Raphael Reichmann Rolim

Fundamentos da Aritmética Formal

UFPB, João Pessoa, PB

2023

Raphael Reichmann Rolim

Fundamentos da Aritmética Formal

Trabalho de dissertação apresentado como exigência para o título de Mestre em Matemática pela Universidade Federal da Paraíba – UFPB, Campus João Pessoa. Área de concentração: Álgebra.

Universidade Federal da Paraíba – UFPB
Centro de Ciências Exatas e da Natureza
Programa de Pós–Graduação em Matemática

Orientador: Daniel Marinho Pellegrino
Coorientador: Anselmo Baganha Raposo Júnior

UFPB, João Pessoa, PB
2023

Catalogação na publicação
Seção de Catalogação e Classificação

R748f Rolim, Raphael Reichmann.
Fundamentos da aritmética formal / Raphael Reichmann Rolim. - João Pessoa, 2023.
135 f.

Orientação: Daniel Marinho Pellegrino.
Coorientação: Anselmo Baganha Raposo Júnior.
Dissertação (Mestrado) - UFPB/CCEN.

1. Álgebra linear. 2. Teoria dos números. 3. Axiomas de peano. 4. Formalismo de Hilbert. 5. Números primos. I. Pellegrino, Daniel Marinho. II. Raposo Júnior, Anselmo Baganha. III. Título.

UFPB/BC CDU 517.986.3(043)

Elaborado por GRACILENE BARBOSA FIGUEIREDO - CRB-15/794

Raphael Reichmann Rolim

Fundamentos da Aritmética Formal

Trabalho de dissertação apresentado como exigência para o título de Mestre em Matemática pela Universidade Federal da Paraíba – UFPB, Campus João Pessoa. Área de concentração: Álgebra.

Trabalho aprovado. UFPB, João Pessoa, PB, 18 de Agosto de 2023:

Prof. Dr. Daniel Marinho Pellegrino
(Orientador, UFPB)

Prof. Dr. Anselmo Baganha Raposo Junior
(Co-orientador, UFMA)

Prof. Dr. Jean Carlos de Aguiar Lélis
(Examinador, UFPA)

Prof. Dr. Wallace Mangueira de Sousa
(Examinador, UFPB)

Agradecimentos

Agradeço à minha família e aos meus amigos.

Agradeço à CAPES e à FAPESQ, que financiaram esta pesquisa e garantiram o mínimo de segurança material necessária para a dedicação integral ao desenvolvimento.

Agradeço ao professor orientador Daniel pela valorosa oportunidade que ele me conferiu, ao, ainda em meu mestrado, me permitir investigar estes temas originais. Agradeço também ao meu coorientador Anselmo, com quem pude trocar algumas conversas.

Agradeço ao professor Uberlandio, que me acompanhou e apoiou por anos, e com quem ainda realizei o estágio docência deste Mestrado.

Agradeço ao professor Wallace, que, ainda ano passado, me fez algumas perguntas que ajudaram o trabalho a amadurecer.

Agradeço também ao coordenador da PPGMAT Fágner, por sua solicitude e competência.

Acrescento um agradecimento a Jean Lélis, que junto com Daniel e Wallace comporam a minha banca, assim como a Diogo. Todos testemunharam o pássaro invadindo o quarto e repousando tranquilo na minha mão, durante a defesa.

Agradeço aos professores Bruno Torrez e Maria Lewtchuk Espindola, que, na época do meu ensino médio, fizeram respectivamente as perguntas "Por que a senóide é 'nota pura' (timbristicamente)?", e "O que é número?". Para esta última, após ter minhas tentativas de resposta rejeitadas, recebi o silêncio contemplativo, que costuma ser a resposta mais digna às grandes perguntas.

"Segundo o nosso modo de ver, o número, em seu conjunto, é o Ser."
(Platão em "Sofista", 238 b.)

"Tu conhecerás, tanto quanto é possível a um mortal, que a Natureza é em tudo semelhante a si mesma."
(Versos áureos de Pitágoras)

"We may, however, take this opportunity of expanding some remarks which we made in § 17.1. We could construct a formal theory of Dirichlet series in which 'analysis' played no part. This theory would include all identities of the 'Mobius' type, but the notions of the sum of an infinite series, or the value of an infinite product, would never occur. We shall not attempt to construct such a theory in detail, but it is interesting to consider how it would begin."
Hardy e Wright (2009, p. 329), 6ª edição.

Resumo

Neste trabalho propus a união da axiomática de Peano à axiomática dos espaços vetoriais, através do conceito de base ordenada, culminando na definição de espaço aritmético. Esta união permitiu uma sistematização universal dos procedimentos mais comuns do estudo da teoria dos números através de funções geradoras, desenvolvendo uma linguagem compreensiva e coesa. Defini a noção de aritmética, função sucessora e gerador, operações aritméticas iterativas e endomórficas, e de monóides de operações e seus homomorfismos, assim como a noção autossimilar de meta-aritmética. Desenvolvi o conceito de álgebra de operações aritméticas, transportando completamente a teoria das operações aritméticas para dentro da teoria das transformações lineares. Mostrei como as álgebras definidas podem ser compreendidas de diversas maneiras já bem estabelecidas da Álgebra, e a relação destas estruturas com álgebras convolutivas. Estudei seus homomorfismos quando são álgebras de Banach e, em particular, o problema da inversão aritmética nestas álgebra. Provei a decomposição do grupo de seus elementos invertíveis em fatores elementares, teorema consideravelmente mais útil que o Teorema Fundamental da Álgebra. Investiguei combinatorialmente algumas relações, em especial a construção das multiplicações primas pelas naturais, a Lei das Fatorações Naturais e algumas fórmulas primitivas. Criei a noção de álgebra simetrizada de operações e a teoria vaga dos correspondentes simetrizados. Descrevi como a álgebra das operações aditivas circulares faz nascer, da maneira mais natural, o conceito da Transformada de Fourier Discreta, noção fundamental da disciplina de processamento de sinais. Obtive representações de funções aritmeticamente notáveis, como a função de Mertens de maneira abstrata, sem recorrer à função Zeta, por meio da análise harmônica aplicada aos grupos de operações invertíveis. Por fim, mostrei um argumento heurístico para a obtenção de uma assíntota intimamente ligada à hipótese de Riemann, utilizando resíduos complexos da teoria clássica.

Palavras-chave: Teoria dos Números. Álgebra Linear. Axiomas de Peano. Formalismo de Hilbert. Convoluções. Números primos.

Abstract

In this work I proposed the union of Peano's axiomatics to the axiomatics of vector spaces, through the concept of ordered basis, culminating in the definition of arithmetic space. This union allowed a universal systematization of the most common procedures in the study of number theory through generating functions, developing a comprehensive cohesive language. I defined the notion of arithmetic, successor function and generator, iterative and endomorphic arithmetic operations, and monoids of operations and their homomorphisms, as the self-similar notion of meta-arithmetic. I developed the concept of algebra of arithmetic operations, completely translating the theory of arithmetic operations into the theory of linear transformations. I showed how the defined algebras can be understood in several well-established ways of Algebra, and the relationship of these structures with convolutional algebras. I studied their homomorphisms when they are Banach algebras and, in particular, the problem of arithmetic inversion in these algebras. I proved the decomposition of the group of its invertible elements into elementary factors, a theorem considerably more useful than the Fundamental Theorem of Algebra. I investigated some relations combinatorially, in particular the construction of prime multiplications by natural ones, the Law of Natural Factorizations and some primitive formulas. I created the notion of symmetrized algebra of operations and the vague theory of symmetrized correspondents. I described how the algebra of circular additive operations gives rise, in the most natural way, to the concept of the Discrete Fourier Transform, a fundamental notion of the discipline of signal processing. I obtain representations of arithmetically remarkable functions, such as the Mertens function, in an abstract way, without resorting to the Zeta function, through harmonic analysis applied to groups of invertible multiplicative operations. Finally, I show a heuristic argument for obtaining an asymptote closely linked to the Riemann hypothesis, using complex residues of the classical theory.

Keywords: Number Theory. Linear Algebra. Peano Axioms. Hilbert's Formalism. Convolutions. Prime Numbers.

Sumário

Contraste crítico entre os conceitos de número natural e Aritmética

Os números naturais são objetos de contemplação e fascínio pela humanidade desde os tempos imemoriais. Não nos é possível determinar quando começamos a concebê-los, a contá-los, a usá-los nas mais diversas atividades. Apontando as evidências para o fogo ter sido dominado pelos Homo entre 1 e 2 milhões de anos atrás, como não suspeitar que a ancestralidade da língua e do número seja abismalmente maior que a que nos permitimos usualmente conceber? Que limites encontrou a imaginação do homem ao inspirar-se na generosidade da natureza, ao contemplar os céus e a própria ignorância frente ao infinito? Tais histórias, que aqui nos trazem, guardarão eternamente seus segredos, e nos restará somente o prazer insípido das especulações obscuras.

Nosso saber, apegado aos resquícios poupados pelo tempo, há de se contentar com evidências esparsas, das quais a mais famosa é o osso de Ishango, encontrado em escavações de uma vila no Congo, preservada por uma erupção vulcânica que a atingiu há 20 mil anos. Nela, restam marcações que indicam alguma forma de contagem ou até uma operação mais complexa, o que é pouco claro. Outro achado interessante data de alguns dos primeiros assentamentos de Sapiens no solo que hoje é europeu, datado de 40 mil anos, talvez carregado de uma cultura ainda mais velha: achada em Hohle Fels, na Alemanha, a flauta mais antiga já encontrada apresenta um padrão de furos que demonstra um conhecimento rudimentar de harmonia e consonância, outra forma profundamente intuitiva pela qual o ser humano se aproximou do número.

São somente das grandes civilizações da antiguidade que recebemos provas indubitáveis da consideração do número claramente abstraído de suas manifestações. O Egito é citado por diversos escritos da antiguidade como uma grande fonte do estudo místico, lógico e numérico. No entanto, não nos restaram evidências egípcias de declarações explicitamente abstratas e estruturadas logicamente acerca do número, fato que faz as investigações da civilização egípcia serem caracterizadas como apenas de cunho prático por alguns autores. Isto é improvável, para um cultura tão ligada à linguagem, às ciências e à metafísica. A evidência sobrevivente mais marcante desta faixa histórica talvez venha do crescente fértil, onde hoje é o sul do Iraque. Com quase 4 mil anos de idade, a tábua de argila acadiana catalogada como Plimpton 322 mostra claramente uma lista do que conhecemos como triplas pitagóricas, isto é, pares de números quadrados cuja soma é outro quadrado. Algumas destas triplas nos chamam a atenção, como $12.709^2 + 13.500^2 = 18.541^2$, pois sugerem que algum *método* desconhecido estava envolvido, mais do que mera adivinhação. Neugebauer e Sachs, em 1945, sugeriram o uso de álgebra para gerar as triplas, fato contestado como anacrônico, restando-nos novamente o mistério.

Esclarecimentos explícitos e lógicos que arquitetam o complexo por meio de partes simples nos chegam essencialmente através de textos gregos. A literatura grega foi em grande medida perdida. A figura de Pitágoras sintetiza uma das grandes linhagens do pensamento grego, onde havia menos distinção entre mística, lógica, e matemática do que nos acostumamos contemporaneamente. Dos pitagóricos restou pouco, e mesmo as grandes obras de Aristóteles sobre o grupo não sobreviveram ao tempo. Apesar das triplas pitagóricas terem despertado a curiosidade humana muito antes de Pitágoras, a matemática pitagórica foi aparentemente a primeira a demonstrar claramente que simples triângulos já carregavam relações impossíveis para as proporções fracionárias (os incomensuráveis). Uma das soluções mais práticas a respeito destes irracionais foi dada após alguns séculos por Eudoxo, que definiu a igualdade entre números irracionais i, j como a equivalência $i = j \Leftrightarrow (i < a \Leftrightarrow j < a, \forall a)$, sendo os números a fracionários. É uma definição de identidade de irracionais totalmente expressa a partir de suas relações com números fracionários, feita através de uma relação de equivalência que evita afirmações existenciais de irracionais particulares.

O trabalho máximo grego, e um dos sobreviventes mais simbólicos da antiguidade, é o texto de Euclides, Os Elementos. Nele, tanto quanto possível, o autor busca explicar relações matemáticas da maneira mais lógica e indubitável, até mesmo de coisas que julgávamos óbvias e simples, e ainda demonstrar o complexo, na geometria e na aritmética.

A quantidade, simetria, ordem, ou simplicidade, que para os pitagóricos dava fundamento ao estudo da harmonia do mundo em diversas esferas da vida, coerentemente, foi investigada no fim com o escrutínio da lógica e razão: mantendo que a noção de unidade corresponde à condição própria existencial do ente, da mônada[1]; da categoria abstrativa fundamental, *o número*, a quantidade, soma ou multitude, onde entes distintos são reunidos sob uma mesma abstração conforme suas semelhanças (a exemplo das primeiras duas definições do $7^{\underline{o}}$ tomo d'Os Elementos). O trabalho de Euclides reuniu boa parte da ciência matemática construída em seu tempo e lugar. Não só uma janela para o passado, suas categorias foram aceitas por gerações de filósofos desde esta época até as modernas e contemporâneas - mesmo por estes amantes da discussão e de difícil consenso.

Dentre muitas das questões que o livro considera, está a dos números primos, das proporções naturais irredutíveis. O livro demonstra que são infindáveis e, com ressalvas[2], que todo número natural tem fatoração única como produto de primos em ordem. A existência e distribuição dos números primos entre os naturais encantou e frustrou gerações de matemáticos desde então, que tentam encontrar algum padrão claro para construí-los. O paradigma pitagórico legou às gerações o encantamento com a ordem e a proporção como medida do mundo, e elevou os primos às proporções irredutíveis da própria Natureza.

[1] Em consonância, alguns pitagóricos anteriores ainda a Platão chegavam mesmo a dizer que 1 não era número, que número se reservava ao que era múltiplo.

[2] As afirmações de Euclides não correspondem exatamente ao Teorema Fundamental da Aritmética, tradicionalmente atribuído ao *Disquisitiones* de Gauss.

O maior legado histórico d'Os Elementos talvez seja oferecer um exemplo claro do poder sintetizador, organizador e demonstrativo do método axiomático que, de tão associado ao livro, foi por séculos chamado de *método geométrico*.

Ao longo dos últimos séculos, em particular a partir do XIX em solo europeu, diversas aplicações da lógica dentro e fora da matemática tradicional levaram a um criação tão numerosa de linguagens e sistemas complexos que o rigor lingüístico explícito e mecânico passou a ser naturalmente necessário, a fim de enfrentar os erros mais sutis.

Dentre a complexidade destes movimentos, surgiram as primeiras axiomatizações modernas da aritmética, geralmente creditadas a Grassmann, Peirce e principalmente Peano.

Os axiomas de Peano para os números naturais basicamente declaram[3] que (1) há um primeiro número natural 1; que (2) existe uma função injetiva $+1$ entre os naturais que leva cada número em seu sucessor, tal que 1 não é imagem desta função (1 não é sucessor de nenhum natural), e que (3) um subconjunto dos naturais que contenha 1 e contenha o sucessor de todo elemento que a ele pertença é o próprio conjunto $\mathbb{N}$ dos naturais. Destes axiomas, mostrou-se que uma grande quantidade de afirmações sobre os números naturais pode ser enunciada e provada. A axiomática incorporou-se na ciência moderna, e desde então é celebrada por seu carácter unificador.

Pode-se ver na literatura, como no vulgo[4] *Elinho*[5] (LIMA, 2016, p. 1), a afirmação de que estes axiomas caracterizam os números naturais. O leitor atento talvez perceba que os axiomas de Peano, tomados abstrata e formalmente da realidade que descreviam, são modelados em uma classe muito maior de estruturas e objetos que os números naturais: afinal número, função sucessora e unidade são por eles tomados primitiva, abstratamente. Por exemplo, até mesmo o conjunto das potências de 2 satisfaz os axiomas de Peano, desde que a função injetiva seja a restrição da função $\cdot 2$ ao conjunto destas potências.

A axiomática de Euclides, que buscava o rigor formal, sem no entanto separar-se tão clinicamente da substância de que tratava, como propõe o formalismo hilbertiano, talvez seja a imagem que nos elucide a razão da axiomática de Peano, dada em sua plena abstração, ser por vezes confusamente dada como a definição de número natural. Esta axiomática, que estabelece relações entre os objetos primitivos *número natural*, *função sucessora* e *unidade* nada carrega da semântica atribuída implicitamente às palavras em itálico, que aqui

[3] O próprio Peano inicialmente publicou seu trabalho utilizando o 1 como primeiro número, introduzindo depois o 0. Ambas as formulações são interessantes ao matemático. Aqui escolhemos o número 1 como ponto de partida por o considerarmos de carácter existencial e logicamente precedente a 0 (Quantos zeros naturais existem?). Isso está de em consonância com a tradição filosófica ocidental, em particular com as ponderações medievais de Scotus acerca da unidade e do ser, e as considerações de Santos acerca da precedência da afirmação sobre a negação, que interpreta como um tipo particular de afirmação.

[4] Análise Real, volume 1: funções de uma variável.

[5] Curiosamente, a pesquisa atual, levada por outras motivações, aqui me remonta ao meu primeiro período de graduação - em particular à primeira vez que tentei ler o *Elinho*, sob indicação do professor Daniel Pellegrino, quando nem imaginávamos estabelecer a presente orientação. Na primeira página, já encontrei dificuldades: como era possível que aquilo resumisse o que era número? Apesar disso, mais tarde o livro me foi um dos mais valiosos.

são tomadas como mero símbolo vazio. De certa forma, o fato da axiomática permitir-nos demonstrar tantas de suas afirmações sem nunca requerer uma especificação da natureza de seus entes primitivos a torna ainda mais admirável.

O conflito entre a pluralidade dos modelos que satisfazem os axiomas de Peano e o conceito de número natural como coisa determinada e única é reconhecido em Russell (1920, p. 9): à primeira chama de axiomas das *progressões*; ao segundo, o problema de definir os números naturais eles mesmos, que segundo ele foi solucionado somente com Frege. Frege (1884) definiu número cardinal como classe da relação de equivalência $\sim$ entre conjuntos, onde $\sim$ indica a existência de uma relação bijetiva entre eles. Neste sentido, o cardinal 2 é para Frege a classe de todas as duplas de um universo de discurso. Sua definição de número a princípio não inclui afirmações existenciais a respeito dos números; mesmo a consideração que obtivemos a respeito de 2 só faz sentido mediante a afirmação independente da existência das duplas[6]. Neste sentido, a definição de Frege tem uma qualidade lógica semelhante à definição de irracionais de Eudoxo, sem determinações existenciais per se.

Em vários aspectos, a consideração de classes de equivalência e quocientes se relaciona com o conceito filosófico tradicional de essência, que abstrai de uma coleção de seres o que lhes é idêntico, e os analoga[7] (Santos, 2000). Neste sentido, a resposta de Frege talvez seja uma resposta atual à mesma busca presente em Pitágoras.

Se para Frege "2" é abstraído da condição comum de tudo que é duplo, é de se crer que "1" deva ser abstraído da condição comum de tudo que é único, sendo que ser é ser único, e portando 1 é abstraído da condição mesma de ser[8]. Frege define conceitos como conjuntos, e números naturais como as classes de equivalência de uma relação lógica, a de existência de uma relação bijetiva entre os conceitos, chamada *equinumérica*, mas definida tão somente pelas equações e distinções da condição bijetiva. A definição não apela a nenhum número em particular e é sugerida como o que é essencial ao número. Não é capaz, no entanto, de implicar a existência de qualquer número (qualquer classe), sendo independente a afirmação de existência do conjunto vazio ou mesmo de quaisquer elementos com os quais formaríamos conjuntos.

De fato, parte fundamental do nosso vocabulário pôde ser aprendida graças a exemplos de seu uso, de onde tiramos o que lhes é comum facilmente, e incorporamos; quando se ensina primeiramente o que é 2, não se passa justamente pela apresentação de duplas de

[6] Em Russell (1920, p. 25), podemos constatar a mesma percepção: um universo finito implicaria na inexistência de n-uplas grandes, que, pela definição de Frege, identificaria todos os números correspondentes com o conjunto vazio. É digno notar que é justamente esta estrutura que é implicada na formação do que definiremos como aritmética finita nilpotente.

[7] Realmente, as classes de equivalência são freqüentemente interpretadas como identificando seus elementos sob uma qualidade comum, reduzindo-os a um único representante.

[8] No sentido de ser elemental. Frege (1884) considera a estranheza da unidade como predicado: "Sócrates é um". A estranheza talvez nasça da redundância: nada acrescenta à sentença "Sócrates é", sem predicado (sobre o elemento Sócrates).

coisas? E 3 pela de trios? E o aprendiz, que já intui a dualidade, a trialidade às quais apelávamos, as reconhece nos exemplos e aprende a se referir aos termos 2 e 3. [9]

E 1, pela apresentação das coisas - apelando à intuição de ser. É símbolo de ser, elementalmente - sem complementar; absoluto. Frege e Russell participam com o rigor lógico moderno da história das respostas a essa intuição, a da natureza das coisas[10].

A posição desta aritmética formal

Preocupados com dúvidas mais particulares, nos voltamos ao ponto de partida da presente pesquisa: a distinção entre *número natural* e *aritmética*, respectivamente entre as abstrações máximas existenciais e os modelos dos axiomas de Peano e considerações algébricas sobre suas operações. Aqui, nos interessamos justamente em estudar as operações aritméticas de soma, multiplicação e potência para as mais variadas progressões, finitas[11] ou infinitas. Neste sentido, foi interessante definir como *Aritmética* um conjunto que preservasse de um lado a estrutura algébrica implicada pelos axiomas de Peano (única a menos de isomorfismos), e de outro, a informação sobre os objetos particulares aos quais se aplicam. Conforme veremos, isso é tão simples quanto defini-las como um par (x_1, s), onde x_1 é o primeiro elemento da progressão, e s é a função sucessora da progressão.[12]

Com este formalismo, é possível descrever em uma única linguagem todas as instâncias onde relações aritméticas ocorrem, antes de determiná-las particularmente. Isso nos permite adicionar à vontade afirmações independentes a respeito dos elementos x_n das progressões, da forma que for mais conveniente para a investigação aritmética. Tal formalismo, bastante simples e geral, talvez permita grande sorte de aplicações; aqui nos limitaremos à adição de uma **condição vetorial** aos "números", constituindo o que chamaremos de *espaços aritméticos*[13]. Em tais espaços é possível considerar álgebras de operações aritméticas, adequadas para o estudo de funções geradoras. As álgebras de soma respeitam uma forma de fatoração compositiva das operações aritméticas aditivas em termos da base aditiva. Quando o anel dos coeficientes é corpo algebricamente fechado, a forma simplifica-se para o clássico teorema fundamental da álgebra para polinômios. Assim como no caso aditivo, os elementos de álgebras de multiplicação destes espaços sempre admitem uma fatoração compositiva em termos da base multiplicativa. Além disso, contém um

[9] Fruto do reconhecimento intuitivo do estado das coisas; neste caso, das primeiras finitudes naturais. A existência das finitudes e suas relações é um fato independente da formulação conceitual de número de Frege, que delas trata somente quando é expressamente admitida a existência de um conjunto com a específica cardinalidade. Intuímos inclusive sucessões infinitas de coisas! Mesmo Russell admite que há fundamentalmente uma admissão independente de infinidade de objetos, para enfim tratar de número natural como tal.

[10] Para Frege, os conjuntos unitários, em identificação com os elementos. Por coisa, entendemos o que existe como mero elemento - ente, por existir, ou ser (elementar).

[11] O chamado *finitismo de Skolem* não tem relação com as idéias aqui presentes.

[12] Isso é análogo a distingüir um grupo do conjunto no qual age.

[13] Em outras palavras, o estudo das progressões restrito às progressões de vetores.

elemento que respeita um produto de Euler generalizado, nos casos infinito e finito nilpotente. Este elemento é, para a álgebra das séries de Dirichlet com respeito à multiplicação convencional, a clássica função Zeta; por este motivo o chamaremos Z-elemento, ou Z-função. Z-elementos carregam uma informação especial em qualquer espaço aritmético, pois sua inversa[14] tem n-ésimos coeficientes $\mu(n)$, dados pela função de Möbius.

De fato, isso demonstra a posição matemática fundamental das operações convolutivas aditivas e multiplicativas, uma vez que emergem naturalmente na estrutura de coeficientes das álgebras de operações aritméticas de qualquer espaço aritmético. A interpretação fornece uma forma de organizar muitos objetos e procedimentos distintos da teoria dos números.

Funcionais lineares destas álgebras para o conjunto de coeficientes representam funções aritméticas clássicas. De fato, copiosos exemplos históricos de tentativas de se provar o teorema dos números primos ocorreram por meio de procedimentos particulares da inversão multiplicativa de uma Z-função, no caso de um espaço de funções de base ortonormal enumerável, onde o funcional era o de avaliação das funções em um ponto ou alguma forma de resíduo. É o caso de algumas tentativas fracassadas do final do século XIX, inclusive por Tchebycheff; nos Handbuchs de Landau, e mesmo no caso da célebre função Zeta.

Em alguns destes casos, o teorema dos números primos estaria determinadamente provado, a depender tão somente de uma comutação de limites: o da entrada do funcional avaliação, à medida que se aproxima de um ponto, e o limite que define a série vetorial (e dimensão aritmética). Assim o foi para a função Zeta desde Euler, que constatou com facilidade que

$$\lim_{x\to 1} \frac{\mu(n)}{n^x} = \frac{\mu(n)}{n}$$

e que

$$\lim_{x\to 1^+} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^x} = 0,$$

uma vez que em $x > 1$ convergem as séries da expressão

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^x} \cdot \sum_{n=1}^{\infty} \frac{1}{n^x} = 1,$$

mas não pôde provar que

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0.$$

[14] Que é o automorfismo multiplicativo cuja avaliação na soma dos vetores da progressão retorna o próprio gerador aritmético.

Também ocorre este problema na decomposição da senóide em ondas triangulares:

$$\sin(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} g(nx),$$

onde $g(0) = 0,\ g(x) = \pi/2 - x/2,\ x \in (0, 2\pi)$ é 2π periódica. A série não converge uniformemente ao redor de 0; se o fizesse, bastava-nos tomar o limite $x \to 0^+$ para obter o resultado, pois o limite passaria sob o sinal da série.

Estas limitações se mostraram um impedimento para gerações de matemáticos, que só viriam a prová-las utilizando a não anulação da função zeta na linha de parte real 1 do plano complexo. No presente texto, trouxemos brevemente a ferramente mais límpida desta teoria, o Teorema Tauberiano de Wiener, que aplica a teoria de Gelfand para obter resultados da álgebra convolutiva.

Como marca geral das contribuições deste trabalho, estão as considerações estruturais gerais que permitem identificar mais facilmente conexões aritméticas e investigá-las através da sistematização algébrica. Com isso, fomos capazes de expressar os temas fundamentais da teoria dos números através do parco formalismo abstrato.

Convido, pois, o leitor, em especial o apaixonado pelos temas da teoria dos números, a se debruçar sobre a axiomática que defini e desenvolvi, e se possível, avançá-la e reforçá-la, a fim de que se revele a universalidade e aplicabilidade da sistematização.

Introdução

Este texto nasceu após uma investigação pessoal de alguns temas da teoria dos números, especialmente o estudo de quantidades aritmeticamente notáveis esclarecido pelo uso de funções geradoras. Estas quantidades são notáveis enquanto respostas a dúvidas simples acerca das propriedades da soma e da multiplicação.

Dentre as buscas desta área, destaca-se a compreensão do comportamento assintótico de coeficientes de séries de funções, normalmente de potências ou de exponenciais de naturais, através de estudos analíticos pormenorizados, quando não altamente particulares e especializados, dos próprios valores que as séries assumem.

Nestes dois casos, a construção dos coeficientes desejados ocorre através da multiplicação destas séries - a operação, fechada nestes espaços de funções, tem um efeito convolutivo (discreto) na formação dos coeficientes da série resultante. A posição fundamental da ciência das convoluções se justifica tanto pela naturalidade dos processos que as geram como pela profundidade de suas conseqüências: em última instância, é desta ciência que surgiu a prova mais límpida e sistemática do Teorema dos Números Primos, através de teoria tauberiana de Wiener.[15]

Algumas das quantidades aritméticas mais estudadas provém de processos de inversão aditiva ou multiplicativa das séries de potências ou de Dirichlet. Estes métodos, dependentes de uma álgebra cuja multiplicação é a multiplicação complexa das imagens das séries, concedem às raízes destas o papel de regiões de não invertibilidade dos elementos na álgebra. De uma maneira ou de outra, os avanços mais proeminentes no estudo das quantidades aritméticas se deram por meio da análise destas regiões de não invertibilidade[16]. O exemplo clássico da teoria aditiva talvez seja o método do círculo de Hardy e seus colaboradores aplicado às partições como coeficiente do inverso da função de Euler; o da teoria multiplicativa, provavelmente o estudo dos primos com o inverso ou logaritmo da função Zeta, por diversos métodos.

Apesar disso, é notório que convoluções aditivas e multiplicativas são modeladas em diversos objetos da matemática, através de operações distintas da multiplicação convencional. Este fato levou pesquisadores a investigarem quantidades aritméticas através de diversas relações conhecidas, muitas das quais elusivamente promissoras e sugestivas, mas finalmente vãs e infrutíferas. Nesta situação se encontraram muitos matemáticos do século

[15] A referência que utilizei foi Folland (1995). Limpidamente, a transformada de Gelfand da álgebra de Banach das funções integráveis em um dado grupo G abeliano, onde a multiplicação da álgebra é a convolução integral das funções, é a própria transformada de Fourier; isto é, as transformadas de Fourier das funções $L^1(G)$ são exatamente os homomorfismos daquela álgebra. A condição de não anulação da transformada resulta diretamente em condições de convergência de convoluções. Além disso, a transformada é construída em correspondência com os caracteres multiplicativos do grupo.

[16] Ou mesmo na fronteira do grupo dos elementos invertíveis de uma álgebra de Banach.

XIX, crentes na veracidade de antigas conjecturas a respeito da distribuição dos números primos, e, a despeito de todas as evidências, incapazes de prová-las.

De fato, o processo de inversão multiplicativa pode ser efetuado num grande número de espaços através de operações independentemente definidas e conhecidas. Enquanto eu escrevia meu trabalho anterior (ROLIM, 2020), generalizei muitas versões da inversão multiplicativa sob uma única forma:

Se $\{f_n\}_{n\in\mathbb{N}^*}$ é uma família de funções de A em B subconjuntos de $\mathbb{C}$, e se está bem definida a família $\{g_n\}_{n\in\mathbb{N}^*}$ pela relação

$$g_k(z) = \sum_{n=1}^{\infty} f_{nk}(z),$$

então

$$f_k(z) = \sum_{n=1}^{\infty} \mu(n) g_{nk}(z),$$

e a recíproca é também verdadeira. Uma condição suficiente para a convergência é, analogamente ao dado por Hardy e Wright (2008, p. 308), a convergência da série $\sum_{l,n} |f_{nlk}(z)| = \sum_c d(c)|f_{ck}(z)|$, onde $d(n)$ é a quantidade de divisores de n, embora não seja condição necessária.

A fórmula me chamou alguma atenção na época, mas a esqueci. Foi apenas mais tarde que suas conseqüências se mostraram úteis. Dos meus tempos como estudante de música, tive contato com debates a respeito do timbre, em particular o da posição de "nota pura"conferida por vezes aos sons provocados pelas ondas senoidais. É possível que isso seja historicamente justificado pela descoberta das séries de Fourier, este que constatou a densidade das somas de translações de senoides compostas à direita com multiplicações naturais no espaço das funções periódicas[17]. Com as considerações multiplicativas logo acima expostas, percebi que podia caracterizar multiplicativamente séries de Fourier pares e ímpares, por meio daquelas composições laterais à direita com multiplicações por números naturais. A caracterização multiplicativa da construção de séries de Fourier me permitiu executar uma inversão multiplicativa, e obter representações das próprias senoides pelas mesmas composições à direita, agora aplicadas à função periódica inicialmente representada: se

$$g(x) = \sum_{n=1}^{\infty} b_n \sin(nx),$$

com $b_1 \neq 0$, então

[17] Quase sempre.

$$\sin(x) = \frac{1}{b_1}g(x) - \frac{b_2}{b_1^2}g(2x) - \frac{b_3}{b_1^2}g(3x) - \left(\frac{b_4}{b_1^2} - \frac{b_2^2}{b_1^3}\right)g(4x) - \frac{b_5}{b_1^2}g(5x) - \left(\frac{b_6}{b_1^2} - 2\frac{b_2 b_3}{b_1^3}\right)g(6x) + \cdots$$

Musicalmente, a conclusão é que diversos outros timbres, que não o gerado pelas ondas senoidais, são assim capazes de gerar o mesmo espaço - ao custo de, possivelmente, complicar os coeficientes para representar as ondas mais conhecidas.

Já matematicamente, o espaço das senoides munido da soma usual das imagens e de uma multiplicação definível a partir destas composições laterais, forma uma álgebra isomorfa à álgebra convencional das séries de Dirichlet. Este acontecimento despertou minha curiosidade para a descrição geral de todas as instâncias onde o processo ocorre, me levando a empregar uma linguagem vetorial e os métodos da álgebra linear. Inicialmente formalizando conceitos da teoria multiplicativa desta forma, **percebi a presença de uma teoria muito mais fundamental, simples e vasta**, que parte de um conjunto parco de axiomas e definições, mas capaz de expressar de uma só vez a totalidade das relações algébricas combinatórias visíveis na manipulação das funções geradoras tal como utilizadas nas teorias aditiva e multiplicativa dos números.[18]

Unifiquei o ambiente característico destes procedimentos aditivos e multiplicativos no conceito de *espaço aritmético*. Isto foi possível primeiro graças a uma descrição rigorosa do conceito de Aritmética, a uma interpretação de que a aritmética não é meramente a ciência dos números, mas das coisas numeradas (bem ordenadas).

A conseqüência mais fundamental é a de que a princípio o objeto de discurso da aritmética não se limita a ser número puro, mas pode admitir determinações adicionais e independentes, **induzindo também sobre sua função sucessora essas qualidades**. Por exemplo, a consideração de espaço aritmético leva à consideração de espaço de operações.

As definições fundamentais e investigações puramente aritméticas encontram-se no capítulo 1. Dado um conjunto totalmente ordenado $U = \{x_1,\ x_2,\ \cdots\}$, definimos sua aritmética formal A como o par (x_1, s), sendo s a função sucessora de U, assim como a noção de extensão de uma aritmética formal finita, em especial a extensão nilpotente e a circular. Isso corresponde exatamente a um modelo dos axiomas de Peano para o caso enumerável, e uma adaptação destes, no caso finito.

Para realizar a estrutura operacional aritmética, transportada da aritmética natural convencional, definimos a noção de operações aritméticas iterativas, e fizemos um contraste com as operações aritméticas endomórficas, ambas definidas a partir da noção de somas, as iterações da função sucessora. Descobrimos que da quarta operação em diante,

[18] O problema que Hardy colocou para a demonstração de fórmulas convolutivas discretas a partir da manipulação algébrica de séries de potências ou de Dirichlet, a saber, de que dependiam de condições adicionais de convergência destas séries, desaparece completamente no caso linearmente independente (a informação é distribuída em infinitas dimensões), ambiente lógico simples para a prova destas identidades convolutivas pelas relações algébricas.

as operações superioras aqui definidas coincidem estruturalmente com as operações historicamente denotadas hiperoperações inferioras.

Além disso, introduzimos as estruturas algébricas dos monóides de operações aritméticas para as operações aritméticas iterativas nilpotentemente estendidas, estrutura básica de toda a nossa teoria, e investigamos algumas de suas propriedades, que carregam informações aritméticas. A noção de monóide misto é especialmente importante, por conta da lei de comutação entre somas e multiplicações aritméticas. Para o caso finito não estendido, foi necessário criar uma variação desta estrutura, a qual chamamos inframonóide, que, em particular, não é um magma. Trazemos o conceito de monóide topológico para fundamentar a construção topológica que se estenderá espacialmente nos próximos capítulos.

A noção de homomorfismos de monóides aritméticos nos permitiu provar o teorema (1.4.2), que diz que para quaisquer duas aritméticas infinitas, os monóides de operações aritméticas são isomorfos andar a andar. O mesmo vale para aritméticas finitas de mesma extensão. Com estas definições, fomos capazes de investigar a noção de **automorfismos aritméticos**. Em particular, provamos que para aritméticas infinitas, h é automorfismo aritmético do monóide $(A_2, \circ)$ de multiplicações se, e somente se, h permuta multiplicações primas. Para o estudo dos casos finitos, desenvolvemos a noção de **homomorfismos limitado**, que é capaz de ser bem definida sobre os monóides nilpotentemente estendidos. A quantidade e características destes homomorfismos pode revelar informações. Por exemplo, vale

$$|End_{\lim}(A_1)| = ord(A) = N.$$

Se considerarmos todos os endomorfismos limitados, temos

$$|End_{\lim}(A_2)| = N^{\pi(N)}.$$

Por outro lado, para os endomorfismos limitados decrescentes de A_2, vale

$$|End^{\geq}_{\lim}(A_2)| = \#N,$$

sendo $\#$ o primorial.

