos observar de tais simetrias: i) podemos compor simetrias, ii) toda simetria tem um inverso. Disso, surge a definição:

Definição 1.2. Um grupo $(G, \cdot)$ é um conjunto G com uma operação $\cdot : G \times G \to G$ tal que: i) existe $e \in G$ tal que $e \cdot g = g \cdot e = g$ para todo $g \in G$, ii) para qualquer $g \in G$, existe $g^{-1} \in G$ tal que $g \cdot g^{-1} = g^{-1} \cdot g = e$, iii) $\cdot$ é associativo.

Exemplo 1.3. Os seguintes são exemplos de grupos.

- Simetrias de um n-ágono regular. Chamado de D_n, Tem tamanho $2n$.
- Simetrias de um conjunto $\{1, \ldots, n\}$, ou seja, permutações. Chamado de S_n, tem tamanho $n!$.
- Simetrias de sólidos platônicos.
- $(\mathbb{Z}, +)$ e $(\mathbb{Z}/n\mathbb{Z}, +)$.
- $\mathrm{GL}_n(\mathbb{R})$, o grupo de matrizes invertíveis $n \times n$.

Seguindo o ponto 2 da filosofia descrita anteriormente, vamos analisar mapas entre grupos.

Definição 1.4. Um mapa $G \to H$ é um morfismo de grupos se: i) $f(e) = e$, ii) $f(gg') = f(g)f(g')$ para todo $g, g' \in G$.

Nota 1.5. É automático que $f(g^{-1}) = f(g)^{-1}$.

Exemplo 1.6. Os sequintes são exemplos de morfismos de grupos.

- $D_n \subseteq D_m$ se $n \mid m$.
- $S_a \times S_b \subseteq S_{a+b}$.
- $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$.
- $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$.

O terceiro exemplo sugeste que podemos tentar criar quocientes G/K. Note que em $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$, os elementos que mapeiam para a identidade 0 são exatamente o "denominador" $n\mathbb{Z}$.

Definição 1.7. O kernel de um morfismo de grupos $f\colon G \to H$ é $\ker f = \{g \in G\colon f(g) = e\}$.

Note que o kernel $K = \ker f$ é um subgrupo de G. Mas mais é verdade: se $g \in G$ e $k \in K$, temos

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)ef(g)^{-1} = f(g)f(g)^{-1} = e,$$

logo $gkg^{-1} \in K$. Isso motiva a definição:

Definição 1.8. Um subgrupo $K \subseteq G$ é normal se $gKg^{-1} \subseteq K$ para todo $g \in G$.

Proposição 1.9. *Subgrupos normais são exatamente os kernels de morfismos.*

Demonstração. Vimos acima que kernels são subgrupos normais.

Para o contrário, seja $K \subseteq G$ normal. Vamos construir o grupo G/K, com um morfismo $f\colon G \to G/K$ tal que $K = \ker f$. Para isso, considere a relação de equivalência $a \sim b$ se $a \in bK$. Agora sejam $a \sim b$ e $c \sim d$. Para checar que $ac \sim bd$, escreva $a = bk_1$ e $c = dk_2$, e note que

$$ac = bk_1dk_2 = (bd)(d^{-1}k_1d)k_2 \in bdK.$$

Para checar que $a^{-1} \sim b^{-1}$, note que

$$a^{-1} = k_1^{-1}b^{-1} = b^{-1}(bk_1^{-1}b^{-1}) \in b^{-1}K.$$

Portanto G/K é um grupo como queríamos. □

Corolário 1.10. *Todo morfismo $f\colon G \to H$ fatora como*

$$G \twoheadrightarrow G/\ker f \hookrightarrow H.$$

1.2. **Anéis.** Anéis surgem da abstração das propriedades de $\mathbb{Z}$. Temos o seguinte: i) $(\mathbb{Z}, +)$ é um grupo comutativo, ii) $\cdot$ é comutativo e associativo, iii) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Definição 1.11. Um anél $(A, +, \cdot)$ é tal que: i) $(A, +)$ é um grupo comutativo, ii) $\cdot$ é associativo e comutativo, e possui identidade 1, iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ para todo $a, b, c \in A$.

Nota 1.12. É automático que $a \cdot 0 = 0$ e $a \cdot (-b) = -a \cdot b$.

Exemplo 1.13. Os seguintes são exemplos de anéis.

- $0 = \{0\}$ o anel com 1 elemento.
- $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ por adição.
- $R[x]$ para um anel R.
- $\{\text{funções } \mathbb{R} \to \mathbb{R}\}$ por adição e multiplicação ponto a ponto.

Definição 1.14. Um morfismo de anéis $f\colon A \to B$ é tal que i) $(A, +) \to (B, +)$ é um morfismo de grupos, ii) $f(ab) = f(a)f(b)$, iii) $f(1) = 1$.

Exemplo 1.15. Os seguintes são morfismos de anéis.

- $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, ou $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ para $d \mid n$.
- $\mathbb{C}[x] \to \mathbb{C}$ onde $x \mapsto 5$.
- $\{\text{funções } \mathbb{R} \to \mathbb{R}\} \to \mathbb{R}$ onde $f \mapsto f(0)$.

Da mesma maneira que aconteceu com grupos, poderemos criar quocientes por kernels.

Definição 1.16. Se $f\colon A \to B$ é um morfismo de anéis, $\ker f = \{a \in A\colon f(a) = 0\}$.

Nota 1.17. $K = \ker f$ quase nunca é um anél! Não necessariamente temos que $1 \in K$. Porém, temos que $0 \in K$, $K + K \subseteq K$ e $A \cdot K \subseteq K$.

Definição 1.18. Um ideal $I \subseteq A$ é tal que i) $0 \in I$, ii) $I + I \subseteq I$, iii) $A \cdot I \subseteq I$.

Da mesma forma que para grupos, podemos construir o anel A/I e provar o seguinte.

Proposição 1.19. *Ideais são o mesmo que kernels de morfismos de anéis.*

Exemplo 1.20. Os seguintes são exemplos de ideais.

- 0 e A são sempre ideais de A.
- Se $a \in A$, temos o ideal $(a) := aA$. Chamamos tais ideais de *ideais principais*.
- $I = \{\text{funções } \mathbb{R} \to \mathbb{R} \text{ tais que } f(0) = 0\} \subseteq A = \{\text{funções } \mathbb{R} \to \mathbb{R}\}$.

1.3. **Corpos.** Corpos surgem da abstração das propriedades de $\mathbb{Q}$. Além de ser um anél, $\mathbb{Q} - \{0\}$ é um grupo.

Definição 1.21. Um corpo $(K, +, \cdot)$ é tal que i) $(K, +, \cdot)$ é um anél, ii) $(K - \{0\}, \cdot)$ é um grupo.

Exemplo 1.22. Os seguintes são exemplos de corpos.

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- $\mathbb{Z}/p\mathbb{Z}$.
- $\mathbb{R}((x)) = \{\sum_{n \geq -N} a_n x^n : a_n \in \mathbb{R}, N \in \mathbb{N}\}$.

Note que $K \to L$ ser um morfismo de corpos é o mesmo que ser um morfismo de anéis, e portanto temos que inverstigar ideais de um corpo K.

Proposição 1.23. *Um anél A é um corpo se e somente se tem exatamente dois ideais 0 e A.*

Demonstração. Se A tem examente dois ideais 0 e A e $a \in A$ é não-zero, então o ideal (a) tem que ser A. Em particular, existe $b \in A$ tal que $ab = 1$, e portanto a é invertível.

Se A é um corpo e $I \subseteq A$ é não-zero, tome $i \in I$ não-zero. Como A é um corpo, $1 = i \cdot i^{-1} \in I$, e portanto $a = 1 \cdot a \in I$ para todo $a \in A$. Logo $I = A$. □

Corolário 1.24. *Todo morfismo de corpos é injetor.*

Demonstração. Um morfismo de corpos não pode ser 0 porque $1 \mapsto 1$ e $1 \neq 0$. □

Para $K \hookrightarrow L$, dizemos que L é uma *extensão* de K.

	Abstraindo	Operações	Kernels
Grupos	simetrias	$\cdot$, inverso	subgrupos normais
Anéis	$\mathbb{Z}$	$+, -, \cdot$	ideais
Corpos	$\mathbb{Q}$	$+, -, \cdot, /$	0

1.4. **Fatoração única.** Vamos lembrar como provamos fatoração única em $\mathbb{Z}$. Lembrando que temos a ambiguidade de sinal ± 1.

- Fatorar é fácil, pois o tamanho dos elementos diminui quando de fatora um primo.
- Para unicidade, se prova que $p \mid ab \implies p \mid a$ ou $p \mid b$, e usa isso para cancelar p_1 de ambos os lados de $p_1^{a_1} \cdots p_n^{a_n} = q_1^{b_1} \cdots q_m^{b_m}$.

A parte difícil é provar que $p \mid ab \implies p \mid a$ ou $p \mid b$. Para isso, se usa Bezout: $\{\alpha a + \beta p\} = d\mathbb{Z}$ para algum d. Em termos de ideais, Bezout diz que (a, p) é um ideal principal. Como $d \mid p$, temos $d = \pm 1$ ou $d = \pm p$. Se $d = \pm p$, temos $p \mid a$ pois $d \mid a$. Se $d = \pm 1$, temos $\alpha a + \beta p = 1$, e então $b = \alpha ab + \beta pb$, que é múltiplo de p.

A história em, por exemplo, $\mathbb{Z}[i]$, é bem parecida. As únicas mudanças é que a ambiguidade é de $\pm 1, \pm i$ e que a prova de Bezout é um pouco mais difícil.

Vamos tentar abstrair isso:

Definição 1.25. Para um anél A, $a \in A$ é uma *unidade* se existe a^{-1} com $a \cdot a^{-1} = 1$. Denotamos o grupo de unidades por $A^\times$. $a \in A$ é *irredutível* se $b \mid a \implies b \in R^\times$ ou $b \in aR^\times$. Finalmente, $a \in A$ é *primo* se $a \mid bc \implies a \mid b$ ou $a \mid c$.

Temos a seguinte estratégia para fatoração única em elementos irredutíveis:

(1) Fatora: precisamos de uma noção de "tamanho".
(2) Prova que irredutível $\implies$ primo: usaremos uma versão de Bezout.
(3) Cancela o fator.

Para a terceira parte, criamos a seguinte definição.

Definição 1.26. Um anél A é um *domínio* se $ab = 0 \implies a = 0$ ou $b = 0$.

Note que $ab = ac \iff a(b - c) = 0$, então podemos cancelar um $a \neq 0$ em um domínio. Para a segunda parte, definimos:

Definição 1.27. A é um *domínio de ideais principais* (PID) se é um domínio onde todo ideal é principal.

Então temos a seguinte "implicação"

$$PID \implies \text{fatoração única}$$

desde que tenhamos uma boa noção de "tamanho".[1]

Vamos analisar mais de perto a prova de Bezout, e tentar generalizá-la.

Teorema 1.28 (Bezout)**.** *$\mathbb{Z}$ é um PID.*

[1]Isso na verdade não é necessário: a implicação é verdade sempre.

Demonstração. Seja $I \subseteq \mathbb{Z}$ um ideal não-zero. Seja $d \in I$ um dos menores elemento de I diferente de 0. Se $a \in I$, temos a divisão euclideana $a = qd + r$ com $0 \leq r < |d|$. Como $r = a - qd \in I$ e d é mínimo, temos que ter $r = 0$. Logo todo elemento de I é múltiplo de d, ou seja, $I = d\mathbb{Z}$. □

Pensando em que partes da prova não generalizam, definimos

Definição 1.29. Um *domínio Euclideano* (ED) A é um domínio com uma função $|\cdot| \colon A - \{0\} \to \mathbb{Z}_{\geq 0}$ tal que para quaisquer elementos $a, b \neq 0$, existem q, r com $a = qb + r$, e tal que ou $r = 0$ ou $|r| < |b|$.

e daí temos

Teorema 1.30 (Bezout)**.** *Todo ED é um PID.*

Para concluir que todo ED tem fatoração única, basta utilizar a função $|\cdot|$ como a nossa noção de tamanho. Os detalhes serão um exercício.

Teorema 1.31. *Todo ED tem fatoração única.*[2]

Exemplo 1.32. Os seguintes são exemplos de ED.

- $\mathbb{Z}[i]$ onde $|a + bi| = a^2 + b^2$.
- $\mathbb{Z}[\omega]$ onde $|a + b\omega| = a^2 + ab + b^2$
- $K[x]$ para um corpo K, onde $|f(x)| = \deg f$.

Para um exemplo de anél sem fatoração única, tome $\mathbb{Z}[\sqrt{-5}|$. Temos $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, e todos os 4 elementos são irredutíveis. Iremos "consertar" isso no futuro.

Em $\mathbb{Z}$, reduzir módulo um primo p nos dá um corpo $\mathbb{Z}/p\mathbb{Z}$. Isso generaliza para os casos acima:

Proposição 1.33. *Se A é um ED e $p \in A$ é um primo, então $A/(p)$ é um corpo.*

Demonstração. Seja $\overline{a} \in A/(p)$ um elemento diferente de 0, e seja $a \in A$ que reduz para $\overline{a}$. Então $p \nmid a$, e por Bezout temos $px + ay = 1$. Mas daí $\overline{ay} = 1$, portanto $\overline{a}$ é invertível, e $A/(p)$ é um corpo. □

Exemplo 1.34. Considere $3 \in \mathbb{Z}[i]$. Então $\mathbb{Z}[i]/(3) = \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\}$ é um corpo de $9 = 3^2$ elementos.

Nos casos que nos interessam, corpos que surgem assim serão finitos, então estudaremos corpos finitos em mais detalhe na próxima aula.

[2]Domínios com fatoração única são chamados de *domínios de fatoração única* (UFD).

Exercícios

Dicas estão no rodapé.

(1) Eu usei implicitamente na aula que se $f\colon G \to H$ é um morfismo de grupos com $\ker f = e$, então f é injetor. Prove isso. Prove o resultado análogo para anéis.

(2) Se H é um subgrupo de um grupo finito G, prove que $|H| \mid |G|$. Deduza disso que $g^{|G|} = e$ para todo $g \in G$.[3]

(3) Seja H um subgrupo normal de G. Verifique que existe uma bijeção

$$\{\text{subgrupos de } G/H\} \leftrightarrow \{\text{subgrupos de } G \text{ que contém } H\}.$$

Se I é um ideal de A, verifique também a bijeção

$$\{\text{ideais de } A/I\} \leftrightarrow \{\text{ideais de } A \text{ que contém } I\}.$$

(4) Prove que $a \cdot 0 = 0$ e $a \cdot (-b) = -a \cdot b$ seguem dos axiomas de um anél.[4]

(5) Seja K um corpo e $f(x) \in K[x]$ um polinômio. Quando é que $K[x]/(f(x))$ é um corpo?[5]

(6) Seja $R = \mathbb{Z}[\sqrt{2}]$. Determine $R^\times$.

(7) Seja $R = \mathbb{Z}[\sqrt{-5}]$. Ache um ideal que não é principal.[6]

(8) Prove que os seguintes anéis tem fatoração única, e ache suas unidades e seus primos

(a) $\mathbb{Z}[i]$,

(b) $\mathbb{Z}[\omega]$ onde $\omega = e^{2\pi i/3}$,

(c) $\mathbb{Q}[\![x]\!] := \{\text{funções geratrizes com coeficientes em } \mathbb{Q}\} = \{\sum_{n\geq 0} a_n x^n \colon a_n \in \mathbb{Q}\}$.

(9) Prove que sempre podemos fatorar em irredutíveis em um ED, e conclua que ED's tem fatoração única:

(a) Seja $f\colon A - \{0\} \to \mathbb{Z}_{\geq 0}$ a função dada para o ED A. Defina $g\colon A - \{0\} \to \mathbb{Z}_{\geq 0}$ por

$$g(a) = \min_{b \in A - \{0\}} f(ab).$$

Prove que A tem divisão euclideana com g, e que $g(ab) \geq g(a)$ para todos $a, b \neq 0$.

(b) Prove que se $a, b \neq 0$ com $b \notin A^\times$, então $g(ab) > g(a)$.

(c) Conclua que sempre é possível fatorar em A.

---

[3] prove que $aH = bH \iff b \in aH$

[4] o que acontece se $b = 0$ em $a \cdot (b + c) = a \cdot b + a \cdot c$?

[5] use o exercício 3.

[6] use alguns dos elementos em $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

2. 13 de Março

2.1. **Corpos Finitos.** Aula passada comentamos como corpos finitos aparecerão em breve como quocientes por primos. Será útil entendermos mais sobre corpos finitos.

Definição 2.1. Para todo anél R, temos um único morfismo de anéis $f\colon \mathbb{Z} \to R$. Se $\ker f = n\mathbb{Z}$ para $n \geq 0$, dizemos que R tem *característica* n, denotado $\operatorname{char}(R) = n$.

Proposição 2.2. *Se R é um domínio, então $\operatorname{char}(R)$ ou é 0 ou é um primo.*

Demonstração. Se $n = \operatorname{char}(R)$ é positivo, e se $p \mid n$ é um primo, então temos $p \cdot (n/p) = 0$. Mas R é um domínio, e como $n/p \notin n\mathbb{Z}$, isso força que $p = 0$, e logo $n = p$. □

Corolário 2.3. *Se R é um domínio finito, então $|R| = p^n$ para algum primo p.*

Demonstração. Em geral, para qualquer corpo F e anel R com $F \subseteq R$, temos que R é um espaço vetorial sobre F.

Então R é um espaço vetorial sobre $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, e a dimensão precisa ser finita pois R é finito. □

Agora seja F um corpo finito. Como vimos acima, $|F| = p^n$ para algum primo p. Não usaremos o seguinte teorema, mas é um fato importante cuja prova será um exercício.

Teorema 2.4. *Existe um único corpo finito de ordem p^n para toda potência de primo. Denotamos tal corpo de $\mathbb{F}_{p^n}$. Além disso, $\mathbb{F}_{p^n}$ contém $\mathbb{F}_{p^m}$ se e somente se $m \mid n$.*

O que usaremos é que, assim como $\mathbb{F}_p$, todo corpo finito tem raiz primitiva. A prova é a mesma prova para $\mathbb{F}_p$.

Teorema 2.5. *Seja F um corpo finito. Então F tem uma raiz primitiva, ou seja, temos que $F^\times \simeq \mathbb{Z}/(p^n - 1)\mathbb{Z}$.*

Demonstração. Seja c_d a quantidade de elementos de $F^\times$ de ordem d. Note que $c_d = 0$ se $d \nmid |F^\times| = p^n - 1$. Então temos

$$\sum_{d \mid p^n - 1} c_d = |F^\times| = p^n - 1.$$

Se $a \in F$ é tem ordem d, então $1, a, a^2, \ldots, a^{d-1}$ são raízes de $x^d - 1$, e como $F[x]$ tem fatoração única, são todas as raízes. Ou seja, se tal a existe, $c_d = \varphi(d)$. Se tal a não existe, $c_d = 0$. Mas

$$\sum_{d \mid p^n - 1} \varphi(d) = p^n - 1,$$

e portanto temos que ter $c_d = \varphi(d)$ para todo $d \mid p^n - 1$. Em particular $c_{p^n-1} > 0$, e existe raiz primitiva. □

Mudança de foco para ideais. Em 1843, Kummer, na tentativa de resolver $x^n + y^n = z^n$, introduziu a ideia de *números ideais*. No período de 1870 a 1896, Dedekind formalizou esse conceito no que aprendemos como *ideais*, e extendeu as ideais de Kummer para outras situações. Hoje temos o objetivo de entender essas ideias.

2.2. **Aritmética de ideais.** Iremos começar a tratar ideais como o objeto fundamental invés de números. Para isso, vamos definir operações aritméticas em ideais.

Definição 2.6. Sejam $I, J \subseteq R$ dois ideais de R. Então temos os seguintes ideais

(1) $I + J = \{i + j \colon i \in I, j \in J\}$.
(2) $I \cap J$.
(3) $I \cdot J = \{\sum_{k=1}^{n} i_k j_k \colon i_k \in I, j_k \in J\}$.

Nota 2.7. Note que $I \cdot J \subseteq I \cap J$. Isso não necessariamente é uma igualdade, por exemplo se $I = J = (p) \subseteq \mathbb{Z}$.

Exemplo 2.8. Seja R um ED. Então temos

(1) $(a) + (b) = (\mathrm{mdc}(a, b))$.
(2) $(a) \cap (b) = (\mathrm{mmc}(a, b))$.
(3) $(a) \cdot (b) = (ab)$.
(4) $a \mid b$ se e somente se $(b) \subseteq (a)$.

Queremos também generalizar a noção de primo e irredutível para ideais. Do ponto 4 acima, os análogo de irredutível e primo são:

Definição 2.9. Seja R um anel. Um ideal próprio $I \subset R$ é *maximal* se para qualquer outro ideal $I \subseteq J \subseteq R$ temos que ter $J = I$ ou $J = R$.

Definição 2.10. Seja R um anel. Um ideal próprio $I \subseteq R$ é *primo* se para quaisquer ideais J_1, J_2, temos que $J_1 J_2 \subseteq I \implies J_1 \subseteq I$ ou $J_2 \subseteq I$.

Normalmente, essas noções são definidas como o que segue.

Proposição 2.11. *Seja $I \subseteq R$ um ideal. Então I é maximal se e somente se R/I é um corpo.*

Demonstração. Segue do exercício 3 da primeira aula. □

Proposição 2.12. *Seja $I \subseteq R$ um ideal. Então I é primo se e somente se R/I é um domínio.*

Demonstração. Seja I primo. Considere $\overline{a}\overline{b} = 0 \in R/I$. Isso significa que $ab \in I$, e então $(a)(b) \subseteq I$. Mas I é primo, então $a \in I$ ou $b \in I$, ou seja, $\overline{a} = 0$ ou $\overline{b} = 0$.

Agora seja I tal que R/I é um domínio. A mesma prova acima prova que $ab \in I \implies a \in I$ ou $b \in I$. Agora suponha que $J_1 J_2 \subseteq I$ mas $J_1 \nsubseteq I$ e $J_2 \nsubseteq I$. Seja $a \in J_1 - I$ e $b \in J_2 - I$. Então $ab \in J_1 J_2 \subseteq I$, e temos um absurdo. □

Nota 2.13. Note que da discussão acima, temos que I maximal $\implies$ I primo.

Nota 2.14. Ideais maximais não são exatos análogos de elementos irredutíveis. Em um domínio, elementos primos são irredutíveis, mas em ideais a implicação é no outro caminho. O que aconteceu? Acontece que fizemos a tradução assumindo que todo ideal é principal, mas se isso não é verdade, pode ser que (a) não é maximal para um irredutível a. Tome $R = \mathbb{Z}[\sqrt{-5}]$ e $a = 2$. Então a é irredutível, mas $(2) \subset (2, 1 + \sqrt{-5})$.

A aritmética de ideais não é muito diferente da aritmética que estamos acostumados desde que lembramos o dicionário do Exemplo 2.8.

Exemplo 2.15. A falha de fatoração única em $\mathbb{Z}[\sqrt{-5}]$ será remediada com ideais. O contra-exemplo $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ será "concertado" pois

$$(2, 1 + \sqrt{-5})^2 = (4, 2 + 2\sqrt{-5}, 6) = (2),$$
$$(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = (9, 3 + 3\sqrt{-5}, 3 - 3\sqrt{-5}, 6) = (3),$$

portanto (6) tem fatoração em ideais primos dada por

$$(6) = (2, 1 + \sqrt{-5})^2 (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

Note também que

$$(2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5}) = (6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, 6) = (1 + \sqrt{-5}).$$

Outro exemplo é que o Teorema Chinês dos restos também funciona para ideais. A prova será um exercício.

Teorema 2.16. *Seja R um anel e I, J ideais tais que $I + J = R$. Então $IJ = I \cap J$ e temos um isomorfismo*

$$R/(I \cap J) \xrightarrow{\sim} R/I \times R/J.$$

2.3. **Estratégia para fatoração única em ideais.** Eventualmente queremos provar que certos anéis tem fatoração única em ideais. Vamos usar o que discutimos de fatoração como inspiração para tentar provar isso.

Lembre-se que provamos fatoração única para certos anéis do seguinte modo:

(1) Prova que existe fatoração em irredutíveis.
(2) Prova que irredutível $\implies$ primo.
(3) Prova que é possível cancelar irredutíveis.

Traduzindo para as noções análogas em ideais, temos a estratégia:

(1) Prova que um ideal I é um produto de ideais maximais.
(2) Prova que ideais maximais também são ideais primos.
(3) Prova que podemos cancelar ideais maximais.

Note que o ponto (2) agora é automático!

Vamos pensar no ponto (3). Queremos provar que se $\mathfrak{p}I = \mathfrak{p}J$ para um ideal maximal $\mathfrak{p}$, então $I = J$. Se pensarmos na situação nos inteiros, temos $pa = pb$, e normalmente pensamos que isso implica $a = b$ pois podemos multiplicar por $p^{-1} \in \mathbb{Q}$. Considere a situação que temos um anél R dentro de um corpo K. Queremos o seguinte:

($\star$) Se $\mathfrak{p} \subseteq R$ é um ideal maximal, existe um conjunto $\mathfrak{p}^{-1} \subseteq K$ tal que $\mathfrak{p}\mathfrak{p}^{-1} = R$.

Dado isso, temos a seguinte estratégia para provar (1):

(a) Provar que existe um ideal maximal $\mathfrak{p}$ com $I \subseteq \mathfrak{p}$. Por ($\star$), obtemos $I = \mathfrak{p}J$ onde $J = I\mathfrak{p}^{-1}$. J é um ideal pois $J = I\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R$.
(b) Provar que o processo termina.

Para isso, usaremos que

($\star\star$) Se $I \subseteq R$ é um ideal, então R/I é finito.

Como R/I é finito, possui um ideal maximal, e isso corresponde a um ideal maximal contendo I. Para provar (b), basta provar que $|R/I| > |R/J|$. Mas isso só não acontece se $I = J$, ou seja, se

$I = \mathfrak{p}I$. Então $I = \mathfrak{p}^n I$ para todo n, e teríamos $I \subseteq \mathfrak{p}^n$ para todo n, e em particular $|R/I| \geq |R/\mathfrak{p}^n|$ para todo n. Mas então

$$|R/\mathfrak{p}| \leq |R/\mathfrak{p}^2| \leq \cdots \leq |R/I|,$$

então existe n com $|R/\mathfrak{p}^n| = |R/\mathfrak{p}^{n+1}|$, e portanto $\mathfrak{p}^n = \mathfrak{p}^{n+1}$. Mas multiplicando por $\mathfrak{p}^{-1}$ repetidamente, obteríamos $\mathfrak{p} = R$, um absurdo. Isso prova o seguinte:

Teorema 2.17. *Seja $R \subseteq K$ on anél dentro de um corpo satisfazendo $(\star)$ e $(\star\star)$. Então R tem fatoração única em ideais maximais.*

Nota 2.18. Pode se provar que um anél com fatoração única necessariamente satisfaz $(\star)$, mas não necessariamente $(\star\star)$.

Algumas consequências (esperadas):

- Todo ideal primo é maximal: Se I é primo e $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ é sua fatoração, então $\mathfrak{p}_i \subseteq I$ para algum i pois I é primo, mas então $\mathfrak{p}_i = I$ pois $\mathfrak{p}_i$ é maximal.
- $I \subseteq J \iff J \mid I$. Se $J = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ com $\mathfrak{p}_i$ não-necessariamente distintos, enão $J_0 := I\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1} \subseteq R$ é um ideal, e $I = JJ_0$.
- $I + J = \prod_{\mathfrak{p}} \mathfrak{p}^{\min(\mu_{\mathfrak{p}}(I), \mu_{\mathfrak{p}}(J))}$: Segue do anterior pois é o menor ideal que contém I e J.
- $I \cap J = \prod_{\mathfrak{p}} \mathfrak{p}^{\max(\mu_{\mathfrak{p}}(I), \mu_{\mathfrak{p}}(J))}$: Segue como acima pois é o maior ideal contido em I e J.
- Quando temos também $(\star\star)$, temos que $N(I) := |R/I|$ é totalmente multiplicativo. Ela é multiplicativa por Chinês dos Restos. Então basta ver que $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$. Seja $\pi \in \mathfrak{p} - \mathfrak{p}^2$. Então $(\pi) + \mathfrak{p}^n = \mathfrak{p}$. Agora considere o mapa de grupos $R/\mathfrak{p}^n \xrightarrow{\cdot\pi} \mathfrak{p}/\mathfrak{p}^{n+1}$. Esse mapa é sobrejetor pois sua imagem é $(\pi) + \mathfrak{p}^n = \mathfrak{p}$. Ele é injetor pois se $\mathfrak{p}^{n+1} \mid (\pi\alpha)$, então $\mathfrak{p}^n \mid (\alpha)$. Finalmente, note que $|R/\mathfrak{p}^{n+1}| = |R/\mathfrak{p}| \cdot |\mathfrak{p}/\mathfrak{p}^{n+1}|$.

2.4. **Números algébricos e inteiros algébricos.** Vamos definir os anéis que estaremos interessados, e provar que eles satisfazem as propriedades $(\star)$ e $(\star\star)$ na próxima aula.

Primeiro lembramos das seguintes definições:

Definição 2.19. Dizemos que $\alpha \in \mathbb{C}$ é *algébrico* se existe $f \in \mathbb{Z}[x]$ não-zero com $f(\alpha) = 0$. Dizemos que α é *inteiro algébrico* se tal f pode ser escolhido mônico. Denotamos por $\overline{\mathbb{Q}}$ e $\mathcal{O}$ os números algébricos e os inteiros algébricos.

Proposição 2.20. *$\overline{\mathbb{Q}}$ é um corpo e $\mathcal{O}$ é um anel.*

Demonstração. Se $f, g \in \mathbb{Z}[x]$ são irredutíveis e diferentes de x com raízes $\alpha_1, \dots, \alpha_n$ e $\beta_1, \dots, \beta_m$, então considere

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i-\beta_j) = \prod_{i=1}^{n} g(x-\alpha_i), \quad \prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i\beta_j) = \prod_{i=1}^{n} \alpha_i^{\deg g} g(x/\alpha_i).$$

Seus coeficientes são inteiros pois são polinômios simétricos nos α_i. Isso prova que $\overline{\mathbb{Q}}$ e $\mathcal{O}$ são anéis.

Para ver que $\overline{\mathbb{Q}}$ é um corpo, se $\alpha \neq 0$ é algébrico com polinômio minimal f com raízes $\alpha, \beta_1, \dots, \beta_n$, então $\alpha^{-1} = \beta_1 \cdots \beta_n \cdot f(0)(-1)^{\deg f}$. □

Se α é algébrico, podemos considerar o corpo $\mathbb{Q}[\alpha] = \mathbb{Q} + \mathbb{Q}\alpha + \cdots$. Como α é algébrico, essa soma é finita, e $\mathbb{Q}[\alpha]/\mathbb{Q}$ é uma extensão finita. De fato, toda extensão finita é dessa forma.

Teorema 2.21 (Elemento primitivo)**.** *Seja L/K uma extensão finita de corpos de característica 0. Então existe $\alpha \in L$ tal que $L = K[\alpha]$.*

Definição 2.22. Um *corpo numérico* é uma extensão finita de corpos $K/\mathbb{Q}$. Seu *anél de inteiros* é $\mathcal{O}_K := K \cap \mathcal{O}$.

Exemplo 2.23. Seja $K = \mathbb{Q}[\sqrt{d}]$. Podemos assumir que $d \neq 1$ é livre de quadrados. Vamos calcular $\mathcal{O}_K$. Para $\alpha + \beta\sqrt{d}$ ser inteiro algébrico, temos que ter $a, b \in \mathbb{Z}$ tal que

$$(\alpha + \beta\sqrt{d})^2 - a(\alpha + \beta\sqrt{d}) + b = 0.$$

Ou seja, $\alpha^2 + d\beta^2 - a\alpha + b = 0$ e $2\alpha\beta - a\beta = 0$. Se $\beta = 0$, então temos que ter $\alpha \in \mathbb{Z}$. Se $\beta \neq 0$, então $a = 2\alpha$, e daí $b = \alpha^2 - d\beta^2$, ou seja, $\beta^2 = \frac{a^2-4b}{4d}$. Como d é livre de quadrados, temos que ter $2\beta \in \mathbb{Z}$. Então $4b = (2\alpha)^2 - d(2\beta)^2$. Se $d \not\equiv 1 \mod 4$, temos que ter que $2\alpha, 2\beta$ são pares e portanto $\alpha, \beta \in \mathbb{Z}$. Se $d \equiv 1 \mod 4$, temos que ter $2\alpha \equiv 2\beta \mod 2$. Portanto

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{se } d \not\equiv 1 \mod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{se } d \equiv 1 \mod 4. \end{cases}$$

Exemplo 2.24. Seja $K = \mathbb{Q}[2^{1/3}]$. Pode-se provar que $\mathcal{O}_K = \mathbb{Z}[2^{1/3}]$.

Nota 2.25. Não é necessariamente verdade que existe $\alpha \in \mathcal{O}_K$ com $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Nota 2.26. Por que considerar $\mathcal{O}_K$ e não outro anél dentro de K? Suponha que $R \subseteq K$ é outro anel tal que todo elemento de K é uma fração em R. Assuma que R tem fatoração única. Seja $f(x) \in \mathbb{Z}[x]$ mônico com raiz $x/y \in K$ com $x, y \in R$ sem fatores em comum. O teorema da

raiz racional (que funciona pois R tem fatoração única!) nos diz que y é uma unidade. Portanto $\mathcal{O}_K = K \cap \mathcal{O} \subseteq R$. Também pode-se provar que se R tem fatoração única em ideais, então $\mathcal{O}_K \subseteq R$. Então $\mathcal{O}_K$ é o menor anél que podemos tentar imaginar ter fatoração única.

Próxima aula iremos provar que $\mathcal{O}_K \subseteq K$ satisfaz as condições $(\star)$ e $(\star\star)$. Pelo o que vimos, isso implica que $\mathcal{O}_K$ tem fatoração única em ideais. Também vamos ver como se fatora ideais na prática.

2.5. **Equações Diofantinas.** O que ganhamos com fatoração em ideais? A priori, pode parecer que não ajuda muito, pois estamos interessados nas soluções de equações em si. Existem dois resultados complementares que remediam isso:

Teorema 2.27 (Teorema das unidades de Dirichlet)**.** *Seja $K = \mathbb{Q}[\alpha]$ um corpo numérico com α tendo polinômio minimal f. Seja $\mathcal{O}_K$ seu anél de inteiros. Então ${\mathcal{O}_K}^\times \simeq \mu(K) \times \mathbb{Z}^{r+s-1}$ onde f tem r raízes reais e $2s$ raízes complexas, e onde $\mu(K)$ são as raízes da unidade dentro de K.*

Teorema 2.28 (Grupo de classes é finito)**.** *Se $\mathcal{O}_K$ é um anél de inteiros, existe uma coleção finita de ideais $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ tal que para qualquer outro ideal I, exatamente um dos ideais $\mathfrak{a}_i I$ é principal.*

Iremos comentar mais sobre esses resultados depois. Basicamente podemos ir e voltar no seguinte diagrama.

$$\text{elementos de } \mathcal{O}_K \xleftrightarrow{{\mathcal{O}_K}^\times} \text{ ideais principais } \xleftrightarrow{\text{grupo de classes}} \text{ ideais.}$$

Exemplo 2.29. Considere $2y^3 = x^2 + 5$. Vamos trabalhar em $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Lembre-se que $\mathcal{O}_K$ não tem fatoração única! O que os dois teoremas acima nos dizem nesse caso é que ${\mathcal{O}_K}^\times = \{\pm 1\}$ e que $\mathfrak{a}_1 = (1), \mathfrak{a}_2 = (2, 1 + \sqrt{-5})$. Fatorando,

$$2y^3 = (x + \sqrt{-5})(x - \sqrt{5}).$$

Agora $\text{mdc}((x + \sqrt{-5}), (x - \sqrt{-5})) = (x + \sqrt{-5}) + (x - \sqrt{-5}) = (2\sqrt{-5}, x + \sqrt{-5}) \mid (2\sqrt{-5})$. Note que $(\sqrt{-5})$ é um ideal primo, pois $\mathcal{O}_K/(\sqrt{-5}) = \mathbb{Z}/5\mathbb{Z}$ é um corpo. Se $(\sqrt{-5}) \mid (x + \sqrt{-5})$, isso implicaria que $\sqrt{-5} \mid x$, e portanto que $5 \mid x$. Podemos ver que isso não é possível. Logo

$$\text{mdc}((x + \sqrt{-5}), (x - \sqrt{-5})) \mid (2) = (2, 1 + \sqrt{-5})^2.$$

Mas $(2) \nmid (x + \sqrt{-5})$, e $(2, 1 + \sqrt{-5}) \mid (x + \sqrt{-5})$ pois podemos ver que x é ímpar. Portanto temos que ter que $(x + \sqrt{-5}) = \mathfrak{a}_2 I^3$ para um ideal I. Se I fosse principal, então I^3 e $\mathfrak{a}_2 I^3$ seriam

principais, mas isso não pode ser verdade pelo teorema acima. Portanto I não é principal, mas $\mathfrak{a}_2 I$ é. Multiplicando por $\mathfrak{a}_2^2$ dos dois lados, temos $(2x+2\sqrt{-5}) = (\mathfrak{a}_2 I)^3$. Portanto, existe um sinal $\pm \in {\mathcal{O}_K}^\times$ e inteiros a, b tal que $2x + 2\sqrt{-5} = \pm(a + b\sqrt{-5})^3$. Trocando a, b por $\pm a, \pm b$, podemos assumir que $\pm = +$. Então

$$2x = a^3 - 15ab^2, \quad 2 = 3a^2b - 5b^3.$$

A segunda equação só tem soluções $(a, b) = (\pm 1, -1)$, e portanto $x = \pm 7$. Portanto as soluções são $(x, y) = (\pm 7, 3)$.

Exercícios

Dicas estão no rodapé.

(1) Em classe eu assumi implicitamente que se α é algébrico, então $K = \mathbb{Q}[\alpha]$ é um corpo. Prove isso.[7]

(2) (Teorema Chinês dos Restos) Seja R um anél e I, J ideais com $I + J = R$. Prove que $IJ = I \cap J$, e que

$$R/IJ \xrightarrow{\sim} R/I \times R/J.$$

(3) Resolva a equação Diofantina $y^3 = x^2 + 13$ usando $K = \mathbb{Q}[\sqrt{-13}]$. Use que ${\mathcal{O}_K}^\times = \pm 1$ e que para qualquer ideal I, exatamente um dentre I ou $(2, 1 + \sqrt{-13})I$ é principal.

(4) Seja R um anél com fatoração única em ideais como discutido em aula. Seja I um ideal que não é 0 e não é R, e escolha $a \in I$. Prove que existe $b \in I$ tal que $I = (a, b)$. Em particular, todo ideal é gerado por dois elementos.[8]

(5) Prove o teorema do elemento primitivo. Vamos assumir a seguinte tecnicalidade sobre $K \subseteq \mathbb{C}$: todo polinômio irredutível em K (ou seja, elementos irredutíveis de $K[x]$) não tem raiz repetida.

   (a) Seja L/K uma extensão finita. Prove que existem $\alpha_1, \ldots, \alpha_n \in L$ tal que $L = K[\alpha_1, \ldots, \alpha_n]$.

   (b) Reduza a prova do teorema para o caso $L = K[\alpha, \beta]$.

   (c) Considere $\gamma = \alpha + r\beta$ para racionais r. Sejam $f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$ e $(x - \beta_1) \cdots (x - \beta_m) \in K[x]$ os polinômios minimais de $\alpha = \alpha_1$ e $\beta = \beta_1$ sobre K. Prove que se $\gamma_r \neq \alpha_i + r\beta_j \neq 0$ para todo par $(i, j) \neq (1, 1)$, então $L = K[\gamma_r]$.[9]

   (d) Conclua que existe $L = \gamma$ com $L = K[\gamma]$.

(6) Esse exercício vai provar que existe um único corpo finito de cardinalidade p^n para toda potência de primo p^n.

   (a) Seja F um corpo finito. Prove que existe $\alpha \in F$ tal que $F = \mathbb{F}_p[\alpha]$. Conclua que existe $f(x) \in \mathbb{F}_p[x]$ irredutível tal que $F \simeq \mathbb{F}_p[x]/(f(x))$.[10]

---

[7] seja $\beta \in K$. Como K é um espaço vetorial de dimensão finita sobre $\mathbb{Q}$, os elementos $1, \beta, \beta^2, \ldots$ são linearmente dependentes sobre $\mathbb{Q}$.

[8] considere $R' = R/(a)$ e use o Teorema Chinês dos restos.

[9] considere $h(x) = g(\gamma_r - rx)$. Seja $L_0 = K[\gamma_r]$. Então $L = L_0[\beta]$, e considere o polinômio minimal $f_\beta(x) \in L_0[x]$ de β em L_0. Prove que $f_\beta \mid h$, e que $f_\beta \mid g$. Conclua que f_β tem grau 1.

[10] o que sabemos sobre $F^\times$?

(b) Seja $f \in \mathbb{F}_p[x]$ um polinômio mônico de grau d. Prove que $f(x) \mid x^{p^d} - x$ mas $f(x) \nmid x^{p^{d-1}} - x$ em $\mathbb{F}_p[x]$.[11]

(c) Seja M_d o conjunto de polinômios mônicos irredutíveis de grau d em $\mathbb{F}_p[x]$. Prove que $\prod_{d \leq n} \prod_{f \in M_d} f(x) = x^{p^n} - x$. Conclua que $\sum_{d \leq n} d \cdot |N_d| = p^n$. Conclua que $N_d \neq 0$ para todo d, e portanto que existem um corpo finito de cardinalidade p^d.

(d) Seja F um corpo finito de ordem p^n. Seja N_d o conjunto de elementos de F cujo polinômio minimal sobre $\mathbb{F}_p$ tem grau d. Prove que $|N_d| \leq d \cdot |M_d|$. Conclua que isso é uma igualdade para todo $d \leq n$.

(e) Seja $F' = \mathbb{F}_p[x]/(g(x))$ outro corpo finito de cardinalidade p^n. Do item anterior, conclua que existe $\alpha \in F$ com polinômio minimal $g(x)$. Conclua que $\mathbb{F}_p[x]/(g(x)) \to F$ dado por $x \mapsto \alpha$ é um isomorfismo, e portanto que $F \simeq F'$.

[11] seja $F = \mathbb{F}_p[x]/(f)$. É suficiente provar as duas partes sobre $F[x]$.

3. 20 de Março

3.1. **Prova de fatoração única.** Seja K um corpo numérico e $\mathcal{O}_K$ seu anél de inteiros. Lembre-se que queremos provar

($\star$) Se $\mathfrak{p} \subseteq R$ é um ideal maximal, existe um conjunto $\mathfrak{p}^{-1} \subseteq K$ tal que $\mathfrak{p}\mathfrak{p}^{-1} = R$

e

($\star\star$) Se $I \subseteq R$ é um ideal, então R/I é finito.

Para $K = \mathbb{Q}[\sqrt{d}]$, lembre-se que temos a noção de uma norma $N(a + b\sqrt{d}) = a^2 - db^2$. Vamos começar generalizando isso.

Definição 3.1. Para $\alpha \in K$, veja K como um espaço vetorial sobre $\mathbb{Q}$ e considere a matrix $M_\alpha \colon K \to K$ dada por multiplicação por α. Chamamos $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}(M_\alpha)$ o *traço* de α, e $\mathrm{Nm}_{K/\mathbb{Q}}(\alpha) = \det(M_\alpha)$ a *norma* de α.

Proposição 3.2. *Para um corpo numérico K, $\mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{Z}$ e $\mathrm{Nm}_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{Z}$.*

Demonstração. Seja $\alpha \in \mathcal{O}_K$. Considere $K' = \mathbb{Q}[\alpha]$. Se $x^m + \cdots a_0$ é o polinômio minimal de α, então escolhendo a base $1, \alpha, \ldots, \alpha^{m-1}$, a matrix de multiplicação de α em K' é

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{m-1} \end{pmatrix}.$$

Então M_α é n/m cópias de A, e portanto $\mathrm{Tr}(M_\alpha) = -\frac{n}{m} \cdot a_{m-1}$ e $\det(M_\alpha) = (-1)^n a_0^{n/m}$. □

Com isso, vamos provar o seguinte

Lema 3.3. *Seja K um corpo numérico de dimensão n. Considere um ideal $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$. Então existem $\alpha_1, \ldots, \alpha_n$ tal que $\mathfrak{a} = \alpha_1\mathbb{Z} \oplus \cdots \alpha_n\mathbb{Z}$.*

Demonstração. Seja $x_1, \ldots, x_n$ uma base de K sobre $\mathbb{Q}$. Podemos assumir que $x_i \in \mathcal{O}_K$. Considere a matrix $(\mathrm{Tr}(x_i x_j))_{(i,j)}$. Vamos provar que ela é não-singular. Se fosse, teríamos uma combinação

linear de linhas que é 0, ou seja, existiria $k \in K$ tal que $\mathrm{Tr}(kx_j) = 0$ para todo j. Mas daí $n = \mathrm{Tr}(kk^{-1}) = 0$, um absurdo.

Então existe $y_1, \dots, y_n$ com $\mathrm{Tr}(x_i y_j) = \delta_i^j$. Isto é, se $z = z_1 x_1 + \cdots z_n x_n$, então $z_i = \mathrm{Tr}(x_i z)$. Seja N tal que $Ny_i \in \mathcal{O}_K$ para todo i. Então

$$x_1\mathbb{Z} \oplus \cdots x_n\mathbb{Z} \subseteq \mathcal{O}_K \subseteq \frac{1}{N} x_1\mathbb{Z} \oplus \cdots x_n\mathbb{Z}.$$

Seja $p_i \colon \mathfrak{a} \to \mathbb{Z}$ dado por $p_i(z) = Nz_i$. Agora seja $\varphi_1 \colon \mathfrak{a} \to \mathbb{Z}$ dado por $z \mapsto p_1(z)$. Então $\varphi_1(\mathfrak{a})$ é um ideal, e podemos achar α_1 com $\varphi_1(\alpha_1)$ que gere ele. Então dado $z \in \mathfrak{a}$ existe um único $c_1 = c_1(z)$ tal que $\varphi_1(z - c_1(z)\alpha_1) = 0$. Então seja $\varphi_2 \colon \mathfrak{a} \to \mathbb{Z}$ dado por $z \mapsto p_2(x - c_1(x)\alpha_1)$. Então $\varphi_2(\mathfrak{a})$ é um ideal, e seja α_2 tal que $\varphi_2(\alpha_2)$ gere ele. Podemos continuar assim até α_n. □

Corolário 3.4. *Seja $0 \neq \mathfrak{a} \subseteq \mathcal{O}_K$ um ideal, e $\alpha \in K$ com $\alpha\mathfrak{a} \subseteq \mathfrak{a}$. Então $\alpha \in \mathcal{O}_K$.*

Demonstração. Seja $\mathfrak{a} = \alpha_1\mathbb{Z} \oplus \cdots \alpha_n\mathbb{Z}$. Escreva M_α nessa base. Essa é uma matrix com entradas inteiras, e temos que $M_\alpha \alpha_i = \alpha\alpha_i$, então $\det(M_\alpha - \alpha I) = 0$. Isso é um polinômio mônico em α com coeficientes inteiros, então $\alpha \in \mathcal{O}_K$. □

Finalmente, vamos concluir a prova de fatoração única.

Teorema 3.5. *$\mathcal{O}_K$ tem fatoração única em ideais maximais.*

Demonstração. Precisamos provar $(\star\star)$ e $(\star)$.

Para $(\star\star)$, seja $\mathfrak{a}$ um ideal e considere $\alpha \in \mathfrak{a}$. Como $(\alpha) \subseteq \mathfrak{a}$, basta provarmos que $\mathcal{O}_K/(\alpha)$ é finito. Escreva $\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \cdots \alpha_n\mathbb{Z}$. Nessa base, M_α tem coeficientes inteiros, e seu determinante é o volume de um domínio fundamental de $\alpha\mathcal{O}_K$. Tal volume é o mesmo que $|\mathcal{O}_K/(\alpha)|$.

Para $(\star)$, considere $\mathfrak{p}$ maximal. Seja

$$\mathfrak{p}^{-1} := \{\alpha \in K \colon \alpha\mathfrak{p} \subseteq \mathcal{O}_K\}.$$

Então $\mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$ é um ideal que contém $\mathfrak{p}$. Como $\mathfrak{p}$ é maximal, basta provarmos que $\mathfrak{p}\mathfrak{p}^{-1}$ não é $\mathfrak{p}$. Mas se isso fosse verdade, então $\alpha\mathfrak{p} \subseteq \mathfrak{p}$ para todo $\alpha \in \mathfrak{p}^{-1}$, e pelo corolário anterior, isso implicaria que $\mathfrak{p}^{-1} = \mathcal{O}_K$. Então basta encontrar $\alpha \in \mathfrak{p}^{-1} \setminus \mathcal{O}_K$. Isso será um exercício. □

3.2. **Como computar ideais primos.** Seja $\mathfrak{p} \subseteq \mathcal{O}_K$ um ideal primo. Como $\mathcal{O}_K/\mathfrak{p}$ é um corpo, temos que ter $p \in \mathfrak{p}$ para algum primo p. Ou seja, $\mathfrak{p} \mid p\mathcal{O}_K$. Isto é, todo ideal primo divide $p\mathcal{O}_K$ para algum primo $p \in \mathbb{Z}$. Então para entender todos os primos de $\mathcal{O}_K$, basta sabermos fatorar todo $p\mathcal{O}_K$.

Lema 3.6. *Seja $\alpha \in \mathcal{O}_K$, e considere $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. Seja N_α o índice $N_\alpha = |\mathcal{O}_K/\mathbb{Z}[\alpha]|$. Seja $f(x) \in \mathbb{Z}[x]$ o polinômio minimal de α e p um primo com $p \nmid N_\alpha$. Então se $f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r} \mod p$ é a fatoração em irredutíveis, então $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ onde $\mathfrak{p}_i = (p, f_i(\alpha))$.*

Demonstração. Escreva $p\mathcal{O}_K = \mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_s^{e_r'}$. Pelo Teorema chinês dos restos, temos

$$\mathcal{O}_K/(p) = \prod_{i=1}^{r} \mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$

Como $p \nmid N_\alpha$, temos que $\mathbb{Z}[\alpha]/(p) = \mathcal{O}_K/(p)$, e portanto, novamente pelo Teorema chinês dos restos,

$$\mathcal{O}_K/(p) = \mathbb{Z}[\alpha]/(p) = \mathbb{Z}[x]/(p, f(x)) = \mathbb{F}_p[x]/(f(x)) = \prod_{i=1}^{r'} \mathbb{F}_p[x]/(f_i(x)^{e_i'})$$

onde $f(x) = f_1(x)^{e_1'} \cdots f_s(x)^{e_s'}$ é a fatoração em irredutíveis.

Comparando as duas expressões, podemos provar que podemos reordenar of f_i de tal modo que $\mathfrak{p}_i^{e_i'} = (p, f_i(\alpha)^{e_i})$. Como $(p, f_i(\alpha)^{e_i})$ é o mdc de (p) e $(f_i(\alpha)^{e_i})$ e como $(p, f_i(\alpha))$ é um ideal máximo, temos que ter $(p, f_i(\alpha)) = \mathfrak{p}_i$ e $(p, f_i(\alpha)^{e_i}) = (p, f_i(\alpha))^{e_i}$, então $e_i = e_i'$. □

Exemplo 3.7. Seja $K = \mathbb{Q}[\sqrt{d}]$ com d livre de quadrados. Considere $\alpha = \sqrt{d}$. Então $N_\alpha = 1$ se $d \not\equiv 1 \mod 4$, e $N_\alpha = 2$ se $d \equiv 1 \mod 4$. De qualquer forma, para fatorar $p\mathcal{O}_K$ com $p > 2$ consideramos $x^2 - d \mod p$. Portanto,

$$p\mathcal{O}_K = \begin{cases} p\mathcal{O}_K & \text{se } \left(\frac{d}{p}\right) = -1, \\ (p, \sqrt{d})^2 & \text{se } \left(\frac{d}{p}\right) = 0, \\ (p, \sqrt{d} - x)(p, \sqrt{d} + x) & \text{se } \left(\frac{d}{p}\right) = 1 \text{ e } x^2 \equiv d \mod p. \end{cases}$$

Exemplo 3.8. Seja ζ_n uma raiz da unidade, e $K = \mathbb{Q}[\zeta_n]$. Pode-se provar que $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. Portanto a fatoração de $p\mathcal{O}_K$ depende da fatoração de $\Phi_n(x) \mod p$. Em particular, $p\mathcal{O}_K$ é primo se e somente se $\Phi_n(x) \mod p$ é irredutível.

Exemplo 3.9. Seja $K = \mathbb{Q}[2^{1/3}]$, com $\mathcal{O}_K = \mathbb{Z}[2^{1/3}]$. Então $p\mathcal{O}_K$ é primo se e somente se $x^3 - 2 \mod p$ é irredutível, ou seja, se e somente se 2 não é um resíduo cúbico módulo p.

Corolário 3.10. *Existem somente finitos primos p tal que $p\mathcal{O}_K$ não seja livre de quadrados. Chamamos tais finitos p de* ramificados.

De fato, se $\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \cdots \alpha_n\mathbb{Z}$ e $D_K := \det((\mathrm{Tr}(\alpha_i\alpha_j))_{(i,j)})$, então p é ramificado se e somente se $p \mid D_K$. Tal D_K é o *discriminante* de K. Se $\mathcal{O}_K = \mathbb{Z}[\alpha]$, então D_K é o discriminante do polinômio minimal de α.

3.3. **Grupo de classes.** Como vimos anteriormente, iremos provar que ideais não são muito diferentes de ideais principais em $\mathcal{O}_K$. Para isso, vamos dizer que dois ideais $\mathfrak{a}, \mathfrak{b}$ são equivalentes se existe $\alpha, \beta \in \mathcal{O}_K$ tal que $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, e denotamos $\mathfrak{a} \sim \mathfrak{b}$.

Definição 3.11. Para um corpo numérico K, seu *grupo de classes* $\mathrm{Cl}(K)$ é um grupo cujos elementos são classes de equivalência de ideais de $\mathcal{O}_K$ como acima, e cuja multiplicação é a multiplicação de ideais. Denotamos por $[\mathfrak{a}]$ a classe do ideal $\mathfrak{a}$.

Note que de fato ele forma um grupo pois se $\alpha \in \mathfrak{a}$, então $\mathfrak{a} \mid (\alpha)$, portanto $(\alpha) = \mathfrak{a}\mathfrak{b}$ e então $\mathfrak{a}\mathfrak{b} = (\alpha) \sim (1)$.

Um dos teoremas mais importantes em teoria algébrica dos números é o seguinte.

Teorema 3.12. *Para qualquer corpo numérico K, temos que $\mathrm{Cl}(K)$ é finito.*

Ele segue do seguinte lema:

Lema 3.13. *Existe uma constante M_K tal que para todo ideal $\mathfrak{a}$, existe $0 \neq \alpha \in \mathfrak{a}$ com*

$$|\mathrm{Nm}(\alpha)| \leq M_K \cdot |\mathcal{O}_K/\mathfrak{a}|.$$

De fato, se $\alpha \in \mathfrak{a}$ satisfaz a desigualdade acima, então $(\alpha) = \mathfrak{a}\mathfrak{a}_0$ para algum $\mathfrak{a}_0$, e $N(\alpha) = N(\mathfrak{a})N(\mathfrak{a}_0)$, e então $N(\mathfrak{a}_0) \leq M_K$. Como $[\mathfrak{a}][\mathfrak{a}_0] = 1$, isso prova que todo elemento de $\mathrm{Cl}(K)$ é $[\mathfrak{a}_0]$ para algum $\mathfrak{a}_0$ com $N(\mathfrak{a}_0) \leq M_K$, e existem somente finitos tais ideais.

Antes de ver a ideia da prova, vamos ver como podemos provar a finitude para $K = \mathbb{Q}[\sqrt{d}]$. Seja p um primo. Se $p \nmid 2d$, assuma que $p\mathcal{O}_K$ não é primo. Então $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$. Por lema de Thue, podemos escrever $p \mid a^2 - db^2$ com $|a|, |b| \leq \lceil\sqrt{p}\rceil$. Portanto $a^2 - db^2 = kp$ para $k < (1 + |d|)(\lceil\sqrt{p}\rceil)^2/p$. Em particular, $k < N_k$ para uma constante N_k. Agora note que $a + b\sqrt{d} \in \mathfrak{p}_1$ tem norma no máximo $N_K|\mathcal{O}_K/\mathfrak{p}_1|$. Ou seja, o argumento acima prova que o corpo de classes é gerado por ideais de norma no máximo N_K.

Lema 3.14 (Cota de Minkowski)**.** *Seja $K = \mathbb{Q}[\alpha]$ e f o polinômio minimal de α. Se f tem $2s$ raízes complexas e se $n = \dim_{\mathbb{Q}} K$, então o lema acima é verdade com*

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|D_K|}.$$

Demonstração. Sejam $\alpha_1, \dots, \alpha_r$ as raízes reais de f e $\alpha_{r+1}, \overline{\alpha_{r+1}}, \dots, \alpha_{r+s}, \overline{\alpha_{r+s}}$ as raízes complexas. Considere o mapa $\phi\colon K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$ onde $\alpha \mapsto (\alpha_1, \dots, \alpha_n)$. O ponto chave da prova é que $\phi(\mathcal{O}_K)$ é um lattice.

Agora a ideia é usar o teorema de Minkowski: Se $\Lambda \subseteq \mathbb{R}^n$ é um lattice cuja região fundamental tem volume $\mathrm{vol}(\Lambda)$, e se S é uma região convexa e simétrica com volume maior que $2^n \mathrm{vol}(\Lambda)$, então S possui um ponto de Λ diferente da origem.

Podemos provar que $\mathrm{Nm}(\beta) = \prod_{i=1}^r \phi(\beta)_i \cdot \prod_{i=r+1}^{r+s} |\phi(\beta)_i|^2$. Considerando

$$S_c = \left\{ x \in \mathbb{R}^r \times \mathbb{C}^s \colon \sum_{i=1}^r |x_i| + 2 \sum_{i=r+1}^{r+s} |x_i| \leq c \right\},$$

temos por MA-MG que se $\phi(\beta) \in S_x$, então $|\mathrm{Nm}(\beta)| \leq (c/n)^n$. Temos que $\mathrm{vol}(\phi(\mathfrak{a})) = N(\mathfrak{a})\mathrm{vol}(\phi(\mathcal{O}_K))$, e pode-se computar que $\mathrm{vol}(\phi(\mathcal{O}_K)) = 2^{-s}\sqrt{|D_K|}$.

Então se $\mathrm{vol}(S_c) \geq 2^n \sqrt{|D_K|} N(\mathfrak{a})$, temos um $0 \neq \beta \in \mathfrak{a}$ com $|\mathrm{Nm}(\beta)| \leq (c/n)^n$. Como $\mathrm{vol}(S_c) = c^n \mathrm{vol}(S_1)$, podemos escolher $c^n = \frac{2^{n-s}\sqrt{|D_K|}N(\mathfrak{a})}{\mathrm{vol}(S_1)}$, e então o lema é verdade com

$$M_K = \frac{1}{\mathrm{vol}(S_1)} \frac{2^{r+s}}{n^n} \sqrt{|D_K|}.$$

Então basta computar que

$$\mathrm{vol}(S_1) = \frac{2^r(\pi/2)^s}{n!},$$

e isso pode ser feito por indução. Seja $S_c(r,s)$ o volume de S_c com os parâmetros r, s. Então se $r \geq 1$,

$$S_c(r,s) = \int_{-c}^{c} S_{c-|x_1|}(r-1,s)\ \mathrm{d}x_1 = 2\int_0^c (c-x_1)^{n-1} S_1(r-1,s)\ \mathrm{d}x_1 = 2S_1(r-1,s)\frac{c^n}{n}$$

e de maneira parecida, se $D(R)$ é o disco de raio R, então

$$\begin{aligned} S_c(r,s) &= \int_{D(c/2)} S_{c-2|x_{r+s}|}(r,s-1)\ \mathrm{d}x_{r+s} = S_1(r,s-1)\int_{D(c/2)} (c-2|x_{r+s}|)^{n-2}\ \mathrm{d}x_{r+s} \\ &= S_1(r,s-1)\int_o^{c/2} 2\pi(c-2R)^{n-2}R\ \mathrm{d}R = \frac{\pi}{2} S_1(r,s-1)\int_0^c (c-R)^{n-2}R\ \mathrm{d}R \end{aligned}$$

e note que $(c-R)^{n-2}R = c(c-R)^{n-2} - (c-R)^{n-1}$, portanto temos

$$S_c(r,s) = \frac{\pi}{2} S_1(r,s-1)\left(c\frac{c^{n-1}}{n-1} - \frac{c^n}{n}\right) = \frac{\pi}{2} S_1(r,s-1)\frac{c^n}{n(n-1)}. \qquad \square$$

Exemplo 3.15. Temos os seguintes examplos de grupos de classe.

- Se $K = \mathbb{Q}[2^{1/3}]$, temos $n = 3, r = 1, s = 1$ e $D_K = -2^2 3^3$, e então $M_K < 3$. Mas $2\mathcal{O}_K = (2^{1/3})^3$, e então $\mathrm{Cl}(K) = 1$.
- Se $K = \mathbb{Q}[\zeta_5]$, então $n = 4, r = 0, s = 2$ e $D_k = 5^3$, e então $M_K < 2$. Portanto $\mathrm{Cl}(K) = 1$.
- Se $K = \mathbb{Q}[\sqrt{82}]$, então $n = 2, r = 2, s = 0$ e $D_K = 4 \cdot 82$, e então $M_K < 10$. Portanto precisamos fatorar $p\mathcal{O}_K$ com $p < 10$. Isso é primo para $p = 5$ e $p = 7$, e temos

$$2\mathcal{O}_K = (2, \sqrt{82})^2, \quad 3\mathcal{O}_K = (3, \sqrt{82} - 1)(3, \sqrt{82} + 1).$$

  Então se $\mathfrak{p}_2 = (2, \sqrt{82})$ e $\mathfrak{p}_3 = (3, \sqrt{82} - 1)$, temos que $\mathrm{Cl}(K)$ é gerado por $[\mathfrak{p}_2]$ e $[\mathfrak{p}_3]$. Agora temos que

$$\mathrm{Nm}(10 + \sqrt{82}) = 100 - 82 = 18 = 2 \cdot 3^2,$$

  e como $3 \nmid 10 + \sqrt{82}$, temos que ter $(10 + \sqrt{82}) = \mathfrak{p}_2\mathfrak{p}_3^2$ ou $(10 + \sqrt{82}) = \mathfrak{p}_2\overline{\mathfrak{p}_3}^2$. De qualquer forma, isso implica que $[\mathfrak{p}_2] = [\mathfrak{p}_3]^2$. Então $\mathrm{Cl}(K)$ é gerado por $[\mathfrak{p}_3]$. Como $[\mathfrak{p}_3]^4 = [\mathfrak{p}_2]^2 = 1$ e como $[\mathfrak{p}_3]^2 = [\mathfrak{p}_2] \neq 1$, temos que $\mathrm{Cl}(K) \simeq \mathbb{Z}/4\mathbb{Z}$.

3.4. **Unidades.** Próxima aula, iremos provar o seguinte teorema.

Teorema 3.16 (Teorema das unidades de Dirichlet)**.** *Seja K um corpo numérico, e denote por μ_K o grupo das raízes da unidade dentro de K. Então ${\mathcal{O}_K}^\times \simeq \mu_K \times \mathbb{Z}^{r+s-1}$.*

Podemos pensar nisso como uma generalização da teoria de equações de Pell: se $K = \mathbb{Q}[\sqrt{d}]$ com d livre de quadrados, então se $d \not\equiv 1 \mod 4$, o grupo ${\mathcal{O}_K}^\times$ é o grupo de soluções da equação de Pell

$$x^2 - dy^2 = \pm 1.$$

Se $d \equiv 1 \mod 4$, o grupo ${\mathcal{O}_K}^\times$ também inclui as soluções de $x^2 - dy^2 \mid 4$. O fato de termos soluções fundamentais corresponde ao fator de $\mathbb{Z}^{r+s-1} = \mathbb{Z}$ no teorema.

Com isso, completaremos o diagrama

$$\text{elementos de } \mathcal{O}_K \xleftarrow{{\mathcal{O}_K}^\times} \text{ ideais principais } \xleftarrow{\text{grupo de classes}} \text{ ideais.}$$

Exercícios

Dicas estão no rodapé.

(1) Complete a prova de fatoração única em ideais. Prove que se $\mathfrak{p}$ é maximal, então existe $\alpha \in \mathfrak{p}^{-1} \setminus \mathcal{O}_K$:
   (a) Use $(\star\star)$ para provar que I é primo se e somente se é maximal.[12]
   (b) Seja $\beta \in \mathcal{O}_K$. Prove por indução em $|\mathcal{O}_K/(\beta)|$ que (β) contém um produto finito de ideais primos.
   (c) Seja $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (\beta)$ com r mínimo (se soubéssemos fatoração, isso seria uma igualdade). Prove que $\mathfrak{p} = \mathfrak{p}_i$ para algum i.
   (d) No item acima, assuma que $\mathfrak{p} = \mathfrak{p}_1$ sem perda de generalidade. Escolha $\beta_0 \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ com $\beta_0 \notin (\beta)$ e prove que $\beta_0/\beta \in \mathfrak{p}^{-1} \setminus \mathcal{O}_K$.

(2) Seja $K = \mathbb{Q}[\sqrt{-d}]$ com $d > 0$ livre de quadrados. Se d não é primo, prove que $\mathrm{Cl}(K) \neq 1$ fatorando algum primo $p \mid d$. Se d for primo mas não é da forma $4q - 1$ para um primo q, então prove que $\mathrm{Cl}(K) \neq 1$ fatorando 2 ou $(d+1)/4$.

(3) Use o problema anterior para achar todos os $0 < d \leq 200$ livres de quadrado tal que $\mathrm{Cl}(\mathbb{Q}[\sqrt{-d}]) = 1$. Pode-se provar que não existe nenhum tal d com $d > 200$, mas isso é bem difícil.

(4) Seja α tal que $\alpha^3 - 3\alpha + 1 = 0$, e considere $K = \mathbb{Q}[\alpha]$. Prove que se p é um primo, então existe a com $p \mid a^3 - 3a + 1$ se e somente se existe $\beta \in \mathcal{O}_K$ com $\mathrm{Nm}(\beta) = p$. E possível fazer uma conta explícita para provar que $\mathrm{Nm}(\beta)$ é sempre ou múltipla de 3 ou $\equiv \pm 1 \mod 9$, mas vamos provar isso próxima aula de uma maneira mais simples.[13]

(5) Considere $K = \mathbb{Q}[\zeta]$ com $\zeta = e^{2\pi i/p}$ e $p > 3$. Temos que $\mathcal{O}_K = \mathbb{Z}[\zeta]$. Suponha que $p \nmid \#\mathrm{Cl}(K)$. Vamos provar que $z^p = x^p - y^p$ não tem solução com $p \nmid xyz$ e $\mathrm{mdc}(x, y, z) = 1$. (Esse é conhecido como o caso 1 de Fermat, e um argumento parecido mas mais difícil resolve o caso 2, que é se $p \mid z$)
   (a) Prove que podemos assumir $p \nmid x + y$.
   (b) Fatore a equação em $\mathcal{O}_K$ e prove que $(x - \zeta y) = \mathfrak{a}^p$ para algum $\mathfrak{a} \subseteq \mathcal{O}_K$.
   (c) Use que $p \nmid \#\mathrm{Cl}(K)$ para concluir que $\mathfrak{a}$ é principal, digamos $\mathfrak{a} = (\alpha)$. Conclue que $x - \zeta y = u\alpha^p$ para algum $u \in {\mathcal{O}_K}^{\times}$.

[12] prove que todo domínio finito R é um corpo, usando gira-gira: se $\alpha \in R$ não é 0, considere a multiplicação por α e use gira-gira.
[13] Combine o fato de que $\mathrm{Cl}(K) = 1$ com o algoritmo de fatoração.

(d) Prove que $\frac{u}{\overline{u}} = \pm\zeta^b$ para algum $1 \leq b \leq p$.[14]

(e) Prove que existe $a \in \mathbb{Z}$ com $\alpha^p \equiv a \mod p\mathcal{O}_K$ e conclua que $x - \zeta y \mp \zeta^b(x - \zeta^{-1}y) \in p\mathcal{O}_K$.

(f) Use que $p \geq 5$ para provar que isso implicaria que $p \mid xyz(x + y)$.

[14]Use o teorema das unidades de Dirichlet tanto para K quanto para $\mathbb{Q}[\zeta + \zeta^{-1}]$.

4. 27 de Março

4.1. **Unidades.** Seja K um corpo numérico. Lembre-se que se $K = \mathbb{Q}[\alpha]$ e f é o polinômio minimal de α, denotamos por r a quantidade de raízes reais de f, e $2s$ a quantidade de raízes complexas.

Primeiro vamos ver como achar ${\mathcal{O}_K}^\times$ no caso que K é quadrático. Se $K = \mathbb{Q}[\sqrt{d}]$ com livre de quadrados, então $a+b\sqrt{d} \in \mathcal{O}_K$ é uma unidade se e somente se sua norma é uma unidade, ou seja, se e somente se

$$a^2 - db^2 = \pm 1.$$

Lembre-se que a, b podem ter um denominador de 2 se $d \equiv 1 \mod 4$. Se $d > 0$, isso é uma equação de Pell, e a teoria de Pell implica que

$${\mathcal{O}_K}^\times \simeq \{\pm 1\} \times \mathbb{Z},$$

where the $\mathbb{Z}$ component correspond to powers of a certain minimal solution of a Pell equation.

Se $d < 0$, então $a^2 - db^2 = \pm 1$ tem somente finitas soluções: se $d = -1$, são $\pm 1, \pm i$, se $d = -3$ são $\pm 1, \pm\omega, \pm\omega^2$ e se $d < -3$, são somente ± 1. Em todos os casos, temos

$${\mathcal{O}_K}^\times = \mu_K$$

onde μ_K são as raízes da unidade dentro de K.

Teorema 4.1 (Teorema das unidades de Dirichlet)**.** *Seja K um corpo numérico, e denote por μ_K o grupo das raízes da unidade dentro de K. Então ${\mathcal{O}_K}^\times \simeq \mu_K \times \mathbb{Z}^{r+s-1}$.*

Demonstração. considere o mapa $\phi\colon K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$ da prova da cota de Minkowski. Queremos analizar as unidades, então para transformar a estrutura multiplicativa em aditiva, temos que tirar logaritmo. Isto é, considere $\log\colon (\mathbb{R}\setminus\{0\})^r \times (\mathbb{C}\setminus\{0\})^s \to \mathbb{R}^{r+s}$ dado por

$$\log(x_1, \dots, x_{r+s}) = (\log|x_1|, \dots, \log|x_r|, 2\log|x_{r+1}|, \dots, 2\log|x_{r+s}|).$$

Seja $\mathrm{Log} = \log\circ\phi$. Então $\alpha \in \mathcal{O}_K$ é uma unidade se e somente se $1 = |\mathrm{Nm}(\alpha)| = \prod_{i=1}^{r}|\phi(\beta)_i| \cdot \prod_{i=r+1}^{r+s}|\phi(\beta)_i|^2$, ou seja, se e somente se a soma das cordenadas de $\mathrm{Log}(\alpha)$ é 0. Seja $\mathbb{R}_0^{r+s-1} \subseteq \mathbb{R}^{r+s}$ o sub-espaço com soma das coordenadas 0. Temos que $\mathrm{Log}({\mathcal{O}_K}^\times)$ é um subgrupo de $\mathbb{R}_0^{r+s-1}$. Queremos provar que é um lattice. Para isso, basta provar dois fatos:

(1) Para todo $R \geq 0$, a quantidade de pontos em $\mathrm{Log}({\mathcal{O}_K}^\times)$ com tamanho $\leq R$ é finito.

(2) Existe B tal que para todo $z \in \mathbb{R}_0^{r+s-1}$, existe um ponto de $\mathrm{Log}({\mathcal{O}_K}^\times)$ com distância $\leq B$ de z.

Para (1), se $\mathrm{Log}(\alpha)$ tem tamanho $\leq \log R$, isso significa que todos os coeficientes do polinômio minimal de α são menores ou iguais que $\binom{n}{i}R^i$. Como os coeficientes são inteiros, isso significa que existem somente finitos tais α.

Para (2), seja $B' = (2/\pi)^s\sqrt{|D_K|}$. Então por Minkowski, se $c \in \mathbb{R}^r \times \mathbb{C}^s$ é tal que $\mathrm{Nm}(c) = B'$, necessariamente temos $\alpha \in \mathcal{O}_K$ não zero com $|\phi(\alpha)_i| \leq |c_i|$, e em particular $|\mathrm{Nm}(\alpha)| \leq B'$.

Agora seja $y \in \mathbb{R}^r \times \mathbb{C}^s$ tal que $\log(y) = x$, e considere $h \in \mathbb{R}^{r+s}$ tal que $h_i > 0$ e $\sum_i h_i = \log B'$. Considere $c \in \mathbb{R}^r \times \mathbb{C}^s$ onde $c_i = y_i e^{h_i}$ se $i \leq r$ e $c_i = y_i e^{h_i/2}$ se $i > r$. Então $\mathrm{Nm}(c) = B'$, e podemos encontrar $\alpha \in \mathcal{O}_K$ com $|\mathrm{Nm}(\alpha)| \leq B'$ e tal que $|\phi(\alpha)_i| \leq |c_i|$. Portanto $\mathrm{Log}(\alpha)_i \leq x_i + h_i$. Isso implica que a distância de $\mathrm{Log}(\alpha)$ e x é no máximo B' pois também sabemos que $\sum_i \mathrm{Log}(\alpha)_i \geq 0$.

Agora considere os finitos ideais principais de norma $\leq B'$, digamos $(\alpha_1), \ldots, (\alpha_k)$. Então $(\alpha) = (\alpha_i)$ para algum i, e então $\alpha/\alpha_i \in {\mathcal{O}_K}^\times$. Então $\mathrm{Log}(\alpha/\alpha_i) = \mathrm{Log}(\alpha) - \mathrm{Log}(\alpha_i)$, podemos tomar $B = B' + \max_i|\mathrm{Log}(\alpha_i)|$.

Então $\mathrm{Log}({\mathcal{O}_K}^\times) \simeq \mathbb{Z}^{r+s-1}$. Para terminar a prova do teorema, note que o kernel de $\mathrm{Log}\colon \mathcal{O}_K \to \mathbb{R}^{r+s}$ são elementos cujos todos os conjugados tem tamanho 1. É um problema clássico que isso só pode acontecer para raízes da unidade, e isso será um exercício.

Pode-se concluir da discussão acima que ${\mathcal{O}_K}^\times \simeq \mu_K \times \mathbb{Z}^{r+s-1}$. □

Definição 4.2. O volume do lattice $\mathrm{Log}({\mathcal{O}_K}^\times)$ é chamado de o *regulador* de K, e denotado por $\mathrm{Reg}(K)$.

Nota 4.3. Como computar as unidades e o grupo de classe? A cota de Minkowski faz com que podemos encontrar uma cota por cima do grupo de classes, ou seja, podemos computar que ele é gerado por certos elementos, mas temos que encontrar quais são as possíveis relações. Achar todas as relações necessita que entendamos sobre a aritmética de $\mathcal{O}_K$ e portanto que entendamos sobre as unidades. Para as unidades, podemos encontrar uma cota por baixo delas, achando $r + s - 1$ independentes, ou seja, podemos cotar $\mathrm{Reg}(K)$ por cima. Mas novamente, provar que elas são minimais é difícil. A maneira que temos de lidar com isso é que podemos computar $|\mathrm{Cl}(K)| \cdot \mathrm{Reg}(K)$ de maneira analítica, e portanto podemos descobrir quando achamos todas as relações e todas as unidades.

Proposição 4.4. *Seja $\mathfrak{a} \subseteq \mathcal{O}_K$ um ideal. Seja $N_{\mathfrak{a}}(t) := |\{\alpha \in \mathfrak{a} \colon |\mathrm{Nm}(\alpha)| \leq t\}/{\mathcal{O}_K}^{\times}|$. Então*

$$N_{\mathfrak{a}}(t) = \frac{2^r(2\pi)^s \mathrm{Reg}(K)}{|\mu_K|\sqrt{|D_K|}N(a)}t + O(t^{1-\frac{1}{n}}).$$

Ideia da prova. Considere uma região fundamental S_0' do lattice $\mathrm{Log}({\mathcal{O}_K}^{\times}) \subseteq \mathbb{R}_0^{r+s-1}$ tal que só contenha o ponto 0 do lattice. Seja $S'_{\leq t}$ a região em $\mathbb{R}^{r+s}$ que projeta em S_0 e tal que $\sum_i x_i \in [0, \log t]$. Isso é exatamente tal que $\mathrm{Log}^{-1}(S_{\leq t}) \cap \mathcal{O}_K$ tem $N_{\mathfrak{a}}(t)$ elementos.

Denote $S_{\leq t} = \log^{-1}(S'_{\leq t})$. Pode-se calcular que que $\mathrm{vol}(S_{\leq t}) = 2^r(\pi)^s \mathrm{Reg}(K)t$.