O mais importante destes resultados concerne a quantidade de endomorfismos limitados de A_2 cuja imagem ainda gera todo o monóide, pois estes endomorfismos são projeções finitas dos automorfismos do caso infinito. Se a ordem da aritmética é N, a quantidade destes endomorfismos é

$$|End^{*}_{\lim}(A_2, \circ)| = \pi(N)!.$$

Como estes endomorfismos limitados de operações se estendem para os homomorfismos limitados da R-álgebra de operações, isto também conta os endomorfismos limitados desta álgebra.

Definimos brevemente a noção de **transformada fundamental** e **operações aritméticas duais**, antecipando o conceito de Transformada de Gelfand de álgebras para os monóides. A segunda é construída como extensão linear da primeira.

Desenvolvemos também o conceito de meta-aritmética, *uma aplicação do conceito de aritmética a si mesma*, relevante para a compreensão estrutural das operação. Através da meta-aritmética das operações nilpotentes, descobrimos a relação

$$End_{\lim}(A_1) \cong A_2.$$

conceito que se estende linearmente para às álgebras de operações nilpotentes:

$$End_{\lim}(S_A) \cong F_A.$$

A_2 atua em U assim como End(A_1) atua em A_1.

Finalmente, a partir da noção de extensão do conjunto originário U a fim de garantir a existência de operações aritméticas inversas, fizemos alguns comentários sobre as noções de integralização, fracionalização, algebraização e completamento aritmético. São construções teóricas importantes e fundamentais, mas, no entanto, não nos debruçaremos devidamente sobre elas neste trabalho.

Conforme anunciamos, a contribuição mais importante deste texto para os fundamentos das teorias aditivas e multiplicativas segundo funções geradoras foi a definição dos espaços aritméticos, dada no capítulo 2. Trata-se da admissão de axiomas adicionais aos axiomas de Peano, que acrescentam uma estrutura vetorial sobre os elementos além da estrutura aritmética, simplesmente por considerar progressões de vetores. Quando tais vetores são linearmente independentes, é possível considerar a **extensão linear das operações aritméticas** sobre todo o espaço gerado pelos vetores ordenados, assim como o próprio espaço $E(A)$ destas extensões, e mesmo este espaço como álgebra $Alg(A)$ de operadores quando equipado com a composição de suas funções, assunto sobre o qual nos debruçamos no capítulo 3. Ainda no capítulo 2, definimos a noção de **gerador aritmético** e **avaliação gerativa**, o mais importante recurso que liga a teoria aritmética abstrata a estruturas presentes no espaço vetorial sobre o qual as operações agem.

Com isto, cria-se o ambiente lógico algébrico adequado para a demonstração de inúmeras fórmulas primitivas convolutivas, sem ser necessário nos debruçarmos sobre questões de convergência de séries, como colocado por Hardy. Portanto **sistematizei o ambiente lógico fundamental** para a demonstração sistemática destas famosas identidades, evitando os argumentos elementares diretos. A estrutura de Alg(A) até a terceira operação pôde ser descrita como anel em múltiplas variáveis, da forma

$$\frac{R[s,\ f_2, \cdots, f_p, J_2, \cdots, J_q]}{(s^N)(f_p \circ s - s^p \circ f_p)(J_{p_1} \circ f_{p_2} - f_{p_2}^{p_1} \circ J_{p_1})}$$

sendo $p \leq N$ primo e $q \leq \log_2 N$ primo. Comentamos também sobre a Lei de correspondência entre o caso enumerável o nilpotente, fruto de nossas considerações sobre a extensão nilpotente recuperar o caso finito não estendido. Citamos alguns resultados clássicos da teoria das álgebras de Banach e da análise harmônica, conforme Folland (1995), e sugerimos que as informações críticas aritméticas possivelmente podem ser obtidas através do grupo fundamental destas álgebras (ou de seus grupos de elementos invertíveis), o estudo da monodromia, ou mesmo ao complexo de grupos de homologia associados.

Como a axiomática aqui estabelecida forma o ambiente universal para todas as aritméticas, o tema convolutivo que surge nos coeficientes das bases destas álgebras mostra-se parte logicamente intrínseca da aritmética e dos resultados número-teoréticos, fornecendo uma interpretação sólida para a razão do fato. Em especial, pudemos mostrar que o importante Teorema Tauberiano de Wiener, aqui exposto na generalidade do Teorema Tauberiano de Wiener-Pitt, encaixa-se como uma luva na linguagem aqui declarada e desenvolvida, culminando no seguinte teorema Tauberiano: Seja $\varphi \in S_A$ com coeficientes $\phi(n)$ limitados, $\alpha \in S_A$ com coeficientes a_n absolutamente somáveis. Suponhamos que $\hat{a}$ não se anule, e que os coeficientes $\phi * a(n)$ de $\varphi \circ \alpha$ tendam a $d \sum |a_n|$, quando $n \to \infty$. Então

i) os coeficientes de $\varphi \circ \beta$ tendem a $d \sum |b_n|$, quando $x \to \infty$, **para todo** $\beta \in S_A$ cujos coeficientes b_n sejam absolutamente somáveis;

ii) Se ϕ é lentamente oscilante, então $\phi(n) \to d$, quando $n \to \infty$.

Também consideramos brevemente o estudo do espectro de F_A para coeficientes absolutamente somáveis (o espectro do caso aditivo é determinado pelo espectro da função sucessora, o disco unitário complexo.)

Foi de especial proveito considerar as subálgebras definidas pelas restrições da álgebra de operações a cada uma das operações separadamente. As chamaremos S_A e F_A para as restrições à soma e multiplicação aritméticas, respectivamente. Como toda aritmética de mesma ordem e extensão é isomorfa, podemos falar de "a"R-álgebra de operações aritméticas infinitas, "a"R-álgebra de operações aritméticas finitas nilpotentes de ordem N, etc. Mostramos como as aritméticas aditivas tem como elementos avaliações polinomiais da função sucessora, independentemente da extensão.

Estudei a forma destas álgebras segundo a teoria de anéis de polinômios. Para uma aritmética infinita, S_A é isomorfo a $R(s)$, e F_A ao anel de polinômios em infinitas variáveis $R(f_1,\ ..., f_p,\ ...)$. Os casos finitos serão investigados na seção adequada. Estas álgebras,

consideráveis naturalmente após a definição geral de espaço aritmético, formam o ambiente lógico para a expressão das funções geradoras e investigações da combinatória. Em particular, valem relações de invertibilidade aditivas e multiplicativas gerais para os elementos desta álgebra, generalizando por completo a inversão para a senóide dada pouco acima. Mais abaixo retornaremos ao tema destas inversões.

A álgebra de operações aritméticas estabelece ligações entre S_A e F_A independentes da mera consideração conjunta das variáveis para um anel de polinômios, afinal as funções multiplicativas exibem uma dependência da função sucessora e exigem os quocientes pelos ideais $(f_p \circ s - s^p \circ f_p)$. Estas condições parecem estabelecer algo diferente da manipulação de séries de potências ou de Dirichlet em separado. Neste sentido, a álgebra de operações finita nilpotente de ordem N também parece ser nova na literatura, e pode ser obtida como quociente pelo ideal (s^N) sem se mostrar necessário quocientar pelas multiplicativas em separado. A relação entre os f_p e s acima nesse caso já implica $f_K \equiv 0,\ K > N$ e outras anulações com respeito a suas ações no conjunto recursivo U.

O grupo dos elementos invertíveis da álgebra de operações, com respeito à composição, carrega implicitamente uma informação aritmética fina, decorrente de sua construção em termos de somas das extensões lineares das operações aritméticas, cujas implicações são parcialmente estudadas no capítulo 6. Provamos um resultado importantíssimo para estes elementos: a decomposição em fatores elementares[19]. De fato, é um **teorema muito mais simples e geral que o teorema fundamental da álgebra**, que pode ser atingido facilmente pela forma inversa de inversão compositiva multiplicativa usando a decomposição como lema e a noção de fechamento algébrico do anel R. Mostramos que se a é elemento invertível de S_A de determinante 1, então existem únicos $b_1, \cdots,\ b_{N-1} \in R$ tais que

$$a^{-1} = \bigcirc_{k=1}^{N-1}(s_0 - b_k s_k). \text{ (Inversão compositiva aditiva direta)}$$

Também existem únicos $b_1, \cdots,\ b_{N-1} \in R$ tais que

$$a = \bigcirc_{k=1}^{N-1}(s_0 - b_k s_k). \text{ (Inversão compositiva aditiva inversa)}$$

Resultados análogos valem para $F_A^{\times}$: existem números no próprio anel R tais que

$$a^{-1} = \bigcirc_{k=2}^{N}(f_1 - b_k f_k), \text{ (Inversão compositiva multiplicativa direta)}$$

e

$$a = \bigcirc_{k=2}^{N}(f_1 - b_k f_k). \text{ (Inversão compositiva aditiva inversa)}$$

[19] Tais fatores são diferenças entre a identidade e os elementos da base do espaço, como $(s_0 - y_n s_n)$ e $(f_1 - y_n f_n)$, sendo $y_n \in R$

A investigação proposta pelo capítulo 4 é combinatória e investiga as conseqüências de certos produtos algébricos, em especial o generalizado de Euler para F_A. De fato, o reflexo destas relações algébricas no espaço primitivo dos coeficientes é a existência de diversas relações numéricas combinatórias elementares interessantes. Nos dedicamos a descrever, em especial, relações explícitas entre $Z = \sum_n f_n$ e $P = \sum_p f_p$, como a construção algébrica de Z por P e de P por Z. Em relação à última, a construção é sugestiva e possivelmente reserva frutos para a investigação futura. Me refiro, por exemplo à simplificação dos coeficientes[20] da fórmula

$$P := \sum_p f_p = \sum_{l=1}^{\infty} \frac{1}{l} \sum_{k\cdot n=l} \mu(k)(-1)^{n+1}\mathbf{J}_k(Z - f_1)^n,$$

fato relacionado às condições que tornam a iteração de Frobënius um automorfismo de corpos primos, e mesmo à existência de automorfismos mais complicados para todos os anéis cíclicos de cardinalidade livre de quadrados. Do ponto de vista dos números naturais e primos, a fórmula descreve uma maneira de categorizar os compostos, e oferece uma família de pesos inteiros para cada contagem de categoria destes compostos, que permite o cálculo da quantidade de números primos abaixo de uma dada quantidade.

Este cálculo não se mostra útil para quem deseja obter estimações da quantidade, uma vez que a contagem das categorias de compostos é um problema difícil. No entanto, é logicamente relevante, uma vez que permite a enunciação de uma pergunta em termos de números naturais em geral, sem citar primos uma vez sequer, que guarda exatamente a quantidade de primos, como a exemplo do resultado convolutivo

$$\sum_{k=1}^{\infty} \frac{(-1)^k}{k} d_k^*(n) = \begin{cases} 1/j, \text{ se } n = p^j, \text{ para algum p primo, ou} \\ 0, \text{ noutros casos.} \end{cases}$$

Por conta disso, chamei o resultado sobre a função indicadora de primos de *Lei das Fatorações Naturais*. Vejamos a seguir dois exemplos numéricos. Tomemos, por exemplo, o número N=6. A representação de P em termos de Z nos diz que devemos contar os números maiores que dois até N, N-1=5, e dele retirar uma unidade para cada produto menor ou igual a N de dois números maiores que dois, sendo eles neste caso o par $2\cdot 2 = 4$ e $2\cdot 3 = 6$, obtendo-se assim $N-1-2 = 3$, que de fato é a quantidade de primos menores ou iguais que 6, $\pi(6) = 3$. Para o outro exemplo, consideremos $N = 12$. Neste caso também tomamos a quantidade de números maiores que dois até N, que é $N - 1 = 11$, e também retiramos uma unidade para cada produto até N de números naturais maiores ou iguais a dois, a saber os 7 produtos $2 \cdot 2,\ 2 \cdot 3,\ 2 \cdot 4,\ 2 \cdot 5,\ 2 \cdot 6, 3 \cdot 3, 3 \cdot 4$. Com isso, Chegamos

[20] O fator $1/k$ é cancelado pelos fatores da somação interna, sem que necessariamente os termos dessa somação sejam eles mesmos divisíveis por k.

ao número $N - 1 - 7 = 4$. No entanto, a expressão para P em termos de Z, neste caso, também nos faz levar em conta[21] produtos de quadrados por naturais maiores ou iguais a 2, com peso +1, e produtos de três naturais distintos maiores ou iguais a 2, com peso +2. Até 12, temos apenas o próprio número $12 = 2^2 \cdot 3$. Adicionamos 1 portanto à nossa conta, chegando a $N - 1 - 7 + 1 = 5$. De fato, $\pi(12) = 5$.

A minha negligência sobre a extensão circular de uma aritmética finita me fez levar dois anos para finalmente, em Maio de 2023, descobrir que a álgebra de operações aditivas circulares $S_\circ(A)$ está irremediavelmente envolvida com peças chave de uma teoria muito mais distinta que a meramente linear: (1) **as matrizes canônicas dos elementos desta álgebra são exatamente as matrizes circulantes de Toeplitz**; (2) se diagonalizam numa mesma base ortogonal; (3) a matriz de mudança de base para estes autovetores é nada mais, nada menos, que a transformada de Fourier discreta; (4) toda matriz diagonal conjugada pela transformada de Fourier discreta pertence a $S_\circ(A)$, e (5) os autovalores da função sucessora estendida circularmente são exatamente as N N-ésimas raízes de unidade, onde N é a ordem da aritmética. Todos os elementos são a avaliação de um polinômio matricial na função sucessora c e portanto o mapa espectral determina que os autovalores de qualquer elemento desta álgebra são dados pela avaliação polinomial numérica diretamente nos autovalores de c, um a um. É possível efetuar o cálculo finito e exato destes autovalores, cujo argumento é a média dos argumentos complexos individuais, ponderada pelas normas individuais. Este resultado é descrito pelo lema da redução, e diz que se $z_1, \cdots, z_N$ são números complexos cujas formas polares são $\rho_1 e^{i\theta_1}, \cdots, \rho_N e^{i\theta_N}$, e se $\rho_* e^{i\theta_*} = \sum_{n=1}^{N} z_n$, então

$$\rho_* = \sqrt{\sum_{n=1}^{N} \rho_n^2 + 2 \sum_{1 \le i < j \le N} \rho_i \rho_j \cos(\theta_i - \theta_j)}, \ e$$

$$\theta_* = \frac{\sum_{n=1}^{N} \theta_n \rho_n}{\sum_{n=1}^{N} |\rho_n|}.$$

Com isto, obtive fórmulas exponencias que determinam toda forma de convolução discreta circular, desde que o anel dos coeficientes convoluídos inclua as N raízes de unidade. A determinação dos coeficientes da base exponencial é obtida por um problema independente, o da análise dos autovalores das matrizes circulantes envolvidas. Desta forma, fui capaz de simplificar grandemente a teoria das convoluções circulares e seu cálculo. Se consideramos somas ponderadas de convoluções circulares iteradas, estas são formadas exatamente por uma avaliação polinomial de um elemento a da álgebra $S_\circ(A)$, igualando $P(a) = 1/N \ F_N^{-1} \times \Lambda_{P(a)} \times F_N$, de onde a avaliação do problema convolutivo na j-ésima entrada ($j = 1, 2, \cdots, N$) é

[21] Notem que, conforme a fórmula, os números cúbicos são desprezados nesta estrutura

$$\frac{1}{N}\sum_{b=1}^{N} P(\lambda_b)e^{-2\pi i\frac{(j-1)(b-1)}{N}},$$

se os autovalores de a são λ_b. Por exemplo, a auto-convolução circular simples é simplesmente obtida por a^2, e

$$\sum_{l_1+l_2\equiv j \mod N} a_{l_1}a_{l_2} = \frac{1}{N}\sum_{b=1}^{N}\lambda_b^2 e^{-2\pi i\frac{(j-1)(b-1)}{N}}.$$

Isto me inspirou a, nos casos finito nilpotente e enumerável, considerar uma álgebra maior, a qual chamei de álgebra simetrizada $\mathbf{Alg}(A)$, no capítulo 5. Gerada pelas operações aritméticas e suas transpostas, é uma aritmética auto-adjunta com grandes qualidades e conexões (com devidas considerações sobre a completude do anel em uma norma, pode ser uma C^*-álgebra.). Me permitiu expressar uma teoria da simetrização das operações nilpotentes ou enumeráveis, e obter alguns dos resultados mais importantes de todo o texto[22]. O caso nilpotente, que não gera matrizes de Toepliz diagonalizáveis, pode ser modificado de maneiras naturais para tornar-se uma, dentro do tema da **teoria vaga dos correspondente simetrizados**: correspondentes que utilizam o fato do monóide aritmético adjunto ser um monóide aritmético de mesmo andar para adicionar componentes preservando algumas propriedades aritméticas do elemento original. A mais importante destas teorias foi dada pelas equações de tradução, que constroem a função sucessora estendida circularmente e suas iterações pela nilpotente de mesma ordem e sua adjunta (isto é, o espaço das somas circulares está contido no espaço das nilpotentes simetrizadas, sem sequer precisarmos definir a noção de composição no espaço). Esta conexão permite estabelecer uma conexão entre a noção de convolução linear e convolução circular, que podem ser relacionadas por meio algébrico, a partir das operações aditivas nilpotentes adjuntas.

Como mostrei há alguns parágrafos, fui capaz de obter equações de representação de cada coeficiente das bases de operações consideradas em termos de combinações **finitas** de exponenciais. Em outras palavras, deduzi a existência e forma de combinações finitas de exponenciais (autovalores das circulantes correspondentes) que representam as convoluções circulares. No entanto, não fui capaz de transportar esses resultados de volta às convoluções lineares, cuja representação seria de extrema importância, pois permitiria uma representação de todos os seus coeficientes como combinação finita de exponenciais. É de se perguntar se haveria algum anel algebricamente fechado tal que, quando utilizado

[22] É importante destacar que o caso nilpotente, como álgebra, gera todo o espaço das matrizes $N \times N$. Mesmo assim, a noção de limitação do número de composições funciona, tendo sida declarada a forma geral de todos os elementos gerados, se quisermos evitar que se gere todo o espaço de matrizes (sendo um espaço, mas não sendo a operação de composição fechada). Este problema não existe no caso infinito enumerável, onde a álgebra nunca gera todo o espaço de matrizes.

como coeficientes destas matrizes, tornasse a função sucessora nilpotentemente estendida diretamente diagonalizável. Se existe, não o vislumbrei.

Estudei alguns problemas análogos a certas convoluções lineares através de seus correspondentes circulares. Em particular, pude utilizar o famoso teorema pentagonal de Euler (em sua forma algébrica) para construir combinações finitas de exponenciais de freqüência pentagonal idênticos à soma dos divisores de um número, e ao número de partições. A representação é notória, no sentido que tanto a estrutura da soma quanto dos números envolvidos é simples e independente de problemas de convolução, fatoração, ou coisa parecida, a partir dos autovalores do elemento $E_\circ$, cujos autovalores, a cada período completo, tem seus argumentos determinados perfeitamente por

$$Arg(\eta_{j+1}) = 2\pi j \frac{(6k+3)}{4(k^2+k)} \mod 2\pi,\ j = 0, \cdots, N-1.$$

Estudei no capítulo 6 uma generalização da teoria de caracteres de grupo com imagens em corpos para domínios abelianos com unidade, afinal o espaço pode ser um módulo sobre um anel R. Como o grupo considerado é o dos elementos invertíveis da R-álgebra das operações, consideramos o problema de representar os funcionais da álgebra para o próprio domínio R por meio de caracteres. Ele não é imediatamente passível de solução, pois o R pode não ter raízes de unidade suficiente para representar $G = G(R)$. Tentei resolver o caso finito considerando a menor extensão R_{ext} construída a partir da decomposição do grupo abeliano finito G em termos de grupos cíclicos, e os caracteres ganham uma definição $\chi : G(R) \to R_{ext}$. Apesar da generalização ter sido um sucesso, seus detalhes mostraram a impossibilidade da aplicação direta para os grupos $S_A^\times$ e $F_A^\times$. De toda forma, fomos capazes de desenvolver uma teoria bem sustentada dos R_{ext}-espectros, onde definimos as transformadas de Fourier de grupos finitos (cuja cardinalidade não seja divisível pela característica do anel) como

$$\hat{f}(\chi) = (|G|) \cdot c_{\overline{\chi}} = \sum_{a \in G} f(a)\chi(a).$$

A transformada inversa garante a representação trigonométrica

$$f = \frac{1}{(|G|)} \sum_{\chi \in \widehat{G}} \hat{f}(\overline{\chi})\chi,$$

quando $(|G|)$ é invertível.

Se R é um domínio topológico, o grupo G dos elementos invertíveis da R-álgebra das operações é um grupo topológico. Quando estes são localmente compactos, sempre admitem uma medida de Radon invariante por translações, chamada medida de Haar, o que

permite criar uma teoria natural de integração de funcionais destes grupos. (FOLLAND, 1995, p. 37). Em particular, se consideramos os funcionais f de S_A ou F_A restritos a $G = S_A^\times$ ou $G = F_A^\times$ tais que $f \in L^1(G)$ e $\hat{f} \in L^1(\widehat{G})$, vale a representação

$$f(a) = \int_{\widehat{G}} \chi(a)\hat{f}(\chi)d\chi$$

para quase todo $a \in G$[23].

Os funcionais $f : G(R) \to R \subset R_{ext}$ naturalmente representam quantidades aritmeticamente notáveis, ainda mais quando também distribuem-se em relação à composição, como homomorfismos da álgebra. Desejávamos para estes funcionais, restritos ao elementos invertíveis da álgebra, uma representação trigonométrica em termos dos caracteres do grupo, cujos coeficientes são dados pela inversão de Fourier. Isso só se mostrou de fato possível para anéis cuja característica é 0. Em particular, provamos que se R é subanel de $\mathbb{C}$, vale a representação trigonométrica para os funcionais das álgebras comutativas unitais de operações[24]:

$$f(x) = \int_{\xi \in \widehat{G}} \xi(x)\hat{f}(\xi)d\xi.$$

Em particular, a representação da função de Mertens para uma aritmética de ordem N,

$$M(N) = \int_{\xi \in \widehat{F_A^\times}} \frac{\widehat{h}(\xi)}{\xi(Z)}d\xi.$$

Esta fórmula tem diversas características interessantes, afinal a computação do grupo, de seu dual, e das raízes de unidade $\chi(Z)$ não dependem de uma informação aritmética, são problemas de outro gênero. Em especial, nota-se como as propriedades dos caracteres fizeram desaparecer da expressão à direita a função Z^{-1}, exatamente como a transformada inversa de Mellin da função Zeta o faz, caso em que a composição de funções é identificada com a multiplicação convencional, dada pela fórmula de Perron:

$$M(x) = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} \frac{x^s}{s\zeta(s)}ds.$$

A representação geral, que não consegui obter, permitiria a representação de $M_R(N) = \sum_n \mu_R(n)f(r_n)$, a função de Mertens adaptada para a unidade específica do domínio.

É interessante notar como estas fórmulas e representações são encontradas ao analisarmos construções gerais sobre os espaços aritméticos das operações, sem considerações particulares acerca da natureza dos vetores linearmente independentes em progressão sobre

[23] Uma aplicação da análise harmônica abstrata, como em Folland (1995, p. 102).

[24] Estes resultados são imprecisos, pois os funcionais não são L_1, mas naturalmente elementos do espaço de medida das medidas complexas de Radon $M = M(G)$, como em Folland (1995, p. 94).

os quais está definida a aritmética em questão. Isso é a princípio diferente de considerar-se, por exemplo, os espaços de funções das séries de potência ou de Dirichlet e obter informações sobre coeficientes a partir da análise complexa, utilizando a dependência dos vetores de uma variável independente.

Por último, sugerimos no capítulo 7 uma investigação analítica independente, nos moldes da teoria harmônica aplicada às séries de Dirichlet complexas, em particular a teoria de resíduos, tal como em Titchmarsh (1986), aplicada para a função de contagem ponderada de primos J. A fórmula linear

$$LN(Z) = \sum_k \frac{(-1)^k}{k}(Z - Id)^k$$

rende, ao retirarmos o produto interno de ambos os lados com Z, a fórmula

$$J(x) = \sum_{k=1}^{h} \frac{(-1)^k}{k} D_k^*(x).$$

sendo $h \geq log_2(x)$[25]. Resolvemos investigar as conseqüências desta fórmula calculando as D_k^* pelos resíduos de $(\zeta(s) - 1)^k$, onde $\zeta(s)$ é a função Zeta de Riemann. O resultado, um tanto surpreendente, é que as D_k^* resultam da soma de três tipos diferentes de contribuição: a principal, a secundária e terciária.

$$D_k^*(x) = W_k(x) + Y_k(x) + \Delta_k^*(x),$$

onde W_k é o termo principal, Y_k é uma função dependente de uma família de constantes γ_k explicitamente definidas

$$\gamma_k \stackrel{\text{def}}{=} \int_1^\infty \frac{(x - \lfloor x \rfloor)}{x^2}(-\ln x)^k dx$$

e Δ_k^* é o erro clássico de divisores de Piltz adaptado para fatores maiores ou iguais a dois.

Estas representações permitem escrever $J(x)$ (assim como $M(x)$) como

$$J(x) = -\sum_{1 \leq k \leq h} \frac{1}{k} + +A_1(x,h) + B_1(x,h) + B_2(x,h),$$

onde

$$B_1(x,h) = \sum_{2 \leq k \leq h} \frac{(-1)^{k+1}}{k} Y_k(x) \quad e \quad B_2(x,h) = \sum_{1 \leq k \leq h} \frac{(-1)^{k+1}}{k} \Delta_k^*(x).$$

[25] Curiosamente, a liberdade da variável h é parte crucial no argumento desenvolvido.

É fácil mostrar que

$$\lim_{h\to\infty} A_1(x,h) = Li(x) + O(\ln(x)),$$

sendo Li a célebre integral logarítmica. O termo B_2 envolve todos os erros de Piltz, que, segundo a conjectura clássica a respeito destes termos, são limitadas no infinito (em k) por $x^{\varepsilon}\sqrt{x},\ \forall\varepsilon > 0$. Este fato é equivalente à famosa hipótese de Lindelöf de que $\zeta(1/2+it) = O(t^{\varepsilon}),\ \forall\varepsilon > 0$. Esta hipótese é também equivalente ao número de zeros de $\zeta(s)$ com $Re(s) > 1/2+\varepsilon$ e $T < Im(s) < T+1$ ser $o(\ln(T))$ (TITCHMARSH, 1986, p. 331). Parece natural conjecturar que a hipótese de Lindelöf é equivalente a $B_2(x,h) = O(x^{\varepsilon}\sqrt{(}x)),\ \forall\varepsilon$.

Neste caso, recai sobre $B_1(x,h)$ a atenção daqueles interessados pela hipótese de Riemann, uma vez que os outros termos são governados por hipóteses mais brandas. De fato, como as equações $J(x) - Li(x) = O(x^{\varepsilon}\sqrt{x}),\ \forall\varepsilon > 0$ são sabidamente equivalentes à hipótese, a suspeita é de que seja equivalente à mesma limitação sobre $B_1(x,h)$.

O estudo do limite quando h cresce para a função se mostrou proveitoso. Não consegui descobrir a forma explícita simplificada desta misteriosa função que aparentemente guarda a informação da hipótese de Riemann. No entanto, fui capaz de obter uma pista de sua estrutura, possivelmente desconhecida na literatura, através da descrição de sua expansão assintótica semiconvergente. Analogamente a uma técnica que gera a famosa expansão assintótica semiconvergente do termo principal, a integral logarítmica Li

$$Li(x) \approx \frac{x}{\ln(x)} + \frac{x}{\ln^2(x)} + \frac{2x}{\ln^3(x)} + \frac{6x}{\ln^4(x)} + \cdots,$$

obtemos para a curiosa função $B_1(x,h)$, no limite em h, a expansão

$$\begin{aligned}
B_1(x,\infty) \approx & \left(\frac{1}{\ln(x)} - \frac{1}{x^{\gamma_0}\ln(x)}\right) \\
& + \left(\frac{\gamma_0^2 - \gamma_0 - \gamma_1}{x^{\gamma_0}} + \frac{1}{\ln(x)} - \frac{1}{x^{\gamma_0}\ln(x)}\right) \\
& + \left(\frac{1}{x^{\gamma_0}}\left(\gamma_0^3 - \frac{\gamma_0^4\ln(x)}{2} + \gamma_0^3\ln(x) - 2\gamma_0^2 - \frac{\gamma_0}{\ln(x)} - \frac{1}{\ln(x)^2} + 3\gamma_1\gamma_0\right.\right. \\
& \left. - \gamma_1\gamma_0^2\ln(x) - \frac{1}{2\ln(x)} + \gamma_0 - \frac{\gamma_0^2\ln(x)}{2} - \gamma_1\gamma_0\ln(x) - \frac{\gamma_1^2\ln(x)}{2} + \frac{\gamma_2}{2}\right) \\
& \left. + \frac{1}{\ln^2(x)} + \frac{1}{2\ln(x)}\right) + \cdots
\end{aligned}$$

1 Aritméticas formais

1.1 Definições. Função sucessora. Gerador. Aritmética finita e infinita. Contra-sucessão

Definições prévias úteis.

Os conjuntos $\mathbb{N}_0$ e $\mathbb{N}_1$ são o conjunto dos números naturais partindo-se de 0 e 1, respectivamente.

Definição 1.1.1 (Conjunto finito) *Um conjunto U é dito **finito** se, e somente se sua cardinalidade é igual a um número natural n. É o mesmo que dizer que existe uma seqüência bijetiva finita $r : I_N \to U$, sendo $I_n = \{1,\ 2,\ \cdots,\ N\}$, o conjunto dos primeiros n naturais de $\mathbb{N}_1$. Se levada em consideração a ordem dos naturais, estes convenientemente induzem uma ordem sobre U por meio de r.*

Definição 1.1.2 (Conjunto enumerável) *Um conjunto U é dito **enumerável** se, e somente se sua cardinalidade é igual à cardinalidade $\aleph_0$. É o mesmo que dizer que há uma seqüência bijetiva infinita entre U e $\mathbb{N}_1 = \{1,\ 2,\ 3,\ \cdots\}$.*

Definição 1.1.3 (Conjunto contável) *Um conjunto U é dito **contável** se, e somente se, é finito ou enumerável. Neste caso diremos que há uma seqüência contável que o conta bijetivamente em alguma ordem, chamada **progressão**.*

Uma progressão C parte de um primeiro elemento x_1. Se é finito, há x_N último elemento.

Equivalentemente, existe uma função sucessora $s_C : U/\{x_N\} \to U/\{x_1\}$ tal que $s_C(x_n) = x_{n+1},\ n = 1, \ldots,\ N-1$. Certamente

i) não há $u \in U$ tal que $s_C(u) = x_1$;

ii) s_C é injetiva;

iii) os elementos de U são todos da forma $s_C^n(x_1)$, indexados pelas interações de s_C.

Se, por outro lado, U é infinito enumerável, há também um função sucessora, com mesmas propriedades e declaração mais simples $s_C : U \to U$.

Quando é possível atribuir a s algum significado independente ou ação, isso é o mesmo que dizer que todo elemento em ordem de U é formado por repetições desta ação sobre

um mesmo, denotado $x = x_1$. Tais elementos x são o que chamaremos de **elementos geradores** de suas respectivas aritméticas.

Definição 1.1.4 (Funções sucessoras de U) *São aquelas da forma estabelecida acima.*

De fato, cada iteração de uma função sucessora deve ter seus domínios e imagens adequadamente restritos, quando necessário.

Aqui preferimos adicionar um componente formal para o caso finito, admitindo que s agora tenha seu domínio estendido para o último elemento x_N da progressão, de maneira arbitrária. A razão é prática: nos permitirá recuperar o caso original considerando que $s(x_N)$ apenas um símbolo vazio, descarte de informação ou como $\{\}$ ou 0, e ao mesmo tempo conferir a $s(x_N)$ um significado à escolha e independente, ao custo de, possivelmente, perder a injetividade no contexto considerado.

Esta adição completa a formalização na generalidade pretendida.

Definição 1.1.5 (Funções sucessoras finitas estendidas) *Se denotamos $x = x_1, a = s(x_N)$, então uma **função sucessora de U** s estendida a x_N é da forma*

$$s : U \to (U \cup \{a\}) / \{x\},$$

sendo o restante de sua imagem determinado pela função sucessora original. Este é o modelo mais geral de função sucessora finita que abordaremos.

Definição 1.1.6 (Aritmética) *Seja U conjunto contável, s função sucessora em U e $x \in U$ gerador na ordem estabelecida por s. Então definimos uma **aritmética em** U como o par ordenado $A = (x, s)$.*

Se U é finito, uma aritmética finita estendida é um trio $A = (x, s, a)$, onde s é estendida.[1]

*Em todos os casos consideramos a **ordem** da aritmética como card(U).*

Conforme vimos, o conhecimento de uma aritmética em U determina U totalmente, uma vez que, conhecidos x e s, $U = \{x,\ s(x),\ \cdots,\ s^n(x), \cdots\}$, e U é **recursivamente gerado**.

[1] Estando livre o leitor para a partir do conceito estabelecer mais alguma condição sobre o elemento "a" desejada.

Definição 1.1.7 (Ariméticas nilpotente e circular) *Neste trabalho trataremos basicamente de aritméticas finitas estendidas de duas formas:*

i) quando ***a*** *representa a perda da informação, um símbolo vazio ou mesmo 0, chamamos a aritmética* $(x, s, 0)$ *de* ***nilpotente****, e recupera o caso não estendido, mais simples. Neste caso fazemos* $U_0 = U \cup \{0\}$ *e estendemos* s *a* $s : U_0 \to U_0$*, e definimos sua imagem como* $s(0) = 0$.[2]

ii) quando a=x, chamamos a aritmética (x, s, x) *de* ***circular****, e geralmente denotaremos* $s = c$*. Esta aritmética já foi bastante estudada e aqui nos servirá para comparações.*

Conforme comentamos no contraste entre os conceitos de número natural e aritmética, a aritmética finita nilpotente respeita exatamente a estrutura da aritmética dos números naturais de Frege em um universo finito de elementos[3]. O conceito de número de Frege leva todos os números maiores que a quantidade de elementos do universo a se identificar com o conjunto vazio. Isso é análogo a função sucessora de uma aritmética finita nilpotente gerar uma seqüência da forma $x_1, x_2, x_3, \cdots, x_N,\ 0,\ 0,\ 0 \cdots$ que, como comentei, recupera o caso não estendido, $x_1, x_2, x_3, \cdots, x_N$.

Uma coisa que não observamos até agora, é que um conjunto bem ordenado finito admite outras boas ordens, totalizando $N!$. Não as estudaremos aqui, a menos da contra-aritmética $A^{[-1]} = (x_N, s^{[-1]})$, sendo $s^{[-1]}$ chamada **contra-sucessão**, tal que $s^{[-1]}(x_n) = x_{n-1},\ n = N,\ N-1,\ \cdots,\ 2$.

Exemplo 1.1.1 (Aritmética Natural) *A mais importante de todas as aritméticas é a aritmética natural* $A = (1, s_1)$*, onde* 1 *é primeiro elemento de* $\mathbb{N}_1$*,* $s_1 : \mathbb{N}_1 \to \mathbb{N}_1$ *e* $\forall n \in \mathbb{N}_1(s_1(n) = n + 1)$.

1.2 As operações aritméticas iterativas

1.2.1 Iterações da função sucessora e suas simetrias

A operação aritmética fundamental é a aplicação da função sucessora. Suas iteradas aplicações constituem o conjunto fundamental de operações A_1, a família das somas. A iteração de uma soma permite definir a multiplicação. A iteração de uma multiplicação permite definir uma potência. A composição de iterações é aditiva; a iteração de iterações,

[2] É interessante notar que na linguagem que desenvolveremos $s(0) = 0$ implica $s^k(0) = 0$, e ainda que $s^N \equiv 0 : U$ é mínima em N com a propriedade; e que $f_{k+1}(x_n) = s^{(k)n}(x_n)$, também temos que $f_{N+1} \equiv 0$ é a menor multiplicação nula.

[3] Notando que a definição de função sucessora de Russell (1920, p. 24) só se aplica a um universo infinito, evitemos confusões.

multiplicativa. Estas operações aritméticas, aqui chamadas de iterativas, formam uma cadeia infinita, que corresponde ao que tradicionalmente chama-se de hiperoperações inferioras.

No entanto, não há uma maneira única de definir as operações aritméticas. Um outro conceito, o de simetria (homomórfica), também tem seu apelo para a definição de operações aritméticas, estas que chamaremos endomórficas.

Faremos uma análise comparativa, mostrando que o conceito iterativo e endomórfico são iguais para as primeiras operações, isomórficos para as segundas operações e que as terceiras operações iterativas determinam uma estrutura isomórfica a uma subestrutura da estrutura determinada pelas terceiras operações endomórficas.

Uma iteração só pode ser executada quando a entrada é uma função cuja imagem tem intersecção não nula com o domínio, levando à definição do domínio de iteração sobre a restrição das entradas àquela intersecção. Se quisermos considerar um ambiente simples para a consideração ilimitada de iterações, um candidato são as funções com contradomínio contido no domínio. Este é o caso para uma função sucessora, e será para os conjuntos de operações iterativas definidos a seguir.

Definição 1.2.1 (Primeira família de operações aritméticas iterativas) *A família $A_1 = (s_n)_{n\in\mathbb{N}_0}$ das somas de uma aritmética $A = (x, s)$ ou $A = (x, s, a)$ é precisamente a composta pelas funções $s_n = s^n,\ \forall n$, as n-ésimas iterações de s, quando não nulas.*

No caso finito a operação s_n é definida como $s_n : \{x_1, \cdots,\ x^{N-n}\} \to \{x_{n+1}, \cdots,\ x_N\}$, apesar de poder ter seu domínio estendido a todo U para as aritméticas circular e nilpotente de maneira natural. A fim de simplificar a declaração das funções neste trabalho, consideramos apenas estes casos, e **todas as operações a seguir podem ser consideradas com domínio em U**[4]. Inclusive, esta simplificação de declarações é uma das razões para tratar o caso finito por meio de sua extensão nilpotente [5]

Proposição 1.2.1 *No caso em que a aritmética é circular ou nilpotente, esse conjunto é finito, de cardinalidade igual à da contagem associada.*

Dem.: Basta notar que no caso circular temos $s^N = Id$, e no nilpotente $s^N \equiv 0$, sendo N o menor número com a propriedade, e $s^j \neq s^k$, se $j \neq k$.

A inclusão de $s^0 = Id$ em A_1 é opcional, havendo mínimas vantagens circunstanciais para ambas as opções.

Nota-se que $s_n \circ s_k = s_{n+k},\ \forall n, k$, e sua composição é **aditiva**.

[4] Ou $U_0 = U \cup \{0\}$, no caso nilpotente.

[5] Para o caso geral de operação dada abaixo, seria necessário recorrermos às hiperoperações inversas para a determinação dos índices corretos dos elementos dos domínios, complicação que não nos interessa.

Definição 1.2.2 (Segunda família de operações) *A família $A_2 = (f_n)_{n\in\mathbb{N}_1}$ das multiplicações de uma aritmética $A = (x, s)$ ou $A = (x, s, a)$ tem seus elementos definidos pelas seguintes relações:*

$$f_1 = Id;$$
$$f_{n+1}(x_j) = s_j(f_n(x_j)),\ \forall n, j.$$

Conforme notamos anteriormente, consideramos $f_n : U \to U$ no caso circular, ou $f_n : U \cup \{0\} \to U \cup \{0\}$, com $f_n(0) = 0,\ \forall n$ no caso nilpotente, fato implicado pela aplicação da recursão acima a 0.

Neste caso, na notação geral escreveremos $f_n = a_{2,n}$ para representar a n-ésima operação do segundo andar.

Verifica-se, de fato, que $f_n(x_j) = x_{nj}$, quando $n \cdot j \leq N$, fato que inclusive lhes serve equivalentemente de definição. Ainda mais,

$$f_n(x_j) = x_{nj \mod N},\ \text{no caso circular, e, para o nilpotente,}$$
$$f_n(x_j) = \begin{cases} x_{nj},\ \text{se } nj \leq N; \\ 0,\ \text{se } nj > N. \end{cases}$$

A definição de multiplicação é a primeira das operações que chamaremos de superioras, as $a_{k,n},\ k \geq 2$. Todas estas são definidas pelo mesmo tipo de recursão, que inclui a própria multiplicação, já definida.

Definição 1.2.3 (Famílias de operações aritméticas superioras) *A família $A_k = (a_{k,n})_{n\in\mathbb{N}_1},\ k \geq 2$ de operações de k-ésimo nível de uma aritmética (x, s) ou (x, s, a) tem seus elementos recursivamente definidos pelas relações:*

$$a_{k,1} = Id$$
$$a_{k+1,n+1}(x_j) = a_{k,j}(a_{k+1,n}(x_j)),\ \forall n, j,$$

sendo $a_{k,n} : U \to U$ no caso circular e $a_{k,n} : U \cup \{0\} \to U \cup \{0\}$ no caso nilpotente, sendo $a_{k,n}(0) = 0, \forall n, k$.

Assim temos que $s_n = a_{1,n}$ a n-ésima operação do primeiro andar, se excepcionalmente consideramos s^0 a 0-ésima. Esta definição, que com sucesso imita o comportamento esperado de multiplicações para $f_n = a_{2,n}$ e potências para $J_n = a_{3,n}$, gera, para $k \geq 4$, as chamadas hiperoperações inferioras, que estendem as operações aritméticas através

da associatividade à esquerda. Neste trabalho nos interessará apenas o estudo dos casos tradicionais $k = 1, 2, 3$, as chamadas operações de soma, multiplicação e potência.

Afirmação 1.2.1 *Valem as seguintes propriedades:*

i) $a_{k+1,n+1}(x_j) = a^n_{k,j}(x_j),\ \forall n, j, k.$

ii) $s_k \circ s_n = s_{n+k}$; $f_n \circ f_k = f_{nk}$; $J_n \circ J_k = J_{nk},\ \forall n, k$

iii) $a_{k+1,n} \circ a_{k,v} = a^n_{k,v} \circ a_{k+1,n}, k = 1, 2, \forall n,$

iv) $a_{k,n} \circ a_{k,v} = a_{k,v} \circ a_{k,n},\ k = 1, 2, 3,\ \forall n.$

Dem.: As demonstrações são imediatas. De fato, i) decorre da expansão da recursão de definição; ii) e iii) simplesmente por suas avaliações para cada x_j como a seguir

$$f_n(s_k(x_j)) = x_{n(k+j)} = x_{nk+nj} = s^n_k(f_n(x_j)),\ e$$
$$J_v(f_n(x_j)) = x_{(nj)^v} = x_{n^v j^v} = f^v_n(J_v(x_j))\ \forall j,$$

sendo iv) é implicado pela comutatividade dos índices em ii).

A propriedade "i"nos revela que as operações superioras definidas podem sempre ser interpretadas como iterações das funções de um andar inferior, assim como a multiplicação é uma iteração de somas, a potência uma iteração de multiplicações, etc. Neste sentido fica claro como a noção de iteração permeia a construção aritmética de todas as famílias, desde a definição da primeira família, até as superioras.

Como contraste comparativo a essa construção de A_1, A_2, A_3, ..., ofereceremos abaixo um caminho distinto para a investigação aritmética, o da consideração da estrutura iterativa A_1, $End(A_1, \circ)$, $End(End(A_1, \circ), \circ)$, ... De fato, um dos resultados meta-aritméticos abaixo é que $A_2 \cong End(A_1)$. Apesar disso, A_3 não é isomorfo a $End(End(A_1, \circ), \circ)$, mas a um pequeno subconjunto deste, o que já diferencia as duas estruturas.[6]

1.3 Monóides e inframonóides de composição de operações

Monóides são semelhantes a grupos, sem no entanto haver necessidade da existência de um elemento inverso.

[6] Esta diferenciação não leva em conta as leis de comutação entre somas e multiplicações, pois estamos lindando com monóides por andar de operações, não monóides mistos.

Definição 1.3.1 (Monóides) *Definimos monóide como um par* $(D, *)$*,*

i) sendo $* : D \times D \to D$*;*
ii) havendo $e \in D$ *tal que* $e * g = g,\ \forall g \in D$*;*
iii) valendo $(a * b) * c = a * (b * c),\ \forall a, b, c \in D$*, isto é, associatividade.*

Definição 1.3.2 (Inframonóides) *Definimos inframonóide como um par* $(D, *)$*,*

i) sendo $* : B \subset D \times D \to D$*;*
ii) havendo $e \in D$ *tal que* $e * g = g,\ \forall g \in D$*;*
iii) valendo $(a * b) * c = a * (b * c),\ \forall a, b, c \in D$*, isto é, associatividade.*

A única diferença entre monóides e inframonóides, tal como definidos acima, é que um inframonóide pode ter como domínio apenas um subconjunto dos pares que definem o cartesiano $D \times D$, e portanto a estrutura algébrica não é nem mesmo um magma.

Se a aritmética A é infinita, $(A_1, \circ)$ e $(A_2, \circ)$ são monóides. Se é finita, existem funções cuja composição não está definida para nenhum elemento (a menos como a função vazia), pois a imagem de uma função poder ter intersecção nula com o domínio da outra. Neste caso, a composição está definida apenas para um subconjunto do produto cartesiano mencionado, fato que justifica a definição dos inframonóides (assim há menor expressividade da álgebra composicional, nem todas as composições são válidas). Se admitirmos uma extensão aritmética nilpotente, a estrutura de composição volta a ser descrita por monóides, mas com divisores de zero, afinal as composições que geravam a função vazia, no caso finito, agora retorna o valor nulo - e portanto as composições não nulas correspondem exatamente às composições definidas no caso finito não estendido, que gera o inframonóide. Neste aspecto, o estudo da aritmética finita permanece totalmente compreendido pelo estudo da aritmética finita estendida nilpotentemente.

Compreendido isto, teremos justificativa para, mais abaixo, considerar a definição de homomorfismo limitado, que são os homomorfismos de inframonóide.

Por último, para aritméticas infinitas consideraremos a noção de **monóide topológico**, cuja operação composição é contínua com respeito à topologia empregada.

1.3.1 Monóides de somas

Trata-se de $(A_1, \circ)$, gerado por s. Todo elemento é da forma

$$s_k = s^k = \bigcirc_{n=1}^{k}(s).$$

Respeita $s_k \circ s_j = s_{k+j},\ \forall k, j$.

1.3.2 Monóides de multiplicações

Trata-se de $(A_2, \circ)$, gerado por $P_2 = \{f_p\}$ algebricamente independentes, onde p é primo menor ou igual a N. Este fato é equivalente ao teorema fundamental da aritmética.

Fatoração em multiplicações primas

A fatoração prima de n é reproduzida fielmente na fatoração das f_n:

$$f_n = \bigcirc_{p_i,k_i:n=p_1^{k_1}p_2^{k_2}\ldots}(f_{p_1^{k_1}}f_{p_2^{k_2}}\cdots) \tag{1.1}$$

1.3.3 Monóides mistos

Neste caso, considera-se o monóide simultaneamente gerado por s e pelas f_p, levando em consideração a propriedade $s_p f_p = f_p s$, que é essencialmente a propriedade distributiva. No caso aritmético finito, o monóide permanece finito. No entanto, não é comutativo. b

O monóide misto é um conceito importante, porque conecta a teoria aditiva com a multiplicativa através de equações de carácter algébrico.

1.4 Homomorfismos de monóides aritméticos

Como uma aritmética determina várias operações aritméticas diferentes, há várias maneiras de se definir homomorfismos entre operações. Uma alternativa é construir relações entre os conjuntos U e W sobre os quais agem as operações aritméticas, para destas relações estabelecer ligações entre as operações. Outra forma é definir abstratamente os homomorfismos entre operações.

Dados dois conjuntos bem ordenados U e V e as duas aritméticas infinitas $L = (x, s)$ e $J = (y, d),\ x \in U, y \in W$ induzidas, podemos considerar a bijeção $b : U \to V$ tal que $b(x_n) = y_n$. Nota-se como $b(s_n(x)) = b(x_{n+1}) = y_{n+1} = d_n(y) = d_n(b(x))$. Também vale $b(f_n(x_k)) = b(x_{nk}) = y_{nk} = g_n(y_k) = g_n(b(x_k))$. O padrão se generaliza.

Teorema 1.4.1 *Sejam L, J, b como no parágrafo anterior. Para cada par de operações $(l_{k,n},\ j_{k,n})$, de L e J, vale $b \circ l_{k,n} = j_{k,n} \circ b$.*

Demonstração 1.4.1 *Suponhamos que o teorema seja válido para todo o k-ésimo andar de operações.*

Aplicando o item i da afirmação 1.2.1 para as aritméticas J e L e operando com b, obtemos $b \circ l_{k+1,n+1}(x_i) = b \circ l^n_{k,i}(x_i) = j^n_{k,i} \circ b(x_i) = j_{k+1,n+1} \circ b(x_i),\ \forall n, i, k$ pela hipótese de indução.

Como vimos, o teorema vale para os primeiros e segundos andares de operações de J e L. Portanto a afirmação vale para todos os andares de operações iterativas.

Definição 1.4.1 (Homomorfismos aritméticos) *Seja A uma aritmética infinita. Definimos como homomorfismo aritmético um homomorfismo de monóides cujo domínio é um monóide $(A_k,\ \circ)$ de k-ésimas operações A_k, isto é, uma função tal que $h(Id_{A_k}) = Id_{Im(h)}$ e $h(l_n \circ l_k) = h(l_n) \cdot h(l_k),\ \forall l_n,\ l_k \in A_k$. Os homomorfismos aritméticos definidos sobre A_1 e A_2 são chamados respectivamente de aditivos e multiplicativos.*

Adaptando os conceitos clássicos da literatura, definimos endomorfismo aritmético como um homomorfismo aritmético cujo contradomínio é igual ao domínio, e automorfismo como um endomorfismo bijetivo, monomorfismo como um homomorfismo injetivo, etc.

Teorema 1.4.2 *Sejam $L,\ J$ duas aritméticas infinitas. Então os monóides de operações iterativas de L e J são isomorfos, a cada andar.*

Demonstração 1.4.2 *O teorema 1.4.1 fornece diretamente as representações $j_{k,n} = b \circ l_{k,n} \circ b^{-1}$ e $l_{k,n} = b^{-1} \circ j_{k,n} \circ b$. Nos resta simplesmente provar que a conexão é um isomorfismo.*

Isso nos leva a definir a função $w : \cup_i(L_i, \circ) \to \cup_i(J_i, \circ)$ tal que $w(l_{k,n}) = b \circ l_{k,n} \circ b^{-1}$.

Como $w(l_{k,n}) \circ w(l_{k,i}) = b \circ l_{k,n} \circ b^{-1} \circ b \circ l_{k,i} \circ b^{-1} = b \circ l_{k,n} \circ l_{k,i} \circ b^{-1} = w(l_{k,n} \circ l_{k,i})$, a restrição de w a cada enésimo monóide de operações iterativas de J é um homomorfismo aritmético com a imagem no enésimo monóide de operações iterativas de L. Como b é uma bijeção, w é claramente bijeção, com inversa $w^{-1} : \cup_i(J_i, \circ) \to \cup_i(L_i, \circ)$ tal que $w^{-1}(j_{n,k}) = b^{-1} \circ j_{k,n} \circ b$, que é homomorfismo aritmético do enésimo monoide de L para o enésimo monóide de J. Então as ditas restrições de w são isomorfismos aritméticos para cada andar de operação.

Afirmação 1.4.1 *Nas mesmas condições do teorema anterior, a menos da condição de A ser aritmética finita nilpotentemente (ou circularmente), vale o teorema. Isto é, todos os monóides de operação de operação são isomorfos.*

Poderíamos nos questionar se é possível haver homomorfismos entre aritméticas diferentes, por exemplo, em sua ordem. No entanto, as condições algébricas que estipulamos nas extensões são muito fortes. Para tanto, é possível, sim, considerar homomorfismos de uma aritmética finita para a enumerável, por exemplo, no sentido de homomorfismos limitados, que recuperam os homomorfismos de inframonóide.

Os endomorfismos e de $(A_1, \circ)$ são enumerados por k como $e_k(s) = s_k$, que determina $e_k(s_n) = s_{nk}, \forall n$. O único automorfismo deste monóide é a identidade.

Como $(A_2,\ \circ)$ é gerado por $(P_2,\ \circ)$, cada endomorfismo do primeiro monóide é determinado por $\pi(N)$ equações $e(f_p) = f_n$, para algum n. Estas equações determinam $e(f_n),\ \forall n$, por conta da decomposição prima (1.1).

Teorema 1.4.3 *h é automorfismo de $(A_2,\ \circ)$ infinito se, e somente se, h induz uma bijeção à restrição $h|_{P_2} : P_2 \to P_2$, isto é, h permuta multiplicações primas.*

Demonstração 1.4.3 *De fato, se h é automorfismo de $(A_2, \circ)$, é um homomorfismo bijetivo $h : (A_2, \circ) \to (A_2, \circ)$, determinado por contáveis equações $h(f_p) = f_n$ em decorrência de (1.1). Como $h(f_1) = f_1$, a injetividade não permite que outras avaliações retornem a identidade f_1. Além disso, qualquer restrição de h permanece injetiva.*

Se houvesse f_q, q primo, tal que não há p tal que $h(f_p) = f_q$, também não haveria $n = a \cdot b$, $a, b \geq 2$, tal que $h(f_n) = h(f_a) \circ h(f_b) = f_q$, pois q é primo, e h não seria sobrejetiva. Portanto $P_2 \subset Im(h|_{P_2})$.

Se $h(f_p) = f_n = f_{a\cdot b}$, valeria $f_p = h^{-1}(f_a) \circ h^{-1}(f_b)$, o que contrariaria p ser primo. Portanto $Im(h|_{P_2}) \subset P_2$.

A conclusão é que $Im(h|_{P_2}) = P_2$, e $h|_{P_2} : P_2 \to P_2$ é uma bijeção.

Por outro lado, se há uma bijeção $g = h|_{P_2} : P_2 \to P_2$, é possível definir, por meio de (1.1), um $h : A_2 \to A_2$ tal que $h(f_n) = \bigcirc_i g^{k_i}(f_{p_i})$. Este h é endomorfismo de A_2 por definição. Como g é bijeção, é invertível, e podemos definir o endomorfismo d de A_2 $d(f_n) = \bigcirc_i g^{-k_i}(f_{p_i})$. Com estas definições, fica evidente que $d = h^{-1}$, e h é automorfismo.

1.4.1 Homomorfismos limitados

Para a linguagem dos monóides operacionais nilpotentes recuperar os análogos a homomorfismos do caso finito não estendido, aplica-se a condição distributiva de homomorfismo apenas quando tanto a composição de pares de operações do domínio quanto a do contradomínio sejam não nulas. No entanto, prefiro fazer a seguinte definição.

Definição 1.4.2 (Homomorfismo limitado) *Defino como **homomorfismo limitado** $h \in Hom_{\lim}(A_k)$ de um monóide de operações nilpotente como $h : A_k \to D \cup \{0\}$, sem a função nula no domínio, sendo D algum monóide.*

Uma importante pergunta torna-se se a imagem dos endomorfismos limitados gera, por composições, todo o monóide operacional. Neste caso, **estes homomorfismos se correspondem exatamente aos automorfismos do caso infinito** que averiguamos acima. Em outras palavras, permutam primos. Assim, sua quantidade é aritmeticamente relevante:

Afirmação 1.4.2 *Seja A aritmética finita de ordem N. Então*

$$|End^*_{\lim}(A_2, \circ)| = \pi(N)!,$$

sendo $End^*_{\lim}$ o conjunto dos endomorfismos limitados cuja imagem ainda gera A_2.

Demonstração 1.4.4 *Basta considerar o argumento do teorema 1.4.3 aplicado ao inframonóide $(A_2, \circ)$, afinal este é gerado pelas multiplicações primas menores ou iguais a N, conforme visto em (1.1), que portanto devem obrigatoriamente ser imagem do endomorfismo. São portanto $\pi(N)$ multiplicações aritméticas, e o número de permutações $\pi(N)!$ pelo princípio fundamental da contagem.*

Por argumentos semelhantes, se mostra que $|End_{lim}(A_1)| = ord(A) = N$ e $|End_{lim}(A_2)| = N^{\pi(N)}$, de maneira geral. Para os endomorfismos limitados decrescentes h cuja imagem leva gerador em gerador de A_2 de índice menor, vale

$$|End^{>}_{lim}(A_2)| = \#N,$$

sendo # o primorial.

Não podemos aqui utilizar a noção de automorfismo para o caso finito como usamos para o infinito sem requerer uma definição muito intricada da variação dos domínios e imagens. Diferentemente do caso infinito, estes monomorfismos permutadores de primos não são sobrejetores, ainda que atinjam todos os primos, pois nem toda composição entre elementos do inframonóide está bem definida (Ex.: Se N=10, $f_2 \circ f_7 \equiv 0$, e o homomorfismo h tal que $h(f_2) = f_2$, $h(f_7) = 3$) não atinge f_6, pois existir k tal que $h(f_k) = f_6 = f_2 \circ f_3 = h(f_2) \circ h(f_7) = h(f_2 \circ f_7) = h(0)$, sendo no entanto $0 \notin Dom(h)$).

Uma sucessão de aritméticas de ordem crescente determina uma sucessão destes homomorfismos que aproxima de forma simples os homomorfismos do caso infinito, e todas suas identidades. Isso foi tornado rigoroso pela Lei da Correspondência (3.1.2).

Afirmação 1.4.3 *Estes endomorfismos limitados se extendem unicamente linearmente para os endomorfismos das álgebras de operações nilpotentes.*

De maneira semelhante, pode-se estudar o comportamento dos endomorfismos limitados com respeito a outras extensões (x, s, a) de (x, s).

1.5 Operações aritméticas endomórficas

Trata-se de uma maneira diferente de se interpretar a aritmética. Por esta noção, parte-se do monóide de somas $H_1 = A_1$, como no caso iterativo, mas se define a família de operações seguinte H_{k+1} a partir dos endomorfismos da anterior $End(H_k)$ (no caso finito nilpotente, limitados), tal como $H_k = End^{k-1}(A_1)$.

Cada H_k é monóide $(H_k, \circ)$ e opera indiretamente sobre os monóides iterativos. Por exemplo, conforme provaremos na seção meta-aritmética, vale

$$A_2 \cong H_2,$$

mas o mesmo já não vale para a terceira operação.

$$A_3 \cong C \subsetneq H_3.$$

1.6 A transformada fundamental. Operações aritméticas duais.

Para uma aritmética infinita, podemos considerar os homomorfismos aritméticos h das $a_{k,n}$ a $(\mathbb{C}, \cdot)$ e assim definir $T : (A_k, \circ) \to C(\sigma((A_k, \circ)))$ tal que $T(a_{k,n}) = \hat{a}_{k,n}$, a operação aritmética dual sobre $\sigma(A_k)$, sendo

$$\hat{a}_{k,n}(h) = h(a_{k,n}).$$

No capítulo 3 construiremos $\mathbb{C}$-álgebras a partir destes monóides. As álgebras $(A_k, +, \circ)$, construídas linearmente das A_k, tem como homomorfismos de álgebras aritméticas de imagem complexa exatamente as extensões lineares dos homomorfismos dos monóides aritméticos. Neste sentido, vale o seguinte resultado:

Afirmação 1.6.1 *Seja A aritmética infinita. Então a transformada fundamental $T : (A_k, \circ) \to C(\sigma((A_k, \circ)))$ se estende unicamente linearmente para a transformada de Gelfand $\Gamma : (A_k, +, \circ) \to C(\sigma((A_k, +, \circ)))$*

Propriedades importantíssimas são conferidas pelo estudo dos homomorfismos e elementos duais de álgebras, e portanto o mesmo estudo para os monóides também deve garantir importantes informações estruturais. Não desenvolvemos, no entanto, essa teoria.

1.7 Meta-aritméticas

Esta seção se refere a um estudo à parte e incipiente sobre a simetria das próprias operações quando aritmeticamente consideradas sobre si mesmas, ou melhor, de aritméticas determinadas sobre operações em ordem de outras aritméticas, arbitrariamente.

Definição 1.7.1 *Dada uma aritmética A, chamamos de meta-aritmética uma aritmética $B = (x, s)$ cujo conjunto U totalmente ordenado que a define é ele próprio a família A_k de operações de k-ésimo nível de A. Nesse caso, chamamos k de seu nível.*

A família A_2 respeita uma forma multiplicativa em suas composições, isto é, $f_n \circ f_k = f_{nk},\ \forall n, k$, e vale a relação de comutação $f_n \circ s_k = s_{nk} f_n$, fato que reflete a distributividade usual da multiplicação sobre a soma. Isso revela que a definição das f_n está relacionada às simetrias das operações s_n.

Se consideramos os endomorfismos aritméticos $h : A_1 \to A_1$ tais que $h(s_n \circ s_k) = h(s_n) \circ h(s_k)$, observamos que $h(s_n) = h(s)^n,\ \forall n$,e que A_1 tem seus endomorfismos h determinados pelas respectivas imagens $h(s)$. Tratando explicitamente do caso $h_k(s) = s^k$, para algum k, fica claro que $h_k(s_n) = s^{nk}$, e que portanto a imagem de h_k é $\{Id,\ s^k,\ s^{2k},\ \cdots\}$.

Com isto, a lei de comutação descrita pouco acima é reescrita como $f_n \circ s_k = h_n(s_k) \circ f_n$. A conexão entre a noção de multiplicação aritmética e de endomorfismos das somas aritméticas é ainda mais íntima. De fato, ao considerarmos a aritmética (x, s), podemos considerar a aritmética induzida (Id_{A_1}, ψ) sobre o conjunto ordenado A_1. Neste caso, $\psi^n(Id) = s^n$. Para esta aritmética, as multiplicações tomam a forma $\varphi_n(s_k) = s^{n(k+1)-1}$, e portanto a lei de comutação toma a forma $\psi(\varphi_n(s_k)) = s \circ \varphi_n(s_k) = s^{n(k+1)} = h_n(s_k \circ s) = h_n(\psi(s_k))$. Assim $\psi \circ \varphi_n = h_n \circ \psi$. Esta lei estabelece um isomorfismo entre B_2 e $End(A_1, \circ)$, pois ψ é injetiva.

Afirmação 1.7.1 *Se $A = (x, s)$ é uma aritmética com família de somas A_1 e $B = (Id_{A_1}, \psi)$ é a aritmética construída sobre A_1, então as multiplicações φ_n de B_2 são isomorfas*[7] *aos endomorfismos $h \in End(A_1)$ sobre as s^kde A_1, ou seja, $B_2 \cong End(A_1)$.*

Corolário 1.7.1 *É válido o isomorfismo*

$$End(A_1) \cong A_2.$$

para aritméticas finitas e infinitas.

Demonstração 1.7.1 *Pelo teorema de isomorfismo entre aritméticas 1.4.1, vale $A_2 \cong B_2$; em conjunto com a afirmação anterior, vale o isomorfismo.*

No caso finito nilpotente, é os resultados são válidos para os endomorfismos limitados.

A aritmética $B = (s, \psi)$ é o primeiro exemplo de uma meta-aritmética de primeiro nível, a que $\psi : L(U) \to L(U) = (\psi(f) = s \circ f)$. Sua família de somas $B_1 = (\psi^k)$ é, exatamente $\psi^k(f) = s^k \circ f$, composições da função sucessora de A.

Algo semelhante ocorre para as segundas operações de uma meta aritmética de segundo nível, que operam em A_2 como $\varphi^k(f) = f_k \circ f$. Por conta disso, podemos nos perguntar se $End(A)_2$ seria isomorfo a A_3. Esse não é o caso.

[7] Na verdade, se houvéssemos considerado a aritmética (s, ψ), teríamos obtido algo mais forte, que $B_2 = End(A_1, \circ)$, uma igualdade de elementos. Optamos pela relação mais complicada, partindo-se de Id, apenas para que no caso finito a meta-aritmética de primeiro nível tenha a mesma ordem aritmética da aritmética que a gerou. A partir de s, obteríamos uma aritmética cuja ordem é uma unidade inferior.

Afirmação 1.7.2 *A_3 é isomorfo a um subconjunto de $End(A_2)$.*

Dem.: Basta notar que todo J_k é tal que $J_k(x_n) = x_{n^k}$, $\forall n$, em isomorfismo com os endomorfismos $e_k(f_n) = f_n^k$. Basta agora notar que $End(A_2)$ contem muitos outros endomorfismos, livremente determinados pela imagem das multiplicações primas.

1.7.1 Representações aritméticas por meio da avaliação gerativa

O reflexo da existência das relações aritmético-algébricas sobre o espaço específico sobre o qual age é dado, principalmente, pela avaliação das operações aritméticas no gerador x. Conforme vimos, a avaliação gerativa dos monóides de soma e multiplicação geram recursivamente U.

Afirmação 1.7.3 *A noção de avaliação gerativa mantém a propriedade de gerar unicamente a todo V para as combinações de operações aritméticas linearmente estendidas de A_1 ou A_2, que definiremos no próximo capítulo.*

Para compreender a importância desta avaliação, confira sua aplicação para inversões particulares em 3.4.

1.8 Extensões de U. Operações iterativas inversas. Monóides estendidos.

Esta pequena seção serve para atentar o leitor que todo o processo de criação dos números negativos, racionais, algébricos, reais, complexos, etc, pode ser totalmente transportada para a Aritmética Formal!

Não nos ateremos neste livro a desenvolver este aspecto da teoria, mas é importante reconhecê-lo.

1.8.1 Comentários sobre integralização. Fracionalização. Algebraização. Completamento.

A integralização se refere à investigação da função sucessora inversa s^{-1}, quando bem definida[8] em uma extensão $\mathrm{U}_{\mathbb{Z}}$ de U, e das subseqüentes $s^{-n}, n \in \mathbb{N}_1$, integrando as operações de soma.

No caso enumerável, $(A_1, \circ)$ adquire estrutura de grupo, com $s_n \circ s_{n-1} = Id$. Seus endomorfismos permanecem isomorfos ao monóide $(A_2, \circ)$ (cujos operadores tem seus domínios alargados para os novos elementos de U) estendido para abarcar os operadores

[8] Não confundir com contra-sucessão, conceito semelhante

$f_0,\ f_{-n}$, manipulando a definição de A_2 para escrever $f_{n-1}(x_j) = s^{-j} f_n(x_j), \forall n, j \in \mathbb{Z}$, de onde se conclui que $f_0(x_j) = 0,\ f_{-1}(x_j) = x_{-j},\ \forall j$, etc. De fato, f_{-1} comporta-se como uma involução.

As considerações espaciais do próximo capítulo nos levam a algumas considerações. A sucessão s passa a adquirir pontos fixos no caso infinito, quando as coordenadas de um vetor v são iguais todas iguais a c. Com respeito às álgebras de operações, isso leva à existência de um elemento $a = c\sum_{n\in\mathbb{Z}} s_n \in S_A$ que espelhe o vetor tal que $s \circ a = a$, ou seja, $(s - s_0) \circ a \equiv 0$, o que nunca ocorria na aritmética original. No entanto $a(x_j) = \sum_{n\in\mathbb{Z}} x_n,\ \forall j$. Isso significa que a não pode agir sobre todos os elementos do espaço, pois sua avaliação qualquer rende o vetor v multiplicado pela soma dos coeficientes a^2 não está definido. Esse fato alude à famosa fórmula errônea de Euler, $\cdots + x^{-1} + 1 + x + \cdots = 0$. Isso exige uma limitação maior sobre os coeficientes admitidos, como por exemplo, a somabilidade absoluta dos coeficientes.

De maneiras análogas, se pode definir a fracionalização através da admissão de elementos em U que permitam a existência de operações inversas às multiplicações aritméticas f_n. Com racionalização, diz-se uma integralização e fracionalização simultâneas.

Com algebraização, quer-se dizer a extensão de U que nos permita definir as operações inversas das potências aritméticas J_n.

Pode-se perguntar que extensões são necessárias para garantir as inversas das hiperoperações inferioras seguintes.

Por fim, o completamento aritmético é possível para aritméticas racionais e algébricas, gerando as reais e complexas. O fato mais notório desta teoria real é que a existência de uma inversa de operação de potência garante a existência de todas as outras (pois uma única raiz de unidade com componente imaginária não nula já é linearmente independente da reta real, e com a unidade gera o plano complexo).

2 Espaços aritméticos

2.1 Definição e exemplos

Neste capítulo nos ateremos a aritméticas sobre elementos de K-espaços vetoriais V ou mesmo R-módulos M.

Em geral, estaremos interessados nas conseqüências da extensão linear da função sucessora e das subseqüentes operações aritméticas definidas sobre estes elementos, sendo de especial importância o caso em que estes compõe uma base do espaço vetorial ou R-módulo livre considerado.

Definição 2.1.1 (Espaços aritméticos) *Chamamos **espaço aritmético** de ordem N qualquer aritmética definida sobre N elementos ordenados $x_1, \cdots, x_N$ de um R-módulo M à escolha. A menos que declarado o contrário, consideraremos que podemos gerar M como $M = [x_n]_{n=1,2,...}$*

É estendido, circular, nilpotente, etc., exatamente quando a aritmética o for. Se nilpotente, convenientemente determinamos que 0 é 0 do R-módulo, e que $a \in M$ em geral.

Exemplo 2.1.1 *Considere o espaço aritmético infinito $Q = (v, +v)$, sendo v vetor e $+v : U \to U(+v(u) = u + v, \forall u \in U)$, operação restrita de V a U. Temos que $U = \{v, 2v, 3v, \cdots\}$, e $+v(nv) = (n+1)v$. Na notação das famílias de operações, as operações de Q_1 são exatamente as $(+v)^k(u) = u + k \cdot v, k \in \mathbb{N}_0$, e as de Q_2 as multiplicações por escalar $(n\cdot) : U \to U((n\cdot)(u) = n \cdot u)$, curiosamente lineares em $[v]$.*

Neste caso a função sucessora não se estende linearmente em $[v]$, afinal isso implicaria no mínimo que $3v = 2v + v = (+v)(2v) = (+v)(v + v) = (+v)(v) + (+v)(v) = 4v$ e forçosamente $v = 0$, mas as funções multiplicativas se estendem. É um dos únicos casos onde a soma aritmética coincide com a soma vetorial.

Se os vetores são considerados como funções em variáveis independentes, as operações aritméticas podem também depender destas variáveis. O casos serão melhor analisados em um seção própria.

Exemplo 2.1.2 (Espaços aritméticos de senoides) *Seja $A = (\sin(t), s_t)$ espaço aritmético infinito sobre $\{\sin(t), \sin(2t), \cdots\}$, $s_t(\sin(nt)) = \sin((n+1)t)$. Neste caso as multiplicações f_n da aritmética comportam-se como composições à direita com a função multiplicação usual por n, $f_n(p(t)) = p(nt)$. Se $t \in \mathbb{N}$, $x_n(t) = x_t(n)$.*

Alguns espaços de funções reais ou complexas são tais que a adição e multiplicação aritméticas tomam a forma da multiplicação usual entre os membros do conjunto ordenado

sobre o qual a aritmética está estabelecida. A seguir estão os exemplos concretos, as séries de potências e as séries de Dirichlet. Os casos serão mais profundamente estudados mais adiante, na página 61.

Exemplo 2.1.3 (Espaços aritméticos de potências naturais) *Seja $A = (t, s_t)$ espaço aritmético infinito sobre $\{t, t^2, \cdots\}$, $t : \mathbb{R} \to \mathbb{R}$ ou $\mathbb{C}$, e onde $s_t = t\cdot$, e $s_t(t^n) = t^{n+1}$. A cada $p(t) \in [t, t^2, \cdots]$, temos para A_1 que $s^k(p(t)) = t^k \cdot p(t)$, e que $f_n(p(t)) = p(t^n) = (p\circ()^n)(t)$ para A_2, ou seja, as multiplicações da aritmética comportam-se como composições laterais à direita com as funções de potência natural. A operação produto " $\cdot$"respeita a distributividade usual com respeito à soma do espaço, e a extensão linear lhe é natural.*

Exemplo 2.1.4 (Espaços Aritméticos de exponenciais de naturais) *Seja $A = (1, s_t)$ espaço aritmético infinito sobre $\{1, 2^{-t}, 3^{-t}, \cdots n^{-t}, \cdots\}$, $t \in \mathbb{R}$. Então $s_t(y) = (y^{-1/t} + 1)^{-t}$. Neste caso as funções compõe uma base linearmente independente e é possível estender s_t linearmente para todo o espaço gerado formalmente; no entanto, isso não preserva a forma radical que acabamos de enunciar, restrita apenas aos elementos de U. s_t é uma função meromórfica em t tal que $\sum_{n=0}^{\infty} s_t^n(1) = \zeta(t)$, a função Zeta de Riemann. Neste caso, as multiplicações da aritmética são as funções f_n tais que $f_{n,t}(y) = n^{-t} \cdot y$, a multiplicação usual pelo n-ésimo elemento da base. A extensão dessa operação para todo o espaço V das séries de Dirichlet é natural, devido à distributividade da multiplicação usual com respeito à adição do espaço.*

É claro que $\dim([x_1, \cdots, x_N]) \leq N$, e que a igualdade vale se U é base ordenada de V, no caso de módulos livres.

2.2 Espaço das operações aritméticas iterativas

Sabemos que qualquer R-módulo M nos permite considerar o conjunto $\mathrm{Hom}(M, M)$ de seus endomorfismos h também como R-módulo, cuja adição é herdada de M pela lei $(h_1 +_{Hom} h_2)(m) = h_1(m) +_M h_2(m)$.

Definição 2.2.1 *Chamamos de **espaço das operações aritméticas finitas** $E(A)$ o subconjunto do R-módulo $Hom(M, M)$ gerado pelas operações aritméticas[1] de $O = A_1 \cup A_2 \cup A_3$. Em outras palavras, seus elementos são precisamente da forma*

$$\sum_{i=1}^{k} a_i O_i,$$

sendo $k \in \mathbb{N}_1$, $a_i \in R$ e $O_i \in O$, $\forall i$.

[1] Eliminamos os casos A_k, $k \geq 4$ apenas por não lhes ver utilidade atualmente.