Agora vamos usar o seguinte fato: se $S \subseteq \mathbb{R}^n$ é uma região que é "bonita" o suficiente[15], então para qualquer lattice $\Lambda \subseteq \mathbb{R}^n$, temos

$$|cS \cap \Lambda| = \frac{\mathrm{vol}(S)}{\mathrm{vol}(\Lambda)}c^n + O(c^{n-1}).$$

Tomando $c = t^{1/n}$, temos que $cS_{\leq 1} = S_{\leq t}$, e então

$$|S_{\leq t} \cap \phi(\mathfrak{a})| = \frac{2^r\pi^s \mathrm{Reg}(K)}{\mathrm{vol}(\phi(\mathfrak{a}))}t + O(t^{1-\frac{1}{n}}).$$

Como $|\mu_K| \cdot N_{\mathfrak{a}}(t) = |S_{\leq t} \cap \phi(\mathfrak{a})|$ e como $\mathrm{vol}(\phi(\mathfrak{a})) = 2^{-s}\sqrt{|D_K|}N(\mathfrak{a})$, o teorema segue. □

Corolário 4.5. *Temos que $|\{\mathfrak{a} \subseteq \mathcal{O}_K \colon N(\mathfrak{a}) \leq t\}| = c_K t + O(t^{1-\frac{1}{n}})$ onde*

$$c_K = \frac{2^r(2\pi)^s \mathrm{Reg}(K)|\mathrm{Cl}(K)|}{|\mu_K|\sqrt{|D_K|}}.$$

Ou seja, a quantidade de ideais com norma no máximo t é basicamente linear em t.

Demonstração. Seja $c \in \mathrm{Cl}(K)$ e considere

$$N_c(t) = |\{\mathfrak{a} \subseteq \mathcal{O}_K \colon [\mathfrak{a}] = c,\ N(\mathfrak{a}) \leq t\}|.$$

Seja $\mathfrak{a}_c$ um ideal tal que $[\mathfrak{a}_c] = c^{-1}$. Então multiplicando por $\mathfrak{a}_c$ temos uma bijeção

$$\{\mathfrak{a} \subseteq \mathcal{O}_K \colon [\mathfrak{a}] = c,\ N(\mathfrak{a}) \leq t\} \longleftrightarrow \{\mathfrak{a} \subseteq \mathcal{O}_K \colon [\mathfrak{a}] = 1,\ N(\mathfrak{a}) \leq tN(\mathfrak{a}_c)\},$$

ou seja, $N_c(t) = N_{\mathfrak{a}}(tN(\mathfrak{a}_c))$. Então

$$N_c(t) = \frac{2^r(2\pi)^s \mathrm{Reg}(K)}{|\mu_K|\sqrt{|D_K|}N(\mathfrak{a}_c)}(tN(\mathfrak{a}_c)) + O((tN(\mathfrak{a}_0))^{1-\frac{1}{n}}) = \frac{c_K}{|\mathrm{Cl}(K)|}t + O(t^{1-\frac{1}{n}}).$$

Somando sobre todo $c \in \mathrm{Cl}(K)$ obtemos o resultado. □

[15] A condição precisa é que ∂S é $(n-1)$-Lipschitz parametrizável.

4.2. **Funções zeta.** Lembramos que temos a função zeta de Riemann

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}, \quad \text{para } \mathrm{Re}(s) > 1.$$

Iremos ver depois que $\zeta(s)$ pode ser extendida para todo o plano complexo exceto $s = 1$. Podemos ver já que ζ se parece com $1/(s-1)$ perto de $s = 1$:

Proposição 4.6. *Temos que*

$$\lim_{s\to 1^+} (s-1)\zeta(s) = 1.$$

Demonstração. Escreva $\zeta(s) = \frac{1}{s-1} + \phi(s)$. Escrevendo $\frac{1}{s-1} = \int_1^\infty x^{-s}\, \mathrm{d}x$, temos que

$$\phi(s) = \sum_{n\geq 1} \left(\frac{1}{n^s} - \int_n^{n+1} x^{-s}\, \mathrm{d}x \right).$$

Para $s > 0$, x^{-s} é decrescente, e portanto

$$0 < \phi(s) < \sum_{n\geq 1} \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) = 1.$$

Ou seja, $\lim_{s\to 1}(s-1)\phi(s) = 0$, e então

$$\lim_{s\to 1^+} (s-1)\zeta(s) = 1 + \lim_{s\to 1^+} (s-1)\phi(s) = 1. \qquad \square$$

Também podemos definir funções análogas para corpos numéricos.

Definição 4.7. A *função zeta de Dedekind* de um corpo numérico K é

$$\zeta_K(s) = \sum_{\mathfrak{a}\subseteq \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s}.$$

O resultado que provamos implica que $\zeta_K(s)$ converge absolutamente para $\mathrm{Re}(s) > 1$. Seja $a_t = |\{\mathfrak{a} \subseteq \mathcal{O}_K : N(\mathfrak{a}) = t\}|$, de modo que

$$\zeta_K(s) = \sum_{k\geq 1} \frac{a_k}{k^s}.$$

O resultado que provamos anteriormente diz que $a_k = c_K + b_k$ onde $b_k = O(k^{1-\frac{1}{n}})$, e portanto podemos escrever

$$\zeta_K(s) = c_K\zeta(s) + \sum_{k\geq 1} \frac{b_k}{k^s}.$$

E de fato, $\sum_{k\geq 1} \frac{b_k}{k^s}$ converge absolutamente para $\mathrm{Re}(s) > 1 - \frac{1}{n}$. Ou seja, temos

Teorema 4.8 (Fórmula do número de classe)**.** $\zeta_K(s)$ *converge absolutamente para* $\mathrm{Re}(s) > 1$, *e temos*

$$\lim_{s\to 1^+} \zeta_K(s) = \frac{2^r(2\pi)^s \mathrm{Reg}(K)|\mathrm{Cl}(K)|}{|\mu_K|\sqrt{|D_K|}}$$

Exemplo 4.9. Seja $K = \mathbb{Q}[\sqrt{d}]$. Então

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1} = \prod_{p} \prod_{\mathfrak{p}\mid p\mathcal{O}_K} (1 - N(\mathfrak{p})^{-s})^{-1}$$

e podemos ver que

$$\prod_{\mathfrak{p}\mid p\mathcal{O}_K} (1 - N(\mathfrak{p})^{-s})^{-1} = \begin{cases} (1-p^{-s})^{-1} & \text{se } p \mid D_K, \\ (1-p^{-s})^{-2} & \text{se } \left(\frac{D_K}{p}\right) = 1, \\ (1-p^{-2s})^{-1} & \text{se } \left(\frac{D_K}{p}\right) = -1, \end{cases} = (1-p^{-s})^{-1}\left(1 - \left(\frac{D_K}{p}\right)p^{-s}\right)^{-1}.$$

Ou seja,

$$\zeta_K(s) = \zeta(s)\prod_p \left(1 - \left(\frac{D_K}{p}\right)p^{-s}\right)^{-1}.$$

Note que por reciprocidade quadrática, $\left(\frac{D_K}{p}\right)$ só depende de $p \mod D_K$, e é multiplicativa em p. Ou seja, para $p \nmid D_K$,

$$\left(\frac{D_K}{p}\right) = \chi_K(p)$$

onde $\chi_K \colon (\mathbb{Z}/D_K\mathbb{Z})^\times \to \{\pm 1\}$ é multiplicativa.

Ou seja, $\zeta_K(s) = \zeta(s)L(s,\chi_K)$ onde

$$L(s,\chi_K) = \sum_{n\geq 1} \frac{\chi_K(n)}{n^s}, \quad \text{para } \mathrm{Re}(s) > 1,$$

onde denotamos $\chi(n) = 0$ se $(n, D_K) \neq 1$. A fórmula do número de classe implica que

$$\lim_{s\to 1^+} L(s,\chi_K) = c_K \neq 0.$$

Para provarmos o teorema de Dirichlet, um passo crucial será usar que $L(1,\chi) \neq 0$ para todo caracter de Dirichlet χ. A prova disso será similar ao exemplo acima: se $\chi \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, vamos encontrar $L(s,\chi)$ como um fator de $\zeta_K(s)$ onde $K = \mathbb{Q}[\zeta_N]$. Isso requer entender os primos de $\mathbb{Q}[\zeta_N]$ melhor, e para isso vamos usar teoria de Galois.

4.3. **Teoria de Galois.** O resto da aula de hoje será para discutir os resultados de Teoria de Galois.

Definição 4.10. Seja L/K uma extensão finita de corpos. Denotamos por $\mathrm{Aut}(L/K) = \{\sigma\colon L \to L\colon \sigma(k) = k, \text{ para todo } k \in K\}$.

De maneira concreta, se $L = K[\alpha]$, e se $f(x) \in K[x]$ é o polinômio minimal de α, com raízes $\alpha_1, \ldots, \alpha_n$, então os elementos de $\mathrm{Aut}(L/K)$ estão em bijeção com os α_i tal que $\alpha_i \in L$. Em particular, $|\mathrm{Aut}(L/K)| \leq n = \dim_K L$.

Exemplo 4.11. Seja $K = \mathbb{Q}$. Para $L = \mathbb{Q}[\sqrt{d}]$, $\mathrm{Aut}(L/K)$ tem dois elementos: a identidade e a conjugação, que leva $\sqrt{d} \mapsto -\sqrt{d}$. Portanto $\mathrm{Aut}(L/K) \simeq \mathbb{Z}/2\mathbb{Z}$.

Exemplo 4.12. Seja $K = \mathbb{Q}$ e $L = \mathbb{Q}[2^{1/3}]$. Então $\mathrm{Aut}(L/K)$ só tem a identidade, pois as outras raízes de $x^3 - 2$ são complexas, e portanto não estão em L.

Exemplo 4.13. Seja $K = \mathbb{Q}$ e $L = \mathbb{Q}[\zeta_n]$. Então as raízes do polinômio minimal de ζ_n são ζ_n^i para $(i, n) = 1$, que estão todas em L. Ou seja,

$$\mathrm{Aut}(L/K) = \{\sigma_i\colon i \in (\mathbb{Z}/n\mathbb{Z})^\times\}$$

onde $\sigma_i(\zeta_n) = \zeta_n^i$. Note que $\sigma_i(\sigma_j(\zeta_n)) = \sigma_i(\zeta_n^j) = \zeta_n^{ij} = \sigma_{ij}(\zeta_n)$, portanto $\mathrm{Aut}(L/K) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Definição 4.14. Seja L/K uma extensão finita de corpos de característica 0. Dizemos que L/K é *Galois* se $|\mathrm{Aut}(L/K)| = \dim_K L$, e nesse caso denotamos $\mathrm{Gal}\,(L/K) := \mathrm{Aut}(L/K)$.

Se $L = K[\alpha]$, isso é equivalente a todos os conjugados de α pertencerem a L.

Exemplo 4.15. Vimos acima que $\mathbb{Q}[\sqrt{d}]/\mathbb{Q}$ e $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ são Galois. Seja $K = \mathbb{Q}[\alpha]$ com $\alpha^3 - 3\alpha + 1 = 0$. Então podemos ver que $\alpha^2 - 2$ e $2 - \alpha - \alpha^2$ são raízes de $x^3 - 3x + 1$. Portanto $K/\mathbb{Q}$ é Galois.

Iremos usar o seguinte teorema sem provar.

Teorema 4.16 (Teorema Fundamental da teoria de Galois)**.** *Seja L/K uma extensão finita Galois. Então existe uma bijeção*

$$\{\textit{corpos } K \subseteq K_0 \subseteq L\} \longleftrightarrow \{\textit{subgrupos de } G := \mathrm{Gal}\,(L/K)\}$$

$$K_0 \mapsto \mathrm{Aut}(L/K_0)$$

$$L^H \hookleftarrow H$$

onde $L^H := \{x \in L\colon \sigma(x) = x \text{ para todo } \sigma \in H\}$.

Além disso, tal correspondência satisfaz as seguintes propriedades:

(a) Ela respeita inclusões de maneira reversa, ou seja, $H_1 \subseteq H_2 \iff L^{H_2} \subseteq L^{H_1}$.

(b) L/L^H *é Galois, e* $\dim_{L^H}(L) = |H|$.

(c) L^H/K *é Galois se e somente se* H *é normal em* G*, e nesse caso* $\mathrm{Gal}\left(L^H/K\right) \simeq G/H$.

Exemplo 4.17. Seja $L = \mathbb{Q}[\sqrt{2}, i]$. Então temos que $\mathrm{Gal}\,(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$ onde $\sigma(\sqrt{2}) = -\sqrt{2}$ e $\tau(i) = -i$. A correspondência é

$$\{1\} \mapsto L$$

$$\{1, \sigma\} \mapsto \mathbb{Q}[i]$$

$$\{1, \tau\} \mapsto \mathbb{Q}[\sqrt{2}]$$

$$\{1, \sigma\tau\} \mapsto \mathbb{Q}[\sqrt{-2}]$$

$$\{1, \sigma, \tau, \sigma\tau\} \mapsto \mathbb{Q}.$$

Exemplo 4.18. Seja $L = \mathbb{Q}[2^{1/3}, \omega]$. Então $\mathrm{Gal}\,(L/\mathbb{Q})$ não é abeliano. Se $x(2^{1/3}) = \omega 2^{1/3}$ e $x(\omega) = \omega$ e $y(2^{1/3}) = 2^{1/3}$ e $y(\omega) = \overline{\omega} = \omega^2$, então $\mathrm{Gal}\,(L/\mathbb{Q}) = \{1, x, x^2, y, yx, yx^2\}$, e temos $xy = yx^2$. A correspondência é

$$\{1\} \mapsto L$$

$$\{1, y\} \mapsto \mathbb{Q}[2^{1/3}]$$

$$\{1, yx\} \mapsto \mathbb{Q}[\omega 2^{1/3}]$$

$$\{1, yx^2\} \mapsto \mathbb{Q}[\omega^2 2^{1/3}]$$

$$\{1, x, x^2\} \mapsto \mathbb{Q}[\omega]$$

$$\{1, x, x^2, y, yx, yx^2\} \mapsto \mathbb{Q}.$$

Note que $K = \mathbb{Q}[2^{1/3}]$ não é Galois porque as outras duas raízes de $x^3 - 2$ não são elementos de K. De fato, isso pode ser feito preciso:

Definição 4.19. Seja $K \subseteq \mathbb{C}$ e considere um polinômio $f(x) \in K[x]$. O *corpo de fatoração* de f é $L := K[\alpha_1, \ldots, \alpha_n]$ onde $\alpha_i \in \mathbb{C}$ são as raízes de f.

Teorema 4.20. *Seja* L/K *uma extensão finita de corpos com* $L \subseteq \mathbb{C}$*. Então* L/K *é Galois se e somente se* L *é o corpo de fatoração de algum* $f(x) \in K[x]$.

Definição 4.21. Seja $f(x) \in K[x]$ para um corpo $K \subseteq \mathbb{C}$. O grupo de Galois de f, denotado $\mathrm{Gal}(f)$, é o grupo de Galois $\mathrm{Gal}\,(L/K)$ onde L é o corpo de fatoração de f.

Vamos considerar dois exemplos clássicos para ver como Galois é usado.

Primeiro, vamos mostrar que equações de grau ≥ 5 não tem fórmula fechada com radicais. Seja $K \subseteq \mathbb{C}$ um corpo e considere um número complexo da forma $\alpha = a + b\sqrt[n]{c}$ para $a, b, c \in K$. Então α é raiz do polinômio $f(x) = (x-a)^n - b^n c$, e seu corpo de fatoração é $L = K[\zeta_n, \sqrt[n]{c}]$. Seja $L_0 = K[\zeta_n]$. Primeiro note que L_0/K é Galois, e seu grupo de Galois é um subgrupo de $(\mathbb{Z}/n\mathbb{Z})^\times$. Agora note que L/L_0 é Galois, e seu grupo de Galois é um subgrupo de $\mathbb{Z}/n\mathbb{Z}$. Ambos esses grupos são abelianos.

De maneira geral, se α é uma expressão em termos de elementos de K_0 e radicais, escreva $\alpha = \alpha_n$ onde $\alpha_{i+1} = a_i + \sqrt[e_i]{b_i}$. para $a_i, b_i \in K_i$ onde $K_{i+1} = K_i[\alpha_{i+1}, \zeta_{e_i}]$. Agora considere o polinômio cujas raízes são a expressão com todas as possíveis escolhas de raízes da unidade. Pode-se ver que tal polinômio f tem coeficientes em K_0 e que K_n é o corpo de fatoração de f. Portanto K_n/K_0 é Galois. Da mesma forma, temos que K_i/K_j é Galois para todo $i \geq j$. Vamos analisar o grupo de Galois de K_{i+1}/K_i. Seja $K_i' = K_i[\zeta_{e_i}]$. Então K_{i+1}/K_i' é Galois e seu grupo de Galois é um subgrupo de $\mathbb{Z}/e_i\mathbb{Z}$. Também, K_i'/K_i é Galois e seu grupo de Galois é um subgrupo de $(\mathbb{Z}/e_i\mathbb{Z})^\times$. Portanto, se $G_{2i} = \mathrm{Gal}\left(K_n/K_{n-i}\right)$ e se $G_{2i+1} = \mathrm{Gal}\left(K_n/K'_{n-i-1}\right)$, temos uma sequência de subgrupos

$$1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{2n} = \mathrm{Gal}\left(K_n/K_0\right)$$

tal que G_i é normal em G_{i+1}, e tal que G_{i+1}/G_i é abeliano.

Definição 4.22. Um grupo G é *solúvel* se existe uma sequência de subgrupos $1 = G_0 \subseteq \cdots \subseteq G_n = G$ onde G_{i+1}/G_i é um grupo abeliano para todo i.

Pode-se provar que subgrupos e quocientes the grupos solúveis também são solúveis. Isso será um exercício.

Agora considere $g(x) \in K[x]$ irredutível para $K \subseteq \mathbb{C}$ e suponha que uma de suas raízes α pode ser escrita com radicais. Considerando o f como acima, então $g \mid f$, e se K_f, K_g são os corpos de fatoração, temos que $\mathrm{Gal}\left(K_f/K_g\right)$ corresponde a um subgrupo normal de $\mathrm{Gal}\left(K_f/K\right)$. Como $\mathrm{Gal}\left(K_f/K\right)$ é solúvel, então $\mathrm{Gal}(g) = \mathrm{Gal}\left(K_g/K\right)$ também é. Ou seja, provamos que:

Teorema 4.23. *Seja $f \in K[x]$ para $K \subseteq \mathbb{C}$ tal que uma de suas raízes pode ser escrita com radicais em K. Então $\mathrm{Gal}(f)$ é solúvel.*

Exemplo 4.24. Considere $f(x) = x^5 - 4x - 1$. Pode-se provar que $\mathrm{Gal}(f) \simeq S_5$, e podemos ver que S_5 não é solúvel pois seu único subgrupo normal é A_5, e A_5 não tem nenhum subgrupo normal não trivial.

O outro exemplo é sobre construções com régua e compasso. Considere os papel como o plano complexo $\mathbb{C}$ e a unidade da régua com distãncia 1. Então podemos marcar todos os pontos inteiros com régua, e podemos fazer divisão de segmentos, e obtemos todos os racionais. Agora considere uma sequência de corpos $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots$ onde $K_{i+1} = K_i[\alpha_{i+1}]$ onde α_{i+1} é o primeiro ponto marcado que não está em K_i. É simples ver que todo K_{i+1}/K_i são extensões quadráticas. Então se podemos marcar $\alpha \in \mathbb{C}$, isso significa que podemos escrever α com uma combinação de raízes quadradas. Repetindo o argumento do exemplo, anterior, temos que se f é o polinômio minimal de α, então $\mathrm{Gal}(f)$ tem tamanho uma potência de 2.

Teorema 4.25. *$\alpha \in \mathbb{C}$ com polinômio minimal $f \in \mathbb{Q}[x]$ é construtível com régua e compasso se e somente se* $\mathrm{Gal}(f)$ *tem ordem uma potência de* 2.

Demonstração. Provamos acima que isso é necessário. Para ver que isso é suficiente, usamos o seguinte resultado de teoria dos grupos: se $|G| = 2^n$, então existe uma sequência de subgrupos

$$1 = G_0 \subseteq \cdots \subseteq G_n = G$$

tal que G_i é normal em G_{i+1} e que $G_{i+1}/G_i \simeq \mathbb{Z}/2\mathbb{Z}$. Assim, cada G_i corresponde a um K_i, com $\mathbb{Q} = K_n \subseteq K_{n-1} \subseteq \cdots \subseteq K_0$, com $\alpha \in K_0$ e todo K_i/K_{i+1} quadrático. Como podemos resolver toda equação quadrática com régua e compasso, α é construtível. □

Exemplo 4.26. Seja ζ_n uma raiz da unidade. Então ζ_n é construtível se e somente se $\phi(n)$ é uma potência de 2. Em particular, é impossível trissectar ângulos, pois daí poderíamos construir ζ_9, e $\phi(9) = 6$ não é uma potência de 2.

Exercícios

Dicas estão no rodapé.

(1) Seja $f(x) \in \mathbb{Z}[x]$ um polinômio mônico onde todas as suas raízes tem valor absoluto 1. Prove que todas as raízes são raízes da unidade.[16]

(2) Seja $K = \mathbb{Q}[\alpha]$ com $\alpha^3 - 3\alpha + 1 = 0$.

(a) Prove que $3\mathcal{O}_K = (\alpha + 1)^3$.

(b) Prove que se $p \neq 3$, então ou $x^3 - 3x + 1 \in \mathbb{F}_p[x]$ ou é irredutível ou tem 3 raízes distintas.[17]

(c) Conclua que

$$\zeta_K(s) = \zeta(s) \prod_{p \equiv \pm 1 \mod 9} (1 - p^{-s})^{-2} \prod_{p \not\equiv \pm 1 \mod 9} (1 + p^{-s} + p^{-2s})^{-1}.$$

(d) Seja g uma raiz primitiva módulo 9, e considere os caracteres $\chi_1, \chi_2 \colon (\mathbb{Z}/9\mathbb{Z})^\times \to \mathbb{C}^\times$ dados por $\chi_1(g) = \omega$ e $\chi_2(g) = \omega^2$ para uma raiz cúbica da unidade ω. Prove que

$$\zeta_K(s) = \zeta(s) L(s, \chi_1) L(s, \chi_2).$$

Conclua que

$$\mathrm{Reg}(K) = \frac{9|L(1, \chi_1)|^2}{4}.$$

(e) Vamos ver que $\alpha, \alpha^2 - 2$ são unidades fundamentais para K. Calcule que o volume do lattice gerado por $\mathrm{Log}(\alpha)$ e $\mathrm{Log}(\alpha^2 - 2)$ é menor que 0.85 (use uma calculadora). Use um computador para se convencer de que

$$\frac{9|L(1, \chi_1)|^2}{4} > \frac{0.85}{2},$$

e conclua que α e $\alpha^2 - 2$ são unidades fundamentais.

(3) Seja ζ uma raiz p-ésima da unidade para p primo ímpar. $K = \mathbb{Q}[\zeta]$. Lembre-se que $\mathcal{O}_K = \mathbb{Z}[\zeta]$.

(a) Calcule que $D_K = (-1)^{(p-1)/2} p^{p-2}$.

(b) Seja $\pi = \zeta - 1$. Prove que $\mathrm{Nm}(\pi) = p$, e conclua que $p\mathcal{O}_K = (\pi)^p$.

---

[16] Assuma f irredutível, e se α_i são as raízes, considere os polinômios $f_k(x) = \prod_i (x - \alpha_i^k)$.

[17] Note que $\alpha^2 - 2$ também é uma raiz de $x^3 - 3x + 1$.

(c) Agora seja $q \neq p$. Como $q \nmid D_K$, q é não ramificado. Prove que $q\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_g$ onde todos os $f_i := \dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}_i)$ são iguais a $\mathrm{ord}_p(q)$.[18] Conclua que

$$\prod_{\mathfrak{p}|q\mathcal{O}_K} (1 - N(\mathfrak{p})^{-s})^{-1} = (1 - q^{-fs})^{-n/f}, \quad \text{onde } f = \mathrm{ord}_p(q).$$

(d) Agora considere todos os caracteres $\chi\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ (o trivial e $p-2$ outros não triviais). Prove que para $q \neq p$, temos

$$\prod_{\chi} (1 - \chi(q)q^{-s})^{-1} = (1 - q^{-fs})^{-n/f}, \quad \text{onde } f = \mathrm{ord}_p(q).$$

(e) Conclua que $\zeta_K(s) = \zeta(s)\prod_{\chi\neq 1} L(s,\chi)$. É um fato que $L(s,\chi)$ para $\chi \neq 1$ pode ser extendido para $s = 1$. Com isso, conclua que $L(1,\chi) \neq 0$.

(4) Os detalhes de teoria dos grupos sobre a insolubilidade da quíntica:

(a) Para um grupo G, denote por G' o subgrupo gerado todos os elementos da forma $aba^{-1}b^{-1}$. Prove que G' é o menor subgrupo normal tal que G/G' é abeliano.

(b) Seja $G^{(0)} = G$ e tome $G^{(i+1)} = (G^{(i)})'$. Prove que G é solúvel se e somente se $G^{(n)} = 1$ para algum n.

(c) Seja $H \subseteq G$. Prove que $H^{(i)} \subseteq G^{(i)}$. Se H é normal, prove que $G^{(i)} \twoheadrightarrow (G/H)^{(i)}$. Conclua que subgrupos e quocientes de grupos solúveis são solúveis.

(d) (extra) Prove que se $H \subseteq G$ é um subgrupo normal e se H e G/H são solúveis, então G também é solúvel.[19]

(5) Os detalhes sobre as construções de régua e compasso:

(a) Seja G um grupo, e $g \in G$. A órbita de g é o conjunto de elementos da forma hgh^{-1} para $h \in G$. Prove que as órbitas de elementos particionam G, e que seus tamanhos dividem $|G|$.

(b) Agora assuma que $|G| = p^n$ para um primo p. Conclua que o centro de G, dado por $Z(G) := \{z \in G\colon gz = zg \text{ para todo } g \in G\}$, é não-trivial.[20]

(c) Note que $Z(G)$ é normal em G, e conclua que existe uma sequência de subgrupos $1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ tal que $G_{i+1}/G_i \simeq \mathbb{Z}/p\mathbb{Z}$ para todo i.[21]

---

[18] Lembre-se que provamos anteriormente que $x^{p^n} - x \mod p$ é o produto de todos os polinômios mônicos irredutíveis de grau menor ou igual a n.

[19] Como que $G^{(i)}$ se relaciona com $H^{(j)}$ e $(G/H)^{(j)}$?

[20] Os elementos do centro estão em bijeção com as órbitas de tamanho 1.

[21] Prove primeiro para grupos abelianos. Depois faça indução em $|G|$, e note que $|G/Z(G)|$ tabém é uma potência de p.

5. 3 de Abril

5.1. **Elemento de Frobenius.** Seja L/K uma extensão finita de corpos numéricos. Assuma que L/K é Galois. Vamos denotar $G := \mathrm{Gal}\,(L/K)$. Note que se $\sigma \in G$ e $I \subseteq \mathcal{O}_L$ é um ideal, $\sigma(I)$ também é um ideal.

Proposição 5.1. *Seja $\sigma \in G$ e $I \subseteq \mathcal{O}_L$ um ideal. Então σ induz um isomorfismo*

$$\sigma^* \colon \mathcal{O}_L/I \xrightarrow{\sim} \mathcal{O}_L/\sigma(I).$$

Em particular, se $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$ é um ideal primo, então $\sigma(\mathfrak{P}) \mid p\mathcal{O}_L$ também é um ideal primo. Vamos provar que, de fato, todos os fatores primos de $\mathfrak{p}\mathcal{O}_L$ são atingidos dessa forma.

Lema 5.2. *Sejam $\mathfrak{P}, \mathfrak{P}' \mid \mathfrak{p}\mathcal{O}_L$ ideais primos. Então existe $\sigma \in G$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

Demonstração. Considere $\alpha \in \mathcal{O}_L$ tal que $\mathfrak{P} \mid (\alpha)$ mas tal que $\mathfrak{P}_0 \nmid (\alpha)$ para todo $\mathfrak{P}_0 \mid \mathfrak{p}\mathcal{O}_L$ diferente de $\mathfrak{P}$. Considere $N := \prod_{\sigma \in G} \sigma(\alpha)$. Como $\sigma(N) = N$ para todo $\sigma \in G$, temos que $N \in \mathcal{O}_L^G = \mathcal{O}_K$. Logo $\mathfrak{p} \mid N$. Ou seja, existe $\sigma \in G$ tal que $\mathfrak{P}' \mid (\sigma(\alpha))$. Mas $\sigma(\alpha)$ é tal que o único fator primo que divide $\mathfrak{p}\mathcal{O}_K$ e $\sigma(\alpha)$ é $\sigma(\mathfrak{P})$, e portanto temos que ter $\mathfrak{P}' = \sigma(\mathfrak{P})$. □

Corolário 5.3. *Se L/K é Galois, então $\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ onde $\mathfrak{P}_i$ são distintos, e temos que $f_i = f$ para todo i, onde $n = efg$.*

Demonstração. Seja $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$. Pelo lema acima para todo i, j existe $\sigma \in G$ com $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Daí $\mathfrak{P}_i^e \mid \mathfrak{p}\mathcal{O}_L \iff \mathfrak{P}_j^e = \sigma(\mathfrak{P}_i^e) \mid \mathfrak{p}\mathcal{O}_K$, e portanto que $e_i = e_j$. Finalmente, como $\sigma^* \colon \mathcal{O}_L/\mathfrak{P}_i \xrightarrow{\sim} \mathcal{O}_L/\mathfrak{P}_j$, também temos que $f_i = f_j$.

O fato de que $n = efg$ segue de

$$n = \sum_{i=1}^{g} e_i f_i = efg.$$ □

Exemplo 5.4. Seja $K = \mathbb{Q}[\zeta_n]$. Seja p um primo. Pelo algoritmo de fatoração, o corolário acima diz que

$$\Phi_n(x) \equiv F_1(x)^e \cdots F_g(x)^e \mod p$$

onde todos os F_i tem o mesmo grau f.

Definição 5.5. Seja $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$ um ideal primo de $\mathcal{O}_L$. O *subgrupo de decomposição* de $\mathfrak{P}$, denotado por $D_{\mathfrak{P}|\mathfrak{p}} \subseteq G$ é

$$D_{\mathfrak{P}|\mathfrak{p}} := \{\sigma \in G \colon \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Pelos resultados acima, temos que $|D_{\mathfrak{P}|\mathfrak{p}}| = n/g = ef$. Note também que $D_{\sigma(\mathfrak{P})|\mathfrak{p}} = \sigma D_{\mathfrak{P}|\mathfrak{p}}\sigma^{-1}$.

Proposição 5.6. *Seja $L/\mathbb{Q}$ Galois e $K = L^H \subseteq L$. Seja $\mathfrak{p} \mid p\mathcal{O}_K$, $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$. Então $D_{\mathfrak{P}|\mathfrak{p}} = H \cap D_{\mathfrak{P}|p}$. Se $K/\mathbb{Q}$ é Galois, então $D_{\mathfrak{p}|p} = D_{\mathfrak{P}|p} \mod H$.*

Demonstração. A primeira parte é trivial. Para a segunda parte, como $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ para todo $\sigma \in \mathrm{Gal}\,(L/\mathbb{Q})$, temos que se $\sigma \in D_{\mathfrak{P}|p}$, então $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K = \sigma(\mathfrak{P}) \cap \sigma(\mathcal{O}_K) = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \sigma(\mathfrak{p})$. Portanto $D_{\mathfrak{p}|p} \supseteq D_{\mathfrak{P}|p} \mod H$. Agora se $\sigma \in D_{\mathfrak{p}|p}$, escolha $\tilde{\sigma} \in \mathrm{Gal}\,(L/\mathbb{Q})$ que reduza para σ. Seja $\mathfrak{P}' = \sigma^{-1}(\mathfrak{P})$. Então podemos escolher $\sigma_0 \in \mathrm{Gal}\,(L/K) = H$ tal que $\sigma_0(\mathfrak{P}) = \mathfrak{P}'$, e daí $\tilde{\sigma}\sigma_0 \in D_{\mathfrak{P}|p}$ e também reduz para σ. □

Para um ideal primo $\mathfrak{P}$, denote $k(\mathfrak{P}) := \mathcal{O}_L/\mathfrak{P}$. Pela definição de $D_{\mathfrak{P}|\mathfrak{p}}$, todo elemento $\sigma \in D_{\mathfrak{P}|\mathfrak{p}}$ induz um isomorfismo

$$\sigma^* \colon k(\mathfrak{P}) \to k(\mathfrak{P}),$$

ou seja, $\sigma^* \in \mathrm{Aut}(k(\mathfrak{P})/k(\mathfrak{p}))$.

Proposição 5.7. *Sejam F'/F corpos finitos com $\dim_F F' = f$. Então $\mathrm{Aut}(F'/F) \xrightarrow{\sim} \mathbb{Z}/f\mathbb{Z}$ de maneira canônica, onde $\sigma \mapsto 1$ onde $\sigma(x) = x^{|F|}$ é o* elemento de Frobenius.

Demonstração. É fácil ver que $\sigma(x) = x^{|F|}$ pertence a $\mathrm{Aut}(F'/F)$. Como F tem raiz primitiva α, temos que $\sigma^k = 1 \iff \alpha^{|F|^k} = \alpha$, ou seja, se e somente se $|F|^f - 1 \mid |F|^k - 1 \iff n \mid k$. Portanto temos f automorfismos distintos $1, \sigma, \ldots, \sigma^{f-1}$. Como $f = \dim_F F'$, esses são todos os automorfismos. □

Teorema 5.8. *Seja $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$ um ideal primo. Então o mapa acima*

$$D_{\mathfrak{P}|\mathfrak{p}} \to \mathrm{Aut}(k(\mathfrak{P})/k(\mathfrak{p}))$$

é sobrejetor.

Demonstração. Seja $K_0 = L^{D_{\mathfrak{P}|\mathfrak{p}}}$. Então para todo $\mathfrak{P}_0 \subseteq \mathfrak{p}\mathcal{O}_{K_0}$, temos $D_{\mathfrak{P}_0|\mathfrak{p}} = 1$, ou seja, $\mathfrak{p}\mathcal{O}_{K_0} = \mathfrak{P}_1 \ldots \mathfrak{P}_g$ onde $k(\mathfrak{P}_i) \simeq k(\mathfrak{p})$.

Seja i tal que $\mathfrak{P} \mid \mathfrak{P}_i\mathcal{O}_L$. Escolha $\alpha_0 \in k(\mathfrak{P})$ uma raiz primitiva, e escolha algum $\alpha \in \mathcal{O}_L$ tal que $\alpha_0 = \alpha \mod \mathfrak{P}$. Considere o polinômio $f(x) = \prod_{\sigma \in D_{\mathfrak{P}|\mathfrak{p}}}(x - \sigma(\alpha))$. Seus coeficientes estão em K_0. Então $f(x) \mod \mathfrak{P}_i$ é divisível pelo polinômio minimal de α_0. Como $\alpha_0^{|k(\mathfrak{p})|}$ também é uma raiz do polinômio minimal, existe $\sigma \in D_{\mathfrak{P}|\mathfrak{p}}$ tal que $\alpha_0^{|k(\mathfrak{p})|} = \sigma(\alpha) \mod \mathfrak{P}_i$. Isso significa que tal σ reduz ao Frobenius de $\mathrm{Aut}(k(\mathfrak{P})/k(\mathfrak{p}))$, portanto o mapa acima é sobrejetor. □

Definição 5.9. Se $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$ é um primo, o *grupo de inércia* $I_{\mathfrak{P}|\mathfrak{p}} \subseteq D_{\mathfrak{P}|\mathfrak{p}}$ é o kernel de $D_{\mathfrak{P}|\mathfrak{p}} \twoheadrightarrow \mathrm{Aut}(k(\mathfrak{P})/k(\mathfrak{p}))$. Isto é, $I_{\mathfrak{P}|\mathfrak{p}} = \{\sigma \in G \colon \sigma(x) \equiv x \mod \mathfrak{P} \text{ para todo } x \in \mathcal{O}_L\}$.

Em particular,

$$|D_{\mathfrak{P}|\mathfrak{p}}| = |I_{\mathfrak{P}|\mathfrak{p}}| \cdot |\mathrm{Aut}(k(\mathfrak{P})/k(\mathfrak{p}))|,$$

e portanto $|I_{\mathfrak{P}|\mathfrak{p}}| = e$. Ou seja, se $\mathfrak{p}$ não é ramificado, então $I_{\mathfrak{P}|\mathfrak{p}} = 1$ e $D_{\mathfrak{P}|\mathfrak{p}} \xrightarrow{\sim} \mathrm{Aut}(k(\mathfrak{P})/k(\mathfrak{p}))$.

Definição 5.10. Seja $\mathfrak{p} \subseteq \mathcal{O}_K$ não ramificado e considere $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$. Então o *elemento de Frobenius* de $\mathfrak{P}$ é o elemento $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}} \in D_{\mathfrak{P}|\mathfrak{p}}$ que é levado ao Frobenius no isomorfismo acima. De maneira concreta, é o único $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}} \in G$ tal que

$$\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}}(x) \equiv x^{|k(\mathfrak{p})|} \mod \mathfrak{P} \quad \text{para todo } x \in \mathcal{O}_L.$$

Note que $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}}$ gera o grupo cíclico $D_{\mathfrak{P}|\mathfrak{p}}$. Portanto, a ordem do elemento $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}}$ é f. Note também que temos $\mathrm{Frob}_{\sigma(\mathfrak{P})|\mathfrak{p}} = \sigma \mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}} \sigma^{-1}$. Portanto, se G é abeliano, $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}}$ só depende de $\mathfrak{p}$, e daí denotamos de $\mathrm{Frob}_{\mathfrak{p},L}$, ou $\mathrm{Frob}_{\mathfrak{p}}$ se L é implícito. O mesmo é verdade para $D_{\mathfrak{P}|\mathfrak{p}}$ e $I_{\mathfrak{P}|\mathfrak{p}}$, e os denotamos da mesma maneira.

Em geral, se $\mathfrak{p}$ é ramificado, então $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}}$ é um elemento de $D_{\mathfrak{P}|\mathfrak{p}}/I_{\mathfrak{P}|\mathfrak{p}}$.

Exemplo 5.11. Seja $K = \mathbb{Q}[\sqrt{d}]$. Identifique $\mathrm{Gal}\,(K/\mathbb{Q}) = \{\pm 1\}$. Seja $p \nmid D_K$. Vimos que $p\mathcal{O}_K$ é primo exatamente quando $\left(\frac{D_K}{p}\right) = -1$. Mas $p\mathcal{O}_K$ é primo exatamente quando $f = 2$. Portanto, temos que $\mathrm{Frob}_p = \left(\frac{D_K}{p}\right)$.

Exemplo 5.12. Seja $K = \mathbb{Q}[\zeta_n]$, e considere $p \nmid n$. Seja $\sigma_i(\zeta_n) = \zeta_n^i$. Podemos observar que $\sigma_p(x) \equiv x^p \mod p$ para todo x, e portanto temos que ter que $\mathrm{Frob}_p = \sigma_p$. Em particular, primos $p \equiv a \mod n$ para $(a, n) = 1$ são exatamente os primos tal que $\mathrm{Frob}_p = \sigma_a$.

Proposição 5.13. *Seja $L/\mathbb{Q}$ Galois, e seja $K = L^H \subseteq L$. Seja p não ramificado em L. Seja $\mathfrak{p} \mid p\mathcal{O}_K$ e $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$ ideais primos. Então* $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}} = \mathrm{Frob}_{\mathfrak{P}|p}^{f(\mathfrak{p}|p)}$. *Se $K/\mathbb{Q}$ é Galois, então* $\mathrm{Frob}_{\mathfrak{p}|p} = \mathrm{Frob}_{\mathfrak{P}|p} \mod H$.