Não há uma relação geral direta entre a soma vetorial aqui expressa e a soma aritmética definida anteriormente. Apenas em alguns casos, a relação pode ser estabelecida, como no exemplo 2.1.1, sem no entanto a soma aritmética poder ser linearmente estendida sobre todo V. Isso não foi um impedimento para a linearidade das multiplicações aritméticas.

2.3 Aritméticas sobre bases ordenadas

O caso em que os $x_1, \cdots x_N$ elementos ordenados de M compõe uma base deste são de especial interesse pelas simplificações dos cálculos das simetrias de M.

Neste caso todo elemento de M têm única representação em termos dos dados elementos ordenados, dependente de N variáveis independentes do anel R, e podemos sem dificuldade o representar em um sistema de coordenadas canônicas, além de realizar boa parte da teoria homomórfica através de matrizes canônicas com entradas no anel R.

A partir daqui, quando declararmos um espaço aritmético, será sobre uma base, a menos que explicitamente dito o contrário.

2.3.1 Extensão linear das operações aritméticas

Neste caso as operações aritméticas $a_{k,n} : U = \{x_1, \cdots x_N\} \to U \cup \{0\}$ podem ser linearmente (homomorficamente) estendidas de maneira única para transformações $a_{k,n} : M = [x_1, \cdots x_n] \to M$, que são consideradas daqui em diante.

Estes endomorfismos de M podem ser canonicamente identificados com matrizes de entradas em R, o que nos dá um exemplo mais palpável da teoria que desenvolveremos.

2.3.2 Representações matriciais canônicas

As representações canônicas são decorrentes da declaração que $x_1 = (1, 0, \cdots, 0)$; $\cdots$; $x_N = (0, 0, \cdots, 1)$.

Caso nilpotente

No caso de uma aritmética finita nilpotente, s é identificada como a matriz NxN

$$s = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

que tem elementos

$$a_{i,j} = \begin{cases} 1, \text{ se } i = j + 1; \\ 0, \text{ noutros casos.} \end{cases}$$

Em geral, as somas aritméticas s^k tem elementos que respeitam

$$a_{i,j} = \begin{cases} 1, \text{ se } i = j + k; \\ 0, \text{ noutros casos,} \end{cases}$$

e passam a ser representadas como

$$s^2 = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

$$s^3 = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

etc.

As matrizes referentes às multiplicações f_n têm elementos determinados por

$$a_{i,j} = \begin{cases} 1, \text{ se } i = n \cdot j; \\ 0, \text{ noutros casos.} \end{cases}$$

Por exemplo, f_2 tem a forma

$$f_2 = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

As matrizes das potências J_v, por sua vez têm elementos determinados por

$$a_{i,j} = \begin{cases} 1, \text{ se } i = j^v; \\ 0, \text{ noutros casos.} \end{cases}$$

Caso circular

No caso de uma aritmética finita circular, s é identificada como a matriz NxN

$$s = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

que tem elementos

$$a_{i,j} = \begin{cases} 1, \text{ se } i \equiv j + 1 \mod N; \\ 0, \text{ noutros casos.} \end{cases}$$

De fato para a matriz sucessora só há diferença no resultado da última coordenada, em relação ao caso nilpotente.

Em geral, as somas aritméticas s^k tem elementos que respeitam

$$a_{i,j} = \begin{cases} 1, \text{ se } i \equiv j + k \mod N; \\ 0, \text{ noutros casos,} \end{cases}$$

e passam a ser representadas como

$$s^2 = \begin{pmatrix} 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

$$s^3 = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

etc.

As matrizes referentes das multiplicações f_n têm elementos determinados por

$$a_{i,j} = \begin{cases} 1, \text{ se } i \equiv n \cdot j \mod N; \\ 0, \text{ noutros casos,} \end{cases}$$

e a das potências J_v,

$$a_{i,j} = \begin{cases} 1, \text{ se } i \equiv j^v \mod N; \\ 0, \text{ noutros casos.} \end{cases}$$

2.3.3 Elementos aritmeticamente geradores do espaço de origem

Dada uma aritmética (x, s) ou $(x, s, 0)$, sabemos que as recursões de s no gerador x geram todos os elementos do conjunto totalmente ordenado U que a determina.

Quando consideramos um espaço aritmético sobre uma base, isto é o mesmo que dizer que as iterações de s sobre x geram a base U de M. No entanto, o gerador x não é o único com a propriedade de gerar uma base por meio de aplicações sucessivas de s. Isso nos estimula à seguinte definição:

Definição 2.3.1 *Seja $(x, s, 0)$ espaço aritmético nilpotente de ordem N sobre os elementos de uma base de um R-módulo M. Então $m \in M$ é **gerador aritmético de M por A** se, e só se, $m, s(m), \cdots, s^{N-1}(m)$ é base de M.*

No caso de uma aritmética (x, s) infinita, os $s^k(m)$, $k = 0,\ 1,\ 2,\ \cdots$ devem ser uma base de M.

Afirmação 2.3.1 *Dado um espaço aritmético (x, s) ou $(x, s, 0)$ sobre uma base e um elemento m de M cuja representação gerada por x é*

$$m = \sum_{n=1}^{N} a_n x_n,$$

então m é gerador se, e somente se, a_1 é invertível em R.

Demonstração 2.3.1 *Notemos que a projeção de $s^n(m)$ em x é 0, $\forall n > 1$, e portanto combinações destes elementos certamente não geram x. Assim uma combinação linear que o gere depende do elemento m. Se a projeção $Proj_x^m$ m em x é a_1 não invertível, não há $r \in R$ tal que $Proj_x^{rm} = 1$, e não resta maneira possível de combinar os m_n restantes que resulte em x (apenas em a_1x).*

A volta da equivalência será apresentada no teorema de inversão aditiva, na página 74.

Espaços aritméticos cuja função sucessora (considerada sobre M) é a mesma também compartilham das demais operações aritméticas. Isso nos permite considerar uma relação de equivalência entre as bases ordenadas $B \in \mathbb{B}$ de M que definem as mesmas operações aritméticas sobre M: $B_1 \sim B_2 \iff s_1 = s_2$, sendo s_i as funções sucessoras induzidas sobre B_i. Conforme veremos nas inversões do próximo capítulo, duas bases estão relacionadas se, e somente se, são imagens de automorfismos lineares aritméticos uma da outra.

Como exemplo da importância desta relação de equivalência, tomemos o exemplo das senóides. O espaço gerado pelas $\sin(nx)$ pode ser descrito por diversas outras bases, todas com a simetria multiplicativa natural. A relação de equivalência captura essa condição comum, e nos permite falar nas simetrias multiplicativas naturais de todas as funções periódicas ímpares, que geram o mesmo espaço, através da avaliação gerativa da mesma aritmética.

2.4 Espaços aritméticos de funções

Constitui um estudo importante que não desenvolveremos. De imediato, temos três casos a destacar:

i)As aritméticas da forma (x_t, s_t), onde o gerador e a função sucessora dependem de uma variável independente t;

ii) as da forma (x, s_t), onde somente a função sucessora é dependente de t, e

iii) as da forma (x_t, s), onde somente o gerador depende da variável t.

As aritméticas de funções que aqui veremos serão da forma i) e ii).

É certamente possível descrever uma teoria topológica e diferencial a partir da dependência nesta variável. Além disso, a variável induz uma dependência nas operações. É sem dúvida importante desenvolver os fundamentos deste estudo no caso infinito, para

que possamos compreender os fenômenos de convergência ligados à avaliação dos vetores pelas operações aritméticas.

3 Álgebra das operações aritméticas

3.1 Definição. Homomorfismos. Lei da correspondência. Tema convolutivo.

Definição 3.1.1 (Álgebra das operações aritméticas) *Definimos a álgebra das operações aritméticas $Alg(A)$ como o conjunto gerado pelas operações aritméticas*[1] $O = \cup_{n=1}^{3} A_n$, *munido com as operações $+, \circ$, sendo a segunda operação a composição de funções.*

Em particular, $E(A) \subset Alg(A)$, afinal há expressões mistas de A_k em $Alg(A)$. Nos exemplos que veremos, nos restringiremos a subálgebra de cada operação por vez, que é comutativa, se R é comutativo. A de somas, chamaremos S_A. A de multiplicações, F_A. Em geral serão enumeráveis ou nilpotentes. quando necessário, diferenciaremos entre $S_{nil}(a)$ e $S_\circ(A)$.

Se o espaço aritmético é circular ou nilpotente e o anel R é finito, $Alg(A)$ é finita.

3.1.1 Descrição estrutural

Transportam-se os geradores dos monóides de operações aritméticas para a suas álgebras. No caso nilpotente de ordem N, a R-álgebra das operações aritméticas iterativas nilpotentes (até o terceiro andar) é da forma

$$\frac{R[s,\ f_2, \cdots, f_p, J_2, \cdots, J_q]}{(s^N)(f_p \circ s - s^p \circ f_p)(J_{p_1} \circ f_{p_2} - f_{p_2}^{p_1} \circ J_{p_1})}$$

sendo $p \leq N$ primo e $q \leq \log_2 N$ primo.

Apesar de a seguir considerarmos uma operação por vez a fim de simplificar certas investigações, a descrição das subálgebras por operação exige declarações adicionais às dadas em $Alg(A)$. No caso acima, o quociente pelo ideal (s^N) já anula, por exemplo, as multiplicações aritméticas acima de N. Isso decorre da existência das equações de vínculo; sem estas equações, estas anulações devem ser independentemente declaradas, como no caso da álgebra F_A das operações aritméticas nilpotentes de ordem N, que têm de ser quocientada pelos ideais $(f_a \circ f_b)$ tais que $a \cdot b > N$, os mesmos que não são considerados pelos homomorfismos limitados.

[1] Pela mesmas razões práticas, omitimos da álgebra as operações superioras à potenciação.

3.1.2 O tema convolutivo dos coeficientes de composições. Fórmulas primitivas. Informações aritméticas clássicas codificadas no produto interno.

Em qualquer álgebra de operações a composição de elementos resulta em um novo elemento cujos coeficientes são convoluções dos coeficientes anteriores. Estas álgebras, portanto, tem sua existência intimamente ligada com a teoria das convoluções lineares aditivas e multiplicativas de seqüências, adaptada para seus coeficientes.

O conhecimento independente de um produto interno em V=[U] induz gerativamente o produto interno sobre S_A ou F_A, segundo o qual podemos representar os coeficientes. Isso liga **fórmulas numéricas elementares** geradas convolutivamente a **expressões angulares**, através das **estruturas espaciais e algébricas**, como no exemplo a seguir.

Afirmação 3.1.1 *O Teorema dos Números Primos é equivalente a* $\cos(Z, Z^{-1}) \to 0$*, quando* $N \to \infty$*.*

F_A, como espaço finito de dimensão N, pode ser interpretado como uma base ortonormal segundo o produto escalar. Neste caso a função de Mertens pode ser representada por

$$M(N) = Z \cdot Z^{-1} = ||Z|| \cdot ||z^{-1}|| \cos(Z, Z^{-1}) = \sqrt{N}\sqrt{Q(N)}\cos(Z, Z^{-1}),$$

e assim

$$\cos(Z, Z^{-1}) = \frac{M(N)}{\sqrt{N \cdot Q(N)}}.$$

de onde se conclui que $\cos(Z, Z^{-1}) \to 0$*, quando* $N \to \infty$*, é* ***equivalente*** *ao teorema dos números primos, na forma* $M(N) = o(N)$*.*

No entanto, não encontrei uma relação simples entre produtos internos e a noção compositiva da álgebra.

Como as avaliações polinomiais e ademais composições entre os elementos destas álgebras operam paralelamente pela álgebra das convoluções no coeficientes, podemos transportar cada uma das identidades algébricas para uma identidade construtiva na álgebra das convoluções, as quais chamamos de **fórmulas primitivas**, versões numéricas das identidades algébricas. De todas, a mais importante é a fórmula primitiva para a contagem ponderada de primos de Riemann J,

$$J(N) = \sum_{1 \le k \le h} \frac{(-1)^{k+1}}{k} \sum_{1 \le n \le N} \sum_{\substack{a_1 \cdot \ldots \cdot a_k = n \\ Arr;\ a_i \ge 2,\ \forall i}} 1,$$

obtida por convoluções da seqüência contante 1.

A álgebra exterior também deve dar informações aritméticas importantes, por sua informação angular. Nos perguntamos, em especial, com sua relação com a função seno, e o jogo que isso poderia permitir com o produto interno. No entanto, não no alongamos nas investigações.

3.1.3 Extensões lineares de homomorfismos aritméticos em $\mathbb{C}$

Teorema 3.1.1 *Dada uma aritmética enumerável, os homomorfismos $h : (A_k,\ \circ) \to \mathbb{C}$ do k-ésimo monóide de operações $(A_k,\ \circ)$ são unicamente linearmente estendidos para $h : A_k^{\Sigma} \to \mathbb{C}$ definida sobre o $\mathbb{C}$-módulo $(A_k^{\Sigma},\ +)$ livremente gerado pelas $a_{k,n} \in A_k$.*

Dem.: Os homomorfismos de monóide já estão definidos sobre as bases dos espaços, de onde a extensão é obtida unicamente ao impormos linearidade.

Afirmação 3.1.2 *O mesmo pode ser dito dos endomorfismos limitados para as aritméticas nilpotentes, e os homomorfismos limitados com imagem em $\mathbb{C}$*

Teorema 3.1.2 (Lei da correspondência entre o caso enumerável e o nilpotente) *Seja $U\infty$ conjunto bem ordenado e U_n os conjuntos dos primeiros n elementos de U. Seja A_∞ a aritmética de $U\infty$ com operações $B_{\infty,\ k}$e A_n as aritméticas nilpotentes de U_n com operações $B_{n,k}$.*

Então $o \in B_{n,\ k}$ se, e somente se, é restrição de uma operação $O \in B_{\infty,\ k}$.

Dem.: Decorre da relação entre o caso nilpotente e o enumerável já presente na estrutura monoidal, e significa que os casos finitos nilpotentes aproximam de maneira bastante ordenada o enumerável.

3.1.4 O conceito de álgebra de Banach para S_A de ordem infinita

Um espaço vetorial normado completo é uma álgebra de Banach A se a operação de multiplicação da álgebra e a norma vetorial satisfazem a condição $||x \cdot y|| \leq ||x|| \cdot ||y||, \forall x, y \in A$. Os resultados estão todos no primeiro capítulo do livro de Folland (1995). Podemos aplicá-los a S_A, desde que R seja $R = \mathbb{C}$.

Para uma álgebra de Banach unital, define-se o espectro $\sigma(a)$ de um elemento a seu como o conjunto

$$\sigma(a) = \{\lambda \in \mathbb{C} : Id\lambda - a \text{ é invertível}\}.$$

Além disso, seu raio espectral $\rho(a)$ é

$$\rho(a) = \sup\{|\lambda| : \lambda \in \sigma(a)\},$$

e vale (1995, p. 5)

$$\rho(a) = \lim_{n\to\infty} ||a^n||^{1/n}.$$

Quando a álgebra A é também comutativa, a teoria dos homomorfismos da álgebra de Banach unital na álgebra complexa simplifica a descrição dos fatos. Isso porque os **homomorfismos não nulos** $h \in \sigma(A)$ respeitam (1995, p. 5) $h(Id) = 1$; se a é invertível, então $h(a) \neq 0$, e $||h(a)|| \leq ||a||$, $\forall a \in A$. O resultado fundamental é que os ideais maximais de A são exatamente os $\ker(h)$ (1995, p. 6)[2].

Mais do que isso, o estudo de cada elemento de A através destes homomorfismos, chamado teoria de Gelfand, leva a uma caracterização diferente de A. O elemento dual $\hat{a} : \sigma(A) \to \mathbb{C}$ tal que $\hat{a}(h) = h(a)$ e a transformada $\Gamma : A \to C(\sigma(A))$ tal que $\Gamma(a) = \hat{a}$ respeitam (1995, p. 7)

i) Γ é homomorfismo e $\widehat{Id} \equiv 1$;

ii) a é invertível se, e somente se, $\hat{a}$ nunca se anula;

iii) $\mathrm{Im}(\hat{a}) = \sigma(a)$;

iv) $||\hat{a}||_{\sup} = \rho(a) \leq ||a||$.

Além disso, para a álgebra gerada por $Id,\ s$, vale que $\hat{s}$ é homeomorfismo de $\sigma(A)$ a $\sigma(s)$ (1995, p. 8). Isso significa que para compreender $\sigma(S_A)$, **basta estudarmos o espectro da função sucessora.**

Seqüências equipadas com soma e convoluções aditivas lineares como multiplicação formam uma álgebra de Banach são estudadas por Folland, e são totalmente análogas à nossa teoria de S_A quando $N = \aleph_0$. Tratemos em especial o conjunto l_1 das seqüências absolutametne somáveis, e os homomorfismos de $\sigma(l_1)$. É suficiente que compreendamos o espectro de da função sucessora s. Como ele é o disco unitário complexo, $||z|| \leq 1$, se satisfaz $h_z(s) = z$ homeomorficamente por z, e vale

$$\hat{a}(h_z) = \sum_{n=0}^{\infty} a_n z^n,$$

[2] E o núcleo do homomorfismo nulo é todo A

analogamente ao teorema 1.17 de Folland (1995, p. 9).

Este resultado, talvez inocente, tem a seguinte conseqüência:

Corolário 3.1.1 *Se* $\hat{a}(h_z) = \sum a_n z^n$, *sendo* $||z|| \leq 1$ *e* $\sum ||a_n|| < \infty$, *e se* $\hat{a}$ *nunca é nula, então* $1/\hat{a}(h_z) = b$ *é* $b = \sum b_n z^n$, *com* $\sum ||b_n|| < \infty$.

A transformada de Gelfand se torna um $*$-isomorfismo isométrico quando a álgebra de banach unital é uma C^*-álgebra (1995, p. 11).

Mais à frente, estudaremos o grupo dos elementos invertíveis da álgebra. Para este elementos, vale o seguinte:

Afirmação 3.1.3 *Seja A álgebra de Banach unital e* a_0 *um ponto da fronteira do conjunto de elementos invertíveis de A. Se* a_n *é invertível para cada n e se* $a_n \to a_0$, *quando* $n \to \infty$, *então* $||a_n^{-1}|| \to \infty$.

A teoria espectral para C^*-álgebras esta totalmente descrita em Folland (1995, p. 22-28).

A teoria quase completa dos homomorfismos de álgebra $h \in \sigma(Alg(A))$ **sobre** $Alg(A)$ **para** $\mathbb{C}$ **e os elementos duais**

$Alg(A)$ é não comutativa e a teoria dos homomorfismos de espectro complexo é insuficiente para estudá-la. Assim, o texto de Folland é insuficiente. Não obtive fontes literárias para fundamentar esse estudo homomórfico, exigindo anéis especiais como espectro dos elementos das álgebras. Tentar generalizar os argumentos de Folland para o cenário não comutativo foi pouco proveitoso, seria tremendamente trabalhoso. Portanto dediquei-me ao estudo dos espectros $\sigma(S_A)$ e $\sigma(F_A)$ de S_A e F_A. Ratificando o que foi dito há pouco, o teorema mais importante sobre o estudo de Gelfand é encontrado em Folland (1995, p. 2)

Teorema 3.1.3 *Seja A uma álgebra de Banach comutativa unital. Então o mapa* $h \to \ker(h)$ *é uma bijeção entre* $\sigma(A)$ *e o conjunto dos ideais maximais de A.*

Lembremos que para S_A (ou F_A), a transformada de Gelfand é homeomorfismo $\Gamma : S_A \to C(\sigma(S_A))$, e um isomorfismo de álgebras (para as nossa teoria, a transformada também estabelece uma correspondência natural entre os subconjuntos fechados de $\sigma(S_A)$ e conjuntos fechados de S_A (1995, p. 107)).

A conclusão é que a aditividade das s_n e a multiplicatividade das f_n são impressos nos seus respectivos elementos duais $\hat{a} \in \widehat{S_A}$, ou $\widehat{F_A}$, as álgebras dos elementos duais contínuos atuantes sobre os espectros $\sigma(S_A)$ e $\sigma(F_A)$.

Tema de investigações futuras: grupo fundamental e monodromia das álgebras aritméticas duais de $\widehat{Alg}(A)$

Algo crítico que não estudaremos neste trabalho é o estudo do **grupo fundamental** das álgebras de operações aritméticas topológicas, e o estudo da **monodromia**.

Totalmente análogo ao processo de continuação analítica de funções não lacunárias (no sentido do teorema da lacuna de de Ostrowski-Hadamard e Fabry), podemos nos perguntar quando os homomorfismos das álgebras aritméticas, determinados nos geradores por imagens no disco unitário complexo, podem ser analiticamente continuadas para uma região maior do plano complexo. Como os homomorfismos são indexados por números complexos, os elementos duais partem de uma potência cartesiana de $\mathbb{C}$.

Agora que definimos as álgebras de operações aritméticas e suas duais, estão prontos para compreender esta linha de investigação. De fato, podemos estudamos os homomorfismos das álgebras e os elementos duais, cujas imagens são em $\mathbb{C}$, para investigar a possibilidade de continuação analítica diretamente através do **Teorema da Monodromia**.

A expectativa é que haja uma conexão mais profunda a monodromia de $\hat{a}$, e que seja possível provar profundos resultados análogos às fórmulas de traço de Selberg, Langlands e Arthur.

O Teorema Tauberiano Aritmético para S_A

O teorema de Wiener-Pitt tem imediata aplicabilidade para os elementos de S_A com $N = \aleph_0$, e a álgebra convolutiva, quando R é subanel de $\mathbb{C}$. Ao mesmo tempo é geral, dedicando-se a todos os grupos topológicos abelianos localmente compactos. De fato, ele diz que (FOLLAND, 1995, p. 116)

Teorema 3.1.4 (Teorema Tauberiano de Wiener-Pitt) *Seja $\phi \in L^\infty(G)$, $a \in L^1(G)$, suponhamos que $\hat{a}$ não se anule, e que $\phi * a(x) \to d \int a$, quando $x \to \infty$. Então*

*i) $\phi * b(x) \to d \int b$ quando $x \to \infty$, **para todo** $b \in L^1(G)$;*

*ii) Se ϕ é lentamente oscilante, **a própria** $\phi(x) \to d$, quando $x \to \infty$.*

Em particular, se φ tem coeficientes limitados, α tem coeficientes absolutamente somáveis e os coeficientes de $\varphi \circ \alpha$ tendem a zero, os coeficiente de $\varphi \circ \beta$ tendem a zero para todo β de coeficientes absolutamente somáveis (desde que ϕ e a possam ser estendidas a funções respectivamente limitadas e absolutamente somáveis ou integráveis em $\mathbb{Z}$, $\mathbb{R}$, ou mesmo $\mathbb{R}^+$, no caso multiplicativo).

A teoria é perfeitamente transportada para a nossa, onde podemos considerar ϕ, a como seqüências de coeficientes de elementos de S_A ou F_A, e transportar as condições do teorema para os coeficientes das operações e suas composições.

Corolário 3.1.2 (Teorema Tauberiano Aritmético) *Seja $\varphi \in S_A$ com coeficientes $\phi(n)$ limitados, $\alpha \in S_A$ com coeficientes $a(n)$ absolutamente somáveis. Suponhamos que $\hat{a}$ não se anule, e que os coeficientes $\phi * a(n)$ de $\varphi \circ \alpha$ tendam a $d\sum |a_n|$, quando $n \to \infty$. Então*[3].

*i) os coeficientes de $\varphi \circ \beta$ tendem a $d\sum |b(n)|$, quando $x \to \infty$, **para todo** $\beta \in S_A$ cujos coeficientes b_n sejam absolutamente somáveis;*

ii) Se ϕ é lentamente oscilante, então $\phi(n) \to d$, quando $n \to \infty$.

O teorema dos números primos

$$\pi(x) \sim \frac{\ln(x)}{x}, \text{ ou ainda } M(x) = o(x),$$

é famoso corolário pouco trabalhoso do resultado original de Wiener, sendo a condição de não anulação do elemento dual a não anulação da função Zeta de Riemann $\zeta(s)$ em $\mathrm{Re}(s)= 1$, pelos argumentos de Ikehara. (HARDY, 1949, p. 303), de onde ζ^{-1} não tem polos na reta. Já a convolução anular-se no infinito é simplesmente (HARDY, 1949, p. 303)

$$\begin{aligned}\frac{1}{x}\int_1^\infty \lfloor x/t \rfloor \frac{M(t)}{t} dt \frac{1}{x} &= \int_1^\infty \sum_{m\leq x/t} 1 \sum_{n\leq t} \mu(n \frac{dt}{t} = \frac{1}{x}\sum_{mn\leq x} \mu(n) \int_n^{x/m} \frac{dt}{t} \\ &= \frac{1}{x}\sum_{mn\leq x} \mu(n)\ln(x/mn) = \frac{1}{x}\sum_{q\leq x} \ln(x/q) \sum_{n|q} \mu(n) = \frac{\ln(x)}{x} \\ &\to 0,\end{aligned}$$

que, em conjunto com o fato da função $f(x) = M(x)/x$ ser lentamente oscilante $()f(y) - f(x) = O\left(\frac{y-x}{x}\right) = o(1)$, quando $x \to \infty$, $y/x \to 1$), leva a

$$\frac{M(x)}{x} \to 0,$$

o Teorema dos Números Primos.

[3] Precisamos que ϕ e a permaneçam com essas propriedades quando estendidas de $\mathbb{N}_0$ para o grupo $(\mathbb{Z}, +)$, para que estejam definidas sobre um grupo, e aplicar o Teorema Tauberiano de Wiener. Isso pode ser simplesmente feito estendendo as funções como zero para os negativos

Isso é feito de tal forma que a imagem dos homomorfismos são séries de Dirichlet, como no caso anterior foram potências. Por conta disso, parece natural imaginar uma relação íntima entre as séries de Dirichlet e a álgebra F_A. Que relação seria essa?

A teoria presente teoria ainda não o expressou!, Pois F_A tem infinitos geradores f_p. Admitida uma noção de norma de Banach sobre F_A, então $\sigma(F_A)$ é gerado pelas $\hat{f_p}$.

Devemos considerar que a toda imagem de cada homomorfismos h é determinada pelas imagens $h(f_p)$, $||h(f_p)|| \leq 1$, e assim cada $\sigma(F_A)$ é indexado por infinitas variáveis complexas! Neste sentido, se vale uma condição como $||f_p|| \leq c,\ \forall p$ primo, um elemento de $a \in F_A$ respeita

$$||a|| \leq \sum_{n=p} ||a_n||c + \sum_{n=p_1p_2} ||a_n||c^2 + \sum_{n=p_1p_2p_3} ||a_n||c^3 + \cdots$$

É possível que a aplicação da teoria acima para este caso acabe por nos mostrar que se $\hat{a}(h) \neq 0,\ \forall h \in \sigma(F_A)$, então $a_{-1} = b \in F_A$, com $\sum ||b_n|| < \infty$.

Neste caso, a convergência absoluta da soma dos coeficientes gerados por inversão convolutiva multiplicativa a partir da convergência absoluta da soma dos coeficientes originais é equivalente ao elemento original não ser anulado por nenhum homomorfismo h.

Condições diferentes da convergência absoluta podem ser utilizadas para restringir de outras formas as álgebras, porque a condição de não anulação dos homomorfismos basicamente garante que o elemento inverso pertence à álgebra.

A transformada de Fourier definida no capítulo 6 é homomorfismo da álgebra convolutiva $L^1(S_A^\times)$, que engloba os funcionais das álgebras. Seria interessante observar se as convoluções destes funcionais apresentam propriedades notáveis.

3.2 Avaliações polinomiais dos elementos da álgebra

Trata-se da consideração de elementos $P : End(V) \to End(V)$ da forma

$$p(L) = \sum_{n=0}^{k} a_n L^n,$$

restritos a $L \in Alg(A)$ e $a_n \in R,\ \forall n$. Os casos de nota são, em especial, identidades algébricas respeitadas pelas matrizes das operações, a exemplo do polinômio característico.

A investigação do caso em que L é elemento nilpotente de uma álgebra finita sobre uma aritmética nilpotente só requer a consideração dos polinômios até certo grau, a depender das operações envolvidas. Isso é útil, frente a lei de correspondência, pois avaliações de grau infinito de elementos de álgebras de operações aritméticas infinitas ficam efetivamente

reduzidas a avaliações polinomiais de elementos das álgebras de operações nilpotentes, exemplificados mais abaixo com a exponencial e o logaritmo.

Afirmação 3.2.1 *Por construção, todo elemento de S_{Nil} ($S_\circ$) de A é uma avaliação polinomial da função sucessora s (c).*

Dem.: É o teorema da Avaliação Gerativa aplicado à meta-aritmética de primeiro nível de A.

3.2.1 Potências restritas

A ação dos polinômios sobre as operações é determinada pela combinação das potências. Portanto, resta-nos compreender o comportamento das potências. Para os fins deste texto, me limitarei a expressar apenas potências dos elementos puramente aditivos ou multiplicativos. Torna-se evidente que são respectivamente

$$\left(\sum_{n=0}^{N-1} a_n s^n\right)^k = \sum_{n=0}^{N-1} v_n s_n, \text{ sendo}$$
$$v_n = \sum_{j_1 t_1 + \cdots + j_w t_w = n} a_{t_1}^{j_1} \cdot \ldots \cdot a_{t_w}^{j_w} \frac{(j_1 + \cdots + j_w)!}{j_1! \cdot \ldots \cdot j_w!}$$

com $0 \leq t_1 < \cdots < t_w,\ j_1 + \cdots + j_w = k$, ou seja, uma partição de n com k elementos, e

$$\left(\sum_{n=1}^{N} a_n f^n\right)^k = \sum_{n=1}^{N} v_n s_n, \text{ sendo}$$
$$v_n = \sum_{t_1^{j_1} \cdot \ldots \cdot t_w^{j_w} = n} a_{t_1}^{j_1} \cdot \ldots \cdot a_{t_w}^{j_w} \frac{(j_1 + \cdots + j_w)!}{j_1! \cdot \ldots \cdot j_w!}$$

com $1 \leq t_1 < \cdots < t_w,\ j_1 + \cdots + j_w = k$, ou seja, uma fatoração de n com k elementos.

3.2.2 O caso infinito. A avaliação Exponencial. A avaliação logarítmica.

No caso infinito, a presença de uma norma é suficiente para expressar as circunstâncias em que as avaliações convergem. Por exemplo, a convergência da expressão na norma do operador é suficiente para obter a convergência da aplicação sobre operações lineares contínuas em V.

Fora a avaliação inversão, as avaliações mais importantes que veremos virão da aplicação das funções $EXP, LN : Alg(A) \to Alg(A)$, e existem quando houverem racionais em R análogos aos coeficientes destas funções no caso $R = \mathbb{Q}$. EXP está sempre bem definida, quando existe. Já LN fica limitada às operações invertíveis.

No caso de uma aritmética nilpotente finita de ordem N, as avaliações podem se tornar finitas, a depender do índice de nilpotência da entrada.

$$EXP(X) = \sum_{k=0}^{\infty} \frac{1}{k!} X^k,$$

$$LN(X) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} (X - Id)^k, \ e$$

$$(X)^{-1} = \sum_{k=0}^{\infty} (-1)^k (X - Id)^k,$$

sendo este último a inversão.

3.3 Alg(A) restrita a cada uma das operações aritméticas

3.3.1 Invertibilidade em Alg(A)

Uma caracterização de invertibilidade dos elementos de uma álgebra comutativa com unidade é dada através de homomorfismos de álgebra não nulos, às vezes chamados de funcionais multiplicativos e a transformada de Gelfand.

Alg(A), no entanto, não é comutativa. Por conta disso, investigaremos operação por operação.

3.3.2 Restrição da álgebra à adição aritmética

Definição 3.3.1 (Espaço de Soma) *Chamamos de **espaço de soma** S_A de um espaço aritmético o subespaço de $Hom(M, M)$ gerado pelas iterações não nulas de s. Para os casos circular e nilpotente, $S_A = [s^0, \ s, \ \cdots, \ s^{N-1}]$.*

Definição 3.3.2 (Álgebra de Soma) *Chamamos de **álgebra de soma** a álgebra gerada por considerar S_A munido da operação de composição, e também a chamamos de S_A.*

Para aritméticas **nilpotentes** de ordem N, os elementos de S_A são exatamente os b da forma

$$b = \sum_{n=0}^{N-1} b_n s^n,$$

onde $b_n \in R,\ \forall n$.

A operação de composição entre estas funções nos permite interpretar o espaço de soma como uma álgebra sobre o anel R finita, associativa e **comutativa**, se R é finito e comutativo. Neste caso, os elementos respeitam uma lei semelhante à multiplicação polinomial, sob a forma

$$b \circ c = \left(\sum_{n=0}^{N-1} b_n s^n\right) \circ \left(\sum_{n=0}^{N-1} c_n s^n\right) = \sum_{n=0}^{N-1} s^n \sum_{i+j=n} b_i c_j. \tag{3.1}$$

Nota-se que a diferença é a anulação de todos os termos com fator $s^N \equiv 0_{S_A}$. Assim S_A é isomorfo a $R[x]/(x^N)$ como álgebra.

Os elementos invertíveis de S_A são precisamente aqueles cujo primeiro coeficiente é invertível em R. Se R é um corpo e a aritmética nilpotente, todo elemento não invertível da álgebra é nilpotente, e S_A comporta-se como anel local.

Teorema 3.3.1 (Invertibilidade na álgebra de soma) *Seja $b = \sum_{n=0}^{N-1} b_n s^n \in S_A$. Então $b^{-1} \in S_A$ se, e somente se, $b_0^{-1} \in R$.*

Demonstração 3.3.1 *Se tomarmos $b \circ c = Id$ na equação (3.1), temos que o coeficiente do primeiro componente da multiplicação arbitrária é $b_0 c_0 = 1$, ou seja, b_0 é invertível em R.*

Por outro lado, se b_0 é invertível em R, existe

$$c = \sum_{n=0}^{N-1} c_n s^n$$

com coeficientes recursivamente definidos como

$$\begin{aligned} c_0 &= \frac{1}{b_0} \\ c_n &= -\frac{1}{b_0} \sum_{\substack{j \neq n \\ i+j=n}} b_i c_j, \end{aligned}$$

que satisfaz por construção

$$b \circ c = Id_{S_A}.$$

Teorema 3.3.2 *Explicitamente, se $b = \sum_{n=0}^{N-1} b_n s^n$ é invertível em S_A, $c = b^{-1}$ tem a forma*

$$c = \frac{1}{b_0}s^0 - \frac{b_1}{b_0^2}s - \left(\frac{b_2}{b_0^2} - \frac{b_1^2}{b_0^3}\right)s^2 - \cdots,$$

sendo seus coeficientes c_k *representáveis por* $c_0 = b_0^{-1}$ *e, se* $k \geq 1$,

$$c_k = \frac{1}{b_0} \sum_{\substack{j_1 v_1 + \cdots + j_w v_w = k \\ 1 \leq v_1 < \cdots < v_w}} \frac{b_{v_1}^{j_1} \cdot \ldots \cdot b_{v_w}^{j_w}}{(-b_0)^{j_1 + \cdots + j_w}} \frac{(j_1 + \cdots + j_w)!}{j_1! \cdots j_w!}$$

sendo a soma dependente das soluções do problema de particionar-se k *em ordem crescente* $(j_i,\ v_i,\ w,\ \in \mathbb{N}_1)$.

Dem.: Para $b_0 = 1$, *basta considerar que*

$$\begin{aligned} b^{-1} = \frac{Id}{Id + (b - Id)} &= \sum_{k=0}^{N-1}(-1)^k(b - Id)^k = \sum_{k=0}^{N-1}(-1)^k \left(\sum_{n=0}^{N-1} b_n s_n\right)^k \\ &= Id + \sum_{n=1}^{N-1} s^n \sum_{k=0}^{N-1}(-1)^k \sum_{\substack{j_1 + \cdots + j_w = k \\ j_1 t_1 + \cdots + j_w t_w = n}} b_{t_1}^{j_1} \cdot \ldots \cdot b_{t_w}^{j_w} \frac{(j_1 + \cdots + j_w)!}{j_1! \cdot \ldots \cdot j_w!} \\ &= Id + \sum_{n=1}^{N-1} s^n \sum_{j_1 t_1 + \cdots + j_w t_w = n} (-1)^{j_1 + \cdots + j_w} b_{t_1}^{j_1} \cdot \ldots \cdot b_{t_w}^{j_w} \frac{(j_1 + \cdots + j_w)!}{j_1! \cdot \ldots \cdot j_w!}, \end{aligned}$$

onde $j_i \geq 1, \forall i,\ 1 \leq t_1 < \cdots < t_w$, *sendo a quantidade* w *qualquer. Se* $b_0 \neq 1$, *então* $g = b/b_0$ *recai no caso anterior, com coeficientes* $g_n = b_n/b_0$, *o que prova o teorema.*

Automorfismos lineares aditivos

Aqui[4] estudamos algumas relações aditivas entre os geradores do espaço e observamos as formas particulares de mudança de base.

Teorema 3.3.3 *Dados* m, v *elementos de* M, m *gerador de* A, *existe um único* $h \in S_A$ *tal que* $h(m) = v$. *Se* v *é gerador,* h *é elemento invertível de* S_A, *automorfismo aditivo do módulo* M.

Demonstração 3.3.2 *Basta notar que se* $m = m_1$ *é gerador,* $m_1, \cdots, m_N$ *é base de* M, *e portanto existem* $j_1, \cdots, j_N \in R$ *tais que*

$$v = \sum_{n=1}^{N} j_n m_n = \left(\sum_{n=0}^{N-1} j_{n+1} s^n\right)(m).$$

[4] Originalmente inversão e triangulação aditiva.

A unicidade decorre do fato dos m_n comporem uma base, e portanto representarem unicamente v, e o elemento de S_A à direita (que chamamos de h) é o único que leva m à representação à esquerda , pela correspondência gerativa.

Além disso, vimos que se v é gerador, j_1 é invertível, e portanto h é invertível, e um automorfismo.

Neste caso, podemos escrever a inversão

$$m = h^{-1}(v),$$

tendo h^{-1} coeficientes tais como na demonstração anterior.

Mais que isso, h é tal que

$$v_n = s^{n-1}(v) = s^{n-1}(h(m)) = h(s^{n-1}(m)) = h(m_n),$$

estabelecendo uma bijeção entre as duas bases que **preserva sua ordem**.

Este processo, que originalmente denotei triangulação, é uma caso particular de mudança de base. Estes automorfismos determinam precisamente as bases tornadas equivalentes pela relação presente no final do capítulo 2.

3.3.3 Restrição da álgebra à multiplicação aritmética

Definição 3.3.3 (Espaço de Multiplicação) *Chamamos de **espaço de multiplicação** F_A de um espaço aritmético o subespaço de $Hom(M, M)$ gerado pelos elementos de A_2. Para os casos circular e nilpotente, $F_A = [f_1,\ f_2,\ \cdots,\ f_N]$.*

Definição 3.3.4 (Álgebra de multiplicação) *Chamamos de **álgebra de multiplicação** a álgebra gerada por considerar F_A munido da operação de composição, e também a chamamos de F_A.*

Para aritméticas **nilpotentes**, os elementos de F_A são exatamente os b da forma

$$b = \sum_{n=1}^{N} b_n f^n,$$

onde $b_n \in R,\ \forall n$.

A operação de composição entre estas funções nos permite interpretar o espaço de multiplicação como uma álgebra sobre o anel R comutativa e finita, se R assim o for. Seus elementos respeitam uma lei semelhante à multiplicação de séries de Dirichlet, sob a forma

$$b \circ c = \left(\sum_{n=1}^{N} b_n s^n\right) \circ \left(\sum_{n=1}^{N} c_n s^n\right) = \sum_{n=1}^{N} f_n \sum_{i \cdot j = n} b_i c_j. \tag{3.2}$$

Os elementos invertíveis de F_A são precisamente aqueles cujo primeiro coeficiente é invertível em R, como no caso de S_A. Se R é um corpo, todo elemento não invertível da álgebra é nilpotente, e F_A comporta-se como anel local, da mesma maneira que S_A.

Teorema 3.3.4 (Invertibilidade na álgebra de multiplicação) *Seja $b = \sum_{n=1}^{N} b_n f^n \in F_A$. Então $b^{-1} \in F_A$ se, e somente se, $b_1^{-1} \in R$.*

Demonstração 3.3.3 *Se tomarmos $b \circ c = Id$ na equação (3.2), temos que o coeficiente do primeiro componente da multiplicação arbitrária é $b_1 c_1 = 1$, ou seja, b_1 é invertível em R.*

Por outro lado, se b_1 é invertível em R, existe

$$c = \sum_{n=1}^{N} c_n f_n$$

com coeficientes recursivamente definidos como

$$\begin{aligned} c_1 &= \frac{1}{b_1} \\ c_n &= -\frac{1}{b_1} \sum_{\substack{j \neq n \\ i \cdot j = n}} b_i c_j, \end{aligned}$$

que satisfaz por construção $\sum_{i \cdot j = n} b_i c_j = 0,\ n \geq 2$, o que conclui a demonstração de

$$b \circ c = Id_{F_A}.$$

Teorema 3.3.5 *Explicitamente, se $b = \sum_{n=1}^{N} b_n f^n$, $c = b^{-1}$ tem a forma*

$$\begin{aligned} c = &\frac{1}{b_1} f_1 - \frac{b_2}{b_1^2} f_2 - \frac{b_3}{b_1^2} f_3 - \left(\frac{b_4}{b_1^2} - \frac{b_2^2}{b_1^3}\right) f_4 - \frac{b_5}{b_1^2} f_5 - \left(\frac{b_6}{b_1^2} - 2\frac{b_2 b_3}{b_1^3}\right) f_6 \\ &- \frac{b_7}{b_1^2} f_7 - \left(\frac{b_8}{b_1^2} - 2\frac{b_2 b_4}{b_1^3} + \frac{b_2^3}{b_1^4}\right) f_8 - \left(\frac{b_9}{b_1^2} - \frac{b_3^2}{b_1^3}\right) f_9 - \cdots \end{aligned} \tag{3.3}$$

sendo seus coeficientes c_k representáveis por $c_1 = b_1^{-1}$ e, se $k \geq 2$,

$$c_k = \frac{1}{b_1} \sum_{\substack{v_1^{j_1} \cdot \ldots v_w^{j_w} = k \\ 1 \leq v_1 < \cdots < v_w}} \frac{b_{v_1}^{j_1} \cdot \ldots \cdot b_{v_w}^{j_w}}{(-b_1)^{j_1 + \cdots + j_w}} \frac{(j_1 + \cdots + j_w)!}{j_1! \cdots j_w!}$$

sendo a soma dependente das soluções do problema de fatorar-se k como potências de múltiplos naturais positivos j_i de w números naturais v_i maiores que 2, independente de ordem (o peso concernente à ordem já está explícito combinatorialmente no termo), w qualquer.

Dem.: Para $b_1 = 1$, basta considerar que

$$b^{-1} = \frac{Id}{Id + (b - Id)} = \sum_{k=0}^{\log_2(N)} (-1)^k (b - Id)^k = \sum_{k=0}^{\log_2(N)} (-1)^k \left(\sum_{n=2}^{N} b_n f_n \right)^k$$
$$= Id + \sum_{n=2}^{N} f_n \sum_{k=1}^{\log_2(N)} (-1)^k \sum_{\substack{j_1+\cdots+j_w=k \\ t_1^{j_1}\cdot\ldots\cdot t_w^{j_w}=n}} b_{t_1}^{j_1} \cdot \ldots \cdot b_{t_w}^{j_w} \frac{(j_1 + \cdots + j_w)!}{j_1! \cdot \ldots \cdot j_w!}$$
$$= Id + \sum_{n=2}^{N} f_n \sum_{t_1^{j_1}\cdot\ldots\cdot t_w^{j_w}=n} (-1)^{j_1+\cdots+j_w} b_{t_1}^{j_1} \cdot \ldots \cdot b_{t_w}^{j_w} \frac{(j_1 + \cdots + j_w)!}{j_1! \cdot \ldots \cdot j_w!},$$

onde $j_i \geq 1, \forall i$, $2 \leq t_1 < \cdots < t_w$, sendo a quantidade w qualquer. Se $b_1 \neq 1$, então $g = b/b_1$ recai no caso anterior, com coeficientes $g_n = b_n/b_1$, o que prova a afirmação.

Automorfismos lineares multiplicativos

O resultado é análogo ao aditivo.

Teorema 3.3.6 *Dados m, v elementos de M, m gerador de A, existe um único $h \in F_A$ tal que $h(m) = v$. Se v é gerador, h é elemento invertível de F_A, automorfismo multiplicativo do módulo M.*

Demonstração 3.3.4 *Basta notar que se $m = m_1$ é gerador, $m_1, \cdots, m_N$ é base de M, e portanto existem $j_1, \cdots, j_N \in R$ tais que*

$$v = \sum_{n=1}^{N} j_n m_n = \left(\sum_{n=1}^{N} j_n f_n \right)(m).$$

A unicidade decorre do fato dos m_n comporem uma base, e portanto representarem unicamente v, e o elemento de F_A à direita (que chamamos de h) é o único que leva m à representação à esquerda , pela correspondência gerativa.

Além disso, vimos que se v é gerador, j_1 é invertível, e portanto h é invertível, e um automorfismo.

Neste caso, podemos escrever a inversão

$$m = h^{-1}(v),$$

tendo h^{-1} coeficientes tais como na demonstração anterior.

Da mesma maneira, tal h **preserva a ordem das bases**. O resultado acima foi inicialmente chamado por mim de triangulação multiplicativa.

3.3.4 Decomposição em fatores elementares: forma compositiva das inversões

As inversões aditiva e multiplicativa vistas foram executadas do ponto de vista espacial. No entanto, podemos expressar o elemento inverso por meio de composições de diferenças entre a identidade e as operações aritméticas dadas, como

$$(s_0 - y_n s_n), \quad (f_1 - y_n f_n),$$

e todos os elementos invertíveis das álgebras restritas são portanto construídos pela composição destas diferenças simples. Todos os coeficientes a seguir pode ser combinatorialmente compreendidos, mas nos limitaremos, na maior parte, apenas a afirmar sua existência.

Teorema 3.3.7 (Inversão aditiva compositiva (forma direta)) *Seja $a \in S_A^{\times}$, com $a = \sum_{n=0}^{N-1} a_n s_n$, $a_0 = 1$. Então existem únicos $b_1, \cdots, b_{N-1} \in R$ tais que*

$$a^{-1} = \bigcirc_{k=1}^{N-1}(s_0 - b_k s_k),$$

Dem.: É um outro uso do Princípio de Exclusão-Inclusão. Basta notar que se a_n é o coeficiente não nulo distinto de a_0 de menor índice do elemento $a \in S_A$, o elemento $a(s_0 - a_n s_n)$ tem o menor coeficiente não nulo maior ou igual ao índice $n+1$ de s_{n+1}, de onde, recursivamente, pode-se eliminar todos os coeficientes, restando como produto apenas o termo s_0.

Corolário 3.3.1 (Inversão aditiva compositiva (forma inversa)) *Seja $a \in S_A^{\times}$, com $a = \sum_{n=0}^{N-1} a_n s_n$, $a_0 = 1$.*

Então existem únicos $b_1, \cdots, b_{N-1} \in R$ tais que

$$a = \bigcirc_{k=1}^{N-1}(s_0 - b_k s_k),$$

Dem.: É aplicação do teorema anterior para $b = a^{-1}$.

Além disso, vale

$$b_n = \sum_{u_1+\cdots+u_w=n} (-1)^w a_{u_1}\cdots a_{u_w} \quad e$$
$$a_n = \sum_{v_1+\cdots+v_w=n} (-1)^w b_{v_1}\cdots b_{v_w},$$

sendo as somas indexadas por partições convencionais no caso dos u_i e particões em somandos distintos no caso dos v_i.

Este resultado é sumamente importante, porque vale em completa generalidade para qualquer espaço aritmético nilpotente, qualquer que seja o anel de coeficientes R. Todo espaço destes respeita, portanto, uma forma universal de fatoração em termos de diferenças da identidade para a base operacional. **É, desta forma, um resultado mais fundamental que o teorema fundamental da álgebra**. De fato, a forma direta da inversão se transforma no teorema de Gauss sobre a decomposição de polinômios de coeficientes reais em fatores lineares e quadráticos de coeficientes reais, e no teorema fundamental da álgebra quando se admitem os números complexos como coeficientes.

O argumento para o teorema seguinte é quase idêntico ao caso aditivo.

Teorema 3.3.8 (Inversão multiplicativa compositiva (forma direta)) *Seja $a \in F_A^{\times}$, com $a = \sum_{n=1}^{N} a_n f_n$, $a_1 = 1$.*

Então existem $b_1, \cdots, b_{N-1} \in R$ tais que

$$a^{-1} = \bigcirc_{k=2}^{N}(f_1 - b_k f_k).$$

Teorema 3.3.9 (Inversão multiplicativa compositiva (forma inversa)) *Seja $a \in F_A^{\times}$, com $a = \sum_{n=1}^{N} a_n f_n$, $a_1 = 1$. Então existem $b_1, \cdots, b_{N-1} \in R$ tais que*

$$a = \bigcirc_{k=2}^{N}(f_1 - b_k f_k),$$

3.3.5 E-funções

Definida como

$$E = \prod_{n=1}^{N-1}(s_0 - s_n),$$

generalizando a função estudada por Euler nos anos 1750 tem como coeficientes em S_A os números e_n. Tais coeficientes são nulos para todo n a menos de números conhecidos como números pentagonais generalizados de Euler, conforme o Teorema Pentagonal de Euler para os mesmos. Tais números são exatamente os resultado indexados em naturais pelos seguinte quatro polinômios $h_i : \mathbb{N}_1 \to \mathbb{N}_1$ de segundo grau

$$\begin{aligned} h_1(n) &= 6n^2 - 7n + 2 = (2n-1)(3n-2), \\ h_2(n) &= 6n^2 - 5n + 1 = (2n-1)(3n-1), \\ h_3(n) &= 6n^2 - n, \ e \\ h_4(n) &= 6n^2 + n \end{aligned}$$

sendo $e_\rho = -1$, se ρ é imagem de $h_1,\ h_2$, e $e_\rho = +1$, se ρ é imagem de h_3 ou h_4.

A importância da função é tremenda para o estudo da quantidade de partições $p(n)$ e soma ponderada de divisores $\sigma(n)/n$, pois

$$E^{-1} = \prod_{n=1}^{N-1} \frac{s_0}{s_0 - s_n} = 1 + \sum_{n=1}^{N-1} p_n s_n$$

$$LN(E) = -\sum_{n=1}^{N-1} \frac{\sigma(n)}{n} s_n.$$

A função de Euler original claramente se anula no círculo complexo, pela forma compositiva. Isso significa que $\sum_{n=0}^{\infty} e_n e^{2\pi i \theta n} = 0,\ \forall \theta$, um tremendo cancelamento apresentado pelas freqüências pentagonais. Retornaremos a estas freqüências no capítulo 5.

3.3.6 Z-funções

Uma das utilidades na definição de um espaço aritmético nilpotente aqui considerada é a possibilidade de definir, em generalidade, as funções Z sobre o espaço gerado M.

Definição 3.3.5 (Z-função) *Seja $A = (x, s, 0)$ espaço aritmético nilpotente de dimensão N sobre um R-módulo M. O elemento $Z : M \to M$ de F_A tal que*

$$Z = \sum_{n=1}^{N} f_n$$

será chamado de Z-função de A sobre M.

Sua característica mais imediata e marcante é exposta na seguinte identidade.

Teorema 3.3.10 (Produto de Euler generalizado para funções Z) *Seja Z Z-função de um espaço aritmético nilpotente. Então*

$$Z = \prod_{p \leq N} \frac{f_1}{f_1 - f_p},$$

onde os índices p são os números primos.

Demonstração 3.3.5 *Basta notar que*

$$\begin{aligned} \prod_{p \leq N} \frac{f_1}{f_1 - f_p} &= \prod_{p \leq N} \sum_{n=0}^{\infty} f_p^n \\ &= \sum_{n=1}^{N} a_n f_n, \end{aligned}$$

onde, por distributividade[5]

$$a_n = \sum_{p_1^{b_1} \cdot \ldots \cdot p_w^{b_w} = n} 1, \tag{3.4}$$

onde $p_i \neq p_j$, se $i \neq j$. Ou seja, a_n soma quantas maneiras existem de multiplicar potências de primos distintos que resultem em n.

Como vale o Teorema Fundamental da Aritmética, temos que o termo da direita de (3.4) é um, e portanto $a_n = 1\ \forall n$, e o resultado segue.

As conseqüências provenientes desta conexão, equivalente ao Teorema Fundamental da Aritmética, são de carácter eminentemente algébrico. Correspondentes numéricos e combinatórios podem ser extraídos da conexão em termos dos coeficientes. Se conectam assim de maneira aritmética, algébrica e combinatória os números primos e naturais. A maior influência desta filosofia foi a descoberta da Lei das Fatorações Naturais, dada no capítulo 4.

Como exemplo mais imediato do primeiro, a forma da função inversa de Z segundo a álgebra de operações multiplicativas:

[5] O índice superior infinito foi usado por comodidade, é claro que toda f_p é nilpotente e portanto existem índices finitos para cada p.

Corolário 3.3.2 *Consideremos a função Z de um espaço aritmético nilpotente A. Então*

$$Z^{-1} = \prod_{p \leq N} (f_1 - f_p) = \sum_{n=1}^{N} \mu(n) f_n,$$

sendo μ a função de Möbius definida com imagem em R.

Já um exemplo de identidade elementar associada a esta construção vem da identidade

$$L^{-1} = \frac{Id}{Id + L - Id} = \sum_{n=0}^{\infty} (-1)^n (L - Id)^n,$$

válida sob condições especiais, como a existência de uma norma de uma álgebra de Banach. Aplicando para $L = Z$, temos que $Z - Id$ é nilpotente e portanto a expressão é finita e inteligível, e nos mostra que

$$Z_N^{-1} = Id - (Z_N - Id) + (Z_N - Id)^2 - \cdots .$$

Por unicidade dos coeficientes desta expressão, conclui-se uma relação que expressa $\mu(n)$ pelas $d_k^*(n)$, conforme escrito no capítulo 4.

3.4 Exemplos particulares das inversões aritméticas vistas

Corolário 3.4.1 *Seja $t \in \mathbb{C}$ e $b_0 \neq 0$. Se*

$$b(t) = b_0 t + b_1 t^2 + b_2 t^3 + \cdots ,$$

então

$$t = b(t) \cdot \left(\frac{1}{b_0} - \frac{b_1}{b_0^2} t - \left(\frac{b_2}{b_0^2} - \frac{b_1^2}{b_0^3} \right) t^2 - \cdots \right).$$

.

Demonstração 3.4.1 *Consideremos a aritmética*[6] *$A = (t,\ s_t)$ do exemplo 2.1.3. A inversão aditiva 3.3.2 de um elemento $b \in S_A$ aplicada ao elemento $b(t) \in V$ retorna o gerador t de A, exatamente quando $b_0^{-1} \in \mathbb{C}$, isto é, $b_0 \neq 0$.*

[6] Ou mesmo $(Id(\mathbb{C}), \cdot Id(\mathbb{C})$, sendo $\cdot$ a multiplicação complexa induzida sobre as funções $\mathbb{C} \to \mathbb{C}$

Explicitamente, vimos que $c_0 = b_0^{-1} \in R$ *é equivalente a existência da transformação*

$$c = \frac{1}{b_0}s^0 - \frac{b_1}{b_0^2}s - \left(\frac{b_2}{b_0^2} - \frac{b_1^2}{b_0^3}\right)s^2 - \cdots,$$

em S_A*, que, quando avaliada em* $c(b(t)) = t$ *para o espaço aritmético particular, rende*

$$\begin{aligned} t &= \frac{1}{b_0}b(t) - \frac{b_1}{b_0^2}b(t)t - \left(\frac{b_2}{b_0^2} - \frac{b_1^2}{b_0^3}\right)b(t)t^2 - \cdots \\ &= b(t)\left(\frac{1}{b_0} - \frac{b_1}{b_0^2}t - \left(\frac{b_2}{b_0^2} - \frac{b_1^2}{b_0^3}\right)t^2 - \cdots\right). \end{aligned}$$

Em outras palavras, a inversão aditiva é, para as séries de potências, a inversão do produto usual.

Corolário 3.4.2 *Nas mesmas condições do corolário anterior, a inversão multiplicativa 3.3 se lê que se* $b_1 \neq 0$ *e*

$$b(t) = b_1t + b_2t^2 + b_3t^3 + \cdots,$$

então

$$t = \frac{1}{b_1}b(t) - \frac{b_2}{b_1^2}b(t^2) - \frac{b_3}{b_1^2}b(t^3) - \left(\frac{b_4}{b_1^2} - \frac{b_2^2}{b_1^3}\right)b(t^4) - \frac{b_5}{b_1^2}b(t^5) - \left(\frac{b_6}{b_1^2} - 2\frac{b_2b_3}{b_1^3}\right)b(t^6) - \cdots.$$

Corolário 3.4.3 *Para o espaço aritmético dos exponenciais de naturais do exemplo 2.1.4, a inversão multiplicativa 3.3 se lê que se* $b_1 \neq 0$ *e*

$$b(t) = b_1 + b_2\frac{1}{2^t} + b_3\frac{1}{3^t} + \cdots,$$

então

$$\begin{aligned} 1 &= \frac{1}{b_1}b(t) - \frac{b_2}{b_1^2}b(t)\frac{1}{2^t} - \frac{b_3}{b_1^2}b(t)\frac{1}{3^t} - \left(\frac{b_4}{b_1^2} - \frac{b_2^2}{b_1^3}\right)b(t)\frac{1}{4^t} - \frac{b_5}{b_1^2}b(t)\frac{1}{5^t} - \left(\frac{b_6}{b_1^2} - 2\frac{b_2b_3}{b_1^3}\right)b(t)\frac{1}{6^t} - \cdots \\ &= b(t)\cdot\left(\frac{1}{b_1} - \frac{b_2}{b_1^2}\frac{1}{2^t} - \frac{b_3}{b_1^2}\frac{1}{3^t} - \left(\frac{b_4}{b_1^2} - \frac{b_2^2}{b_1^3}\right)\frac{1}{4^t} - \frac{b_5}{b_1^2}\frac{1}{5^t} - \left(\frac{b_6}{b_1^2} - 2\frac{b_2b_3}{b_1^3}\right)\frac{1}{6^t} - \cdots\right). \end{aligned}$$

Em outras palavras, a inversão multiplicativa é, para as séries de Dirichlet, a inversão do produto usual.

Corolário 3.4.4 *Para o espaço aritmético de senóides do exemplo 2.1.2, a inversão multiplicativa 3.3 se lê que se* $b_0 \neq 0$ *e*

$$b(t) = b_1 \sin(x) + b_2 \sin(2x) + b_3 \sin(3x) + \cdots ,$$

então

$$\sin(x) = \frac{1}{b_1} b(t) - \frac{b_2}{b_1^2} b(2t) - \frac{b_3}{b_1^2} b(3t) - \left(\frac{b_4}{b_1^2} - \frac{b_2^2}{b_1^3} \right) b(4t) - \frac{b_5}{b_1^2} b(5t) - \left(\frac{b_6}{b_1^2} - 2\frac{b_2 b_3}{b_1^3} \right) b(6t) - \cdots .$$

3.4.1 Aplicações particulares para representações de funções

Exemplo 3.4.1 *Consideremos a série de Fourier da forma*

$$\sum_{n=1}^{\infty} \frac{\sin(nx)}{n} = \begin{cases} 0, & \text{se } x = 2\pi k; \\ \frac{\pi}{2} - \pi \left\{ \frac{x}{2\pi} \right\}, & \text{noutros casos.} \end{cases}$$

De acordo com o corolário (3.4.4) acima, podemos inverter a expressão a fim de obter

$$\sin(2\pi x) = \pi \sum_{\substack{n=1 \\ n \neq k/2x, \ \forall k \in \mathbb{Z}}}^{\infty} \frac{\mu(n)}{n} \left(\frac{1}{2} - \{nx\} \right).$$

A condição $n \neq k/2x$ *elimina infinitos múltiplos de termos, quando* x *é um número racional. Para que conservemos a cada avaliação a presença de todos os termos, é necessário que tomemos seqüências sobre irracionais. Por exemplo, se considerarmos uma seqüência* α_y *de irracionais positivos tais que* $\alpha_y \to 0$*, quando* $y \to \infty$*, certamente*

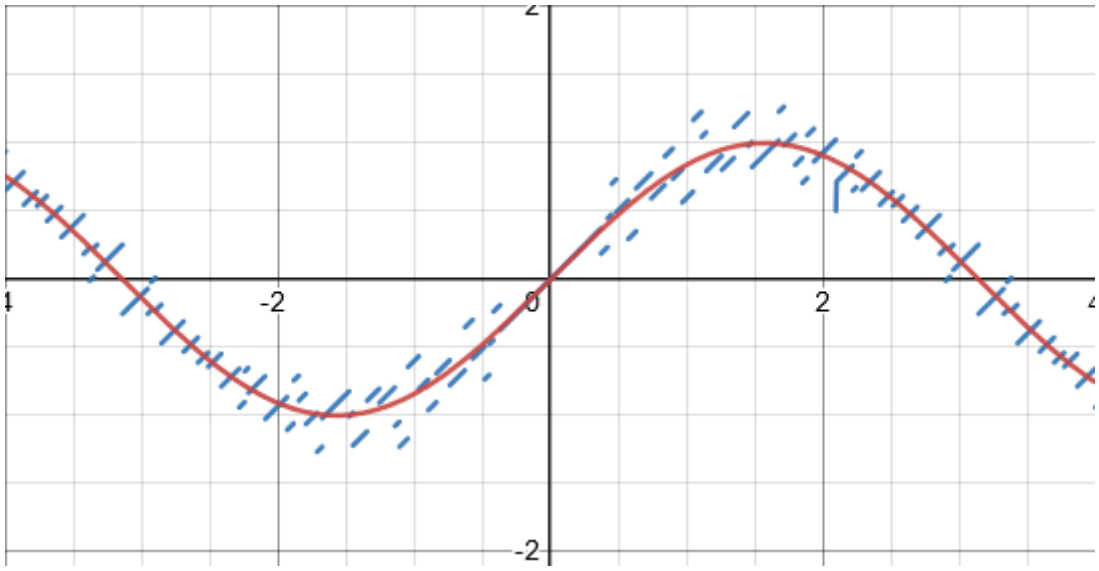
$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} \left(\frac{1}{2} - \{n\alpha_y\} \right) = \sin(2\pi\alpha_y) \to 0.$$

Se o limite da expressão fosse uniforme, poderíamos comutar os limites em n *e* y*, o que garantiria*

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0.$$

Mas este não é o caso.

Na imagem abaixo, a inversão com termos até 17, convergindo para a função seno.



Exemplo 3.4.2 *Consideremos a série de Fourier da forma*

$$\sum_{n=1}^{\infty} \frac{\cos(nx)}{n^2} = g(f(x)),$$

sendo $g(x) = x^2/4 - \pi x/2 + \pi^2/6$ *e* $f(x) = 2\pi\{x/2\pi\}$.

De acordo com o corolário (3.4.4), podemos inverter a expressão a fim de obter

$$\cos(2\pi x) = \pi^2 \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2}(\{nx\}^2 - \{nx\} + 1/6).$$

Neste caso a função é mais bem comportada, porém não fornece meios de avaliar a soma $\sum_n \mu(n)/n$.

O leitor pode experimentar unir as duas fórmulas anteriores através do teorema de Pitágoras!

Muitos outros exemplos são possíveis. Por exemplo, a inversão multiplicativa para a função $e^x - 1$, dentro da aritmética das $x, x^2, x^3, \cdots$ retorna

$$x = (e^x - 1) - \frac{1}{2}(e^{x^2} - 1) - \frac{1}{6}(e^{x^3} - 1) - \left(\frac{1}{24} - \frac{1}{4}\right)(e^{x^4} - 1) - \cdots,$$

etc.

3.4.2 Condições de convergência para inversões de vetores avaliados em uma variável

Para o caso aditivo, basta notarmos que se $g_k(z) = \sum_{n=0}^{\infty} f_{k+n}(z)$, então $f_k(z) = g_k(z) - g_{k+1}(z)$. A finitude da expressão mostra que a convergência da inversão só depende da convergência da série inicial.

Já no caso multiplicativo, se $g_k(z) = \sum_{n=1}^{\infty} f_{kn}(z)$, então $f_k(z) = \sum_{n=1}^{\infty} \mu(n) g_{kn}(z)$, que é outra expressão infinita. A somabilidade absoluta das somas combinadas rende a condição suficiente para a convergência do caso multiplicativo, analogamente ao dado por Hardy e Wright (2008, p. 308): a convergência da série $\sum_{l,n} |f_{nlk}(z)| = \sum_c d(c)|f_{ck}(z)|$, onde $d(n)$ é a quantidade de divisores de n.

De fato, quando isto acontece, podemos certamente garantir a convergência do termo invertido. No entanto, o termo invertido pode convergir mesmo quando a original não converge! A anulação decorrente da oscilação de sinal dos coeficientes é considerável, mas difícil de determinar com precisão.

Este problema é sem dúvida um dos mais fundamentais da área, localizado no contexto de aritméticas de espaços de funções, e está ligado aos profundos problemas de convergência, como a hipótese de Riemann.

3.5 A determinação de $S_A^\times$ e $F_A^\times$

Conforme descobri, os elementos destes grupos[7] são exatamente os elementos gerados pelas composições das diferenças entre a identidade e elementos da base operacional considerada, isto é, por elementos da forma $(s_0 - y_n s_n)$ e $(f_1 - a_n f_n)$, respectivamente. Mais que isto, as formas compositivas inversas são únicas. Para compreender estes grupos, portanto, nos é suficiente compreender estes elementos, os quais chamaremos de **fatores elementares**.

A seguir determinamos perfeitamente suas ordens, e portanto as ordens de todos os elementos. A determinação do grupo pelo conhecimento dessas ordens é uma matéria atualmente reconhecida como OD-caracterizabilidade.

Afirmação 3.5.1 *A ordem de $(s_0 - y s_n)$ em $S_A^\times$ é o menor $k \in \mathbb{N}$ que simultaneamente respeita $k \cdot y = 0$ (k é ordem de y no grupo aditivo do anel R) e $nk \geq N$.*

Dem.: Para determinar as ordens destes elementos, notemos que se k é sua ordem,

$$(s_0 - y s_n)^k = \sum_{i=0}^{k} \binom{k}{i} (-y s_n)^i = s_0$$

nos retorna a condição $k \cdot y = 0$ no coeficiente de s_n da expansão. Como todos os termos seguintes da expansão tem o fator $k \cdot y$, a menos do último, são nulos. Já o último termo, $(-y s_n)^k$, é nulo se, e somente se, $nk \geq N$. Fica portanto determinado que a ordem de $(s_0 - y s_n)$ é o menor k que simultaneamente respeita $k \cdot y = 0$ e $nk \geq N$.

[7] Novamente, nos resumimos ao caso linear especial, do qual o geral decorre em poucos passos.

Corolário 3.5.1 *Seja $a \in S_A^\times$. Então a ordem de a é o* ***mínimo múltiplo comum*** *das ordens de seus fatores elementares.*

Dem.: Conseqüência da forma inversa compositiva da inversão aditiva (3.3.1) e a aplicação da afirmação acima.

Exemplo 3.5.1 *A função E tem decomposição*

$$E = \bigcirc_{k=1}^{N-1}(s_0 - s^n).$$

Neste caso, todos os fatores elementares tem k igual à característica de R. Se essa característica for $k \geq N$, o expoente de todo fator elementar de E em $S_A^\times$ é k.

Afirmação 3.5.2 *A ordem de $(f_1 - yf_n)$ em $F_A^\times$ é o menor $k \in \mathbb{N}$ que simultaneamente respeita $k \cdot y = 0$ (k é ordem de y no grupo aditivo do anel R) e $n^k > N$ (estritamente).*

Dem.: Para determinar as ordens destes elementos, notemos que

$$(f_1 - yf_n)^k = \sum_{i=0}^{k} \binom{k}{i} (-yf_n)^i = f_1$$

também nos retorna a condição $k \cdot y = 0$ no coeficiente de f_n da expansão. Da mesmo forma que no caso aditivo, todos os elementos, a menos do último, são nulos. Já o último termo, $(-yf_n)^k$, é nulo se, e somente se, $n^k > N$, e conclui-se a demonstração.

Corolário 3.5.2 *Seja $a \in F_A^\times$. Então a ordem de a é o* ***mínimo múltiplo comum*** *das ordens de seus fatores elementares.*

Dem.: Conseqüência da forma inversa compositiva da inversão multiplicativa (3.3.9) e a aplicação da afirmação acima.

4 Investigações combinatórias na álgebra de operações

Conforme comentamos na seção 3.3.6, o produto de Euler 3.3.10

$$Z = \prod_{p \leq N} \frac{f_1}{f_1 - f_p},$$

implica a relação primitiva

$$1 = \sum_{p_1^{b1} \cdot \ldots \cdot p_w^{bw} = n} 1, \ \forall n \in \mathbb{N}. \tag{4.1}$$

Este capítulo busca trazer nossas atenções para a classe de fórmulas convolutivas elementares obtidas pela análise dos coeficientes de elementos da álgebra de operações $Alg(A)$.

Consideremos, por exemplo, as identidades algébricas

$$Z \circ \sum_{n=1}^{N} \lambda_n f_n = J_2(Z) \text{ e } \sum_{n=1}^{N} \lambda_n f_n = \frac{J_2(Z)}{Z}$$

obtida por manipulações do produto de Euler,

$$J_2(Z) = \prod_p \frac{f_1}{f_1 - f_p^2} = \prod_p \frac{f_1}{f_1 - f_p} \frac{f_1}{f_1 + f_p} = Z \circ \sum_{n=1}^{N} \lambda_n f_n.$$

onde λ é a função de Lioville, que retorna para cada natural 1 ou -1, dependendo de sua quantidade total de fatores primos ser par ou ímpar, respectivamente. Os correspondentes primitivos são respectivamente

$$\sum_{a \cdot b = n} \lambda_b \begin{cases} 1, \text{ se } n = k^2, k \in \mathbb{N}; \\ 0, \text{ noutros casos, e} \end{cases}$$

$$\lambda(n) = \sum_{a^2 \cdot b = n} \mu(b).$$

A manipulação mais básica a se definir é a de potência.

4.1 Potências naturais de uma Z-função

De todas as potências de elementos de $Alg(A)$, as k-ésimas potências de uma Z-função determinam como coeficientes as funções $d_k(n) = \sum_{n_1 \cdot \ldots \cdot n_k = n} 1$, que conta a quantidade de produtos de naturais iguais a n. Escrevemos a soma destas funções entre o valores 1 e N como $D_k(N) = \sum_{1 \leq n \leq N} d_k(n)$. Úteis, também, são as funções $d_k^*(n) = \sum_{n_1 \cdot \ldots \cdot n_k = n} 1$, cujos fatores devem ser $n_i \geq 2, \forall i$. Estas funções são importantíssimas, pois carregam uma informação aritmética fina. De fato, podemos escrever

$$\begin{aligned} Z^2 &= \sum_{n=1}^{N} d_2(n) f_n = \sum_{n=1}^{N} \sum_{m=1}^{N/n} f_n f_m \\ &= \sum_{n=1}^{\sqrt{N}} \sum_{m=1}^{\sqrt{N}} f_n f_m + 2 \sum_{n=1}^{\sqrt{N}} \sum_{\sqrt{N} < m \leq N/m} f_n f_m \\ &= 2 \sum_{n=1}^{\sqrt{N}} \sum_{m=1}^{N/n} f_n f_m - \sum_{n=1}^{\sqrt{N}} \sum_{m=1}^{\sqrt{N}} f_n f_m. \end{aligned}$$

A avaliação do funcional soma em ambos os lados gera a equação

$$D_2(N) = 2 \sum_{n \leq \sqrt{N}} \lfloor N/n \rfloor - \lfloor \sqrt{N} \rfloor^2,$$

que, ao utilizarmos a estimativa conhecida para os números harmônicos, retorna a estimativa

$$D_2(N) = N \log N + (2\gamma - 1)N + \Delta(N),$$

onde $\Delta(N) = O(\sqrt{N})$. Este erro foi dado por Dirichlet, e o problema de limitar o termo de erro é conhecido como o *problema do divisor*. Hardy conjecturou que $\Delta(N) = O(N^{\varepsilon + 1/4}),\ \forall \varepsilon > 0$, e provou um resultado do tipo ω para o caso sem ε. Para $k \geq 2$, é possível obter elementarmente (TITCHMARSH, 1986, p. 313) que

$$\Delta_k(N) = O(N^{1-1/k} \log^{k-2}(N)).$$

Nota-se que $D_{k+1}(N) = \sum_{1 \leq n \leq x} D_k(x/n)$, pois $Z^{k+1} = Z \circ Z^k$, e que $D_k^*(N) = \sum_{i=0}^{k} \binom{k}{i} D_i(N)(-1)^{k-i}$, pois $(Z - f_1)^k = \sum_{i=0}^{k} \binom{k}{i} Z^i (-1)^{k-i}$.

De maneira mais marcante, podemos encontrar duas conexões entre a teoria das funções decompositoras e os números primos. A primeira decorre do fato de que[1]

[1] A expressão é válida e mesmo finita, uma vez que Z é unipotente em qualquer espaço aritmético finito nilpotente.

]

$$Z^{-1} = \frac{f_1}{Z} = \frac{f_1}{f_1 + Z - f_1} = \sum_{k=0}^{\infty}(-1)^k(Z - f_1)^k$$
$$= \sum_{k=0}^{\infty}(-1)^k \sum_{n=1}^{\infty} d_k^*(n) f_n = \sum_{n=1}^{\infty} f_n \sum_{k=0}^{\infty}(-1)^k d_k^*(n).$$

Pelo produto de Euler, isto implica imediatamente que[2]

$$\mu(n) = \sum_{k=0}^{\infty}(-1)^k d_k^*(n)$$

Ainda mais, $LN(Z)$ rende, da mesma forma,

$$\sum_{k=0}^{\infty} \frac{(-1)^k}{k} d_k^*(n) = \begin{cases} 1/k, \text{ se} n = p^k; \\ 0, \text{ noutros casos,} \end{cases} \tag{4.2}$$

conforme provaremos um pouco mais abaixo.