Demonstração. Isso segue diretamente da definição:

Para todo $x \in \mathcal{O}_L$, temos

$$\mathrm{Frob}_{\mathfrak{P}|p}^{f(\mathfrak{p}|p)}(x) \equiv x^{|k(\mathfrak{p})|} \mod \mathfrak{P},$$

e portanto temos que ter que $\mathrm{Frob}_{\mathfrak{P}|\mathfrak{p}} = \mathrm{Frob}_{\mathfrak{P}|p}^{f(\mathfrak{p}|p)}$.

Para todo $x \in \mathcal{O}_K$, temos

$$\mathrm{Frob}_{\mathfrak{P}|p}(x) \equiv x^p \mod (\mathfrak{P} \cap \mathcal{O}_K),$$

e como $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, temos que ter que $\mathrm{Frob}_{\mathfrak{P}|p} \mod H = \mathrm{Frob}_{\mathfrak{p}|p}$. □

Exemplo 5.14. Seja p um primo ímpar. Seja $L = \mathbb{Q}[\zeta_p]$. Como $G_L = (\mathbb{Z}/p\mathbb{Z})^\times$ é cíclico, existe um único corpo quadrático K dentro de L. Como o único primo ramificado em L é p, temos que ter que $K = \mathbb{Q}[\sqrt{p}]$ ou $K = \mathbb{Q}[\sqrt{-p}]$. Para 2 não ser ramificado, temos que ter $\pm p \equiv 1 \mod 4$. Ou seja, considere $p^* = (-1)^{(p-1)/2}p$, de modo que $K = \mathbb{Q}[\sqrt{p^*}] \subseteq L$. Pela teoria de Galois, K corresponde ou subgrupo H de G_L que corresponde aos resíduos quadráticos módulo p. Portanto, se $q \neq p$ e $q \neq 2$ temos que

$$\left(\frac{p^*}{q}\right) = \mathrm{Frob}_{q,K} = (\mathrm{Frob}_{q,L} \mod H) = (q \mod H).$$

Ou seja,

$$\left(\frac{p^*}{q}\right) = 1 \iff q \in H \iff \left(\frac{q}{p}\right) = 1,$$

que é exatamente a reciprocidade quadrática. Para $q = 2$, o mesmo argumento nos dá que

$$x^2 + x + \frac{1 - p^*}{4} \text{ tem raiz módulo } 2 \iff \left(\frac{2}{p}\right) = 1,$$

e observe que o lado esquerdo é se e somente se $2 \mid (p^* - 1)/4$, ou seja, se e somente se $p \equiv \pm 1 \mod 8$.

Exemplo 5.15. Seja $K = \mathbb{Q}[\alpha]$ com $\alpha^3 - 3\alpha + 1 = 0$. Então podemos pegar $\alpha = \zeta_9 + \zeta_9^{-1}$, e em particular, $K \subseteq L := \mathbb{Q}[\zeta_9]$. Como $\dim_K L = \phi(9)/3 = 2$, temos $K = L^H$ para um subgroup de tamanho 2 de $G_L = (\mathbb{Z}/9\mathbb{Z})^\times$. A única possibilidade é $H = \{\pm 1\}$. Então, se $p \neq 3$, ele é não-ramificado e portanto

$$\mathrm{Frob}_{p,K} = (\mathrm{Frob}_{p,L} \mod H) = (p \mod H).$$

Ou seja, $\mathrm{Frob}_{p,K} = 1 \iff p \equiv \pm 1 \mod 9$. Pelo algoritmo de fatoração, temos que $\mathrm{Frob}_{p,K} = 1 \iff f = 1 \iff x^3 - 3x + 1$ tem raiz módulo p. Ou seja, para $p \neq 3$, temos

$$p \mid a^3 - 3a + 1 \text{ para algum } a \iff p \equiv \pm 1 \mod 9.$$

Exemplo 5.16. Crie seu próprio problema estilo 6 da OBM 2017: i) escolha seu módulo favorito n, ii) escolha seu subgrupo favorito $H \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$, iii) H corresponde a $\mathbb{Q}[\zeta_n]^H$, e $\alpha = \sum_{i\in H} \zeta_n^i$ é um elemento primitivo, e seja $f(x)$ seu polinômio minimal, iv) compute $\operatorname{disc}(f)$.

Como $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = \sqrt{|\operatorname{disc}(f)/D_K|}$ divide $\operatorname{disc}(f)$, você criou o seguinte problema: para todo $p \nmid \operatorname{disc}(f)N$, temos que

$$p \mid f(a) \text{ para algum } a \iff (p \mod n) \in H.$$

Por exemplo, $p \mid a^4 + 3a^2 + 1$ para algum a se e somente se $p = 5$ ou $p \equiv 1, 9 \mod 20$.

5.2. **Aplicações a funções zeta.** Seja L/K uma extensão Galois de corpos numéricos. Assuma que $\operatorname{Gal}(L/K)$ é abeliano.

Para um caracter $\chi : G \to \mathbb{C}^\times$ e um ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, definimos $\chi(\mathfrak{a})$ do seguinte modo: para um primo $\mathfrak{p}$, se $I_\mathfrak{p} \subseteq \ker(\chi)$, então definimos $\chi(\mathfrak{p}) = \chi(\operatorname{Frob}_\mathfrak{p})$ (note que em geral $\operatorname{Frob}_\mathfrak{p} \in D_\mathfrak{p}/I_\mathfrak{p}$, e então $\chi(\operatorname{Frob}_\mathfrak{p})$ é bem definido); caso contrário, dizemos que $\chi(\mathfrak{p}) = 0$. Extendemos χ multiplicativamente.

Vamos provar o seguinte:

Teorema 5.17. *Se L/K é uma extensão abeliana, então*

$$\zeta_L(s) = \prod_{\chi :\, G \to \mathbb{C}^\times} \zeta_K(s, \chi)$$

onde

$$\zeta_K(s, \chi) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_K} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}.$$

Demonstração. Como $\zeta_K(s, \chi) = \prod_\mathfrak{p} (1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}$, basta checarmos a fórmula primo por primo. Do lado esquerdo, temos

$$\prod_{\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L} (1 - N(\mathfrak{P})^{-s})^{-1} = (1 - N(\mathfrak{p})^{-fs})^{-g}.$$

Do lado direito, temos

$$\prod_{\chi :\, G \to \mathbb{C}^\times} (1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1} = \prod_{\chi :\, G/I_\mathfrak{p} \to \mathbb{C}^\times} (1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1} = \prod_{\chi :\, D_\mathfrak{p}/I_\mathfrak{p} \to \mathbb{C}^\times} (1 - \chi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-g} =$$
$$= \prod_{k=0}^{f-1} (1 - e^{2\pi i k/f} N(\mathfrak{p})^{-s})^{-g} = (1 - N(\mathfrak{p})^{-fs})^{-g}.$$

□

Exemplo 5.18. Se consideramos $\mathbb{Q}[\zeta_N]/\mathbb{Q}$, então temos

$$\zeta_{\mathbb{Q}[\zeta_N]}(s) = \prod_{\chi \in S} L(s, \chi)$$

onde S é o conjunto de caracteres de Dirichlet primitivos de condutor dividindo N, ou seja, caracteres $\chi\colon (\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}^\times$ para $M \mid N$ que não fatoram como $(\mathbb{Z}/M\mathbb{Z})^\times \to (\mathbb{Z}/M_0\mathbb{Z})^\times \to \mathbb{C}^\times$ para nenhum $M_0 \mid M$ com $M_0 \neq M$. E $L(s,\chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}$ onde $\chi(n) = 0$ se $(n, M) \neq 1$.

Para ver isso, se $N = p^k N_0$ com $p \nmid N_0$, então $(\mathbb{Z}/N\mathbb{Z})^\times = (\mathbb{Z}/p^k\mathbb{Z})^\times \times (\mathbb{Z}/N_0\mathbb{Z})^\times$, e $K = \mathbb{Q}[\zeta_N]$ é o compósito de $\mathbb{Q}[\zeta_{p^k}]$ e $\mathbb{Q}[\zeta_{N_0}]$. Então $I_p = (\mathbb{Z}/p^k\mathbb{Z})^\times \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$, ou seja, $\chi(p)$ é diferente de 0 se p não divide o condutor de χ.

Nota 5.19. Se $\mathrm{Gal}\,(L/K)$ não é abeliano, ainda assim existe uma fórmula parecida:

$$\zeta_L(s) = \prod_{\rho\colon G \to \mathrm{GL}(V)} L(s,\rho)^{\dim V}$$

onde ρ percorre pelas *representações irredutíveis* de $\mathrm{Gal}\,(L/K)$, e $L(s,\rho)$ é a *função L de Artin*, definida como

$$L(s,\rho) = \prod_{\mathfrak{p}} \det(1 - N(\mathfrak{p})^{-s} \rho(\mathrm{Frob}_\mathfrak{p}) | V^{I_\mathfrak{p}})^{-1}.$$

Não iremos definir exatamente o que a fórmula acima de fato significa, mas temos o exemplo que segue.

Exemplo 5.20. Se $K = \mathbb{Q}[2^{1/3}, \omega]$, então $G_K = S_3$, gerado por $x, y \in G_K$. Então temos 3 representações irredutíveis: o caracter trivial, o caracter $\chi\colon S_3 \to S_3/A_3 \simeq \{\pm 1\}$, e a representação $\rho\colon S_3 \to \mathrm{GL}_2(\mathbb{C})$ é dada por

$$\rho(x) = \begin{pmatrix} \cos(2\pi/3) & -\sin(2\pi/3) \\ \sin(2\pi/3) & \cos(2\pi/3) \end{pmatrix} \quad \text{e} \quad \rho(y) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Como A_3 é o grupo de Galois de $K/\mathbb{Q}[\omega]$, o caracter χ é simplesmente dado por $\chi(p) = \left(\frac{p}{3}\right)$.

$$\zeta_K(s) = \zeta(s) L(s,\chi) L(s,\rho)^2.$$

Para entender $L(s,\rho)$, temos que calcular que se $p \nmid 6$,

$$\begin{aligned} \mathrm{Frob}_{\mathfrak{p}} = 1 &\iff p \equiv 1 \mod 3 \text{ e 2 é uma raiz cúbica,} \\ \mathrm{Frob}_{\mathfrak{p}} \in \{y, xy, x^2y\} &\iff p \not\equiv 1 \mod 3, \\ \mathrm{Frob}_{\mathfrak{p}} \in \{x, x^2\} &\iff p \equiv 1 \mod 3 \text{ e 2 não é uma raiz cúbica.} \end{aligned}$$

e então

$$L(s,\rho) = (1-3^{-s})^{-1} \prod_{\substack{p \equiv -1 \mod 3 \\ \text{ímpar}}} (1-p^{-2s})^{-1} \prod_{\substack{p \equiv 1 \mod 3 \\ \text{2 res cúbico}}} (1-p^{-s})^{-2} \prod_{\substack{p \equiv 1 \mod 3 \\ \text{2 não res cúbico}}} (1+p^{-s}+p^{-2s})^{-1}.$$

Se tivéssemos somente finitos primos p com 2 não sendo resíduo cúbico, daí teríamos que $L(s,\rho) = \zeta(s)L(s,\chi)R(s)$ onde

$$R(s) = (1-2^{-2s}) \prod_{\text{2 não res cúbico mod } p} \frac{(1-p^{-s})^2}{1+p^{-s}+p^{-2s}}$$

mas daí $\zeta_K(s) = \zeta(s)^3 L(s,\chi)^3 R(s)^2$, o que não pode ser verdade pela fórmula do número de classe pois $R(1) \neq 0$. Portanto, existem infinitos primos p tal que 2 não é um resíduo cúbico módulo p.

Exercícios

Dicas estão no rodapé.

(1) Corpos biquadráticos. Sejam n, m livre de quadrados, e $n \neq m$. Considere $L = \mathbb{Q}[\sqrt{n}, \sqrt{m}]$.
   (a) Prove que $L/\mathbb{Q}$ é Galois, e que $\mathrm{Gal}\,(L/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   (b) Descreva a correspondência de Galois para $L/\mathbb{Q}$.
   (c) Sejam K_1, K_2, K_3 os três corpos quadráticos do item anterior. Descreva como $p\mathcal{O}_L$ fatora em função das fatorações de $p\mathcal{O}_{K_i}$ para $i = 1, 2, 3$.[22]

(2) Primos da forma $a^2 + 5b^2$. Seja $K = \mathbb{Q}[\sqrt{-5}]$.
   (a) Prove que $p = a^2 + 5b^2$ para algum a, b se e somente se $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ com $[\mathfrak{p}_1] = 1 \in \{\pm 1\} \simeq \mathrm{Cl}(K)$.
   (b) Seja $L = \mathbb{Q}[\sqrt{-5}, i]$. Prove que $\mathrm{Cl}(L) = 1$, e use isso para provar que se $\mathfrak{p} \subseteq \mathcal{O}_K$, então $\mathrm{Frob}_{\mathfrak{p},L} = 1 \implies [\mathfrak{p}] = 1$.[23]
   (c) Conclua que se $\mathrm{Frob}_{p,L} = 1$, então $p = a^2 + 5b^2$. Use que $L \subseteq \mathbb{Q}[\zeta_{20}]$ para caracterizar tais p em termos de congruências módulo 20. Depois disso, volte para (b) e veja que se fato $\mathrm{Frob}_{\mathfrak{p},L} = 1 \iff [\mathfrak{p}] = 1$. Ou seja, $\mathrm{Cl}(K) \xrightarrow{\sim} \mathrm{Gal}\,(L/K)$, onde $[\mathfrak{p}] \mapsto \mathrm{Frob}_{\mathfrak{p}}$. (Tal L é chamado de o *corpo de classe de Hilbert* de K, e existe para todo K, mas isso é bem difícil.)

(3) Repita o mesmo procedimento do item anterior para os três casos $\mathbb{Q}[\sqrt{-6}] \subset \mathbb{Q}[\sqrt{-6}, \sqrt{2}]$, $\mathbb{Q}[\sqrt{-10}] \subset \mathbb{Q}[\sqrt{-10}, \sqrt{-2}]$ e $\mathbb{Q}[\sqrt{-13}] \subset \mathbb{Q}[\sqrt{-13}, \sqrt{-1}]$. Com isso, você conseguirá descrever todos os primos da forma $a^2 + kb^2$ para $k \leq 13$. O caso $k = 14$ é mais complicado pois $|\mathrm{Cl}(\mathbb{Q}[\sqrt{-14}])| = 4$.

[22] Descreva $D_{p,L}$ em termos de D_{p,K_i} e $I_{p,L}$ em termos de I_{p,K_i}.
[23] Se $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$ e $\mathfrak{p}_1 = (\alpha)$, daí $\mathfrak{p}_2 = (\sigma(\alpha))$ onde $\sigma \in \mathrm{Gal}\,(L/K)$.

6. 10 de Abril

Hoje vamos discutir o básico de análise complexa, e usá-lo para começar o estudo de funções como $\zeta(s), \zeta_K(s)$ e $L(s,\chi)$.

6.1. **Integral de contorno.** Primeiro vamos generalizar a noção de integral para o plano complexo. Normalmente, se $a < b \in \mathbb{R}$, a integral $\int_a^b f(x)\ \mathrm{d}x$ de uma função contínua f é o limite de somas da forma

$$\sum_{i=1}^{k}(a_i - a_{i-1})f(c_i)$$

onde $a = a_0 < \cdots < a_k = b$ e $c_i \in [a_{i-1}, a_i]$, com limite sendo tomado quando $\max_i(a_i - a_{i-1}) \to 0$.

No plano complexo, não existe uma única maneira de irmos de z até w, então a integral será sobre curvas.

Definição 6.1. Uma *curva* é uma função $\gamma\colon [a,b] \to \mathbb{C}$ tal que existem $a = a_0 < \ldots < a_n = b$ tal que $\gamma\colon [a_i, a_{i+1}] \to \mathbb{C}$ são suaves.

Definição 6.2. Se $\gamma\colon [a,b] \to \mathbb{C}$ é suave, $\Omega \subseteq \mathbb{C}$ é aberto contendo γ e $f\colon \Omega \to \mathbb{C}$ é contínua, a *integral de contorno*

$$\int_\gamma f(z)\ \mathrm{d}z$$

é o limite de somas

$$\sum_{i=1}^{k}(\gamma(a_i) - \gamma(a_{i-1})f(\gamma(c_i))$$

onde $a = a_0 < \ldots < a_k = b$ e $c_i \in [a_{i-1}, a_i]$, com limite sendo tomado quando $\max_i(|\gamma(a_i) - \gamma(a_{i-1})|) \to 0$.

Se γ é uma curva, então definimos

$$\int_\gamma f(z)\ \mathrm{d}z := \sum_{i=1}^{n}\int_{\gamma|_{[a_{i-1},a_i]}} f(z)\ \mathrm{d}z$$

Proposição 6.3. *Se $\gamma\colon [a,b] \to \mathbb{C}$ é suave, temos*

$$\int_\gamma f(z)\ \mathrm{d}z = \int_a^b f(\gamma(t))\gamma'(t)\ \mathrm{d}t.$$

O principal objeto de estudo será a seguinte classe de funções:

Definição 6.4. Para $\Omega \subseteq \mathbb{C}$ um subconjunto aberto, dizemos que uma função $f\colon \Omega \to \mathbb{C}$ é *holomórfica* se f é derivável nos complexos. Ou seja, se para todo $z_0 \in \Omega$, temos que o limite

$$f'(z_0) := \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0} \quad \text{existe.}$$

Exemplo 6.5. Polinômios são holomórficos. Séries também. $1/s$ é holomórfico em $\mathbb{C} - \{0\}$.

Exemplo 6.6. $\zeta(s) = \sum_{n \geq 1} n^{-s}$ é holomórfico para $\operatorname{Re}(s) > 1$. De fato, para $\operatorname{Re}(s) > 1$ essa soma converge absolutamente, e temos

$$\frac{\zeta(s+h) - \zeta(s)}{h} = \sum_{n \geq 1} \frac{n^{-(s+h)} - n^{-s}}{h} = \sum_{n \geq 0} n^{-s} \left(\frac{n^{-h} - 1}{h} \right).$$

Como $n^{-h} - 1 = e^{-h \log n} - 1 = -h \log n + O(h^2 (\log n)^2)$, temos

$$\frac{\zeta(s+h) - \zeta(s)}{h} = \sum_{n \geq 1} \left(-n^{-s} \log n + n^s \cdot O(h (\log n)^2) \right).$$

Como $\sum_{n \geq 1} \frac{(\log n)^2}{n^s}$ converge absolutamente para $\operatorname{Re}(s) > 1$, temos que $\zeta'(s) = \sum_{n \geq 0} \frac{\log n}{n^s}$ para $\operatorname{Re}(s) > 1$. Portanto, ζ é holomórfica para $\operatorname{Re}(s) > 1$.

Uma aplicação imediata do teorema fundamental do cálculo é o seguinte.

Proposição 6.7. *Se f é holomórfica, então $\int_\gamma f'(z)\ \mathrm{d}z = f(\gamma(b)) - f(\gamma(a))$.*

Em particular, se f possui uma primitiva, então $\int_\gamma f(z)\ \mathrm{d}z = 0$ para todo γ fechado.

Teorema 6.8 (Goursat)**.** *Seja γ um triângulo e $f\colon \Omega \to \mathbb{C}$ holomórphica onde Ω contém γ e seu interior. Então $\int_\gamma f(z)\ \mathrm{d}z = 0$.*

Demonstração. Divida o triângulo em quatro triângulos $\gamma_1, \ldots, \gamma_4$ pelas bases médias, com a mesma orientação de γ. Então

$$\left| \int_\gamma f(z)\ \mathrm{d}z \right| \leq \sum_{i=1}^{4} \left| \int_{\gamma_i} f(z)\ \mathrm{d}z \right|,$$

portanto existe $\gamma^1 = \gamma_i$ tal que

$$\left| \int_\gamma f(z)\ \mathrm{d}z \right| \leq 4 \left| \int_{\gamma^1} f(z)\ \mathrm{d}z \right|.$$

Continuando da mesma maneira, existem γ^n tal que

$$\left|\int_\gamma f(z)\ \mathrm{d}z\right| \leq 4^n \left|\int_{\gamma^n} f(z)\ \mathrm{d}z\right|.$$

Escolhemos γ^n tal que estejam dentro de γ^{n-1}, e portanto existe um único ponto z_0 no interior ou na borda de γ tal que z_0 está no interior de todo γ^n. Escreva

$$f(z) = f(z_0) + (z - z_0)(f'(z_0) + h(z))$$

onde $\lim_{z\to z_0} h(z) = 0$. Para $\epsilon > 0$, considere $\delta > 0$ tal que $|z - z_0| < \delta \implies |h(z)| < \epsilon$. Se n é tal que γ^n está dentro de $|z - z_0| < \delta$, daí

$$\begin{aligned}\left|\int_\gamma f(z)\ \mathrm{d}z\right| \leq 4^n \left|\int_{\gamma^n} f(z)\ \mathrm{d}z\right| &= 4^n \left|\int_{\gamma^n} f(z_0) + (z - z_0)f'(z_0) + (z - z_0)h(z)\ \mathrm{d}z\right| \\ &= 4^n \left|\int_{\gamma^n} (z - z_0)h(z)\ \mathrm{d}z\right| \leq 4^n \mathrm{per}(\gamma^n)\mathrm{dia}(\gamma^n)\epsilon.\end{aligned}$$

Onde per e dia denotam perímetro e diâmetro. Como $4^n\mathrm{per}(\gamma^n)\mathrm{dia}(\gamma^n)\epsilon = \mathrm{per}(\gamma)\mathrm{dia}(\gamma)\epsilon$, tomando $\epsilon \to 0$ termina a prova. □

Teorema 6.9. *Seja $f\colon \Omega \to \mathbb{C}$ uma holomórfica e assuma que Ω "não tem buracos"[24]. Então f possui uma primitiva.*

Demonstração. Escolha $z_0 \in \Omega$. Para qualquer $z_1 \in \Omega$, podemos achar γ poligonal conectando z_0 e z_1, e definimos $F(z_1) = \int_\gamma f(z)\ \mathrm{d}z$. Pelo teorema anterior, tal definição não depende de γ. Agora se h é suficientemente pequeno,

$$\frac{F(z_1 + h) - F(z_1)}{h} = \frac{\int_\gamma f(z)\ \mathrm{d}z}{h} = f(z_1) + \frac{1}{h}\int_\gamma (f(z) - f(z_1))$$

onde γ é a reta conectando z_1 a $z_1 + h$. Note que quando $h \to 0$, o último termo tende a 0 pois f é contínua em z_1. Isso prova que $F'(z_1) = f(z_1)$. □

Corolário 6.10. *Seja $f\colon \Omega \to \mathbb{C}$ holomórfica e γ uma curva em Ω que é a borda de uma região sem buracos. Então $\int_\gamma f(z)\ \mathrm{d}z = 0$.*

Exemplo 6.11. É necessário que f seja holomórfica no interior da curva: considere $f(z) = 1/z$, e seja γ o círculo unitário. Então

$$\int_\gamma \frac{1}{z}\ \mathrm{d}z \int_\gamma f(z)\ \mathrm{d}z = \int_0^{2\pi} f(e^{it})ie^{it}\ \mathrm{d}t = \int_0^{2\pi} i\ \mathrm{d}t = 2\pi i.$$

[24]Mais específicamente, Ω é *simplesmente conectado.*

6.2. **Funções holomórficas são analíticas.** Do exemplo acima, obtemos a seguinte fórmula:

Teorema 6.12 (Fórmula integral de Cauchy)**.** *Seja $f\colon \Omega \to \mathbb{C}$ holomórfica, e seja $\gamma \subseteq \Omega$ um círculo. Para z_0 no interior de γ, temos que*

$$f(z_0) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z - z_0}\, \mathrm{d}z.$$

Demonstração. Como $f(z)/(z - z_0)$ é holomórfica em $\Omega - \{z_0\}$, podemos trocar γ por qualquer círculo contendo z_0 no interior. Tomando esse círculo para ter raio ϵ e tomando $\epsilon \to 0$, a fórmula basicamente segue to fato que $\int_\gamma \frac{1}{z}\, \mathrm{d}z = 2\pi i$. □

Teorema 6.13. *Se $f\colon \Omega \to \mathbb{C}$ é holomórfica, então f é infinitamente direferenciável. Além disso, se $\gamma \subseteq \Omega$ é um círculo e z_0 está no interior de γ, temos*

$$f^{(k)}(z_0) = \frac{k!}{2\pi i} \int_\gamma \frac{f(z)}{(z - z_0)^{k+1}}\, \mathrm{d}z.$$

Demonstração. Indução em k. O caso $k = 1$ é a fórmula acima.

Então assuma que $f^{(k-1)}(z_0) = \frac{(k-1)!}{2\pi i} \int_\gamma \frac{f(z)}{(z-z_0)^k}\, \mathrm{d}z$. Então para h suficientemente pequeno tal que h está dentro de γ, temos

$$\frac{f^{(k-1)}(z_0 + h) - f^{(k-1)}(z_0)}{h} = \frac{(k-1)!}{2\pi i} \int_\gamma \frac{f(z)}{h} \left(\frac{1}{(z - z_0 - h)^k} - \frac{1}{(z - z_0)^k} \right) \mathrm{d}z.$$

Seja $a = (z - z_0 - h)^{-1}$ e $b = (z - z_0)^{-1}$. Então quando $h \to 0$, temos $a \to b$. Então $\frac{a^k - b^k}{a - b} \to k a^{n-1}$. Como $\frac{1}{a-b} = \frac{h}{(z-z_0-h)(z-z_0)}$, concluímos que

$$f^{(k)}(z_0) = \frac{(k-1)!}{2\pi i} \int_\gamma \frac{f(z)}{(z - z_0)^2} \frac{k}{(z - z_0)^{k-1}}\, \mathrm{d}z,$$

o que conclui a indução. □

Corolário 6.14. *Se $f\colon \Omega \to \mathbb{C}$ é holomórfica que contém um círculo γ de raio R de centro z_0, então*

$$|f^{(k)}(z_0)| \leq \frac{k! \cdot \sup_\gamma |f(z)|}{R^k}.$$

Demonstração. Segue diretamente da fórmula acima. □

Exemplo 6.15. Uma aplicação é o *teorema de Liouville*: se $f\colon \mathbb{C} \to \mathbb{C}$ é holomórfica e limitada, então f é constante. Simplesmente tome $k = 1$ e $R \to \infty$. Podemos com isso provar o teorema fundamental da álgebra: Seja $P(z)$ um polinômio sem raízes. Então $1/P(z)$ é limitado e holomórfico, portanto é constante, e portanto $P(z)$ é constante.

Teorema 6.16. *Se $f\colon \Omega \to \mathbb{C}$ é holomórfica que contém um círculo γ de raio R de centro z_0, então para z dentro de γ, temos*

$$f(z) = \sum_{n\geq 0} a_n (z - z_0)^n$$

onde $a_n = f^{(n)}(z_0)/n!$.

Demonstração. O corolário acima diz que de fato o lado direito converge absolutamente. Escreva

$$\frac{1}{z - z_1} = \frac{1}{z - z_0} \frac{1}{1 - \frac{z_1 - z_0}{z - z_0}} = \frac{1}{z - z_0} \sum_{n\geq 0} \left(\frac{z_1 - z_0}{z - z_0} \right)^n$$

e então

$$f(z_1) = \frac{1}{2\pi i} \int_\gamma \frac{f(z)}{z - z_1}\, \mathrm{d}z = \sum_{n\geq 0} \frac{(z_1 - z_0)^n}{2\pi i} \int_\gamma \frac{f(z)}{(z - z_0)^{n+1}}\, \mathrm{d}z = \sum_{n\geq 0} a_n (z_1 - z_0)^n.$$

□

Ou seja, funções holomórficas são automaticamente analíticas. Uma propriedade de funções analíticas é o seguinte:

Proposição 6.17. *Seja $f\colon \Omega \to \mathbb{C}$ holomórfica, onde Ω é conectado. Se $f(z_i) = 0$ onde $z_i \to z_0 \in \Omega$, então $f = 0$.*

Demonstração. Considere $f(z) = \sum_{n\geq 0} a_n (z - z_0)^n$. Se f não é identicamente igual a 0 perto de z_0, então algum $a_n \neq 0$. Podemos trocar f por $f_0(z) = f(z)/(z - z_0)^n$ para algum n de modo que ainda é holomórfica e de modo que $a_0 \neq 0$. Mas f_0 é contínua, e de $f_0(z_i) = 0$ concluiríamos que $f_0(z_0) = 0$, o que é uma contradição.

Portanto f é 0 em uma bola perto de z_0. Repetindo o mesmo argumento para sequências de pontos na borda dessa bola e assim por diante, pode-se argumentar que porque Ω é conectado, temos que ter $f = 0$. □

Ou seja, se uma função $f\colon \Omega \to \mathbb{C}$ é holomórfica, existe no máximo uma maneira de extender f para uma função $f\colon \Omega' \to \mathbb{C}$ onde $\Omega \subseteq \Omega'$ que ainda seja holomórfia com Ω' conectado.

Eventualmente vamos provar que ζ extende para uma função holomórfica em $\mathbb{C} - \{1\}$. Ela terá uma singularidade em $s = 1$. Como preparação para isso, vamos falar sobre os tipos de singularidade.

6.3. **Singularidades.** Seja $f\colon \Omega \to \mathbb{C}$ uma função holomórfica e $z \notin \Omega$ mas tal que existe um disco D de centro z tal que $D - \{z\} \subseteq \Omega$. É comum considerarmos três tipos de singularidade:

Definição 6.18. Dizemos que z é uma *singularidade removível* se f pode ser extendida para uma função holomórfica sobre $\Omega \cup \{z\}$. Dizemos que z é um *pólo* se $1/f$ é holomórfica perto de z, e se $1/f$ pode ser extendida para uma função g incluindo z com $g(z) = 0$. Se g tem um zero de ordem n, dizemos que z é um pólo de ordem n. Caso contrário, dizemos que z é uma *singularidade essencial*.

Proposição 6.19. *z_0 é um pólo de ordem m se e somente se f é da seguinte forma perto de z_0.*

$$f(z) = \sum_{n \geq -m} a_n (z - z_0)^n$$

com $a_{-m} \neq 0$. Dizemos que o resíduo *de f em z_0 é* $\operatorname{res}_{z_0}(f) := a_{-1}$.

Demonstração. Segue de que podemos expandir $1/f$ como uma serie de Taylor. □

Definição 6.20. Se $f\colon \Omega - \{a_1, \ldots, a_n\} \to \mathbb{C}$ é holomórfica e $a_1, \ldots, a_n$ são pólos, dizemos que f é *meromórfica* em Ω.

Pelas fórmulas de Cauchy, temos que se γ é um círculo em volta de 0 e $k \geq 1$, então

$$\frac{1}{2\pi i} \int_\gamma \frac{a_{-k}}{z^k} \, \mathrm{d}z = \begin{cases} a_{-1} & \text{se } k = 1, \\ 0 & \text{se } k > 1. \end{cases}$$

O seguinte teorema segue imediatamente:

Teorema 6.21 (Fórmula dos resíduos)**.** *Se $f\colon \Omega \to \mathbb{C}$ é meromórfica, e γ é uma curva que não passa por nenhum pólo, então*

$$\int_\gamma f(z) \, \mathrm{d}z = 2\pi i \sum_{z_0} \operatorname{res}_{z_0}(f)$$

onde a soma percorre todos os pólos no interior de γ.

Exemplo 6.22. Vamos provar que $\zeta(s)$ extende para uma função meromórfica em $\operatorname{Re}(s) > 0$ com um pólo simples (ou seja, de ordem 1) em $s = 1$ com resíduo 1. Para isso, escreva $\zeta(s) = \frac{1}{s-1} + \phi(s)$.

Como $\frac{1}{s-1} = \int_1^\infty x^{-s}\,\mathrm{d}x$, podemos escrever, para $\mathrm{Re}(s) > 1$, que

$$\phi(s) = \sum_{n\geq 1}\left(\frac{1}{n^s} - \int_n^{n+1} x^{-s}\,\mathrm{d}x\right) = \sum_{n\geq 1}\int_n^{n+1}\left(n^{-s} - x^{-s}\right)\,\mathrm{d}x.$$

Agora note que se $\mathrm{Re}(s) > 0$, pelo teorema do valor médio temos que

$$(x^{-s} - n^{-s}) = -(x-n)sx_0^{-s-1} \text{ para algum } x_0 \in [n, x_0],$$

e portanto

$$\left|\int_n^{n+1}(n^{-s} - x^{-s})\,\mathrm{d}x\right| \leq \frac{|s|}{n^{\mathrm{Re}(s)+1}}.$$

Portanto, $\phi(s)$ é absolutamente convergente se $\mathrm{Re}(s) > 0$. Falta ver que $\phi(s)$ é holomórfica. Isso segue da convergência absoluta acima, e de que

$$\sum_{n\geq 1}\left(\frac{1}{n^s} - \int_n^{n+1} x^{-s}\,\mathrm{d}x\right)' = \sum_{n\geq 1}\left(-\frac{s\log n}{n^{s+1}} + s\int_n^{n+1}\frac{\log x}{x^{s+1}}\,\mathrm{d}x\right),$$

e podemos ver que isso converge absolutamente com um argumento parecido ao anterior.

Portanto $\frac{1}{s-1} + \phi(s)$ é uma extensão meromórfica de $\zeta(s)$ para $\mathrm{Re}(s) > 0$ com um pólo simples de resíduo 1 em $s = 1$.

Exemplo 6.23. Dado o acima, para um corpo numérico K, basicamente provamos anteriormente que $\zeta_K(s)$ é meromórfica em $\mathrm{Re}(s) > 1 - \frac{1}{n}$, com pólo simples em $s = 1$ com resíduo

$$\mathrm{res}_{s=1}\zeta_K(s) = \frac{2^r(2\pi)^s\mathrm{Reg}(K)|\mathrm{Cl}(K)|}{|\mu_K|\sqrt{|D_K|}}.$$

Essa é a fórmula do número de classe.

Exercícios

(1) Prove que $\int_0^\infty \cos(x^2)\ \mathrm{d}x = \int_0^\infty \sin(x^2)\ \mathrm{d}x = \sqrt{2\pi}/4$.[25]

(2) Calcule $\int_{-\infty}^{\infty} \frac{1}{1+x^4}\ \mathrm{d}x$

(3) Suponha que $u \notin \mathbb{Z}$. Prove que

$$\sum_{n\in\mathbb{Z}} \frac{1}{(u+n)^2} = \frac{\pi^2}{\sin(\pi u)^2}$$

integrando $f(z) = \frac{\pi \cot \pi z}{(u+z)^2}$ sobre círculos $|z| = N + 1/2$ para $N \geq |u|$ um inteiro, e tome $N \to \infty$.[26]

[25]Olhe na página 64 do livro de análise complexa do Stein para uma dica.

[26]Os pólos de $\cot \pi z$ são os zeros de $\sin \pi z = \frac{e^{i\pi z} - e^{-i\pi z}}{2i}$, que são $z \in \mathbb{Z}$, e são todos simples.

7. 17 de Abril

7.1. **Logaritmo.** O último ingrediente que falta para finalmente provarmos Dirichlet é o logaritmo complexo.

Definição 7.1. Seja $f\colon \Omega \to \mathbb{C}$ holomórfica que não possui zeros. Dizemos que $g\colon \Omega \to \mathbb{C}$ é um *logaritmo* de f se $f(z) = e^{g(z)}$ para todo $z \in \Omega$.

Exemplo 7.2. Note que $f(z)\colon \mathbb{C} - \{0\} \to \mathbb{C}$ dado por $f(z) = z$ não possui logaritmo. Se g é um logaritmo, então ao dar a volta por 0, o valor de g mudaria por $2\pi i$.

Se g é um logaritmo de f, então $f'(z) = g'(z)e^{g(z)}$, e portanto $g'(z) = f'(z)/f(z)$. Isso nos leva ao seguinte resultado:

Teorema 7.3. *Seja $f\colon \Omega \to \mathbb{C}$ holomórfica sem zeros onde Ω é uma região sem buracos e conectada. Então f possui um logaritmo g.*

Demonstração. Seja $z_0 \in \Omega$. Para $z_1 \in \Omega$, seja γ conectando z_0 e z_1, e defina

$$g(z_1) = \int_\gamma \frac{f'(z)}{f(z)}\, \mathrm{d}z + c_0$$

onde $e^{c_0} = f(z_0)$.

Isso é bem definido pois Ω não tem buracos. Pela definição, temos que $g'(z) = f'(z)/f(z)$. Agora podemos calcular que

$$(f(z)e^{-g(z)})' = 0,$$

e como $f(z_0) = e^{g(z_0)}$, temos que ter $f(z) = e^{g(z)}$ para todo $z \in \Omega$. □

7.2. **Caracteres de Dirichlet.**

Definição 7.4. Um *caracter de Dirichlet módulo N* é um morfismo de grupos $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$.

Note que se $N = \prod_i p_i^{e_i}$, então pelo TCR,

$$(\mathbb{Z}/N\mathbb{Z})^\times = \prod_i (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times.$$

Como $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ tem uma raiz primitiva, existem $\phi(p_i^{e_i})$ caracteres de Dirichlet módulo $p_i^{e_i}$, e portanto $\phi(N) = \prod_i \phi(p_i^{e_i})$ caracteres de Dirichet módulo N.

Teorema 7.5 (Ortonormalidade de caracteres)**.** *Sejam* $\chi_1, \chi_2 \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ *dois caracteres de Dirichlet. Então*

$$\langle \chi_1, \chi_2 \rangle := \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi_1(a)\overline{\chi_2(a)} = \begin{cases} 0 & \text{se } \chi_1 \neq \chi_2, \\ \phi(N) & \text{se } \chi_1 = \chi_2. \end{cases}$$

Demonstração. Se $\chi := \chi_1 = \chi_2$, então $\chi(a)\overline{\chi(a)} = |\chi(a)|^2 = 1$ pois $\chi(a)$ é uma raiz da unidade, e portanto é claro que $\langle \chi, \chi \rangle = \phi(N)$.

Se $\chi_1 \neq \chi_2$, note que se $b \in (\mathbb{Z}/N\mathbb{Z})^\times$, então

$$\langle \chi_1, \chi_2 \rangle = \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi_1(a)\overline{\chi_2(a)} = \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi_1(ab)\overline{\chi_2(ab)} = \chi_1(b)\overline{\chi_2(b)}\langle \chi_1, \chi_2 \rangle.$$

Em particular, se escolhermos b tal que $\chi_1(b) \neq \chi_2(b)$, isso implica que $\langle \chi_1, \chi_2 \rangle = 0$. □

Corolário 7.6. *Os* $\phi(N)$ *caracteres de Dirichlet módulo* N *formam uma base do espaço vetorial de funções* $\{f \colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}\}$*. Explicitamente,*

$$f = \frac{1}{\phi(N)} \sum_{\chi} \langle f, \chi \rangle \chi.$$

Demonstração. Provamos que os χ são linearmente independentes, e como existem $\phi(N)$ caracteres, eles tem que formar uma base. Então basta ver que a fórmula acima funciona para $f = \chi$, o que segue do teorema. □

7.3. **Funções L de Dirichlet.** Como vimos anteriormente, para um caracter the Dirichlet $\chi \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, podemos associar a função L dada por

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} \quad \text{para } \mathrm{Re}(s) > 1.$$

Onde denotamos $\chi(a) = 0$ se $\mathrm{mdc}(a, N) \neq 1$.

Assim como vimos com a função zeta, é fácil ver que $L(s, \chi)$ é holomórfica.

Proposição 7.7. *Seja* χ *um caracter de Dirichlet não trivial. Então* $L(s, \chi)$ *extende holomórficamente para* $\mathrm{Re}(s) > 0$.

Demonstração. Primeiro, note que como $\langle \chi, 1 \rangle = 0$, temos que $\sum_{n=a}^{a+N} \chi(n) = 0$ para todo a. Portanto, $S_M := \sum_{n=1}^{M} \chi(n)$ é limitado.

Com essa observação, podemos usar a soma por partes: se a_n, b_n são duas sequências e $S_M := \sum_{n=1}^{M} a_n$, então

$$\sum_{n=1}^{M} a_n b_n = S_M b_M - \sum_{n=1}^{M-1} S_n (b_{n+1} - b_n).$$

Portanto para $a_n = \chi(n)$ e $b_n = n^{-s}$, temos para $\mathrm{Re}(s) > 1$ que

$$L(s,\chi) = \lim_{M\to\infty} \sum_{n=1}^{M} a_n b_n = \lim_{M\to\infty} \left(\frac{S_M}{M^s} - \sum_{n=1}^{M-1} S_n((n+1)^{-s} - n^{-s}) \right) = \sum_{n\geq 1} S_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right).$$

Mas agora note que o lado direito converge absoutamente para $\mathrm{Re}(s) > 0$. De fato, como S_n é limitado e como $\frac{1}{(n+1)^s} - \frac{1}{n^s} = -s \int_n^{n+1} x^{-s-1}\, \mathrm{d}x$, seu valor absoluto é no máximo s/n^{s+1}, e $\sum_{n\geq 1} \frac{s}{n^{s+1}}$ converge absolutamente para $\mathrm{Re}(s) > 0$.

Finalmente, é fácil ver que a expressão no lado direito é holomórfica pois cada termo é, e pois temos boa convergência. □

Teorema 7.8. *Para qualquer caracter de Dirichlet χ não trivial, temos $L(1,\chi) \neq 0$.*

Demonstração. Se χ é primitivo, provamos isso anteriormente usando que

$$\zeta_{\mathbb{Q}[\zeta_N]}(s) = \zeta(s) \prod_{\chi} L(s,\chi)$$

onde o produto percorre caracteres de Dirichlet primitivos não-triviais de condutor dividindo N. Pela fórmula do número de classe, sabemos que tanto $\zeta(s)$ quanto $\zeta_{\mathbb{Q}[\zeta_N]}(s)$ tem um pólo simples em $s = 1$, e portanto $\prod_\chi L(s,\chi)$ não é 0 em $s = 1$. Como $L(s,\chi)$ são holomórficas em $s = 1$, temos que $L(1,\chi) \neq 0$.

Em geral, seja $\chi_0 \colon (\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}^\times$ o caracter primitivo associado a $\chi \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, então $M \mid N$. Então para $\mathrm{Re}(s) > 1$, temos

$$L(s,\chi) = \prod_p (1-\chi(p)p^{-s})^{-1} = \prod_{p\nmid N} (1-\chi(p)p^{-s})^{-1} = \prod_{p\nmid N} (1-\chi_0(p)p^{-s})^{-1} = L(s,\chi_0) \prod_{p\mid N, p\nmid M} (1-\chi_0(p)p^{-s}),$$

e portanto isso também tem que ser verdade para $\mathrm{Re}(s) > 0$. Portanto,

$$L(1,\chi) = L(1,\chi_0) \prod_{p\mid N, p\nmid M} \left(1 - \frac{\chi_0(p)}{p}\right)$$

também não é 0. □

7.4. **Teorema de Dirichlet.**

Definição 7.9. Dizemos que um conjunto de primos S tem *densidade de Dirichlet* μ se

$$\mu = \lim_{s\to 1^+} \frac{\sum_{p\in S} p^{-s}}{\sum_p p^{-s}}.$$

Nota 7.10. Pode-se provar que se S tem densidade natural

$$\mu = \lim_{N\to\infty} \frac{|S \cap [1, N]|}{N},$$

daí também tem densidade de Dirichlet μ.

Teorema 7.11. *Seja* $\text{mdc}(a, N) = 1$ *e* $S = \{p\colon p \equiv a \mod N\}$. *Então* S *tem densidade de Dirichlet* $1/\phi(N)$. *Em particular,* S *é infinito.*

Demonstração. A ideia é considerar

$$-\sum_p \log(1 - \chi(p)p^{-s}) = \sum_p \frac{\chi(p)}{p^s} + \sum_{n\geq 2}\sum_p \frac{\chi(p^n)}{p^{ns}} = \sum_p \frac{\chi(p)}{p^s} + O(1).$$

Isso, formalmente, seria $\log L(s, \chi)$, mas temos que tomar cuidado para afirmar isso.

Se $|z| < 1$, podemos considerar $\log(1 - z) = -\sum_{n\geq 1} \frac{z^n}{n}$. Para $\text{Re}(s) > 1$, temos que $|p^{-s}| < 1$, então podemos considerar a expressão acima $l(s, \chi) = -\sum_p \log(1 - \chi(p)p^{-s})$. Isso é holomórfica para $\text{Re}(s) > 1$. Pela definição e tomando um pouco de cuidado com convergência, podemos ver que $e^{l(s,\chi)} = L(s, \chi)$. Se χ não é trivial, então como $L(1, \chi) \neq 0$, temos que ter que $\lim_{s\to 1^+} l(s, \chi) \neq 0$, e portanto que $l(s, \chi) = O(1)$ quando $s \to 1^+$.

Pelas considerações acima, então temos que

$$\sum_{p\equiv a \mod N} \frac{1}{p^s} = \sum_p \frac{1}{\phi(N)} \sum_\chi \overline{\chi(a)} \frac{\chi(p)}{p^s}$$

e como isso converge absolutamente para $\text{Re}(s) > 1$, temos

$$\sum_{p\equiv a \mod N} \frac{1}{p^s} = \frac{1}{\phi(N)} \sum_\chi \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^s} = \frac{1}{\phi(N)} \sum_\chi \overline{\chi(a)} l(s, \chi) + O(1)$$

quando $s \to 1^+$.

Mas então, pelo o que vimos acima, temos que

$$\sum_{p\equiv a \mod N} \frac{1}{p^s} = \frac{1}{\phi(N)} l(s, 1) + O(1) = \frac{1}{\phi(N)} \sum_p \frac{1}{p^s} + O(1),$$

o que significa que $S = \{p\colon p \equiv a \mod n\}$ tem densidade de Dirichlet $1/\phi(N)$. □

Exercícios

(1) Seja $S = \{p\colon n \text{ não é resíduo cúbico módulo } p\}$. Considerando $K = \mathbb{Q}[\sqrt[3]{n}, \omega]$, prove que S tem densidade de Dirichlet $1/3$.

Lembre-se que $\zeta_K(s) = \zeta(s)L(s,\chi)L(s,\rho)^2$ onde χ é o caracter de Dirichlet não trivial módulo 3 e

$$L(s,\rho) = C \cdot \prod_{\substack{p \equiv -1 \mod 3 \\ \text{ímpar}}} (1-p^{-2s})^{-1} \prod_{\substack{p \equiv 1 \mod 3 \\ p \notin S}} (1-p^{-s})^{-2} \prod_{p \in S} (1+p^{-s}+p^{-2s})^{-1}$$

onde C é um fator não zero dependendo dos primos $p \mid N$. Use isso para deduzir propriedades anaíticas de $L(s,\rho)$.

(2) Seja χ um caracter de Dirichlet primitivo de módulo N. Seja $G(\chi) := \sum_{a=1}^{N} \chi(a)\zeta^a$ onde ζ é uma raiz N-ésima primitiva da unidade. Prove que $|G(\chi)| = \sqrt{N}$, e que $G(\overline{\chi}) = \chi(-1)\overline{G(\chi)}$.

8. 1 de Maio

Hoje vamos provar o teorema dos números primos: se $\pi(x)$ é a quantidade de primos no máximo x, então

$$\pi(x) \sim \frac{x}{\log x}.$$

8.1. **Zeros da ζ.**

Proposição 8.1. *Se $\sum|a_n|$ converge, então $\prod(1+a_n)$ converge, e é 0 se e somente se algum a_n é -1.*

Demonstração. Podemos considerar somente o caso que $|a_n| < 1/2$. Daí basta ver que $\sum \log(1+a_n)$ converge, e isso segue de $|\log(1+a_n)| \leq 2|a_n|$. □

Com isso, segue facilmente que $\zeta(s)$ não tem zeros para $\mathrm{Re}(s) > 1$. Vamos provar que também não tem zeros para $\mathrm{Re}(s) = 1$.

Lema 8.2. *Se $\sigma > 1$ e $t \in \mathbb{R}$, então*

$$S(\sigma, t) := |\zeta(\sigma)^3 \zeta(\sigma+it)^4 \zeta(\sigma+2it)| \geq 1.$$

Demonstração. Note que $\mathrm{Re}(n^{-s}) = n^{-\sigma}\cos(t\log n)$.

Então

$$\log S(\sigma,t) = 3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma+it)| + \log|\zeta(\sigma+2it)| = \sum_{n\geq 1} c_n n^{-\sigma}(3+4\cos(t\log n)+\cos(2t\log n))$$

se $\log\zeta(s) = \sum_{n\geq 1} c_n n^{-s}$.

Mas $\log\zeta(s) = \sum_p -\log(1-p^{-s}) = \sum_{p,m} p^{-ms}/m$, portanto $c_n \geq 0$. Note que $3 + 4\cos\theta + \cos(2\theta) = 2(1+\cos\theta)^2 \geq 0$, portanto $\log S(\sigma,t) \geq 0$, e então $S(\sigma,t) \geq 1$. □

Corolário 8.3. *Se $\mathrm{Re}(s) = 1$, então $\zeta(s) \neq 0$.*

Demonstração. Suponha que $\zeta(1+it) = 0$. Então temos $\zeta(\sigma+it) = (\sigma-1)f(\sigma+it)$ para f holomórfica perto de $\sigma = 1$. Como $\zeta(\sigma) = \frac{g(\sigma)}{\sigma-1}$ para g holomórfica com $g(1) = 1$, teríamos, para σ próximo de 1, que

$$S(\sigma,t) = (\sigma-1)|g(\sigma)^3 f(\sigma+it)^4 \zeta(\sigma+2it)|.$$

Mas tomando $\sigma \to 1^+$, teríamos $\lim_{\sigma\to 1^+} S(\sigma,t) = 0$, um absurdo com o lema anterior. □

8.2. **Relação com $\pi(x)$.** Vamos ver que o teorema dos números primos é equivalente a ζ não ter zeros com $\mathrm{Re}(s) = 1$.

Para isso, vamos cosiderar a seguinte função

$$\psi(x) = \sum_{p^m \leq x} \log p = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p.$$

Proposição 8.4. $\psi(x) \sim x \iff \pi(x) \sim x/\log x$.

Demonstração. Temos $\psi(x) = \sum_{p \leq x} \lfloor \log x / \log p \rfloor \log p \leq \sum_{p \leq x} \log x = \pi(x) \log x$.

Para a desigualdade no outro sentido, temos para qualquer $0 < \alpha < 1$ que

$$\psi(x) \geq \sum_{p \leq x} \log p \geq \sum_{x^\alpha < p \leq x} \log p \geq (\pi(x) - \pi(x^\alpha)) \log(x^\alpha).$$

Portanto, se $\alpha = 1 - \epsilon$, temos

$$\psi(x) > (1-\epsilon)\pi(x)\log(x) - \frac{\log x}{x^\epsilon}$$ □

Seja $\psi_1(x) = \int_1^x \psi(u)\ \mathrm{d}u$. O seguinte é verdade pois $\psi(x)$ é não-decrescente:

Proposição 8.5. $\psi(x) \sim x \iff \psi_1(x) \sim x^2/2$.

Demonstração. Como ψ é crescente, temos

$$\frac{1}{\epsilon x} \int_{(1-\epsilon)x}^{x} \psi(u)\ \mathrm{d}u \leq \psi(x) \leq \frac{1}{\epsilon x} \int_{x}^{(1+\epsilon)x} \psi(u)\ \mathrm{d}u,$$

portanto

$$\frac{1}{2\epsilon} \frac{2\psi_1(x)}{x^2} - \frac{(1-\epsilon)^2}{2\epsilon} \frac{2\psi_1((1-\epsilon)x)}{(1-\epsilon)^2 x^2} \leq \frac{\psi(x)}{x} \leq \frac{(1+\epsilon)^2}{2\epsilon} \frac{2\psi_1((1+\epsilon)x)}{(1+\epsilon)^2 x^2} - \frac{1}{2\epsilon} \frac{2\psi_1(x)}{x^2}$$

e note que $\frac{1}{2\epsilon} - \frac{(1-\epsilon)^2}{2\epsilon} = 1 - \epsilon/2$ e $\frac{(1+\epsilon)^2}{2\epsilon} - \frac{1}{2\epsilon} = 1 + \epsilon/2$. □

Agora considere

$$\Lambda(n) = \begin{cases} \log p & \text{se } n = p^m, \\ 0 & \text{caso contrário.} \end{cases},$$

de modo que $\psi(x) = \sum_{n \leq x} \Lambda(n)$. Daí temos trivialmente que $\psi_1(x) = \sum_{n \leq x} \Lambda(n)(x-n)$. Note também que, se $\mathrm{Re}(s) > 1$,

$$-\frac{\zeta'(s)}{\zeta(s)} = -(\log \zeta(s))' = -\sum_{m,p} \left(\frac{p^{-ms}}{m} \right)' = \sum_{m,p} (\log p) p^{-ms} = \sum_{n \geq 1} \frac{\Lambda(n)}{n^s}.$$

Proposição 8.6. *Para todo $c > 1$, temos*

$$\psi_1(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{x^{s+1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)\,\mathrm{d}s.$$

Demonstração. Pelas considerações anteriores, basta provar que

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{a^s}{s(s+1)}\,\mathrm{d}s = \begin{cases} 0 & \text{se } 0 < a < 1, \\ 1 - 1/a & \text{se } 1 \leq a. \end{cases}$$

Note que se $f(s) = a^s/s(s+1)$, então $\mathrm{res}_0 f = 1$ e $\mathrm{res}_{-1} f = -1/a$. Então a fórmula acima segue se uma integral de contorno: no primeiro caso, considera o semicírculo para a direita, e no segundo caso, para a esquerda. Basta ver que a integral no semicírculo vai para 0 quando o raio aumenta. Isso é porque $|s(s+1)| \geq R^2/2$ se R é grande, e $|a^s|$ é limitado independentemente de R, pois se $a < 1$, então $\mathrm{Re}(s) \geq c$, e se $a \geq 1$, então $\mathrm{Re}(s) < c$. □

Seja $F(s) = \frac{x^{s+1}}{s(s+1)}\left(-\frac{\zeta'(s)}{\zeta(s)}\right)$. Queremos poder trocar o contorno acima de $c > 1$ para $c = 1$. Como $\zeta(s)$ não tem zeros em $\mathrm{Re}(s) = 1$, o único problema é o pólo em $s = 1$. De fato, $\mathrm{res}_1 F = x^2/2$ é exatamente o termo que queremos.

Para isso de fato functionar, vamos usar a seguinte cota

Lema 8.7. *Fixe $\epsilon > 0 >$ Se $\sigma \geq 1$ e $|t| \geq 1$, com $s = \sigma + it$, temos $|\zeta'(s)/\zeta(s)| \leq C_\epsilon \cdot |t|^\epsilon$ para alguma constante C_ϵ.*

Ideia da demonstração. Cota $\zeta(s)$, e daí usa fórmula integral de Cauchy para cotar $\zeta'(s)$. Dessas duas cotas e $S(\sigma, t) \geq 1$, pode-se conseguir a cota de $1/\zeta(s)$. Veja Stein, seção 7.1.1. □

Para vermos que podemos trocar o c no contorno na parte não limitada (ou seja, perto do infinito), basta checar que $\int_{c+iN}^{c+i\infty} F(s)\,\mathrm{d}s$ vai para 0. De fato, a cota acima nos dá que $|F(s)| \leq C\frac{x^{c+1}}{t^2}t^\epsilon$, e tomando $\epsilon < 1$ basta.

Então temos

$$\psi_1(x) = \frac{x^2}{2} + \frac{1}{2\pi i}\int_\gamma F(s)\,\mathrm{d}s$$

onde γ é um caminho de $1 - i\infty$ a $1 + i\infty$ que vai pela esquerda do ponto $s = 1$. Note que para $\mathrm{Re}(s) = 1$, temos $|F(s)| \leq C_{1/2}x^2t^{-3/2}$. Então temos um N tal que $\frac{1}{2\pi i}\int_{\gamma_N} F(s)\,\mathrm{d}s < \epsilon x^2/2$ para qualquer $\epsilon > 0$ que quisermos, onde γ_N é a parte de γ com $\mathrm{Im}(s) > N$. Agora escolha δ tal que

$F(s)$ não tenha zeros com $\mathrm{Im}(s) \leq N$ e $\mathrm{Re}(s) > 1-\delta$. Então temos

$$\left|\psi_1(x) - \frac{x^2}{2}\right| < \epsilon x^2 + \frac{1}{2\pi i}\left(\int_{1-\delta-iN}^{1-\delta+iN} F(s)\ \mathrm{d}s + \int_{1-iN}^{1-\delta-iN} F(s)\ \mathrm{d}s + \int_{1-\delta+iN}^{1+iN} F(s)\ \mathrm{d}s\right)$$

Na primeira integral, $|x^{s+1}| = x^{1-\delta+1} = x^{2-\delta}$, e então a integral é no máximo $Cx^{2-\delta}$.

Para as duas outras integrais, podemos cotá-las por

$$\left|\int_{1-\delta+iN}^{1+iN} F(s)\ \mathrm{d}s\right| \leq C\int_{1-\delta}^{1} x^{\sigma+1}\ \mathrm{d}\sigma \leq C\frac{x^2}{\log x}.$$

Portanto,

$$\left|\psi_1(x) - \frac{x^2}{2}\right| < \epsilon x^2 + O(x^{2-\delta}) + O(x^2/\log x),$$

e então

$$|\lim_{x\to\infty} 2\psi_1(x)/x^2 - 1| < 2\epsilon,$$

e tomando $\epsilon \to 0$, provamos o teorema dos números primos.

8.3. **Fórmula para $\pi(x)$.** Com um argumento parecido ao acima, poderíamos dar uma fórmula para $\pi(x)$ se soubéssemos todos os zeros de ζ. A Hipótese de Riemann diria que os erros da fórmula são o menor possível.

Conjectura 8.8 (Hipótese de Riemann)**.** *Se* $\mathrm{Re}(s) > 0$ *e* s *é um zero de* $\zeta(s)$*, então* $\mathrm{Re}(s) = 1/2$.

Defina $\mathrm{Li}(x) = \int_2^x \mathrm{d}u/\log u$, e seja

$$R(x) = \sum_{n\geq 1} \frac{\mu(n)}{n}\mathrm{Li}(x^{1/n}).$$

Teorema 8.9. *Sejam* ρ *os zeros da* ζ *com* $\mathrm{Re}(s) > 0$*. Então*

$$\pi(x) = R(x) - \sum_{n\geq 1} R(x^{-2n}) - \sum_{\rho} R(x^{\rho}).$$

Nota 8.10. Os termos $R(x^{-2n})$ correspondem ao fato que $\zeta(-2n) = 0$, chamados de zeros triviais. Veremos isso próxima aula quando provarmos a extensão meromórfica de ζ.

8.4. **Preliminares para a equação funcional.** Vamos discutir brevemente a função gamma Γ.

Definição 8.11. $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}\ \mathrm{d}t$ para $\mathrm{Re}(s) > 0$.

Isso é holomórfica para $\mathrm{Re}(s) > 0$, e extende meromórficamente para o plano complexo por causa do seguinte lema:

Lema 8.12. *Se* $\mathrm{Re}(s) > 0$, *então* $\Gamma(s+1) = s\Gamma(s)$.

Demonstração. Por integração por partes,

$$[e^{-t}t^s]_\epsilon^N = -\int_\epsilon^N e^{-t}t^s \, \mathrm{d}t + s\int_\epsilon^N e^{-t}t^{s-1} \, \mathrm{d}t,$$

e tomando $\epsilon \to 0$ e $N \to \infty$, temos que o lado esquerdo vai para 0, e a equação que queremos segue. □

Corolário 8.13. *Para* $n \in \mathbb{Z}_{\geq 0,}$ *temos* $\Gamma(n+1) = n!$.

Demonstração. Pelo lema anterior, basta calcular que $\Gamma(1) = 1$:

$$\Gamma(1) = \int_0^\infty e^{-t} \, \mathrm{d}t = [-e^{-t}]_0^\infty = 1.$$ □

Teorema 8.14. Γ *extende meromórficamente para* $\mathbb{C}$, *com pólos simples em* $s \in \mathbb{Z}_{\leq 0}$, *e resíduos* $\mathrm{res}_{-n}\Gamma = (-1)^n/n!$.

Demonstração. Aplicando o lema acima repetidamente, temos para $\mathrm{Re}(s) > 0$ que

$$\Gamma(s) = \frac{\Gamma(s+n+1)}{s(s+1)\cdots(s+n)}.$$

Mas o lado direito é uma função meromórfica para $\mathrm{Re}(s) > -n-1$, e portanto $\Gamma(s)$ extende para uma função meromórfica para $\mathrm{Re}(s) > -n-1$. Tomando $n \to \infty$, $\Gamma(s)$ extende para $\mathbb{C}$.

Pela fórmula acima, podemos ver que os únicos pólos são (no máximo) simples em $s \in \mathbb{Z}_{\leq 0,}$ e podemos calcular o resíduo:

$$\mathrm{res}_{-n}\Gamma = \left[\frac{\Gamma(s+n+1)}{s(s+1)\cdots(s+n-1)}\right]_{s=-n} = \frac{\Gamma(1)}{(-1)^n n!} = \frac{(-1)^n}{n!}.$$ □

Exercícios

(1) Seja $c > 0$ e $a \geq 0$. Prove que

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{a^s}{s}\, \mathrm{d}s = \begin{cases} 1 & \text{se } a \geq 1, \\ 1/2 & \text{se } a = 1, \\ 0 & \text{se } 0 \leq a < 1. \end{cases}$$

(2) Seja p_n o n-ésimo primo. Use o teorema dos números primos para provar que $p_n \sim n \log n$.

(3) Use a expressão em produto de ζ para ver que

$$\frac{1}{\zeta(s)} = \sum_{n\geq 1} \frac{\mu(n)}{n^s} \quad \text{para } \mathrm{Re}(s) > 1.$$

Note como, pelo menos formalmente, temos que

$$\sum_{n\geq 1} \frac{f(n)}{n^s} = \frac{1}{\zeta(s)} \left(\zeta(s) \sum_{n\geq 1} \frac{f(n)}{n^s} \right)$$

é relacionado com a fórmula de inversão de Moebius (veja o Problema 1 na página 203/204 do Stein).

(4) Prove que se $a \in \mathbb{Z}_{\geq 0}$, temos

$$\zeta(s)^2 = \sum_{n\geq 1} \frac{d(n)}{n^s} \quad \text{para } \mathrm{Re}(s) > 1,$$

$$\zeta(s)\zeta(s-a) = \sum_{n\geq 1} \frac{\sigma_a(n)}{n^s} \quad \text{para } \mathrm{Re}(s) > a+1.$$

onde $d(n)$ é a quantidade de divisores e $\sigma_a(n) = \sum_{d|n} d^a$.

9. 8 de Maio

O objetivo de hoje é provar a equação funcional da ζ, dada pelo seguinte theorem.

Teorema 9.1. *Seja $\Lambda(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$. Então Λ extende a uma função meromórfica em $\mathbb{C}$ e satisfaz $\Lambda(s) = \Lambda(1-s)$.*

Analisando pólos e zeros, podemos concluir que os únicos zeros de $\zeta(s)$ fora de $0 < \mathrm{Re}(s) < 1$ são em $s \in 2\mathbb{Z}_{<0}$. Os pólos de Λ são em $s = 0$ e $s = 1$. Tomando $s = -1$ e usando que $\zeta(2) = \pi^2/6$ e $\Gamma(1/2) = \sqrt{\pi}$, obtemos o clássico $\zeta(-1) = -1/12$.

O termo "extra" de $\pi^{-s/2}\Gamma(s/2)$ é pensado como um fator de Euler adicional pelo "primo" ∞. De maneira mais geral, se K é um corpo numérico de grau n, vimos que K tem n injeções $K \hookrightarrow \mathbb{C}$, onde r fatoram por $\mathbb{R}$ e $2s$ não. Então, definimos

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2), \quad \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1)$$

e

$$\Lambda_K(s) := |D_K|^{s/2}\Gamma_{\mathbb{R}}(s)^r\Gamma_{\mathbb{C}}(s)^s\zeta_K(s)$$

onde pensamos, para $F \in \{\mathbb{R}, \mathbb{C}\}$, em $K \hookrightarrow F$ como um "primo", e o fator $\Gamma_F(s)$ é o fator de Euler correspondente.

Teorema 9.2. *$\Lambda_K(s)$ extende meromórficamente para $\mathbb{C}$, e satisfaz $\Lambda_K(s) = \Lambda_K(1-s)$.*

Também vimos funções L associadas com um caracter de Dirichlet primitivo $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}$. Elas também satisfazem equações funcionais: denotamos $\epsilon = 0$ se $\chi(-1) = 1$ e $\epsilon = 1$ se $\chi(-1) = -1$. Daí se

$$\Lambda(s,\chi) := N^{(s+\epsilon)/2}\Gamma_{\mathbb{R}}(s+\epsilon)L(s,\chi),$$

e

$$\epsilon(\chi) := i^\epsilon\frac{\sqrt{N}}{\tau(\chi)}, \quad \tau(\chi) := \sum_{a=0}^{N-1}\chi(a)e^{2\pi ia/N}.$$

Note que $|\tau(\chi)|^2 = \tau(\chi)\tau(\overline{\chi}) = N$, e portanto $|\epsilon(\chi)| = 1$.

Teorema 9.3. *$\Lambda(s,\chi)$ extende meromórficamente para $\mathbb{C}$, e satisfaz*

$$\Lambda(1-s,\overline{\chi}) = \epsilon(\chi)\Lambda(s,\chi).$$

Hoje vamos provar a equação funcional para $\zeta(s)$ e, de maneira mais geral, para $L(s,\chi)$.

9.1. **Transformada de Mellin.**

Definição 9.4. Uma série de Dirichlet é uma função complexa da forma $\sum_{n\geq 1} c_n/n^s$ para $c_n \in \mathbb{C}$.

Se existe n tal que tal série converge absolutamente para $\mathrm{Re}(s) > n$, então ela é holomórfica em tal região.

A seguinte transformada é muito importante no estudo de séries de Dirichlet.

Definição 9.5. Seja f uma função definida em $x > 0$. Sua *transformada de Mellin*, quando convergente, é dada por

$$M\{f\}(s) := \int_0^\infty f(x)x^{s-1}\,\mathrm{d}x.$$

Exemplo 9.6. Temos $M\{e^{-x}\} = \Gamma$.

Proposição 9.7. *Se $f(x) = e^{-cx}$ para $c > 0$, então temos $M\{f\}(s) = c^{-s}\Gamma(s)$ para $\mathrm{Re}(s) > 0$.*

Demonstração. Temos

$$M\{f\}(s) = \int_0^\infty e^{-cx}x^{s-1}\,\mathrm{d}x$$

e se $t = cx$, temos $\mathrm{d}x = c\,\mathrm{d}t$ e portanto

$$M\{f\}(s) = c^{-s}\int_0^\infty e^{-t}t^{s-1}\,\mathrm{d}t = c^{-s}\Gamma(s). \qquad \square$$

Como consequência disso, se $f(s) = \sum_{n\geq 1} c_n/n^s$ é uma série de Dirichlet, então pelo menos formalmente temos:

$$\pi^{-s}\Gamma(s)f(s) = \sum_{n\geq 1} c_n \cdot M\{e^{-\pi n x}\}(s) = M\{\varphi\}$$

onde

$$\varphi(x) = \sum_{n\geq 1} c_n e^{-\pi n x}.$$

Por exemplo:

$$\zeta(s) = \frac{1}{\Gamma(s)} M\left\{\frac{1}{e^x - 1}\right\}(s).$$

É possível usar essa fórmula para mostrar que $\zeta(s)$ extende meromórficamente com único pólo em $s = 1$. Mas para a equação funcinonal, temos que trabalhar um pouco mais.

9.2. **Funções theta e equação funcional.** A ideia para a prova de várias equações funcionais é que se $f(1/x) = x^k f(x)$, então denotando $y = x^{-1}$, temos $\mathrm{d}y = -x^{-2}\,\mathrm{d}x$ e então, pelo menos

formalmente, temos

$$M\{f\}(s) = \int_0^\infty f(x)x^{s-1}\,\mathrm{d}x = \int_0^\infty y^k f(y)y^{1-s}y^{-2}\,\mathrm{d}y = \int_0^\infty f(y)y^{k-1-s}\,\mathrm{d}y = M\{f\}(k-s),$$

e tem a forma de uma equação funcional.

Veremos em próximas aulas como tais f são relacionados com formas modulares!

Por hora, vamos ver o caso específico para $\zeta(s)$. Olhando para a forma da equação funcional, olhamos para

$$\Lambda(2s) = \pi^{-s}\Gamma(s)\zeta(2s) = M\{\varphi\}(s)$$

onde

$$\zeta(2s) = \sum_{n\geq 1}\frac{1}{(n^2)^s} \implies \varphi(x) = \sum_{n\geq 1} e^{-\pi n^2 x}.$$

Definição 9.8. A função theta $\theta(x)$ é dada por $\theta(x) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 x} = 1 + 2\varphi(x)$.

Na próxima seção vamos provar que $\theta(1/x) = x^{1/2}\theta(x)$. Vamos ver como isso implica a equação funcional.

Proposição 9.9. *Assuma que $\theta(1/x) = x^{1/2}\theta(x)$ para $x > 0$. Então $\Lambda(s) = \Lambda(1-s)$ para $0 < \mathrm{Re}(s) < 1$. Portanto $\Lambda(s)$ é meromórfica em $\mathbb{C}$, e a igualdade é verdade para todo $s \in \mathbb{C}$.*

Demonstração. Escrevendo a relação de θ em termos de φ, temos

$$\varphi(1/x) = \frac{x^{1/2}\theta(x) - 1}{2} = \frac{x^{1/2}-1}{2} + x^{1/2}\varphi(x).$$

No entanto, não podemos separar a soma do lado esquerdo ao integrar em $\mathbb{R}_+$. Invés disso, usamos essa fórmula para trocar a integral para ser entre $[0,1]$. Temos, para $\mathrm{Re}(s) > 0$, que

$$\Lambda(2s) = M\{\varphi\}(s) = \int_0^\infty \varphi(x)x^{s-1}\,\mathrm{d}x = \int_0^1 \varphi(x)x^{s-1}\,\mathrm{d}x + \int_0^1 \left(\frac{y^{1/2}-1}{2} + y^{1/2}\varphi(y)\right) y^{1-s}y^{-2}\,\mathrm{d}y$$
$$= \int_0^1 \left(\frac{x^{-s-1/2} - x^{-1-s}}{2} + \varphi(x)(x^{s-1} + x^{-s-1/2})\right)\,\mathrm{d}x = \frac{1}{2(-s+1/2)} - \frac{1}{-2s} + \int_0^1 \varphi(x)(x^{s-1} + x^{-s-1/2})\,\mathrm{d}x$$
$$= \frac{1}{2s} - \frac{1}{2s-1} + \int_0^1 \varphi(x)(x^{s-1} + x^{-s-1/2})\,\mathrm{d}x.$$

Agora note que essa expressão é invariante a $s \mapsto 1/2 - s$.

Portanto $\Lambda(2s) = \Lambda(1-2s)$ para $1/2 > \mathrm{Re}(s) > 0$, e trocando $2s$ por s, temos $\Lambda(s) = \Lambda(1-s)$ para $1 > \mathrm{Re}(s) > 0$. □

Isso prova a extensão meromórfica e a equação funcional de $\zeta(s)$ uma vez que provarmos que $\theta(1/x) = x^{1/2}\theta(x)$.

De maneira parecida, se quisermos a equação funcional de $L(s,\chi)$, podemos considerar

$$\theta(x,\chi) := \sum_{n\in\mathbb{Z}} \chi(n)e^{-\pi n^2 x}.$$

No entanto, note que se $\chi(-1) = -1$, isso é simplesmente 1. Para lidar com χ tal que $\chi(-1) = -1$, temos que considerar

$$\tilde{\theta}(x,\chi) := \sum_{n\in\mathbb{Z}} \chi(n)n\sqrt{x}e^{-\pi n^2 x}.$$

Vamos ver que

$$\theta\left(\frac{1}{N^2x},\chi\right) = \tau(\chi)\sqrt{x}\theta(x,\chi^{-1}) \quad \text{e} \quad \tilde{\theta}\left(\frac{1}{N^2x},\chi\right) = i\tau(\chi)\sqrt{x}\tilde{\theta}(x,\chi^{-1}).$$

Uma vez que se tenha isso, o mesmo argumento prova a equação funcional para $L(s,\chi)$.

9.3. **Transformada de Fourier e propriedades das funções theta.** As fórmulas das funções θ vão ser todas casos particulares da *fórmula de soma de Poisson*, que envolve *transformadas de Fourier*.

Definição 9.10. Seja $f\colon \mathbb{R} \to \mathbb{C}$ uma função absolutamente integrável. Sua *transformada de Fourier* é

$$\hat{f}(\xi) = \int_{\mathbb{R}} f(x)e^{-2\pi i\xi x}\,\mathrm{d}x.$$

Proposição 9.11. *Seja $g\colon \mathbb{R} \to \mathbb{C}$ absolutamente integrável.*

(a) Se $f(x) = g(\lambda x)$, então $\hat{f}(\xi) = \lambda^{-1}\hat{g}(\lambda^{-1}\xi)$.

(b) Se $f(x) = g(x+\lambda)$, então $\hat{f}(\xi) = e^{2\pi i\lambda\xi}\hat{g}(\xi)$.

(c) Se $f(x) = e^{2\pi i\lambda x}g(x)$, então $\hat{f}(\xi) = \hat{g}(\xi - \lambda)$.

(d) Se g' também é absolutamente integrável, então $\widehat{g'}(\xi) = 2\pi i\xi\hat{g}(\xi)$.

(e) Se $f(x) = 2\pi i x g(x)$ também é absolutamente integrável, então $\hat{f}(\xi) = (\hat{g})'(\xi)$.

Exemplo 9.12. Considere a Gaussiana $f(x) = e^{-\pi\lambda x^2}$ para $\lambda > 0$. Se $g(x) = e^{-\pi x^2}$, então $f(x) = g(\lambda^{1/2}x)$, portanto $\hat{f}(\xi) = \lambda^{-1/2}\hat{g}(\lambda^{-1/2}\xi)$. Vamos provar que $\hat{g}(\xi) = e^{-\pi\xi^2}$, e então que

$$\hat{f}(\xi) = \frac{1}{\sqrt{\lambda}}e^{-\pi\xi^2/\lambda}.$$

Para calcular $\hat{g}(\xi)$, note que

$$g'(x) = -2\pi x g(x) \implies 2\pi i \xi \hat{g}(\xi) = -i(\hat{g})'(\xi)$$

portanto

$$(\hat{g})'(\xi) = -2\pi\xi\hat{g}(\xi)$$

e então $\hat{g}(\xi) = ce^{-\pi\xi^2}$ para uma constante

$$c = \int_{\mathbb{R}} e^{-\pi x^2} \, \mathrm{d}x,$$

que pode-se calcular que é 1.

Teorema 9.13 (Fórmula da soma de Poisson)**.** *Seja $f\colon \mathbb{R} \to \mathbb{C}$ uma função Schwartz*[27]*. Então temos*[28]

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

Demonstração. Considere $F(x) = \sum_{n\in\mathbb{Z}} f(x+n)$. Isso é periódica, e então pela expansão em Fourier, temos $F(x) = \sum_{n\in\mathbb{Z}} c_n e^{2\pi i n x}$. Mas daí

$$c_n = \int_0^1 F(x) e^{-2\pi i n x} \, \mathrm{d}x = \sum_{m\in\mathbb{Z}} \int_0^1 f(x+m) e^{-2\pi i n x} \, \mathrm{d}x = \int_{\mathbb{R}} f(x) e^{-2\pi i n x} \, \mathrm{d}x = \hat{f}(n).$$

E portanto

$$\sum_{n\in\mathbb{Z}} f(n) = F(0) = \sum_{n\in\mathbb{Z}} c_n = \sum_{n\in\mathbb{Z}} \hat{f}(n). \qquad \square$$

Agora considere $\theta(x) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 x}$. Tomando $f(y) = e^{-\pi y^2 x}$, a fórmula de Poisson nos dá que

$$\theta(x) = \sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n) = x^{-1/2} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/x} = x^{-1/2}\theta(1/x).$$

Se $\chi(-1) = 1$, considere $\theta(x,\chi) = \sum_{n\in\mathbb{Z}} \chi(n) e^{-\pi n^2 x} = \sum_{a=0}^{N-1} \chi(a) \sum_{n\in\mathbb{Z}} e^{-\pi(nN+a)^2 x}$. Se $f_a(y) = e^{-\pi(yN+a)^2 x}$, temos $f_a(y) = g(yN+a)$ para a Gaussiana $g(y) = e^{-\pi y^2 x}$, e então

$$\hat{f_a}(\xi) = \frac{1}{N} e^{2\pi i a \xi/N} \hat{g}(\xi/N) = \frac{1}{N\sqrt{x}} e^{2\pi i a\xi/N} e^{-\pi\xi^2/(N^2 x)}.$$

[27]Essa é uma certa classe de funções que é preservada pela transformada de Fourier. Basicamente, f é suave e todas as suas derivadas decrescem rápido.