4.2 Algumas equações algébricas e primitivas implicadas pelo produto de Euler generalizado

Teorema 4.2.1 *A funções d_n respeitam a fórmula*

$$d_n(j) = S_{n,b_1} \cdot ... \cdot S_{n,b_w},$$

onde a fatoração de j é $j = p_1^{b_1} \cdot ... \cdot p_w^{b_w}$ e $S_{n,k}$ denota o k-ésimo número n-simplicial:

$$S_{n,k} = \binom{k+n-1}{n-1}, \ k = 0, 1, 2 \cdots, n = 1, 2, 3 \cdots .$$

Dem.: As potências de Z revelam por meio de

$$Z^n = \sum_{j=1}^{N} d_n(j) f_j$$

e do produto de Euler

[2] Reforçamos que estas somas são finitas. De fato, $d_k^*(n) = 0$, se $n < 2^k$.

$$\begin{aligned} Z^n &= \left(\prod_p \frac{f_1}{f_1 - f_p}\right)^n = \left(\prod_p \frac{f_1}{(f_1 - f_p)^n}\right) \\ &= \left(\prod_p \frac{f_1}{\sum_{l=0}^{n} \binom{n}{l}(-1)^l f_p^l}\right) \\ &= \left(\prod_p \sum_{l=0}^{N} S_{n,l} f_p^l\right) \\ &= \sum_{j=1}^{N} f_j \sum_{p_1^{b_1} \cdot \ldots \cdot p_w^{b_w} = j} S_{n,b_1} \cdot \ldots \cdot S_{n,b_w}, \end{aligned}$$

as relações

$$d_n(j) = S_{n,b_1} \cdot \ldots \cdot S_{n,b_w}.$$

Isso evidencia de forma muito clara a independência do valor dos primos particulares das decomposições.

4.2.1 Construção de Z a partir de P

Ao partirmos do produto de Euler generalizado e tirarmos o logaritmo de ambos os lados, obtemos

$$\begin{aligned} LN(Z) = LN\left(\prod_p \frac{f_1}{f_1 - f_p}\right) &= \sum_p \sum_{k=1}^{\infty} \frac{1}{k} f_p^k \\ &= \sum_{k=1}^{\infty} \frac{1}{k} \mathbf{J}_k(P). \end{aligned}$$

Note como naturalmente surge a aplicação das terceiras operações iterativas da meta aritmética de segunda nível, as $\mathbf{J}_n$. Ao retomarmos a forma original pela avaliação exponencial, chegamos à representação

$$Z = \sum_{n=0}^{\infty} \sum_{\substack{j_1 g_1 + \cdots j_w g_w = n \\ 1 \le g_1 < \cdots < g_w}} J_{g_1}(P^{j_1}) \circ \ldots \circ J_{g_w}(P^{j_w}) \cdot \frac{1}{g_1^{j_1} j_1! \cdot \ldots \cdot g_w^{j_w} j_w!},$$

Este processo pode ser generalizado a fim de isolar cada umas das contribuições de números gerados por uma quantidade fixa de primos, que será conteúdo do próximo teorema.

Teorema 4.2.2 *Podemos encontrar os elementos de F_A, denotados P_k, cujos coeficientes a_n são indicadores de n ter exatos k fatores primos, através de somas e multiplicações de potências de $\boldsymbol{J}_m(P)$, $m \in \mathbb{N}$, sendo $\boldsymbol{J}_m$ a m-ésima terceira operação aritmética iterativa da meta-aritmética de segundo nível de A. Para o obtermos, nos será útil considerar o produto*

$$K((\alpha_n), t) = \prod_{\alpha_n} \frac{1}{1 - t \cdot f_{\alpha_n}}$$

para $t \in \mathbb{R}$ ou $\mathbb{C}$. Podemos expandi-lo para a série de potências

$$K((\alpha_n), t) = \sum_{m=0}^{\infty} v_m t^m,$$

com

$$v_m = \sum_{\substack{l_i \in (\alpha_n) \\ 1 \leq i \leq m}} (f_{l_1} \circ ... \circ f_{l_m}), \quad v_0 = 1,$$

sendo os l_i ***membros iguais ou distintos de*** *(α_n), e* ***não levando em conta*** *diferenças de ordem para os termos do somatório.*

Ao mesmo tempo, obtemos

$$\ln(K(\alpha_n), t)) = \sum_{m=1}^{\infty} t^m \frac{1}{m} \sum_{\alpha_n} J_m(f_{\alpha_n}) = \sum_{m=1}^{\infty} t^m \frac{1}{m} J_m(A),$$

onde definimos, por comodidade, $A = \sum_{\alpha_n} f_{\alpha_n}$. Estamos agora em condições de recombinar a série acima retomando a exponencial. Obtemos:

$$K((\alpha_n), t) = \prod_{m=1}^{\infty} \exp\left(\frac{t^m J_m(A)}{m}\right) = \prod_{m=1}^{\infty} \sum_{k=0}^{\infty} \frac{t^{mk} J_m(A^k)}{m^k k!}$$

$$= \sum_{n=0}^{\infty} t^n h(n),$$

com

$$h(n) = \sum_{\substack{j_1 g_1 + \cdots j_w g_w = n \\ 1 \leq g_1 < \cdots < g_w}} J_{g_1}(A^{j_1}) \circ ... \circ J_{g_w}(A^{j_w}) \cdot \frac{1}{g_1^{j_1} j_1! \cdot ... \cdot g_w^{j_w} j_w!}.$$

onde a quantidade de termos somados à direita da última igualdade coincide com o ***número de partições de*** n*. Por unicidade dos coeficientes de uma série de potências, somos levados a concluir que* $v_n = h_n$*, ou seja,*

$$\sum_{\substack{l_i\in(\alpha_n)\\1\leq i\leq m}} (f_{l_1}\circ ... \circ f_{l_m}) = \sum_{\substack{j_1g_1+\cdots j_wg_w=n\\1\leq g_1<\cdots<g_w}} J_{g_1}(A^{j_1})\circ ... \circ J_{g_w}(A^{j_w})\cdot \frac{1}{g_1^{j_1}j_1!\cdot ... \cdot g_w^{j_w}j_w!}.$$

Por exemplo, tomar $n = 2$ *nos rende*

$$v_2 = \sum_{\substack{l_i\in(\alpha_n)\\i=1,\ 2.}} (f_{l_1}\circ f_{l_2}) = \frac{1}{2!}\left(\sum_{\alpha_n} f_{\alpha_n}\right)^2 + \frac{1}{2^1}\sum_{\alpha_n} J_2(\alpha_n).$$

A aplicação do problema para o caso em que a seqüência (α_n) *é a seqüência dos primos nos rede a solução para a representação dos* P_n *em função da transformação* P *sugerida. Toma assim a forma*

$$P_n = \sum_{\substack{j_1g_1+\cdots j_wg_w=n\\1\leq g_1<\cdots<g_w}} J_{g_1}(P^{j_1})\circ ... \circ J_{g_w}(P^{j_w})\cdot \frac{1}{g_1^{j_1}j_1!\cdot ... \cdot g_w^{j_w}j_w!}.$$

A teoria da função $K((\alpha_n), t)$ *gera outros resultados similares, permitindo extensa investigação combinatória. Nos limitemos a mostrar mais um exemplo de fórmulas do gênero, como a fórmula análoga obtida pela consideração da expansão em série de potências na variável* t *de* $K^{-1}((\alpha_n), t)$

$$\sum_{\substack{l_i\in(\alpha_n)\\1\leq i\leq m}} (f_{l_1}\circ ... \circ f_{l_m}) = (-1)^n \sum_{\substack{j_1g_1+\cdots j_wg_w=n\\g_1<\cdots<g_w}} J_{g_1}(A^{j_1})\circ ... \circ J_{g_w}(A^{j_w})\cdot \frac{(-1)^{j_1+\cdots+j_w}}{g_1^{j_1}j_1!\cdot ... \cdot g_w^{j_w}j_w!}.$$

desta vez sendo os l_i ***necessariamente membros distintos de*** (α_n)*, e igualmente* ***não levando em conta*** *diferenças de ordem na construção dos termos do somatório à esquerda.*

O teorema acima é uma generalização para a linguagem deste livro do teorema análogo para séries de Dirichlet, dado no meu trabalho anterior (Rolim, 2020, p. 102).

4.2.2 Z^t e os polinômios multiplicativos

Nesta subseção, utilizaremos os métodos anteriores para descrever uma curiosa classe de polinômios que emergem da exponenciação numérica de Z, a saber a família de polinômios $q_n(t)$ definida por

$$Z^t = \sum_n q_n(t) f_n.$$

É possível determinar os $q_n(t)$ perfeitamente tomando o logaritmo e retomando o exponencial com t dentro do argumento.

Outra forma de defini-los é através da descrição das d_n em termos dos números triangulares, que demos acima. Neste caso, se $n = p_1^{b_1} \cdots p_w^{b_w}$, vale

$$\begin{aligned} q_n(t) &= S_{t,b_1} \cdot \ldots \cdot S_{t,b_w} \\ &= \binom{t+b_1-2}{t-1} \cdots \binom{t+b_w-2}{t-1}. \end{aligned}$$

Para t fracionário, a combinação é interpretada adequadamente com o símbolo de Pochhammer.

Duas propriedades convolutivas satisfeitas pelos polinômios $q_n(t)$

Afirmação 4.2.1 *Sejam $t, r \in \mathbb{C}$, q_n os polinômios definidos acima. Então*

$$q_l(t+r) = \sum_{n \cdot k = l} q_n(t) q_k(r).$$

Demonstração 4.2.1 *A exponenciação de transformações comutativas respeita*

$$Z^t \circ Z^r = Z^{t+r},$$

de onde a identidade segue ao efetuarmos composição à direita e identificarmos os coeficientes de ambos os lados da equação.

Afirmação 4.2.2 *Nas mesmas condições, vale*

$$||(Z^t)'(0)|| = \sum_{k=1}^{\infty} \frac{\pi(N^{1/k})}{k^2},$$

Na norma euclidiana. Além disso,

$$q_l'(t) = \sum_{p^k \cdot n = l} \frac{q_n(t)}{k},$$

Demonstração 4.2.2 *A diferenciação em t de Z^t é $(Z^t)' = LN(Z) \circ Z^t$, de onde a primeira identidade segue ao se avaliar em $t = 0$ e retirar a norma. Como também*

$$(Z^t)' = \sum_n q_n'(t) f_n,$$

concluímos que -

$$q_l'(t) = \sum_{p^k \cdot n = l} \frac{q_n(t)}{k},$$

de onde novamente a identidade segue ao efetuarmos a composição à direita na primeira expressão e identificarmos os coeficientes de ambos os lados da equação.

4.2.3 O verdadeiro escopo das fórmulas primitivas

Se $P(X) = \sum_{n=0}^{k} a_n X^n$, então, por um lado,

$$P(Z) = \sum_{n=0}^{k} a_n Z^n = \sum_{j=1}^{N} f_j \sum_{n=0}^{k} d_n(j) a_n;$$

por outro,

$$\begin{aligned} P(Z) = P\left(\prod_p \frac{f_1}{f_1 - f_p}\right) &= \sum_{n=0}^{k} a_n \left(\prod_p \frac{f_1}{f_1 - f_p}\right)^n \\ &= \sum_{n=0}^{k} a_n \left(\prod_p \frac{f_1}{(f_1 - f_p)^n}\right) \end{aligned}$$

Teorema 4.2.3 *Vale que*

$$\sum_{k=1}^{\infty} \frac{(-1)^k}{k} d_k^*(n) = \begin{cases} 1/j, \text{ se } n = p^j, \text{ para algum } p \text{ primo, ou} \\ 0, \text{ noutros casos.} \end{cases}$$

Dem.: Como, por um lado,

$$\begin{aligned} Ln(Z) = Ln\left(\prod_p \frac{f_1}{f_1 - f_p}\right) &= -\sum_p Ln(f_1 - f_p) \\ &= \sum_{k=1}^{\infty} \frac{1}{k} J_k(P) \end{aligned}$$

e, por outro,

$$Ln(Z) = Ln(f_1 + (Z - f_1)) = \sum_{k=1}^{\infty} \frac{(-1)^k}{k}(Z - f_1)^k$$
$$= \sum_{k=1}^{\infty} \frac{(-1)^k}{k} \sum_{n=1}^{\infty} d_k^*(n) f_n = \sum_{n=1}^{\infty} f_n \sum_{k=1}^{\infty} \frac{(-1)^k}{k} d_k^*(n),$$

por unicidade dos coeficientes, a prova está terminada.

A expressão anteriora nos permite descrever a contagem ponderada de primos de Riemann $J(x)$ através da álgebra de convoluções da seqüência contante igual a 1, $\forall h \geq \lfloor \log_2(N) \rfloor$:

$$J(N) = \sum_{1 \leq k \leq h} \frac{(-1)^{k+1}}{k} \sum_{1 \leq n \leq N} \sum_{\substack{a_1 \cdot \ldots \cdot a_k = n \\ Arr;\ a_i \geq 2,\ \forall i}} 1,$$

ou ainda, a função de Mertens!

$$M(N) = 1 + \sum_{1 \leq k \leq h} (-1)^k \sum_{1 \leq n \leq N} \sum_{\substack{a_1 \cdot \ldots \cdot a_k = n \\ Arr;\ a_i \geq 2,\ \forall i}} 1.$$

A crucial função generalizada de Euler E computa convolutivamente a quantidade de partições $p(n)$ e a soma ponderada dos divisores $\sigma(n)/n$ através de, respectivamente, E^{-1} e $-LN(E)$:

$$p(n) = \sum_{1 \leq k \leq h} (-1)^k \sum_{\substack{a_1 + \ldots + a_k = n \\ Arr;\ a_i \geq 1,\ \forall i}} e_{a_1} \cdots e_{a_k},$$

$$\frac{\sigma(n)}{n} = \sum_{1 \leq k \leq h} \frac{(-1)^{k+1}}{k} \sum_{\substack{a_1 + \ldots + a_k = n \\ Arr;\ a_i \geq 1,\ \forall i}} e_{a_1} \cdots e_{a_k},$$

Sendo e_n tais que com $e_\rho \in \{1, -1\}$ e havendo quatro polinômios de segundo grau $h_i, i = 1, 2, 3, 4$ que indexam pelos naturais exatamente os pentagonais generalizados, sendo $e_\rho = -1$, se ρ é imagem de $h_1,\ h_2$, e $e_\rho = +1$, se ρ é imagem de h_3 ou h_4.

Estas fórmulas permitem a expressão destas importantes quantidades aritméticas através de funções elementares. Com algumas poucas manipulações, a expressão da contagem ponderada de primos de Riemann em potências de dois transforma-se em

$$J(2^v) = -\sum_{1\leq k\leq v}\frac{1}{k} + \sum_{1\leq k\leq v}\frac{(-1)^{k+1}}{k}\binom{v}{k}\sum_{1\leq l_1,\cdots,l_{k-1}\leq 2^v}\left\lfloor\frac{2^v}{l_1\cdot\ldots\cdot l_{k-1}}\right\rfloor.$$

A expressão correspondente para a própria contagem de primos π, obtida de J pelas fórmulas da próxima subsecção, é

$$\pi(2^v) = \sum_{1\leq l\leq v^2}\frac{1}{l}\sum_{d|l}(-1)^{l/d\ -1}\binom{v}{l/d}\mu(d)\sum_{1\leq l_1,\cdots,l_{l/d-1}\leq 2^v}\left\lfloor\frac{2^{\frac{v}{d}}}{l_1\cdot\ldots\cdot l_{l/d-1}}\right\rfloor.$$

Cada termo em l da fórmula anterior tem propriedades importantes, porque o análogo algébrico é bem comportado, conforme veremos a seguir.

4.2.4 Construção de P a partir de Z e as Lei das Fatorações Naturais

Trata-se de uma conseqüência apoiada no produto de Euler generalizado para F_A, a duplicidade de representações de uma Z-função:

$$Z = \sum_{n=1}^{N} f_n = \prod_{p\leq N}(f_1 - f_p)^{-1}.$$

Conforme vimos, isso implica em

$$LN(Z) = \sum_{k=1}^{\lfloor\log_2(N)\rfloor}\frac{1}{k}\mathbf{J}_k(P).$$

A inversão multiplicativa espacial pode ser aplicada para as terceiras operações aritméticas iterativas da meta-aritmética de segundo nível, afinal têm a propriedade multiplicativa. Isso rende, finalmente,

$$P = \sum_{k=1}^{\lfloor\log_2(N)\rfloor}\frac{\mu(k)}{k}LN(\mathbf{J}_k(Z)),$$

que determina a construção de P a partir de Z. A seguir, verificaremos algumas das conseqüências desta lei, tanto em seu aspecto combinatório, onde faremos uma conjectura, quanto a respeito de uma função indicadora de primos. Esta função, de carácter combinatório primitivo, é formulada inteiramente em termos de problemas de fatoração natural, sem referenciar a primos. Na verdade, podemos reordenar a última equação através de um índice c tal que $c = kv$, onde v é índice do polinômio de LN:

$$P := \sum_p f_p = \sum_{k=1}^{\lfloor \log_2(N) \rfloor} \mathbf{J}_k \sum_{v=1}^{\lfloor \log_2(N)/k \rfloor} \frac{\mu(k)(-1)^{v+1}}{vk}(Z - f_1)^v$$
$$= \sum_{c=1}^{\lfloor \log_2(N) \rfloor} \frac{1}{c} \sum_{k \cdot v = c} \mu(k)(-1)^{v+1} \mathbf{J}_c (Z - f_1)^v. \tag{4.3}$$

A forma exata dada acima carrega uma estrutura muito importante e, acredito, negligenciada pela história. De fato, vejamos a soma termo a termo $c = 1,\ 2, \cdots$:

$$1 \cdot \sum_{2 \le n} f_n = \sum_{2 \le n} f_n$$
$$\frac{1}{2}\left(-\left(\sum_{2 \le n} f_n \right)^2 - \sum_{2 \le n} f_n^2 \right) = - \sum_{2 \le n_1 < n_2} f_{n_1} f_{n_2} - \sum_{2 \le n} f_n^2$$
$$\frac{1}{3}\left(\left(\sum_{2 \le n} f_n \right)^3 - \sum_{2 \le n} f_n^3 \right) = \sum_{2 \le n_1, n_2, \text{ distintos}} f_{n_1}^2 f_{n_2} + 2 \cdot \sum_{2 \le n_1 < n_2 < n_3} f_{n_1} f_{n_2} f_{n_3}$$
$$\frac{1}{4}\left(-\left(\sum_{2 \le n} f_n \right)^4 + \left(\sum_{2 \le n} f_n^2 \right)^2 \right) = - \sum_{2 \le n_1, n_2, \text{ distintos}} f_{n_1}^3 f_{n_2} - \sum_{2 \le n_1 < n_2} f_{n_1}^2 f_{n_2}^2$$
$$- 3 \sum_{2 \le n_1, n_2, n_3 \text{ distintos}} f_{n_1}^2 f_{n_2} f_{n_3} - 6 \sum_{2 \le n_1 < \cdots < n_4} f_{n_1} f_{n_2} f_{n_3} f_{n_4}$$
$$\frac{1}{5}\left(\left(\sum_{2 \le n} f_n \right)^5 - \sum_{2 \le n} f_n^5 \right) = \sum f_{n_1}^4 f_{n_2} + 2 \sum f_{n_1}^3 f_{n_2}^2 + 4 \sum f_{n_1}^3 f_{n_2} f_{n_3}$$
$$+ 6 \sum f_{n_1}^2 f_{n_2}^2 f_{n_3} + 12 \sum f_{n_1}^2 f_{n_2} f_{n_3} f_{n_4}$$
$$+ 24 \sum f_{n_1} f_{n_2} f_{n_3} f_{n_4} f_{n_5}$$

Verifica-se que cada termo de (4.3) **conta certos tipos de natural com pesos inteiros**! Em outras palavras, a divisão $1/c$ é cancelada combinatorialmente de maneira não trivial![3] Para cada p-ésimo termo da soma em (4.3), este fato é equivalente ao endomorfismo de Frobënius ^{p} ser automorfismo de corpo cíclico de ordem p, inclusive destacando sozinho o caso $p = 2$, único primo par. A fórmula descreve uma estrutura reveladora, pois mostra como, de maneira natural, a relação que ocorre nos corpos cíclicos pode ser estendida para os demais anéis cíclicos, em especial aos de ordem livre de quadrados.

Através destas contagens, que principiam a contar, respectivamente, pelos números $2, 4, 12, 24, 48, 96, \cdots 2^n 3, \cdots$, **podemos decididamente dizer que existe** a função indicadora de primos através da álgebra convolutiva, análoga a fórmula (4.2), e **cujos pesos são todos números inteiros**, através das caracterizações das contagens escritas acima,

[3] Por exemplo, o caso $c = 6$.

que atribuem os pesos de acordo com a classe de número composto que o número pertence, razão pela qual escolhemos chamar esta atribuição de Lei das Fatorações Naturais.

Disto, se conclui os exemplos escritos na introdução a respeito da função contagem de primos $\pi(N)$, obtida por através da função indicadora de primos.

5 A R-álgebra simetrizada de operações

Como veremos, antes de mais nada a R-álgebra simetrizada é um R-espaço simetrizado. A noção de composição que lhe confere o carácter de álgebra deve ser construída com certos caprichos, pois composições de tamanho $2(N-1)$ dos geradores já serão suficientes para gerar toda a álgebra de matrizes $N \times N$.

5.1 Definição. Forma das composições e sua lei. Tradução espacial da sucessão circular pela nilpotente e sua adjunta.

Definição 5.1.1 *A R-álgebra simetrizada de operações é* $\boldsymbol{Alg}(A) = (E(A), +, \circ, \cdot^T)$*, ou seja,* $Alg(A)$ *dotado da operação involutiva de transposição.*

Se desejarmos, podemos falar da simetrização de cada uma das álgebras restritas a operações particulares.

Afirmação 5.1.1 *A simetrização* $\boldsymbol{S}_A$ *de* S_A *tem geradores* s *e* $s^{[-1]}$*, sendo a última a contra-sucessão de* s*. De fato,* $s^{[-1]} = s^T$*.*

É possível investigarmos $\mathbf{S}_A$ através do cálculo exato das composições entre as s_n e as $s_n^{[-1]}$. Mais precisamente, descrever as combinações de composições finitas de operações aditivas simetrizadas (nilpotentes ou enumeráveis). Estas composições são os y tais que $y = \bigcirc_{n=1}^{k} a_n$, sendo $a_n \in (\mathbf{A}_1, \circ),\ \forall n$ elemento do monóide simetrizado de somas.

Posso observar que nos basta considerar as composições cujos termos alternam-se entre os geradores. Para tanto, notemos primeiro que se houver dois a_n consecutivos tais que ambos sejam da álgebra de operações original, ou ambos da álgebra adjunta, então o termo é nulo, se a soma de seus índices for maior que $\mathrm{ord}(A)$, ou é a operação cujo índice é a soma dos índices. A conclusão é que a composição é descrita por, no máximo, $k-1$ termos alternantes (ou menos, se novamente houverem vizinhos de mesmo gerador).

Portanto, basta-nos as y **composições alternantes** de k elementos a_n, alternando-se estes ora entre pertencer a $(A_1, \circ)$, ora a $(A_1^T, \circ)$. É digno de nota que certas composições alternantes ainda podem ser reduzidas em termos, se um extremidade comportar-se como a função identidade lateral. Além disso, existem composições não nulas de k elementos, não importando a nilpotência de s e s^T em separado.

Consideremos convenientemente negativos os índices das somas transpostas, no espírito de que $s_{-1}^n(x_j) = s_n^T(x_j) = x_{j-n}$, quando $1 + n \leq j$, e nulas noutros j.

Afirmação 5.1.2 *Se* $y = \bigcirc_{n=1}^{k} a_n$ *com índices* $r_1, \cdots r_k$ *é composição alternante, então* $y = s_{l,a,b}$ *sendo* $l = l_y = \sum_n r_n$, $a = a_y = \min_t \sum_n^t r_n$, $b = b_y = \max_t \sum_n^t r_n$ *e*

$$s_{l,a,b}(x_j) = \begin{cases} s_l(x_j), \ \textit{se } \max(1, 1-a) \leq j \leq \min(N, N-b); \\ 0(), \ \textit{noutros casos.} \end{cases}$$

Em outras palavras, é algum s_l*, numa faixa, e nula fora dela. Dos geradores do caso enumerável, apenas as* s_n^T *anulam vetores (pois* $s^T(x_1) = 0$*), e portanto um elemento alternante só deixa de ser injetivo se* $a < 0$*.*

A composição das composições alternantes é bem comportada. Mais precisamente, lembremos que $s_{l,a,b}$ é nula nas primeiras $-a$ e nas últimas b colunas, mas é também nula nas primeiras $l - a$ e últimas $b - l$ linhas. Com esta noção, as mesmas limitações podem ser estipuladas para qualquer composição $s_{l,a,b} \circ s_{k,u,p} = s_{k+l,y,d}$, sendo esta posição igual a s_{k+l} limitada respectivamente nas colunas e linhas por $-u$, $p\ l - a$, $b - l$. A relação entre estes números e $l + k$ determina totalmente os y, d em mais poucos passos.

A razão de querermos limitar no número de termos aceitos é que para um número suficientemente alto de termos, $\mathbf{S}_A$ torna-se a álgebra de **todas** as matrizes $N \times N$.

Vale ainda dizer que o caso enumerável é totalmente distinto, e nunca atinge todo o espaço dos operadores, por maior que seja o número de termos da composição.

Afirmação 5.1.3 *No caso enumerável, as composições* y *cuja soma da seqüência de índices é* $l_y = 0$ *são identidades em vizinhanças do infinito, isto é, existe* $m \in \mathbb{N}$ *tal que que para todo* n *tal que* $m \leq n$*, vale* $y(x_n) = x_n$*.*

Mais que isso, $y \sim_\infty Id$. A noção de igualdade em uma vizinhança do infinito é uma relação de equivalência $\sim_\infty$ as funções que particiona o conjunto destas composições através das operações de soma e soma adjunta. Então não só vale o resultado anterior, mas, se $l_y = k$, então $y \sim_\infty s_k$. Essa equivalência mostrar que $\mathbf{S}_A$ **age de maneira simplificada em vizinhanças do infinito**, na noção de ordem de uma base enumerável.

Conjecturo, também, haver uma tendência da concentração do ruído ao redor do centro das matrizes, especialmente de composições longas, devido aos cancelamentos que ocorrem nas extremidades, em boa parte das manipulações desta álgebra, ainda que os elementos que construiremos inicialmente não os apresentem.

Teorema 5.1.1 (Tradução entre as sucessões espaciais nilpotente e circular) *A álgebra* $\boldsymbol{S}_A$ *inclui como subálgebra* $S_\circ(A)$*. Mais precisamente, se* s *e* c *são respectivamente as extensões nilpotente e circular de uma função sucessora de ordem N,*

$$c = s + s_{N-1}^T, \ e$$

$$c_n = s_n + s^T_{N-n}.$$

Isso implica

$$\sum_{n=1}^{N-1} a_n c_n = \sum_{n=1}^{N-1} a_n s_n + \sum_{n=1}^{N-1} a_n s^T_{N-n},$$

que traduz limpidamente as relações espaciais entre as c_n, s_n e s^T_n.

A importância deste teorema para a teoria é imensa, pois sendo um resultado meramente espacial, existe desde $\mathbf{S}_A$ como espaço! E permanecem estas fórmulas válidas ao tomarmos as composições com número limitado ou ilimitado de termos.

Com algumas pesquisas, descobri que as matrizes canônicas dos elementos de $\mathbf{S}_A$ já foram exatamente descritas na literatura, cunhadas como as matrizes de Toeplitz quadradas.

Mais precisamente, c gera exatamente o conjunto das matrizes circulantes. A omissão de elementos da base construída de s e s^T é chamada limitação de banda.

As equações de tradução versam sobre elementos sem componente identidade. Ao incluí-lo em ambos os lados da equação de tradução, podemos escrever

$$\sum_{n=0}^{N-1} a_n c_n = \sum_{n=0}^{N-1} a_n s_n + \sum_{n=1}^{N-1} a_n s^T_{N-n}.$$

Neste caso, obtemos a tradução completa entre as extensões circulares e nilpotentes. Denotemos as três somas acima por C, H, T. Nota-se que a diferença $C - H$, descrita pelas somas adjuntas T, permanece não incluindo a identidade! Assim T é um elemento não invertível independentemente do anel R, e de fato nilpotente, de índice mínimo N. Em outras palavras, $(C - H)^N = 0$.

5.2 Teoria vaga dos correspondentes simetrizados

Existem elementos das álgebras simetrizadas que admitem diagonalização. De fato, para cada elemento da álgebra original, há mais de uma maneira de construir elementos diagonalizáveis da álgebra simetrizada que conservam propriedades do elemento original. Do ponto de vista da estrutura combinatória dos coeficientes, a formação convolutiva original é complementada por uma estrutura maior e aparentemente mais complexa, mas que na verdade é solúvel como uma combinação dos autovalores do correspondente simetrizado. O objetivo desse processo é obter informações sobre as convoluções lineares.

De fato, essa complementação não é única, e o que caracteriza um elemento como correspondente em geral é deixado vago. No entanto, mostramos três exemplos de correspondência aditiva que preservam propriedades do elemento original em um sentido forte.

Notemos que em todos esses casos, as avaliações polinomiais dos correspondentes resultam em uma matriz da qual o correspondente da avaliação polinomial da operação original pode ser facilmente diferenciado, sendo o componente puro do resultado (cujos membros são s_n ou suas adjuntas).

Um caso de especial interesse, não aprofundado aqui, é o de uma consideração especial de norma que se estenda à S_A^T tal que $\mathbf{S}_A$ seja C_*-álgebra, estrutura bem compreendida e rica em teoremas, inclusive espectrais (FOLLAND, 1995, p. 22). Não é de meu conhecimento quais aspectos dos teoremas citados permanecem válidos mesmo se omitirmos as composições longas da álgebra, a fim de evitar que descreva todo o grupo de matrizes $N \times N$.

5.2.1 Correspondente espacial simétrico

A correspondência se trata da transformação linear $\kappa : S_{Nil}(A) \to \mathbf{S}_A$ tal que $\kappa(Id) = Id$ e $\kappa(s_n) = s_n + s_n^T$, se $n \geq 1$. Como é espacial, existe ainda que consideremos admissível apenas um número finito qualquer de composições. Assim, para $\sum_{n=1}^{N} a_n s_n = v \in S_{Nil}(A)$,

$$\kappa(v) = \sum_{n=1}^{N} a_n (s_n + s_n^T).$$

$\kappa(v)$ é simétrico, pois as matrizes $\kappa(s_n)$ são todas simétricas. Mais que isso, são exatamente a base do espaço das matrizes de Toeplitz simétricas.

As composições destas funções **não** são fechadas dentro do subespaço destas correspondentes. É possível descrever as composições e avaliações polinomiais destes elementos perfeitamente, através das leis sobre composições alternantes.

As avaliações polinomiais destas correspondentes constroem nos coeficientes do produto as somas de "potências convolutivas"dos coeficientes da variável. Esta, então, pode ser calculada rapidamente através da descrição diagonal das $\kappa(s_n)$. No entanto, neste caso não diagonalizam-se numa mesma base, ou tem os mesmos autovalores.

A descrição detalhada deste processo certamente vale a pena, mas não o calculei.

5.2.2 Correspondente iterativo

A correspondência se trata da transformação linear $\kappa : S_{Nil}(A) \to \mathbf{S}_A$ tal que $\kappa(s_n) = (s + s^T)^n$. Assim, para $\sum_{n=1}^{N} a_n s_n = v \in S_{Nil}(A)$,

$$\kappa(v) = \sum_{n=1}^{N} a_n (s + s^T)^n.$$

Novamente, comentamos que as composições destes elementos não são mais nilpotentes. Mesmo assim, neste caso, são fechadas no subespaço quando $N = \aleph_0$. Podem ser descritas perfeitamente, através das composições alternantes.

Diferentemente do caso anterior, neste caso toda $\kappa(s_n)$ é diagonalizável na mesma base e autovalores: como $\kappa(s^n) = \kappa(s)^n$, só é necessário diagonalizar $\kappa(s)$ para descrever os autovalores de todo espaço gerado por estes correspondentes, e assim todo análogo convolutivo gerado pelas avaliações polinomiais destes.

Os autovalores da função desta sucessora simetrizada são todos reais, como no caso anterior, e ligados a avaliações cossenoidais de divisão racionais do círculo. vejamos um exemplo.

Exemplo 5.2.1 *Consideremos S_A para o $\mathbb{R}$-espaço aritmético de dimensão $N = 4$. Neste caso, podemos calcular todo tipo de convolução correspondente utilizando apenas 4 números, os autovalores de $s + s^T$.*

Nesta dimensão, os autovalores são $\varphi,\ -\varphi,\ \varphi^{-1}$, e $-\varphi^{-1}$, onde φ é a proporção áurea!,

$$\varphi = \frac{1 + \sqrt{5}}{2}.$$

Como todo correspondente destes é $P(\kappa(s))$ para alguma avaliação polinomial P, obtemos que nesta dimensão todos os correspondentes tem a forma $M \times \Lambda_{P(\varphi)} \times M^{-1}$, sendo

$$M = \begin{pmatrix} -1 & 1 & -1 & 1 \\ \frac{1}{2}(1+\sqrt{5}) & \frac{1}{2}(1-\sqrt{5}) & \frac{1}{2}(1-\sqrt{5}) & \frac{1}{2}(1+\sqrt{5}) \\ \frac{1}{2}(-1-\sqrt{5}) & \frac{1}{2}(1-\sqrt{5}) & \frac{1}{2}(-1+\sqrt{5}) & \frac{1}{2}(1+\sqrt{5}) \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

$$M^{-1} = \begin{pmatrix} \frac{1}{20}(-5+\sqrt{5}) & \frac{\sqrt{5}}{10} & -\frac{\sqrt{5}}{10} & \frac{1}{20}(5-\sqrt{5}) \\ \frac{1}{20}(5+\sqrt{5}) & -\frac{\sqrt{5}}{10} & -\frac{\sqrt{5}}{10} & \frac{1}{20}(5+\sqrt{5}) \\ \frac{1}{20}(-5-\sqrt{5}) & -\frac{\sqrt{5}}{10} & \frac{\sqrt{5}}{10} & \frac{1}{20}(5+\sqrt{5}) \\ \frac{1}{20}(5-\sqrt{5}) & \frac{\sqrt{5}}{10} & \frac{\sqrt{5}}{10} & \frac{1}{20}(5-\sqrt{5}) \end{pmatrix}$$

e

$$\Lambda_{P(\varphi)} = \begin{pmatrix} P(-\varphi) & 0 & 0 & 0 \\ 0 & P(-\varphi^{-1}) & 0 & 0 \\ 0 & 0 & P(\varphi^{-1}) & 0 \\ 0 & 0 & 0 & P(\varphi) \end{pmatrix},$$

Notem como M é completamente independente de P! Isso facilita tremendamente os cálculos. Além disso, P pode ser simplificado, utilizando o fato das raízes satisfazerem as propriedades $x^2 = x + 1$ *(*φ *e* $-\varphi^{-1}$*) e* $x^2 = 1 - x$ *(*$-\varphi$ *e* φ^{-1}*).*

5.2.3 Correspondente circular

A correspondência se trata da transformação linear $\kappa : S_{Nil}(A) \to \mathbf{S}_A$ tal que $\kappa(s_n) = c_n$. Assim, para $\sum_{n=1}^{N} a_n s_n = d \in S_{Nil}(A)$,

$$\kappa(d) = \sum_{n=1}^{N} a_n c_n.$$

Já antecipamos, pelas equações de tradução (5.1.1), que $\kappa(s_n) = s_n + s^T_{N-n}$. A convolução circular passa a ser uma soma entre convoluções lineares: para cada n, $n = 1, \cdots, N$, a ação de d e $\kappa(d)$ sobre um elemento qualquer de V $\sum_{v=1}^{N} b_v x_v$ determina que

$$\sum_{v+l\equiv\ n\ mod N} a_l b_v = \sum_{v+l=n} a_l b_v + \sum_{v+l=n+N} a_l b_v,$$

sendo $1 \leq v \leq N$ em todos os casos, $0 \leq l \leq N-1$ nos dois primeiros casos e $1 \leq l \leq N-1$ no último.

A sucessão circular c é uma matriz ortogonal, e portanto diagonalizável pelo teorema espectral para estas matrizes. Satisfaz $c^N = Id$, que é de fato seu polinômio característico. Seus autovalores portanto são exatamente as N N-ésimas raízes de unidade $e^{2\pi i n/N}$, $n = 0, \cdots, N-1$.Seus N autovetores compõe a famosa matriz conhecida como matriz da **transformada de Fourier discreta** de N pontos.