[28]De maneira mais geral, se $f\colon \mathbb{R}^n \to \mathbb{C}$ é Schwartz e $\Lambda \subseteq \mathbb{R}^n$ é um lattice, então

Portanto a fórmula de Poisson nos dá que

$$\theta(x,\chi)=\sum_{a=0}^{N-1}\chi(a)\sum_{n\in\mathbb{Z}}f_a(n)=\sum_{a=0}^{N-1}\chi(a)\sum_{n\in\mathbb{Z}}\hat{f}_a(n)=\frac{x^{-1/2}}{N}\sum_{a=0}^{N-1}\chi(a)\sum_{n\in\mathbb{Z}}e^{2\pi ian/N}e^{-\pi n^2/(N^2x)}$$
$$=\frac{x^{-1/2}}{N}\sum_{n\in\mathbb{Z}}e^{-\pi n^2/(N^2x)}\sum_{a=0}^{N-1}\chi(a)e^{2\pi ian/N}.$$

Agora note que se $(n,N)=1$,

$$\sum_{a=0}^{N-1}\chi(a)e^{2\pi ian/N}=\chi(n)^{-1}\sum_{a=0}^{N-1}\chi(a)e^{2\pi ia/N}=\chi^{-1}(n)\tau(\chi).$$

Se $(n,N)\neq 1$, é fácil ver que essa soma é 0 pois χ é primitivo. Portanto

$$\theta(x,\chi)=\frac{\tau(\chi)}{N\sqrt{x}}\theta\left(\frac{1}{N^2x},\chi^{-1}\right).$$

Se $\chi(-1)=-1$, considere $\tilde{\theta}(x,\chi)=\sum_{n\in\mathbb{Z}}\chi(n)n\sqrt{x}e^{-\pi n^2x}=\sum_{a=0}^{N-1}\chi(a)\sum_{n\in\mathbb{Z}}(nN+a)\sqrt{x}e^{-\pi(nN+a)^2x}$. Se $f_a(y)=(yN+a)\sqrt{x}e^{-\pi(yN+a)^2x}$, temos $f_a(y)=\sqrt{x}g(yN+a)$ para $g(y)=ye^{-\pi y^2x}$, e então

$$\hat{f}_a(\xi)=\frac{\sqrt{x}}{N}e^{2\pi ia\xi/N}\hat{g}(\xi/N)=\frac{i\xi}{N^2x}e^{2\pi ia\xi/N}e^{-\pi y^2/(N^2x)}.$$

e portanto pela fórmula da soma de Poisson,

$$\tilde{\theta}(x,\chi)=\sum_{a=0}^{N-1}\chi(a)\sum_{n\in\mathbb{Z}}f_a(n)=\sum_{a=0}^{N-1}\chi(a)\sum_{n\in\mathbb{Z}}\hat{f}_a(n)=\frac{i}{N^2x}\sum_{a=0}^{N-1}\chi(a)\sum_{n\in\mathbb{Z}}ne^{2\pi ian/N}e^{-\pi n^2/(N^2x)}$$
$$=\frac{i}{N^2x}\sum_{n\in\mathbb{Z}}ne^{-\pi n^2/(N^2x)}\sum_{a=0}^{N-1}\chi(a)e^{2\pi ian/N}.$$

Da mesma forma que antes, concluímos que

$$\tilde{\theta}(x,\chi)=\frac{i\tau(\chi)}{N\sqrt{x}}\tilde{\theta}\left(\frac{1}{N^2x},\chi^{-1}\right).$$

9.4. **Um pouco de filosofia.** Vou focar em 3 jeitos de conseguir funções L. K denota um corpo numérico e $\mathfrak{p}$ um ideal primo com $\mathcal{O}_K/\mathfrak{p}\simeq\mathbb{F}_q$.

(1) Representações Galois: dado L/K uma extensão de corpos numéricos Galois e $\rho\colon \mathrm{Gal}\,(L/K)\to \mathrm{GL}(V)$ onde V é um espaço vetorial sobre $\mathbb{C}$ (ou outros corpos...), defina $L_{\mathfrak{p}}(s,\rho)=\det(1-\mathrm{Frob}_{\mathfrak{p}}q^{-s}|V^{I_{\mathfrak{p}}})$. Daí $L(s,\rho)=\prod_{\mathfrak{p}}L_{\mathfrak{p}}(s,\rho)$.

(2) Geometria: dado uma variedade algébrica X sobre K (com certas boas propriedades) e primos tal que X "módulo" $\mathfrak{p}$ seja "bom", defina $\zeta_{\mathfrak{p}}(s, X) = \exp\left(-\sum_{m\geq 1} \frac{N_{q^m}}{m} q^{-sm}\right)$ onde N_{q^m} é a quantidade de soluções em $\mathbb{F}_{q^m}$. Daí $\zeta(s, X/K) := \prod_{\mathfrak{p}} \zeta_{\mathfrak{p}}(s, X)$.

(3) Formas automórficas: esse será um assunto futuro, mas o exemplo mais básico são os caracteres de Dirichlet χ, que nos dão $L(s, \chi)$.

Exemplo 9.14. Considerando $L = K$ e a representação trivial, isso nos dá $\zeta_K(s)$.

Exemplo 9.15. Seja $X = \mathbb{A}^k$ o k-espaço. Então a quantidade de pontos sobre $\mathbb{F}_q$ é simplesmente q^k. Daí $\zeta_{\mathfrak{p}}(s, \mathbb{A}^k) = \exp(\sum_{m\geq 1} q^{mk-sm}/m) = (1 - q^{k-s})^{-1}$. Portanto $\zeta(s, \mathbb{A}^k/K) = \zeta_K(s - k)$.

Exemplo 9.16. Seja $X = \mathbb{P}^k$ o k-espaço projetivo. Daí a quantidade de pontos sobre $\mathbb{F}_q$ é $(q^{k+1} - 1)/(q - 1) = 1 + q + \cdots + q^k$, e portanto

$$\zeta(s, \mathbb{P}^k/K) = \zeta(s, \mathbb{A}^0/K)\zeta(s, \mathbb{A}^1/K) \cdots \zeta(s, \mathbb{A}^k/K) = \zeta_K(s)\zeta_K(s - 1) \cdots \zeta_K(s - k)$$

correspondendo ao fato que $\mathbb{P}^k = \mathbb{A}^k \sqcup \mathbb{A}^{k-1} \sqcup \cdots \sqcup \mathbb{A}^0$.

Exemplo 9.17. Seja E/K uma curva elíptica. Pode-se provar que se $\mathfrak{p}$ é "bom", $E(\mathbb{F}_{q^n})$ satisfaz uma recursão linear de grau 2, e que

$$\zeta_{\mathfrak{p}}(s, E/K) = \frac{(1 - q^{-s})(1 - q^{-s-1})}{(1 - a_q q^{-s} + q^{1-2s})}$$

onde $a_q = q + 1 - |E(\mathbb{F}_q)|$. Portanto, a menos de finitos fatores,

$$\zeta(s, E/K) = \frac{L(s, E/K)}{\zeta_K(s)\zeta_K(s + 1)}$$

onde

$$L(s, E/K) = \prod_{\mathfrak{p}} (1 - a_q q^{-s} + q^{1-2s})^{-1}.$$

Existem diversas relações (conjecturais) entre os 3 tipos. As $\zeta_K(s)$ forem inicialmente definidas no lado Galois, e se L/K é abeliano vimos como representações de $\mathrm{Gal}\,(L/K)$ aparecem naturalmente, mas se $L = \mathbb{Q}[\zeta_N]$ e $K = \mathbb{Q}$, relacionamos tais representações com caracteres de Dirichlet (automórfico). Foi pelo lado automórfico que provamos a equação funcional.

Teorema 9.18 (Kronecker–Weber)**.** *Toda extensão abeliana de $\mathbb{Q}$ está dentro de um corpo ciclotômico.*

Esse teorema diz que representações 1-dimensionais de $\mathrm{Gal}\,(K/\mathbb{Q})$ são correspondentes a caracteres de Dirichlet. A *teoria dos corpos de classe* associa a toda representação 1-dimensional de $\mathrm{Gal}\,(L/K)$ um *caracter de Hecke*, fazendo mais uma ponte entre o lado Galois e automórfico. Hecke então generalizou os argumentos de hoje:

Teorema 9.19 (Teoria dos corpos de classe, Hecke)**.** *Se* $\chi\colon \mathrm{Gal}\,(L/K) \to \mathbb{C}^\times$ *é uma representação* 1*-dimensional, então* $\zeta_K(s,\chi)$ *satisfaz uma equação funcional.*

Em geral, não se sabe que funções L do lado Galois extendem meromórficamente, e a esperança que se possa relacioná-las com o lado automórfico é parte das *conjecturas de Langlands*.

Também se espera um vínculo entre o lado geométrico e Galois. A relação no sentido direto é dado pela teoria de *cohomologia étale*, e no lado reverso é conjectural. Como um exemplo, uma curva elíptica nos dá uma certa representação 2-dimensional, e se $K = \mathbb{Q}$, Wiles e seus seguidores provaram que tal representação é relacionada com o lado automórfico–via formas modulares (iremos estudar um pouco sobre elas!). Novamente, é o lado automórfico que nos deixa provar extensão anaítica, e portanto é graças a esse trabalho que sabemos que: se $E/\mathbb{Q}$ é uma curva elíptica, então $L(s, E/\mathbb{Q})$ extende holomórficamente para o plano complexa.

Exercícios

(1) Prove que $\int_{\mathbb{R}} e^{-\pi x^2}\ \mathrm{d}x = 1$.[29]

(2) Prove que $\Gamma(1/2) = \sqrt{\pi}$.[30]

(3) Use a fórmula $\Gamma(s)\zeta(s) = \int_0^\infty \frac{x^{s-1}}{e^x-1}\ \mathrm{d}x$ para ver diretamente que $\zeta(s)$ extende meromórficamente: a integral de 1 a ∞ é holomórfica no plano inteiro, e

$$\int_0^1 \frac{x^{s-1}}{e^x-1}\ \mathrm{d}x = \sum_{m\geq 0} \frac{B_m}{m!(s+m-1)}$$

onde $\frac{z}{e^z-1} = \sum_{m\geq 0} \frac{B_m}{m!} z^m$. Para ver que isso converge, note que $z/(e^z-1)$ é holomórfico para $|z| < 2\pi$, portanto $\limsup_{m\to\infty} |B_m/m!|^{1/m} = 1/(2\pi) < 1$. Note que os pólos dessa expressão são cancelados pelo fator de $\Gamma(s)$ exceto para $s = 1$.

(4) Use a expressão do item anterior para provar que se $n \in \mathbb{Z}_{\geq 0}$, então

$$\zeta(-n) = (-1)^n n! \cdot \lim_{s\to -n} \left((s+n) \int_0^1 \frac{x^{s-1}}{e^x-1}\ \mathrm{d}x \right) = (-1)^n \frac{B_{n+1}}{n+1}.$$

Temos $B_0 = 1$ e $B_1 = 1/2$. Prove que $z/(e^z-1)-1-z/2$ é ímpar, e portanto que $B_{2n+1} = 0$ se $n \geq 1$. Conclua que $\zeta(-2n) = 0$ para $n \geq 1$, e use a equação funcional para provar que se $n \geq 1$, então

$$\zeta(2n) = (-1)^{n+1} \frac{(2\pi)^{2n}}{2(2n)!} B_{2n}.$$

Isso prova que $\zeta(2) = \pi^2/6$ pois $B_2 = 1/6$.

(5) Siga o mesmo argumento da prova da equação funcional de $\zeta(s)$ para provar as equações funcionais de $L(s,\chi)$.

(6) Repita o procedimento acima para provar a equação funcional de $\zeta_K(s)$ para $K = \mathbb{Q}[i]$.

[29] Eleve ao quadrado e use coordenadas polares, lembrando que $\mathrm{d}x\ \mathrm{d}y = R\ \mathrm{d}R\ \mathrm{d}\theta$.

[30] Troque variáveis $t = \pi u^2$ e use o problema anterior.

10. 15 de Maio

10.1. **Motivação.** Lembre-se que a função theta é dada por

$$\theta(x) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 x}$$

para $x > 0$. Na verdade, θ é uma função holomórfica para $\mathrm{Re}(x) > 0$. Podemos observar que $\theta(x + 2i) = \theta(x)$, e provamos com a fórmula da soma de Poisson que

$$\theta(1/x) = x^{1/2}\theta(x).$$

Provamos isso para $x > 0$, mas por extensão analítica isso tem que valer para $\mathrm{Re}(x) > 0$ para um certo branch de $x^{1/2}$. Note que se $x = \sigma + it$, então

$$\frac{1}{x} = \frac{\sigma}{|x|^2} - i\frac{t}{|x|^2},$$

e portanto também $\mathrm{Re}(x) > 0$.

Por conveniência, vamos fazer a troca de variáveis $z = ix$, e então se $\mathbb{H} = \{z \in \mathbb{C} \colon \mathrm{Im}(z) > 0\}$, temos: $\theta_0 \colon \mathbb{H} \to \mathbb{C}$ holomórfica tal que:

(1) $\theta_0(z + 2) = \theta_0(z)$,
(2) $\theta_0(-1/z) = j(z)\theta_0(z)$

onde $j(z) = (z/i)^{1/2}$.

Note que $\theta(x, \chi)$ e $\tilde{\theta}(x, \chi)$ satisfazem o mesmo tipo de equações, com $j(z)$ variando por uma constante.

Formas modulares serão basicamente definidas como funções holomórficas $f \colon \mathbb{H} \to \mathbb{C}$ que transformam de maneira parecida ao acima.

10.2. **Formas modulares para** $\mathrm{SL}_2(\mathbb{Z})$**.** Como vimos acima, tanto $z \mapsto z + 1$ e $z \mapsto -1/z$ preservam $\mathbb{H}$ e são holomórficos.

Proposição 10.1. *O seguinte é um automorfismo holomórfico de* $\mathbb{H}$

$$z \mapsto \frac{az + b}{cz + d}$$

para $a, b, c, d \in \mathbb{R}$ *com* $ad - bc \neq 0$. *Além disso, temos um mapa de grupos* $\mathrm{GL}_2(\mathbb{R}) \to \mathrm{Aut}(\mathbb{H})$ *com kernel dado pelas matrizes diagonais. Pode-se provar que esse mapa é sobrejetor.*

Demonstração. É fácil ver que compondo $z \mapsto rz + s$ para $r, s \in \mathbb{R}$ e $z \mapsto -1/z$, pode-se obter qualquer mapa acima, portanto são holomórficos e são automorfismos de $\mathbb{H}$. □

Portanto temos uma ação de $\mathrm{GL}_2(\mathbb{R})$ em $\mathbb{H}$.

Agora note que $z \mapsto z + 1$ e $z \mapsto -1/z$ geram o subgrupo $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$, e isso motiva a seguinte definição

Definição 10.2. Uma *quase-função modular de peso* $k \in \mathbb{Z}$ é uma função holomórfica $f\colon \mathbb{H} \to \mathbb{C}$ tal que se $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, então

$$f(\gamma(z)) = (cz + d)^k f(z).$$

Se k é par, isso é equivalente a ter $f(z + 1) = f(z)$ e $f(-1/z) = z^k f(z)$, pois as matrizes $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ e $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ geram $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$.

Nota 10.3. Note que as funções theta seriam exemplos com $k = 1/2$ (e com $z \mapsto z + 2$) mas como tirar raiz requer uma escolha, podemos definir o fator de automorfismo por $\theta(\gamma(z))/\theta(z)$ se quisermos definir funções modulares com $k \in \frac{1}{2} + \mathbb{Z}$.

Nota 10.4. Note que k tem que ser par, pois $\gamma = -1 \in \mathrm{SL}_2(\mathbb{Z})$.

Se f é uma quase-função modular, então $f(z + 1) = f(z)$ significa que podemos considerar a expansão Fourier de f: se $z = x + iy$, então

$$f(z) = \sum_{n \in \mathbb{Z}} c_n(y) e^{2\pi i n x}$$

onde

$$c_n(y) = \int_0^1 f(x + iy) e^{-2\pi i n x} \, \mathrm{d}x.$$

Então

$$c_n(y) e^{2\pi n y} = \int_{iy}^{1+iy} f(z) e^{-2\pi i z} \, \mathrm{d}z$$

e como $f(z)e^{-2\pi i z}$ é holomórfica e periódica por $z \mapsto z + 1$, podemos ver, integrando sobre um retângulo, que o lado direito é constante. Portanto:

Proposição 10.5. *Se $f\colon \mathbb{H} \to \mathbb{C}$ é holomórfica e $f(z+1) = f(z)$, então existem $a_n(f) \in \mathbb{C}$ tal que*

$$f(z) = \sum_{n\in\mathbb{Z}} a_n(f) e^{2\pi i n z}.$$

Denotamos $q = e^{2\pi i z}$, e então $f(z) = \sum_{n\in\mathbb{Z}} a_n(f) q^n$.

Podemos pensar nisso como a expansão de Taylor de f no "ponto" ∞: q é a cordenada desse ponto, pois se $\mathrm{Im}(z)$ é grande, q é pequeno.

Definição 10.6. Uma função quase-modular $f\colon \mathbb{H} \to \mathbb{C}$ é uma

(1) *função modular* se f é meromórfica em ∞, isso é, $a_n(f) = 0$ para n suficientemente pequeno,
(2) *forma modular* se f é holomórfica em ∞, isso é, $a_n(f) = 0$ para $n < 0$,
(3) *forma de cúspide* se f é holomórfica e igual a 0 em ∞, isso é, $a_n(f) = 0$ para $n \leq 0$.

As duas últimas condições são equivalentes a:

(2) $f(z)$ é limitada quando $\mathrm{Im}(z) \to \infty$,
(3) $f(z)$ tende a 0 quando $\mathrm{Im}(z) \to \infty$.

Definição 10.7. Seja $f\colon \mathbb{H} \to \mathbb{C}$ uma forma modular. Sua função L é dada por

$$L(s,f) = \sum_{n\geq 1} \frac{a_n(f)}{n^s}.$$

No entanto, note que não sabemos nada de convergência dessa série. Vamos ver depois em que região isso converge.

Note que, pelo menos formalmente,

$$\Lambda(s,f) := M\{f(ix) - a_0(f)\}(s) = \int_0^\infty (f(ix) - a_0(f)) x^{s-1}\,\mathrm{d}x = \sum_{n\geq 1} \int_0^\infty a_n(f) e^{-2\pi n x} x^{s-1}\,\mathrm{d}x = (2\pi)^{-s}\Gamma(s)L(s,f).$$

Então se $a_0(f) = 0$, formalmente temos que $\Lambda(s,f) = \Lambda(k-s,f)$ se $L(s,f)$ e $L(k-s,f)$ ambas fazem sentido. Vamos discutir como analisar tais questões de convergência depois.

Definição 10.8. Note que formas modulares de peso k formam um espaço vetorial sobre $\mathbb{C}$. Denotamos M_k e S_k os espaços vetoriais de formas modulares e formas de cúspide de peso k.

Também podemos pensar na região fundamental D da ação de $\mathrm{SL}_2(\mathbb{Z})$ em $\mathbb{H}$: ela é dada por

$$D = \{z \in \mathbb{H}\colon \mathrm{re}(z) \in [-1/2, 1/2],\ |z| > 1\}.$$

Então podemos pensar numa função modular como uma função holomórfica em D, que satisfaz certas compatibilidades na borda de D.

10.3. **Formas modulares para Γ.** Em geral, se $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, tem um índice finito, podemos tentar considerar formas modulares que transformam por Γ.

Se $\gamma_1, \ldots, \gamma_n$ são representantes de $\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$ (ou seja, $\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_{i=1}^n \Gamma\gamma_i$) a região fundamental D_Γ de Γ é

$$D_\Gamma = \bigcup_{i=1}^n \gamma_i(D).$$

Como $(a\infty + b)/(b\infty + d) = b/d \in \mathbb{Q}$, a região D_Γ pode conter outros cúspides em $\mathbb{Q}$. Para definir formas modulares, queremos que a função seja holomórfica em todos os cúspides.

Definição 10.9. Uma função holomórfica $f\colon \mathbb{H} \to \mathbb{C}$ que satisfaz

$$f(\gamma(z)) = (cz + d)^k f(z), \quad \text{para todo } \gamma \in \Gamma$$

é uma

(1) *forma modular de peso k* se também para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, temos que $(cz + d)^{-k} f(\gamma(z))$ é limitada quando $\mathrm{Im}(z) \to \infty$,
(2) *forma de cúspide de peso k* se para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, temos que $(cz+d)^{-k} f(\gamma(z))$ converge para 0 quando $\mathrm{Im}(z) \to \infty$.

Denotamos $M_k(\Gamma)$ e $S_k(\Gamma)$ os dois espaços.

Note que se $\Gamma_1 \subseteq \Gamma_2$, então $M_k(\Gamma_1) \supseteq M_k(\Gamma_2)$, ou seja, quanto menor o grupo Γ, mais formas temos.

10.4. **Exemplos.** Até agora, os únicos exemplos que temos é a função 0 e as funções constantes se $k = 0$. Vamos construir alguns exemplos.

Considere novamente a $\theta_0(z)$. Lembre-se que $\theta_0(-1/z) = (z/i)^{1/2}\theta_0(z)$ para alguma raiz quadrada. Podemos tirar essa ambiguidade elevando à quarta potência

$$\theta_0(-1/z)^4 = -z^2\theta_0(z)^4.$$

Note que θ_0 não é periódica em $z \mapsto z+1$, mas é para $z \mapsto z+2$. O que acontece é que $(\theta_0)^4$ é uma forma modular para $\Gamma(2) := \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{F}_2))$, ou seja, γ com $2 \mid b, c$. $\Gamma(2)$ é gerado por

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 1 & 0 \\ 2 & 1. \end{pmatrix},$$

(isso não é verdade para outros N!) e note que a segunda matriz é $-ST^{-2}S$, e portanto os dois sinais de -1 acima cancelam. Portanto

$$(\theta_0)^4 \in M_2(\Gamma(2)).$$

Se maneira parecida, podemos conseguir formas modulares de $\theta(x, \chi)$. Se $\theta_\chi(ix) = \theta(x, \chi)$, pode-se provar que $(\theta_\chi \theta_{\overline{\chi}})^2 \in M_2(\Gamma(4N^2))$, mas isso é mais difícil.

Outra classe de exemplos são dadas por *séries de Eisenstein*: Para $k \geq 4$ par (isso é necessário para haver convergência absoluta), considere

$$E_k(z) = \sum_{(a,b) \in \mathbb{Z}^2 - 0} \frac{1}{(az+b)^k}.$$

Claramente $E_k(z+1) = E_k(z)$, e

$$E_k(-1/z) = \sum_{(a,b) \in \mathbb{Z}^2 - 0} \frac{z^k}{(-a+bz)^k} = z^k \sum_{(a,b) \in \mathbb{Z}^2 - 0} \frac{1}{(-a+bz)^k} = z^k E_k(z).$$

Portanto $E_k(z) \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ desde que seja holomórfica no ∞. Vamos calcular a série de Fourier de E_k e confirmar que isso é verdade:

Proposição 10.10. *Seja $k \geq 4$ par. A expansão de Fourier de $E_k(z)$ é dada por*

$$E_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

onde $\sigma_l(n) = \sum_{d|n} d^l$. Em particular, $E_k(z) \in M_k(\mathrm{SL}_2(\mathbb{Z}))$. Usando que se $k \geq 2$ é par então $\zeta(k) = -(2\pi i)^k B_k / 2k!$, temos

$$E_k(z) = 2\frac{(2\pi i)^k}{(k-1)!} \left(\frac{-B_k}{2k} + \sum_{n \geq 1} \sigma_{k-1}(n) q^n \right).$$

Demonstração. Primeiro vamos calcular $\sum_{n\in\mathbb{Z}}(n+z)^{-k}$ para $\mathrm{Im}(z)>0$ usando a fórmula de soma de Poisson. Para isso, seja $f(x)=(x+z)^{-k}$. Temos

$$\hat{f}(\xi)=\int_{\mathbb{R}}(x+z)^{-k}e^{-2\pi ix\xi}\,\mathrm{d}x.$$

A função $g(s)=(s+z)^{-k}e^{-2\pi iz\xi}$ tem solmente um pólo em $s=-z$ e

$$g(s-z)=\frac{1}{s^k}e^{2\pi iz\xi}e^{-2\pi is\xi}=e^{2\pi iz\xi}\sum_{n\geq 1}\frac{(-2\pi is\xi)^n}{n!s^k}$$

e portanto $\mathrm{res}_{-z}g=e^{2\pi iz\xi}\frac{(-2\pi i\xi)^{k-1}}{(k-1)!}$.

Podemos trocar a integral por uma integral de contorno: Se γ_R é o semi-círculo acima da reta real de raio R no sentido anti-horário, temos

$$\hat{f}(\xi)=\lim_{R\to\infty}\int_{\gamma_R}g(s)\,\mathrm{d}s.$$

Temos $|g(s)|=|s+z|^{-k}e^{2\pi\mathrm{Im}(s)\xi}$. Se R é suficientemente grande, $|s+k|\geq R/2$, portanto $|g(s)|\leq (R/2)^{-k}e^{2\pi\mathrm{Im}(s)\xi}$. Se $\xi\leq 0$, temos $e^{2\pi\mathrm{Im}(s)\xi}\leq 1$ para $s\in\gamma_R$, e portanto

$$\left|\int_{\gamma_R}g(s)\,\mathrm{d}s\right|\leq (R/2)^{-k}\pi R=\frac{\pi}{2^k}R^{1-k}\to 0.$$

Logo $\hat{f}(\xi)=0$ se $\xi\leq 0$. De maneira parecida, podemos trocar a integral para o semicírculo acima da reta, e obtemos que se $\xi\geq 0$,

$$\hat{f}(\xi)=-2\pi i\cdot\mathrm{res}_{-z}g=(-2\pi i)^k\xi^{k-1}\frac{e^{2\pi iz\xi}}{(k-1)!}.$$

Portanto, pela fórmula de soma de Poisson, se $\mathrm{Im}(z)>0$,

$$\sum_{n\in\mathbb{Z}}\frac{1}{(n+z)^k}=\frac{(-2\pi i)^k}{(k-1)!}\sum_{n>0}n^{k-1}e^{2\pi izn}.$$

Portanto, usando que k é par,

$$\begin{aligned}E_k(z)&=2\sum_{b>0}\frac{1}{b^k}+2\sum_{a>0}\sum_{b\in\mathbb{Z}}\frac{1}{(az+b)^k}=2\zeta(k)+2\sum_{a>0}\frac{(2\pi i)^k}{(k-1)!}\sum_{n>0}n^{k-1}e^{2\pi iazn}\\&=2\zeta(k)+2\frac{(2\pi i)^k}{(k-1)!}\sum_{m>0}e^{2\pi imz}\sum_{n|m}n^{k-1}=2\zeta(k)+2\frac{(2\pi i)^k}{(k-1)!}\sum_{n>0}\sigma_{k-1}(n)q^n.\end{aligned}$$

□

De fato, a fórmula acima ainda vale para $k = 2$, mas daí a ordem da soma é impotante, pois a seguinte expressão não é absolutamente convergente:

$$E_2(z) := \sum_{b\neq 0} \frac{1}{b^2} + \sum_{a\neq 0}\sum_{b\in\mathbb{Z}} \frac{1}{(az+b)^2}.$$

No entanto, temos

$$E_2(-1/z) = \sum_{b\neq 0} \frac{1}{b^2} + \sum_{a\neq 0}\sum_{b\in\mathbb{Z}} \frac{z^2}{(-a+bz)^2} = z^2\sum_{a\neq 0} \frac{1}{(az)^2} + z^2\sum_{b\neq 0}\sum_{a\in\mathbb{Z}} \frac{1}{(az+b)^2} =: z^2\tilde{E}_2(z).$$

Note que $E_2(z)$ e $\tilde{E}_2(z)$ são diferentes, pois a soma não é absolutamente convergente. De fato, pode-se provar que $E_2(z) - \tilde{E}_2(z) = \frac{2\pi i}{z}$. Pode-se deduzir isso da equação funcional da ζ (exercício). Agora note que

$$E_2^*(z) := E_2(z/2) - 4E(2z)$$

é um elemento de $M_2(\Gamma(2))$ pois $E_2^*(-1/z) = -z^2E_2^*(z)$.

Próxima aula usaremos análise complexa para provar que os espaços M_k tem dimensão finita sobre $\mathbb{C}$, e vamos calcular exatamente sua dimensão.

Por exemplo, veremos que $S_8 = 0$, e portanto E_4^2 e E_8 tem que ser proporcionais, isso é, existe c tal que

$$\left(-\frac{B_4}{8} + \sum_{n\geq 1}\sigma_3(n)q^n\right)^2 = c\cdot\left(-\frac{B_8}{16} + \sum_{n\geq 1}\sigma_7(n)q^n\right).$$

Como $B_4 = B_8 = -1/30$, temos $c = -16B_4^2/(8^2B_8) = 1/120$, e então

$$c\cdot\sigma_7(n) = \frac{-2B_4}{8}\sigma_3(n) + \sum_{k=1}^{n-1}\sigma_3(k)\sigma_3(n-k),$$

portanto

$$\sigma_7(n) = \sigma_3(n) + 120\sum_{k=1}^{n-1}\sigma_3(k)\sigma_3(n-k).$$

Também veremos que $M_0 = \mathbb{C}$, e como $(\theta_0)^4/E_2^* \in M_0$, (precisamos saber que θ_0 e E_2^* tem os mesmos zeros para saber que isso é holomórfico), temos $(\theta_0)^4 = cE_2^*$. Note que

$$\begin{aligned} E_2^*(z) = E_2(z/2) - 4E(2z) &= 2(2\pi i)^2 \left(\frac{3B_2}{4} + \sum_{n\geq 1} \sigma_1(n)(e^{2\pi inz/2} - 4e^{4\pi inz}) \right) \\ &= -8\pi^2 \left(\frac{1}{8} + \sum_{n\geq 1} \sigma_1(n)e^{\pi inz} - \sum_{4|n} 4\sigma_1(n/4)e^{\pi inz} \right) \\ &= -\pi^2 \left(1 + 8\sum_{n\geq 1} \sigma_1^*(n)e^{\pi inz} \right) \end{aligned}$$

onde $\sigma_1^*(n) = \sum_{4\nmid d|n} d$. Portanto, existem $8\sigma_1^*(n)$ maneiras de escrever n como a soma de 4 quadrados.

Exercícios

(1) (a) Considere $E_2(z) = \pi^2/3 - 8\pi^2 \sum_{n\geq 1} \sigma_1(n) q^n$ como no texto. Seja $f(z) = E_2(z) - \pi^2/3$, e prove que se $\mathrm{Re}(s) > 3$,[31]

$$M\{f\}(s) = 2\pi(1-s)\Lambda(s)\Lambda(s-1).$$

(b) Conclue da equação funcional da ζ que $M\{f\}(s)$ é meromórfica para $s \in \mathbb{C}$, e que $M\{f\}(2-s) = -M\{f\}(s)$. Ache os pólos de $M\{f\}(s)$ e calcule seus resíduos.

(c) A fórmula de inversão de Mellin para $x > 0$

$$E_2(ix) - \frac{\pi^2}{3} = \frac{1}{2\pi i} \int_{c-\infty}^{c+\infty} M\{f\}(s) x^{-s} \, \mathrm{d}s$$

é válida desde que a expressão de $M\{f\}(s)$ seja convergente para $\mathrm{Re}(s) > c$, portanto para $c > 3$ no nosso caso.

Use a fórmula de resíduos para mudar o contorno da integral e provar que

$$E_2(ix) - \frac{\pi^2}{3} = \frac{2\pi}{y} - \frac{\pi^2}{3y^2} + \frac{1}{2\pi i} \int_{-2-\infty}^{-2+\infty} M\{f\}(s) x^{-s} \, \mathrm{d}s$$

(d) Use a equação funcional de $M\{f\}(s)$ para obter que se $x > 0$,

$$E_2(ix) + \frac{E_2(i/x)}{x^2} = \frac{2\pi}{x},$$

e conclua que $E_2(z) - \tilde{E_2}(z) = 2\pi i/z$ para todo $\mathrm{Im}(z) > 0$.

(2) Seja $f \in M_k$. Prove que $f(\omega) = \omega^k f(\omega)$, e conclua que $f(\omega) = 0$ se $3 \nmid k$. Prove também que $f(i) = i^k f(i)$, e portanto conclua que $f(i) = 0$ se $4 \nmid k$.

[31] Use a fórmula da duplicação $\Gamma(s)\Gamma(s+1/2) = 2^{1-2s}\sqrt{\pi}\Gamma(2s)$.

11. 22 de Maio

Hoje vamos provar que M_k tem dimensão finita sobre $\mathbb{C}$, e vamos calcular tal dimensão.

11.1. **Cota por cima.** A ideia para isso é o seguinte: Vamos provar que se $f \in M_k$ não é zero, então não tem muitos zeros. Agora se tivermos $f_1, \dots, f_n \in M_k$, podemos tentar escolher uma combinação linear que tenha vários zeros, mas pelo o que iremos provar, isso implicaria que a combinação linear é 0, e portanto que f_i não são linearmente independentes.

Lembre-se que D é o domínio fundamental para a ação de $\mathrm{SL}_2(\mathbb{Z})$ em $\mathbb{H}$, dado por

$$D = (\{-1/2 \le \mathrm{Re}(z) \le 1/2\} \cap \{|z| > 1\}) \cup (\{-1/2 \le \mathrm{Re}(z) \le 0\} \cap \{|z| = 1\})$$

Teorema 11.1. *Seja $f \in M_k$. Então*

$$\mathrm{ord}_\infty(f) + \frac{\mathrm{ord}_i(f)}{2} + \frac{\mathrm{ord}_\omega(f)}{3} + \sum_{\tau \in D - \{i,\omega\}} \mathrm{ord}_\tau(f) = \frac{k}{12}.$$

Demonstração. Isso segue de integrar f'/f na borda de D, retirando círculos de raio ϵ em volta de cada zero de f no caminho, e tomando $\epsilon \to 0$ (na parte de cima de D, corta em $\mathrm{Im}(z) = R$ e também toma $R \to \infty$). Os pólos de f'/f são os zeros de f com resíduo igual a ordem do zero. Para os pontos na borda, note que integrar uma função holomórfica g em volta de z_0 com ângulo α e raio indo para zero resulta em $\alpha i \cdot \mathrm{res}_{z_0} g$. Todo ponto na borda exceto i e ω aparecem duas vezes módulo $\mathrm{SL}_2(\mathbb{Z})$ e com ângulo π, i aparece uma vez com ângulo π e ω aparece duas vezes (ω e $-\omega^2$) com ângulo $\pi/3$.

Resta ver que a contribuição da integral na borda é $k/12$. A integral nas bordas $\mathrm{Re}(z) = \pm 1/2$ cancelam pois $(f'/f)(z+1) = (f'/f)(z)$. Resta a integral de $e^{2\pi i/3}$ a $e^{2\pi i/6}$. Quebramos isso na metade e usamos $z \mapsto -1/z$ para levar um dos arcos no outro. Como

$$\frac{f'(1/z)}{f(-1/z)} = \frac{kz^{k-1}f(z) + z^k f'(z)}{z^k f(z)} = \frac{k}{z} + \frac{f'(z)}{f(z)},$$

essa integral nos dá $\int_i^\omega k \, \mathrm{d}z/z = (2\pi i)k/12$ pois o arco tem tamanho $\pi/3 - \pi/2 = \pi/6$. □

Denote $\overline{D} = D \cup \infty$. Queremos escolher $f \in M_k$ com o menor $\sum_{\tau \in \overline{D}} \mathrm{ord}_\tau(f)$. Pelo resultado acima, isso é o mesmo que

$$\frac{k}{12} + \frac{\mathrm{ord}_i(f)}{2} + \frac{2\mathrm{ord}_\omega(f)}{3}.$$

Seja $a = \min_{f \in M_k - \{0\}} \operatorname{ord}_i(f)$ e $b = \min_{f \in M_k - \{0\}} \operatorname{ord}_\omega(f)$. Podemos escolher f_1, f_2 tal que $\operatorname{ord}_i(f_1) = a$ e $\operatorname{ord}_\omega(f_2) = b$. Então podemos tomar f_0 com $\operatorname{ord}_i(f_0) = a$ e $\operatorname{ord}_\omega(f_0) = b$: se f_1 e f_2 não funcionam, então $f_1 + f_2$ funciona.

Agora que temos controle sobre a quantidade de zeros de formas modulares, vamos formalizar como isso implica em controlar a dimensão de M_k.

Proposição 11.2. *Temos* $\dim_{\mathbb{C}} M_k \leq \lfloor k/12 \rfloor + 1$, *e se* $k \equiv 2 \mod 12$, *então* $\dim_{\mathbb{C}} M_k \leq \lfloor k/12 \rfloor$.

Demonstração. Primeiro, note pelo teorema anterior que $M_0 = \mathbb{C}$. De fato, se $f \in M_0$, então $f(z) - f(i) \in M_0$, mas se qualquer elemento de M_0 possui um zero, então é zero. Portanto $M_0 = \mathbb{C}$.

Agora escolha $f_0 \in M_k$ como acima. Considere $f \mapsto f/f_0$. f/f_0 transforma como uma função modular de peso 0, mas talvez não seja holomórfica. Seja $N(f) = \sum_{\tau \in \overline{D}} \operatorname{ord}_\tau(f)$. Considere o mapa $f \mapsto f/f_0 \mapsto \mathbb{C}^{N(f)-a-b}$ onde para cada $\tau \notin \{i, \omega\}$, coletamos os termos de $z^{-\operatorname{ord}_\tau(f)}, \ldots, z^{-1}$ na expansão de Taylor, e para i, ω coletamos os termos de $z^{-\operatorname{ord}_i(f)+a}, \ldots, z^{-1}$ e $z^{-\operatorname{ord}_\omega(f)+b}, \ldots, z^{-1}$.

Isso nos dá um mapa $M_k \to \mathbb{C}^{N(f)-a-b}$, e o kernel é dado pelos f tal que $f/f_0 \in M_0 = \mathbb{C}$, e portanto tem dimensão 1. Ou seja, concluímos que $\dim_{\mathbb{C}} M_k \leq 1 + N(f) - a - b$. Portanto

$$\dim_{\mathbb{C}} M_k \leq 1 + \frac{k}{12} - \frac{a}{2} - \frac{b}{3}.$$

Agora note que se $f \in M_k$

$$f(i) = f(1/i) = i^k f(i), \quad \text{e} \quad f(\omega) = f(-\omega^2 - 1) = f(-\omega^2) = f(-1/\omega) = \omega^k f(\omega),$$

e portanto $a \geq 1$ se $4 \nmid k$ e $b \geq 1$ se $3 \nmid k$. Isso dá a desigualdade que queremos. □

11.2. **Cota por baixo.** Vamos provar que essa cota que provamos é a dimensão correta pois podemos construir a mesma quantidade de formas modulares com as séries de Eisenstein.

Lema 11.3. *E_4 e E_6 são algébricamente independentes.*

Demonstração. Assuma que exista $f \in \mathbb{C}[x, y]$ tal que $f(E_4, E_6) = 0$, e escolha f de grau mínimo. Escreva $f = \sum_{i \geq 0} f_i$ onde f_i é homogêneu de grau i, onde x tem grau 4 e y tem grau 6. Como temos

$$f(E_4, E_6)(\gamma(z)) = \sum_{i \geq 0} (cz + d)^i f(E_4, E_6)(z)$$

para todo $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, isso implica que temos que ter $f_i = 0$ para todo i. Agora vamos provar que $xy \mid f$, o que contradizeria a minimalidade de f. Isso segue de $0 = f(E_4, E_6)(i) = f(E_4, E_6)(\omega)$, pois $E_4(\omega) = E_6(i) = 0$ e $E_4(i) \neq 0, E_6(\omega) \neq 0$ (podemos ver que tais zeros são os únicos zeros pelo teorema acima). □

Isso implica que $E_4^a E_6^b \in M_k$ com $4a + 6b = k$ são linearmente independentes. Podemos ver que isso dá o mesmo número da cota anterior. Portanto:

Corolário 11.4. *M_k tem base dada por $\{E_4^a E_6^b \colon 4a + 6b = k\}$.*

Outro jeito de vermos isso, é considerando[32]

$$\Delta = 8000E_4^3 - 147E_6^2.$$

Os coeficientes são simplesmente para fazer $\Delta(\infty) = 0$. Esse é o menor exemplo de forma de cúspide, de peso 12. Pelo teorema, temos que ∞ é o único zero de Δ. Portanto, temos uma bijeção

$$M_{k-12} \xrightarrow[\sim]{\cdot\Delta} S_k.$$

Podemos computar que $M_2 = 0$ e M_4, M_6, M_8, M_{10} são 1-dimensionais gerados pelas séries de Eisenstein pelo teorema, do mesmo jeito que provamos $M_0 = \mathbb{C}$. Como $E_k(\infty) \neq 0$, temos $M_k = \mathbb{C}E_k \oplus S_k$ para $k \geq 4$ par, e da bijeção cima, temos a mesma quantidade de formas modulares que provamos na cota anteriormente.

[32]Veremos que formas modulares podem ser pensadas como funções em curvas elípticas, e essa normalização é escolhida de modo que Δ seja o discriminante da curva elíptica.

Exercícios

(1) Analise o domínio fundamental de $\Gamma(2)$ e use os mesmos métodos para provar que se $f \in M_k(\Gamma(2))$, então $\sum_{\tau \in \overline{D_\Gamma}} \mathrm{ord}_\tau(f) = 1 + k/2$. Conclua que $\dim_{\mathbb{C}} M_k(\Gamma(2)) \leq 1 + k/2$.

(2) Tome $k = 2$ no item anterior. Lembre-se que temos $E_2^*, \theta_0^4 \in M_2(\Gamma(2))$, e lembre-se que ambas satisfazem também a identidade

$$f(-1/z) = -z^2 f(z).$$

Prove que se $f \in M_2(\Gamma(2))$ satisfaz a equação acima, então $f(\infty) = 0 \implies f(0) = f(1) = 0$, e conclua pelo item anterior que isso implica que $f = 0$. Conclua que a maneria de escrever n como a soma de 4 quadrados é igual a

$$8 \sum_{4 \nmid d \mid n} d.$$

(3) Seja $\Delta(z) = \sum_{n \geq 1} \tau(n) q^n$ a expansão de Fourier de Δ. A função τ é chamada de função τ de Ramanujan. Use que $\Delta, E_{12}, E_6^2 \in M_{12}$ para conseguir uma combinação linear delas que é 0, e use isso para concluir que

$$\tau(n) \equiv \sigma_{11}(n) \mod 691.$$

12. 29 de Maio

12.1. **Função L de uma forma modular.** A nossa motivação inicial para considerar formas modulares foi generalizar a prova da equação funcional de ζ. Vamos então discutir com um pouco mais de detalhe a função L associada a $f \in M_k$.

Se $f \in M_k$, então de $f(z+1) = f(z)$ e da holomorficidade em ∞, temos a expansão de Fourier $f(z) = \sum_{n\geq 0} a_n(f) e^{2\pi i n z}$, onde

$$a_n(f) = e^{-2\pi n y} \int_0^1 f(x+iy) e^{2\pi i n x} \, \mathrm{d}x.$$

Lembre-se que definimos

$$L(s,f) = \sum_{n\geq 1} \frac{a_n(f)}{n^s}.$$

Vamos ver que isso converge para alguns s:

Proposição 12.1. *Se $f \in S_k$, então $a_n(f) = O(n^{k/2})$. Se $f \in M_k$, então $a_n(f) = O(n^{k-1})$.*

Demonstração. Seja $k \geq 4$ par. Como $M_k = \mathbb{C}E_k \oplus S_k$, basta provar que $a_n(E_K) = O(n^{k-1})$ e $a_n(f) = O(n^{k/2})$ para $f \in S_k$.

Temos $a_n(E_k)/n^{k-1} = \sigma_{k-1}(n)/n^{k-1} = \sum_{d|n} d^{-(k-1)} \leq \zeta(k-1)$, portanto $a_n(E_K) = O(n^{k-1})$.

Se $f \in S_k$, então queremos usar que $f(\infty) = 0$ para cotar $|f(z)|$. Considere $F(z) = f(z)|\mathrm{Im}(z)|^{k/2}$. Isso é tal que $|F(\gamma(z))| = |F(z)|$. Como $f(\infty) = 0$, temos que $F(z)$ é limitada perto de ∞. Ou seja, existem $N, M > 0$ tal que $|F(z)| < M$ se $\mathrm{Im}(z) > N$. Mas agora $D \cap \{\mathrm{Im}(z) \leq N\}$ é fechado e limitado, portanto F é limitada em D. Então temos

$$|a_n(f)| \leq e^{-2\pi n y} \int_0^1 |F(x+iy)| y^{-k/2} \, \mathrm{d}x \leq C y^{-k/2} e^{-2\pi n y}$$

para qualquer y, e tomando $y = 1/n$, temos $a_n(f) = O(n^{k/2})$. □

Corolário 12.2. *Se $f \in M_k$, então $L(s,f) = \sum_{n\geq 1} a_n(f)/n^s$ converge absolutamente para $\mathrm{Re}(s) > k$, e se $f \in S_k$, converge absolutamente para $\mathrm{Re}(s) > 1 + k/2$.*

Lembre-se que temos $\Lambda(s,f) := (2\pi)^{-s}\Gamma(s)L(s,f) = M\{f - a_0(f)\}(s) := \int_0^\infty (f(ix) - a_0(f)) x^{s-1} \, \mathrm{d}x$.

Teorema 12.3. *$\Lambda(s,f)$ é meromórfica para $s \in \mathbb{C}$, e satisfaz a equação funcional $\Lambda(s,f) = (-1)^{k/2}\Lambda(k-s,f)$. Λ é holomórfica exceto por pólos simples em $s = 0$ e $s = k$ com resíduos $a_0(f)$ e $(-1)^{1+k/2}a_0(f)$.*

Demonstração. Como $f(i/x) = f(-1/ix) = (ix)^k f(ix)$, se denotarmos $f_0(ix) = f(ix) - a_0(f)$, temos $f_0(i/x) = (ix)^k f_0(ix) + a_0(f)((ix)^k - 1)$, e então temos

$$\begin{aligned} M\{f_0\}(s) &= \int_0^1 f_0(ix)x^{s-1}\,\mathrm{d}x + \int_1^\infty f_0(ix)x^{s-1}\,\mathrm{d}x \\ &= \int_0^1 f_0(ix)x^{s-1}\,\mathrm{d}x + \int_0^1 (ix)^k f_0(ix)x^{1-s}x^{-2} + a_0(f)((-1)^{k/2}x^{k-s-1} - x^{-s-1})\,\mathrm{d}x \\ &= a_0(f)\left(\frac{(-1)^{k/2}}{k-s} + \frac{1}{s}\right) + \int_0^1 f_0(ix)\left(x^{s-1} + (-1)^{k/2}x^{k-s-1}\right)\,\mathrm{d}x. \end{aligned}$$

E portanto a equação funcional segue se soubermos que $M\{f_0\}(s)$ é meromórfica.

O segundo termo na expressão acima é holomórfico pois $f_0(ix) = O(e^{-2\pi/x})$ quando $x \to 0$. □

Todas as funções L que encontramos anteriormente tinham um *produto de Euler*, como por exemplo $\zeta_K(s) = \prod_{\mathfrak{p}}(1 - N(\mathfrak{p})^{-s})^{-1}$, ou $L(s,\chi) = \prod_p(1 - \chi(p)p^{-s})^{-1}$ ou para uma curva elíptica $E/\mathbb{Q}$, $L(s, E/\mathbb{Q}) = \prod_p(1 - a_p p^{-s} + p^{1-2s})^{-1}$.

Então se queremos associar uma formas modular f a tais objetos (lembre-se que basicamente fizemos isso com $\zeta(s)$ e $L(s,\chi)$ com as funções θ), então tem que ser verdade que $L(s,f)$ também satisfaz um produto de Euler. Em particular, tem que ser verdade que $a_n(f)$ é multiplicativo. Vamos identificar uma classe de formas modulares, chamadas *autoformas de Hecke*.

Exemplo 12.4. As séries de Eisenstein serão exemplos de autoformas de Hecke: Seja E_k normalizada de modo que $a_1(E_k) = 1$. Então lembre-se que $a_n(E_k) = \sigma_{k-1}(n)$, e note que isso é multiplicativo! Além disso, temos

$$\sigma_{k-1}(p^n) = \sum_{i=0}^{n} p^{(k-1)i} = \frac{p^{(k-1)(n+1)} - 1}{p^{k-1} - 1},$$

e portanto

$$\begin{aligned} \sum_{n\geq 0} \frac{\sigma_{k-1}(p^n)}{p^{ns}} &= \frac{1}{p^k - 1}\sum_{n\geq 0}(p^{n(k-1-s)+k-1} - p^{-ns}) = \frac{p^{k-1}(1 - p^{k-1-s})^{-1} - (1-p^{-s})^{-1}}{p^k - 1} \\ &= (1 - p^{k-1-s})^{-1}(1-p^{-s})^{-1}. \end{aligned}$$

Note que

$$L(s, E_k) = \zeta(s)\zeta(s - k + 1).$$

Exemplo 12.5. Outro exemplo de autoforma será $\Delta(z)$. Ramanujan inicialmente definiu tal função como $\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24}$ (vamos provar essa igualdade num exercício) e conjecturou que

seus coeficientes de Fourier $\tau(n)$ eram multiplicativos. Vamos provar que isso é verdade quando provarmos que $\Delta(z)$ é uma autoforma.

12.2. **Operadores de Hecke.** Vamos criar certas operações em formas modulares que serão a chave para entender as autoformas.

Primeiro, vamos reinterpretar a condição $f(\gamma(z)) = (cz+d)^k f(z)$. Para isso, dado $\tau \in \mathbb{H}$, podemos considerar o lattice $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$. Seja $\mathcal{L}$ o conjunto de lattices em $\mathbb{C}$.

Proposição 12.6. *Temos uma bijeção*

$$\mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \leftrightarrow \mathcal{L}/\mathbb{C}^\times.$$

Note que o lado esquerdo é representado por D.

Demonstração. Dado um lattice Λ, seja $\alpha \in \Lambda$ um ponto não-zero de menor tamanho. Então considere Λ/α para podermos assumir que $\alpha = 1$. Agora se τ é de modo que $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$, podemos escolher τ unicamente de modo que $\tau \in \mathbb{H}$ e $-1/2 \leq \mathrm{Re}(\tau) < 1/2$. Se $|\tau| = 1$, e $\mathrm{Re}(\tau) > 0$, então $-\Lambda/\tau = \mathbb{Z} \oplus \mathbb{Z}(-\tau^{-1})$, e note que $\mathrm{Re}(-\tau^{-1}) < 0$. □

Portanto se f é uma forma modular, queremos construir uma função $F\colon \mathcal{L} \to \mathbb{C}$. Isso será de tal modo que $F(\Lambda_\tau) = f(\tau)$ para $\tau \in \mathbb{H}$. Mas então, temos

$$F(\Lambda_{-\tau^{-1}}) = f(-1/\tau) = \tau^k f(\tau) = \tau^k F(\Lambda_\tau).$$

Como $\Lambda_{-\tau^{-1}} = \tau^{-1}\Lambda_\tau$, temos que $F(\tau\Lambda) = \tau^{-k}F(\Lambda)$ para $\Lambda = \Lambda_{-\tau^{-1}}$.

Junto com a proposição anterior, isso prova que:

Proposição 12.7. *Temos uma bijeção entre $f\colon \mathbb{H} \to \mathbb{C}$ satisfazendo $f(\gamma(z)) = (cz+d)^k f(z)$ e funções $F\colon \mathcal{L} \to \mathbb{C}$ satisfazendo $F(c\Lambda) = c^{-k}F(\Lambda)$.*

Agora podemos definir os *operadores de Hecke*.

Definição 12.8. Seja $n \in \mathbb{Z}_{\geq 1}$ e $F\colon \mathcal{L} \to \mathbb{C}$. O n-ésimo *operador de Hecke* é o operador T_n definido por

$$(T_n F)(\Lambda) = \sum_{\Lambda' \subseteq \Lambda\colon\ [\Lambda:\Lambda']=n} F(\Lambda').$$

Pelas considerações anteriores, é fácil ver que T_n induz um mapa $T_n\colon M_k \to M_k$.

Proposição 12.9. *Se $(n,m)=1$, temos $T_nT_m=T_{nm}$. Para $F\colon \mathcal{L}\to\mathbb{C}$, seja $(R_pF)(\Lambda)=F(p\Lambda)$. Então temos $T_{p^{n+2}}=T_{p^{n+1}}T_p-pT_{p^n}R_p$ para $n\geq 0$.*

Demonstração. Para a primeira igualdade, note que se $[\Lambda:\Lambda']\simeq nm$, existe um único $\Lambda'\subseteq\Lambda_0\subseteq\Lambda$ com $[\Lambda:\Lambda_0]=m$. Isso dá uma bijeção nos lattices envolvidos nos operadores T_nT_m e T_{nm}.

Para a segunda fórmula, considere $\Lambda'\subseteq\Lambda$ com $[\Lambda:\Lambda']=p^{n+2}$. Se $\Lambda'\not\subseteq p\Lambda$, existe um único $\Lambda'\subseteq\Lambda_0\subseteq\Lambda$ tal que $[\Lambda:\Lambda_0]=p$, e portanto esses termos de $T_{p^{n+2}}$ são um subconjunto dos termos de $T_{p^{n+1}}T_p$. Se $\Lambda'\subseteq p\Lambda$, existem $p+1$ tais Λ_0, e portanto temos que subtrair $pT_{p^n}R_p$. □

Corolário 12.10. *Os operadores T_n comutam para todo $n\in\mathbb{Z}_{\geq 1}$.*

Demonstração. Basta ver que R_p e T_q comutam para primos p,q, pois todo T_n é um polinômio nos R_p e T_q. Provamos acima que T_p comutam entre si, e é simples ver que R_p comutam entre si e com os T_q. □

12.3. **Operadores de Hecke na expansão de Fourier.** Vamos calcular como T_n afeta a expansão de Fourier.

Para isso, vamos descrever exatamente quais são os lattices $\Lambda'\subseteq\Lambda$ com $[\Lambda:\Lambda']=n$.

Proposição 12.11. *O conjunto de todos os lattices $\Lambda'\subseteq\Lambda$ com $[\Lambda:\Lambda']=n$ é dado por $\Lambda'=M\Lambda$ onde M percorre as seguintes matrizes:*

$$\left\{\begin{pmatrix} a & b\\ 0 & d\end{pmatrix} : ad=n,\ a,d>0,\ 0\leq b<d\right\}.$$

Demonstração. Isso é o mesmo que encontrar as matrizes M tal que $[\mathbb{Z}^2:M\mathbb{Z}^2]=n$ módulo multiplicação pela esquerda por $\mathrm{SL}_2(\mathbb{Z})$. Note que dado $\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in M_{2\times 2}(\mathbb{Z})$, e se $l=(a,c)$, temos

$$\begin{pmatrix} \alpha & \beta\\ -c/l & a/l\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} * & *\\ 0 & *\end{pmatrix}$$

onde podemos escolher α,β de modo que a primeira matrix esteja em $\mathrm{SL}_2(\mathbb{Z})$. Então queremos encontrar

$$\left\{M=\begin{pmatrix} a & b\\ 0 & d\end{pmatrix} : \mathbb{Z}^2/M\mathbb{Z}^2\simeq\mathbb{Z}/n\mathbb{Z}\right\}$$

módulo multiplicação por $\mathrm{SL}_2(\mathbb{Z})$ na esquerda. Como o determinante de M é n, temos que ter $ad = n$. Agora note que

$$\begin{pmatrix} 1 & l \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b+ld \\ 0 & d \end{pmatrix},$$

e portanto podemos tomar $0 \leq b + ld < d$. Trocando M por $-M$, também podemos assumir $a, d > 0$.

Agora resta ver que se $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ e $M' = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$ estão no conjunto mencionado e são distintos, então $M\mathbb{Z}^2 = M'\mathbb{Z}^2$ implica $M = M'$. Ou seja, queremos ver que se $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ e $\sigma M = M'$, então $\sigma = 1$. Mas temos

$$\sigma = M'M^{-1} = \frac{1}{n} \begin{pmatrix} a'd & ab' - a'b \\ 0 & ad' \end{pmatrix},$$

e daí $n \mid a'd, ad'$, e como $ad = a'd' = n$, isso implica $a = a', d = d'$. Mas daí $n \mid a(b'-b) \implies d \mid b' - b$, e portanto $b = b'$. □

Corolário 12.12. *Se $f \in M_k$ tem expansão de Fourier $\sum_{n\geq 0} a_n q^n$, então*

$$(T_m f)(z) = m^{1-k} \sum_{n\geq 0} q^n \sum_{d|(n,m)} d^{k-1} a_{nm/d^2}.$$

Em particular, T_m mantém formas de cúspide.

Demonstração. Se $F\colon \mathcal{L} \to \mathbb{C}$ corresponde a f, pela proposição acima, temos

$$(T_m f)(z) = \sum_{d|m} \sum_{b=0}^{d-1} F\left(\mathbb{Z}(\frac{m}{d}z + b) \oplus d\mathbb{Z}\right) = \sum_{d|m} \sum_{b=0}^{d-1} d^{-k} f((mz+bd)/d^2).$$

Portanto

$$(T_m f)(z) = \sum_{n\geq 0} \sum_{d|m} d^{-k} \sum_{b=0}^{d-1} a_n e^{2\pi i n(mz+bd)/d^2}.$$

Note que se $d \nmid n$, então $\sum_{b=0}^{d-1} e^{2\pi i n(mz+bd)/d^2} = 0$. Se $d \mid n$, isso é $d \cdot e^{2\pi i n m/d^2}$. Portanto

$$\begin{aligned}(T_m f)(z) &= \sum_{d|m} d^{-k} \sum_{d|n} \sum_{b=0}^{d-1} a_n e^{2\pi i n(mz+bd)/d^2} = \sum_{d|m} d^{-k} \sum_{n\geq 0} \sum_{b=0}^{d-1} a_{nd} e^{2\pi i n(mz+bd)/d} \\ &= \sum_{d|m} d^{1-k} \sum_{n\geq 0} a_{nd} e^{2\pi i n m z/d} = m^{1-k} \sum_{d|m} d^{k-1} \sum_{n\geq 0} a_{nm/d} e^{2\pi i n d z} \\ &= m^{1-k} \sum_{n\geq 0} q^n \sum_{d|(n,m)} d^{k-1} a_{nm/d^2}\end{aligned}$$

□

Agora denote $T(m) := R_{m^{-1}} T_m / m$, de modo que se $f \in M_k$, então

$$T(m)f = m^{k-1} T_m f = \sum_{n\geq 0} q^n \sum_{d|(n,m)} d^{k-1} a_{nm/d^2}.$$

Portanto,

$$T(m)f = \sigma_{k-1}(n) a_0 + a_m q + \cdots .$$

12.4. **Autoformas de Hecke.**

Definição 12.13. Dizemos que $f \in M_k$ é uma *autoforma de Hecke* se f é um autovetor de todos os $T(n)$. Isso é, se existem $\lambda_n \in \mathbb{C}$ tal que $T(n)f = \lambda_n f$.

Proposição 12.14. *Seja $f \in M_k$ uma autoforma. Então $a_1 = 0 \iff f$ é constante, e se $f \neq 0$, então $\lambda_n = a_n/a_1$. Além disso, se $f \notin S_k$, então $f = cE_k$ para $c \in \mathbb{C}$ ou f é constante.*

Demonstração. Pelo cálculo acima, temos que $a_n = \lambda_n a_1$, e portanto se $a_1 = 0$, temos $a_n = 0$ para todo $n \geq 1$, e portanto f é uma constante, o que não é possível se $k \neq 0$ a não ser que $f = 0$.

Agora se $a_1 \neq 0$, a observação acima diz que $\lambda_n = a_n/a_1$.

Se $f \notin S_k$, isso significa que $a_0 \neq 0$. Pelo cálculo acima, temos que $\lambda_n = \sigma_{k-1}(n)$, e portanto que $a_n = \sigma_{k-1}(n) a_1$, e portanto $f = C + a_1 E_k$ para uma constante C, e portanto $f = a_1 E_k$ ou f é constante. □

Corolário 12.15. *Se $f \in M_k$ é uma autoforma normalizada com $a_1 = 1$, então a_n é multiplicativo, e $a_{p^{n+2}} = a_p a_{p^{n+1}} - p^{k-1} a_{p^n}$. Em particular, temos*

$$L(s, f) = \prod_p (1 - a_p p^{-s} + p^{k-1} p^{-2s})^{-1}.$$

Demonstração. Pela normalização, temos $a_n = \lambda_n$, e agora as relações seguem das relações de T_n. Por exemplo:

$$\begin{aligned} a_{p^{n+2}} f &= T(p^{n+2})(f) = p^{(n+2)(k-1)} T_{p^{n+2}}(f) = p^{(n+2)(k-1)} T_p T_{p^{n+1}}(f) - p^{(n+1)(k-1)} T_{p^n}(f) \\ &= T(p)T(p^{n+1})f - p^{k-1}T(p^n)f = (a_p a_{p^{n+1}} - p^{k-1} a_{p^n}) f. \end{aligned}$$

A fatoração de $L(s, f)$ segue formalmente dessas relações. □

O que iremos provar na aula seguinte é que de fato, S_k tem uma base dada por autoformas! Portanto teremos exatamente $\dim_{\mathbb{C}} S_k$ autoformas normalizadas, que formam uma base canônica para S_k.

No entanto, já podemos provar que Δ é uma autoforma, provando a conjectura de Ramanujan.

Exemplo 12.16. Nós provamos anteriormente que $S_{12} = \mathbb{C} \cdot \Delta$. Mas vimos também que $T(n)$ mantém S_k, e portanto Δ é uma autoforma. Em particular, $\tau(n)$ é multiplicativo!

Exercícios

(1) Seja E_2 a série de Eisenstein proibida. Lembre-se que E_2 *não* é uma forma modular, mas provamos num exercício anterior que $E_2(-1/z) = z^2(\frac{1}{2\pi i} + E_2(z))$. Considere o operador $\theta = \frac{1}{2\pi i}\frac{\mathrm{d}}{\mathrm{d}z} = q\frac{\mathrm{d}}{\mathrm{d}q}$, ou seja, que leva $f(z) = \sum_{n\geq 0} a_n q^n$ em $(\theta f)(z) = \sum_{n\geq 0} n a_n q^n$.

Considere $\delta := 4\pi^2\theta - kE_2$. Prove que se $f \in M_k$, então $\delta f \in M_{k+2}$.

(2) Use o item anterior com $f = \Delta$ para provar que $\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24}$.

13. 5 de Junho

13.1. **Autoformas de Hecke.** Primeiro vamos concluir a discussão da semana passada. Queremos encontrar uma base para M_k que consista em autoformas.

Introduzimos os operadores de Hecke $T(n)\colon M_k \to M_k$, e definimos *autoformas* para serem os autovetores de todos os $T(n)$. Vimos que as autoformas são tais que suas funções L tem um produto de Euler.

Também vimos que E_k são autoformas, e portanto precisamos encontrar uma base de S_k de autoformas. Ou seja, queremos diagonalizar todos os operadores $T(n)\colon S_k \to S_k$ simultaneamente. Usaremos o seguinte resultado de álgebra linear:

Teorema 13.1. *Seja V um espaço vetorial sobre $\mathbb{C}$ de dimensão finita com um produto interno $\langle\cdot,\cdot\rangle\colon V\times V\to\mathbb{C}$. Suponha que S é um conjunto de operadores lineares $f\colon V\to V$* normais *(ou seja, que $\langle fv, v'\rangle = \langle v, fv'\rangle$) e que comutam entre si. Então V pode ser diagonalizado simultaneamente para todos os operadores em S.*

Demonstração. Vamos provar isso por indução em $\dim V$. Se $\dim V = 1$, isso é trivial.

Se todos os operadores de S atuam como um escalar, também terminamos. Caso contrário, existe $f \in S$ que não é um escalar. Vamos provar depois que $V = \bigoplus_\lambda V_\lambda$ pode ser diagonalizado tal que $f|_{V_\lambda} = \lambda \cdot \mathrm{id}$. Então se $g \in S$ e $v \in V_\lambda$, temos que f, g comutam, e portanto que $\lambda g(v) = g(\lambda v) = g(f(v)) = f(g(v))$, e portanto $g(v) \in V_\lambda$, ou seja, temos que $g\colon V_\lambda \to V_\lambda$. Portanto podemos aplicar indução para cada um dos V_λ (que são menores que V pois f não é um escalar).

Ou seja, reduzimos o problema para o caso que $S = \{f\}$. Podemos encontrar um autovetor de f, digamos v_0 de autovalor λ. Considere $V^\perp := \{v \in V\colon \langle v, v_0\rangle = 0\}$. Note que

$$\langle f(v), v_0\rangle = \langle v, f(v_0)\rangle = \overline{\lambda}\langle v, v_0\rangle,$$

portanto $v \in V^\perp \implies f(v) \in V^\perp$. Portanto $f\colon V^\perp \to V^\perp$, e por indução temos que f pode ser diagonalizado em $V^\perp$. □

Portanto, para achar uma base de autoformas, precisamos somente encontrar um produto interno em S_k de tal forma que $T(n)$ sejam operadores normais. Isso é dado pelo seguinte:

Definição 13.2. O *produto escalar de Petersson* em S_k é dado por

$$\langle f, g\rangle := \int_D f(z)\overline{g(z)}y^k \frac{\mathrm{d}x\ \mathrm{d}y}{y^2}.$$

Isso é bem definido pois f, g decrescem exponencialmente em ∞. Os expoente de y são escolhidos de modo a termos:

Lema 13.3. *Seja $\gamma \in \mathrm{GL}_2(\mathbb{R})$ com $\det(\gamma) > 0$. Denote $\gamma(z) = (\gamma(x), \gamma(y))$. Então*

$$\frac{\mathrm{d}\gamma(x)\ \mathrm{d}\gamma(y)}{\gamma(y)^2} = \frac{\mathrm{d}x\ \mathrm{d}y}{y^2} \quad e \quad \gamma(y) = \frac{\det(\gamma)}{|cz+d|^2} y.$$

Demonstração. Temos $\gamma'(z) = \frac{a(cz+d)-c(az+b)}{(cz+d)^2} = \frac{\det(\gamma)}{(cz+d)^2}$ e $\gamma(y) = \frac{\det(\gamma)y}{|cz+d|^2}$, portanto

$$\begin{aligned}\frac{\mathrm{d}\gamma(x)\ \mathrm{d}\gamma(y)}{\gamma(y)^2} &= |\gamma'(z)|^2 \frac{y^2}{\gamma(y)^2} \frac{\mathrm{d}x\ \mathrm{d}y}{y^2} = \left|\frac{\det(\gamma)}{(cz+d)^2}\right|^2 \frac{|cz+d|^4}{\det(\gamma)^2} \frac{\mathrm{d}x\ \mathrm{d}y}{y^2} \\ &= \frac{\mathrm{d}x\ \mathrm{d}y}{y^2}.\end{aligned}$$

□

Portanto, o produto escalar é escolhido exatamente de modo que ele não depende da escolha do domínio fundamental D, pois se $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, também temos

$$f(\gamma(z))\overline{g(\gamma(z))}\gamma(y)^k = (cz+d)^k\overline{(cz+d)^k} f(z)\overline{g(z)} \frac{1}{|cz+d|^{2k}} y^k = f(z)\overline{g(z)} y^k.$$

Se $F, G \colon \mathcal{L} \to \mathbb{C}$ são associadas a f, g, podemos pensar nesse produto interno como

$$\int_{\mathcal{L}/\mathbb{C}^\times} F(\Lambda)\overline{G(\Lambda)} \det(\Lambda)^k\ \mathrm{d}\Lambda$$

pois temos $\det(\mathbb{Z} \oplus \mathbb{Z}z) = y$.

Proposição 13.4. *$T(n)$ são operadores simétricos em respeito ao produto escalar de Petersson.*

Demonstração. Pela observação acima, temos

$$\langle f, g\rangle = \int_{\mathcal{L}/\mathbb{C}^\times} F(\Lambda)\overline{G(\Lambda)}(\det\Lambda)^k\ \mathrm{d}\Lambda$$

e daí temos

$$\langle T(n)f, g\rangle = n^{1-k}\int_{\mathcal{L}/\mathbb{C}^\times} \overline{G(\Lambda)}(\det\Lambda)^k \sum_{[\Lambda:\Lambda']=n} F(\Lambda')\,\mathrm{d}\Lambda = n^{1-k}\int_{\mathcal{L}/\mathbb{C}^\times} F(\Lambda')(\det\Lambda'/n)^k \sum_{[\Lambda:\Lambda']=n} \overline{G(\Lambda)}\,\mathrm{d}\Lambda'.$$

Agora note que $\Lambda' \subseteq \Lambda$ tem índice n se e somente se $n\Lambda \subseteq \Lambda'$ tem índice n. Portanto podemos re-escrever a quantidade acima como

$$n^{1-k}\int_{\mathcal{L}/\mathbb{C}^\times} F(\Lambda')(\det\Lambda')^k \overline{\sum_{[\Lambda':n\Lambda]=n} G(\Lambda)n^{-k}}\ \mathrm{d}\Lambda' = n^{1-k}\int_{\mathcal{L}/\mathbb{C}^\times} F(\Lambda')(\det\Lambda')^k \overline{\sum_{[\Lambda':\Lambda]=n} G(\Lambda)}\ \mathrm{d}\Lambda'$$

que é simplesmente

$$\int_{\mathcal{L}/\mathbb{C}^\times} F(\Lambda)\overline{(T(n)G)(\Lambda)}(\det\Lambda)^k \, \mathrm{d}\Lambda = \langle f, T(n)g\rangle. \qquad \square$$

Corolário 13.5. *Para todo k, o espaço de formas modulares M_k possui uma base como espaço vetorial dada por autoformas de Hecke.*

Exemplo 13.6. Vamos tomar $k = 24$, o menor k tal que $\dim S_k > 1$ e calcular as autoformas. Nós sabemos que $M_{12} \xrightarrow[\sim]{\cdot\Delta} S_{24}$, e portanto podemos tomar $E_4^3\Delta$ e Δ^2 como uma base de S_{24}. Temos

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + \cdots,$$
$$E_4^3 = 1 + 720q + 179280q^2 + 16954560q^3 + 396974160q^4 + \cdots,$$

e daí

$$\Delta^2 = q^2 - 48q^3 + 1080q^4 + \cdots,$$
$$E_4^3\Delta = q + 696q^2 + 162252q^3 + 12831808q^4 + \cdots.$$

Vamos considerar

$$S := E_4^3\Delta - 696\Delta^2 = q + 195660q^3 + 12080128q^4 + \cdots.$$

Agora lembrando que

$$(T(2)f)(z) = \sigma_{k-1}(2)a_0 + a_2q + (2^{k-1}a_1 + a_4)q^2 + \cdots,$$

podemos computar

$$T(2)\Delta^2 = q + 1080q^2 + \cdots,$$
$$T(2)S = 20468736q^2 + \cdots.$$

Portanto, com a base $\{S, \Delta^2\}$, o operador $T(2)$ é dado por

$$\begin{pmatrix} 0 & 1 \\ 20468736 & 1080 \end{pmatrix}$$

cujos autovalores são

$$540 \pm 12\sqrt{144169}.$$

Portanto as duas autoformas em S_{24} tem expansão de Fourier que começa por

$$q + (540 \pm 12\sqrt{144169})q^2 + \cdots$$

e portanto são

$$S + (540 \pm 12\sqrt{144169})\Delta^2 = E_4^3\Delta - (156 \pm 12\sqrt{144169})\Delta^2.$$

Você pode ver mais sobre essa autoforma nesse link.

No exemplo acima, todas as autoformas de S_{24} são conjugadas. De fato, isso é conjecturado de maneira mais geral.

Conjectura 13.7. *O polinômio característico de $T(p)$ em S_k é irredutível. Em particular, todas as autoformas de S_k são conjugadas.*

13.2. **Curvas elípticas.** Agora vamos tomar uma tangente para discutir um pouco sobre curvas elípticas.

Definição 13.8. Seja F um corpo. Uma curva elíptica sobre F é uma curva projetiva E suave sobre F de genus 1 junto com um dado ponto $O \in E(F)$.

É um fato que toda curva elíptica é isomórfica às soluções de uma equação não degenerada $f \in F[x, y, z]$ de grau 3 no plano projetivo $\mathbb{P}(x : y : z)$. Além disso, se $\mathrm{char}(F) \neq 2, 3$, podemos tomar ainda $f(x, y, z) = y^2z - (x^3 - axz^2 + bz^3)$. Nesse caso, desde que $4a^3 - 27b^2 \neq 0$, a projetivização de $y^2 = x^3 - ax + b$ é um curva elíptica, com $O = (0 : 1 : 0)$.

13.3. **Funções duplamente periódicas.** Vamos provar que curvas elípticas sobre $\mathbb{C}$ estão e bijeção com lattices de $\mathbb{C}$ (e portanto com o domínio fundamental D).

Dado um lattice Λ, vamos formar $\mathbb{C}/\Lambda$ e vamos ver que isso é uma curva elíptica. Nesse caso, as coordenadas x/z e y/z são funções de $\mathbb{C}/\Lambda$, e portanto estamos interessados em funções $\mathbb{C}/\Lambda \to \mathbb{C} \cup \{\infty\}$. Ou seja, vamos considerar funções meromórficas de $\mathbb{C}/\Lambda \to \mathbb{C}$.

Proposição 13.9. *Seja $f\colon \mathbb{C} \to \mathbb{C}$ meromórfica e Λ-periódica. Então se D_Λ denota um domínio fundamental de Λ, temos*

$$\sum_{\tau \in D_\Lambda} \mathrm{ord}_\tau(f) = 0.$$

Demonstração. Como f é Λ-periódica, f' também é. Portanto, integrando f'/f na borda de D (possivelmente deslocando para evitar os pólos), temos o resultado. □

Proposição 13.10. *Seja $f\colon \mathbb{C} \to \mathbb{C}$ meromórfica e Λ-periódica. Se f tem no máximo 1 pólo simples, então f é constante.*

Demonstração. Suponha primeiro que f é holomórica. Como f é Λ-periódica, temos que $\sup f = \sup_{D_\Lambda} f$, e como D_Λ é limitada, segue que f é limitada. Mas f é holomórfica, e portanto por Liouville temos que f é constante.

Se f tivesse exatamente um pólo simples em z_0, escolha um domínio fundamental D' em que z_0 esteja no interior, note que $0 \neq 2\pi i \cdot \operatorname{res}_{z_0} f = \int_{\partial D'} f(z)\,\mathrm{d}z$, mas também podemos ver que essa integral é 0 pela periodicidade de f. □

Ou seja, os zeros e pólos de uma funçào Λ-periódica f basicamente determinam f. Vamos usar isso para classificar todas as funções Λ-periódicas.

Definição 13.11. Seja $\Lambda \subseteq \mathbb{C}$ um lattice. A *função $\wp$ de Weierstrass* é dada por

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0,0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Note que isso converge absolutamente em $\mathbb{C} - \Lambda$, pois pelo teorema do valor intermediário

$$\left| \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right| = \frac{2|z|}{\lambda_0^3}$$

onde λ_0 está entre λ e $\lambda - z$. Para algum R grande (que depende de z), temos $|\lambda| > R \implies |\lambda_0| > R/2$, e isso é o suficiente para concluir a convergência.

Proposição 13.12. *$\wp$ é Λ-periódica, par, e seus únicos pólos são pólos duplos em Λ. Além disso, $\wp'$ é Λ-periódica, ímpar, seus pólos são triplos em Λ e seus zeros são simples em $\frac{1}{2}\Lambda - \Lambda$.*

Demonstração. Pode-se provar a periodicidade rearranjando a soma e tomando cuidado com a convergência, mas também podemos ver isso pela derivada:

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

$\wp'$ é claramente Λ-periódica, e portanto isso prova que existe um morfismo de grupos $u\colon \Lambda \to \mathbb{C}$ tal que $\wp(z+\lambda) = \wp(z) + u(\lambda)$.

Mas $\wp$ também é par, e daí $\wp(\lambda/2) = \wp(-\lambda/2) + u(\lambda) = \wp(\lambda/2) + u(\lambda)$, o que prova que $u = 0$ e portanto que $\wp$ é Λ-periódica.

Os pólos de $\wp'$ são claros pela fórmula acima, e os zeros seguem de que se $\lambda \in \Lambda - 2\Lambda$, daí $\wp'$ é holomórfica em $\lambda/2$ e $\wp'(\lambda/2) = -\wp'(-\lambda/2) = -\wp'(\lambda/2)$, portanto $\wp'(\lambda/2) = 0$. □

Teorema 13.13. *Seja $f\colon \mathbb{C} \to \mathbb{C}$ meromórfica e Λ-periódica. Então existem polinômios $P_1, P_2, P_3 \in \mathbb{C}[x]$ tal que*

$$f = \frac{P_1(\wp) + \wp' \cdot P_2(\wp)}{P_3(\wp)}.$$

Demonstração. Sempre podemos escrever

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

e então podemos reduzir o problema para f par e f ímpar. Como $\wp'$ é ímpar, se f é ímpar podemos considerar $f/\wp'$. Portanto reduzimos o problem para provar que se f é par e Λ-periódica, então f é uma função racional em $\wp$.

Como f é par, podemos denotar por $\pm a_1, \ldots, \pm a_m$ os zeros de f com multiplicidade, e por $\pm b_1, \ldots, \pm b_m$ os pólos de f com multiplicidade em D_Λ. Note que $\wp(z) - \wp(a)$ tem zeros $a, -a$ em D_Λ com multiplicidade. Daí

$$\prod_{i=1}^{m} \frac{\wp(z) - \wp(a_i)}{\wp(z) - \wp(b_i)}$$

possui exatamente os mesmos zeros e pólos de f, e portanto f é tal expressão vezes uma constante.

□

Portanto $\wp$ e $\wp'$ são as funções Λ-periódica universais, com a única relação sendo o seguinte.

Teorema 13.14. *Sejam e_1, e_2, e_3 os três valores de $\wp$ em $\frac{1}{2}\Lambda - \Lambda$. Eles são distintos dois a dois, e temos*

$$(\wp'(z))^2 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3).$$

Demonstração. Considere $\wp(z) - e_1$. Isso só possui dois zeros módulo Λ. Um dos zeros está em $\frac{1}{2}\Lambda - \Lambda$, e como $\wp$ é par, possui ordem 2, e portanto é o único possível zero. Portanto e_i são distintos.