Lema 5.2.3.1 (Diagonalização das matrizes circulantes) *Seja A uma aritmética finita de ordem N. Então todo elemento W de* $S_\circ(A)$ *diagonaliza em uma mesma base e, se* $\sum_{n=0}^{N-1} w_n c^n = W \in S_\circ(A)$*, seus autovalores são*

$$\lambda_{j+1} = \sum_{n=0}^{N-1} w_n e^{2\pi i n j/N},\ j = 0, \cdots, N-1,$$

a avaliação de F_N *no vetor da primeira coluna de W.*

Dem.: Todo elemento W de $S_\circ(A)$ *é* $W = \sum_{n=0}^{N-1} w_n c^n$*, a avaliação do polinômio* $P : M(N \times N) \to M(N \times N) (P(X) = \sum_{n=0}^{N-1} w_n X^n)$ *em c, a função sucessora estendida circularmente, conforme comentamos em 3.2.1. A avaliação de P na matriz diagonal dos autovalores implica que os autovalores de W são da forma* $P(e^{2\pi i n/N})$, $j = 1, \cdots, N$*. De fato, mesmo se P fosse de grau infinito, valeria o resultado, desde que P fosse analítico ao redor das raízes de unidade, pelo Teorema do Mapa Espectral.*

Toda matriz diagonal conjugada pela matriz da transformada de Fourier discreta é uma matriz circulante.

Teorema 5.2.1 (Decomposição exponencial finita das convoluções circulares) *A ação de um elemento genérico $k \in S_\circ(A)$ no espaço considerado é*

$$k(v) = \sum_{n=0}^{N-1} a_n c^n \left(\sum_{l=1}^{N} b_l x_l \right) = \sum_{j=1}^{\infty} x_j \sum_{n+l=j \mod N} a_n b_l.$$

Pela diagonalização da função sucessora e o lema anterior,

$$k(v) = \frac{1}{N} F_N^{-1} \times \Lambda \times F_N(v),$$

que tem descrição simples quando v é expressa na base de autovetores.

Em particular, m-ésimas convoluções circulares de mesmos coeficientes são descritas através de avaliações polinomiais das matrizes circulantes na primeira coluna de $k^m = \frac{1}{N} F_N \times \Lambda^m \times F_N$, e portanto

$$\sum_{l_1+\cdots+l_m=j \mod N} a_{l_1} \cdots a_{l_N} = \frac{1}{N} \sum_{b=1}^{N} \lambda_b^m e^{-2\pi i \frac{(j-1)(b-1)}{N}}.$$

Como a m-ésima potência de uma matriz determina a m-ésima convolução dos coeficientes, polinômios e séries de potências P analíticas ao redor dos autovalores determinam problemas de composições convergentes ponderadas de convoluções, que são rapidamente calculadas por

$$\frac{1}{N} \sum_{b=1}^{N} P(\lambda_b) e^{-2\pi i \frac{(j-1)(b-1)}{N}}.$$

Lema 5.2.3.2 *[Lema de redução] Sejam $z_1, \cdots, z_N$ números complexos cujas formas polares são $\rho_1 e^{i\theta_1}, \cdots, \rho_N e^{i\theta_N}$. Se $\rho_* e^{i\theta_*} = \sum_{n=1}^{N} z_n$, então*

$$\rho_* = \sqrt{\sum_{n=1}^{N} \rho_n^2 + 2 \sum_{1 \le i < j \le N} \rho_i \rho_j \cos(\theta_i - \theta_j)}, \ e$$

$$\theta_* = \frac{\sum_{n=1}^{N} \theta_n \rho_n}{\sum_{n=1}^{N} |\rho_n|}.$$

Afirmação 5.2.1 (Cálculo da norma e argumento dos autovalores envolvidos) *Seja $W \in S_\circ(A)$, sendo $R = \mathbb{R}$. A aplicação do lema anterior ao autovalores de W determina para $j = 0, \cdots, N-1$ que*

$$||\lambda_{j+1}|| = \sqrt{\sum_{n=1}^{N} w_n^2 + 2 \sum_{1 \le k < h \le N} w_k w_h \cos(2\pi j(k-h)/N)}, \ e$$

$$Arg(\lambda_{j+1}) = \frac{2\pi j \sum_{n=1}^{N} n \cdot w_n}{N \cdot \sum_{n=1}^{N} |w_n|} \mod 2\pi = j \cdot Arg(\lambda_2).$$

5.2.4 Comentários acerca da simetrização multiplicativa

Trata-se do transporte destas ideias para F_A. A simetrização resultante é tão ou mais interessante que o caso aditivo, em especial, por serem **matrizes esparsas**. Não me alongarei, no entanto, sobre este tema. É digno de nota que a simetrização espacial multiplicativa pode dar resultados. Por exemplo, a função

$$\mathbf{Z} = f_1 + \sum_{n=2}^{N} (f_n + f_n^T)$$

é diagonalizável, para todo N, e suas avaliações polinomiais estão mais fortemente ligados às avaliações polinomiais dos elementos originais, pois as matrizes $f)n^T$ apresentam um tremendo anulamento composicional com as f_n não presente no caso aditivo. É importante, portanto, investigar o problema dos autovalores de $\mathbf{Z}$ e a relação entre o problema convolutivo simetrizado e original.

Pode não ser possível investigar $LN(\mathbf{Z})$, pois podem haver autovalores negativos, mas deve ser possível investigar os autovalores de $\mathbf{Z}^{-1}$.

5.3 Representação finita de $p_\circ$ e Σ por exponenciais de freqüências pentagonais

Consideremos $p_\circ(n)$ e $\Sigma(n)$ os correspondentes convolutivos circulares das convoluções lineares aditivas que geram $p(n)$ e $\sigma(n)/n$.

É possível executar o cálculo direto destas duas funções de uma maneira agradavelmente simples, através do famoso Teorema Pentagonal de Euler e das propriedades do correspondente circular $E_\circ$ da função generalizada de Euler E_{Nil}, ao aplicarmos a decomposição exponencial finita das convoluções circulares e o lema de redução.

5.3.1 Cálculo exato dos autovalores de $E_\circ$

Em decorrência do lema da redução (5.2.3.2), o correspondente circular $E_\circ$ de ordem N da função de Euler nilpotente de ordem N E_{Nil} tem autovalores $\eta_{j+1} \in \Lambda_\eta$ $(j = 0, \cdots, N-1)$ tais que

$$||\eta_{j+1}|| = \sqrt{Q_{\rho \leq N} + 2 \sum_{1 \leq k < h \leq N,\ k,h \in P} e_k e_h \cos(2\pi j(k-h)/N)},\ e$$

$$Arg(\eta_{j+1}) = \frac{2\pi j \sum_{n=1}^{N} \rho \cdot e_n}{N \cdot Q_{\rho \leq N}} \mod 2\pi,$$

sendo $Q_{\rho \leq N} = \sum_{\rho \leq N} 1$ e os $\rho \in P$ e e_n determinados em no capítulo 4 como os números pentagonais generalizados de Euler[1], com $e_\rho \in \{1, -1\}$: quatro equações $h_i : \mathbb{N}_1 \to \mathbb{N}_1$ de segundo grau

$$\begin{aligned}
h_1(n) &= 6n^2 - 7n + 2 = (2n-1)(3n-2), \\
h_2(n) &= 6n^2 - 5n + 1 = (2n-1)(3n-1), \\
h_3(n) &= 6n^2 - n,\ e \\
h_4(n) &= 6n^2 + n
\end{aligned}$$

indexam pelos naturais exatamente os pentagonais generalizados, sendo $e_\rho = -1$, se ρ é imagem de $h_1,\ h_2$, e $e_\rho = +1$, se ρ é imagem de h_3 ou h_4.

Na ordem natural, os números formados pelas h alternam-se perfeitamente nos naturais, formando ciclos de período 4 no sinal dos coeficientes não nulos de $E_{Nil} - Id$: $-1, -1, +1, +1, \ldots$.

Cálculo no período completo

Nos é conveniente, na busca de simplificações, estudar o comportamento destes números a cada período, que fecha num número da forma h_4. Consideremos, pois, $N = h_4(k) = k^2 + k$, para algum $k \in \mathbb{N}$. Neste caso, correram-se exatamente k períodos, totalizando $4k$ números pentagonais contabilizados, de onde concluímos que

$$Q_{\rho \leq k^2+k} = 4k,\ \forall k$$

e que, como $h_3(n) + h_4(n) - h_1(n) - h_2(n) = (6n^2 - n) + (6n^2 + n) - (6n^2 - 7n + 2) - (6n^2 - 5n + 1) = 12n - 3,\ \forall n$, os ângulos simplificam-se para

[1] Sem o 0, expoente relativo à identidade

$$Arg(\eta_{j+1}) = 2\pi j \frac{(6k+3)}{4(k^2+k)} \mod 2\pi, \tag{5.1}$$

Por outro lado, as normas dos autovalores são no período completo são

$$||\eta_{j+1}|| = \sqrt{4k+2 \sum_{1\le l<h\le k^2+k,\ l,h\in P} e_l e_h \cos(2\pi j(h-l)/(k^2+k))}.$$

Não me é claro como simplificar estas normas como o fizemos para os ângulos.

5.3.2 A função partição

O elemento E_{Nil}^{-1} tem como coeficientes $p(n)$, o número de partições de n.

Como a álgebra $S_{Nil}(A)$ admite polinômio inversão $H = H_N : S_{Nil}(A)^\times \to S_{Nil}(A)$ dos elementos invertíveis $a = a_0 Id + B$, sendo B nilpotente de ordem no mínimo N, em particular no caso linear especial[2] ($a_0 = 1$), como

$$H(a) = \sum_{k=0}^{N-1} (-1)^k B^k.$$

A teoria deste capítulo nos leva a considerar a avaliação deste mesmo polinômio H no análogo circular $E_\circ$:

$$H(E_\circ) = \frac{1}{N} F_N^{-1} \times \Lambda_{H(\eta)} \times F_N, \tag{5.2}$$

sendo

$$H(\eta_n) = \sum_{k=0}^{N-1} (-1)^k (\eta_n - 1)^k,$$

e o j-ésimo coeficiente $p_\circ(j)$ de $H(E_\circ)$ na base ordenada das operações c_j, $j = 0, \cdots, N-1$ é o resultado final a se calcular.

Analisando-se a primeira coluna de ambos os lados de 5.2, obtém-se

$$p_\circ(j) = \frac{1}{N} \sum_{n=1}^{N} H(\eta_n) e^{-2\pi i \frac{j(n-1)}{N}}.$$

[2] Este caso é suficiente para E_{Nil}. De qualquer forma, o caso linear geral (a_0 invertível) segue rapidamente do especial

Não o fizemos explicitamente aqui, mas $Arg(H(\eta(n)))$ pode ser calculado aplicando novamente o lema da redução para avaliar $H(\eta_n)$ n a n, em termos de

$$H(\eta_n) = \sum_{k=0}^{N-1} (-1)^k (\eta_n - 1)^k,$$

já que sabemos exatamente $Arg(\eta_n)$ por 5.1, so necessitando de mais alguma compreensão sobre o tamanho das normas para atingir o cálculo efetivo de $p_\circ(j)$.

5.3.3 A função soma dos divisores

A avaliação logarítmica de E_{Nil} tem como coeficientes $\sigma(n)/n$. Procedendo com uma análise análoga a acima, verifica-se que a álgebra $S_{Nil}(A)$ admite polinômio logarítmico $G = G_N : S_{Nil}(A)^\times \to S_{Nil}(A)$ dos elementos invertíveis $a = a_0 Id + B$, que no caso linear especial ($a_0 = 1$) é como

$$G(a) = \sum_{k=1}^{N-1} \frac{(-1)^{k+1}}{k} B^k.$$

A teoria deste capítulo nos leva a considerar a avaliação deste mesmo polinômio G no análogo circular $E_\circ$:

$$G(E_\circ) = \frac{1}{N} F_N^{-1} \times \Lambda_{G(\eta)} \times F_N,$$

sendo

$$G(\eta_n) = \sum_{k=1}^{N-1} \frac{(-1)^{k+1}}{k} (\eta_n - 1)^k,$$

e o j-ésimo coeficiente Σ_j de $G(E_\circ)$ na base ordenada das operações c_j, $j = 0, \cdots, N-1$ é

$$\Sigma_j = \frac{1}{N} \sum_{n=1}^{N} G(\eta_n) e^{-2\pi i \frac{j(n-1)}{N}},$$

podendo os $G(\eta_n)$, assim como os $H(\eta_n)$, ser finitamente calculados, em especial pelo lema de redução, que provavelmente ainda pode ser aprimorado quanto ao resultado da norma.

6 $\mathbb{C}$-espectros de grupos finitos, R_{ext}-espectros e extração de informações aritméticas dos grupos de operações aritméticas invertíveis.

Este capítulo é dividido em duas seções, e a proposta de um problema.

A **primeira seção** é uma breve exposição sobre $\mathbb{C}$-espectros de funcionais especiais restritos de $Alg(A)$ a $Alg(A)^{\times}$, em particular à imagem espectral da Z^{-1}-função, que recupera trigonometricamente $M(N)$, M a função de Mertens, quando A é aritmética finita nilpotente[1]. Nos apoiamos em Folland (1995) para o caso em que os grupos são abelianos localmente compactos, em especial gerados por R subanel unitário de $\mathbb{C}$.

A **segunda seção** é uma generalização da teoria de caracteres sobre grupos finitos de contradomínio complexo tal como exposto em Babai (2002) para imagens em extensões integrais de domínios de integridade R (em especial sobre corpos finitos, afinal todo domínio finito é corpo). Isso foi feito por mim a fim de aplicar a teoria aos grupos comutativos $(S_A^{\times}, \circ)$, $(F_A^{\times}, \circ)$, restritas das funções invertíveis da álgebra de operações Alg(A) com respeito à composição de funções, e seus subgrupos, e implicaria em representações trigonométricas para os próprios funcionais restritos de $Alg(A)$.

Isso se mostrou impossível, porque $(|S_A^{\times}|) = (|R|)^{N-1}$, $(|R|) = |R| \mod c \equiv 0$, onde c é a característica de R. Considero que uma topologia sobre o fechamento algébrico do corpo de frações do anel R, induza uma topologia sobre $S_A^{\times}$, agora grupo topológico, e permita a convergência das representações trigonométricas de funcionais restritos de S_A. De toda forma, isso nos distanciou das pretensões finitistas.

Proponho, pois o **problema**: existe uma forma de construir uma representação trigonométrica finita dos funcionais $f : S_A \to R$ de S_A, para R finito?

6.1 $\mathbb{C}$-espectros de funcionais restritos de Alg(A) a $Alg(A)^{\times}$

Afirmação 6.1.1 *Seja R domínio finito comutativo com unidade*[2]*, seja A uma aritmética finita nilpotente. Então o grupo* $(Alg(A)^{\times}, \circ)$ *das operações invertíveis com respeito a composição é finito.*

---

[1] Até agora, as únicas pessoas que viram este resultado estavam na primeira sessão da palestra de teoria dos números do IV CBJM, em Agosto de 2022, assim como algumas conjecturas sobre a representação trigonométrica dos funcionais.

[2] Domínios nos livram de discursar sobre divisores de zero. É uma investigação possível, a de generalizar para anéis mais gerais.

Com $\mathbb{C}$-espectro, queremos dizer a imagem de caracteres $\chi : S_A^\times \to \mathbb{C}$ e a representação trigonométrica das funções $f \in \mathbb{C}^G$.

Verifica-se em poucas páginas a total validez das transformadas de Fourier abstratas, finitas, de imagem complexa, sobre grupos abelianos finitos (BABAI, 2002). Como generalizaremos essa noção para o R-espectro na próxima seção, nela exporemos com detalhe as definições e argumentos de Babai. Aqui, basicamente expomos que a teoria de caracteres sobre estes grupos leva à conclusão que toda $f \in \mathbb{C}^G$ pode ser escrita como uma única combinação linear de caracteres (rep. trigonométrica),

$$f = \sum_{\chi \in \widehat{G}} c_\chi \chi$$

cujos coeficientes podem ser explicitamente calculados pela transformada $\hat{f} : \widehat{G} \to \mathbb{C}$ tal que

$$\hat{f}(\chi) = |G| c_{\overline{\chi}} = \sum_{a \in G} f(a)\chi(a),$$

isto é,

$$f = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\overline{\chi},$$

e mais: $G \cong \widehat{G}$, no caso finito.

Se A é aritmética finita nilpotente e R é anel finito comutativo com unidade, os grupos $S_A^\times$ e $F_A^\times$ existem e são comutativos. Neste caso, a teoria da representação trigonométrica pode descrever as funções em $\mathbb{C}$ livremente definidas sobre os grupos de operações aritméticas. Assim, é possível extrair informações de todos esses grupos. Apesar disso, não é possível recuperar diretamente os funcionais de S_A com a representação. Isso será possível a seguir, no caso infinito, quando o próprio R é subanel de $\mathbb{C}$.

Por outro lado, a teoria aritmética desenvolvida no presente texto pode adaptar-se a anéis de qualquer natureza, mesmo infinitos. Basta escolhermos os anéis adequados para que os grupos $S_A^\times$, $F_A^\times$ tornem-se compactos, ou abelianos e localmente compactos, ambientes próprios da análise harmônica abstrata; todos estes argumentos são sustentados por Folland (1995), dentro da teoria da dualidade de Pontrjagin.

Seja $M(G)$ o conjunto das medidas de Radon complexas definidas em G. Se $\mu \in M(\widehat{G})$, $\phi_\mu(x) = \int \chi(x) d\mu(\chi)$ é uma função limitada contínua (1995, p. 94). Seja $B(G) = \{\phi_\mu : \mu \in M(\widehat{G})\}$.

Teorema 6.1.1 *Seja $f \in B(G) \cap L_1(G)$, então $\hat{f} \in L_1(\widehat{G})$. Além disso, se a medida de Haar $d\xi$ em $\widehat{G}$ é adequadamente normalizada em relação a dada medida de Haar dx em G, vale $d\mu_f(\xi) = \hat{f}(\xi)d\xi$, ou seja,*

$$f(x) = \int_{\widehat{G}} \xi(x)\hat{f}(\xi)d\xi. \quad (1995, p.97)$$

Na verdade, a transformada de Fourier assim definida pode ser identificada com o espectro homomórfico de $L^1(G)$ com operação de soma convencional, e multiplicação como convolução sobre todo o grupo (1995, p. 88).

Afirmação 6.1.2 *Se G é compacto e a medida de Haar é escolhida tal que $|G| = 1$, a medida dual em $\widehat{G}$ é a de contagem. Se G é discreto e a medida de Haar é escolhida como a de contagem, a medida dual em $\widehat{G}$ é a tal que $|\widehat{G}| = 1$.*

Teorema 6.1.2 *Se $f \in L^1(G)$ e $\hat{f} \in L^1(\widehat{G})$, então*

$$f(x) = \int \xi(x)\hat{f}(\xi)d\xi$$

para quase todo x. Se f é contínua, a fórmula vale para todo x. Todas estas representações são únicas (1995, p. 102-103).

O teorema de Plancherel é generalizado para funções $f \in L^1(G) \cap L^2(G)$, valendo

$$\int f(x)^2 dx = \int \hat{f}(\xi)^2 d\xi.$$

Além disso, $\widehat{G}$ forma uma base ortonormal para $L^2(G)$, quando G é compacto e $|G| = 1$ (1995, p. 100).

Podemos assim garantir o seguinte teorema, aplicando a teoria às estruturas algébricas descobertas no presente texto.

Lema 6.1.0.1 *Seja R subanel unital de $\mathbb{C}$. Seja A aritmética finita. Então $S_A^\times$, $F_A^\times$ é grupo abeliano localmente compacto.*

Teorema 6.1.3 *Seja A R-espaço aritmético finito nilpotente. Seja $R \subset \mathbb{C}$ subanel unital completo. Então os funcionais contínuos $f \in L^1$ sobre S_A (F_A) restritos a $S_A^\times$ ($F_A^\times$) tais que $\widehat{f} \in L^1(\widehat{G})$, respeitam* [3]

[3] Reconsidero este importante teorema como incompleto, afinal os funcionais não são propriamente $L^1(G)$. Não retornei a este problema, apenas imaginei se a álgebra convolutiva das medidas complexas de Radon $M = M(G)$, como em Folland (1995, p. 94)., poderia fornecer a linguagem necessária para a expressão das relações intuídas nestas integrais.

$$f(x) = \int_{\xi \in \widehat{G}} \xi(x)\hat{f}(\xi)d\xi$$

para todo $x \in S_A$ *(*F_A*).*

A transformada de Fourier tem a forma

$$\hat{f}(\xi) = \int \overline{\xi(x)} f(x)dx.$$

Para $S_A^\times$*, conforme estabelecido pela forma inversa da inversão compositiva (3.3.1), existem* $b_i \in R$ *tais que* $a = \bigcirc_{i=1}^{N-1}(s_0 - b_i s_i)$*, com* $a_n = \sum_{v_1+\cdots+v_w=n}(-1)^w b_{v_1}\cdots b_{v_w}$*, particionando-se* n *em* v_i *distintos entre si,* $v_i \in \mathbb{N}_1$*,* $\forall i$*. As imagens possíveis dos caracteres são determinadas por* $\chi(a) = \prod_{i=1}^{N-1}\chi(s_0 - b_i s_i)$ *e pelos expoentes encontrados em na afirmação (3.5.1), quando finitos. Isso nos leva a*

$$\begin{aligned}\hat{f}(\xi) &= \int_{a\in S_A^\times} f(a)\xi(a)d\mu(a) \\ &= \int_{(b_1,\cdots,b_{N-1})\in R^{N-1}} \prod_{k=1}^{N=1}\chi(s_0 - b_k s_k)\sum_{n=0}^{N-1} f(s_n)a_n d\mu(a).\end{aligned}$$

No caso linear geral, notem que a linearidade de f implica que, para estas $\hat{f}$, vale

$$\int_{\xi\in\widehat{G}} \xi(x)\hat{f}(\xi)d\xi + \int_{\xi\in\widehat{G}} \xi(y)\hat{f}(\xi)d\xi = \int_{\xi\in\widehat{G}} \xi(x+y)\hat{f}(\xi)d\xi,\ \forall x, y \in S_A^\times,$$

curiosamente apresentando uma espécie de semilinearidade nos caracteres.

Além disso, esta transformada comporta-se exatamente como os homomorfismos da álgebra L_1 com multiplicação convolutiva (FOLLAND, 1995, p. 88).

Neste sentido, seria interessante que calculássemos a convolução entre as nossas funções de interesse, as funções de G em $\mathbb{C}$ que são restrições dos funcionais de S_A.

Em decorrência da proposição 4.4 de Folland (1995, p. 89), notemos que se G é compacto, $\widehat{G}$ é discreto, e a representação trigonométrica complexa dos funcionais de $Alg(A)$ é um somatório discreto.

6.1.1 Análise das transformada para as subálgebras de cada andar de operações A_k

Os funcionais coeficientes restritos aos elementos invertíveis da álgebra de operações

Tratemos aqui dos funcionais k_n em S_A e F_A que retornam o enésimo coeficiente a_n da representação das transformações nas respectivas bases aditivas e multiplicativas, restritos

ao elementos invertíveis destas álgebras. Notemos que é integrável sobre G, desde que expandindo o domínio de integração simetricamente desde a identidade. Sua transformada de Fourier abstrata é[4]

$$\widehat{k_n}(\chi) = \int_{a \in S_A^\times} a_n \xi(a) d\mu(a),$$

onde $a_n = \sum_{v_1+\cdots+v_w=n} (-1)^w b_{v_1} \cdots b_{v_w}$, e sua representação trigonométrica é

$$k_n(a) = \int_{\xi \in \widehat{S_A^\times}} \xi(a) \hat{f}(\xi) d\xi.$$

Fórmulas análogas valem para $F_A^\times$.

O funcional soma

O funcional soma ocorreu naturalmente na teoria das séries de Dirichlet e exponenciais, em geral. Pode ser descrito simplesmente como $h = \sum_{n=0}^{N-1} k_n$, no caso aditivo, e $h = \sum_{n=1}^{N} k_n$, no multiplicativo.

Representações trigonométricas da função de Mertens

Teorema 6.1.4 *Vale*

$$M(N) = \int_{\xi \in \widehat{F_A^\times}} \frac{\widehat{h}(\xi)}{\xi(Z)} d\xi.$$

Demonstração 6.1.1 *A aplicação do funcional soma h ao elemento $Z^{-1} \in F_A^\times$ rende o valor $M(N)$, para qualquer R subanel unital completo de $\mathbb{C}$, segundo o teorema 6.1.3. A cada caractere, temos $\xi(Z^{-1}) = \xi(Z)^{-1}$. Aplicando estes fatos à transformada inversa que há pouco vimos, segue a fórmula.*

Representações trigonométricas da soma $\sigma(N)$ dos divisores de N

Vale $\Sigma := -\sum_{n=1}^{N-1} \frac{\sigma(n)}{n} s^n = LN(E) = \sum_{n=1}^{h} \frac{(-1)^{n+1}}{n} (E - f_1)^k$, $\forall h \geq \lfloor \log_2(N) \rfloor$, sendo que $(E - f_1)^k = (-1)^k s_0 + \sum_{i=1}^{k} \binom{k}{i} E^i (-1)^{k-i}$. Como $E \in S_A^\times$, podemos calcular seus coeficientes como

$$k_n(E) = \int_{\xi \in \widehat{S_A^\times}} \hat{k}_n(\xi) \prod_{n=1}^{N-1} \chi(s_0 - s^n) d\xi.$$

[4] Nota pós-defesa: estes resultados, derivados nos últimos dias do desenvolvimento desta dissertação, estão incompletos. De fato, não há garantia de que a tomada simétrica do domínio de integração, analogamente ao "sentido de Cauchy"de certas integrais, resolva o problema da função não ser diretamente L_1. Portanto a aplicação da teoria harmônica para a representação dos funcionais ficou comprometida, a ser consertada, se possível, em trabalhos futuros.

Representação trigonométrica das contagens de fatores naturais

Teorema 6.1.5 *Vale*

$$D_k(N) = \int_{\xi \in \widehat{F_A^\times}} \hat{h}(\xi)\xi(Z)^k d\xi.$$

Dem.: Simples soma de coeficientes de Z_k.

Quantidade ponderada de primos de Riemann

A relação entre o comportamento espacial e o compositivo de Z rende primitivamente

$$J(N) = \sum_{k=1}^{h} D_k^*(N),$$

forall $h \geq \log_2(N)$. Já $(Z - f_1)^k = (-1)^k f_1 + \sum_{i=1}^{k} \binom{k}{i} Z^i (-1)^{k-i}$ rende primitivamente

$$D_k^*(N) = (-1)^k + \sum_{i=1}^{k} \binom{k}{i} D_i(N)(-1)^{k-i}.$$

O resultado anterior confere

$$J(N) = \sum_{k=1}^{h} \left((-1)^k + \sum_{i=1}^{k} \binom{k}{i} (N)(-1)^{k-i} \int_{\xi \in \widehat{F_A^\times}} \hat{h}(\xi)\xi(Z)^i d\xi \right).$$

6.2 R_{ext}-espectros

6.2.1 Desenvolvimento de representações trigonométricas de elementos de R_{ext}^G

Dado um espaço aritmético nilpotente sobre R como acima, suas subálgebras aditiva S_A ou multiplicativa F_A são abelianas. Os grupos $(S_A^\times, \circ)$, $(F_A^\times, \circ)$ contidos nas subálgebras são subgrupos abelianos de $(\mathrm{Alg}(A)^\times, \circ)$, finitos.

Lema 6.2.1.1 (Teorema fundamental dos grupos abelianos finitos) *Para cada grupo abeliano finito é possível construir uma soma direta de anéis cíclicos a ele isomorfa. Existe uma única soma direta de grupos cíclicos de ordem da potência de primos que é a ele isomorfa, na ordem dos naturais.*

Funcionais lineares das álgebras de operações para os anéis R podem fornecer informações ou representações dos coeficientes nas bases dos espaços de operações. Representações destes funcionais através da teoria de caracteres são interessantes, à medida que estes se distribuem em relação à composição entre operações aritméticas, por exemplo os $\chi : (S_A^{\times}, \circ) \to (R^{\times}, \cdot)$ de $(R, +, \cdot)$ tais que $\chi(a \circ b) = \chi(a) \cdot \chi(b)$ e $\chi(Id) = 1_R$.

Cada elemento a de um grupo abeliano finito G tem ordem finita m_a menor natural tal que $a^{m_a} = Id \in G$. Assim certamente sua imagem através de um caractere de G em um domínio R com unidade 1_R é

$$\chi(a)^{m_a} = \chi(a^{m_a}) = \chi(Id) = 1_R, \tag{6.1}$$

isto é, $\chi(a)$ é uma raiz da unidade de R.

Chamaremos de **principal** o caractere χ_0 tal que $Im(\chi_0) = \{1_R\}$.

De fato, a depender das soluções da equação (6.1), o caractere principal é o único caractere possível com imagem em R. Em outras palavras, R pode não ter raízes da unidade 1_R suficientes para que caracteres não principais com imagem em R possam existir, dado G. Conforme mostraremos, a existência destes caracteres não principais permite representar todos os elementos de alguns conjuntos R^H, H grupo, mas, por exemplo, falha em representar as funções de um grupo abeliano finito H qualquer para R precisamente se os H têm decomposição fundamental que envolva grupos cíclicos não representáveis pelas raízes de unidade de R.

Isso nos motiva a estender integralmente o anel R de forma a incluir as raízes capazes de representar os subgrupos cíclicos desejados. Neste sentido, pode-se optar por robustez ou economia. No primeiro caso, a consideração do fecho integral do anel de frações de R certamente tem raízes suficientes para representar muito mais do que o necessário para o exemplo atual, sobre grupos abelianos finitos G. No segundo, se admite uma extensão integral de R artesanalmente, apenas sobre algumas raízes de unidade, a fim de representar no anel estendido somente os elementos necessários para representar a decomposição cíclica dos G, em particular dos $(S_A^{\times}, \circ)$, $(F_A^{\times}, \circ)$, em um anel $R_{ext} = R_{ext}(G)$. É este sentido, o econômico, o que gostaríamos de empregar aqui.

Para avançarmos sobre o problema, devemos (1) mostrar algumas propriedades dos caracteres, como comportamentos dos caracteres não principais, o conjunto dos caracteres como grupo, e o respeito dos caracteres à decomposição dos grupos por somas diretas; (2) resolver o problema de representação trigonométrica de funcionais das álgebras aditivas e multiplicativas $(S_A^{\times}, \circ)$, $(F_A^{\times}, \circ)$; (3) Definir a transformada abstrata de Fourier e sua inversa, e investigar a representação de funcionais lineares $g : S_A \to R$ (ou F_A) estendidos a $g : S_A \to R_{ext}$, elementos de $R_{ext}^{(S_A^{\times}, \circ)}$, em especial o funcional soma sobre uma Z-função inversa.

Conforme adiantamos no início do capítulo, os objetivos 3 e 4 não sem mostraram diretamente possíveis na perspectiva finitista.

Definição 6.2.1 *Aqui consideramos como caractere de G um homomorfismo $\chi : (G, +) \to (R_{ext}^{\times}, \cdot)$.*

A imagem de qualquer caractere é raiz da unidade de A:

$$\chi(a)^n = \chi(n \cdot a) = \chi(0_G), \quad \forall a \in G.$$

Por conveniência, destacamos o caractere $\chi_0(a) = 1, \ \forall a \in G$ como **principal**.

Proposição 6.2.1 *Para todo caractere não principal χ de G,*

$$S := \sum_{a \in G} \chi(a) = 0.$$

Demonstração 6.2.1 *Como χ é não principal, existe $b \in G$ tal que $\chi(b) \neq 1$. Assim*

$$\chi(b) \cdot S = \sum_{a \in G} \chi(b) \cdot \chi(a) = \sum_{a \in G} \chi(a + b) = S,$$

e $S(\chi(b) - 1) = 0$, e portanto $S = 0$, afinal R é domínio.

O conjunto $\widehat{G}$ de caracteres forma naturalmente um grupo $(\widehat{G}, \cdot)$ com a operação herdada da multiplicação do anel, chamado de *Grupo Dual de G*. De fato se χ, ψ são caracteres de G, então podemos definir

$$(\chi\psi)(a) := \chi(a)\psi(a).$$

A associatividade da operação é imediata. Além disso, $(\chi\psi)(a + b) := \chi(a + b)\psi(a + b) = \chi(a)\psi(a)\chi(b)\psi(b) = (\chi\psi)(a)(\chi\psi)(b)$, e portanto a operação é fechada no grupo de caracteres. Se $\overline{\chi}(a) := \chi(-a), \ \forall a \in G$, é fácil notar que $\overline{\chi}$ é um caractere que satisfaz $\chi\overline{\chi} = \chi_0$, mostrando que $(\widehat{G}, \cdot)$ é mesmo um grupo.

Corolário 6.2.1 *Sejam χ e ψ dois caracteres de G. Então*

$$\sum_{a \in G} \overline{\chi(a)}\psi(a) = \begin{cases} (|G|), \ \textit{se } \chi = \psi; \\ 0, \ \textit{noutros casos}, \end{cases}$$

sendo $(|G|) = \sum_{g \in G} 1_R$.

Dem.: O caso $\chi = \psi$ decorre do fato de ser $\chi(-a)\chi(a) = \chi(0) = 1$.

Se $\chi \neq \psi$, então $\overline{\chi}\psi$ é um caractere não principal, e o resultado segue da proposição 6.2.1.

Esse corolário, generalização do resultado em $\mathbb{C}$-espectros, mostra uma grande diferença no caso da igualdade de caracteres, afinal ($|G|$) pode não ser elemento invertível de R, ou pior[5], pode ser 0.

A proposição a seguir é possível graças à existência das raízes de unidade necessárias para a representação de G em R_{ext} ("n"é tomado como cardinalidade de um dos grupos cíclicos da decomposição de G).

Proposição 6.2.2 *Seja $j \in \mathbb{Z}$, ω uma raiz de unidade n-ésima primitiva de R_{ext}. Então o mapa $\chi_j : \mathbb{Z}_n \to R_{ext}^{\times}$ tal que $\chi_j(\bar{a}) = \omega^{ja}$ satisfaz:*

i) $\chi_k = \chi_j$ se, e somente se, $j \equiv k \mod n$;

ii) $\chi_j = \chi_1^j$;

iii) $\widehat{\mathbb{Z}}_n = \{\chi_0, \cdots, \chi_{n-1}\}$;

Demonstração 6.2.2 *Demonstremos apenas **iii**. De fato, se χ é caractere qualquer de $\widehat{\mathbb{Z}}_n$, sabemos que sua imagem é n-ésima raiz de unidade. Desta forma, há j tal que $0 \leq j \leq n-1$ e $\chi = \chi_j$, mostrando que todos os seus caracteres são dessa forma.*

Corolário 6.2.2 *A afirmação anterior nos permite concluir que*

$$\mathbb{Z}_n \cong \widehat{\mathbb{Z}}_n,$$

afinal

$$\chi_j\chi_l(a) = \omega^{(j+l)a}, \ \forall a \in G$$

estabelece um isomorfismo de grupos, através dos elementos $\chi_j \cdot \chi_l$ e $\overline{j} + \overline{l}$.

Proposição 6.2.3 *Se $G = H_1 \oplus H_2$ e h_i é um caractere de H_i, então $\chi = h_1 \oplus h_2$ tal que*

$$\chi(a_1, a_2) = h_1(a_1) \cdot h_2(a_2)$$

é um caractere de G, e todos seus caracteres são dessa forma. Assim $\widehat{G} = \widehat{H_1} \oplus \widehat{H_2}$.

[5] Como foi o caso com $S_A^{\times}$, etc

Demonstração 6.2.3 *Se χ é um caractere qualquer de G, $\chi(a+b,c) = \chi(a,c)\chi(b,c)$ para qualquer $c \in H_2$, e portanto sua restrição a H_1 se comporta como um caractere deste. O mesmo se dá para a segunda entrada, e verifica-se sem demora a forma dos caracteres de G.*

Corolário 6.2.3 *Vale*

$$G \cong \widehat{G}.$$

Demonstração 6.2.4 *Pelo teorema fundamental dos grupos abelianos finitos, temos que G é congruente a uma soma direta de grupos cíclicos cujas ordens são potências de primos $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. Pelas proposições anteriores $\widehat{G} \cong \widehat{\mathbb{Z}}_{n_1} \oplus \cdots \oplus \widehat{\mathbb{Z}}_{n_k}$, e o corolário segue.*

Se consideramos $R_{ext}^G = \{f : G \to R_{ext}\}$ equipado com a soma induzida da soma em R_{ext} de suas imagens e com a multiplicação por escalares do anel, R_{ext}^G se torna um módulo livre de dimensão G. Quando $(|G|)$ é invertível em R, podemos definir um produto interno pela equação[6]

$$(f,g) = \frac{1}{(|G|)} \sum_{a \in G} \overline{f(a)} g(a).$$

Teorema 6.2.1 *$\widehat{G}$ forma uma base ortonormal de R_{ext}^G.*

Demonstração 6.2.5 *A ortogonalidade decorre do corolário (6.2.1). Pelo corolário (6.2.3), $|\widehat{G}| = |G| = \dim(R_{ext}^G)$. Assim $\widehat{G}$ é um conjunto linearmente independente de cardinalidade igual a dimensão do espaço, e portanto uma base do espaço.*

Também é possível estabelecer relações de ortogonalidade duais.