Agora vemos que os dois lados da expressão possuem os mesmos zeros, e podemos determinar a constante 4 comparando o resíduo dos dois lados em $z = 0$. □

13.4. **Relação com séries de Eisenstein.** Lembre-se que dado $E_k\colon \mathbb{H} \to \mathbb{C}$, também podemos pensar como uma função de lattices $E_k\colon \mathcal{L} \to \mathbb{C}$, dada em $\Lambda_\tau := \mathbb{Z} \oplus \tau\mathbb{Z}$ por

$$E_k(\Lambda_\tau) = \sum_{(a,b)\in\mathbb{Z}^2-\{0,0\}} \frac{1}{(a\tau+b)^k} = \sum_{\lambda\in\Lambda_\tau-\{0,0\}} \frac{1}{\lambda^k}$$

e portanto, em geral,

$$E_k(\Lambda) = \sum_{\lambda\in\Lambda-\{0,0\}} \frac{1}{\lambda^k}.$$

Proposição 13.15. *Temos a seguinte expansão de $\wp_\Lambda(z)$ em volta de $z = 0$:*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n\geq 1}^{\infty} (2n+1)E_{2n+2}(\Lambda)z^{2n}.$$

Demonstração. Se $|z|$ é menor que qualquer elemento não trivial de Λ, temos

$$\begin{aligned}\wp_\Lambda(z) &= \frac{1}{z^2} + \sum_{\lambda\in\Lambda-\{0,0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda-\{0,0\}} \left(\frac{1}{\lambda^2}\sum_{n\geq 1}(n+1)(z/\lambda)^n\right) \\ &= \frac{1}{z^2} + \sum_{n\geq 1}(n+1)z^n \sum_{\lambda\in\Lambda-\{0,0\}} \frac{1}{\lambda^{n+2}} = \frac{1}{z^2} + \sum_{n\geq 1}(n+1)z^n E_{n+2}(\Lambda).\end{aligned}$$

□

Corolário 13.16. *Temos $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$ se $g_2 = 60E_4$ e $g_3 = 140E_6$.*

Demonstração. Simplesmente compare coeficientes na com a expansão acima, de modo que a diferença seja holomórfica e tenha um zero na origem, de onde concluímos que tem que ser identicamente 0. □

13.5. **Relação com curvas elípticas.** Dado um lattice $\Lambda \subseteq \mathbb{C}$, vimos acima que temos uma curva elíptica

$$E_\Lambda\colon y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

Proposição 13.17. *Temos uma bijeção $\mathbb{C}/\Lambda \xrightarrow{\sim} E_\Lambda(\mathbb{C})$ dada por $z \mapsto (\wp(z), \wp'(z))$ (aqui, pensamos que o 0 vai para o ponto do infinito $(0:1:0)$ de $E_\Lambda(\mathbb{C})$).*

Demonstração. Que o mapa é injetor segue das considerações anteriores: $\wp(z) = a$ tem somente duas soluções z_0 e $-z_0$, e como $\wp'(z)$ é ímpar, só temos que tomar cuidado no caso que $\wp'(z_0) = 0$, mas isso implica que $z_0 \equiv -z_0 \mod \Lambda$.

Agora dado um ponto $(x, y) \in E_\Lambda(\mathbb{C})$, considere $\wp(z) - x$. Isso é uma função Λ-periódica e par, e portanto tem que possuir dois zeros $\pm z_0$. Portanto, tem que ser verdade que $\wp'(z_0)^2 = \wp'(-z_0)^2 = y^2$. Daí ou $\wp'(z_0) = y$ ou $\wp'(-z_0) = y$. □

Portanto os pontos da curva elíptica estão em bijeção com $\mathbb{C}/\Lambda$. O seguinte resultado é um pouco mais difícil.

Teorema 13.18. *Seja E uma curva elíptica sobre $\mathbb{C}$. Então existe um lattice $\Lambda \subseteq \mathbb{C}$ tal que $E \simeq E_\Lambda$. Além disso, morfismos (algébricos) $E_\Lambda \to E_{\Lambda'}$ estão em bijeção com mapas lineares $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. Em particular, temos $E_\Lambda \simeq E_{\Lambda'} \iff \Lambda = \lambda\Lambda'$ para algum $\lambda \in \mathbb{C}^\times$.*

Ideias da demonstração. Para uma curva elíptica sobre $\mathbb{C}$, primeiro prova que podemos transformar numa equação da forma $y^2 = x^3 + ax + b$. Então definimos a invariante j dada por $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$. Então prova-se que $E \simeq E'$ sobre $\mathbb{C}$ se e somente se $j(E) \simeq j(E')$.

Agora note que $j(E_\Lambda) = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}$, e então se denotarmos $j(\Lambda) = j(E_\Lambda)$, isso é uma função modular de peso $3 \cdot 4 - 12 = 0$. Ela é modular em $\mathbb{H}$, mas tem um pólo simples em ∞. Agora se $c \in \mathbb{C}$, $j(z) - c$ ainda é uma função modular de peso 1, e portanto

$$\frac{\mathrm{ord}_i(j(z)-c)}{2} + \frac{\mathrm{ord}_\omega(j(z)-c)}{3} + \sum_{\tau \in D - \{i,\omega\}} \mathrm{ord}_\tau(j(z)-c) = \frac{0}{12} - \mathrm{ord}_\infty(j(z)-c) = 1,$$

ou seja, existe $z \in \mathbb{H}$ tal que $j(z) = c$. Portanto se $\Lambda = \Lambda_z$, e $j(z) = j(E)$, temos $E \simeq E_\Lambda$. □

Isso quer dizer que o domínio fundamental D para $\mathrm{SL}_2(\mathbb{Z})$ também está em bijeção com curvas elípticas sobre $\mathbb{C}$! Portanto formas modulares também podem ser pensados como certas funções $(\{\text{curvas elípticas}/\mathbb{C}\}/\sim) \to \mathbb{C}$. O discriminante de uma curva elíptica é dado por

$$\mathrm{disc}(E_\Lambda) = 16(g_2^3 - 27)g_3^2 = 2^{16}\pi^{12}\Delta.$$

Isso prova (o que já sabíamos!) que $\Delta(z) \neq 0$ para todo $z \in \mathbb{H}$.

Então se E é um curva elíptica, existe um lattice Λ com $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$. Note que o lado direito tem uma estrutura de grupo por adição. Isso corresponde a estrutura de grupo em $E(\mathbb{C})$ também, por causa do seguinte lemma:

Lema 13.19. *Se $a, b \in \mathbb{C}$, então os três pontos*

$$(\wp(a), \wp'(a)), \quad (\wp(b), \wp'(b)), \quad (\wp(-a-b), \wp'(-a-b))$$

são colineares.

Demonstração. Escolha α, β, γ tal que $\alpha\wp(z) + \beta\wp'(z) + \gamma = 0$ tenha raízes a, b. Se $\beta = 0$, então temos somente duas raízes, e portanto $a = -b$. Daí $-a - b = 0$, e de fato os três pontos são colineares.

Se $\beta \neq 0$, então a expressão tem um pólo triplo em 0, e portanto tem exatamente três raízes. Basta provar que a terceira raiz é $-a - b$. Na verdade, podemos provar em geral que se f é Λ-periódica, então $\sum_{\tau \in \mathbb{C} \mod \Lambda} (\mathrm{ord}_\tau f) \cdot \tau \in \Lambda$. Isso segue de integrar $zf'(z)/(2\pi i f(z))$ na borda de um domínio fundamental. □

Exercícios

(1) Seja $d = \dim_{\mathbb{C}} S_k$. Mostre como construir uma base $f_0, \dots, f_d$ de M_k onde $a_n(f_i) \in \mathbb{Z}$ para todo i e $n \geq 0$ e $a_i(f_j) = \begin{cases} 1 & \text{se } i = j, \\ 0 & \text{se } i \neq j, \end{cases}$ para todo $0 \leq i, j \leq d$. Essa base se chama base de Miller[33].

(2) Prove que todos os autovalores de $T(n)$ são inteiros algébricos reais[34]. Conclua que se $f \in S_k$ é uma autoforma normalizada, então $a_n(f)$ é um inteiro algébrico real.

(3) Seja $f \in S_k$ uma autoforma normalizada. Vamos provar que $\mathbb{Q}[a_i(f),\ i \geq 1]$ é um corpo numérico.

   (a) Denote por $S_k(\mathbb{Z}) \subseteq S_k$ o subgrupo de formas modulares com todos os coeficientes de Fourier inteiros. Use a base de Miller para provar que $S_k(\mathbb{Z})$ tem uma $\mathbb{Z}$-base dada por $f_1, \dots, f_d$.

   (b) Considere os operadores de Hecke como operadores lineares em $\mathrm{GL}(S_k)$. Seja $\mathbb{T}$ o anel gerado por todos os $T(n)$. Isso é, $\mathbb{T} := \mathbb{Z}[T(n),\ n \geq 1] \subseteq \mathrm{GL}(S_k)$. Use a base de Miller para ver que a ação de $T(n)$ preserva $S_k(\mathbb{Z})$, e induz um mapa injetor de grupos $\mathbb{T} \hookrightarrow \mathrm{End}(S_k(\mathbb{Z}))$.

   (c) Como grupos, temos $S_k(\mathbb{Z}) \simeq \mathbb{Z}^d$, e portanto $\mathrm{End}(S_k(\mathbb{Z})) \simeq \mathbb{Z}^{d^2}$. Prove que isso implica que $\mathbb{T} \simeq \mathbb{Z}^m$ para algum m[35].

   (d) Para $T \in \mathbb{T}$, temos $Tf = \lambda_T f$ para algum $\lambda_T \in \mathbb{C}$. Conclua que se $T_1, \dots, T_m$ é uma $\mathbb{Z}$-base de $\mathbb{T}$, então $\mathbb{Q}[a_n(f),\ n \geq 1] = \mathbb{Q}[\lambda_{T_1}, \dots, \lambda_{T_m}]$, e portanto que isso é um corpo numérico K_f.

(4) Sejam $x, y \in \mathbb{C}$ com $\wp(x) \neq \wp(y)$. Então temos $A, B \in \mathbb{C}$ tal que $\wp'(z) = A\wp(z) + B$ tem soluções exatamente em $x, y, -(x+y)$. Eleve isso ao quadrado e use a fórmula de $(\wp')^2$ para transformar isso numa cúbica em $\wp(z)$, e use a relação de Vieta para provar que

$$\wp(x) + \wp(y) + \wp(x+y) = \frac{1}{4}\left(\frac{\wp'(x) - \wp'(y)}{\wp(x) - \wp(y)}\right)^2.$$

Tome o limite $y \to x$ para provar que

$$\wp(2x) = \frac{1}{16}\left(\frac{12\wp(x)^2 - g_2}{\wp'(x)}\right)^2 - 2\wp(x).$$

[33] Use E_4 e Δ.

[34] Use a base dada pelo exercício anterior. Se f é um autovetor de autovalor λ, use que $\langle T(n)f, f\rangle = \langle f, T(n)f\rangle$.

[35] Seja $M \subseteq \mathbb{Z}^a$, prove por indução em a que $M \simeq \mathbb{Z}^b$ para algum b: considere $\mathbb{Z}^a \to \mathbb{Z}^{a-1}$ que esquece a primeira coordenada. Considere $M \subseteq \mathbb{Z}^a \to \mathbb{Z}^{a-1}$ e analize a imagem e o kernel.

14. 12 de Junho

Dado um subgrupo $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ de índice finito, descrevemos formas modulares $M_k(\Gamma)$ de peso k com relação à Γ. Na prática, vamos considerar somente certos Γ.

Definição 14.1. Para $N \geq 1$, denote por $\Gamma(N)$ o kernel do mapa de redução módulo p dado por $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Dizemos que $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ é um *subgrupo de congruência* se $\Gamma(N) \subseteq \Gamma$ para algum N.

Os principais exemplos são

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Note que

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z}),$$

e que temos mapas sobrejetores

$$\Gamma_1(N) \twoheadrightarrow \mathbb{Z}/N\mathbb{Z}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto b \mod N,$$

$$\Gamma_0(N) \twoheadrightarrow (\mathbb{Z}/N\mathbb{Z})^\times, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod N.$$

com kernels $\Gamma(N)$ e $\Gamma_1(N)$.

14.1. **Expansão de Fourier.** Anteriormente, para formas modulares f para $\mathrm{SL}_2(\mathbb{Z})$, nós usamos que f é invariante sobre $z \mapsto z+1$ e holomórfica para concluir que $f(z) = \sum_{n \geq 0} a_n(f) q^n$ onde $q = e^{2\pi i z}$.

No entanto, se $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ é um subgrupo e $f \in M_k(\Gamma)$, não é sempre que f é invariante a $z \mapsto z+1$. No entanto, se Γ é um subgrupo de congruência $\Gamma(N) \subseteq \Gamma$, então temos que f é invariante por $z \mapsto z+N$. Em geral, se f é invariante por $z \mapsto z+w$ e se denotarmos $q_w := e^{2\pi i z/w}$, temos a expansão de Fourier em ∞

$$f(z) = \sum_{n \geq 0} a_n q_w^n.$$

Onde a soma é para $n \geq 0$ pela holomorficidade.

Agora se temos outro cuspe $c \in \mathbb{Q} \cup \{\infty\}$, podemos encontrar $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tal que $c = \gamma(\infty)$. Daí, considere $g(z) = (cz+d)^{-k} f(\gamma(z))$. Isso é uma forma modular para $\gamma\Gamma\gamma^{-1}$. Se Γ é de congruência, $\Gamma(N) \subseteq \Gamma$, então também $\Gamma(N) \subseteq \gamma\Gamma\gamma^{-1}$, e portanto temos uma expansão de Fourier

$$g(z) = \sum_{n \geq 0} a_n(\gamma, f) q_N^n.$$

Note que isso pode depender de γ, pois podemos tomar $\gamma' = \pm \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \gamma$ para qualquer $j \in \mathbb{Z}$, e daí temos $a_n(\gamma', f) = (\pm 1)^k a_n(\gamma, f) \mu_N^{nj}$ onde $\mu_N = e^{2\pi i/N}$. Pensamos nisso como a expansão de Fourier em $\gamma(\infty)$.

Exemplo 14.2. Considere $E_{2,N}(z) := E_2(z) - NE_2(Nz)$. Pode-se provar que $E_{2,N} \in M_2(\Gamma_0(N))$.

Para $N = 2$, temos que $\Gamma_0(2)$ tem dois cuspes $0, \infty$. Temos a expansão

$$E_{2,2}(z) = -\frac{\pi^2}{3}\left(1 + 24 \sum_{n \geq 1} \left(\sum_{2 \nmid d | n} d \right) q^n \right)$$

em ∞. Para obtermos a expansão em 0, note que $0 = S\infty$, e portanto se $g(z) = z^{-2} E_{2,N}(Sz)$, temos

$$g(z) = \tilde{E}_2(z) - N^{-1}\tilde{E}_2(z/N) = E_2(z) - N^{-1}E_2(z/N) - \frac{2\pi i}{z} + N^{-1}\frac{2\pi i}{z/N} = -N^{-1}E_{2,2}(z/N).$$

Portanto a expansão de Fourier de $E_{2,2}$ em 0 é

$$g(z) = \frac{2\pi^2}{3}\left(1 + 24 \sum_{n \geq 1} \left(\sum_{2 \nmid d | n} d \right) q_2^n \right).$$

14.2. **Domínio fundamental e lattices/curvas elípticas.** Vimos que o domínio fundamental D de $\mathrm{SL}_2(\mathbb{Z})$ está em bijeção com $\mathcal{L}/\mathbb{C}^\times$ e também com curvas elípticas sobre $\mathbb{C}$ módulo isomorfismo.

Podemos usar isso para dar uma descrição semelhante aos domínios fundamentais $D_1(N) := D_{\Gamma_1(N)}$ e $D_0(N) := D_{\Gamma_0(N)}$.

Teorema 14.3. *Temos bijeções*

$$D_1(N) \longleftrightarrow \{(E, P) \colon E \text{ curva elíptica}/\mathbb{C},\ P \in E(\mathbb{C}) \text{ de ordem } N\}/\sim,$$

e

$$D_0(N) \longleftrightarrow \{(E, C)\colon E \text{ curva elíptica}/\mathbb{C},\ C \subseteq E(\mathbb{C}) \text{ subgrupo cíclico de ordem } N\}/\sim .$$

Demonstração. Para a primeira bijeção, se $E = E_{\Lambda_\tau}$, então $P = (c\tau + d)/N + \Lambda_\tau$ para $c, d \in \mathbb{Z}$, e temos que ter $\gcd(c, d, N) = 1$ pois P tem ordem N. Então podemos escolher $a, b \in \mathbb{Z}$ tal que $ad - bc \equiv 1 \mod N$ e podemos trocar a, b, c, d módulo N (sem trocar P) de modo que $ad - bc = 1$. Agora se $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, temos

$$(c\tau + d)\Lambda_{\gamma(\tau)} = \Lambda_\tau, \quad (c\tau + d)\left(\frac{1}{N} + \Lambda_{\gamma(\tau)}\right) = P,$$

e portanto todo par (E, P), módulo isomorfismos, é da forma

$$(E_\tau,\ 1/N + \Lambda_\tau).$$

Dois tais elementos são isomorfos se e somente se existe $\lambda \in \mathbb{C}^\times$ tal que $\lambda\Lambda_\tau = \Lambda_{\tau'}$ e $\lambda(1/N + \Lambda_\tau) = (1/N + \Lambda_{\tau'})$. A primeira condição é o mesmo que existir $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tal que

$$\begin{pmatrix} \lambda\tau' \\ \lambda \end{pmatrix} = \gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$$

portanto $\lambda = c\tau' + d$ e $\tau = \gamma(\tau')$, e a segunda condição vira que

$$\frac{c\tau' + d}{N} - \frac{1}{N} \in \Lambda_{\tau'},$$

ou seja, que $c \equiv 0 \mod N$ e $d \equiv 1 \mod N$, ou seja, que $\gamma \in \Gamma_1(N)$.

Pode-se fazer um argumento parecido para $\Gamma_0(N)$. □

Ou seja, da mesma forma que fizemos para M_k, podemos pensar em $f \in M_k(\Gamma_1(N))$ como uma função $F\colon \mathcal{L}_1(N) \to \mathbb{C}$ onde $\mathcal{L}_1(N) = \{(E, P)\}/\sim$ e F satisfaz $F(E_{c\Lambda}, cP) = c^{-k}F(E, P)$. Pode-se dar uma descrição análoga para $M_k(\Gamma_0(N))$ e também para $M_k(\Gamma(N))$, mas essa última é mais técnica.

14.3. **Operadores diamante.** Vamos denotar $M_k(N) := M_k(\Gamma_0(N))$.

Agora vamos pensar na diferença entre $M_k(\Gamma_0(N))$ e $M_k(\Gamma_1(N))$. Lembre-se que $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$ onde $\gamma \mapsto d$.

Definição 14.4. Seja $d' \in (\mathbb{Z}/N\mathbb{Z})^\times$. Para $f \in M_k(\Gamma_1(N))$, o *operador diamante* é dado por

$$(\langle d' \rangle f)(z) = (cz+d)^{-k} f(\gamma(z))$$

onde $\gamma \in \Gamma_0(N)$ é tal que $d' = d \mod N$.

Note que isso é bem definido pois $\Gamma_1(N)$ é normal em $\Gamma_0(N)$, então $\langle d' \rangle f \in M_k(\gamma\Gamma_1(N)\gamma^{-1}) = M_k(\Gamma_1(N))$.

Em termos de curvas elípticas, temos

$$(\langle d \rangle F)(E,P) = F(E, dP).$$

Agora note que $M_k(\Gamma_0(N))$ é o subespaço de $M_k(\Gamma_1(N))$ tal que $\langle d \rangle$ atuam de maneira trivial. Além disso, podemos diagonalizar o espaço $M_k(\Gamma_1(N))$:

Teorema 14.5. *Dado um caracter de Dirichlet* $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, *seja* $M_k(N,\chi) = \{f \in M_k(N)\colon \langle d \rangle f = \chi(d) f\}$. *Então*

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} M_k(N,\chi).$$

Demonstração. Dado $f \in M_k(N)$, a decomposição acima é dada por $f = \sum_\chi f_\chi$ onde

$$f_\chi = \frac{1}{\phi(N)} \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \overline{\chi(d)} (\langle d \rangle f). \qquad \square$$

14.4. **Operadores de Hecke.** Podemos definir operadores de Hecke para $M_k(N)$ de maneira parecida que fizemos para M_k.

Lembre-se que se $f \in M_k$ e $F\colon \mathcal{L} \to \mathbb{C}$ é a função correspondente, então tinhamos definido

$$(T(m)F)(\Lambda) = m^{k-1} \sum_{[\Lambda:\Lambda']=m} F(\Lambda') = \frac{1}{m} \sum_{[\Lambda':\Lambda]=m} F(\Lambda').$$

Em termos de curvas elípticas, um superlattice Λ' corresponde a um mapa sobrejetor $E_\Lambda \to E_{\Lambda'}$, e $[\Lambda', \Lambda] = m$ corresponde ao kernel ter tamanho m (o kernel é Λ'/Λ como um grupo).

Definição 14.6. Seja $F\colon \mathcal{L}_1(N) \to \mathbb{C}$ e $m \geq 1$. O *operador de Hecke* é dado por

$$(T_m F)(E,P) = \sum_{(E',P')} F(E',P')$$

onde a soma é sobre mapas sobrejetores $E \to E'$ com kernel de tamanho m, onde $P \mapsto P'$ e tal que $P' \in E'(\mathbb{C})$ tem ordem N.

Nota 14.7. Se $(m, N) = 1$, então P' automaticamente tem ordem N.

Assim como fizemos no caso $N = 1$, pode-se provar que:

Teorema 14.8. *Temos que T_m são multiplicativos, e que*

$$T_{p^{n+2}} = \begin{cases} (T_p)^{n+2} & \text{se } p \mid N, \\ T_{p^{n+1}} T_p - p T_{p^n} \langle p \rangle R_{p^{-1}} & \text{se } p \nmid N. \end{cases}$$

Em particular, T_m comutam entre si. Além disso, T_m comutam com os operadores diamante. Ainda, se $f \in M_k(N, \chi)$, temos $T_m f \in M_k(N, \chi)$, e

$$(T_m f)(z) = m \sum_{n \geq 1} \left(q^n \sum_{d \mid (n,m)} \chi(d) d^{k-1} a_{nm/d^2} \right).$$

Demonstração. Se $p \mid N$, dado um mapa $E \to E'$ de kernel com ordem p^n e $P \mapsto P'$ tem ambos ordem N, então o kernel tem que ser $\mathbb{Z}/p^n\mathbb{Z}$, pois caso contrário iria conter todos os pontos de ordem p, e conteria $(N/p)P$, mas $(N/p)P' \neq O$. Portanto existe um único jeito de fatorar $E \to E'$ em uma sequência de n mapas de ordem p. Portanto $T_{p^n} = T_p^n$.

Se $(m, N) = 1$, e é dado um mapa $E \to E'$ com kernel de tamanho n e $P \in E(\mathbb{C})$ de ordem N, note que $P' \in E'(\mathbb{C})$ tem ordem N.

Seja $E \to E'$ com kernel de ordem p^{n+2} com $p \nmid N$. Agora como no caso $N = 1$, temos dois casos: se $E \to E'$ contém $E[p]$ no kernel ou não. Se não contém, fatora de maneira única em um mapa de ordem p e um de ordem p^{n+1}. Se contém, existem $p + 1$ tais fatorações, e portanto precisamos retirar p delas. A fórmula segue dessas considerações pois

$$f(E_{\frac{1}{p}\Lambda}, P') = (\langle p \rangle R_{p^{-1}} f)(E_\Lambda, P). \qquad \square$$

Portanto, se $T(m) := T_m/m$, queremos novamente provar que $M_k(N, \chi)$ tem uma base de autoformas para $T(m)$.

Mas note que se $f \in M_k(N, \chi)$ fosse um autovetor para todos os $T(n)$ e normalizada com $a_1 = 1$, sua função L teria a forma

$$L(f, s) = \prod_p (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1}.$$

Note que se $p \mid N$, então o fator de Euler tem grau 1 (ou 0 se $a_p = 0$) em p^{-s} invés de grau 2.

14.5. **Autoformas.** Não é verdade que conseguimos achar uma base de autovetores para todos os $T(m)$.

Definição 14.9. $f \in M_k(N, \chi)$ é uma *autoforma* se é um autovetor para todo $T(m)$ com $(m, N) = 1$.

Da mesma maneira que definimos o produto escalar de Petersson para $\mathrm{SL}_2(\mathbb{Z})$, podemos definir o produto escalar de Petersson para $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ por

$$\langle f, g\rangle = \int_{D_\Gamma} f(z)\overline{g(z)}y^k \frac{\mathrm{d}x\ \mathrm{d}y}{y^2}, \quad f, g \in S_k(\Gamma).$$

Do mesmo jeito que provamos anteriormente que $T(m)$ eram simétricos em M_k, podemos ver que:

Lema 14.10. *Se $(m, N) = 1$ temos*

$$\langle T(m)f, g\rangle = \langle f, \langle m\rangle^{-1}T(m)g\rangle, \quad \langle\langle m\rangle f, g\rangle = \langle f, \langle m\rangle^{-1}g\rangle.$$

Demonstração. Podemos pensar no produto escalar como

$$\langle f, g\rangle = \int_{\mathcal{L}_1(N)/\mathbb{C}^\times} F(E, P)\overline{G(E, P)}\det(E)^k\ \mathrm{d}(E, P).$$

Agora se $(m, N) = 1$ temos que $(E, P) \mapsto (E, mP)$ é um automorfismo de $\mathcal{L}_1(N)/\mathbb{C}^\times$, portanto se $m_0 \equiv m^{-1} \mod N$, temos

$$\begin{aligned}\langle\langle m\rangle f, g\rangle &= \int_{\mathcal{L}_1(N)/\mathbb{C}^\times} F(E, mP)\overline{G(E, P)}\det(E)^k\ \mathrm{d}(E, P)\\ &= \int_{\mathcal{L}_1(N)/\mathbb{C}^\times} F(E, P)\overline{G(E, m_0P)}\det(E)^k\ \mathrm{d}(E, P) = \langle f, \langle m\rangle^{-1}g\rangle.\end{aligned}$$

Para $T(m)$, usamos o mesmo truque que fizemos no caso $N = 1$. Note que se $E_\Lambda \to E_{\Lambda'}$ tem kernel de ordem m, então podemos considerar $E_{\Lambda'} \to E_{\frac{1}{m}\Lambda}$. Daí

$$G(E_{\frac{1}{m}\Lambda}, P) = m^k G(E_\Lambda, m_0P) = m^k(\langle m\rangle^{-1}G)(E_\Lambda, P),$$

E portanto a prova do caso $N = 1$ prova o que queremos. □

Note que $T(p)$ e $\langle p\rangle$ não são simétricos, mas ainda assim eles são *normais*: um operador T é normal se T e T^* comutam, onde T^* é tal que $\langle Tf, g\rangle = \langle f, T^*g\rangle$.

Proposição 14.11. *Seja T um operador normal num espaço vetorial V de dimensão finita sobre $\mathbb{C}$. Então T é diagonalizável.*

Demonstração. Note que

$$\langle v, Tw\rangle = \overline{\langle Tw, v\rangle} = \overline{\langle w, T^*v\rangle} = \langle T^*v, w\rangle.$$

E então

$$\langle Tv - \lambda v, Tv - \lambda v\rangle = \langle Tv, Tv\rangle - \lambda\langle v, Tv\rangle - \overline{\lambda}\langle Tv, v\rangle + |\lambda|^2\langle v, v\rangle$$

e podemos trocar T por T^* e λ por $\overline{\lambda}$, pois no primeiro termo temos $\langle Tv, Tv\rangle = \langle v, T^*Tv\rangle = \langle v, TT^*v\rangle = \langle T^*v, T^*v\rangle$ pela normalidade. Portanto

$$\langle Tv - \lambda v, Tv - \lambda v\rangle = \langle T^*v - \overline{\lambda}v, T^*v - \overline{\lambda}v\rangle,$$

e em particular $Tv = \lambda v \iff T^*v = \overline{\lambda}v$.

Agora a mesma prova de operadores simétricos funciona: seja v um autovetor de T, e $W = (\mathbb{C}\cdot v)^\perp$. Daí temos

$$\langle Tw, v\rangle = \langle w, T^*v\rangle = \lambda\langle w, v\rangle,$$

e portanto $w \in W \implies Tw \in W$, e analogamente para T^*, e portanto T é um operador normal para W e o resultado segue por indução. □

Portanto, concluímos da mesma maneira que anteriormente;

Proposição 14.12. *$S_k(N)$ tem uma base de autoformas para*

$$\{T(m), \langle m\rangle \colon (m, N) = 1\}.$$

Poderíamos concluir que $M_k(N)$ tem tal base se construirmos as séries de Eisenstein.

Gostaríamos de extender esse resultado para autovetores de $T(p)$ para $p \mid N$ também. Acontece que isso não é possível, e próxima aula discutiremos com mais detalhes o que acontece.

Exercícios

(1) Prove que $E_{2,N}(z) := E_2(z) - NE_2(Nz) \in M_k(N)$.

15. 19 de Junho

Aula passada discutimos $S_k(\Gamma_1(N))$ e como existe uma base de formas que são autovetores para $\langle m\rangle$ e $T(m)$ para $(m,N)=1$. Gostaríamos de extender isso para todos os $T(m)$, mas isso não é possível.

O que acontece é que dentro de $S_k(\Gamma_1(N))$ temos formas que pertencem a $S_k(\Gamma_1(M))$ para $M \mid N$, e essas formas não serão autovetores para todos os $T(m)$.

15.1. **Formas antigas.** Se $M \mid N$, como $\Gamma_1(N) \subseteq \Gamma_1(M)$, naturalmente temos que $S_k(\Gamma_1(M)) \subseteq S_k(\Gamma_1(N))$.

Também existe outro jeito de levar $S_k(\Gamma_1(M))$ em $S_k(\Gamma_1(N))$:

Proposição 15.1. *Seja $f \in S_k(\Gamma_1(M))$ e $N = Md_0$. Então $z \mapsto f(d_0 z)$ é uma forma modular para $\Gamma_1(N)$. Vamos denotá-la por $\alpha_{d_0} f$. Sua expansão de Fourier é $\sum_{n\geq 1} a_n(f) q^{d_0 n}$.*

Demonstração. Seja $g(z) = f(d_0 z)$. Seja $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$, ou seja, $a, d \equiv 1 \mod N$ e $c \equiv 0 \mod N$. Daí temos

$$g(\gamma(z)) = f\left(d_0 \frac{az+b}{cz+d}\right) = f\left(\frac{a(d_0 z)+bd_0}{\frac{c}{d_0}(d_0 z)+d}\right) = f(\gamma'(d_0 z))$$

onde $\gamma' = \begin{pmatrix} a & bd_0 \\ c/d_0 & d \end{pmatrix} \in \Gamma_1(M)$, e portanto $g(\gamma(z)) = f(\gamma'(d_0 z)) = ((c/d_0)(d_0 z)+d)^k f(d_0 z) = (cz+d)^k g(z)$. □

Definição 15.2. Para $N = Md$, definimos $i_d \colon (S_k(\Gamma_1(M))^2 \to S_k(\Gamma_1(N))$ por

$$i_d(f,g)(z) = f(z) + g(dz).$$

Denotamos

$$S_k^{\text{ant}}(\Gamma_1(N)) := \sum_{p\mid N} \operatorname{im}(i_p).$$

Em termos de lattices, o primeiro mapa de i_d é dado por $(\Lambda, P) \mapsto (\Lambda, d\cdot P)$ e o segundo por $(\Lambda, P) \mapsto (\Lambda + M\mathbb{Z}\cdot P, P)$ a menos de uma constante.

Proposição 15.3. *$\langle m\rangle$ e $T(m)$ preservam $S_k^{\text{ant}}(\Gamma_1(N))$.*

Demonstração. Vamos primeiro considerar $S_k^{\text{ant}}(\Gamma_1(N))$.

Pela descrição acima, é fácil ver que

$$i_q(\langle m\rangle f, \langle m\rangle g) = \langle m\rangle i_q(f,g)$$

se $(m,N)=1$.

Note que temos

$$a_n(i_q(f,g)) = a_n(f) + \begin{cases} a_{n/q}(g) & \text{se } q \mid n, \\ 0 & \text{se } q \nmid n, \end{cases} \qquad a_n(T(p)f) = a_{pn}(f) + \begin{cases} p^{k-1}a_{n/p}(\langle p\rangle f) & \text{se } p \mid n, \\ 0 & \text{se } p \nmid n. \end{cases}$$

Portanto

$$a_n(T(p)i_q(f,g)) = a_{pn}(i_q(f,g)) + \begin{cases} p^{k-1}a_{n/p}(\langle p\rangle i_q(f,g)) & \text{se } p \mid n, \\ 0 & \text{se } p \nmid n, \end{cases}$$

$$= a_{pn}(f) + \begin{cases} a_{pn/q}(g) & \text{se } q \mid np, \\ 0 & \text{se } q \nmid np, \end{cases} + \begin{cases} p^{k-1}a_{n/p}(\langle p\rangle f) & \text{se } p \mid n, \\ 0 & \text{se } p \nmid n, \end{cases} + \begin{cases} p^{k-1}a_{n/pq}(\langle p\rangle g) & \text{se } pq \mid n, \\ 0 & \text{se } pq \nmid n. \end{cases}$$

Agora, se $p \neq q$, é simples ver que isso é o mesmo que $a_n(i_q(T(p)f, T(p)g))$, e portanto $T(p)i_q(f,g) \in S_k^{\text{ant}}(\Gamma_1(N))$.

Se $p=q$, temos $\langle p\rangle = 0$ em $S_k(\Gamma_1(N))$, e portanto

$$a_n(T(p)i_p(f,g)) = a_{pn}(f) + a_n(g) = a_n(T(p)f) - a_n(\alpha_p(p^{k-1}\langle p\rangle f)) + a_n(g) = i_p(T(p)f+g, p^{k-1}\langle p\rangle f).$$

Portanto $T(p)i_p(f,g) \in S_k^{\text{ant}}(\Gamma_1(N))$. □

15.2. **Formas novas.**

Definição 15.4. Denotamos por $S_k^{\text{novo}}(\Gamma_1(N))$ o complemento de $S_K^{\text{ant}}(\Gamma_1(N))$ pelo produto interno de Petersson.

Queremos também provar que $S_k^{\text{novo}}(\Gamma_1(N))$ é mantido pelos operadores de Hecke. Para isso, note que:

Lema 15.5. *Seja V um espaço vetorial de dimensão finita com um produto escalar, e $T\colon V \to V$ uma transformação linear, e T^* tal que $\langle Tv, w\rangle = \langle v, T^*w\rangle$. Seja $W \subseteq V$ um subespaço que é mantido por T^*. Então W é mantido por T.*

Demonstração. Seja $v \in W \perp$ e $w \in W$. Então temos

$$\langle Tv, w\rangle = \langle v, T^*w\rangle.$$

Isso é 0 pois $T^*w \in W$ e $v \in W^\perp$. Portanto $Tv \in W^\perp$. □

Ou seja, precisamos provar que $S_k^{\text{ant}}(\Gamma_1(N))$ é mantido por $T(m)^*$ e $\langle m\rangle^*$. Vimos aula passada que $\langle m\rangle^* = \langle m\rangle^{-1}$ e $T(m)^* = \langle m\rangle^{-1}T(m)$ se $(m, N) = 1$. Portanto, basta analisarmos $T(p)$ para $p \mid N$.

Para isso, seja $w = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Podemos ver que

$$w^{-1}\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} w = \begin{pmatrix} d & -c \\ -Nb & a \end{pmatrix},$$

e portanto que $w^{-1}\Gamma_1(N)w = \Gamma_1(N)$. Note também que $w^2 = \begin{pmatrix} -N & 0 \\ 0 & -N \end{pmatrix}$. Portanto, se $f \in S_k(\Gamma_1(N))$, podemos considerar, de maneira parecida com os operadores diamante,

$$(W_N f)(z) = i^k N^{k/2}(Nz)^{-k} f(-1/(Nz)),$$

normalizado de tal forma que $W_N^2 = 1$.

Proposição 15.6. *Temos $T(m)^* = W_N T(m) W_N^{-1}$ em $S_k(\Gamma_1(N))$.*

Ideia da prova. Basicamente, $T(m)^*$ é uma soma sobre lattices contendo Λ. Mas W_N é uma inversão, e portanto se conjugarmos por W_N, isso vira uma soma sobre lattices contidos em $W_N\Lambda$. □

Portanto, para checar que $S_k^{\text{novo}}(\Gamma_1(N))$ é mantido por todo $T(m)$, basta ver que $S_k^{\text{ant}}(\Gamma_1(N))$ é mantido por W_N.

Proposição 15.7. *$S_k^{\text{ant}}(\Gamma_1(N))$ é mantido por W_N.*

Demonstração. Seja $p \mid N$ e $N = pM$. Então se $h = i_p(f, g)$, temos

$$\begin{aligned}(w_N h)(z) = h(-1/(Nz)) &= \left(i^k N^{-k/2} z^{-k}\right)\left(f(-1/(Nz)) + g(-p/(Nz))\right) \\ &= p^{-k/2}(W_M f)(pz) + (W_M g)(z) = p^{-k/2} i_p(g, f).\end{aligned}$$

□

Corolário 15.8. *$S_k^{\text{novo}}(\Gamma_1(N))$ é mantido por todo $\langle m\rangle$ e $T(m)$. Além disso, também é mantido por W_N.*

Demonstração. Para ver que é mantido por W_N, basta provar que W_N é simétrico, e isso será um exercício. □

15.3. **Decomposição de $S_k(\Gamma_1(N))$.** Agora seja $f \in S_k^{\text{novo}}(\Gamma_1(N))$ uma autoforma para todos os $\langle m\rangle, T(m)$ com $(m, N) = 1$.

Lema 15.9 (Lema Principal)**.** *Se $a_1(f) = 0$, então $f = 0$.*

Uma vez que sabemos isso, podemos considerar para qualquer m

$$T(m)f - a_m f,$$

e como $a_1(T(m)f - a_m f) = a_m - a_m = 0$, teríamos $T(m)f - a_m f = 0$, ou seja, que f é um autovetor para todos os $T(m)$. Portanto

Teorema 15.10. *$S_k^{\text{novo}}(\Gamma_1(N))$ possui uma base de formas que são autovetores para todos os $\langle m\rangle, T(m)$ normalizadas com $a_1 = 1$. Chamamos tais formas de* newforms.

15.4. **Funções L de newforms.** Seja $f \in S_k^{\text{novo}}(\Gamma_1(N))$ uma newform com caracter χ. Então do mesmo jeito que fizemos anteriormente para $f \in S_k$, temos

Teorema 15.11. *A função L de f é dada por*

$$L(f, s) = \prod_p (1 - a_p p^{-s} + \chi(p)p^{k-1-2s})^{-1}.$$

Se $\Lambda(f, s) := N^{s/2}\Gamma(s)L(f, s)$, então

$$\Lambda(f, s) = (-1)^{k/2}\Lambda(W_N f, k - s).$$

15.5. **Multiplicidade 1.** O seguinte teorema é bem difícil.

Teorema 15.12 (Multiplicidade Um)**.** *Sejam $f, g \in S_k^{\text{novo}}(\Gamma_1(N))$. Suponha que f, g tem os mesmo autovalores para $T(p)$ para todos menos finitor primos p. Então $f = \lambda g$.*

Como consequência, se $f \in S_k^{\text{novo}}(\Gamma_0(N))$, temos que f e $W_N f$ tem o mesmo autovalor em $T(m)$ para $(m, N) = 1$, e portanto temos $W_N f = \lambda f$, e assim $W_N f = wf$ para algum $w \in \{\pm 1\}$.