Afirmação 6.2.1 *Sejam $a, b \in G$. Então*

$$\sum_{\chi \in \widehat{G}} \overline{\chi}(a)\chi(b) = \begin{cases} (|G|), & \text{se } a = b; \\ 0, & \text{noutros casos.} \end{cases}$$

[6] O leitor atento pode perceber que não definimos o conjugado sobre os caracteres, e não toda função f. No entanto, é possível estender naturalmente o conjugado para toda $f : G \to R_{ext}$, uma vez que são combinações de caracteres.

6.2.2 A "transformada de Fourier"de grupos através de caracteres em domínios estendidos

A conclusão das afirmações anteriores é que toda função $f \in R_{ext}^G$ pode ser escrita como

$$f = \sum_{\chi \in \widehat{G}} c_\chi \chi.$$

Esta representação, chamada trigonométrica, tem seus coeficientes determinados como

$$c_\chi = (\chi, f)$$

por ortonormalidade. A transformada de Fourier abstrata é definida em $\widehat{G}$ por meio desta expressão para os coeficientes como

$$\hat{f}(\chi) = (|G|) \cdot c_{\overline{\chi}} = \sum_{a \in G} f(a)\chi(a).$$

O estudo dos valores desta transformada, quando passível de execução, pode revelar informações importantes a respeito da função f, uma vez que a representação trigonométrica é o mesmo que a transformada inversa

$$f = \frac{1}{(|G|)} \sum_{\chi \in \widehat{G}} \hat{f}(\overline{\chi})\chi,$$

quando $(|G|)$ é invertível.

Aplicação aos funcionais de S_A

A aplicação da teoria diretamente a S_A ou F_A não é possível, desde que a característica de R divide a ordem destes grupos.

Como coloquei, considero que uma topologia sobre o fechamento algébrico R do corpo de frações do anel R, induza uma topologia sobre $S_A^\times$, agora grupo topológico, e permita a convergência das representações trigonométricas de funcionais restritos de S_A. Em particular, seriam finalmente obtidas representações dos funcionais com imagem no anel original R. Como a teoria exige anéis infinitos, são de toda forma tratados pela próxima seção.

6.2.3 Prováveis fórmulas análogas para anéis infinitos

Todo grupo localmente compacto admite uma medida de Haar à esquerda, segundo o teorema 2.10 em Folland (1995, p. 37). A medida tem imagem real, positiva. Para a teoria

aqui desenvolvida, seria importante que a imagem da medida se encontrasse em R_{ext}. Como isso pode não ser garantido, a perspectiva do fechamento algébrico $\mathbf{R}$ do corpo de frações de R resolve o problema, e acredito ser possível transportar a teoria das medidas de Haar sem problemas para medidas com imagem em $\mathbf{R}$. No entanto não confirmei a hipótese.

É claro que uma noção de compacidade local do anel unital $\mathbf{R}$ provavelmente implica diretamente na compacidade local dos grupos das transformações aritméticas invertíveis, sejam circulares ou nilpotentes (ou mesmo uma adaptação da norma de Banach em S_A).

O caso infinito **precisa ser investigado**. A aplicação de uma norma de Banach nestas álgebras deve ser suficiente para expressar as condições de convergência no infinito. Mais ainda, deve-se estudar o espectro de homomorfismos, cujos núcleos são exatamente os ideais maximais da álgebra.

Quando R é abeliano, os grupos de composição de elementos invertíveis das álgebras restritos a uma operação aritmética são abelianos. A teoria das transformadas de Fourier sobre grupos $G = S_A^\times$ ou $G = F_A^\times$ abelianos localmente compactos (sendo o espaço aritmético $\mathbf{R}$-módulo), permite representar os funcionais $f : Alg(A) \to \mathbf{R}$ restritos a G através do espectro em R, dos caracteres $\chi : G \to \mathbf{R}$. Em vista da forma inversa da inversão compositiva aditiva (3.3.1), as equações passam a ter a forma

$$\begin{aligned}\hat{f}(\chi) &= \int_{a\in S_A^\times} f(a)\chi(a)d\mu(a) \\ &= \int_{(b_1,\cdots,\ b_{N-1})\in\mathbf{R}^{N-1}} \prod_{k=1}^{N=1} \chi(s_0 - b_k s_k) \sum_{n=0}^{N-1} f(s_n)a_n d\mu(a),\end{aligned}$$

com

$$a_n = \sum_{v_1+\cdots+v_w=n} (-1)^w b_{v_1}\cdots b_{v_w},\ e$$

$$f(a) = \int_{\chi\in\widehat{S_A^\times}} \widehat{f}(\chi)\chi(a)d\nu(\chi).$$

onde μ é a medida de Haar em $S_A^\times$ e ν é a medida de Haar induzida em $\widehat{S_A^\times}$.

7 Análise assintótica para a contagem ponderada de primos conforme a teoria de resíduos complexos

Apesar deste capítulo utilizar técnicas da análise complexa fora do escopo da aritmética desenvolvida no livro, um de seus passos chave envolve a mudança de paradigma de perguntas sobre fatoração prima para perguntas sobre fatoração natural, tal como elaborado no capítulo 4, culminando na Lei das Fatorações Naturais. De fato, foi através da representação da inversa de $\zeta(s)$ por suas potências naturais que obtivemos os resultados principais deste capítulo, todos do segundo semestre de 2020, ainda na minha graduação.

Conforme vimos, a expressão primitiva para a contagem ponderada de primos é

$$J(x) = \sum_{1\leq k\leq h} \frac{(-1)^{k+1}}{k} \sum_{1\leq n\leq x} \sum_{\substack{a_1\cdot\cdots\cdot a_k=n \\ Arr;\ a_i\geq 2,\ \forall i}} 1 \ = \ \sum_{1\leq k\leq h} \frac{(-1)^{k+1}}{k} D_k^*(x), \tag{7.1}$$

sendo os $a_i \geq 2$ e h qualquer número tal que $h \geq \lfloor \log_2(x) \rfloor$, uma vez que $k > \log_2(x)$ implica $D_k^*(x) = 0$.

7.0.1 Aproximação das funções decompositoras

As funções decompositoras $D_k^*(x)$ podem ser aproximadas por simetrias existentes na fatoração natural dos naturais em ordem. Estas aproximações podem variar na precisão, desde a mais elementar

$$D_k^*(x) \sim x\frac{\ln^{k-1}(x)}{(k-1)!}; \tag{7.2}$$

à aproximação $W_k(x)$ pelo problema hiperbólico contínuo, de erro $E_k(x)$

$$\begin{aligned} D_k^*(x) &= \int_1^x \int_1^{x/a_1} \cdots \int_1^{x/(a_1\cdots a_{k-1})} 1 \ da_k \cdots da_1 + E_k(x) = \\ &= x \cdot \sum_{n=1}^{k} \frac{\ln^{k-n}(x)(-1)^{n+1}}{(k-n)!} + (-1)^k + E_k(x) \qquad (7.3) \\ &= W_k(x) + E_k(x), \qquad (7.4) \end{aligned}$$

e finalmente à mais completa descrição que, apesar de passível de obtenção elementar, alcançaremos pelo cálculo de resíduos de uma função complexa:

$$D_k^*(x) = W_k(x) + Y_k(x) + \Delta_k^*(x), \tag{7.5}$$

sendo os $Y_k(x)$ e $\Delta_k^*(x)$ definidos na próxima seção.

A identidade (7.1) e a aproximação (7.2) rendem

$$J(x) \approx \frac{x}{\ln(x)} \cdot g_h(-\ln x),$$

onde

$$g_h(-\ln x) = -\sum_{1\leq k\leq h} \frac{(-\ln x)^k}{k!}$$

e $g_h(t)$ é polinômio de Taylor de grau $\lfloor h \rfloor$ de $1 - e^t$, o que implica $g_h(x) \to 1$ se $h, x \to \infty,\ h \geq \lfloor \log_2(x) \rfloor$, e portanto somos levados a considerar

$$J(x) \approx \frac{x}{\ln(x)}.$$

Por outro lado, ao combinarmos (7.1) com a aproximação (7.3) obtemos

$$\begin{aligned} J(x) &= \sum_{1\leq k\leq h} \frac{(-1)^{k+1}}{k} \left(x \cdot \sum_{n=1}^{k} \frac{\ln^{k-n}(x)(-1)^{n+1}}{(k-n)!} + (-1)^k + E_k(x) \right) = \\ &= -\sum_{1\leq k\leq h} \frac{1}{k} + +A_1(x,h) + A_2(x,h). \end{aligned}$$

O primeiro termo cresce como $\ln h$ e é bem compreendido. O segundo, o qual chamaremos **termo principal** e denotaremos por $A_1(x,h)$, é

$$\begin{aligned} A_1(x,h) &= x \cdot \sum_{1\leq k\leq h} \frac{(-1)^{k+1}}{k} \sum_{n=1}^{k} \frac{\ln^{k-n}(x)(-1)^{n+1}}{(k-n)!} \\ &= x \cdot \sum_{1\leq n\leq h} (-1)^{n+1} \sum_{n\leq k\leq h} \frac{\ln^{k-n}(x)(-1)^{k+1}}{k(k-n)!} \\ &= \sum_{1\leq n\leq h} \frac{x}{\ln^n(x)} g_{h,n}(-\ln x), \end{aligned}$$

sendo $g_{h,n}(t)$ polinômio de Taylor de grau $\lfloor h \rfloor$ de

$$V_n(t) = (n-1)! + (-1)^n \left(e^t \sum_{k=1}^{n} \frac{(n)_k}{n} t^{n-k} (-1)^{k+1} \right), \tag{7.6}$$

pois

$$V_1(t) = 1 - e^t$$

e

$$\begin{aligned} V_{n+1}(t) &= (-1)^{n+1} \sum_{n+1\le k<\infty} \frac{t^k}{k(k-n-1)!} = (-1)^{n+1} \sum_{n\le k<\infty} \frac{k-n}{k(k-n)!} t^k = \\ &= (-1)^{n+1} \left(\sum_{n\le k<\infty} \frac{t^k}{(k-n)!} - n \sum_{n\le k<\infty} \frac{t^k}{k(k-n)!} \right) \\ &= (-1)^{n+1} t^n e^t + n V_n(t), \end{aligned}$$

de onde (7.10) segue por indução.

Fica claro que $g_{h,n}(t) \to (n-1)!$ quando $t \to -\infty$ e chegamos à aproximação

$$A_1(x,h) \approx \frac{x}{\ln(x)} + \frac{x}{\ln^2(x)} + \frac{2x}{\ln^3(x)} + \frac{6x}{\ln^4(x)} + \cdots + \frac{(\lfloor h \rfloor - 1)! x}{\ln^{\lfloor h \rfloor}(x)}$$

Podemos[1] ser bem mais precisos que isso para $A_1(x,h)$, pois é fácil mostrar a igualdade $\frac{\partial A_1(x,h)}{\partial x} = \sum_{1\le j\le h} \frac{(-\ln(x))^{j-1}}{j!}$. Em particular, $\frac{\partial A_1(x,h)}{\partial x} \to 1/\ln(x) - 1/x\ln(x)$, quando $h \to \infty$.

O terceiro é

$$A_2(x,h) = \sum_{1\le k\le h} \frac{(-1)^{k+1}}{k} E_k(x),$$

que reúne os termos de erro originados da aproximação das funções decompositoras pela integral (7.3). Para obtermos resultados ainda mais precisos acerca de $J(x)$, nos será necessário apelar à aproximação (7.5) obtida pelo cálculo de resíduos. A próxima seção se dedicará à obtenção desta aproximação e a uma caracterização bem mais precisa de $J(x)$.

Aproximações do cálculo de resíduos

É sabido que os resíduos de $(\zeta(s)-1)^k x^s/s$ são tanto da forma[2] $D_k^*(x) - \Delta_k^*(x)$, $\Delta_k^*(x) = o(x)$ como da forma $x \cdot P_{k-1}(\ln(x))$, onde $P_n(t)$ é um polinômio de grau n na variável t (TITCHMARSH, 1986, p. 312-313[3]). Calculemos explicitamente os resíduos.

[1] Esta precisão, muito bem vinda, não pôde ser reproduzida por mim para A_2. Por este motivo, preservamos a exposição da expansão assintótica semiconvergente, pois as mesmas técnicas heurísticas levarão ao principal resutlado do capítulo.

[2] De fato, conjectura-se que $\Delta_k^*(x) = O(x^{(k-1)/(2k)+\epsilon})$, principalmente devido à fórmula de Voronoi do início do século passado e alguns subsequentes trabalhos de Hardy. Esta hipótese é equivalente à hipótese de Lindelöf (TITCHMARSH, 1986, p. 330).

[3] Titchmarsh falava dos semelhantes $D_k(x)$. Os resultados valem analogamente para $D_k^*(x)$.

Nos é útil notar que

$$\zeta(s) - 1 = \frac{1}{s-1} - sA(s), \tag{7.7}$$

onde $A(s) = \int_1^\infty (x - \lfloor x \rfloor) x^{-s-1} dx$ converge para $Re(s) > 0$. Assim

$$(\zeta(s) - 1)^k = \sum_{n=0}^{k} \binom{k}{n} \frac{(-sA(s))^n}{(s-1)^{k-n}},$$

e portanto os tais resíduos são os provenientes dos polos em $s \in \mathbb{C}$ de

$$x^s \sum_{n=0}^{k-1} \binom{k}{n} \frac{(-1)^n s^{n-1} A^n(s)}{(s-1)^{k-n}}.$$

Tratemos separadamente do caso $n = 0$. Devemos, pois, tratar dos resíduos de $x^s/s(s-1)^k$. O caso $s = 0$ rende imediatamente o resíduo $(-1)^k$. O caso $s = 1$ depende do cálculo de

$$\frac{1}{(k-1)!} \frac{d^{k-1} x^s/s}{d^{k-1}}(1).$$

Como

$$\begin{aligned} \frac{d^{k-1} x^s/s}{d^{k-1}} &= \sum_{\substack{a+b=k-1 \\ a,b \geq 0, \text{ com ordem}}} \frac{(k-1)!}{a!b!} \ln^a(x) x^s \frac{(-1)^b b!}{s^{b+1}} \\ &= \sum_{a=0}^{k-1} \frac{(k-1)!}{a!} \ln^a(x) x^s \frac{(-1)^{k-1-a}}{s^{k-a}}, \end{aligned}$$

esta parte do resíduo se mostra

$$x \sum_{a=0}^{k-1} \frac{\ln^a(x)}{a!} (-1)^{k-1-a},$$

e portanto o resíduo total em $n = 0$ é

$$x \sum_{a=0}^{k-1} \frac{\ln^a(x)}{a!} (-1)^{k-1-a} + (-1)^k,$$

exatamente conforme $W_k(x)$ em (7.3). Podemos assim escrever $D_k^*(x) = W_k(x) + Y_k(x) + \Delta_k^*(x)$, sendo $W_k(x)$ o resíduo dado acima e $Y_k(x)$ igual ao restante dos resíduos em $n =$

$1, \cdots, k-1$. Desta forma, nota-se que $E_k(x) = Y_k(x) + \Delta_k^*(x)$. Encontremos explicitamente a representação de $Y_k(x)$. Nos casos $n = 1, \cdots k-1$ os resíduos são todos provenientes de $s = 1$, e tomam a forma

$$\sum_{n=1}^{k-1} \frac{(-1)^n \binom{k}{n}}{(k-1-n)!} \frac{d^{k-1-n} x^s s^{n-1} A^n(s)}{ds^{k-1-n}}(1). \tag{7.8}$$

Se $h(t) = f_1(t) f_2(t) f_3(t)$, certamente sua k-ésima derivada em t depende de todas as soluções em $a\ b,\ c \in \mathbb{N}$ de

$$h^{(k)}(t) = \sum_{\substack{a+b+c=k \\ a,\ b,\ c\ \geq 0}} f_1^{(a)}(t) f_2^{(b)}(t) f_3^{(c)}(t) \frac{k!}{a!b!c!}.$$

Antes de aplicarmos isto para (7.8), devemos compreender a k-ésima derivada do termo $A^n(s)$. Analogamente ao processo exposto acima, será

$$\begin{aligned} \frac{d^k A^n(s)}{ds^k} &= \sum_{t_1+\cdots+t_n=k} A^{(t_1)}(s) \cdot \ldots \cdot A^{(t_n)}(s) \frac{k!}{t_1! \cdot \ldots \cdot t_n!} \\ &= \sum_{\substack{l_1 t_1 + \cdots + l_w t_w = k \\ l_1+\cdots+l_w=n}} A^{l_1}_{(t_1)}(s) \cdot \ldots \cdot A^{l_w}_{(t_w)}(s) \frac{k!}{(t_1!)^{l_1} \cdot \ldots \cdot (t_w!)^{l_w}} \frac{n!}{l_1! \cdot \ldots \cdot l_w!} \end{aligned}$$

onde $t_i \neq t_j$, se $i \neq j$, e $l_i \geq 1,\ t_i \geq 0, \forall i$, sem ordem, afinal organizamos a partição já contando a multiplicidade dos elementos. Conclui-se que

$$\begin{aligned} &\frac{d^{k-1-n} x^s s^{n-1} A^n(s)}{ds^{k-1-n}}(t) \\ &= \sum_{\substack{a+b+c=k-1-n \\ a,\ b,\ c\ \geq 0,\ b \leq n-1}} \left[\ln^a(x) x^t t^{n-1-b} (n-1) \cdot \ldots \cdot (s-b) \frac{d^c A^n(s)}{ds^c}(t) \frac{(k-1-n)!}{a!b!c!} \right] \end{aligned}$$

e portanto, por (7.8), obtemos finalmente a representação[4]

$$\begin{aligned} &Y_k(x) = \\ &x \sum_{n=1}^{k-1} (-1)^n \binom{k}{n} \sum_{a=0}^{k-1-n} \frac{\ln^a(x)}{a!} \sum_{c=0}^{k-1-n-a} \sum_{\substack{l_1 t_1 + \cdots + l_w t_w = c \\ l_1+\cdots+l_w=n}} \frac{\gamma_{t_1}^{l_1} \cdot \ldots \cdot \gamma_{t_w}^{l_w} n!}{(t_1!)^{l_1} l_1! \cdot \ldots \cdot (t_w!)^{l_w} l_w!} \binom{n-1}{k-1-n-a-c} \end{aligned} \tag{7.9}$$

[4] É importante notar que na fórmula apresentada a última combinação ora mostra-se nula. Poderíamos explicitar a condição de c majorar $k - 2n - a$. Reservamos essa notação, porém, para uma futura simplificação em índice v das somas j a se definir.

onde fizemos

$$\gamma_k \stackrel{\text{def}}{=} A^{(k)}(1) = \int_1^\infty \frac{(x - \lfloor x \rfloor)}{x^2}(-\ln x)^k dx$$

derivando sob o sinal da integral.

Aproximação aprimorada da contagem de primos

Os resultados contidos nesta secção partem da fórmula (7.1) e da caracterização $D_k^*(x) = W_k(x) + Y_k(x) + \Delta_k^*(x)$ obtida na seção anterior. Havíamos colocado

$$J(x) = -\sum_{1\leq k\leq h} \frac{1}{k} + A_1(x,h) + A_2(x,h),$$

sendo $A_1(x,h)$ o **termo principal**

$$A_1(x,h) = \sum_{1\leq n\leq h} \frac{x}{\ln^n(x)} g_{h,n}(-\ln x),$$

com $g_{h,n}(t)$ polinômio de Taylor de grau $\lfloor h \rfloor$ de

$$V_n(t) = (n-1)! + (-1)^n \left(e^t \sum_{k=1}^{n} \frac{(n)_k}{n} t^{n-k}(-1)^{k+1} \right). \tag{7.10}$$

Conforme estabelecemos, $E_k(x) = Y_k(x) + \Delta_k^*(x)$, e portanto

$$A_2(x,h) = \sum_{1\leq k\leq h} \frac{(-1)^{k+1}}{k} E_k(x) = B_1(x,h) + B_2(x,h),$$

onde[5]

$$B_1(x,h) = \sum_{2\leq k\leq h} \frac{(-1)^{k+1}}{k} Y_k(x) \quad e \quad B_2(x,h) = \sum_{1\leq k\leq h} \frac{(-1)^{k+1}}{k} \Delta_k^*(x)$$

É importante notar que $B_2(x) = O(x^{\frac{k-1}{2k}+\epsilon}),\ \forall \epsilon > 0$ é equivalente à hipótese de Lindelöf (TITCHMARSH, 1986, p. 330). Trataremos deste termo posteriormente. Nesta seção, nos dedicaremos à uma compreensão mais sólida do termo $B_1(x)$. De fato, como $\ln(\zeta(s)) = s\int_1^\infty J(x)x^{-s-1}dx$ e os resultados clássicos de Riemann, von Mangoldt e Hadamard fazem $J(x) = Li(x) + O(x^{\alpha+\epsilon}),\ \forall \epsilon > 0$, onde $\alpha = \sup_{\rho:\zeta(\rho)=0} Re(\rho)$, a hipótese de Riemann

[5] Notemos que $B_1(x)$ parte de $k = 2$, afinal $Y_1(x) \equiv 0$.

nos leva a esperar de $B_1(x)$ um comportamento da forma[6] $O(x^{1/2}+\epsilon)$ ou $O(x^{\epsilon})\,\forall\epsilon>0$, afinal $Li(x)$ tem expansão assintótica divergente $x(\ln^{-1}(x)+\cdots+(n-1)!\ln^{-n}(x))+\cdots$. Contemplemos, pois, $B_1(x)$. Chamemo-lo **primeiro termo de erro** e o estudemos.

Cálculo heurístico do primeiro termo de erro

Heurístico, pois simplesmente ignoremos duas caudas no processo, termos de erro adicionais.

Invertendo as somas em a e n na representação (7.9)de $Y_k(x)$ para evidenciar a forma $x\cdot P_{k-2}(\ln(x))$, onde $P_k(t)$ é algum polinômio de grau k na variável t, obtemos

$$Y_k(x)=$$
$$x\sum_{a=0}^{k-2}\frac{\ln^a(x)}{a!}\sum_{n=1}^{k-1-a}n!(-1)^n\binom{k}{n}\sum_{c=0}^{k-1-n-a}\sum_{\substack{l_1t_1+\cdots+l_wt_w=c\\ l_1+\cdots+l_w=n}}\frac{\gamma_{t_1}^{l_1}\cdot\ldots\cdot\gamma_{t_w}^{l_w}}{(t_1!)^{l_1}l_1!\cdot\ldots\cdot(t_w!)^{l_w}l_w!}\binom{n-1}{k-1-n-a-c}.$$

Como tomaremos $B_1(x,h)=\sum_{2\le k\le h}Y_k(x)(-1)^{k+1}/k$, nos será útil reordenar a soma por cortes diagonais, assim como fizemos para $W_k(x)$. Neste caso, a maior potência de $\ln(x)$ é $k-2$, para cada $k\ge 2$; a segunda maior é $k-3$, para cada $k\ge 3$, etc. Escrevemos

$$\begin{aligned}B_1(x,h)&=x\cdot\sum_{2\le v\le h}\sum_{v\le k\le h}\frac{(-1)^{k+1}}{k}\frac{\ln^{k-v}(x)}{(k-v)!}\sum_{n=1}^{v-1}n!\binom{k}{n}\alpha_{v,n}\\&=x\cdot\sum_{2\le v\le h}\sum_{n=1}^{v-1}n!\alpha_{v,n}k(-\ln x,h,n,v),\end{aligned}$$

onde escrevemos

$$\alpha_{v,n}=(-1)^n\sum_{c=0}^{v-1-n}\sum_{\substack{l_1t_1+\cdots+l_wt_w=c\\ l_1+\cdots+l_w=n}}\frac{\gamma_{t_1}^{l_1}\cdot\ldots\cdot\gamma_{t_w}^{l_w}}{(t_1!)^{l_1}l_1!\cdot\ldots\cdot(t_w!)^{l_w}l_w!}\binom{n-1}{v-1-n-c}.$$

e

$$\begin{aligned}k(-\ln x,h,n,v)&=\sum_{v\le k\le h}\frac{(-1)^{k+1}}{k}\binom{k}{n}\frac{\ln^{k-v}(x)}{(k-v)!}\\&=\frac{(-1)^{v+1}}{n!}\sum_{0\le j\le h-v}\frac{(j+v-1)!}{(j+v-n)!j!}(-\ln x)^j\end{aligned}$$

[6] Como o termo que origina o polo em $s=1$ já foi exposto como $A_1(x)$, $B_1(x)$ ou compõe parte dos termos que originam os polos internos da faixa crítica, ou compõe um termo de crescimento $O(x^{\epsilon})\,\forall\epsilon>0$, que cria um polo em $s=0$ anulado pelo termo s fora da integral, como em outros casos de séries de Dirichlet, a exemplo de $\eta(s)$.

Afirmamos que $k(t,h,n,v)$ é polinômio de Taylor de grau $\lfloor h \rfloor - v$ em t da função

$$G(t,n,v) = \frac{(-1)^{v+1}}{n!} e^t \cdot \sum_{i=0}^{n-1} \binom{n-1}{i} (v-1)_i \cdot t^{n-1-i}$$

Realmente, podemos partir da série de potências da função exponencial para construir tanto

$$t^{n-v} \frac{d^{n-1} x^{v-1} e^x}{dx^{n-1}}(t) = \sum_{0 \leq j < \infty} \frac{(j+v-1)!}{(j+v-n)!j!} t^j$$

como

$$\begin{aligned} t^{n-v} \frac{d^{n-1} x^{v-1} e^x}{dx^{n-1}}(t) &= t^{n-v} \cdot \sum_{a+b=n-1} t^{\overset{(a)}{v-1}} e^{\overset{(b)}{t}} \binom{n-1}{a} \\ &= e^t \cdot \sum_{a=0}^{n-1} (n-1)_a t^{n-1-a} \binom{n-1}{a} \end{aligned}$$

.

A seguir escreveremos $G(t,n,v) = k(t,h,n,v) + r_2(t,h,n,v)$, reservando o termo r_2 da cauda para posterior análise. Temos, portanto, que

$$B_1(x,h) = H(-\ln x, h) - R_2(-\ln x, h),$$

onde

$$H(t,h) = x \cdot \sum_{2 \leq v \leq h} \sum_{n=1}^{v-1} n! \alpha_{v,n} G(t,n,v)$$

e

$$R_2(t,h) = x \cdot \sum_{2 \leq v \leq h} \sum_{n=1}^{v-1} n! \alpha_{v,n} r_2(t,h,n,v).$$

Prossigamos a análise a partir de $H(-\ln x, h)$. Evidenciemos das somas de índice n e i as k-ésimas potências de logaritmo em ordem, e cortemos os termos lineares em x. Obtém-se:

$$H(-\ln x, h) = \sum_{2 \leq v \leq h} (-1)^{v+1} \sum_{k=0}^{v-2} (-\ln x)^k \sum_{n=k+1}^{v-1} \alpha_{v,n} \binom{n-1}{n-1-k} (v-1)^{n-1-k}$$

Recolhamos novamente a soma por cortes diagonais. Chegamos à representação

$$H(-\ln x, h) = \sum_{2\leq k\leq h} (-1)^{k+1} \sum_{k\leq v\leq h} \ln^{v-k}(x) \sum_{n=1}^{k-1} \alpha_{v,v-n} \binom{v-1-n}{k-1-n} (v-1)_{k-1-n}$$

Por hora finalizamos as análises de $B_1(x)$ expandindo os $\alpha_{v,v-n}$, de onde obtemos

$$H(-\ln x, h) = \sum_{2\leq k\leq h} \sum_{n=1}^{k-1} (-1)^{n-1} \sum_{c=0}^{n-1} j(-\ln x, h, k, n, c), \tag{7.11}$$

escrevendo[7]

$$j(t,h,k,n,c) = \sum_{\substack{k\leq v\leq h \\ 2n-c\leq v}} t^{v-k} \binom{v-1-n}{k-1-n} (v-1)_{k-1-n} \cdot \sum_{\substack{l_1 t_1+\cdots+l_w t_w=c \\ l_1+\cdots+l_w=v-n}} \frac{\gamma_{t_1}^{l_1} \cdot \ldots \cdot \gamma_{t_w}^{l_w}}{(t_1)!^{l_1} l_1! \cdot \ldots \cdot (t_w)!^{l_w} l_w!} \cdot \binom{v-n-1}{n-1-c} \quad .$$

Estas funções j podem ser inteiramente compreendidas em seu limite em h, conforme desejávamos. Há três anos atrás, me desinteressei deste problema, tendo calculado, no entanto, os primeiros casos, expostos a seguir.

Computação exata dos três primeiros $k = 2, 3, 4$ termos de H através do horizonte $h \to \infty$

Em $k = 1$, não há termo assintótico de $B_1(x, h)$.

Em $k = 2$, temos $n = 1, c = 0$ e

$$j(t,h,2,1,0) = \gamma_0 \sum_{0\leq v\leq h-2} \frac{(-\ln(x)\gamma_0)^v}{(v+1)!},$$

de onde se conclui claramente que

$$\lim_{h\to\infty} j(t,h,2,1,0) = -\frac{1}{x^{\gamma_0}\ln(x)} + \frac{1}{\ln(x)}.$$

Em $k = 3$, temos os casos $n = 1, c = 0$, $n = 2, c = 0$, $n = 2, c = 1$, correspondendo a

$$j(t,h,3,1,0) + j(t,h,3,2,0) + j(t,h,3,2,1) =$$
$$= \gamma_0^2 \sum_{3\leq v\leq h} \frac{(-\gamma_0 \ln(x))^{v-3}}{(v-3)!} + \frac{1}{\ln(x)} \sum_{4\leq v\leq h} \frac{(-\gamma_0 \ln(x))^{v-2}(v-3)}{(v-2)!} - \gamma_1 \sum_{3\leq v\leq h} \frac{(-\gamma_0 \ln(x))^{v-3}}{(v-3)!}$$

[7] Conforme mencionamos na definição das constantes $\alpha_{v,n}$, a combinação ora rende termos nulos, aqui explicitamente cortados pela condição $2n - c \leq v$.

cujos limites são

$$\lim_{h\to\infty}\left(j(t,h,3,1,0)+j(t,h,3,2,0)+j(t,h,3,2,1)\right)=\frac{\gamma_0^2-\gamma_0-\gamma_1}{x^{\gamma_0}}+\frac{1}{\ln(x)}-\frac{1}{x^{\gamma_0}\ln(x)}.$$

Já em $k=4$, temos seis termos, $n=1,c=0$, $n=2,c=0$, $n=2,c=1$, $n=3,c=0$, $n=3,c=1$ e $n=3,c=2$ totalizando

$$\begin{aligned}
&j(t,h,4,1,0)+j(t,h,4,2,0)+j(t,h,4,2,1)+j(t,h,4,3,0)+j(t,h,4,3,1)+j(t,h,4,3,2)=\\
&\quad=\sum_{0\le v\le h-4}\frac{(-\gamma_0\ln(x))^v}{(v)!}(v+2)+\frac{1}{\ln^2(x)}\sum_{2\le v\le h-4}\frac{(-\gamma_0\ln(x))^v}{(v)!}(v-1)^2(v+1)\\
&\quad+\gamma_1\gamma_0\sum_{0\le v\le h-4}\frac{(-\gamma_0\ln(x))^v}{(v)!}(v+3)-\frac{1}{2\ln(x)}\sum_{2\le v\le h-5}\frac{(-\gamma_0\ln(x))^{v+1}}{(v+1)!}v(v-1)\\
&\quad-\gamma_1\gamma_0\ln(x)\sum_{5\le v\le h}\frac{(-\gamma_0\ln(x))^{v-5}}{(v-5)!}-\frac{\gamma_1^2\ln(x)}{2}\sum_{5\le v\le h}\frac{(-\gamma_0\ln(x))^{v-5}}{(v-5)!}\\
&\quad+\frac{\gamma_2}{2}\sum_{4\le v\le h}\frac{(-\gamma_0\ln(x))^{v-4}}{(v-4)!}
\end{aligned}$$

com limite

$$\begin{aligned}
&\lim_{h\to\infty}\left(j(t,h,4,1,0)+j(t,h,4,2,0)+j(t,h,4,2,1)+j(t,h,4,3,0)+j(t,h,4,3,1)+j(t,h,4,3,2)\right)=\\
&\quad=+\left(\frac{1}{x^{\gamma_0}}\left(\gamma_0^3-\frac{\gamma_0^4\ln(x)}{2}+\gamma_0^3\ln(x)-2\gamma_0^2-\frac{\gamma_0}{\ln(x)}-\frac{1}{\ln(x)^2}+3\gamma_1\gamma_0\right.\right.\\
&\quad\left.-\gamma_1\gamma_0^2\ln(x)-\frac{1}{2\ln(x)}+\gamma_0-\frac{\gamma_0^2\ln(x)}{2}-\gamma_1\gamma_0\ln(x)-\frac{\gamma_1^2\ln(x)}{2}+\frac{\gamma_2}{2}\right)\\
&\quad\left.+\frac{1}{\ln^2(x)}+\frac{1}{2\ln(x)}\right).
\end{aligned}$$

Fica assim compreendido que é possível obter informações sobre a função em x $\lim_{h\to\infty}B_1(x,h)$, que pode guardar o segredos da hipótese de Riemann.

8 Conclusão

Esta dissertação desenvolveu com sucesso uma axiomática simples, que conseguiu unir os conceitos aritméticos aos da álgebra linear. As conseqüências desta união são tremendas e só investigamos alguns temas de sua superfície. Isso é evidenciado pelo trabalho estar repleto de sugestões para futuros estudos. Em particular, a teoria supera parcialmente o uso de funções geradoras numéricas, e não exige o estudo delicado de quaisquer regiões de convergência das funções.

A nossa investigação aritmética inicial aparentemente é um trabalho radicalmente original, que é transportado com toda naturalidade para o espaço aritmético, onde podemos aplicar a teoria tão desenvolvida da álgebra linear. O comportamento das álgebras de operações e seus homomorfismos, conforme vimos, guardam informações aritméticas da mais alta importância, que podem ser extraída por métodos diversos, com a vantagem da solidez e naturalidade lógica dos princípios estabelecidos. Esta naturalidade foi a principal responsável pela aparição de resultados relevantes que extrapolaram completamente as intenções do trabalho, como as formas inversas das inversões compositivas, ou ainda os autovetores das matrizes aditivas circulares formarem a matriz de transformada discreta de Fourier de N pontos.

De todos os estudos futuros propostos, talvez o mais importante seja o estudo do grupo fundamental destas álgebras topológicas e de seus homomorfismos, e o estudo de sua monodromia. A aplicação do Teorema da Correspondência de Lefschetz por Grothendiek para analisar algumas séries de Dirichlet, que culminou na prova de Deligne da última conjectura de Weil, deixa evidente a importância da compreensão topológica para estes problemas. Outro estudo importante a se fazer é o estudo do fechamento algébrico do corpo de frações de uma álgebra de operações nilpotentes, que poderia revelar uma teoria espectral mais refinada da álgebra. Também é preciso estudar a álgebra mista de operações, em particular utilizar a análise harmônica sobre grupo compactos para estudar o grupo das operações invertíveis desta álgebra não comutativa.

Referências

[1] BABAI, L.. The Fourier Transform and Equations over finite Groups. Disponível online em https://people.cs.uchicago.edu/ laci/reu02/fourier.pdf . University of Chicago, 2002. Acesso em 15 de Maio de 2022.

[2] EDWARDS, H. M.. *Riemann's Zeta Function*. New York: Academic Press, 1974.

[3] EULER, L. *De seriebus divergentibus.* Primeiro publicado em "Novi Commentarii academiae scientiarum Petropolitanae 5", 1760, p. 205-237; reimpresso em "Opera Omnia: Series 1", Volume 14, p. 585-617. Tradução para o inglês por Alexander Aycock.

[4] FOLLAND, G. B.. *A course in abstract harmonic analysis*. Boca Raton: CRC, 1995.

[5] HARDY, G. H.. *Divergent Series*. Oxford: Clarendon Press, 1949.

[6] HARDY, G. H.; WRIGHT, E. M.. *An Introduction to the Theory of Numbers*. Sexta edição. Revisão: D. R. Heath-Brown e J. H. Silverman. Oxford: University Press, 2008. Original de 1938.

[7] LIMA, E. L.. *Análise Real, volume 1: Funções de Uma Variável*. 12 ed. Rio de Janeiro: IMPA, 2016.

[8] PEIRCE, C. FREGE, G. Peirce, Frege. Coleção "Os Pensadores". Seleção e tradução de Luís Henrique dos Santos. 3ª ed. São Paulo: Abril Cultural, 1983. Os artigos de Frege aqui presentes são: "Sobre uma justificação científica de uma conceitografia", e "Os Fundamentos da Aritmética". Original de 1884.

[9] ROLIM, R. R.. *Preâmbulos aritméticos: da função Zeta às fórmulas explícitas*. João Pessoa: UFPB/CCEN, 2020.

[10] RUSSELL, B. *Introduction to Mathematical Philosophy*. Edição Online Corrigida, 2010, baseada na 2 ed. de Londres, 1920.

[11] SANTOS, M. F.. *Pitágoras e o tema do número*. São Paulo: IBRASA, 2000.

[12] TITCHMARSH, E. C.. *The Theory of the Riemann Zeta-Function*. Segunda edição. Revisão: D. R. Heath-Brown. Oxford: Clarendon Press, 1986.